Stateful Manifest Contracts
(Supplementary Material)

Taro Sekiyama[1] sekiym@jp.ibm.com

Atsushi Igarashi[2] igarashi@kuis.kyoto-u.ac.jp

[1]IBM Research – Tokyo
[2]Graduate School of Informatics, Kyoto University

1 Definition

1.1 Syntax

Variables, Labels, Addresses, Regions, Regions Sets, and Effects

$$\begin{array}{rcl}
x, y, z & ::= & \text{term variables} \\
\ell & ::= & \text{labels} \\
a, b & ::= & \text{memory addresses} \\
r, s, t, u & ::= & \text{region variables} \\
\gamma, \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} & ::= & \{r_1, \ldots, r_n\} \\
\varrho & ::= & \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle
\end{array}$$

Stores

$$\begin{array}{rcl}
\mu & ::= & \{a_1@r_1 \mapsto v_1, \ldots, a_n@r_n \mapsto v_n\}
\end{array}$$

Base Types, Conditions, and Types

$$\begin{array}{rcl}
B & ::= & \mathsf{bool} \mid \mathsf{unit} \mid \ldots \\
A & ::= & \top \mid A, c \\
T & ::= & B \mid x{:}T_1 \to T_2 \mid \{x{:}T \mid c\} \mid \mathsf{Ref}_r\, T \mid \{A_1\}x{:}T\{A_2\}^{\varrho} \mid \forall r. T
\end{array}$$

Constants, Values, Terms, Commands, Computations, and Checking States

$$\begin{array}{rcl}
k & ::= & \mathsf{true} \mid \mathsf{false} \mid () \mid \ldots \\
v & ::= & k \mid \lambda x{:}T.e \mid \langle T_1 \Leftarrow T_2 \rangle^{\ell} \mid \mathsf{do}\, c \mid \lambda r.e \mid a@r \mid T_1 \Leftarrow^{\ell} T_2 : v \\
e & ::= & x \mid v \mid op(e_1, \ldots, e_n) \mid e_1\, e_2 \mid e_1 \mathrel{==} e_2 \mid r \mathrel{==} s \mid e\{r\} \mid \\
 & & \Uparrow\ell \mid \langle\!\langle \{x{:}T \mid c\}, e \rangle\!\rangle^{\ell} \mid \langle \{x{:}T \mid c\}, p, v \rangle^{\ell} \\
d & ::= & \mathsf{ref}_r\, e \mid\, !e \mid e_1 := e_2 \\
c & ::= & \mathsf{return}\, e \mid x \leftarrow e_1; c_2 \mid x \Leftarrow d_1; c_2 \mid \nu r.\, c \mid \mathsf{assert}\,(c_1)^{\ell}; c_2 \mid \langle \mathsf{assert}\,(c_1), p_2 \rangle^{\ell}; c_3 \mid \Uparrow\ell \\
p & ::= & \nu\gamma.\langle \mu \mid c \rangle
\end{array}$$

Evaluation Contexts and Computation Contexts

$$\begin{array}{rcl}
E & ::= & [\,] \mid op(v_1, \ldots, v_n, E, e_1, \ldots, e_n) \mid E\, e_2 \mid v_1\, E \mid E \mathrel{==} e_2 \mid v_1 \mathrel{==} E \mid E\{r\} \mid \langle\!\langle \{x{:}T \mid c_1\}, E \rangle\!\rangle^{\ell} \\
D & ::= & \mathsf{ref}_r E \mid\, !E \mid E := e_2 \mid v_1 := E \\
C^{\mathsf{e}} & ::= & \mathsf{return}\, E \mid x \leftarrow E; c_2 \mid x \Leftarrow D; c_2 \\
C^{\mathtt{l}} & ::= & x \leftarrow \mathsf{do}\,[\,]\,; c_2 \mid \langle \mathsf{assert}\,(c_1),\, \nu\gamma.\langle \mu \mid [\,] \rangle \rangle^{\ell}; c_3
\end{array}$$

Typing Contexts and Store Typing Contexts

$$\begin{array}{rcl}
\Gamma & ::= & \emptyset \mid \Gamma, x{:}T \mid \Gamma, r \\
\Sigma & ::= & \emptyset \mid \Sigma, a@r{:}T
\end{array}$$

Convention. *We assume that term and region variables declared in typing contexts and references of the form $a@r$ declared in store typing contexts are distinct. We use metavariable σ to denote pairs of finite mappings from term variables to terms and from region variables to region variables. We write $\sigma_1 \uplus \sigma_2$ to denote the concatenation of σ_1 and σ_2 with the disjoint domains. We write $dom\,(\mu)$ and $dom\,(\Sigma)$ for the sets of references declared in μ and Σ, respectively. A store typing context Σ identifies an permutation of it (for Lemma 42). We write $\Sigma_1 \subseteq \Sigma_2$ when, for any $a@r \in dom\,(\Sigma_1)$, $a@r \in dom\,(\Sigma_2)$ and $\Sigma_1(a@r) = \Sigma_2(a@r)$. We write γ, r for the disjoint union $\gamma \uplus \{r\}$. We write γ^c for the complement of γ, that is, the set of all regions which do not belong to γ. Moreover, Γ_1, Γ_2 means the concatenation of Γ_1 and Γ_2; the similar notations are applied to Σ and γ.*

We write $fv\,(e)$ for the variable set whose variables are free in term e. A term e is said to be term-closed *if $fv\,(e) = \emptyset$. Similarly, we write $frv\,(e)$ for the region set whose regions are free in term e, and say that a term e is* region-closed *if $frv\,(e) = \emptyset$. Furthermore, $[\,e'/x\,]\,e$ (resp. $[\,s/r\,]\,e$) denotes capture avoiding substitution of e' (resp. s) for x (resp. r) in e. A term e identifies an α-equivalent term. These notions and notations are applied to other syntactic categories. Free variable sets of stores, typing contexts, and store typing contexts are given as sets of variables free in values and types mapped by them, respectively. For example, $fv\,(\mu)$ is defined as follows:*

$$fv\,(\mu) \overset{def}{=} \bigcup_{a@r \,\in\, dom\,(\mu)} fv\,(\mu(a@r))$$

The partial order $A_1 \subseteq A_2$ over conditions means that, for any c in A_1, there exist some A and A' such that $A_2 = A, c, A'$. We write $\varrho_1 \cup \varrho_2$ and $\varrho_1 \subseteq \varrho_2$ for the element-wise union and the element-wise comparison of ϱ_1 and ϱ_2, respectively. We write $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \setminus \gamma$ for $\langle \gamma_{\mathtt{r}} \setminus \gamma, \gamma_{\mathtt{w}} \setminus \gamma \rangle$. We write $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \uplus \gamma$ for $\langle \gamma_{\mathtt{r}} \uplus \gamma, \gamma_{\mathtt{w}} \uplus \gamma \rangle$. We write $[\,r/s\,]\,\varrho$ for the element-wise application of substitution $[\,r/s\,]$.

Definition 1 (Partial order on typing context)**.** *We define partial order on typing contexts as follows:*

$$\begin{array}{rcl} \Gamma_1, x{:}T \subseteq \Gamma_2 & \iff & \text{there exist some } \Gamma \text{ and } \Gamma' \text{ such that } \Gamma_2 = \Gamma, x{:}T, \Gamma' \text{ and } \Gamma_1 \subseteq \Gamma \\ \emptyset \subseteq \Gamma_2 & & \end{array}$$

Remark. *We can show that constructs of evaluation context E and command context D are closed under term substitution because variables are not values and so value construction is closed under term substitution (Lemma 1).*

Separation of region variables into abstract ones (put in Γ) and nonabstract ones (put in γ) ensures only abstracted region variables are substituted; this is important to analyze regions and show, say, Lemma 50.

Finally, we introduce syntax sugar:

- $\mathsf{let}\, x = e_1 \,\mathsf{in}\, e_2$ denotes $(\lambda x{:}T.e_2)\, e_1$ for some adequate type T;
- $\mathsf{assert}\,(A)^{\ell}; c$ denotes $\mathsf{assert}\,(c_1)^{\ell}; ...; \mathsf{assert}\,(c_n)^{\ell}; c$ where $A = c_1, ..., c_n$;
- $\mathsf{let}\, x = e; c$ denotes $x \leftarrow \mathsf{do}\,\mathsf{return}\, e; c$;
- $T_1 \rightarrow T_2$ denotes $x{:}T_1 \rightarrow T_2$ where $x \notin fv\,(T_2)$;
- $\{A_1\}T\{A_2\}^{\varrho}$ denotes $\{A_1\}x{:}T\{A_2\}^{\varrho}$ where $x \notin fv\,(A_2)$;

1.2 Semantics

We define the call-by-value operational semantics in the small-step style by giving four relations: reduction relation ($\rightsquigarrow$) over term-closed terms, command relation ($\rightarrowtail$), computation relation ($\longrightarrow$) over pairs of a term-closed store and a term-closed computation, and checking state computation relation ($\longrightarrow$) over pairs of a term-closed store and a term-closed checking state. We write R^* to denote the reflexive and transitive closure of a binary relation R. We write $\mu \mid p_1 \hookrightarrow^* p_2$ when there is a computation sequence $\mu_1 \mid p_1 \hookrightarrow p_2, \mu_1 \mid p_2 \hookrightarrow p_3, ..., \mu_1 \mid p_{n-1} \hookrightarrow p_n$.

Definition 2 (Unguard function)**.** *We define function $ungrd\,(v)$ to peel off reference guards:*

$$\begin{array}{lcl} ungrd\,(a@r) & = & a@r \\ ungrd\,(T_1 \Leftarrow^{\ell} T_2 : v) & = & ungrd\,(v) \end{array}$$

$\boxed{e_1 \rightsquigarrow e_2}$ **Reduction Rules**

$$\frac{}{op(k_1, \ldots, k_n) \rightsquigarrow [\![op]\!](k_1, \ldots, k_n)}\ \textsc{R\_Op} \qquad \frac{}{(\lambda x{:}T.e)\, v \rightsquigarrow [\,v/x\,]\, e}\ \textsc{R\_Beta}$$

$$\frac{ungrd\,(v_1) = ungrd\,(v_2)}{v_1 == v_2 \rightsquigarrow \mathsf{true}}\ \textsc{R\_Eq} \qquad \frac{ungrd\,(v_1) \neq ungrd\,(v_2)}{v_1 == v_2 \rightsquigarrow \mathsf{false}}\ \textsc{R\_NEq} \qquad \frac{}{r == r \rightsquigarrow \mathsf{true}}\ \textsc{R\_REq}$$

$$\frac{r \neq s}{r == s \rightsquigarrow \mathsf{false}}\ \textsc{R\_RNEq} \qquad \frac{}{\langle B \Leftarrow B \rangle^{\ell}\, v \rightsquigarrow v}\ \textsc{R\_Base}$$

$$\frac{y \text{ is a fresh variable}}{\langle x{:}T_{11} \rightarrow T_{12} \Leftarrow x{:}T_{21} \rightarrow T_{22} \rangle^{\ell}\, v \rightsquigarrow \lambda x{:}T_{11}.\mathsf{let}\, y = \langle T_{21} \Leftarrow T_{11} \rangle^{\ell}\, x \,\mathsf{in}\, (\langle T_{12} \Leftarrow [\,y/x\,]\, T_{22} \rangle^{\ell}\, (v\, y))}\ \textsc{R\_Fun}$$

$$\frac{}{\langle T_1 \Leftarrow \{x{:}T_2 \mid c\} \rangle^{\ell}\, v \rightsquigarrow \langle T_1 \Leftarrow T_2 \rangle^{\ell}\, v}\ \textsc{R\_Forget}$$

$$\frac{\forall\, y, T, c.\; T_2 \neq \{y{:}T \mid c\}}{\langle \{x{:}T_1 \mid c_1\} \Leftarrow T_2 \rangle^{\ell}\, v \;\rightsquigarrow\; \langle\!\langle\, \{x{:}T_1 \mid c_1\}, \langle T_1 \Leftarrow T_2 \rangle^{\ell}\, v \,\rangle\!\rangle^{\ell}}\ \textsc{R\_PreCheck}$$

$$\frac{}{\langle\!\langle\, \{x{:}T \mid c\}, v \,\rangle\!\rangle^{\ell} \;\rightsquigarrow\; \langle \{x{:}T \mid c\}, \nu\emptyset.\langle \emptyset \mid [\, v/x \,]\, c \rangle, v \rangle^{\ell}}\ \textsc{R\_Check}$$

$$\frac{\emptyset \mid p \hookrightarrow p'}{\langle \{x{:}T \mid c\}, p, v \rangle^{\ell} \;\rightsquigarrow\; \langle \{x{:}T \mid c\}, p', v \rangle^{\ell}}\ \textsc{R\_Checking}$$

$$\frac{}{\langle \{x{:}T \mid c\}, \nu\gamma.\langle \mu \mid {\Uparrow}\ell' \rangle, v \rangle^{\ell} \;\rightsquigarrow\; {\Uparrow}\ell'}\ \textsc{R\_Blame}$$

$$\frac{}{\langle \{x{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return\,true} \rangle, v \rangle^{\ell} \;\rightsquigarrow\; v}\ \textsc{R\_OK}$$

$$\frac{}{\langle \{x{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return\,false} \rangle, v \rangle^{\ell} \;\rightsquigarrow\; {\Uparrow}\ell}\ \textsc{R\_Fail}$$

$$\frac{}{\langle \mathsf{Ref}_r\, T_1 \Leftarrow \mathsf{Ref}_r\, T_2 \rangle^{\ell}\, v \;\rightsquigarrow\; T_1 \Leftarrow^{\ell} T_2 : v}\ \textsc{R\_Ref}$$

$$\frac{r \neq s}{\langle \mathsf{Ref}_r\, T_1 \Leftarrow \mathsf{Ref}_s\, T_2 \rangle^{\ell}\, v \;\rightsquigarrow\; {\Uparrow}\ell}\ \textsc{R\_RefFail}$$

$$\frac{}{(\lambda r.e)\{s\} \;\rightsquigarrow\; [\, s/r \,]\, e}\ \textsc{R\_RBeta}$$

$$\frac{}{\langle \forall r.\, T_1 \Leftarrow \forall r.\, T_2 \rangle^{\ell}\, v \;\rightsquigarrow\; \lambda r.\langle T_1 \Leftarrow T_2 \rangle^{\ell}\, (v\{r\})}\ \textsc{R\_RFun}$$

$$\frac{y \text{ is a fresh variable} \quad \varrho_2 \subseteq \varrho_1}{\langle \{A_{11}\}x{:}T_1\{A_{12}\}^{\varrho_1} \Leftarrow \{A_{21}\}x{:}T_2\{A_{22}\}^{\varrho_2} \rangle^{\ell}\, v \;\rightsquigarrow\; \mathsf{do\,assert}\,(A_{21})^{\ell};\, y \leftarrow v;\, \mathsf{let}\, x = \langle T_1 \Leftarrow T_2 \rangle^{\ell}\, y;\, \mathsf{assert}\,(A_{12})^{\ell};\, \mathsf{return}\, x}\ \textsc{R\_Hoare}$$

$$\frac{\varrho_2 \not\subseteq \varrho_1}{\langle \{A_{11}\}x{:}T_1\{A_{12}\}^{\varrho_1} \Leftarrow \{A_{21}\}x{:}T_2\{A_{22}\}^{\varrho_2} \rangle^{\ell}\, v \;\rightsquigarrow\; {\Uparrow}\ell}\ \textsc{R\_HoareFail}$$

$\boxed{\mu_1 \mid d_1 \;\rightarrowtail\; \mu_2 \mid c_2}$ **Command Rules**

$$\frac{}{\mu \mid \mathsf{ref}_r v \;\rightarrowtail\; \mu \uplus \{a@r \;\mapsto\; v\} \mid \mathsf{return}\; a@r}\ \textsc{C\_New}$$

$$\frac{}{\mu \mid {!a@r} \;\rightarrowtail\; \mu \mid \mathsf{return}\; \mu(a@r)}\ \textsc{C\_Deref}$$

$$\frac{}{\mu \uplus \{a@r \;\mapsto\; v'\} \mid a@r := v \;\rightarrowtail\; \mu \uplus \{a@r \;\mapsto\; v\} \mid \mathsf{return}\; ()}\ \textsc{C\_Assign}$$

$$\frac{}{\mu \mid {!}(T_1 \Leftarrow^{\ell} T_2 : v) \;\rightarrowtail\; \mu \mid x \Leftarrow {!v};\, \mathsf{return}\; (\langle T_1 \Leftarrow T_2 \rangle^{\ell}\, x)}\ \textsc{C\_GuardDeref}$$

$$\frac{}{\mu \mid (T_1 \Leftarrow^{\ell} T_2 : v_2) := v_1 \;\rightarrowtail\; \mu \mid x \Leftarrow v_2 := (\langle T_2 \Leftarrow T_1 \rangle^{\ell}\, v_1);\, \mathsf{return}\; ()}\ \textsc{C\_GuardAssign}$$

$\boxed{\mu_1 \mid c_1 \;\longrightarrow\; \mu_2 \mid c_2}$ **Computation Rules**

$$\frac{e_1 \;\rightsquigarrow\; e_2}{\mu \mid C^{\mathsf{e}}\,[\, e_1 \,] \;\longrightarrow\; \mu \mid C^{\mathsf{e}}\,[\, e_2 \,]}\ \textsc{C\_Red}$$

$$\frac{\mu_1 \mid c_1 \;\longrightarrow\; \mu_2 \mid c_1'}{\mu_1 \mid x \leftarrow \mathsf{do}\; c_1;\, c_2 \;\longrightarrow\; \mu_2 \mid x \leftarrow \mathsf{do}\; c_1';\, c_2}\ \textsc{C\_Comput}$$

$$\frac{}{\mu \mid C^{\mathsf{e}}\,[\, {\Uparrow}\ell \,] \;\longrightarrow\; \mu \mid {\Uparrow}\ell}\ \textsc{C\_RBlame}$$

$$\frac{}{\mu \mid C^{1}\,[\, {\Uparrow}\ell \,] \;\longrightarrow\; \mu \mid {\Uparrow}\ell}\ \textsc{C\_CBlame}$$

$$\frac{}{\mu \mid x \leftarrow \mathsf{do\,return}\; v_1;\, c_2 \;\longrightarrow\; \mu \mid [\, v_1/x \,]\, c_2}\ \textsc{C\_Return}$$

$$\frac{\mu_1 \mid d_1 \;\rightarrowtail\; \mu_2 \mid c_1}{\mu_1 \mid x \Leftarrow d_1;\, c_2 \;\longrightarrow\; \mu_2 \mid x \leftarrow \mathsf{do}\; c_1;\, c_2}\ \textsc{C\_Command}$$

$$\frac{r \notin \mathit{frv}\,(c_2)}{\mu \mid x \leftarrow (\mathsf{do}\, \nu r.\, c_1);\, c_2 \;\longrightarrow\; \mu \mid \nu r.\, (x \leftarrow \mathsf{do}\; c_1;\, c_2)}\ \textsc{C\_Region}$$

$$\frac{}{\mu \mid \mathsf{assert}\,(c_1)^{\ell};\, c_2 \;\longrightarrow\; \mu \mid \langle \mathsf{assert}\,(c_1), \nu\emptyset.\langle \emptyset \mid c_1 \rangle \rangle^{\ell};\, c_2}\ \textsc{C\_Assert}$$

$$\frac{\mu \mid p_1 \;\hookrightarrow\; p_2}{\mu \mid \langle \mathsf{assert}\,(c_1), p_1 \rangle^{\ell};\, c_2 \;\longrightarrow\; \mu \mid \langle \mathsf{assert}\,(c_1), p_2 \rangle^{\ell};\, c_2}\ \textsc{C\_Checking}$$

$$\frac{}{\mu \mid \langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu \mid \mathsf{return\,true} \rangle \rangle^{\ell};\, c_2 \;\longrightarrow\; \mu \mid c_2}\ \textsc{C\_OK}$$

$$\frac{}{\mu \mid \langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu \mid \mathsf{return\,false} \rangle \rangle^{\ell};\, c_2 \;\longrightarrow\; \mu \mid {\Uparrow}\ell}\ \textsc{C\_Fail}$$

$\boxed{\mu_1 \mid p_1 \;\hookrightarrow\; p_2}$ **Checking State Computation Rules**

$$\frac{\mu \uplus \mu_1 \mid c_1 \;\longrightarrow\; \mu \uplus \mu_2 \mid c_2}{\mu \mid \nu\gamma.\langle \mu_1 \mid c_1 \rangle \;\hookrightarrow\; \nu\gamma.\langle \mu_2 \mid c_2 \rangle}\ \textsc{P\_Comput}$$

$$\frac{}{\mu \mid \nu\gamma.\langle \mu' \mid \nu r.\, c \rangle \;\hookrightarrow\; \nu(\gamma, r).\langle \mu' \mid c \rangle}\ \textsc{P\_Region}$$

Remark. *The rule (*R_Op*) uses a denotation function* $[\![-]\!]$ *to give each primitive operation op a meaning. The requirements to the denotation function are described in Section 1.3.*

1.3 Type System

Notation. *We write $ty\,(k)$ and $ty\,(op)$ for types of constant k and primitive operation op.*

Definition 3 (Term Evaluation)**.** *We write $e_1 \longrightarrow e_2$ if (1) e_1 and e_2 are term-closed and (2) there exist some E, e'_1 and e'_2 such that $e_1 = E[e'_1]$ and $e_2 = E[e'_2]$ and $e'_1 \rightsquigarrow e'_2$.*

Definition 4 (Type Equivalence)**.**

1. *The relation $\Rrightarrow$ over types is defined as follows: $T_1 \Rrightarrow T_2$ iff there exist some T, x, e_1, and e_2 such that $T_1 = [\,e_1/x\,]\,T$ and $T_2 = [\,e_2/x\,]\,T$ and $e_1 \longrightarrow e_2$.*
2. *The* type equivalence $\equiv$ *is the symmetric and transitive closure of $\Rrightarrow$.*

Definition 5 (Assertion Equivalence)**.**

1. *The relation $\Rrightarrow$ over assertion sequences is defined as follows: $A_1 \Rrightarrow A_2$ iff there exist some A, x, e_1, and e_2 such that $A_1 = [\,e_1/x\,]\,A$ and $A_2 = [\,e_2/x\,]\,A$ and $e_1 \longrightarrow e_2$.*
2. *The* assertion equivalence $\equiv$ *is the symmetric and transitive closure of $\Rrightarrow$.*

Definition 6 (Bound Regions)**.** *The function regions, a mapping from typing contexts to sets of regions declared in the typing contexts, is defined as follows:*

$$\begin{array}{lcl} regions\,(\emptyset) & = & \emptyset \\ regions\,(\Gamma, x{:}T) & = & regions\,(\Gamma) \\ regions\,(\Gamma, r) & = & regions\,(\Gamma) \cup \{r\} \end{array}$$

Definition 7 (Restriction of Store Typing Context and Store)**.** *We write $\Sigma|_\gamma$ for the same store typing context as Σ except that the domain is defined for only regions in γ. Formally,*

$$\Sigma|_\gamma = \{a@r \mapsto \Sigma(a@r) \mid a@r \in dom\,(\Sigma) \text{ and } r \in \gamma\}$$

Similarly, we write $\mu|_\gamma$ for the same store as μ except that the domain is defined for only regions in γ.

The type system consists of seven judgments—typing context well-formedness $\Sigma;\gamma \vdash \Gamma$, type well-formedness $\Sigma;\gamma;\Gamma \vdash T$, assertion well-formedness $\Sigma;\gamma;\Gamma \vdash^{\varrho} A$, term typing judgment $\Sigma;\gamma;\Gamma \vdash e : T$, computation typing judgment $\mu;\Sigma;\gamma;\Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$, checking state typing judgment $\mu;\Sigma;\gamma \vdash p : T^{\gamma'}$, and store well-formedness judgment $\gamma \vdash \mu : \Sigma^{\gamma'}$—and one auxiliary judgment, type compatibility $T_1 \parallel T_2$. We show inference rules in what follows.

$\boxed{T_1 \parallel T_2}$ **Compatibility Rules**

$$\frac{}{B \parallel B}\ \textsc{Sim\_Base} \qquad \frac{T_{11} \parallel T_{21} \quad T_{12} \parallel T_{22}}{x{:}T_{11} \to T_{12} \parallel x{:}T_{21} \to T_{22}}\ \textsc{Sim\_Fun} \qquad \frac{T_1 \parallel T_2}{\mathsf{Ref}_r\,T_1 \parallel \mathsf{Ref}_s\,T_2}\ \textsc{Sim\_Ref}$$

$$\frac{T_1 \parallel T_2}{\{x{:}T_1 \mid c_1\} \parallel T_2}\ \textsc{Sim\_RefineL} \qquad \frac{T_1 \parallel T_2}{T_1 \parallel \{x{:}T_2 \mid c_2\}}\ \textsc{Sim\_RefineR}$$

$$\frac{T_1 \parallel T_2}{\{A_{11}\}x{:}T_1\{A_{12}\}^{\varrho_1} \parallel \{A_{21}\}x{:}T_2\{A_{22}\}^{\varrho_2}}\ \textsc{Sim\_Hoare} \qquad \frac{T_1 \parallel T_2}{\forall r.\,T_1 \parallel \forall r.\,T_2}\ \textsc{Sim\_RFun}$$

$\boxed{\Sigma;\gamma \vdash \Gamma}$ **Typing Context Well-Formedness Rules**

$$\frac{}{\Sigma;\gamma \vdash \emptyset}\ \textsc{WF\_Empty} \qquad \frac{\Sigma;\gamma \vdash \Gamma \quad \Sigma;\gamma;\Gamma \vdash T}{\Sigma;\gamma \vdash \Gamma, x{:}T}\ \textsc{WF\_ExtendVar} \qquad \frac{\Sigma;\gamma \vdash \Gamma \quad r \notin \gamma}{\Sigma;\gamma \vdash \Gamma, r}\ \textsc{WF\_ExtendRegion}$$

$\boxed{\Sigma;\gamma;\Gamma \vdash T}$ **Type Well-Formedness Rules**

$$\frac{\Sigma;\gamma \vdash \Gamma}{\Sigma;\gamma;\Gamma \vdash B}\ \textsc{WF\_Base} \qquad \frac{\Sigma;\gamma;\Gamma \vdash T_1 \quad \Sigma;\gamma;\Gamma, x{:}T_1 \vdash T_2}{\Sigma;\gamma;\Gamma \vdash x{:}T_1 \to T_2}\ \textsc{WF\_Fun} \qquad \frac{\Sigma;\gamma;\Gamma \vdash T \quad r \in \gamma \cup regions\,(\Gamma)}{\Sigma;\gamma;\Gamma \vdash \mathsf{Ref}_r\,T}\ \textsc{WF\_Ref}$$

$$\frac{\Sigma;\gamma;\Gamma \vdash T \quad \emptyset;\Sigma;\gamma;\Gamma, x{:}T \vdash c : \{\top\}y{:}\mathsf{bool}\{\top\}^{\langle\emptyset,\emptyset\rangle}}{\Sigma;\gamma;\Gamma \vdash \{x{:}T \mid c\}}\ \textsc{WF\_Refine}$$

$$\frac{\Sigma;\gamma;\Gamma \vdash^{\varrho} A_1 \quad \Sigma;\gamma;\Gamma \vdash T \quad \Sigma;\gamma;\Gamma, x{:}T \vdash^{\varrho} A_2}{\Sigma;\gamma;\Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}}\ \textsc{WF\_Hoare} \qquad \frac{\Sigma;\gamma;\Gamma, r \vdash T}{\Sigma;\gamma;\Gamma \vdash \forall r.\,T}\ \textsc{WF\_RFun}$$

$\boxed{\Sigma; \gamma; \Gamma \vdash^{\varrho} A}$ **Assertion Well-Formedness Rules**

$$\frac{\gamma_{\texttt{r}} \cup \gamma_{\texttt{w}} \ \subseteq \ \gamma \cup \mathit{regions}\,(\Gamma)}{\Sigma; \gamma; \Gamma \ \vdash^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle} \ \top} \ \textsc{WF\_EmptyAssert}$$

$$\frac{\Sigma; \gamma; \Gamma \ \vdash^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle} \ A \quad \emptyset; \Sigma; \gamma; \Gamma \vdash c \ : \ \{A\} x{:}\mathsf{bool}\{\top\}^{\langle \gamma_{\texttt{r}}, \emptyset \rangle}}{\Sigma; \gamma; \Gamma \ \vdash^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle} \ A, c} \ \textsc{WF\_ExtendAssert}$$

$\boxed{\Sigma; \gamma; \Gamma \vdash e \ : \ T}$ **Typing Rules**

$$\frac{\Sigma; \gamma \vdash \Gamma \quad x{:}T \ \in \ \Gamma}{\Sigma; \gamma; \Gamma \vdash x \ : \ T} \ \textsc{T\_Var} \qquad \frac{\Sigma; \gamma \vdash \Gamma}{\Sigma; \gamma; \Gamma \vdash k \ : \ \mathit{ty}\,(k)} \ \textsc{T\_Const}$$

$$\frac{\begin{array}{c} \Sigma; \gamma \vdash \Gamma \quad \mathit{ty}\,(\mathit{op}) \ = \ x_1{:}T_1 \to \ldots \to x_n{:}T_n \to T \\ \forall\, i \ \in \ \{1, \ \ldots, n\}.\, \Sigma; \gamma; \Gamma \vdash e_i \ : \ [\, e_1/x_1, \ \ldots, e_{i-1}/x_{i-1}\,]\ T_i \end{array}}{\Sigma; \gamma; \Gamma \vdash \mathit{op}(e_1, \ldots, e_n) \ : \ [\, e_1/x_1, \ \ldots, e_n/x_n\,]\ T} \ \textsc{T\_Op}$$

$$\frac{\Sigma; \gamma; \Gamma, x{:}T_1 \vdash e \ : \ T_2}{\Sigma; \gamma; \Gamma \vdash \lambda x{:}T_1.e \ : \ x{:}T_1 \to T_2} \ \textsc{T\_Abs} \qquad \frac{\Sigma; \gamma; \Gamma \vdash T_1 \quad \Sigma; \gamma; \Gamma \vdash T_2 \quad T_1 \parallel T_2}{\Sigma; \gamma; \Gamma \vdash \langle T_1 \Leftarrow T_2 \rangle^{\ell} \ : \ T_2 \to T_1} \ \textsc{T\_Cast}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \ : \ x{:}T_1 \to T_2 \quad \Sigma; \gamma; \Gamma \vdash e_2 \ : \ T_1}{\Sigma; \gamma; \Gamma \vdash e_1\, e_2 \ : \ [\, e_2/x\,]\ T_2} \ \textsc{T\_App} \qquad \frac{\Sigma; \gamma \vdash \Gamma \quad a@r{:}T \ \in \ \Sigma \quad \Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_r\, T}{\Sigma; \gamma; \Gamma \vdash a@r \ : \ \mathsf{Ref}_r\, T} \ \textsc{T\_Address}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \ : \ \mathsf{Ref}_r\, T_1 \quad \Sigma; \gamma; \Gamma \vdash e_2 \ : \ \mathsf{Ref}_s\, T_2 \quad T_1 \parallel T_2}{\Sigma; \gamma; \Gamma \vdash e_1 == e_2 \ : \ \mathsf{bool}} \ \textsc{T\_Eq} \qquad \frac{\emptyset; \Sigma; \gamma; \Gamma \vdash c \ : \ \{A_1\} x{:}T\{A_2\}^{\varrho}}{\Sigma; \gamma; \Gamma \vdash \mathsf{do}\, c \ : \ \{A_1\} x{:}T\{A_2\}^{\varrho}} \ \textsc{T\_Do}$$

$$\frac{\Sigma; \gamma \vdash \Gamma \quad r \ \in \ \gamma \cup \mathit{regions}\,(\Gamma) \quad s \ \in \ \gamma \cup \mathit{regions}\,(\Gamma)}{\Sigma; \gamma; \Gamma \vdash r == s \ : \ \mathsf{bool}} \ \textsc{T\_REq} \qquad \frac{\Sigma; \gamma; \Gamma, r \vdash e \ : \ T}{\Sigma; \gamma; \Gamma \vdash \lambda r.e \ : \ \forall r.T} \ \textsc{T\_RAbs}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e \ : \ \forall s.T \quad r \ \in \ \gamma \cup \mathit{regions}\,(\Gamma)}{\Sigma; \gamma; \Gamma \vdash e\{r\} \ : \ [\, r/s\,]\ T} \ \textsc{T\_RApp} \qquad \frac{\Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash T}{\Sigma; \gamma; \Gamma \vdash \Uparrow\ell \ : \ T} \ \textsc{T\_Blame}$$

$$\frac{\Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash \{x{:}T \mid c\} \quad \Sigma; \gamma; \emptyset \vdash e \ : \ T}{\Sigma; \gamma; \Gamma \vdash \langle\!\langle\, \{x{:}T \mid c\}, e \,\rangle\!\rangle^{\ell} \ : \ \{x{:}T \mid c\}} \ \textsc{T\_WCheck} \quad \frac{\begin{array}{c} \Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash \{x{:}T \mid c\} \quad \Sigma; \gamma; \emptyset \vdash v \ : \ T \\ \emptyset; \Sigma; \gamma \vdash p \ : \ \mathsf{bool}^{\emptyset} \quad \emptyset \mid \nu\emptyset.\langle \emptyset \mid [\, v/x\,]\ c \rangle \hookrightarrow^{*} p \end{array}}{\Sigma; \gamma; \Gamma \vdash \langle \{x{:}T \mid c\}, p, v \rangle^{\ell} \ : \ \{x{:}T \mid c\}} \ \textsc{T\_ACheck}$$

$$\frac{\Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash v \ : \ \mathsf{Ref}_r\, T_2 \quad T_1 \parallel T_2 \quad \Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_r\, T_1}{\Sigma; \gamma; \Gamma \vdash \ T_1 \Leftarrow^{\ell} \ T_2 : v \ : \ \mathsf{Ref}_r\, T_1} \ \textsc{T\_Guard}$$

$$\frac{\Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash v \ : \ T \quad \Sigma; \gamma; \emptyset \vdash \{x{:}T \mid c\} \quad \emptyset \models [\, v/x\,]\ c}{\Sigma; \gamma; \Gamma \vdash v \ : \ \{x{:}T \mid c\}} \ \textsc{T\_Exact}$$

$$\frac{\Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash v \ : \ \{x{:}T \mid c\}}{\Sigma; \gamma; \Gamma \vdash v \ : \ T} \ \textsc{T\_Forget} \qquad \frac{\Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash e \ : \ T_1 \quad T_1 \ \equiv \ T_2 \quad \Sigma; \gamma; \emptyset \vdash T_2}{\Sigma; \gamma; \Gamma \vdash e \ : \ T_2} \ \textsc{T\_Conv}$$

$\boxed{\mu; \Sigma; \gamma; \Gamma \vdash c \ : \ \{A_1\} x{:}T\{A_2\}^{\varrho}}$ **Computation Typing Rules**

$$\frac{\Sigma; \gamma; \Gamma \vdash e \ : \ T \quad \Sigma; \gamma; \Gamma, x{:}T \ \vdash^{\varrho} \ A}{\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{return}\ e \ : \ \{[\, e/x\,]\ A\} x{:}T\{A\}^{\varrho}} \ \textsc{CT\_Return}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \ : \ \{A_1\} y{:}T_1\{A_3\}^{\varrho_1} \quad \emptyset; \Sigma; \gamma; \Gamma, y{:}T_1 \vdash c_2 \ : \ \{A_3\} x{:}T_2\{A_2\}^{\varrho_2} \quad \Sigma; \gamma; \Gamma \vdash \{A_1\} x{:}T_2\{A_2\}^{\varrho_1 \cup \varrho_2}}{\mu; \Sigma; \gamma; \Gamma \vdash y \leftarrow e_1; c_2 \ : \ \{A_1\} x{:}T_2\{A_2\}^{\varrho_1 \cup \varrho_2}} \ \textsc{CT\_Bind}$$

$$\frac{\Sigma; \gamma \vdash \Gamma \quad \mu; \Sigma; \gamma; \emptyset \vdash c_1 \ : \ \{A_1\} y{:}T_1\{A_3\}^{\varrho_1} \quad \emptyset; \Sigma; \gamma; y{:}T_1 \vdash c_2 \ : \ \{A_3\} x{:}T_2\{A_2\}^{\varrho_2} \quad \Sigma; \gamma; \emptyset \vdash \{A_1\} x{:}T_2\{A_2\}^{\varrho_1 \cup \varrho_2}}{\mu; \Sigma; \gamma; \Gamma \vdash y \leftarrow \mathsf{do}\, c_1; c_2 \ : \ \{A_1\} x{:}T_2\{A_2\}^{\varrho_1 \cup \varrho_2}} \ \textsc{CT\_CBind}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e \ : \ T' \quad \emptyset; \Sigma; \gamma; \Gamma, y{:}\mathsf{Ref}_r\, T' \vdash c \ : \ \{A_1\} x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle} \quad \Sigma; \gamma; \Gamma \vdash \{A_1\} x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \cup \{r\} \rangle}}{\mu; \Sigma; \gamma; \Gamma \vdash y \Leftarrow \mathsf{ref}_r\, e; c \ : \ \{A_1\} x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \cup \{r\} \rangle}} \ \textsc{CT\_New}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e \ : \ \mathsf{Ref}_r\, T' \quad \emptyset; \Sigma; \gamma; \Gamma, y{:}T' \vdash c \ : \ \{A_1\} x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle} \quad \Sigma; \gamma; \Gamma \vdash \{A_1\} x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}} \cup \{r\}, \gamma_{\texttt{w}} \rangle}}{\mu; \Sigma; \gamma; \Gamma \vdash y \Leftarrow\, !e; c \ : \ \{A_1\} x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}} \cup \{r\}, \gamma_{\texttt{w}} \rangle}} \ \textsc{CT\_Deref}$$

$$\dfrac{\begin{array}{c}\Sigma; \gamma; \Gamma \vdash e_1 \;:\; \mathsf{Ref}_r\, T' \quad \Sigma; \gamma; \Gamma \vdash e_2 \;:\; T' \\ \emptyset; \Sigma; \gamma; \Gamma, y{:}\mathsf{unit} \vdash c \;:\; \{\top\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} \quad \Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \cup \{r\} \rangle}\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash y \Leftarrow e_1 := e_2; c \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \cup \{r\} \rangle}} \ \textsc{CT\_Assign}$$

$$\dfrac{\mu; \Sigma; \gamma; \Gamma \vdash c \;:\; \{A_1'\}x{:}T\{A_2'\}^{\varrho} \quad A_1' \subseteq A_1 \quad A_2 \subseteq A_2' \quad \Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}}{\mu; \Sigma; \gamma; \Gamma \vdash c \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho}} \ \textsc{CT\_Weak}$$

$$\dfrac{\emptyset; \Sigma; \gamma; \Gamma \vdash c_2 \;:\; \{A_1, c_1\}x{:}T\{A_2\}^{\varrho}}{\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{assert}\,(c_1)^{\ell}; c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho}} \ \textsc{CT\_Assert}$$

$$\dfrac{\begin{array}{c}\Sigma; \gamma \vdash \Gamma \quad \emptyset; \Sigma; \gamma; \emptyset \vdash c_3 \;:\; \{A_1, c_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} \\ \mu; \Sigma; \gamma \vdash p_2 \;:\; \mathsf{bool}^{\gamma_{\mathtt{r}}} \quad \mu \mid \nu\emptyset.\langle \emptyset \mid c_1 \rangle \hookrightarrow^{*} p_2\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash \langle \mathsf{assert}\,(c_1), p_2 \rangle^{\ell}; c_3 \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}} \ \textsc{CT\_Check}$$

$$\dfrac{\Sigma; \gamma \vdash \Gamma \quad \Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}}{\mu; \Sigma; \gamma; \Gamma \vdash \Uparrow\ell \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho}} \ \textsc{CT\_Blame}$$

$$\dfrac{\mu; \Sigma; \gamma, r; \Gamma \vdash c \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}} \quad \Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}}{\mu; \Sigma; \gamma; \Gamma \vdash \nu r.\, c \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho}} \ \textsc{CT\_LetRegion}$$

$$\dfrac{\Sigma; \gamma \vdash \Gamma \quad \mu; \Sigma; \gamma; \emptyset \vdash c \;:\; \{A_{11}\}x{:}T_1\{A_{12}\}^{\varrho} \quad \{A_{11}\}x{:}T_1\{A_{12}\}^{\varrho} \equiv \{A_{21}\}x{:}T_2\{A_{22}\}^{\varrho} \quad \Sigma; \gamma; \emptyset \vdash \{A_{21}\}x{:}T_2\{A_{22}\}^{\varrho}}{\mu; \Sigma; \gamma; \Gamma \vdash c \;:\; \{A_{21}\}x{:}T_2\{A_{22}\}^{\varrho}} \ \textsc{CT\_Conv}$$

$\boxed{\mu; \Sigma; \gamma \vdash p \;:\; T^{\gamma'}}$ **Checking State Typing Rules**

$$\dfrac{\gamma, \gamma' \vdash \mu' \;:\; (\Sigma, \Sigma')^{\gamma'} \quad \mathit{dom}\,(\mu') \;=\; \mathit{dom}\,(\Sigma') \quad \mu \uplus \mu'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c' \;:\; \{A_1\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle} \quad \mu \uplus \mu' \models A_1}{\mu; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu' \mid c' \rangle \;:\; T^{\gamma''}} \ \textsc{PT}$$

$\boxed{\gamma \vdash \mu \;:\; \Sigma^{\gamma'}}$ **Store Well-Formedness**

$$\dfrac{\mathit{dom}\,(\mu) \;=\; \mathit{dom}\,(\Sigma|_{\gamma'}) \quad \forall\, a@r \;\in\; \mathit{dom}\,(\mu).\, \Sigma; \gamma; \emptyset \vdash \mu(a@r) \;:\; \Sigma(a@r)}{\gamma \vdash \mu \;:\; \Sigma^{\gamma'}} \ \textsc{WF\_Store}$$

$\boxed{\mu \models A}$ **Successful Assertions**

$$\dfrac{}{\mu \models \top} \ \textsc{OK\_Empty} \qquad \dfrac{\mu \models A \quad \mu \mid \nu\emptyset.\langle \emptyset \mid c \rangle \hookrightarrow^{*} \nu\gamma'.\langle \mu' \mid \mathsf{return\,true} \rangle}{\mu \models A, c} \ \textsc{OK\_ExtendAssert}$$

In what follows, we formalize properties of types of constants and primitive operations to show type soundness.

Definition 8 (Unrefinement)**.** *The function unref, which eliminates outer refinements of an argument type, is defined as follows:*

$$\begin{array}{lcll} \mathit{unref}\,(\{x{:}T \mid c\}) & = & \mathit{unref}\,(T) & \\ \mathit{unref}\,(T) & = & T & (\mathit{if}\ T \;\neq\; \{x{:}T' \mid c\}\ \mathit{for\ any}\ x,\, T',\ \mathit{and}\ c) \end{array}$$

Definition 9 (Refinements)**.** *We define function refines, a map from types to refinements, as follows:*

$$\begin{array}{lcl} \mathit{refines}\,(\{x{:}T \mid c\}) & = & \{\lambda x{:}T.\mathsf{do}\, c\} \cup \mathit{refines}\,(T) \\ \mathit{refines}\,(T) & = & \emptyset \quad (\mathit{if}\ T \;\neq\; \{x{:}T' \mid c\})\ \mathit{for\ any}\ x,\, T',\ \mathit{and}\ c) \end{array}$$

We write $\models v \;:\; T$ *if, for any* $\lambda x{:}T'.\mathsf{do}\, c \;\in\; \mathit{refines}\,(T)$, $\emptyset \mid \nu\emptyset.\langle \emptyset \mid [\,v/x\,]\, c \rangle \hookrightarrow^{*} \nu\gamma.\langle \mu \mid \mathsf{return\,true} \rangle$.

Assumption (Constants and Operations)**.** *We assume that, for each base type* B*, there exists the set* $\mathcal{K}(B)$ *of constants of* B*. In particular,* $\mathcal{K}(\mathsf{bool}) = \{\mathsf{true}, \mathsf{false}\}$ *and* $\mathcal{K}(\mathsf{unit}) = \{()\}$*. Any constant belongs to exactly one constant set* $\mathcal{K}(B)$*.*

We assume that, for any k *and* op*,* $\mathit{ty}\,(k)$ *and* $\mathit{ty}\,(op)$ *are well formed in the empty store typing context, the empty region set, and the empty typing context. Also, we suppose that constant* k *satisfies the refinement contract of its type; formally,* $\models k \;:\; \mathit{ty}\,(k)$ *holds. Moreover, we suppose that* $\mathit{unref}\,(\mathit{ty}\,(k)) \;=\; B$ *for any* $k \;\in\; \mathcal{K}(B)$ *and that, for any argument type* T *of an operation* op*,* $\mathit{unref}\,(T) \;=\; B$ *for some* B*. When given constants* k_i *satisfying contracts in argument types of* $\mathit{ty}\,(op)$*, the denotation* $[\![op]\!](k_1, \ldots, k_n)$ *satisfies the contracts of the range type of* $\mathit{ty}\,(op)$*; conversely, when values that do not satisfy the conditions above are passed,* $[\![op]\!](k_1, \ldots, k_n)$ *is undefined.*

1.4 Contextual Equivalence

Contexts

$$\begin{array}{lcl}
K^{\mathsf{e}} & = & [\,]_i \mid x \mid k \mid op(K_1^{\mathsf{e}}, \ldots, K_n^{\mathsf{e}}) \mid \lambda x{:}K^{\mathsf{T}}.K^{\mathsf{e}} \mid \langle K_1^{\mathsf{T}} \Leftarrow K_2^{\mathsf{T}} \rangle^{\ell} \mid K_1^{\mathsf{e}}\, K_2^{\mathsf{e}} \mid \lambda r.K^{\mathsf{e}} \mid K^{\mathsf{e}}\{r\} \mid K_1^{\mathsf{e}} = K_2^{\mathsf{e}} \mid r = s \mid \mathsf{do}\, K^{\mathsf{c}} \\
K^{\mathsf{d}} & = & \mathsf{ref}_r K^{\mathsf{e}} \mid {!K^{\mathsf{e}}} \mid K_1^{\mathsf{e}} := K_2^{\mathsf{e}} \\
K^{\mathsf{c}} & = & [\,]_i \mid \mathsf{return}\, K^{\mathsf{e}} \mid x \leftarrow K_1^{\mathsf{e}}; K_2^{\mathsf{c}} \mid x \Leftarrow K_1^{\mathsf{d}}; K_2^{\mathsf{c}} \mid \nu r.\, K^{\mathsf{c}} \mid \mathsf{assert}\,(K_1^{\mathsf{c}})^{\ell}; K_2^{\mathsf{c}} \\
K^{\mathsf{T}} & = & B \mid x{:}K_1^{\mathsf{T}} \to K_2^{\mathsf{T}} \mid \{x{:}K^{\mathsf{T}} \mid K^{\mathsf{c}}\} \mid \mathsf{Ref}_r K^{\mathsf{T}} \mid \{K_1^{\mathsf{A}}\}x{:}K^{\mathsf{T}}\{K_2^{\mathsf{A}}\}^{\varrho} \mid \forall r.K^{\mathsf{T}} \\
K^{\mathsf{A}} & = & \top \mid K^{\mathsf{A}}, K^{\mathsf{c}}
\end{array}$$

Notation. *We write $\mu \mid p \not\hookrightarrow$ when $\mu \mid p \hookrightarrow p'$ is not derived for any p'.*

Definition 10 (Observation)**.** *We write*

- *$c \mid \Uparrow\ell$ to denote $\emptyset \mid \nu\emptyset.\langle \emptyset \mid c \rangle \hookrightarrow^* \nu\gamma.\langle \mu \mid \Uparrow\ell \rangle$ for some γ and μ; and*
- *$c \mid \mathsf{stuck}$ to denote $\emptyset \mid \nu\emptyset.\langle \emptyset \mid c \rangle \hookrightarrow^* p$ for some p such that*
  - *$p \neq \nu\gamma.\langle \mu \mid \mathsf{return}\, v \rangle$ for any γ, μ, and v;*
  - *$p \neq \nu\gamma.\langle \mu \mid \Uparrow\ell \rangle$ for any γ, μ, and ℓ; and*
  - *$\emptyset \mid p \not\hookrightarrow$.*

Definition 11 (Observational Equivalence)**.** *We write $c_1 \Downarrow c_2$ when*

- *$c_1 \mid \Uparrow\ell$ iff $c_2 \mid \Uparrow\ell$ for any ℓ; and*
- *$c_1 \mid \mathsf{stuck}$ iff $c_2 \mid \mathsf{stuck}$.*

Remark. *Observational equivalence does not deal with whether computations terminate at values because it reduces to whether computations terminate at exceptions.*

Definition 12 (Contextual Equivalence)**.** *Computations c_1 and c_2 are contextually equivalent at $\{A_1\}x{:}T_1\{A_2\}^{\varrho}$ under γ and Γ, written as $\gamma; \Gamma \vdash c_1 =_{\mathtt{ctx}} c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$, when:*

1. *$\emptyset; \emptyset; \gamma; \Gamma \vdash c_1 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$;*
2. *all free term and region variables in c_2 are contained by Γ and γ; and*
3. *for any K^{c} and T', if $\emptyset; \emptyset; \emptyset; \emptyset \vdash K^{\mathsf{c}}[\,c_1\,] \,:\, \{\top\}T'\{\top\}^{\langle \emptyset, \emptyset \rangle}$, then $K^{\mathsf{c}}[\,c_1\,] \Downarrow K^{\mathsf{c}}[\,c_2\,]$.*

1.5 Assertion Elimination

Definition 13 (Image of Regions)**.** *We write $\sigma(\gamma)$ for the image of γ under σ.*

Definition 14 (Closing Substitution and Possible Store)**.** *We write $\Sigma; \gamma; \Gamma \vdash \langle \mu, \sigma \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ when there exist some Σ' and γ' such that:*

- *$\Sigma \subseteq \Sigma'$;*
- *$\gamma \subseteq \gamma'$;*
- *for any $r \in \gamma$, $r \notin dom\,(\sigma)$;*
- *for any $r \in \Gamma$, $\sigma(r) \in \gamma'$;*
- *for any $x{:}T \in \Gamma$, $\Sigma'; \gamma'; \emptyset \vdash \sigma(x) \,:\, \sigma(T)$;*
- *$\gamma' \vdash \mu \,:\, \Sigma'^{\sigma(\gamma_{\mathtt{r}}) \cup \sigma(\gamma_{\mathtt{w}})}$; and*
- *σ maps term variables to values.*

We write $\Sigma; \gamma; \Gamma \vdash \sigma$ when $\Sigma; \gamma; \Gamma \vdash \langle \emptyset, \sigma \rangle^{\langle \emptyset, \emptyset \rangle}$.

Definition 15 (Nested Computation Context)**.** *Nested computation contexts, denoted by $C_{\mathtt{n}}^{\mathsf{c}}$, are defined as follows:*

$$C_{\mathtt{n}}^{\mathsf{c}} ::= [\,] \mid x \leftarrow \mathsf{do}\, C_{\mathtt{n}}^{\mathsf{c}}; c_2$$

Definition 16. *We write $\Sigma; \gamma; \Gamma \vdash \gamma_1 \,\mathsf{disj}\, \gamma_2$ when, for any σ such that $\Sigma; \gamma; \Gamma \vdash \sigma$, $\sigma(\gamma_1) \cap \sigma(\gamma_2) = \emptyset$.*

Remark. *The constraint ($\gamma' \cap regions\,(\Gamma) = \emptyset$) should not be added to show Lemma 113.*

$\boxed{\Sigma; \gamma; \Gamma \vdash T_1 \sim T_2}$ **Type Rules**

$$\frac{}{\Sigma; \gamma; \Gamma \vdash B \sim B}\ \textsc{AETy\_Base} \qquad \frac{\Sigma; \gamma; \Gamma \vdash T_{11} \sim T_{21} \quad \Sigma; \gamma; \Gamma, x{:}T_{11} \vdash T_{12} \sim T_{22}}{\Sigma; \gamma; \Gamma \vdash x{:}T_{11} \to T_{12} \sim x{:}T_{21} \to T_{22}}\ \textsc{AETy\_Fun}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash T_1 \sim T_2}{\Sigma; \gamma; \Gamma \vdash \mathsf{Ref}_r\, T_1 \sim \mathsf{Ref}_r\, T_2}\ \textsc{AETy\_Ref} \quad \frac{\Sigma; \gamma; \Gamma \vdash T_1 \sim T_2 \quad \emptyset; \Sigma; \gamma; \Gamma, x{:}T_1 \vdash c_1 \sim c_2 \ :\ \{\top\}y{:}\mathsf{bool}\{\top\}^{\langle \emptyset, \emptyset \rangle}}{\Sigma; \gamma; \Gamma \vdash \{x{:}T_1 \mid c_1\} \sim \{x{:}T_2 \mid c_2\}}\ \textsc{AETy\_Refine}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash^{\varrho} A_{11} \sim A_{21} \quad \Sigma; \gamma; \Gamma \vdash T_1 \sim T_2 \quad \Sigma; \gamma; \Gamma, x{:}T_1 \vdash^{\varrho} A_{12} \sim A_{22}}{\Sigma; \gamma; \Gamma \vdash \{A_{11}\}x{:}T_1\{A_{12}\}^{\varrho} \sim \{A_{21}\}x{:}T_2\{A_{22}\}^{\varrho}}\ \textsc{AETy\_Hoare}$$

$$\frac{\Sigma; \gamma; \Gamma, r \vdash T_1 \sim T_2}{\Sigma; \gamma; \Gamma \vdash \forall r.\, T_1 \sim \forall r.\, T_2}\ \textsc{AETy\_RFun}$$

$\boxed{\Sigma; \gamma; \Gamma \vdash^{\varrho} A_1 \sim A_2}$ **Assertion Rules**

$$\frac{}{\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} \top \sim \top}\ \textsc{AEAss\_Empty}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A_1 \sim A_2 \quad \emptyset; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ \{A_1\}x{:}\mathsf{bool}\{\top\}^{\langle \gamma_{\mathtt{r}}, \emptyset \rangle}}{\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A_1, c_1 \sim A_2, c_2}\ \textsc{AEAss\_Extend}$$

$\boxed{\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \ :\ T}$ **Term Rules**

$$\frac{x{:}T \in \Gamma}{\Sigma; \gamma; \Gamma \vdash x \sim x \ :\ T}\ \textsc{AETm\_Var} \qquad \frac{}{\Sigma; \gamma; \Gamma \vdash k \sim k \ :\ \mathit{ty}\,(k)}\ \textsc{AETm\_Const}$$

$$\frac{\begin{array}{c} \mathit{ty}\,(\mathit{op}) = x_1{:}T_1 \to \ldots \to x_n{:}T_n \to T \\ \forall\, i \in \{1, \ldots, n\}.\, \Sigma; \gamma; \Gamma \vdash e_{1i} \sim e_{2i} \ :\ [\, e_{11}/x_1, \ldots, e_{1i-1}/x_{i-1} \,]\, T_i \end{array}}{\Sigma; \gamma; \Gamma \vdash \mathit{op}(e_{11}, \ldots, e_{1n}) \sim \mathit{op}(e_{21}, \ldots, e_{2n}) \ :\ [\, e_{11}/x_1, \ldots, e_{1n}/x_n \,]\, T}\ \textsc{AETm\_Op}$$

$$\frac{\Sigma; \gamma; \Gamma, x{:}T_{11} \vdash e_1 \sim e_2 \ :\ T_{12} \quad \Sigma; \gamma; \Gamma \vdash T_{11} \sim T_{21}}{\Sigma; \gamma; \Gamma \vdash \lambda x{:}T_{11}.e_1 \sim \lambda x{:}T_{21}.e_2 \ :\ x{:}T_{11} \to T_{12}}\ \textsc{AETm\_Abs}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash T_{11} \sim T_{21} \quad \Sigma; \gamma; \Gamma \vdash T_{12} \sim T_{22}}{\Sigma; \gamma; \Gamma \vdash \langle T_{11} \Leftarrow T_{12} \rangle^{\ell} \sim \langle T_{21} \Leftarrow T_{22} \rangle^{\ell} \ :\ T_{12} \to T_{11}}\ \textsc{AETm\_Cast}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_{11} \sim e_{21} \ :\ x{:}T_1 \to T_2 \quad \Sigma; \gamma; \Gamma \vdash e_{12} \sim e_{22} \ :\ T_1}{\Sigma; \gamma; \Gamma \vdash e_{11}\, e_{12} \sim e_{21}\, e_{22} \ :\ [\, e_{12}/x \,]\, T_2}\ \textsc{AETm\_App} \quad \frac{a@r{:}T \in \Sigma}{\Sigma; \gamma; \Gamma \vdash a@r \sim a@r \ :\ \mathsf{Ref}_r\, T}\ \textsc{AETm\_Address}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_{11} \sim e_{21} \ :\ \mathsf{Ref}_r\, T_1 \quad \Sigma; \gamma; \Gamma \vdash e_{12} \sim e_{22} \ :\ \mathsf{Ref}_s\, T_2}{\Sigma; \gamma; \Gamma \vdash e_{11} == e_{12} \sim e_{21} == e_{22} \ :\ \mathsf{bool}}\ \textsc{AETm\_Eq} \quad \frac{}{\Sigma; \gamma; \Gamma \vdash r == s \sim r == s \ :\ \mathsf{bool}}\ \textsc{AETm\_REq}$$

$$\frac{\emptyset; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}}{\Sigma; \gamma; \Gamma \vdash \mathsf{do}\, c_1 \sim \mathsf{do}\, c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}}\ \textsc{AETm\_Do} \qquad \frac{\Sigma; \gamma; \Gamma, r \vdash e_1 \sim e_2 \ :\ T}{\Sigma; \gamma; \Gamma \vdash \lambda r.e_1 \sim \lambda r.e_2 \ :\ \forall r.\, T}\ \textsc{AETm\_RAbs}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \ :\ \forall s.\, T}{\Sigma; \gamma; \Gamma \vdash e_1\{r\} \sim e_2\{r\} \ :\ [\, r/s \,]\, T}\ \textsc{AETm\_RApp} \qquad \frac{}{\Sigma; \gamma; \Gamma \vdash \Uparrow\!\ell \sim \Uparrow\!\ell \ :\ T}\ \textsc{AETm\_Blame}$$

$$\frac{\Sigma; \gamma; \emptyset \vdash \{x{:}T_1 \mid c_1\} \sim \{x{:}T_2 \mid c_2\} \quad \Sigma; \gamma; \emptyset \vdash e_1 \sim e_2 \ :\ T_1}{\Sigma; \gamma; \Gamma \vdash \langle\!\langle\, \{x{:}T_1 \mid c_1\}, e_1 \,\rangle\!\rangle^{\ell} \sim \langle\!\langle\, \{x{:}T_2 \mid c_2\}, e_2 \,\rangle\!\rangle^{\ell} \ :\ \{x{:}T_1 \mid c_1\}}\ \textsc{AETm\_WCheck}$$

$$\frac{\Sigma; \gamma; \emptyset \vdash \{x{:}T_1 \mid c_1\} \sim \{x{:}T_2 \mid c_2\} \quad \Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ T_1 \quad \emptyset; \Sigma; \gamma \vdash p_1 \sim p_2 \ :\ \mathsf{bool}^{\emptyset}}{\Sigma; \gamma; \Gamma \vdash \langle \{x{:}T_1 \mid c_1\}, p_1, v_1 \rangle^{\ell} \sim \langle \{x{:}T_2 \mid c_2\}, p_2, v_2 \rangle^{\ell} \ :\ \{x{:}T_1 \mid c_1\}}\ \textsc{AETm\_ACheck}$$

$$\frac{\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ \mathsf{Ref}_r\, T_{12} \quad \Sigma; \gamma; \emptyset \vdash T_{11} \sim T_{21} \quad \Sigma; \gamma; \emptyset \vdash T_{12} \sim T_{22}}{\Sigma; \gamma; \Gamma \vdash T_{11} \Leftarrow^{\ell} T_{12} : v_1 \sim T_{21} \Leftarrow^{\ell} T_{22} : v_2 \ :\ \mathsf{Ref}_r\, T_{11}}\ \textsc{AETm\_Guard}$$

$$\frac{\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ \{x{:}T \mid c\}}{\Sigma; \gamma; \Gamma \vdash v_1 \sim v_2 \ :\ T}\ \textsc{AETm\_Forget}$$

$$\frac{\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ T}{\Sigma; \gamma; \Gamma \vdash v_1 \sim v_2 \ :\ \{x{:}T \mid c\}}\ \textsc{AETm\_Exact} \qquad \frac{\Sigma; \gamma; \emptyset \vdash e_1 \sim e_2 \ :\ T' \quad T' \equiv T}{\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \ :\ T}\ \textsc{AETm\_Conv}$$

$\boxed{\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ T}$ **Computation Rules**

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \;:\; T}{\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{return}\, e_1 \sim \mathsf{return}\, e_2 \;:\; \{[\, e_1/x\,]\, A\} x{:}\, T\{A\}^{\varrho}}\ \textsc{AEC\_Return}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \;:\; \{A_1\} y{:}\, T_1 \{A_3\}^{\varrho_1} \quad \emptyset; \Sigma; \gamma; \Gamma, y{:}\, T_1 \vdash c_1 \sim c_2 \;:\; \{A_3\} x{:}\, T_2\{A_2\}^{\varrho_2}}{\mu; \Sigma; \gamma; \Gamma \vdash y \leftarrow e_1; c_1 \sim y \leftarrow e_2; c_2 \;:\; \{A_1\} x{:}\, T_2 \{A_2\}^{\varrho_1 \cup \varrho_2}}\ \textsc{AEC\_Bind}$$

$$\frac{\mu; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} \;:\; \{A_1\} y{:}\, T_1 \{A_3\}^{\varrho_1} \quad \emptyset; \Sigma; \gamma; y{:}\, T_1 \vdash c_{12} \sim c_{22} \;:\; \{A_3\} x{:}\, T_2 \{A_2\}^{\varrho_2}}{\mu; \Sigma; \gamma; \Gamma \vdash y \leftarrow \mathsf{do}\, c_{11}; c_{12} \sim y \leftarrow \mathsf{do}\, c_{21}; c_{22} \;:\; \{A_1\} x{:}\, T_2 \{A_2\}^{\varrho_1 \cup \varrho_2}}\ \textsc{AEC\_CBind}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \;:\; T' \quad \emptyset; \Sigma; \gamma; \Gamma, y{:}\mathsf{Ref}_r\, T' \vdash c_1 \sim c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}}{\mu; \Sigma; \gamma; \Gamma \vdash y \Leftarrow \mathsf{ref}_r\, e_1; c_1 \sim y \Leftarrow \mathsf{ref}_r\, e_2; c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \cup \{r\} \rangle}}\ \textsc{AEC\_New}$$

$$\frac{\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \;:\; \mathsf{Ref}_r\, T' \quad \emptyset; \Sigma; \gamma; \Gamma, y{:}\, T' \vdash c_1 \sim c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}}{\mu; \Sigma; \gamma; \Gamma \vdash y \Leftarrow\, !e_1; c_1 \sim y \Leftarrow\, !e_2; c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}} \cup \{r\}, \gamma_{\mathtt{w}} \rangle}}\ \textsc{AEC\_Deref}$$

$$\frac{\begin{array}{c}\Sigma; \gamma; \Gamma \vdash e_{11} \sim e_{21} \;:\; \mathsf{Ref}_r\, T' \quad \Sigma; \gamma; \Gamma \vdash e_{12} \sim e_{22} \;:\; T' \\ \emptyset; \Sigma; \gamma; \Gamma, y{:}\mathsf{unit} \vdash c_1 \sim c_2 \;:\; \{\top\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash y \Leftarrow e_{11} := e_{12}; c_1 \sim y \Leftarrow e_{21} := e_{22}; c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \cup \{r\} \rangle}}\ \textsc{AEC\_Assign}$$

$$\frac{\emptyset; \Sigma; \gamma; \Gamma \vdash c_{11} \sim c_{21} \;:\; \{A_1\} y{:}\mathsf{bool}\{\top\}^{\langle \gamma_{\mathtt{r}}, \emptyset \rangle} \quad \emptyset; \Sigma; \gamma; \Gamma \vdash c_{12} \sim c_{22} \;:\; \{A_1, c_{11}\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}}{\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{assert}\,(c_{11})^{\ell}; c_{12} \sim \mathsf{assert}\,(c_{21})^{\ell}; c_{22} \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}}\ \textsc{AEC\_Assert}$$

$$\frac{\begin{array}{c}\emptyset; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} \;:\; \{A_1\} y{:}\mathsf{bool}\{\top\}^{\langle \gamma_{\mathtt{r}}, \emptyset \rangle} \\ \mu; \Sigma; \gamma \vdash p_1 \sim p_2 \;:\; \mathsf{bool}^{\gamma_{\mathtt{r}}} \quad \emptyset; \Sigma; \gamma; \emptyset \vdash c_{12} \sim c_{22} \;:\; \{A_1, c_{11}\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash \langle \mathsf{assert}\,(c_{11}), p_1 \rangle^{\ell}; c_{12} \sim \langle \mathsf{assert}\,(c_{21}), p_2 \rangle^{\ell}; c_{22} \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}}\ \textsc{AEC\_Check}$$

$$\frac{}{\mu; \Sigma; \gamma; \Gamma \vdash \Uparrow\!\ell \sim \Uparrow\!\ell \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho}}\ \textsc{AEC\_Blame}$$

$$\frac{\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \;:\; \{A_1'\} x{:}\, T\{A_2'\}^{\varrho} \quad A_1' \subseteq A_1 \quad A_2 \subseteq A_2'}{\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho}}\ \textsc{AEC\_Weak}$$

$$\frac{\mu; \Sigma; \gamma; \emptyset \vdash c_1 \sim c_2 \;:\; \{A_{11}\} x{:}\, T_1\{A_{12}\}^{\varrho} \quad \{A_{11}\} x{:}\, T_1\{A_{12}\}^{\varrho} \equiv \{A_{21}\} x{:}\, T_2\{A_{22}\}^{\varrho}}{\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \;:\; \{A_{21}\} x{:}\, T_2\{A_{22}\}^{\varrho}}\ \textsc{AEC\_Conv}$$

$$\frac{\mu; \Sigma; \gamma, r; \Gamma \vdash c_1 \sim c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho \uplus \{r\}}}{\mu; \Sigma; \gamma; \Gamma \vdash \nu r.\, c_1 \sim \nu r.\, c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho}}\ \textsc{AEC\_LetRegion}$$

$$\frac{\begin{array}{c}\emptyset; \Sigma; \gamma; \Gamma \vdash c_{12} \sim c_{22} \;:\; \{A_1, c_{11}\} x{:}\, T\{A_2\}^{\varrho} \\ A_1' \subseteq A_1 \quad \varrho' \subseteq \varrho \quad \Sigma; \gamma; \Gamma \vdash^{\varrho'} A_1', c_{11} \\ \forall\, \mu', \sigma'.\, (\Sigma; \gamma; \Gamma \vdash \langle \mu', \sigma' \rangle^{\varrho'} \text{ and } \mu' \models \sigma'(A_1')) \implies \mu' \models \sigma'(c_{11})\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{assert}\,(c_{11})^{\ell}; c_{12} \sim c_{22} \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho}}\ \textsc{AEC\_ElimAssert}$$

$$\frac{\begin{array}{c}\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} \quad \langle \gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}} \rangle \subseteq \varrho \\ \Sigma; \gamma; \Gamma \vdash^{\langle {\gamma_{\mathtt{r}}}', \emptyset \rangle} A \quad \Sigma; \gamma; \Gamma \vdash {\gamma_{\mathtt{r}}}'\, \mathsf{disj}\, \gamma_{\mathtt{w}} \quad y \text{ is a fresh variable}\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash y \leftarrow \mathsf{do}\, c_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim c_2 \;:\; \{A_1, A\} x{:}\, T\{A_2, A\}^{\varrho}}\ \textsc{AEC\_Frame}$$

$$\frac{\begin{array}{c}s \in \gamma \cup \mathit{regions}\,(\Gamma) \quad \Sigma; \gamma; \Gamma \vdash \{A_1\} x{:}\, T\{A_2\}^{\varrho} \\ \mu; \Sigma; \gamma, r; \Gamma, y{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(r =\!= s)\} \vdash c_1 \sim c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho \uplus \{r\}}\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash \nu r.\, \mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathtt{not}\,(r =\!= s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c_1 \sim \nu r.\, \mathsf{let}\, y = \mathsf{true}; c_2 \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho}}\ \textsc{AEC\_RegionNEq1}$$

$$\frac{\begin{array}{c}s \in \gamma \quad \Sigma; \gamma, r; \emptyset \vdash \{A_1'\} x{:}\, T'\{A_2'\}^{\varrho' \uplus \{r\}} \quad \Sigma; \gamma; \emptyset \vdash \{A_1\} x{:}\, T\{A_2\}^{\varrho} \\ \Sigma; \gamma, r \vdash C^{\mathtt{c}}_{\mathtt{n1}} \sim C^{\mathtt{c}}_{\mathtt{n2}} \;:\; \{A_1'\} x{:}\, T'\{A_2'\}^{\varrho' \uplus \{r\}} \Rightarrow \{A_1\} x{:}\, T\{A_2\}^{\varrho \uplus \{r\}} \\ \mu; \Sigma; \gamma, r; y{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(r =\!= s)\} \vdash c_1 \sim c_2 \;:\; \{A_1'\} x{:}\, T'\{A_2'\}^{\varrho' \uplus \{r\}}\end{array}}{\mu; \Sigma; \gamma; \Gamma \vdash \nu r.\, C^{\mathtt{c}}_{\mathtt{n1}}\, [\, \mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathtt{not}\,(r =\!= s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c_1\,] \sim \nu r.\, C^{\mathtt{c}}_{\mathtt{n2}}\, [\, \mathsf{let}\, y = \mathsf{true}; c_2\,] \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho}}\ \textsc{AEC\_RegionNEq2}$$

$\boxed{\Sigma; \gamma \vdash C^{\mathtt{c}}_{\mathtt{n1}} \sim C^{\mathtt{c}}_{\mathtt{n2}} \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho} \Rightarrow \{A_1'\} y{:}\, T'\{A_2'\}^{\varrho'}}$ **Nested Computation Context Rules**

$$\frac{}{\Sigma; \gamma \vdash [\,] \sim [\,] \;:\; \{A_1\} x{:}\, T\{A_2\}^{\varrho} \Rightarrow \{A_1\} x{:}\, T\{A_2\}^{\varrho}}\ \textsc{AECc\_Hole}$$

$$\frac{\begin{array}{c}\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}z{:}T_1\{A_3\}^{\varrho_1} \\ \emptyset; \Sigma; \gamma; z{:}T_1 \vdash c_1 \sim c_2 \;:\; \{A_3\}y{:}T'\{A'_2\}^{\varrho_2} \quad \Sigma; \gamma; \emptyset \vdash \{A'_1\}y{:}T'\{A'_2\}^{\varrho_1 \cup \varrho_2}\end{array}}{\Sigma; \gamma \vdash z \leftarrow \mathsf{do}\; C^{\mathsf{c}}_{\mathtt{n}1}; c_1 \sim z \leftarrow \mathsf{do}\; C^{\mathsf{c}}_{\mathtt{n}2}; c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho_1 \cup \varrho_2}} \text{ AECc\_CBind}$$

$$\frac{\begin{array}{c}\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A''_1\}y{:}T''\{A''_2\}^{\varrho'} \\ A''_1 \subseteq A'_1 \quad A'_2 \subseteq A''_2 \quad \Sigma; \gamma; \emptyset \vdash \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}\end{array}}{\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}} \text{ AECc\_Weak}$$

$$\frac{\begin{array}{c}\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A''_1\}y{:}T''\{A''_2\}^{\varrho'} \\ \{A''_1\}y{:}T''\{A''_2\}^{\varrho'} \equiv \{A'_1\}y{:}T'\{A'_2\}^{\varrho'} \quad \Sigma; \gamma; \emptyset \vdash \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}\end{array}}{\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}} \text{ AECc\_Conv}$$

$$\frac{\begin{array}{c}\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle} \\ \langle {\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}' \rangle \subseteq \varrho' \quad \Sigma; \gamma; \Gamma \vdash^{\langle {\gamma_{\mathtt{r}}}'', \emptyset \rangle} A \quad \Sigma; \gamma; \Gamma \vdash {\gamma_{\mathtt{r}}}'' \,\mathsf{disj}\, {\gamma_{\mathtt{w}}}' \quad z \text{ is a fresh variable}\end{array}}{\Sigma; \gamma \vdash z \leftarrow \mathsf{do}\; C^{\mathsf{c}}_{\mathtt{n}1}; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\; z \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1, A\}y{:}T'\{A'_2, A\}^{\varrho'}} \text{ AECc\_Frame}$$

$\boxed{\mu; \Sigma; \gamma \vdash p_1 \sim p_2 \;:\; T^{\gamma'}}$ **Checking State Rules**

$$\frac{\gamma, \gamma' \vdash \mu'_1 \sim \mu'_2 \;:\; \Sigma, {\Sigma'}^{\gamma'} \quad \mu \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c'_1 \sim c'_2 \;:\; \{A_1\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}}{\mu; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle \sim \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle \;:\; T^{{\gamma_{\mathtt{r}}}''}} \text{ AEP}$$

$\boxed{\gamma \vdash \mu_1 \sim \mu_2 \;:\; \Sigma^{\gamma'}}$ **Store Rules**

$$\frac{\mathit{dom}\,(\mu_1) = \mathit{dom}\,(\mu_2) \quad \mathit{dom}\,(\mu_1) = \mathit{dom}\,(\Sigma|_{\gamma'}) \quad \forall\, a@r \in \mathit{dom}\,(\mu_1).\, \Sigma; \gamma; \emptyset \vdash \mu_1(a@r) \sim \mu_2(a@r) \;:\; \Sigma(a@r)}{\gamma \vdash \mu_1 \sim \mu_2 \;:\; \Sigma^{\gamma'}} \text{ AES}$$

2 Proofs

2.1 Cotermination

Lemma 1 (Value Construction Closed Substitution)**.** *For any v and σ, $\sigma(v)$ is a value.*

Proof. Straightforward by structural induction on v. □

Lemma 2. *If e_1 is not a value and $[\,e_1/x\,]\,e_2$ is, then e_2 is a value.*

Proof. By case analysis on e_2. The only interesting case is $e_2 = y$ for some y. If $x = y$, then $[\,e_1/x\,]\,e_2 = e_1$, which leads to a contradiction from the assumptions that e_1 is not a value and $[\,e_1/x\,]\,e_2$ is. Otherwise, if $x \neq y$, then there is a contradiction because $[\,e_1/x\,]\,e_2$ is a value but $[\,e_1/x\,]\,e_2 = y$ is not. □

Lemma 3. *If $e_1 \longrightarrow e_2$ and $[\,e_1/x\,]\,e$ is a value, then so is $[\,e_2/x\,]\,e$.*

Proof. By Lemmas 2 and 1. □

Lemma 4. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,\mathit{op}(v_1, \ldots, v_n) \rightsquigarrow e$, then $[\,e_2/x\,]\,\mathit{op}(v_1, \ldots, v_n) \rightsquigarrow e$.*

Proof. By Lemma 1, for any i, $[\,e_1/x\,]\,v_i$ and $[\,e_2/x\,]\,v_i$ are values. Note that if $[\,e_1/x\,]\,\mathit{op}(v_1, \ldots, v_n)$ is term-closed, then so is $[\,e_2/x\,]\,\mathit{op}(v_1, \ldots, v_n)$. Since $[\,e_1/x\,]\,\mathit{op}(v_1, \ldots, v_n)$ takes a step, it is found that, for any i, $[\,e_1/x\,]\,v_i = k_i\ (= v_i)$ for some k_i from the assumption of op. Thus, $[\,e_1/x\,]\,\mathit{op}(v_1, \ldots, v_n) = \mathit{op}(k_1, \ldots, k_n) = [\,e_2/x\,]\,\mathit{op}(v_1, \ldots, v_n)$. □

Lemma 5. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,\mathit{op}(v_1, \ldots, v_n) \rightsquigarrow e$, then $[\,e_2/x\,]\,\mathit{op}(v_1, \ldots, v_n) \rightsquigarrow e$.

(2) If $[\,e_2/x\,]\,\mathit{op}(v_1, \ldots, v_2) \rightsquigarrow e$, then $[\,e_1/x\,]\,\mathit{op}(v_1, \ldots, v_2) \rightsquigarrow e$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 4. □

Lemma 6. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,(v_1\, v_2) \rightsquigarrow e$, then $[\,e_2/x\,]\,(v_1\, v_2) \rightsquigarrow [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.*

Proof. By Lemma 1, $[\,e_1/x\,]\,v_1$, $[\,e_2/x\,]\,v_1$, $[\,e_1/x\,]\,v_2$ and $[\,e_2/x\,]\,v_2$ are values. We proceed by case analysis on v_1. Note that v_1 takes the form of either lambda abstraction or cast since $[\,e_1/x\,]\,(v_1\,v_2)$ takes a step and that $[\,e_2/x\,]\,(v_1\,v_2)$ is term-closed since so is $[\,e_1/x\,]\,(v_1\,v_2)$. In the following, let $i \in \{1, 2\}$.

Case $v_1 \;=\; \lambda y{:}T.e'$: Without loss of generality, we can suppose that y is fresh. By (R_Beta),

$$[\,e_i/x\,]\,((\lambda y{:}T.e')\;v_2) \;\rightsquigarrow\; [\,[\,e_i/x\,]\,v_2/y\,]\,[\,e_i/x\,]\,e' = [\,e_i/x\,]\,[\,v_2/y\,]\,e'.$$

Case $v_1 \;=\; \langle B \Leftarrow B\rangle^{\ell}$: Obvious because $[\,e_i/x\,]\,(\langle \mathsf{bool} \Leftarrow \mathsf{bool}\rangle^{\ell}\;v_2) \;\rightsquigarrow\; [\,e_i/x\,]\,v_2$ by (R_Base).

Case $v_1 \;=\; \langle y{:}T_{11} \to T_{12} \Leftarrow y{:}T_{21} \to T_{22}\rangle^{\ell}$: Without loss of generality, we can suppose that y is fresh. By (R_Fun),

$$\begin{array}{l}
[\,e_i/x\,]\,(\langle y{:}T_{11} \to T_{12} \Leftarrow y{:}T_{21} \to T_{22}\rangle^{\ell}\;v_2) \rightsquigarrow \\
\quad \lambda y{:}[\,e_i/x\,]\,T_{11}.\mathsf{let}\,z = \langle [\,e_i/x\,]\,T_{21} \Leftarrow [\,e_i/x\,]\,T_{11}\rangle^{\ell}\;y\;\mathsf{in}\;\langle [\,e_i/x\,]\,T_{12} \Leftarrow [\,z/y\,]\,[\,e_i/x\,]\,T_{22}\rangle^{\ell}\,([\,e_i/x\,]\,v_2\,z) \\
= [\,e_i/x\,]\,(\lambda y{:}T_{11}.(\lambda z{:}T_{21}.\langle T_{12} \Leftarrow [\,z/y\,]\,T_{22}\rangle^{\ell}\,(v_2\,z))\,(\langle T_{21} \Leftarrow T_{11}\rangle^{\ell}\;y))
\end{array}$$

for some fresh variable z.

Case $v_1 \;=\; \langle T_1 \Leftarrow \{y{:}T_2 \mid c_2\}\rangle^{\ell}$: By (R_Forget),

$$[\,e_i/x\,]\,(\langle T_1 \Leftarrow \{y{:}T_2 \mid c_2\}\rangle^{\ell}\;v_2) \;\rightsquigarrow\; \langle [\,e_i/x\,]\,T_1 \Leftarrow [\,e_i/x\,]\,T_2\rangle^{\ell}\,[\,e_i/x\,]\,v_2 = [\,e_i/x\,]\,(\langle T_1 \Leftarrow T_2\rangle^{\ell}\;v_2).$$

Case $v_1 \;=\; \langle \{y{:}T_1 \mid c_1\} \Leftarrow T_2\rangle^{\ell}$ where $T_2 \;\neq\; \{z{:}T \mid c\}$ for any z, T, and c: By (R_PreCheck),

$$\begin{array}{rcl}
[\,e_i/x\,]\,(\langle \{y{:}T_1 \mid c_1\} \Leftarrow T_2\rangle^{\ell}\;v_2) & \rightsquigarrow & \langle\!\langle\, [\,e_i/x\,]\,\{y{:}T_1 \mid c_1\}, \langle [\,e_i/x\,]\,T_1 \Leftarrow [\,e_i/x\,]\,T_2\rangle^{\ell}\,[\,e_i/x\,]\,v_2 \,\rangle\!\rangle^{\ell} \\
& = & [\,e_i/x\,]\,\langle\!\langle\, \{y{:}T_1 \mid c_1\}, \langle T_1 \Leftarrow T_2\rangle^{\ell}\;v_2 \,\rangle\!\rangle^{\ell}.
\end{array}$$

Case $v_1 \;=\; \langle \mathsf{Ref}_r\,T_1 \Leftarrow \mathsf{Ref}_s\,T_2\rangle^{\ell}$: If $r \;=\; s$, then, by (R_Ref),

$$\begin{array}{rcl}
[\,e_i/x\,]\,(\langle \mathsf{Ref}_r\,T_1 \Leftarrow \mathsf{Ref}_r\,T_2\rangle^{\ell}\;v_2) & \rightsquigarrow & [\,e_i/x\,]\,T_1 \Leftarrow^{\ell} [\,e_i/x\,]\,T_2 : [\,e_i/x\,]\,v_2 \\
& = & [\,e_i/x\,]\,(T_1 \Leftarrow^{\ell} T_2 : v_2).
\end{array}$$

Otherwise, if $r \;\neq\; s$, then, by (R_RefFail),

$$[\,e_i/x\,]\,(\langle \mathsf{Ref}_r\,T_1 \Leftarrow \mathsf{Ref}_r\,T_2\rangle^{\ell}\;v_2) \;\rightsquigarrow\; \Uparrow\!\ell.$$

Case $v_1 \;=\; \langle \forall r.\,T_1 \Leftarrow \forall r.\,T_2\rangle^{\ell}$: Without loss of generality, we can suppose that r is fresh. By (R_RFun),

$$\begin{array}{rcl}
[\,e_i/x\,]\,(\langle \forall r.\,T_1 \Leftarrow \forall r.\,T_2\rangle^{\ell}\;v_2) & \rightsquigarrow & \lambda r.\langle [\,e_i/x\,]\,T_1 \Leftarrow [\,e_i/x\,]\,T_2\rangle^{\ell}\,[\,e_i/x\,]\,v_2 \\
& = & [\,e_i/x\,]\,(\lambda r.\langle T_1 \Leftarrow T_2\rangle^{\ell}\;v_2).
\end{array}$$

Case $v_1 \;=\; \langle \{A_{11}\}y{:}T_1\{A_{12}\}^{\varrho_1} \;\Leftarrow\; \{A_{21}\}y{:}T_2\{A_{22}\}^{\varrho_2}\rangle^{\ell}$: Without loss of generality, we can suppose that y is fresh. If $\varrho_2 \;\subseteq\; \varrho_1$, then, by (R_Hoare),

$$\begin{array}{l}
[\,e_i/x\,]\,(\langle \{A_{11}\}y{:}T_1\{A_{12}\}^{\varrho_1} \Leftarrow \{A_{21}\}y{:}T_2\{A_{22}\}^{\varrho_2}\rangle^{\ell}\;v_2) \rightsquigarrow \\
\quad \mathsf{do\,assert}\,([\,e_i/x\,]\,A_{21})^{\ell}; z \leftarrow [\,e_i/x\,]\,v_2; \mathsf{let}\,y = \langle [\,e_i/x\,]\,T_1 \Leftarrow [\,e_i/x\,]\,T_2\rangle^{\ell}\,z; \mathsf{assert}\,([\,e_i/x\,]\,A_{12})^{\ell}; \mathsf{return}\,y \\
= [\,e_i/x\,]\,(\mathsf{do\,assert}\,(A_{21})^{\ell}; z \leftarrow v_2; \mathsf{let}\,y = \langle T_1 \Leftarrow T_2\rangle^{\ell}\,z; \mathsf{assert}\,(A_{12})^{\ell}; \mathsf{return}\,y)
\end{array}$$

where z is a fresh variable. Otherwise, if $\varrho_2 \;\not\subseteq\; \varrho_1$, then, by (R_HoareFail),

$$[\,e_i/x\,]\,(\langle \{A_{11}\}y{:}T_1\{A_{12}\}^{\varrho_1} \Leftarrow \{A_{21}\}y{:}T_2\{A_{22}\}^{\varrho_2}\rangle^{\ell}\;v_2) \;\rightsquigarrow\; \Uparrow\!\ell.$$

□

Lemma 7. *Let e_1 and e_2 be terms such that $e_1 \;\longrightarrow\; e_2$.*

(1) If $[\,e_1/x\,]\,(v_1\,v_2) \;\rightsquigarrow\; e$, then $[\,e_2/x\,]\,(v_1\,v_2) \;\rightsquigarrow\; [\,e_2/x\,]\,e'$ for some e' such that $e \;=\; [\,e_1/x\,]\,e'$.

(2) If $[\,e_2/x\,]\,(v_1\,v_2) \;\rightsquigarrow\; e$, then $[\,e_1/x\,]\,(v_1\,v_2) \;\rightsquigarrow\; [\,e_1/x\,]\,e'$ for some e' such that $e \;=\; [\,e_2/x\,]\,e'$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 6.

□

Lemma 8. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,(v_1 \;{=\!=} v_2) \;\rightsquigarrow\; e$, then $[\,e_2/x\,]\,(v_1 \;{=\!=} v_2) \;\rightsquigarrow\; [\,e_2/x\,]\,e'$ for some e' such that $e \;=\; [\,e_1/x\,]\,e'$.*

Proof. By Lemma 1, $[\,e_1/x\,]\,v_1$, $[\,e_2/x\,]\,v_1$, $[\,e_1/x\,]\,v_2$ and $[\,e_2/x\,]\,v_2$ are values. Note that v_1 and v_2 take the forms of either address or guard since $[\,e_1/x\,]\,(v_1 =\!= v_2)$ takes a step and that $[\,e_2/x\,]\,(v_1 =\!= v_2)$ is closed since so is $[\,e_1/x\,]\,(v_1 =\!= v_2)$. We proceed by induciton on the sizes of v_1 and v_2 with case analysis on v_1 and v_2. In the following, let $i \in \{1, 2\}$.

Case $v_1 = a@s$ and $v_2 = b@t$: Obvious because $[\,e_1/x\,]\,(v_1 =\!= v_2) = [\,e_2/x\,]\,(v =\!= v_2) = v_1 =\!= v_2$.

Case $v_1 = T_1 \Leftarrow^{\ell} T_2 : v_1'$: Since $\mathit{ungrd}\,(v_1) = \mathit{ungrd}\,(v_1')$, we finish by the IH.

Case $v_1 = a@s$ and $v_2 = T_1 \Leftarrow^{\ell} T_2 : v_2'$: Since $\mathit{ungrd}\,(v_2) = \mathit{ungrd}\,(v_2')$, we finish by the IH. □

Lemma 9. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,(v_1 =\!= v_2) \rightsquigarrow e$, then $[\,e_2/x\,]\,(v_1 =\!= v_2) \rightsquigarrow [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.

(2) If $[\,e_2/x\,]\,(v_1 =\!= v_2) \rightsquigarrow e$, then $[\,e_1/x\,]\,(v_1 =\!= v_2) \rightsquigarrow [\,e_1/x\,]\,e'$ for some e' such that $e = [\,e_2/x\,]\,e'$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 8. □

Lemma 10. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,(v\{r\}) \rightsquigarrow e$, then $[\,e_2/x\,]\,(v\{r\}) \rightsquigarrow [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.*

Proof. By Lemma 1, $[\,e_1/x\,]\,v$ and $[\,e_2/x\,]\,v$ are values. Note that v takes the form of region abstraction and that $[\,e_2/x\,]\,v$ is term-closed since so is $[\,e_1/x\,]\,v$. Suppose that $v = \lambda s.e'$ where s is fresh. Letting $i \in \{1, 2\}$, by (R_RApp),

$$[\,e_i/x\,]\,((\lambda s.e')\{r\}) \rightsquigarrow [\,r/s\,]\,[\,e_i/x\,]\,e' = [\,e_i/x\,]\,[\,r/s\,]\,e'.$$

□

Lemma 11. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,(v\{r\}) \rightsquigarrow e$, then $[\,e_2/x\,]\,(v\{r\}) \rightsquigarrow [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.

(2) If $[\,e_2/x\,]\,(v\{r\}) \rightsquigarrow e$, then $[\,e_1/x\,]\,(v\{r\}) \rightsquigarrow [\,e_1/x\,]\,e'$ for some e' such that $e = [\,e_2/x\,]\,e'$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 10. □

Lemma 12. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell} \rightsquigarrow e$, then $[\,e_2/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell} \rightsquigarrow [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.*

Proof. Without loss of generality, we can suppose that y is fresh. By Lemma 1, $[\,e_1/x\,]\,v$ and $[\,e_2/x\,]\,v$ are values. Note that $[\,e_2/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell}$ is term-closed since so is $[\,e_1/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell}$. Letting $i \in \{1, 2\}$, by (R_Check),

$$\begin{array}{rcl} [\,e_i/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell} & \rightsquigarrow & \langle [\,e_i/x\,]\,\{y{:}T \mid c\}, \nu\emptyset.\langle \emptyset \mid [\,[\,e_i/x\,]\,v/y\,]\,[\,e_i/x\,]\,c\rangle, [\,e_i/x\,]\,v\rangle^{\ell} \\ & = & [\,e_i/x\,]\,\langle \{y{:}T \mid c\}, \nu\emptyset.\langle \emptyset \mid [\,v/y\,]\,c\rangle, v\rangle^{\ell}. \end{array}$$

Thus, we finish. □

Lemma 13. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell} \rightsquigarrow e$, then $[\,e_2/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell} \rightsquigarrow [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.

(2) If $[\,e_2/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell} \rightsquigarrow e$, then $[\,e_1/x\,]\,\langle\!\langle\,\{y{:}T \mid c\}, v\,\rangle\!\rangle^{\ell} \rightsquigarrow [\,e_1/x\,]\,e'$ for some e' such that $e = [\,e_2/x\,]\,e'$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 12. □

Lemma 14. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,\langle \{y{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell} \rightsquigarrow e$, then $[\,e_2/x\,]\,\langle \{y{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell} \rightsquigarrow [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.*

Proof. By Lemma 1, $[\,e_1/x\,]\,v_1$ and $[\,e_2/x\,]\,v_1$ are values. Note that v_1 takes the form of Boolean values and that $[\,e_2/x\,]\,\langle \{y{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell}$ is term-closed since so is $[\,e_1/x\,]\,\langle \{y{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell}$. By case analysis on v_1. In the following, let $i \in \{1, 2\}$.

Case $v_1 = \mathsf{true}$: By (R_OK), $[\,e_i/x\,]\,\langle \{y{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return\,true}\rangle, v_2\rangle^{\ell} \rightsquigarrow [\,e_i/x\,]\,v_2$.

Case $v_2 = \mathsf{false}$: By (R_Fail), $[\,e_i/x\,]\,\langle \{y{:}T \mid c\}, \nu\gamma.\langle \mu \mid \mathsf{return\,false}\rangle, v_2\rangle^{\ell} \rightsquigarrow \Uparrow\!\ell$. □

Lemma 15. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,\langle\{y{:}T \mid c\}, \nu\gamma.\langle\mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell} \leadsto e$, then $[\,e_2/x\,]\,\langle\{y{:}T \mid c\}, \nu\gamma.\langle\mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell} \leadsto [\,e_2/x\,]\,e'$ for some e' such that $e = [\,e_1/x\,]\,e'$.

(2) If $[\,e_2/x\,]\,\langle\{y{:}T \mid c\}, \nu\gamma.\langle\mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell} \leadsto e$, then $[\,e_1/x\,]\,\langle\{y{:}T \mid c\}, \nu\gamma.\langle\mu \mid \mathsf{return}\,v_1\rangle, v_2\rangle^{\ell} \leadsto [\,e_1/x\,]\,e'$ for some e' such that $e = [\,e_2/x\,]\,e'$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 14. □

Lemma 16. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(\mathsf{ref}_r v) \rightarrowtail \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\,(\mu \uplus \{a@r \mapsto v\})$ and $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(\mathsf{ref}_r v) \rightarrowtail [\,e_2/x\,]\,(\mu \uplus \{a@r \mapsto v\}) \mid [\,e_2/x\,]\,c''$ for some a and c'' such that $c' = [\,e_1/x\,]\,c''$.*

Proof. By Lemma 1, $[\,e_1/x\,]\,v$ and $[\,e_2/x\,]\,v$ are values. Note that $[\,e_2/x\,]\,\mu$ and $[\,e_2/x\,]\,(\mathsf{ref}_r v)$ are term-closed since so are $[\,e_1/x\,]\,\mu$ and $[\,e_1/x\,]\,(\mathsf{ref}_r v)$. Letting $i \in \{1, 2\}$, by (C_New),

$$[\,e_i/x\,]\,\mu \mid [\,e_i/x\,]\,(\mathsf{ref}_r v) \rightarrowtail [\,e_i/x\,]\,(\mu \uplus \{a@r \mapsto v\}) \mid \mathsf{return}\; a@r.$$

for some fresh address a. □

Lemma 17. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(\mathsf{ref}_r v) \rightarrowtail \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\,(\mu \uplus \{a@r \mapsto v\})$ and $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(\mathsf{ref}_r v) \rightarrowtail [\,e_2/x\,]\,(\mu \uplus \{a@r \mapsto v\}) \mid [\,e_2/x\,]\,c''$ for some a and c'' such that $c' = [\,e_1/x\,]\,c''$.

(2) If $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(\mathsf{ref}_r v) \rightarrowtail \mu' \mid c'$, then $\mu' = [\,e_2/x\,]\,(\mu \uplus \{a@s \mapsto v\})$ and $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(\mathsf{ref}_s v) \rightarrowtail [\,e_1/x\,]\,(\mu \uplus \{a@s \mapsto v\}) \mid [\,e_1/x\,]\,c''$ for some a and c'' such that and $c' = [\,e_2/x\,]\,c''$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 16. □

Lemma 18. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(!v) \rightarrowtail \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\,\mu$ and $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(!v) \rightarrowtail [\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,c''$ for some c'' such that $c' = [\,e_1/x\,]\,c''$.*

Proof. By Lemma 1, $[\,e_1/x\,]\,v$ and $[\,e_2/x\,]\,v$ are values. Note that v takes the form of either address or guard since $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(!v)$ takes a step and that $[\,e_2/x\,]\,\mu$ and $[\,e_2/x\,]\,(!v)$ are term-closed since so are $[\,e_1/x\,]\,\mu$ and $[\,e_1/x\,]\,(!v)$. By case analysis on v.

Case $v = a@s$: Obvious by (C_Deref).

Case $v = T_1 \Leftarrow^{\ell} T_2 : v'$: Letting $i \in \{1, 2\}$, by (C_GuardDeref),

$$\begin{array}{rcl} [\,e_i/x\,]\,\mu \mid [\,e_i/x\,]\,(!(T_1 \Leftarrow^{\ell} T_2 : v')) & \longrightarrow & [\,e_i/x\,]\,\mu \mid y \Leftarrow ![\,e_i/x\,]\,v'; \mathsf{return}\,(\langle [\,e_i/x\,]\,T_1 \Leftarrow [\,e_i/x\,]\,T_2\rangle^{\ell}\, y) \\ & = & [\,e_i/x\,]\,\mu \mid [\,e_i/x\,]\,(y \Leftarrow !v'; \mathsf{return}\,(\langle T_1 \Leftarrow T_2\rangle^{\ell}\, y)) \end{array}$$

for some fresh variable y. □

Lemma 19. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(!v) \rightarrowtail \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\,\mu$ and $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(!v) \rightarrowtail [\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,c''$ for some c'' such that $c' = [\,e_1/x\,]\,c''$.

(2) If $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(!v) \rightarrowtail \mu' \mid c'$, then $\mu' = [\,e_2/x\,]\,\mu$ and $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(!v) \rightarrowtail [\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,c''$ for some c'' such that $c' = [\,e_2/x\,]\,c''$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 18. □

Lemma 20. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_1/x\,]\,(v_1 := v_2) \rightarrowtail [\,e_1/x\,]\,\mu_1 \uplus \mu' \mid c'$, then $[\,e_2/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_2/x\,]\,(v_1 := v_2) \rightarrowtail [\,e_2/x\,]\,(\mu_1 \uplus \mu'') \mid [\,e_2/x\,]\,c''$ for some μ'' and c'' such that $\mu' = [\,e_1/x\,]\,\mu''$ and $c' = [\,e_1/x\,]\,c''$.*

Proof. By Lemma 1, $[\,e_1/x\,]\,v_1$, $[\,e_2/x\,]\,v_1$, $[\,e_1/x\,]\,v_2$ and $[\,e_2/x\,]\,v_2$ are values. Note that v_1 takes the form of either address or guard since $[\,e_1/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_1/x\,]\,(v_1 := v_2)$ takes a step and that $[\,e_2/x\,]\,(\mu_1 \uplus \mu_2)$ and $[\,e_2/x\,]\,(v_1 := v_2)$ are term-closed since so are $[\,e_1/x\,]\,(\mu_1 \uplus \mu_2)$ and $[\,e_1/x\,]\,(v_1 := v_2)$. By case analysis on v_1.

Case $v_1 = a@s$: Obvious by (C_Assign).

Case $v_1 = T_1 \Leftarrow^{\ell} T_2 : v_1'$: Letting $i \in \{1,2\}$, by (C_GuardAssign),

$$\begin{array}{rl} & [\,e_i/x\,](\mu_1 \uplus \mu_2) \mid [\,e_i/x\,]((T_1 \Leftarrow^{\ell} T_2 : v_1') :=v_2) \\ \longrightarrow & [\,e_i/x\,](\mu_1 \uplus \mu_2) \mid y \Leftarrow [\,e_i/x\,]\, v_1' :=(\langle [\,e_i/x\,]\, T_2 \Leftarrow [\,e_i/x\,]\, T_1 \rangle^{\ell}\, [\,e_i/x\,]\, v_2); \mathsf{return}\,() \\ = & [\,e_i/x\,](\mu_1 \uplus \mu_2) \mid [\,e_i/x\,](y \Leftarrow v_1' :=(\langle T_2 \Leftarrow T_1 \rangle^{\ell}\, v_2); \mathsf{return}\,()) \end{array}$$

for some fresh variable y. □

Lemma 21. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,](\mu_1 \uplus \mu_2) \mid [\,e_1/x\,](v_1 :=v_2) \rightarrowtail [\,e_1/x\,]\mu_1 \uplus \mu' \mid c'$, then $[\,e_2/x\,](\mu_1 \uplus \mu_2) \mid [\,e_2/x\,](v_1 :=v_2) \rightarrowtail [\,e_2/x\,](\mu_1 \uplus \mu'') \mid [\,e_2/x\,]\, c''$ for some μ'' and c'' such that $\mu' = [\,e_1/x\,]\mu''$ and $c' = [\,e_1/x\,]\, c''$.

(2) If $[\,e_2/x\,](\mu_1 \uplus \mu_2) \mid [\,e_2/x\,](v_1 :=v_2) \rightarrowtail [\,e_2/x\,]\mu_1 \uplus \mu' \mid c'$, then $[\,e_1/x\,](\mu_1 \uplus \mu_2) \mid [\,e_1/x\,](v_1 :=v_2) \rightarrowtail [\,e_1/x\,](\mu_1 \uplus \mu'') \mid [\,e_1/x\,]\, c''$ for some μ'' and c'' such that $\mu' = [\,e_2/x\,]\mu''$ and $c' = [\,e_2/x\,]\, c''$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 20. □

Lemma 22. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\mu \mid [\,e_1/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2) \longrightarrow \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\mu$ and $[\,e_2/x\,]\mu \mid [\,e_2/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2) \longrightarrow [\,e_2/x\,]\mu \mid [\,e_2/x\,]\, c''$ for some c'' such that $c' = [\,e_1/x\,]\, c''$.*

Proof. Without loss of generality, we can suppose that y is fresh. By Lemma 1, $[\,e_1/x\,]\, v$ and $[\,e_1/x\,]\, v$ are values. Note that $[\,e_2/x\,]\mu$ and $[\,e_2/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2)$ are term-closed since so are $[\,e_1/x\,]\mu$ and $[\,e_1/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2)$. Letting $i \in \{1,2\}$, by (C_Return),

$$[\,e_i/x\,]\mu \mid [\,e_i/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2) \longrightarrow [\,e_i/x\,]\mu \mid [\,e_i/x\,][\,v/y\,]\, c_2.$$

□

Lemma 23. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\mu \mid [\,e_1/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2) \longrightarrow \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\mu$ and $[\,e_2/x\,]\mu \mid [\,e_2/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2) \longrightarrow [\,e_2/x\,]\mu \mid [\,e_2/x\,]\, c''$ for some c'' such that $c' = [\,e_1/x\,]\, c''$.

(2) If $[\,e_2/x\,]\mu \mid [\,e_2/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2) \longrightarrow \mu' \mid c'$, then $\mu' = [\,e_2/x\,]\mu$ and $[\,e_1/x\,]\mu \mid [\,e_1/x\,](y \leftarrow \mathsf{do\,return}\; v; c_2) \longrightarrow [\,e_1/x\,]\mu \mid [\,e_1/x\,]\, c''$ for some c'' such that $c' = [\,e_2/x\,]\, c''$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 22. □

Lemma 24. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\mu \mid [\,e_1/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2) \longrightarrow \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\mu$ and $[\,e_2/x\,]\mu \mid [\,e_2/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2) \longrightarrow [\,e_2/x\,]\mu \mid [\,e_2/x\,]\, c''$ for some c'' such that $c' = [\,e_1/x\,]\, c''$.*

Proof. Note that $[\,e_2/x\,]\mu$ and $[\,e_2/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2)$ are term-closed since so are $[\,e_1/x\,]\mu$ and $[\,e_1/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2)$. Letting $i \in \{1,2\}$, by (C_Assert),

$$\begin{array}{rcl} [\,e_i/x\,]\mu \mid [\,e_i/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2) & \longrightarrow & [\,e_i/x\,]\mu \mid \langle \mathsf{assert}\,([\,e_i/x\,]\, c_1), \nu\emptyset.\langle \emptyset \mid [\,e_i/x\,]\, c_1 \rangle\rangle^{\ell}; [\,e_i/x\,]\, c_2 \\ & = & [\,e_i/x\,]\mu \mid [\,e_i/x\,](\langle \mathsf{assert}\,(c_1), \nu\emptyset.\langle \emptyset \mid c_1 \rangle\rangle^{\ell}; c_2). \end{array}$$

□

Lemma 25. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\mu \mid [\,e_1/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2) \longrightarrow \mu' \mid c'$, then $\mu' = [\,e_1/x\,]\mu$ and $[\,e_2/x\,]\mu \mid [\,e_2/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2) \longrightarrow [\,e_2/x\,]\mu \mid [\,e_2/x\,]\, c''$ for some c'' such that $c' = [\,e_1/x\,]\, c''$.

(2) If $[\,e_2/x\,]\mu \mid [\,e_2/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2) \longrightarrow \mu' \mid c'$, then $\mu' = [\,e_2/x\,]\mu$ and $[\,e_1/x\,]\mu \mid [\,e_1/x\,](\mathsf{assert}\,(c_1)^{\ell}; c_2) \longrightarrow [\,e_1/x\,]\mu \mid [\,e_1/x\,]\, c''$ for some c'' such that $c' = [\,e_2/x\,]\, c''$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 24. □

Lemma 26. *Let e_1 and e_2 be term-closed terms. If $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2) \longrightarrow \mu'' \mid c'$, then $\mu'' = [\,e_1/x\,]\,\mu$ and $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2) \longrightarrow [\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,c''$ for some c'' such that $c' = [\,e_1/x\,]\,c''$.*

Proof. Note that v takes the form of Boolean value since $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2)$ takes a step and that $[\,e_2/x\,]\,\mu$ and $[\,e_2/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2)$ are term-closed since so are $[\,e_1/x\,]\,\mu$ and $[\,e_1/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2)$. By case analysis on v.

Case $v = \mathsf{true}$: Obvious by (C_OK).

Case $v = \mathsf{false}$: Obvious by (C_FAIL). □

Lemma 27. *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2) \longrightarrow \mu'' \mid c'$, then $\mu'' = [\,e_1/x\,]\,\mu$ and $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2) \longrightarrow [\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,c''$ for some c'' such that $c' = [\,e_1/x\,]\,c''$.

(2) If $[\,e_2/x\,]\,\mu \mid [\,e_2/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2) \longrightarrow \mu'' \mid c'$, then $\mu'' = [\,e_2/x\,]\,\mu$ and $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,(\langle \mathsf{assert}\,(c_1), \nu\gamma.\langle \mu' \mid \mathsf{return}\,v\rangle\rangle^{\ell}; c_2) \longrightarrow [\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,c''$ for some c'' such that $c' = [\,e_2/x\,]\,c''$.

Proof. Since the evaluation relation is defined over term-closed terms, e_1 and e_2 are term-closed. Thus, we finish by Lemma 26. □

Lemma 28. *Suppose that $e_1 \longrightarrow e_2$. If $[\,e_1/x\,]\,e = E_1[\Uparrow\ell]$, then there exists some E_2 such that $[\,e_2/x\,]\,e = E_2[\Uparrow\ell]$.*

Proof. By structural induction on e.

Case $e = y$: If $x \neq y$, then contradictory. Thus, $x = y$ and so $e_1 = [\,e_1/x\,]\,e = E_1[\Uparrow\ell]$. However, $E_1[\Uparrow\ell] \longrightarrow e_2$ does not hold because $\Uparrow\ell$ cannot reduce, so contradictory.

Case $e = v$, $r \mathrel{=\!=} s$, and $\langle \{y{:}T \mid c\}, p, v\rangle^{\ell}$: Contradictory.

Case $e = \Uparrow\ell'$: If $\ell' = \ell$, then obvious. Otherwise, if $\ell' \neq \ell$, then contradictory since $[\,e_1/x\,]\,e = E_1[\Uparrow\ell]$.

Case $e = op(e'_1, \ldots, e'_n)$: Since $[\,e_1/x\,]\,e = E_1[\Uparrow\ell]$, there exists some i and E'_1 such that, for any $j < i$, $[\,e_1/x\,]\,e'_j$ is a value and $[\,e_1/x\,]\,e'_i = E'_1[\Uparrow\ell]$. By the IH, there exists some E'_2 such that $[\,e_2/x\,]\,e'_i = E'_2[\Uparrow\ell]$. By Lemma 3, for any $j < i$, $[\,e_2/x\,]\,e'_j$ is a value. Thus, $op([\,e_2/x\,]\,e'_1, \ldots, [\,e_2/x\,]\,e'_{i-1}, E'_2, [\,e_2/x\,]\,e'_{i+1}, \ldots, [\,e_2/x\,]\,e'_n)$ is an evaluation context.

Case $e = e'_1\,e'_2$: Since $[\,e_1/x\,]\,e = E_1[\Uparrow\ell]$, there are two cases we have to consider.

Case $E_1 = E'_1\,[\,e_1/x\,]\,e'_2$: Since $[\,e_1/x\,]\,e'_1 = E'_1[\Uparrow\ell]$, there exists some E'_2 such that $[\,e_2/x\,]\,e'_1 = E'_2[\Uparrow\ell]$, by the IH. Since $E'_2\,[\,e_2/x\,]\,e'_2$ is an evaluation context and $[\,e_2/x\,]\,e = E'_2[\Uparrow\ell]\,[\,e_2/x\,]\,e'_2$, we finish.

Case $E_1 = [\,e_1/x\,]\,e'_1\,E'_1$ where $[\,e_1/x\,]\,e'_1$ is a value: Since $[\,e_1/x\,]\,e'_2 = E'_1[\Uparrow\ell]$, there exists some E'_2 such that $[\,e_2/x\,]\,e'_2 = E'_2[\Uparrow\ell]$, by the IH. Since $[\,e_2/x\,]\,e'_1$ is a value by Lemma 3, $[\,e_2/x\,]\,e'_1\,E'_2$ is an evaluation context. Since $[\,e_2/x\,]\,e = [\,e_2/x\,]\,e'_1\,E'_2[\Uparrow\ell]$, we finish.

Case $e = e'_1 \mathrel{=\!=} e'_2$, $e'\{r\}$ and $\langle\!\langle\, \{y{:}T \mid c'_1\}, e'_2 \,\rangle\!\rangle^{\ell}$: Similarly to the case for function applications. □

Lemma 29. *Suppose that $e_1 \longrightarrow e_2$. If $[\,e_1/x\,]\,d = D_1[\Uparrow\ell]$, there exists some D_2 such that $[\,e_2/x\,]\,d = D_2[\Uparrow\ell]$.*

Proof. Straightforward by case anlaysis on d with Lemmas 28 and 3. □

Lemma 30. *Let c be a computation and e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\,e_1/x\,]\,c = C^{\mathsf{e}}_1\,[\,\Uparrow\ell\,]$, then there exists some C^{e}_2 such that $[\,e_2/x\,]\,c = C^{\mathsf{e}}_2\,[\,\Uparrow\ell\,]$.

(2) If $[\,e_1/x\,]\,c = C^{1}_1\,[\,\Uparrow\ell\,]$, then there exists some C^{1}_2 such that $[\,e_2/x\,]\,c = C^{1}_2\,[\,\Uparrow\ell\,]$.

Proof.

1. By case analysis on c.

Case $c = \mathsf{return}\,e'$: By Lemma 28.

Case $c = y \leftarrow e'_1; c'_2$: By Lemma 28

Case $c = y \Leftarrow d'; c'$: By Lemma 29.

Case $\nu r.\,c'$, $\mathsf{assert}\,(c'_1)^{\ell}; c'_2$, $\langle \mathsf{assert}\,(c'_1), p'_2\rangle^{\ell}; c'_3$, and $\Uparrow\ell'$: Contradictory.

2. By case analysis on c.

Case $c = \mathsf{return}\, e'$, $y \Leftarrow d'; c'$, $\nu r.\, c'$, $\mathsf{assert}\,(c_1')^{\ell}; c_2'$, and $\Uparrow\ell'$: Contradictory.

Case $c = y \leftarrow e_1'; c_2'$: Since $[\, e_1/x \,]\, c = C_1^1 [\Uparrow\ell]$, we have $e_1' = \mathsf{do}\Uparrow\ell$. Thus, $[\, e_2/x \,]\, c = y \leftarrow \mathsf{do}\Uparrow\ell; [\, e_2/x \,]\, c_2'$. We finish by letting $C_2^1 = y \leftarrow \mathsf{do}\,[\,]\,; [\, e_2/x \,]\, c_2'$.

Case $\langle \mathsf{assert}\,(c_1'), p_2' \rangle^{\ell}; c_3'$: Obvious. □

Lemma 31. *If $e_1 \longrightarrow e_2$, then $E[e_1] \longrightarrow E[e_2]$ for any E*

Proof. Since $e_1 \longrightarrow e_2$, there exists some E', e_1' and e_2' such that $e_1 = E'[e_1']$ and $e_2 = E'[e_2']$ and $e_1' \rightsquigarrow e_2'$. Because $E\,[\, E' \,]$ is an evaluation context, we finish. □

Lemma 32 (Weak bisimulation, left side)**.** *Let e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$.*

(1) If $[\, e_1/x \,]\, e = E_1[e_1']$ and $e_1' \rightsquigarrow e_2'$, then $[\, e_2/x \,]\, e \longrightarrow^* [\, e_2/x \,]\,(E'[e'])$ for some E' and e' such that $E_1 = [\, e_1/x \,]\, E'$ and $e_2' = [\, e_1/x \,]\, e'$.

(2) If $[\, e_1/x \,]\,(\mu_1 \uplus \mu_2) \mid [\, e_1/x \,]\, d \rightarrowtail [\, e_1/x \,]\, \mu_1 \uplus \mu' \mid c'$, then $[\, e_2/x \,]\,(\mu_1 \uplus \mu_2) \mid [\, e_2/x \,]\, d \rightarrowtail [\, e_2/x \,]\,(\mu_1 \uplus \mu'') \mid [\, e_2/x \,]\, c''$ for some μ'' and c'' such that $\mu' = [\, e_1/x \,]\, \mu''$ and $c' = [\, e_1/x \,]\, c''$.

(3) If $[\, e_1/x \,]\,(\mu_1 \uplus \mu_2) \mid [\, e_1/x \,]\, c \longrightarrow [\, e_1/x \,]\, \mu_1 \uplus \mu' \mid c'$, then $[\, e_2/x \,]\,(\mu_1 \uplus \mu_2) \mid [\, e_2/x \,]\, c \longrightarrow^* [\, e_2/x \,]\,(\mu_1 \uplus \mu'') \mid [\, e_2/x \,]\, c''$ for some μ'' and c'' such that $\mu' = [\, e_1/x \,]\, \mu''$ and $c' = [\, e_1/x \,]\, c''$. Moreoever, in the computation sequence $[\, e_2/x \,]\,(\mu_1 \uplus \mu_2) \mid [\, e_2/x \,]\, c \longrightarrow \dots \longrightarrow [\, e_2/x \,]\,(\mu_1 \uplus \mu'') \mid [\, e_2/x \,]\, c''$, the store $[\, e_2/x \,]\, \mu_1$ is never modified.

(4) If $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow p'$, then $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow^* [\, e_2/x \,]\, p''$ for some p'' such that $p' = [\, e_1/x \,]\, p''$.

Proof. By induction on the sizes of e, d, c, and p.

1. By case analysis on e.

Case $e = y$: If $x = y$, then $e_1 = [\, e_1/x \,]\, e = E_1[e_1'] \longrightarrow E_1[e_2']$. Since $e_1 \longrightarrow e_2$, we have $E_1[e_2'] = e_2$ $(= [\, e_2/x \,]\, e)$. Thus, we finish by letting $E' = E_1$ and $e' = e_2'$ (noting that E_1 and e_2' is term-closed). Otherwise, if $x \neq y$, then contradictory because $[\, e_1/x \,]\, e = y$ cannot reduce.

Case $e = v$: Contradictory by Lemma 1.

Case $e = \Uparrow\ell$: Contradictory.

Case $e = op(e_1'', \dots, e_n'')$: Since $[\, e_1/x \,]\, e = E_1[e_1']$, there are two cases we have to consider by case anlysis on E_1.

Case $E_1 = [\,]$: Since $[\, e_1/x \,]\, e = e_1'$ reduces, all terms $[\, e_1/x \,]\, e_i''$ are values. Thus, we finish by Lemmas 2 and 5 (1).

Case $E_1 = op([\, e_1/x \,]\, e_1'', \dots, [\, e_1/x \,]\, e_{i-1}'', E_1', [\, e_1/x \,]\, e_{i+1}'', \dots, [\, e_1/x \,]\, e_n'')$ where $[\, e_1/x \,]\, e_j''$ is a value for any $j < i$: Since $[\, e_1/x \,]\, e = E_1[e_1']$, we have $[\, e_1/x \,]\, e_i'' = E_1'[e_1']$. By the IH, there exist some E'' and e' such that $[\, e_2/x \,]\, e_i'' \longrightarrow^* [\, e_2/x \,]\,(E''[e'])$ and $E_1' = [\, e_1/x \,]\, E''$ and $e_2' = [\, e_1/x \,]\, e'$. Since e_j'' is a value for any $j < i$ by Lemma 2, we finish by letting $E' = op(e_1'', \dots, e_{i-1}'', E'', e_{i+1}'', \dots, e_n'')$, using Lemma 31.

Case $e = e_1''\, e_2''$: Since $[\, e_1/x \,]\, e = E_1[e_1']$, there are three cases we have to consider by case anlysis on E_1.

Case $E_1 = [\,]$: Since $[\, e_1/x \,]\, e = e_1'$ reduces, $[\, e_1/x \,]\, e_1''$ and $[\, e_1/x \,]\, e_2''$ are values. Thus, we finish by Lemmas 2 and 7 (1).

Case $E_1 = E_1'\, [\, e_1/x \,]\, e_2''$: Since $[\, e_1/x \,]\, e = E_1[e_1']$, we have $[\, e_1/x \,]\, e_1'' = E_1'[e_1']$. By the IH, there exist some E'' and e' such that $[\, e_2/x \,]\, e_1'' \longrightarrow^* [\, e_2/x \,]\,(E''[e'])$ and $E_1' = [\, e_1/x \,]\, E''$ and $e_2' = [\, e_1/x \,]\, e'$. Thus, we finish by letting $E' = E''\, e_2''$, using Lemma 31.

Case $E_1 = [\, e_1/x \,]\, e_1''\, E_1'$ where $[\, e_1/x \,]\, e_1''$ is a value: Since $[\, e_1/x \,]\, e = E_1[e_1']$, we have $[\, e_1/x \,]\, e_2'' = E_1'[e_1']$. By the IH, there exist some E'' and e' such that $[\, e_2/x \,]\, e_2'' \longrightarrow^* [\, e_2/x \,]\,(E''[e'])$ and $E_1' = [\, e_1/x \,]\, E''$ and $e_2' = [\, e_1/x \,]\, e'$. Since e_1'' is a value by Lemma 2, we finish by letting $E' = e_1''\, E''$, using Lemma 31.

Case $e = e_1'' =\!= e_2''$: Similarly to the case for term application with Lemma 9 (1).

Case $e = r =\!= s$: Obvious.

Case $e = e_1''\{r\}$: Similarly to the case for term application with Lemma 11 (1).

Case $e = \langle\!\langle\, \{y{:}T \mid c\}, e'' \,\rangle\!\rangle^{\ell}$: Similarly to the case for term application with Lemma 13 (1).

Case $e = \langle \{y{:}T \mid c\}, p, v \rangle^{\ell}$: Obviously, $E_1 = [\,]$ and so $[\, e_1/x \,]\, e = e_1'$ can reduce. There are four reduction rules applicable to $[\, e_1/x \,]\, e$.

Case (R_Blame): We are given $[\,e_1/x\,]\,p = \nu\gamma'.\langle\mu' \mid \Uparrow\ell'\rangle$ and $e_2' = \Uparrow\ell'$ for some γ', μ', and ℓ'. Because $[\,e_2/x\,]\,p = \nu\gamma'.\langle\mu'' \mid \Uparrow\ell'\rangle$ for some μ'', we finish by applying (R_Blame) to $[\,e_2/x\,]\,e$. Note that we can let $E' = [\,]$ and $e' = \Uparrow\ell'$.

Case (R_Checking): We are given $\emptyset \mid [\,e_1/x\,]\,p \hookrightarrow p'$ for some p'. By the IH (case (4)), there exists some p'' such that $\emptyset \mid [\,e_2/x\,]\,p \hookrightarrow^* [\,e_2/x\,]\,p''$ and $p' = [\,e_1/x\,]\,p''$. Thus, we finish by letting $E' = [\,]$ and $e' = \langle\{y{:}T \mid c\}, p'', v\rangle^{\ell}$, using (R_Checking).

Case (R_OK) and (R_Fail): By Lemma 15 (1).

2. By case analysis on d.

Case $d = \mathsf{ref}_r\,e'$: By Lemmas 2 and 17 (1).

Case $d = {!e'}$: By Lemmas 2 and 19 (1).

Case $d = e_1' := e_2'$: By Lemmas 2 and 21 (1).

3. By case analysis on the computation rule applied to $[\,e_1/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_1/x\,]\,c$.

Case (C_Red): We are given $[\,e_1/x\,]\,c = C^{\mathsf{e}}\,[\,e_1'\,]$ for some C^{e} and e_1' such that $e_1' \rightsquigarrow e_2'$. By case analysis on c.

Case $c = \mathsf{return}\,e'$: Since $[\,e_1/x\,]\,c = C^{\mathsf{e}}\,[\,e_1'\,]$, there exists some E_1 such that $[\,e_1/x\,]\,e' = E_1[e_1']$. By (C_Red), $[\,e_1/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_1/x\,]\,c \longrightarrow [\,e_1/x\,]\,(\mu_1 \uplus \mu_2) \mid \mathsf{return}\,E_1[e_2']$. By the IH (case (1)), there exist some E' and e'' such that $[\,e_2/x\,]\,e' \longrightarrow^* [\,e_2/x\,]\,(E'[e''])$ and $E_1 = [\,e_1/x\,]\,E'$ and $e_2' = [\,e_1/x\,]\,e''$. By (C_Red), $[\,e_2/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_2/x\,]\,c \longrightarrow^* [\,e_2/x\,]\,(\mu_1 \uplus \mu_2) \mid \mathsf{return}\,[\,e_2/x\,]\,(E'[e''])$. Since $E_1[e_2'] = [\,e_1/x\,]\,(E'[e''])$, we finish. Note that we let $c'' = \mathsf{return}\,E'[e'']$.

Case $c = y \leftarrow e'; c'$: Similarly to the case for return computation. Note that there exists some E_1 such that $[\,e_1/x\,]\,e' = E_1[e_1']$ since $[\,e_1/x\,]\,c = C^{\mathsf{e}}\,[\,e_1'\,]$.

Case $c = y \Leftarrow d'; c'$: Since $[\,e_1/x\,]\,c = C^{\mathsf{e}}\,[\,e_1'\,]$, there exists some D_1 such that $[\,e_1/x\,]\,d' = D_1[e_1']$. By case analysis on d'.

Case $d' = \mathsf{ref}_r\,e'$: Since $[\,e_1/x\,]\,d' = D_1[e_1']$, $D_1 = \mathsf{ref}_r E_1$ for some E_1 such that $[\,e_1/x\,]\,e' = E_1[e_1']$. By the IH (case (1)), there exist some E' and e'' such that $[\,e_2/x\,]\,e' \longrightarrow^* [\,e_2/x\,]\,(E'[e''])$ and $E_1 = [\,e_1/x\,]\,E'$ and $e_2' = [\,e_1/x\,]\,e''$. By (C_Red), $[\,e_2/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_2/x\,]\,c \longrightarrow^* [\,e_2/x\,]\,(\mu_1 \uplus \mu_2) \mid [\,e_2/x\,]\,(y \Leftarrow \mathsf{ref}_r E'[e'']; c')$. Since $E_1[e_2'] = [\,e_1/x\,]\,(E'[e''])$, we finish. Note that $c'' = y \Leftarrow \mathsf{ref}_r E'[e'']; c'$.

Case $d' = {!e'}$ and $d' = e_1' := e_2'$: Similarly to the case for new command.

Case (C_Comput): By the IH and (C_Comput).

Case (C_RBlame): We are given $[\,e_1/x\,]\,c = C^{\mathsf{e}}\,[\,\Uparrow\ell\,]$ for some C^{e} and ℓ. By Lemma 30 (1) and (C_RBlame).

Case (C_CBlame): We are given $[\,e_1/x\,]\,c = C^{1}\,[\,\Uparrow\ell\,]$ for some C^{1} and ℓ. By Lemma 30 (2) and (C_CBlame).

Case (C_Return): By Lemmas 2 and 23 (1).

Case (C_Command): By the IH (case (2)).

Case (C_Region): By (C_Region).

Case (C_Assert): By Lemma 25 (1).

Case (C_Checking): By the IH and (C_Checking).

Case (C_OK) and (C_Fail): By Lemma 27 (1).

4. By case analysis on the rule applied last to derive $[\,e_1/x\,]\,\mu \mid [\,e_1/x\,]\,p \hookrightarrow p'$.

Case (P_Comput): We are given $p = \nu\gamma'.\langle\mu' \mid c'\rangle$ and, by inversion, $[\,e_1/x\,]\,(\mu \uplus \mu') \mid [\,e_1/x\,]\,c' \longrightarrow [\,e_1/x\,]\,\mu \uplus \mu'' \mid c''$ for some μ'' and c''. By the IH, there exist some μ''' and c''' such that

- $[\,e_2/x\,]\,(\mu \uplus \mu') \mid [\,e_2/x\,]\,c' \longrightarrow^* [\,e_2/x\,]\,(\mu \uplus \mu''') \mid [\,e_2/x\,]\,c'''$,
- $\mu'' = [\,e_1/x\,]\,\mu'''$, and
- $c'' = [\,e_1/x\,]\,c'''$.

Since $[\,e_2/x\,]\,\mu$ is not modified during the computation, we finish by (P_Comput).

Case (P_Region): By (P_Region). □

Lemma 33. *Suppose that $e_1 \longrightarrow e_2$. If $[\,e_2/x\,]\,e$ is a value, then there exists some v such that $[\,e_1/x\,]\,e \longrightarrow^* [\,e_1/x\,]\,v$ and $[\,e_2/x\,]\,e = [\,e_2/x\,]\,v$.*

Proof. By case analysis on e.

Case $e = y$: If $x = y$, then we finish by letting $v = e_2$ since $e_2 = [\, e_2/x \,]\, e$ is a value; otherwise, if $x \neq y$, then contradictory since $[\, e_2/x \,]\, e = y$ is not a value.

Case $e = v$: By Lemma 1.

Case otherwise: Contradictory. □

Lemma 34. *Suppose that* $e_1 \longrightarrow e_2$*. If* $[\, e_2/x \,]\, e = E_2[\Uparrow\ell]$*, then* $[\, e_1/x \,]\, e \longrightarrow^* E_1[\Uparrow\ell]$ *for some* E_1*.*

Proof. By structural induction on e.

Case $e = y$: If $x \neq y$, then contradictory. Thus, $x = y$ and so $e_2 = [\, e_2/x \,]\, e = E_2[\Uparrow\ell]$. Since $[\, e_1/x \,]\, e = e_1 \longrightarrow e_2 = E_2[\Uparrow\ell]$, we finish.

Case $e = v$, $r =\!= s$, and $\langle \{y{:}T \mid c\}, p, v\rangle^{\ell}$: Contradictory.

Case $e = \Uparrow\ell'$: If $\ell' = \ell$, then obvious. Otherwise, if $\ell' \neq \ell$, then contradictory since $[\, e_2/x \,]\, e = E_2[\Uparrow\ell]$.

Case $e = op(e'_1, \ldots, e'_n)$: Since $[\, e_2/x \,]\, e = E_2[\Uparrow\ell]$, there exist some i and E'_2 such that, for any $j < i$, $[\, e_2/x \,]\, e'_j$ is a value and $[\, e_2/x \,]\, e'_i = E'_2[\Uparrow\ell]$. By the IH, there exists some E'_1 such that $[\, e_1/x \,]\, e'_i \longrightarrow^* E'_1[\Uparrow\ell]$. By Lemma 33, for any $j < i$, there exists some v''_j such that $[\, e_1/x \,]\, e'_j \longrightarrow^* [\, e_1/x \,]\, v''_j$ and $[\, e_2/x \,]\, e'_j = [\, e_2/x \,]\, v''_j$. Since $[\, e_1/x \,]\, v''_j$ is a value by Lemma 1, we finish by Lemma 31 when letting $E_1 = op([\, e_1/x \,]\, v''_1, \ldots, [\, e_1/x \,]\, v''_{i-1}, E'_1, [\, e_1/x \,]\, e'_{i+1}, \ldots, [\, e_1/x \,]\, e'_n)$.

Case $e = e'_1\, e'_2$: Since $[\, e_2/x \,]\, e = E_2[\Uparrow\ell]$, there are two cases we have to consider.

Case $E_2 = E'_2\, [\, e_2/x \,]\, e'_2$: Since $[\, e_2/x \,]\, e'_1 = E'_2[\Uparrow\ell]$, there exists some E'_1 such that $[\, e_1/x \,]\, e'_1 \longrightarrow^* E'_1[\Uparrow\ell]$, by the IH. Since $E'_1\, [\, e_1/x \,]\, e'_2$ is an evaluation context and $[\, e_1/x \,]\, e \longrightarrow^* E'_1[\Uparrow\ell]\, [\, e_1/x \,]\, e'_2$ by Lemma 31, we finish.

Case $E_2 = [\, e_2/x \,]\, e'_1\, E'_2$ where $[\, e_2/x \,]\, e'_1$ is a value: Since $[\, e_2/x \,]\, e'_2 = E'_2[\Uparrow\ell]$, there exists some E'_1 such that $[\, e_1/x \,]\, e'_2 \longrightarrow^* E'_1[\Uparrow\ell]$, by the IH. Since $[\, e_2/x \,]\, e'_1$ is a value, there exists some v'_1 such that $[\, e_1/x \,]\, e'_1 \longrightarrow^* [\, e_1/x \,]\, v'_1$ and $[\, e_2/x \,]\, e'_1 = [\, e_2/x \,]\, v'_1$ by Lemma 33. Since $[\, e_1/x \,]\, e \longrightarrow^* [\, e_1/x \,]\, v'_1\, E'_1[\Uparrow\ell]$ by Lemma 31, we finish by Lemma 1.

Case $e = e'_1 =\!= e'_2$, $e'\{r\}$ and $\langle\!\langle\, \{y{:}T \mid c'_1\}, e'_2 \,\rangle\!\rangle^{\ell}$: Similarly to the case for function applications. □

Lemma 35 (Weak bisimulation, right side)**.** *Let* e_1 *and* e_2 *be terms such that* $e_1 \longrightarrow e_2$*.*

(1) If $[\, e_2/x \,]\, e = E_2[e'_1]$ *and* $e'_1 \rightsquigarrow e'_2$*, then* $[\, e_1/x \,]\, e \longrightarrow^* [\, e_1/x \,]\, (E'[e'])$ *for some* E' *and* e' *such that* $E_2 = [\, e_2/x \,]\, E'$ *and* $e'_2 = [\, e_2/x \,]\, e'$*.*

(2) If $[\, e_2/x \,]\, (\mu_1 \uplus \mu_2) \mid [\, e_2/x \,]\, d \rightarrowtail [\, e_2/x \,]\, \mu_1 \uplus \mu' \mid c'$*, then* $[\, e_1/x \,]\, d = D[e']$ *and* $e' \longrightarrow^* e''$ *and* $[\, e_1/x \,]\, (\mu_1 \uplus \mu_2) \mid D[e''] \rightarrowtail [\, e_1/x \,]\, (\mu_1 \uplus \mu'') \mid [\, e_1/x \,]\, c''$ *for some* D'*,* e'*,* e''*,* μ'' *and* c'' *such that* $\mu' = [\, e_2/x \,]\, \mu''$ *and* $c' = [\, e_2/x \,]\, c''$*.*

(3) If $[\, e_2/x \,]\, (\mu_1 \uplus \mu_2) \mid [\, e_2/x \,]\, c \longrightarrow [\, e_2/x \,]\, \mu_1 \uplus \mu' \mid c'$*, then* $[\, e_1/x \,]\, (\mu_1 \uplus \mu_2) \mid [\, e_1/x \,]\, c \longrightarrow^* [\, e_1/x \,]\, (\mu_1 \uplus \mu'') \mid [\, e_1/x \,]\, c''$ *for some* μ'' *and* c'' *such that* $\mu' = [\, e_2/x \,]\, \mu''$ *and* $c' = [\, e_2/x \,]\, c''$*. Moreoever, in the computation sequence* $[\, e_1/x \,]\, (\mu_1 \uplus \mu_2) \mid [\, e_1/x \,]\, c \longrightarrow \ldots \longrightarrow [\, e_1/x \,]\, (\mu_1 \uplus \mu'') \mid [\, e_1/x \,]\, c''$*, the store* $[\, e_1/x \,]\, \mu_1$ *is never modified.*

(4) If $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow p'$*, then* $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow^* [\, e_1/x \,]\, p''$ *for some* p'' *such that* $p' = [\, e_2/x \,]\, p''$*.*

Proof. By induction on the sizes of e, d, and c.

1. By case analysis on e.

Case $e = y$: If $x = y$, then $e_2 = [\, e_2/x \,]\, e = E_2[e'_1] \longrightarrow E_2[e'_2]$. Since $e_1 \longrightarrow e_2 \longrightarrow E_2[e'_2]$, we finish by letting $E' = E_2$ and $e' = e'_2$ (noting that E_2 and e'_2 is term-closed). Otherwise, if $x \neq y$, then contradictory because $[\, e_2/x \,]\, e = y$ cannot reduce.

Case $e = v$: Contradictory by Lemma 1.

Case $e = \Uparrow\ell$: Contradictory.

Case $e = op(e''_1, \ldots, e''_n)$: Since $[\, e_2/x \,]\, e = E_2[e'_1]$, there are two cases we have to consider by case anlysis on E_2.

Case $E_2 = [\,]$: Since $[\, e_2/x \,]\, e = e'_1$ reduces, all terms $[\, e_2/x \,]\, e''_i$ are values. Thus, we finish by Lemmas 33, 1, 31 and 5 (2).

Case $E_2 = op([\, e_2/x \,]\, e''_1, \ldots, [\, e_2/x \,]\, e''_{i-1}, E'_2, [\, e_2/x \,]\, e''_{i+1}, \ldots, [\, e_2/x \,]\, e''_n)$ where $[\, e_2/x \,]\, e''_j$ is a value for any $j < i$: Since $[\, e_2/x \,]\, e = E_2[e'_1]$, we have $[\, e_2/x \,]\, e''_i = E'_2[e'_1]$. By the IH, there exist some E'' and e' such that $[\, e_1/x \,]\, e''_i \longrightarrow^* [\, e_1/x \,]\, (E''[e'])$ and $E'_2 = [\, e_2/x \,]\, E''$ and $e'_2 = [\, e_2/x \,]\, e'$. We finish by Lemmas 33, 1 and 31.

Case $e = e_1'' \, e_2''$: Since $[\, e_2/x \,]\, e = E_2[e_1']$, there are three cases we have to consider by case anlysis on E_2.

Case $E_2 = [\,]$: Since $[\, e_2/x \,]\, e = e_1'$ reduces, $[\, e_2/x \,]\, e_1''$ and $[\, e_2/x \,]\, e_2''$ are values. Thus, we finish by Lemmas 33, 1, 31 and 7 (2).

Case $E_2 = E_2' \, [\, e_2/x \,]\, e_2''$: Since $[\, e_2/x \,]\, e = E_2[e_1']$, we have $[\, e_2/x \,]\, e_1'' = E_2'[e_1']$. By the IH, there exist some E'' and e' such that $[\, e_1/x \,]\, e_1'' \longrightarrow^* [\, e_1/x \,]\, (E''[e'])$ and $E_2' = [\, e_2/x \,]\, E''$ and $e_2' = [\, e_2/x \,]\, e'$. Thus, we finish by letting $E' = E'' \, e_2''$, using Lemma 31.

Case $E_2 = [\, e_2/x \,]\, e_1'' \, E_2'$ where $[\, e_2/x \,]\, e_1''$ is a value: Since $[\, e_2/x \,]\, e = E_2[e_1']$, we have $[\, e_2/x \,]\, e_2'' = E_2'[e_1']$. By the IH, there exist some E'' and e' such that $[\, e_1/x \,]\, e_2'' \longrightarrow^* [\, e_1/x \,]\, (E''[e'])$ and $E_2' = [\, e_2/x \,]\, E''$ and $e_2' = [\, e_2/x \,]\, e'$. We finish by Lemmas 33, 1 and 31.

Case $e = e_1'' =\!= e_2''$: Similarly to the case for term application with Lemma 9 (2).

Case $e = r =\!= s$: Obvious.

Case $e = e_1''\{r\}$: Similarly to the case for term application with Lemma 11 (2).

Case $e = \langle\!\langle \{y{:}T \mid c\}, e'' \rangle\!\rangle^{\ell}$: Similarly to the case for term application with Lemma 13 (2).

Case $e = \langle \{y{:}T \mid c\}, p, v \rangle^{\ell}$: Obviously, $E_2 = [\,]$ and so $[\, e_2/x \,]\, e = e_1'$ can reduce. There are four reduction rules applicable to $[\, e_2/x \,]\, e$.

Case (R_Blame): We are given $[\, e_2/x \,]\, p = \nu\gamma'.\langle \mu' \mid \Uparrow\ell' \rangle$ and $e_2' = \Uparrow\ell'$ for some γ', μ', and ℓ'. Because $p = \nu\gamma'.\langle \mu'' \mid \Uparrow\ell' \rangle$ for some μ'', we finish by applying (R_Blame) to $[\, e_1/x \,]\, e$. Note that we can let $E' = [\,]$ and $e' = \Uparrow\ell'$.

Case (R_Checking): We are given $\emptyset \mid [\, e_2/x \,]\, p \hookrightarrow p'$ for some p'. By the IH (case (4)), there exists some p'' such that $\emptyset \mid [\, e_1/x \,]\, p \hookrightarrow^* [\, e_1/x \,]\, p''$ and $p' = [\, e_2/x \,]\, p''$. Thus, we finish by letting $E' = [\,]$ and $e' = \langle \{y{:}T \mid c\}, p'', v \rangle^{\ell}$, using (R_Checking).

Case (R_OK) and (R_Fail): Similarly to the case for term application with Lemma 15 (2).

2. By case analysis on d.

Case $d = \mathsf{ref}_r \, e'$: By Lemmas 33 and 17 (2).

Case $d = {!}e'$: By Lemmas 33 and 19 (2).

Case $d = e_1' := e_2'$: By Lemmas 33, 1 and 21 (2).

3. By case analysis on the computation rule applied to $[\, e_2/x \,]\, (\mu_1 \uplus \mu_2) \mid [\, e_2/x \,]\, c$.

Case (C_Red): If $[\, e_2/x \,]\, c = C^{\mathsf{e}}\, [\, e_1' \,]$ for some C^{e} and e_1' such that $e_1' \rightsquigarrow e_2'$, then we perform case analysis on c; we mention only interesting cases.

Case $c = \mathsf{return}\, e'$: Since $[\, e_2/x \,]\, c = C^{\mathsf{e}}\, [\, e_1' \,]$, there exists some E_2 such that $[\, e_2/x \,]\, e' = E_2[e_1']$. By (C_Red), $[\, e_2/x \,]\, (\mu_1 \uplus \mu_2) \mid [\, e_2/x \,]\, c \longrightarrow [\, e_2/x \,]\, (\mu_1 \uplus \mu_2) \mid \mathsf{return}\, E_2[e_2']$. By the IH (case (1)), there exist some E' and e'' such that $[\, e_1/x \,]\, e' \longrightarrow^* [\, e_1/x \,]\, (E'[e''])$ and $E_2 = [\, e_2/x \,]\, E'$ and $e_2' = [\, e_2/x \,]\, e''$. By (C_Red), $[\, e_1/x \,]\, (\mu_1 \uplus \mu_2) \mid [\, e_1/x \,]\, c \longrightarrow^* [\, e_1/x \,]\, (\mu_1 \uplus \mu_2) \mid \mathsf{return}\, [\, e_1/x \,]\, (E'[e''])$. Since $E_2[e_2'] = [\, e_2/x \,]\, (E'[e''])$, we finish. Note that we let $\mu'' = \mu_2$ and $c'' = \mathsf{return}\, E'[e'']$.

Case $c = y \leftarrow e'; c_2'$: Similarly to the case for return computation.

Case $c = y \Leftarrow d_1'; c_2'$: Similarly to the case for return computation with case analysis on d_1'.

Case (C_Comput): By the IH and (C_Comput).

Case (C_RBlame): We are given $[\, e_2/x \,]\, c = C^{\mathsf{e}}\, [\, \Uparrow\ell \,]$ for some C^{e} and ℓ. By case analysis on C^{e}.

Case $C^{\mathsf{e}} = \mathsf{return}\, E$ and $x \leftarrow E; c_2$: By Lemma 34, (C_Red), and (C_RBlame).

Case $C^{\mathsf{e}} = y \Leftarrow D; c_2$: Straightforward by case anlaysis on D with Lemmas 34 and 1, (C_Red), and (C_RBlame).

Case (C_CBlame): Straightforward by case analysis on c with (C_CBlame), similarly to Lemma 30 (2).

Case (C_Return): By Lemma 33, (C_Comput) and (C_Red), and Lemma 23 (2).

Case (C_Command): By the IH (case (2)), (C_Red), and (C_Command).

Case (C_Region): By (C_Region).

Case (C_Assert): By Lemma 25 (2).

Case (C_Checking): By the IH (case (4)) and (C_Checking).

Case (C_OK) and (C_Fail): By Lemma 33, (C_Red) and (C_Checking), and Lemma 27 (2).

4. By case analysis on the rule applied last to derive $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow p'$.

Case (P_Comput): We are given $p = \nu\gamma'.\langle \mu \mid c' \rangle$ and, by inversion, $[\, e_2/x \,]\, (\mu \uplus \mu') \mid [\, e_2/x \,]\, c' \longrightarrow [\, e_2/x \,]\, \mu \uplus \mu'' \mid c''$ for some μ'' and c''. By the IH (case (3)) and (P_Comput), we finish.

Case (P_Region): By (P_Region). □

Lemma 36. *Suppose that* $e_1 \longrightarrow e_2$*.*

(1) If $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow^* \nu\gamma'.\langle \mu' \mid \mathsf{return}\, v' \rangle$*, then* $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow^* [\, e_2/x \,]\, (\nu\gamma'.\langle \mu'' \mid \mathsf{return}\, v'' \rangle)$ *for some* μ'' *and* v'' *such that* $\mu' = [\, e_1/x \,]\, \mu''$ *and* $v' = [\, e_1/x \,]\, v''$*.*

(2) If $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow^* \nu\gamma'.\langle \mu' \mid \mathsf{return}\, v' \rangle$*, then* $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow^* [\, e_1/x \,]\, (\nu\gamma'.\langle \mu'' \mid \mathsf{return}\, v'' \rangle)$ *for some* μ'' *and* v'' *such that* $\mu' = [\, e_2/x \,]\, \mu''$ *and* $v' = [\, e_2/x \,]\, v''$*.*

Proof.

1. By mathematical induction on the number of computation steps of $[\, e_1/x \,]\, p$.

   Case 0: By Lemmas 2 and 1.

   Case $i + 1$: We are given $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow p'$ for some p'. By Lemma 32 (4), there exists some p'' such that $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow^* [\, e_2/x \,]\, p''$ and $p' = [\, e_1/x \,]\, p''$. By the IH, we finish.

2. By mathematical induction on the number of evaluation steps of $[\, e_2/x \,]\, p$.

   Case 0: By Lemma 33 and (P_Comput)/(C_Red), we finish.

   Case $i + 1$: We are given $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow p'$ for some p'. By Lemma 35 (4), there exists some p'' such that $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow^* [\, e_1/x \,]\, p''$ and $p' = [\, e_2/x \,]\, p''$. By the IH, we finish. □

Lemma 37 (Cotermination)**.** *Suppose that* $e_1 \longrightarrow e_2$*.*

(1) If $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow^* \nu\gamma.\langle \mu_1 \mid \mathsf{return\, true} \rangle$*, then* $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow^* \nu\gamma.\langle \mu_2 \mid \mathsf{return\, true} \rangle$ *for some* μ_2*.*

(2) If $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow^* \nu\gamma.\langle \mu_2 \mid \mathsf{return\, true} \rangle$*, then* $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow^* \nu\gamma.\langle \mu_1 \mid \mathsf{return\, true} \rangle$ *for some* μ_1*.*

Proof.

1. By Lemma 36 (1), $[\, e_2/x \,]\, \mu \mid [\, e_2/x \,]\, p \hookrightarrow^* \nu\gamma.\langle \mu_2 \mid \mathsf{return}\, [\, e_2/x \,]\, v \rangle$ for some μ_2 and v such that $\mathsf{true} = [\, e_1/x \,]\, v$. Obviously, $v = \mathsf{true}$.

2. By Lemma 36 (2), $[\, e_1/x \,]\, \mu \mid [\, e_1/x \,]\, p \hookrightarrow^* \nu\gamma.\langle \mu_1 \mid \mathsf{return}\, [\, e_1/x \,]\, v \rangle$ for some μ_1 and v such that $\mathsf{true} = [\, e_2/x \,]\, v$. Obviously, $v = \mathsf{true}$.

□

2.2 Type Soundness

Lemma 38. *Suppose that* $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \subseteq \langle \gamma_{\mathtt{r}}', \gamma_{\mathtt{w}}' \rangle$ *and* $\gamma_{\mathtt{r}}', \gamma_{\mathtt{w}}' \subseteq \gamma \cup \mathit{regions}\, (\Gamma)$*. If* $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ *is derived without "run-time" typing rules, that is,* (CT_CBind)*,* (CT_Check)*,* (CT_Blame)*, and* (CT_Conv)*, then* $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}', \gamma_{\mathtt{w}}' \rangle}$*.*

Proof. We can show that:

- if $\Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}', \gamma_{\mathtt{w}}' \rangle}$;
- if $\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$, then $\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}', \gamma_{\mathtt{w}}' \rangle} A$; and
- If $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}', \gamma_{\mathtt{w}}' \rangle}$

straightforwardly by induction on the derivations, assuming the derivations do not use run-time typing rules. Note that if run-time typing rules are used, we cannot prove it. □

Lemma 39. *(1) If* $\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$*, then* $\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}} \subseteq \gamma \cup \mathit{regions}\, (\Gamma)$*.*

(2) If $\Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$*, then* $\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}} \subseteq \gamma \cup \mathit{regions}\, (\Gamma)$*.*

Proof. The second case is shown immediately by the first case. If $\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$, then we can show that $\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}} \subseteq \gamma \cup \mathit{regions}\, (\Gamma)$ straightforwardly by induction on the derivation of $\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A_1$. □

Lemma 40. *Suppose that* $r \notin \gamma \cup \mathit{regions}\, (\Gamma)$*.*

(1) If $\Sigma; \gamma \vdash \Gamma$*, then* $\Sigma; \gamma, r \vdash \Gamma$*.*

(2) If $\Sigma; \gamma; \Gamma \vdash T$*, then* $\Sigma; \gamma, r; \Gamma \vdash T$*.*

(3) If $\Sigma; \gamma; \Gamma \vdash^{\varrho} A$*, then* $\Sigma; \gamma, r; \Gamma \vdash^{\varrho} A$*.*

(4) If $\Sigma; \gamma; \Gamma \vdash e : T$*, then* $\Sigma; \gamma, r; \Gamma \vdash e : T$*.*

(5) If $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$*, then* $\mu; \Sigma; \gamma, r; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$*.*

(6) If $\mu; \Sigma; \gamma \vdash p : T^{\gamma'}$*, then* $\mu; \Sigma; \gamma, r \vdash p : T^{\gamma'}$*.*

(7) If $\gamma \vdash \mu : \Sigma^{\gamma'}$*, then* $\gamma, r \vdash \mu : \Sigma^{\gamma'}$*.*

Proof. Straightforward by induction on the derviation of each judgment. □

Lemma 41. *Suppose that* $r \notin \gamma \cup \mathit{regions}(\Gamma_1) \cup \mathit{regions}(\Gamma_2)$*.*

(1) If $\Sigma; \gamma \vdash \Gamma_1, \Gamma_2$*, then* $\Sigma; \gamma \vdash \Gamma_1, r, \Gamma_2$*.*

(2) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash T$*, then* $\Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash T$*.*

(3) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash^{\varrho} A$*, then* $\Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash^{\varrho} A$*.*

(4) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash e : T$*, then* $\Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash e : T$*.*

(5) If $\mu; \Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$*, then* $\mu; \Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$*.*

Proof. Straightforward by induction on the derviation of each judgment. □

Lemma 42. *Suppose that* $a@r \notin \mathit{dom}(\Sigma)$*. Let* T *be a type.*

(1) If $\Sigma; \gamma \vdash \Gamma$*, then* $\Sigma, a@r{:}T; \gamma \vdash \Gamma$*.*

(2) If $\Sigma; \gamma; \Gamma \vdash T'$*, then* $\Sigma, a@r{:}T; \gamma; \Gamma \vdash T'$*.*

(3) If $\Sigma; \gamma; \Gamma \vdash^{\varrho} A$*, then* $\Sigma, a@r{:}T; \gamma; \Gamma \vdash^{\varrho} A$*.*

(4) If $\Sigma; \gamma; \Gamma \vdash e : T'$*, then* $\Sigma, a@r{:}T; \gamma; \Gamma \vdash e : T'$*.*

(5) If $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T'\{A_2\}^{\varrho}$*, then* $\mu; \Sigma, a@r{:}T; \gamma; \Gamma \vdash c : \{A_1\}x{:}T'\{A_2\}^{\varrho}$*.*

(6) If $\mu; \Sigma; \gamma \vdash p : T'^{\gamma'}$*, then* $\mu; \Sigma, a@r{:}T; \gamma \vdash p : T'^{\gamma'}$*.*

(7) If $\gamma \vdash \mu : (\Sigma, \Sigma')^{\gamma'}$ *and* $a@r \notin \mathit{dom}(\Sigma')$ *and* $r \notin \gamma'$*, then* $\gamma \vdash \mu : (\Sigma, a@r{:}T, \Sigma')^{\gamma'}$*.*

Proof. By induction on the derviation of each judgment. The only interesting case is in (PT). In that case, we are given $\mu; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu' \mid c' \rangle : T'^{\gamma''}$. Without loss of generality, we can suppose that $r \notin \gamma'$. By inversion,

- $\gamma, \gamma' \vdash \mu' : (\Sigma, \Sigma')^{\gamma'}$,
- $\mathit{dom}(\mu') = \mathit{dom}(\Sigma')$,
- $\mu \uplus \mu'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c' : \{A_1\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma_{\mathrm{r}}'', \gamma' \rangle}$, and
- $\mu \uplus \mu' \models A_1$.

By the IHs, it suffices to show that $a@r \notin \mathit{dom}(\Sigma')$. Since $\mathit{dom}(\mu') = \mathit{dom}((\Sigma, \Sigma')\,|_{\gamma'})$ from $\gamma, \gamma' \vdash \mu' : (\Sigma, \Sigma')^{\gamma'}$, and $\mathit{dom}(\mu') = \mathit{dom}(\Sigma')$, we have $\mathit{dom}(\Sigma') = \mathit{dom}((\Sigma, \Sigma')\,|_{\gamma'})$. Thus, for any $b@s \in \mathit{dom}(\Sigma')$, $s \in \gamma'$. Since $r \notin \gamma'$, we have $a@r \notin \mathit{dom}(\Sigma')$ and so we finish. □

Lemma 43. *If* $\Sigma; \gamma \vdash \Gamma$*, then* $\gamma \cap \mathit{regions}(\Gamma) = \emptyset$*.*

Proof. By induction on the derivation.

Case (WF_Empty): Obvious since $\mathit{regions}(\Gamma) = \emptyset$.

Case (WF_ExtendVar): By the IH.

Case (WF_ExtendRegion): We are given $\Sigma; \gamma \vdash \Gamma', r$ for some Γ' and r. By inversion, we have $\Sigma; \gamma \vdash \Gamma'$ and $r \notin \gamma$. By the IH, $\gamma \cap \mathit{regions}\,(\Gamma') = \emptyset$. Since $\mathit{regions}\,(\Gamma', r) = \mathit{regions}\,(\Gamma') \cup \{r\}$, we finish. □

Lemma 44. *Suppose that $\Sigma; \gamma_1; \Gamma_1 \vdash T$ and x is a fresh variable.*

(1) If $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, \Gamma_2$, then $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, x{:}T, \Gamma_2$.

(2) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, \Gamma_2 \vdash T'$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash T'$.

(3) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, \Gamma_2 \vdash^{\varrho} A$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash^{\varrho} A$.

(4) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, \Gamma_2 \vdash e \,:\, T'$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash e \,:\, T'$.

(5) If $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, \Gamma_2 \vdash c \,:\, \{A_1\}y{:}T'\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash c \,:\, \{A_1\}y{:}T'\{A_2\}^{\varrho}$.

Proof. By induction on the derivation of each judgment. The only interesting cases are in (WF_Empty) and (WF_ExtendVar).

Case (WF_Empty): We are given $\Sigma; \gamma_1, \gamma_2 \vdash \emptyset$. Since $\Gamma_1 = \emptyset$, we have $\Sigma; \gamma_1; \emptyset \vdash T$. By Lemma 40 (2), $\Sigma; \gamma_1, \gamma_2; \emptyset \vdash T$. Thus, by (WF_ExtendVar), we finish.

Case (WF_ExtendVar): If $\Gamma_2 = \emptyset$, then it suffices to show that $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, x{:}T$. Since $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1$ by inversion and $\Sigma; \gamma_1, \gamma_2; \Gamma_1 \vdash x \,:\, T$ by Lemmas 40 (2) and 43, we finish by (WF_ExtendVar).

Otherwise, if $\Gamma_2 = \Gamma_2', y{:}T'$ for some Γ_2', y and T', then, by inversion, we have $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, \Gamma_2'$ and $\Sigma; \gamma_1, \gamma_2; \Gamma_1, \Gamma_2' \vdash y \,:\, T'$. By the IHs, $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, x{:}T, \Gamma_2'$ and $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2' \vdash y \,:\, T'$. By (WF_ExtendVar), we finish. □

Lemma 45. *If $T_1 \parallel T_2$, then, for any e and x,*

(1) $[\,e/x\,]\, T_1 \parallel T_2$ and

(2) $T_1 \parallel [\,e/x\,]\, T_2$.

Proof. By induction on the derivation of $T_1 \parallel T_2$. □

Lemma 46. *Suppose that $\Sigma; \gamma_1; \Gamma_1 \vdash e \,:\, T$.*

(1) If $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, x{:}T, \Gamma_2$, then $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, [\,e/x\,]\,\Gamma_2$.

(2) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash T'$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e/x\,]\,\Gamma_2 \vdash [\,e/x\,]\, T'$.

(3) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash^{\varrho} A$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e/x\,]\,\Gamma_2 \vdash^{\varrho} [\,e/x\,]\, A$.

(4) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash e' \,:\, T'$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e/x\,]\,\Gamma_2 \vdash [\,e/x\,]\, e' \,:\, [\,e/x\,]\, T'$.

(5) If $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash c \,:\, \{A_1\}y{:}T\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e/x\,]\,\Gamma_2 \vdash [\,e/x\,]\, c \,:\, [\,e/x\,]\,(\{A_1\}y{:}T\{A_2\}^{\varrho})$.

Proof. By induction on the derivation of each judgment. The interesting cases are (T_Var), (T_Cast), and (T_Eq).

Case (T_Var): We are given $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash y \,:\, T'$ for some y and T'. By inversion, we have $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, x{:}T, \Gamma_2$ and $y{:}T' \in \Gamma_1, x{:}T, \Gamma_2$. By the IH, $\Sigma; \gamma_1, \gamma_2 \vdash \Gamma_1, [\,e/x\,]\,\Gamma_2$. If $y{:}T' \in \Gamma_1, \Gamma_2$, then we finish by (T_Var). If $y = x$, then $T = T'$, and $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e/x\,]\,\Gamma_2 \vdash e \,:\, T$ by the assumption and Lemmas 40 (4), 41 (4) and 44 (4).

Case (T_Cast) and (T_Eq): By the IHs and Lemma 45. □

Lemma 47. *If $T_1 \parallel T_2$, then $[\,r/s\,]\, T_1 \parallel [\,r/s\,]\, T_2$ for any r and s.*

Proof. By induction on the derivation of $T_1 \parallel T_2$. □

Lemma 48. *Suppose that $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \subseteq \langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle$ and ${\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \subseteq \gamma$.*

(1) If $\Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$.

(2) If $\Sigma; \gamma; \Gamma \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$, then $\Sigma; \gamma; \Gamma \vdash^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle} A$.

(3) If $\mu; \Sigma; \gamma; \Gamma \vdash c \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\mu; \Sigma; \gamma; \Gamma \vdash c \,:\, \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$.

(4) If $\mu; \Sigma; \gamma \vdash p \,:\, T^{\gamma_{\mathtt{r}}}$, then $\mu; \Sigma; \gamma \vdash p \,:\, T^{{\gamma_{\mathtt{r}}}'}$.

Proof. Straightforward by induction on each derivation. Note that if ${\gamma_{\mathtt{r}}}'$ or ${\gamma_{\mathtt{w}}}'$ includes region variables bound in Γ, then we cannot prove this lemma for “run-time” typing rules. □

Lemma 49. *If $\gamma_1 \subseteq \gamma_2$, then $[\,r/s\,]\,\gamma_1 \subseteq [\,r/s\,]\,\gamma_2$.*

Proof. Suppose that $t \in [\,r/s\,]\,\gamma_1$. By case analysis on t.

Case $t = r$: Then, $r \in \gamma_1$ or $s \in \gamma_1$, and so $r \in \gamma_2$ or $s \in \gamma_2$.

Case $t = s$: Then, it suffices to show that $r = s$. Since $t \in [\,r/s\,]\,\gamma_1$, there is some u such that $u \in \gamma_1$ and $[\,r/s\,]\,u = s$. If $u = s$, then $[\,r/s\,]\,s = r$ and so $r = s$. Otherwise, if $u \neq s$, then $[\,r/s\,]\,u = u$, which contradicts the assumption that $[\,r/s\,]\,u = s$.

Case $t \neq r, s$: Since $t \in [\,r/s\,]\,\gamma_1$, there is some u such that $u \in \gamma_1$ and $[\,r/s\,]\,u = t$. If $u = s$, then $[\,r/s\,]\,s = r$, which contradicts the assumption that $t \neq r$. Thus, $u \neq s$ and so $u = t$. Since $t \in \gamma_1$, we have $t \in \gamma_2$. Since $t \neq s$, $t \in [\,r/s\,]\,\gamma_2$. □

Lemma 50. *Suppose that $r \in \gamma \cup \mathit{regions}\,(\Gamma_1)$.*

(1) If $\Sigma; \gamma \vdash \Gamma_1, s, \Gamma_2$, then $\Sigma; \gamma \vdash \Gamma_1, [\,r/s\,]\,\Gamma_2$.

(2) If $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash T$, then $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,T$.

(3) If $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash^{\varrho} A$, then $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash^{[\,r/s\,]\,\varrho} [\,r/s\,]\,A$.

(4) If $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash e : T$, then $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,e : [\,r/s\,]\,T$.

(5) If $\mu; \Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,c : [\,r/s\,]\,(\{A_1\}y{:}T\{A_2\}^{\varrho})$.

Proof. By induction on the derivation of each judgment. Note that all free regions are captured by γ and $\mathit{regions}\,(\Gamma_1, s, \Gamma_2)$, which is important in (T_ACheck) and (T_Exact). We mention only some interesting cases.

Case (WF_Ref): We are given $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \mathsf{Ref}_t\, T'$. By inversion, we have $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash T'$ and $t \in \gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2) \cup \{s\}$. By the IH, $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,T'$. If $t = s$, then we have $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash \mathsf{Ref}_r [\,r/s\,]\,T'$ by (WF_Ref) since $r \in \gamma \cup \mathit{regions}\,(\Gamma_1)$ from the assumption. Since $[\,r/s\,]\,(\mathsf{Ref}_s\, T') = \mathsf{Ref}_r [\,r/s\,]\,T'$, we finish. Otherwise, if $t \neq s$, then we finish by (WF_Ref) since $t \in \gamma \cup \mathit{regions}\,(\Gamma_1, [\,r/s\,]\,\Gamma_2)$.

Case (WF_EmptyAssert): We are given $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} \top$. By inversion, we have $\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}} \subseteq \gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2) \cup \{s\}$. By (WF_EmptyAssert), it suffices to show that, $[\,r/s\,]\,(\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}) \subseteq \gamma \cup \mathit{regions}\,(\Gamma_1) \cup \mathit{regions}\,([\,r/s\,]\,\Gamma_2)$. By Lemma 49, we have $[\,r/s\,]\,(\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}) \subseteq [\,r/s\,]\,(\gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2)) \cup \{r\}$. Since $r \in \gamma \cup \mathit{regions}\,(\Gamma_1)$, we have $[\,r/s\,]\,(\gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2)) \cup \{r\} = [\,r/s\,]\,(\gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2)) \subseteq \gamma \cup \mathit{regions}\,(\Gamma_1) \cup [\,r/s\,]\,\mathit{regions}\,(\Gamma_2) = \gamma \cup \mathit{regions}\,(\Gamma_1) \cup \mathit{regions}\,([\,r/s\,]\,\Gamma_2)$.

Case (T_Cast) and (T_Eq): By the IHs and Lemma 47.

Case (T_Address): We are given $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash a@t : \mathsf{Ref}_t\, T'$. By inversion, we have $\Sigma; \gamma \vdash \Gamma_1, s, \Gamma_2$ and $a@t{:}T' \in \Sigma$ and $\Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_t\, T'$, which implies $t \in \gamma$ and $s \notin \mathit{frv}\,(T')$. Thus, $[\,r/s\,]\,(\mathsf{Ref}_t\, T') = \mathsf{Ref}_t\, T'$. By the IH, $\Sigma; \gamma \vdash \Gamma_1, [\,r/s\,]\,\Gamma_2$. By (T_Address), we finish.

Case (T_REq): By the assumption that $r \in \gamma \cup \mathit{regions}\,(\Gamma_1)$.

Case (T_RApp): We are given $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash e'\{t\} : [\,t/u\,]\,T'$ for some e', t, u and T'. By inversion, we have $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash e' : \forall u.\, T'$ and $t \in \gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2) \cup \{s\}$. Without loss of generality, we can suppose that u is fresh. By the IH, $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,e' : \forall u. [\,r/s\,]\,T'$.

We show that $[\,r/s\,]\,t \in \gamma \cup \mathit{regions}\,(\Gamma_1, [\,r/s\,]\,\Gamma_2)$. If $t = s$, then $[\,r/s\,]\,t = r$ and so we finish from the assumption. Otherwise, if $t \neq s$, then $[\,r/s\,]\,t = t$. Since $t \in \gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2)$, we finish.

Thus, by (T_RApp), we have $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,e'\{[\,r/s\,]\,t\} : [\,[\,r/s\,]\,t/u\,]\,[\,r/s\,]\,T'$. Since $[\,[\,r/s\,]\,t/u\,]\,[\,r/s\,]\,T' = [\,r/s\,]\,[\,t/u\,]\,T'$, we finish.

□

Lemma 51. *Type equivalence $\equiv$ is an equivalence relation:*

(1) $T \equiv T$ for any T;

(2) if $T_1 \equiv T_2$ and $T_2 \equiv T_3$, then $T_1 \equiv T_3$; and

(3) if $T_1 \equiv T_2$, then $T_2 \equiv T_1$.

Proof. Since type equivalence is the transitive and symmetric closure of the relation $\Rrightarrow$ over types, it suffices to show that $\Rrightarrow$ is reflexive. Let T be any type, x be a variable such that $x \notin \mathit{fv}(T)$, e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$ (e.g., $e_1 = (\lambda x{:}\mathsf{bool}.x)\,\mathsf{true}$ and $e = \mathsf{true}$). Then, $[\,e_1/x\,]\,T \Rrightarrow [\,e_2/x\,]\,T$ by definition. Since $[\,e_1/x\,]\,T = [\,e_2/x\,]\,T = T$, we finish. □

Lemma 52. *If $B \equiv T$ or $T \equiv B$, then $T = B$.*

Proof. We give a proof for the case of $B \equiv T$ and the other case can be shown similarly. We proceed by induction on $B \equiv T$.

Case $B \Rrightarrow T$: By definition, there exist some T', y, e_1, and e_2 such that $B = [\,e_1/y\,]\,T'$ and $T = [\,e_2/y\,]\,T'$ and $e_1 \longrightarrow e_2$. Since $B = [\,e_1/y\,]\,T'$, we have $T' = B$, and so $T = B$.

Case Transitivity ($B \equiv T'$ and $T' \equiv T$ for some T'): By the IHs.

Case Symmetry ($T \equiv B$): By the IH. □

Lemma 53. *If $x{:}T_1 \rightarrow T_2 \equiv T$ or $T \equiv x{:}T_1 \rightarrow T_2$, then $T = x{:}T_1' \rightarrow T_2'$ for some T_1' and T_2' such that $T_1 \equiv T_1'$ and $T_2 \equiv T_2'$.*

Proof. We give a proof for the case of $x{:}T_1 \rightarrow T_2 \equiv T$ and the other case can be shown similarly. We proceed by induction on $x{:}T_1 \rightarrow T_2 \equiv T$.

Case $x{:}T_1 \rightarrow T_2 \Rrightarrow T$: By definition, there exist some T', y, e_1, and e_2 such that $x{:}T_1 \rightarrow T_2 = [\,e_1/y\,]\,T'$ and $T = [\,e_2/y\,]\,T'$ and $e_1 \longrightarrow e_2$. Since $x{:}T_1 \rightarrow T_2 = [\,e_1/y\,]\,T'$, we have $T' = x{:}T_1' \rightarrow T_2'$ for some T_1' and T_2', and so $x{:}T_1 \rightarrow T_2 = x{:}[\,e_1/y\,]\,T_1' \rightarrow [\,e_1/y\,]\,T_2'$ and $T = x{:}[\,e_2/y\,]\,T_1' \rightarrow [\,e_2/y\,]\,T_2'$. (Note that we can suppose that x is fresh without loss of generality.) Since, for $i \in \{1,2\}$, $T_i = [\,e_1/y\,]\,T_i' \equiv [\,e_2/y\,]\,T_i'$, we finish.

Case Transitivity ($x{:}T_1 \rightarrow T_2 \equiv T'$ and $T' \equiv T$ for some T'): By the IHs and Lemma 51 (2).

Case Symmetry ($T \equiv x{:}T_1 \rightarrow T_2$): By the IH and Lemma 51 (3). □

Lemma 54. *If $\mathsf{Ref}_r\,T_1 \equiv T_2$ or $T_2 \equiv \mathsf{Ref}_r\,T_1$, then $T_2 = \mathsf{Ref}_r\,T_1'$ for some T_1' such that $T_1 \equiv T_1'$.*

Proof. We give a proof for the case of $\mathsf{Ref}_r\,T_1 \equiv T_2$ and the other case can be similarly. We proceed by induction on $\mathsf{Ref}_r\,T_1 \equiv T_2$.

Case $\mathsf{Ref}_r\,T_1 \Rrightarrow T_2$: By definition, there exist some T', x, e_1, and e_2 such that $\mathsf{Ref}_r\,T_1 = [\,e_1/x\,]\,T'$ and $T_2 = [\,e_2/x\,]\,T'$ and $e_1 \longrightarrow e_2$. Since $\mathsf{Ref}_r\,T_1 = [\,e_1/x\,]\,T'$, we have $T' = \mathsf{Ref}_r\,T''$ for some T'', and so $T_1 = [\,e_1/x\,]\,T''$ and $T_2 = \mathsf{Ref}_r[\,e_2/x\,]\,T''$. Since $T_1 = [\,e_1/x\,]\,T'' \equiv [\,e_2/x\,]\,T''$, we finish.

Case Transitivity ($\mathsf{Ref}_r\,T_1 \equiv T_3$ and $T_3 \equiv T_2$ for some T_3): By the IHs and Lemma 51 (2).

Case Symmetry ($T_2 \equiv \mathsf{Ref}_r\,T_1$): By the IH and Lemma 51 (3). □

Lemma 55. *Assertion equivalence $\equiv$ is an equivalence relation:*

(1) $A \equiv A$ for any A;

(2) if $A_1 \equiv A_2$ and $A_2 \equiv A_3$, then $A_1 \equiv A_3$; and

(3) if $A_1 \equiv A_2$, then $A_2 \equiv A_1$.

Proof. Since assertion equivalence is the transitive and symmetric closure of the relation $\Rrightarrow$ over assertion sequences, it suffices to show that $\Rrightarrow$ is reflexive. Let A be any type, x be a variable such that $x \notin \mathit{fv}(A)$, e_1 and e_2 be terms such that $e_1 \longrightarrow e_2$ (e.g., $e_1 = (\lambda x{:}\mathsf{bool}.x)\,\mathsf{true}$ and $e = \mathsf{true}$). Then, $[\,e_1/x\,]\,A \Rrightarrow [\,e_2/x\,]\,A$ by definition. Since $[\,e_1/x\,]\,A = [\,e_2/x\,]\,A = A$, we finish. □

Lemma 56. *If $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \equiv T_2$ or $T_2 \equiv \{A_1\}x{:}T_1\{A_2\}^{\varrho}$, then $T_2 = \{A_1'\}x{:}T_1'\{A_2'\}^{\varrho}$ for some A_1', T_1' and A_2' such that $A_1 \equiv A_1'$ and $T_1 \equiv T_1'$ and $A_2 \equiv A_2'$.*

Proof. We give a proof for the case of $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \equiv T_2$ and the other case can be shown similarly. We proceed by induction on $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \equiv T_2$.

Case $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \Rrightarrow T_2$: By definition, there exist some T', y, e_1, and e_2 such that $\{A_1\}x{:}T_1\{A_2\}^{\varrho} = [\,e_1/y\,]\,T'$ and $T_2 = [\,e_2/y\,]\,T'$ and $e_1 \longrightarrow e_2$. Since $\{A_1\}x{:}T_1\{A_2\}^{\varrho} = [\,e_1/y\,]\,T'$, we have $T' = \{A'_1\}x{:}T'_1\{A'_2\}^{\varrho}$ for some A'_1, T'_1, and A'_2, and so $A_1 = [\,e_1/y\,]\,A'_1$ and $T_1 = [\,e_1/y\,]\,T'_1$ and $A_2 = [\,e_1/y\,]\,A'_2$ and $T_2 = [\,e_2/y\,]\,(\{A'_1\}x{:}T'_1\{A'_2\}^{\varrho})$. (Note that we can suppose that x is fresh without loss of generality.) Since, for $i \in \{1,2\}$, $A_i = [\,e_1/y\,]\,A'_i \equiv [\,e_2/y\,]\,A'_i$ and $T_1 = [\,e_1/y\,]\,T'_1 \equiv [\,e_2/y\,]\,T'_1$, we finish.

Case Transitivity ($\{A_1\}x{:}T_1\{A_2\}^{\varrho} \equiv T_3$ and $T_3 \equiv T_2$ for some T_3): By the IHs and Lemmas 51 (2) and 55 (2).

Case Symmetry ($T_2 \equiv \{A_1\}x{:}T_1\{A_2\}^{\varrho}$): By the IH and Lemmas 51 (3) and 55 (3). □

Lemma 57. *If $\forall r.\, T_1 \equiv T_2$ or $T_2 \equiv \forall r.\, T_1$, then $T_2 = \forall r.\, T'_1$ for some T'_1 such that $T_1 \equiv T'_1$.*

Proof. We give a proof for the case of $\forall r.\, T_1 \equiv T_2$ and the other case can be shown similarly. We proceed by induction on $\forall r.\, T_1 \equiv T_2$.

Case $\forall r.\, T_1 \Rrightarrow T_2$: By definition, there exist some T', x, e_1, and e_2 such that $\forall r.\, T_1 = [\,e_1/x\,]\,T'$ and $T_2 = [\,e_2/x\,]\,T'$ and $e_1 \longrightarrow e_2$. Since $\forall r.\, T_1 = [\,e_1/x\,]\,T'$, we have $T' = \forall r.\, T''$ for some T'', and so $T_1 = [\,e_1/x\,]\,T''$ and $T_2 = \forall r. [\,e_2/x\,]\,T''$. (Note that we can suppose that r is fresh without loss of generality.) Since $T_1 = [\,e_1/y\,]\,T'' \equiv [\,e_2/y\,]\,T''$, we finish.

Case Transitivity ($\forall r.\, T_1 \equiv T_3$ and $T_3 \equiv T_2$ for some T_3): By the IHs and Lemma 51 (2).

Case Symmetry ($T_2 \equiv \forall r.\, T_1$): By the IH and Lemma 51 (3). □

Lemma 58. *If $T_1 \equiv T_2$, then unref $(T_1) \equiv$ unref (T_2).*

Proof. By definition of $T_1 \equiv T_2$, it suffices to show that, for any T, x, and e, *unref* $([\,e/x\,]\,T) = [\,e/x\,]$ *unref* (T). We show it by structurtal induction on T.

Case $T = \{y{:}T' \mid c\}$: Since *unref* $([\,e/x\,]\,T) =$ *unref* $([\,e/x\,]\,T')$ and $[\,e/x\,]$ *unref* $(T) = [\,e/x\,]$ *unref* (T'), we finish by the IH.

Case $T \neq \{y{:}T' \mid c\}$ for any y, T', r, and c: Obvious since *unref* $([\,e/x\,]\,T) = [\,e/x\,]\,T = [\,e/x\,]$ *unref* (T). □

Lemma 59. *Suppose that $\Sigma;\gamma;\emptyset \vdash v : T$.*

(1) If unref $(T) = B$, then $v = k$ for some $k \in \mathcal{K}(B)$.

(2) If unref $(T) = x{:}T_1 \to T_2$, then

- *(a) $v = \lambda x{:}T'_1.e$ for some T'_1 and e, or*
- *(b) $v = \langle T'_1 \Leftarrow T'_2\rangle^{\ell}$ for some T'_1, T'_2, and ℓ.*

(3) If unref $(T) = \mathsf{Ref}_r\, T'$, then

- *(a) $v = a@r$ for some a, or*
- *(b) $v = T_1 \Leftarrow^{\ell} T_2 : v'$ for some T_1, T_2, ℓ, and v'.*

(4) If unref $(T) = \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $v = \mathsf{do}\, c$ for some c.

(5) If unref $(T) = \forall r.\, T$, then $v = \lambda r.e$ for some e.

Proof. By induction on the typing derivation.

Case (T_Var), (T_Op), (T_App), (T_Eq), (T_RApp), (T_Blame), (T_WCheck) and (T_ACheck): Contradictory.

Case (T_Const): Obvious by the assumption of *ty* (k).

Case (T_Abs), (T_Cast), (T_Guard), (T_Do) and (T_RAbs): Obvious.

Case (T_Exact): We are given $\Sigma;\gamma;\emptyset \vdash v : \{x{:}T' \mid c\}$ for some x, T', and c. By inversion, we have $\Sigma;\gamma;\emptyset \vdash v : T'$. Since *unref* $(\{x{:}T' \mid c\}) =$ *unref* (T'), we finish by the IH.

Case (T_Forget): By inversion, we have $\Sigma;\gamma;\emptyset \vdash v : \{x{:}T \mid c\}$ for some x and c. Since *unref* $(T) =$ *unref* $(\{x{:}T \mid c\})$, we finish by the IH.

Case (T_Conv): By inversion, we have $\Sigma; \gamma; \emptyset \vdash v \;:\; T'$ and $T' \equiv T$. By Lemma 58, $\mathit{unref}\,(T') \equiv \mathit{unref}\,(T)$. We perform case anlaysis on $\mathit{unref}\,(T')$.

Case $\mathit{unref}\,(T') = B$: By Lemma 52 and the IH.

Case $\mathit{unref}\,(T') = x{:}T''_1 \rightarrow T''_2$: By Lemma 53 and the IH.

Case $\mathit{unref}\,(T') = \mathsf{Ref}_r\, T''$: By Lemma 54 and the IH.

Case $\mathit{unref}\,(T') = \{A''_1\}x{:}T''\{A''_2\}^{\varrho}$: By Lemma 56 and the IH.

Case $\mathit{unref}\,(T') = \forall r.\, T''$: By Lemma 57 and the IH. □

Lemma 60. *If $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\Sigma; \gamma; \emptyset \vdash v \;:\; T$.*

Proof. Straightforward by induction on the typing derivation. The only interesting case is in (CT_Conv). In that case, we are given $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v \;:\; \{A'_1\}x{:}T'\{A'_2\}^{\varrho}$ for some A'_1, T', and A'_2 such that $\{A'_1\}x{:}T'\{A'_2\}^{\varrho} \equiv \{A_1\}x{:}T\{A_2\}^{\varrho}$ and $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}$. By the IH, $\Sigma; \gamma; \emptyset \vdash v \;:\; T'$. Since $T' \equiv T$ by Lemma 56 and $\Sigma; \gamma; \emptyset \vdash T$ by inversion of $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}$, we have $\Sigma; \gamma; \emptyset \vdash v \;:\; T$ by (T_Conv). □

Lemma 61. *If $\Sigma; \gamma; \Gamma \vdash \lambda x{:}T_1.e \;:\; T$, then $\Sigma; \gamma; \Gamma, x{:}T_1 \vdash e \;:\; T_2$ and $x{:}T_1 \rightarrow T_2 \equiv \mathit{unref}\,(T)$ for some T_2.*

Proof. By induction on the typing derivation.

Case (T_Var), (T_Const), (T_Op), (T_Cast), (T_App), (T_Address), (T_Eq), (T_Do), (T_RAbs), (T_RApp), (T_Blame), (T_WCheck), (T_ACheck) and (T_Guard): Contradictory.

Case (T_Abs): Obvious by Lemma 51 (1).

Case (T_Exact) and (T_Forget): By the IH and Lemmas 44 (4) and 41 (4).

Case (T_Conv): By the IH and Lemmas 44 (4), 41 (4), 58 and 51 (2). □

Lemma 62. *If $\Sigma; \gamma; \Gamma \vdash \langle T_1 \Leftarrow T_2 \rangle^{\ell} \;:\; T$, then $\Sigma; \gamma; \Gamma \vdash T_1$ and $\Sigma; \gamma; \Gamma \vdash T_2$ and $T_1 \parallel T_2$ and $T_2 \rightarrow T_1 \equiv \mathit{unref}\,(T)$.*

Proof. By induction on the typing derivation.

Case (T_Var), (T_Const), (T_Op), (T_Abs), (T_App), (T_Address), (T_Eq), (T_Do), (T_RAbs), (T_RApp), (T_Blame), (T_WCheck), (T_ACheck) and (T_Guard): Contradictory.

Case (T_Cast): Obvious by Lemma 51 (1).

Case (T_Exact) and (T_Forget): By the IH and Lemmas 44 (4) and 41 (4).

Case (T_Conv): By the IH and Lemmas 44 (4), 41 (4), 58 and 51 (2). □

Lemma 63. *If $\Sigma; \gamma; \Gamma \vdash a@r \;:\; T$, then $a@r{:}T' \in \Sigma$ and $\Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_r\, T'$ and $\mathsf{Ref}_r\, T' \equiv \mathit{unref}\,(T)$ for some T'.*

Proof. By induction on the typing derivation.

Case (T_Var), (T_Const), (T_Op), (T_Abs), (T_Cast), (T_App), (T_Eq), (T_Do), (T_RAbs), (T_RApp), (T_Blame), (T_WCheck), (T_ACheck) and (T_Guard): Contradictory.

Case (T_Address): Obvious by Lemma 51 (1).

Case (T_Exact) and (T_Forget): By the IH.

Case (T_Conv): By the IH and Lemmas 58 and 51 (2). □

Lemma 64. *If $\Sigma; \gamma; \Gamma \vdash T_1 \Leftarrow^{\ell} T_2 : v \;:\; T$, then $\Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_r\, T_1$ and $\Sigma; \gamma; \emptyset \vdash v \;:\; \mathsf{Ref}_r\, T_2$ and $T_1 \parallel T_2$ and $\mathsf{Ref}_r\, T_1 \equiv \mathit{unref}\,(T)$ for some r.*

Proof. By induction on the typing derivation.

Case (T_Var), (T_Const), (T_Op), (T_Abs), (T_Cast), (T_App), (T_Address) (T_Eq), (T_Do), (T_RAbs), (T_RApp), (T_Blame), (T_WCheck) and (T_ACheck): Contradictory.

Case (T_Guard): Obvious by Lemma 51 (1).

Case (T_Exact) and (T_Forget): By the IH.

Case (T_Conv): By the IH and Lemmas 58 and 51 (2). □

Lemma 65. *If $\Sigma;\gamma;\Gamma \vdash \mathsf{do}\, c : T$, then $\emptyset;\Sigma;\gamma;\Gamma \vdash c : \{A'_1\}x{:}T'\{A'_2\}^{\varrho}$ and $\{A'_1\}x{:}T'\{A'_2\}^{\varrho} \equiv \mathit{unref}\,(T)$ for some A'_1, x, T', A'_2, and ϱ. In addition, the length of the derivation of $\emptyset;\Sigma;\gamma;\Gamma \vdash c : \{A'_1\}x{:}T'\{A'_2\}^{\varrho}$ is smaller than $\Sigma;\gamma;\Gamma \vdash \mathsf{do}\, c : T$.*

Proof. By induction on the typing derivation.

Case (T_Var), (T_Const), (T_Op), (T_Abs), (T_Cast), (T_App), (T_Address) (T_Eq), (T_RAbs), (T_RApp), (T_Blame), (T_WCheck), (T_ACheck) and (T_Guard): Contradictory.

Case (T_Do): Obvious by inversion and Lemma 51 (1).

Case (T_Exact) and (T_Forget): By the IH and Lemmas 44 (4) and 41 (4).

Case (T_Conv): By the IH and Lemmas 44 (4), 41 (4), 58 and 51 (2). □

Lemma 66. *If $\Sigma;\gamma;\Gamma \vdash \lambda r.e : T$, then $\Sigma;\gamma;\Gamma, r \vdash e : T'$ and $\forall r.T' \equiv \mathit{unref}\,(T)$ for some T'.*

Proof. By induction on the typing derivation.

Case (T_Var), (T_Const), (T_Op), (T_Abs), (T_Cast), (T_App), (T_Address), (T_Eq), (T_Do), (T_RApp), (T_Blame), (T_WCheck), (T_ACheck) and (T_Guard): Contradictory.

Case (T_RAbs): Obvious by Lemma 51 (1).

Case (T_Exact) and (T_Forget): By the IH and Lemmas 44 (4) and 41 (4).

Case (T_Conv): By the IH and Lemmas 44 (4), 41 (4), 58 and 51 (2). □

Lemma 67. *Let v be a term-closed value. If $T_1 \equiv T_2$, then $\models v : T_1$ iff $\models v : T_2$.*

Proof. By induction on $T_1 \equiv T_2$.

Case $T_1 \Rrightarrow T_2$: It suffices to show that, for any v, T, x, e_1, and e_2, if $e_1 \longrightarrow e_2$, then $\models v : [\, e_1/x \,]\, T$ iff $\models v : [\, e_2/x \,]\, T$. We show it by structural induction on T.

Case $T = B$, $y{:}T'_1 \rightarrow T'_2$, $\mathsf{Ref}_r\, T'$, $\{A_1\}y{:}T'\{A_2\}^{\varrho}$, and $\forall r.T'$: Obvious because $\mathit{refines}\,([\, e_i/x \,]\, T) = \emptyset$ for $i \in \{1, 2\}$.

Case $T = \{y{:}T' \mid c\}$: Without loss of generality, we can suppose that y is fresh. By the IH, it suffices to show that $\emptyset \mid \nu\emptyset.\langle \emptyset \mid [\, e_1/x \,]\, [\, v/y \,]\, c\rangle \hookrightarrow^{*} \nu\gamma_1.\langle \mu_1 \mid \mathsf{return\, true}\rangle$ iff $\emptyset \mid \nu\emptyset.\langle \emptyset \mid [\, e_2/x \,]\, [\, v/y \,]\, c\rangle \hookrightarrow^{*} \nu\gamma_2.\langle \mu_2 \mid \mathsf{return\, true}\rangle$. Note that e_1 and e_2 are term-closed. By Lemma 37, we finish.

Case Transitivity ($T_1 \equiv T_3$ and $T_3 \equiv T_1$): By the IHs.

Case Symmetry ($T_2 \equiv T_1$): By the IH. □

Lemma 68. *If $\Sigma;\gamma;\emptyset \vdash v : T$, then $\models v : T$.*

Proof. By induction on the typing derivation.

Case (T_Var), (T_Op), (T_App), (T_Eq), (T_RApp), (T_Blame), (T_WCheck) and (T_ACheck): Contradictory.

Case (T_Const): By the assumption of constants.

Case (T_Abs), (T_Cast), (T_Address), (T_Do), (T_RAbs) and (T_Guard): Obvious because $\mathit{refines}\,(T) = \emptyset$.

Case (T_Exact): By inversion and the IH.

Case (T_Forget): By the IH.

Case (T_Conv): By the IH and Lemma 67. □

Lemma 69. *If $\Sigma;\gamma;\emptyset \vdash v : \mathsf{Ref}_r\, T$, then $\mathit{ungrd}\,(v)$ is defined.*

Proof. By structural induction on v. By Lemma 59 (3), there are two cases we have to consider. If $v = a@r$ for some a and r, then we finish. Otherwise, if $v = T_1 \Leftarrow^{\ell} T_2 : v'$ for some T_1, T_2, ℓ, and v', then $\Sigma;\gamma;\emptyset \vdash v' : \mathsf{Ref}_s\, T'$ for some s and T' by Lemma 64. By the IH, $\mathit{ungrd}\,(v')$ is defined and $\mathit{ungrd}\,(v) = \mathit{ungrd}\,(v')$, so $\mathit{ungrd}\,(v')$ is also defined. □

Lemma 70. *If $\gamma \vdash \mu : \Sigma^{\gamma'}$ and $\gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \subseteq \gamma'$, then $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$.*

Proof. Obvious. □

Lemma 71. *If $\gamma \vdash \mu' : \Sigma^{\gamma'}$, then $\mathit{dom}\,(\mu') = \mathit{dom}\,(\mu'|_{\gamma'})$.*

Proof. It suffices to show that $\mathit{dom}\,(\mu') \subseteq \mathit{dom}\,(\mu'|_{\gamma'})$; $\mathit{dom}\,(\mu'|_{\gamma'}) \subseteq \mathit{dom}\,(\mu')$ holds obviously. Let $a@r \in \mathit{dom}\,(\mu')$. Since $\gamma \vdash \mu' : \Sigma^{\gamma'}$, we have $\mathit{dom}\,(\mu') = \mathit{dom}\,(\Sigma|_{\gamma'})$. Thus, $r \in \gamma'$, and so $a@r \in \mathit{dom}\,(\mu'|_{\gamma'})$. □

Lemma 72. *If*

- $\gamma \vdash \mu : \Sigma^{\gamma''}$,
- $\gamma, \gamma' \vdash \mu' : (\Sigma, \Sigma')^{\gamma'}$,
- $\mathit{dom}\,(\mu') = \mathit{dom}\,(\Sigma')$, *and*
- $\mathit{dom}\,(\Sigma|_{\gamma'}) = \emptyset$,

then $\gamma, \gamma' \vdash (\mu \uplus \mu')|_{\gamma' \cup \gamma''} : (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$.

Proof. By definition, it suffices to show the followings.

- We show that $\mathit{dom}\,((\mu \uplus \mu')|_{\gamma' \cup \gamma''}) = \mathit{dom}\,((\Sigma, \Sigma')|_{\gamma' \cup \gamma''})$. It suffices to show that (1) $\mathit{dom}\,(\mu|_{\gamma' \cup \gamma''}) = \mathit{dom}\,(\Sigma|_{\gamma' \cup \gamma''})$ and (2) $\mathit{dom}\,(\mu'|_{\gamma' \cup \gamma''}) = \mathit{dom}\,(\Sigma'|_{\gamma' \cup \gamma''})$.

  Since $\gamma \vdash \mu : \Sigma^{\gamma''}$, we have $\mathit{dom}\,(\mu) = \mathit{dom}\,(\Sigma \mid_{\gamma''})$ and so $\mathit{dom}\,(\mu) = \mathit{dom}\,(\mu \mid_{\gamma''})$. Since $\mathit{dom}\,(\Sigma \mid_{\gamma'}) = \emptyset$, we have $\mathit{dom}\,(\mu \mid_{\gamma'}) = \emptyset$. Thus, $\mathit{dom}\,(\mu \mid_{\gamma' \cup \gamma''}) = \mathit{dom}\,(\mu \mid_{\gamma''})$ and $\mathit{dom}\,(\Sigma \mid_{\gamma' \cup \gamma''}) = \mathit{dom}\,(\Sigma \mid_{\gamma''})$. Since $\mathit{dom}\,(\mu|_{\gamma''}) = \mathit{dom}\,(\mu)$, it suffices to show that $\mathit{dom}\,(\mu) = \mathit{dom}\,(\Sigma|_{\gamma''})$, which is shown by $\gamma \vdash \mu : \Sigma^{\gamma''}$.

  Since $\mathit{dom}\,(\mu') = \mathit{dom}\,(\mu'|_{\gamma'})$ and $\mathit{dom}\,(\Sigma') = \mathit{dom}\,(\Sigma'|_{\gamma'})$ by Lemma 71 and $\mathit{dom}\,(\mu') = \mathit{dom}\,(\Sigma')$, we have $\mathit{dom}\,(\mu' \mid_{\gamma' \cup \gamma''}) = \mathit{dom}\,(\mu' \mid_{\gamma'}) = \mathit{dom}\,(\mu')$ and $\mathit{dom}\,(\Sigma' \mid_{\gamma' \cup \gamma''}) = \mathit{dom}\,(\Sigma' \mid_{\gamma'}) = \mathit{dom}\,(\Sigma')$. Since $\mathit{dom}\,(\mu') = \mathit{dom}\,(\Sigma')$, we finish.

- We show that, for any $a@r \in \mathit{dom}\,((\mu \uplus \mu') \mid_{\gamma' \cup \gamma''})$, $\Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash ((\mu \uplus \mu') \mid_{\gamma' \cup \gamma''})(a@r) : (\Sigma, \Sigma')(a@r)$. Since $\gamma \vdash \mu : \Sigma^{\gamma''}$ and $\gamma, \gamma' \vdash \mu' : (\Sigma, \Sigma')^{\gamma'}$, we finish by Lemmas 42 (4) and 40 (4).

□

Lemma 73 (Progress)**.**

(1) If $\Sigma; \gamma; \emptyset \vdash e : T$, then:

(a) $e \longrightarrow e'$ for some e';

(b) e is a value; or

(c) $e = E[\Uparrow\ell]$ for some E and ℓ.

(2) Suppose that

- $\mu; \Sigma; \gamma; \emptyset \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ *and*
- $\gamma \vdash \mu|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} : \Sigma^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}$

Let

- $\mu_1 = \mu|_{{\gamma_\mathtt{w}}^c}$ *and*
- $\mu_2 = \mu|_{\gamma_\mathtt{w}}$.

Then,

- $\mu_1 \uplus \mu_2 \mid c \longrightarrow \mu_1 \uplus \mu_2' \mid c'$ *for some μ_2' and c', or*
- *c takes one of:*
  (a) $\nu r.\, c'$ for some c';
  (b) $\mathsf{return}\, v$ for some v; or
  (c) $\Uparrow\ell$ for some ℓ.

(3) If $\mu; \Sigma; \gamma \vdash p : T^{\gamma'}$ and $\gamma \vdash \mu|_{\gamma'} : \Sigma^{\gamma'}$, then:

- *$\mu \mid p \hookrightarrow p'$ for some p'; or*
- *p' is*

  (a) $\nu\gamma'.\langle \mu' \mid \mathsf{return}\, v' \rangle$ for some γ', μ', and v' or

  (b) $\nu\gamma'.\langle \mu' \mid \Uparrow\ell' \rangle$ for some γ', μ', and ℓ'.

Proof. By strong induction on the length of the derivation of each judgment.

1. By case analysis on the typing rule applied last.

Case (T_Var): Contradictory.

Case (T_Const), (T_Abs), (T_Cast), (T_Address), (T_Do), (T_RAbs), (T_Blame), (T_Guard), (T_Exact) and (T_Forget): Obvious.

Case (T_Op): We are given $\Sigma; \gamma; \emptyset \vdash op(e'_1, \dots, e'_n) : [\, e'_1/x_1, \dots, e'_n/x_n \,]\, T'$ and, by inversion, $ty\,(op) = x_1{:}T'_1 \rightarrow \dots \rightarrow x_n{:}T'_n \rightarrow T'$ and, for any i, $\Sigma; \gamma; \emptyset \vdash e'_i : [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1} \,]\, T'_i$. If all terms e'_i are values, then all terms e'_i are constants by the assumption of $ty\,(op)$ and Lemma 59 (1), and so $op(e'_1, \dots, e'_n)$ takes a step by (R_Op) since $[\![op]\!](e'_1, \dots, e'_n)$ is well defined by Lemma 68 and the assumption of op. Otherwise, let j be a natural number such that, for any $i < j$, e'_i is a value and e'_j is not a value. By the IH, e'_j takes a step or $e'_j = E'_j[\Uparrow\ell]$ for some E'_j and ℓ. If e_j takes a step, then we finish by Lemma 31. Otherwise, if $e'_j = E'_j[\Uparrow\ell]$, then we finish by letting $E = op(e'_1, \dots, e'_{j-1}, E'_j, e'_{j+1}, \dots, e'_n)$.

Case (T_App): We are given $\Sigma; \gamma; \emptyset \vdash e'_1\; e'_2 : [\, e'_2/x \,]\, T'_2$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e'_1 : x{:}T'_1 \rightarrow T'_2$ and $\Sigma; \gamma; \emptyset \vdash e'_2 : T'_1$. If e'_1 takes a step or $e'_1 = E'_1[\Uparrow\ell]$ for some E'_1 and $\Uparrow\ell$, then we finish. Otherwise, by the IH, we can suppose that e'_1 is a value. If e'_2 takes a step or $e'_2 = E'_2[\Uparrow\ell]$ for some E'_2 and $\Uparrow\ell$, then we finish. Otherwise, by the IH, we can suppose that e'_2 is a value. By Lemma 59 (2), there are two cases we have to consider.

Case $e'_1 = \lambda x{:}T''_1.e''$: By (R_Beta).

Case $e'_1 = \langle T''_1 \Leftarrow T''_2 \rangle^{\ell}$: By Lemma 62, $T''_1 \parallel T''_2$. We proceed by case analysis on the compatibility rule applied last to derive $T''_1 \parallel T''_2$.

Case (Sim_Base): By (R_Base).

Case (Sim_Fun): By (R_Fun).

Case (Sim_Ref): By (R_Ref) or (R_RefFail).

Case (Sim_RefineL): If T_2 is a refinement type, then by (R_Forget); otherwise, by (R_PreCheck).

Case (Sim_RefineR): By (R_Forget).

Case (Sim_Hoare): By (R_Hoare) or (R_HoareFail).

Case (Sim_RFun): By (R_RFun).

Case (T_Eq): We are given $\Sigma; \gamma; \emptyset \vdash e'_1 == e'_2 : \mathsf{bool}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e'_1 : \mathsf{Ref}_r\, T'_1$ and $\Sigma; \gamma; \emptyset \vdash e'_2 : \mathsf{Ref}_s\, T'_2$. Similarly to the case for (T_App), it suffices to consider the case where e'_1 and e'_2 are values by the IHs. Since $ungrd\,(e'_1)$ and $ungrd\,(e'_2)$ are defined by Lemma 69, we finish by (R_Eq) or (R_NEq).

Case (T_REq): By (R_REq) or (R_RNEq).

Case (T_RApp): By the IH, Lemma 59 (5), and (R_RBeta).

Case (T_WCheck): By the IH and (R_Check).

Case (T_ACheck): We are given $\Sigma; \gamma; \emptyset \vdash \langle \{x{:}T' \mid c_1\}, p_2, v \rangle^{\ell} : \{x{:}T' \mid c_1\}$ and, by inversion, $\emptyset; \Sigma; \gamma \vdash p_2 : \mathsf{bool}^{\emptyset}$ and $\emptyset \mid \nu\emptyset.\langle \emptyset \mid [\, v/x \,]\, c_1 \rangle \hookrightarrow^{*} p_2$. If $\emptyset \mid p_2 \hookrightarrow p'_2$ for some p'_2, then we finish by (R_Checking). If $p_2 = \nu\gamma'.\langle \mu' \mid \Uparrow\ell' \rangle$ for some γ', μ', and ℓ', then we finish by (R_Blame).

Otherwise, since $\gamma \vdash \emptyset : \Sigma^{\emptyset}$, we can suppose that $p_2 = \nu\gamma'.\langle \mu' \mid \mathsf{return}\, v \rangle$ for some γ', μ', and v by the IH (case (3)). By Lemma 60 and inversion of $\emptyset; \Sigma; \gamma \vdash p_2 : \mathsf{bool}^{\emptyset}$, we have $\Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash v : \mathsf{bool}$ for some Σ', and so, by Lemma 59 (1), $v = \mathsf{true}$ or false. If $v = \mathsf{true}$, then we finish by (R_OK); otherwise, by (R_Fail).

Case (T_Conv): By the IH.

2. By case analysis on the typing rule applied last.

Case (CT_Return): We are given $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, e' : \{[\, e'/x \,]\, A_1\}x{:}T\{A_1\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e' : T$. If e' takes a step, then we finish by (C_Red). If $e' = E[\Uparrow\ell]$, then we finish by (C_RBlame). Otherwise, by the IH, e' is a value and so we finish.

Case (CT_Bind): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow e_1'; c_2' : \{A_1\}x{:}T_2\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e_1' : \{A_1\}y{:}T_1\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ for some T_1, A_3, $\gamma_{\mathtt{r}1}$, and $\gamma_{\mathtt{w}1}$ such that $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle$. If e_1' takes a step, then we finish by (C_Red). If $e_1' = E[\Uparrow\ell]$, then we finish by (C_RBlame). Otherwise, by the IH, e_1' is a value. By Lemma 59 (4), $e_1' = \mathsf{do}\, c_1'$ for some c_1'. By Lemmas 65 and 56, $\emptyset; \Sigma; \gamma; \emptyset \vdash c_1' : \{A_1'\}y{:}T_1'\{A_3'\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ for some A_1', T_1', and A_3' such that $A_1' \equiv A_1$ and $T_1' \equiv T_1$ and $A_3' \equiv A_3$. By Lemma 89 (1), $\mu; \Sigma; \gamma; \emptyset \vdash c_1' : \{A_1'\}y{:}T_1'\{A_3'\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$. Since $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle$, we have $\gamma \vdash \mu|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} : \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$ by Lemma 70. Since the length of the derivation of $\mu; \Sigma; \gamma; \emptyset \vdash c_1' : \{A_1'\}y{:}T_1'\{A_3'\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ is smaller than that of $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, c_1' : \{A_1\}y{:}T_1\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, we can apply the IH: if c_1' takes a step, then we finish by the IH and (C_Comput); if $c_1' = \Uparrow\ell$, then we finish by (C_CBlame); if $c_1' = \nu r.\, c'$, then we finish by (C_Region); otherwise, $c_1' = \mathsf{return}\, v'$ for some v', and then we finish by (C_Return).

Case (CT_CBind): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1'; c_2' : \{A_1\}x{:}T_2\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ and, by inversion, $\mu; \Sigma; \gamma; \emptyset \vdash c_1' : \{A_1\}y{:}T_1\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ for some T_1, A_3, $\gamma_{\mathtt{r}1}$, and $\gamma_{\mathtt{w}1}$ such that $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle$. By applying Lemma 70 to $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle$ and $\gamma \vdash \mu|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} : \Sigma^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}$, we have $\gamma \vdash \mu|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} : \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$. Thus, we can apply the IH to $\mu; \Sigma; \gamma; \emptyset \vdash c_1' : \{A_1\}y{:}T_1\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$.

If c_1' takes a step, then we finish by the IH and (C_Comput). If $c_1' = \Uparrow\ell$, then we finish by (C_CBlame). If $c_1' = \nu r.\, c'$, then we finish by (C_Region). Otherwise, by the IH, $c_1' = \mathsf{return}\, v'$ for some v', so we finish by (C_Return).

Case (CT_New): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \Leftarrow \mathsf{ref}_r\, e_1'; c_2' : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ and $r \in \gamma_\mathtt{w}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e_1' : T'$. If e_1' takes a step, then we finish by (C_Red). If $e_1' = E[\Uparrow\ell]$, then we finish by (C_RBlame). Otherwise, by the IH, e_1' is a value and so we finish by (C_Command)/(C_New).

Case (CT_Deref): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \Leftarrow\, !e_1'; c_2' : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ and $r \in \gamma_\mathtt{r}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e_1' : \mathsf{Ref}_r\, T'$. If e_1' takes a step, then we finish by (C_Red). If $e_1' = E[\Uparrow\ell]$, then we finish by (C_RBlame). Otherwise, by the IH, e_1' is a value. By Lemma 59 (3), there are two cases we have to consider by case analysis on e_1'.

Case $e_1' {=} a@r$: Since $a@r \in \mathit{dom}\,(\Sigma)$ by Lemma 63 and $r \in \gamma_\mathtt{r}$, we have $a@r \in \mathit{dom}\,(\mu)$ from $\gamma \vdash \mu|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} : \Sigma^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}$. Thus, we finish by (C_Command)/(C_Deref).

Case $e_1' = T_1' \Leftarrow^\ell T_2' : v'$: By (C_Command)/(C_GuardDeref).

Case (CT_Assign): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \Leftarrow e_1' := e_2'; c_2' : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ and $r \in \gamma_\mathtt{w}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e_1' : \mathsf{Ref}_r\, T'$ and $\Sigma; \gamma; \emptyset \vdash e_2' : T'$. If e_1' takes a step, then we finish by (C_Red). If $e_1' = E[\Uparrow\ell]$, then we finish by (C_RBlame). Otherwise, by the IH, e_1' is a value. Similarly, we can suppose that e_2' is a value (otherwise, we finish by (C_Red) or (C_RBlame)). By Lemma 59 (3), there are two cases we have to consider by case analysis on e_1'.

Case $e_1' {=} a@r$: Since $a@r \in \mathit{dom}\,(\Sigma)$ by Lemma 63 and $r \in \gamma_\mathtt{w}$, we have $a@r \in \mathit{dom}\,(\mu)$ from $\gamma \vdash \mu|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} : \Sigma^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}$. Thus, we finish by (C_Command)/(C_Assign).

Case $e_1' = T_1' \Leftarrow^\ell T_2' : v'$: By (C_Command)/(C_GuardAssign).

Case (CT_Weak): By the IH.

Case (CT_Assert): By (C_Assert).

Case (CT_Check): We are given $\mu; \Sigma; \gamma; \emptyset \vdash \langle \mathsf{assert}\,(c_1'), p_2' \rangle^\ell; c_3' : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ and, by inversion,

- $\mu; \Sigma; \gamma \vdash p_2' : \mathsf{bool}^{\gamma_\mathtt{r}}$,
- $\emptyset; \Sigma; \gamma; \emptyset \vdash c_3' : \{A_1, c_1'\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$, and
- $\mu \mid \nu\emptyset.\langle \emptyset \mid c_1' \rangle \hookrightarrow^* p_2'$.

If p_2' takes a step, then we finish by (C_Checking). If $p_2' = \nu\gamma'.\langle \mu' \mid \Uparrow\ell' \rangle$ for some γ', μ', and ℓ', then we finish by (C_CBlame).

Otherwise, we have $\gamma \vdash \mu|_{\gamma_\mathtt{r}} : \Sigma^{\gamma_\mathtt{r}}$ by Lemma 70. Thus, by the IH, $p_2' = \nu\gamma'.\langle \mu' \mid \mathsf{return}\, v_2' \rangle$ for some γ', μ', and v_2'. By inversion of $\mu; \Sigma; \gamma \vdash p_2' : \mathsf{bool}^{\gamma_\mathtt{r}}$, and Lemmas 60 and 59 (1), we have $v_2' = \mathsf{true}$ or false. If $v_2' = \mathsf{true}$, then we finish by (C_OK); otherwise, by (C_Fail).

Case (CT_LetRegion) and (CT_Blame): Obvious.

Case (CT_Conv): By the IH.

3. We are given $\mu; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu' \mid c' \rangle : T^{\gamma''}$ for some γ', μ', and c'. Without loss of generality, we can suppose $\mathit{dom}\,(\mu|_{\gamma'}) = \emptyset$ and $\mathit{dom}\,(\Sigma|_{\gamma'}) = \emptyset$. By inversion,

- $\gamma, \gamma' \vdash \mu' : (\Sigma, \Sigma')^{\gamma'}$,
- $\mathit{dom}\,(\mu') = \mathit{dom}\,(\Sigma')$, and

- $\mu \uplus \mu'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c' \,:\, \{A'_1\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$

for some Σ' and A'_1. If $c' = \nu r.\, c'$, then we finish by (P_Region). If $c' = \mathsf{return}\, v$ or $\Uparrow \ell$, then we finish. Otherwise, since $\mathit{dom}\,(\mu|_{\gamma'}) = \emptyset$ (that is, regions in γ' do not occur in $\mathit{dom}\,(\mu)$), it suffices to show that

$$\gamma, \gamma' \vdash (\mu \uplus \mu')|_{\gamma' \cup \gamma''} \,:\, (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$$

by the IH and (P_Comput). By Lemma 72, $\gamma, \gamma' \vdash ((\mu|_{\gamma''}) \uplus \mu')|_{\gamma' \cup \gamma''} \,:\, (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$. Since $\mathit{dom}\,(\mu|_{\gamma'}) = \emptyset$, we have $(\mu|_{\gamma''})|_{\gamma' \cup \gamma''} = \mu|_{\gamma''}$. Thus, we finish.

□

Lemma 74. *If $T_1 \equiv T_2$, then $[\, e/x \,]\, T_1 \equiv [\, e/x \,]\, T_2$.*

Proof. By induction on $T_1 \equiv T_2$.

Case $T_1 \Rrightarrow T_2$: By definition, there exist some T, y, e_1, and e_2 such that $T_1 = [\, e_1/y \,]\, T$ and $T_2 = [\, e_2/y \,]\, T$ and $e_1 \longrightarrow e_2$. Suppose that z is a fresh variable. Then, since e_1 and e_2 are term-closed, for $i \in \{1,2\}$ $[\, e/x \,]\, T_i = [\, e/x \,][\, e_i/y \,]\, T = [\, e/x \,][\, e_i/z \,][\, z/y \,]\, T = [\, e_i/z \,][\, e/x \,][\, z/y \,]\, T$. Thus, $[\, e/x \,]\, T_1 \Rrightarrow [\, e/x \,]\, T_2$.

Case $T_1 \equiv T_3$ and $T_3 \equiv T_2$: By the IHs and Lemma 51 (2).

Case $T_2 \equiv T_1$: By the IH and Lemma 51 (3). □

Lemma 75. *If $\forall r.\, T_1 \equiv \forall r.\, T_2$, then $[\, s/r \,]\, T_1 \equiv [\, s/r \,]\, T_2$ for any s.*

Proof. By induction on $\forall r.\, T_1 \equiv \forall r.\, T_2$.

Case $\forall r.\, T_1 \Rrightarrow \forall r.\, T_2$: By definition, there exist some T, x, e_1, and e_2 such that $\forall r.\, T_1 = [\, e_1/x \,] \forall r.\, T$ and $\forall r.\, T_2 = [\, e_2/x \,] \forall r.\, T$ and $e_1 \longrightarrow e_2$. Without loss of generality, we can suppose that $r \notin \mathit{frv}\,(e_1) \cup \mathit{frv}\,(e_2)$. Thus, $T_1 = [\, e_1/x \,]\, T$ and $T_2 = [\, e_2/x \,]\, T$. Since, for $i \in \{1,2\}$, $[\, s/r \,]\, T_i = [\, s/r \,][\, e_i/x \,]\, T = [\, e_i/x \,][\, s/r \,]\, T$, we have $[\, s/r \,]\, T_1 \Rrightarrow [\, s/r \,]\, T_2$.

Case $\forall r.\, T_1 \equiv T_3$ and $T_3 \equiv \forall r.\, T_2$: Since $T_3 = \forall r.\, T'_3$ for some T'_3 by Lemma 57, we finish by the IHs and Lemma 51 (2).

Case $\forall r.\, T_2 \equiv \forall r.\, T_1$: By the IH and Lemma 51 (3). □

Lemma 76. *If $T_1 \parallel T_2$ and $T_2 \parallel T_3$, then $T_1 \parallel T_3$.*

Proof. By induction on the sum of sizes of T_1, T_2, and T_3 with case analysis on the rule applied last to derive $T_1 \parallel T_2$.

Case (Sim_Base): Obvious.

Case (Sim_Fun): We are given $T_1 = x{:}T_{11} \rightarrow T_{12}$ and $T_2 = x{:}T_{21} \rightarrow T_{22}$ and, by inversion, $T_{11} \parallel T_{21}$ and $T_{12} \parallel T_{22}$. Since $x{:}T_{21} \rightarrow T_{22} \parallel T_3$, we have $\mathit{unref}\,(T_3) = x{:}T_{31} \rightarrow T_{32}$ for some T_{31} and T_{32} such that $T_{21} \parallel T_{31}$ and $T_{22} \parallel T_{32}$ by Lemma 79. By the IHs, $T_{11} \parallel T_{31}$ and $T_{12} \parallel T_{32}$, and so we finish by (Sim_Fun) and (Sim_RefineR).

Case (Sim_Ref): We are given $T_1 = \mathsf{Ref}_r\, T'_1$ and $T_2 = \mathsf{Ref}_r\, T'_2$ and, by inversion, $T'_1 \parallel T'_2$. Since $\mathsf{Ref}_r\, T'_2 \parallel T_3$, we have $\mathit{unref}\,(T_3) = \mathsf{Ref}_r\, T'_3$ for some T'_3 such that $T'_2 \parallel T'_3$ by Lemma 80. By the IHs, $T'_1 \parallel T'_3$, and so we finish by (Sim_Ref) and (Sim_RefineR).

Case (Sim_RefineL): We are given $T_1 = \{x{:}T'_1 \mid c'_1\}$ and, by inversion, $T'_1 \parallel T_2$. By the IH, $T'_1 \parallel T_3$, and so we finish by (Sim_RefineL).

Case (Sim_RefineR): We are given $T_2 = \{x{:}T'_2 \mid c'_2\}$ and, by inversion, $T_1 \parallel T'_2$. Since $T'_2 \parallel T_3$ by Lemma 78 (2), we have $T_1 \parallel T_3$ by the IH.

Case (Sim_Hoare): We are given $T_1 = \{A_{11}\}x{:}T'_1\{A_{12}\}^{\varrho_1}$ and $T_2 = \{A_{21}\}x{:}T'_2\{A_{22}\}^{\varrho_2}$ and, by inversion, $T'_1 \parallel T'_2$. Since $\{A_{21}\}x{:}T'_2\{A_{22}\}^{\varrho_2} \parallel T_3$, we have $\mathit{unref}\,(T_3) = \{A_{31}\}x{:}T'_3\{A_{32}\}^{\varrho_3}$ for some A_{31}, T'_3, A_{32}, and ϱ_3 such that $T'_2 \parallel T'_3$ by Lemma 81. By the IH, $T'_1 \parallel T'_3$, and so we finish by (Sim_Hoare) and (Sim_RefineR).

Case (Sim_RFun): We are given $T_1 = \forall r.\, T'_1$ and $T_2 = \forall r.\, T'_2$ and, by inversion, $T'_1 \parallel T'_2$. Since $\forall r.\, T'_2 \parallel T_3$, we have $\mathit{unref}\,(T_3) = \forall r.\, T'_3$ for some T'_3 such that $T'_2 \parallel T'_3$ by Lemma 82. By the IH, $T'_1 \parallel T'_3$, and so we finish by (Sim_RFun) and (Sim_RefineR). □

Lemma 77. *If $T_1 \parallel T_2$, then $T_2 \parallel T_1$.*

Proof. By induction on the derivation of $T_1 \parallel T_2$ with case analysis on the compatibility rule applied last to $T_1 \parallel T_2$.

Case (Sim_Base): Obvious.

Case (Sim_Fun): By the IHs and (Sim_Fun).

Case (Sim_Ref): By the IH and (Sim_Ref).

Case (Sim_RefineL): By the IH and (Sim_RefineR).

Case (Sim_RefineR): By the IH and (Sim_RefineL)

Case (Sim_Hoare): By the IH and (Sim_Hoare)

Case (Sim_RFun): By the IH and (Sim_RFun).

□

Lemma 78.

(1) If $T_1 \parallel \{x{:}T_2 \mid c_2\}$, then $T_1 \parallel T_2$.

(2) If $\{x{:}T_1 \mid c_1\} \parallel T_2$, then $T_1 \parallel T_2$.

Proof.

1. By induction on $T_1 \parallel \{x{:}T_2 \mid c_2\}$. There are only two cases where $T_1 \parallel \{x{:}T_2 \mid c_2\}$ can be derived.

   Case (Sim_RefineL): We are given $\{y{:}T'_1 \mid c'_1\} \parallel \{x{:}T_2 \mid c_2\}$ and, by inversion, $T'_1 \parallel \{x{:}T_2 \mid c_2\}$. Since $T'_1 \parallel T_2$ by the IH, we finish by (Sim_RefineL).

   Case (Sim_RefineR): By inversion.

2. We are given $\{x{:}T_1 \mid c_1\} \parallel T_2$. By Lemma 77, $T_2 \parallel \{x{:}T_1 \mid c_1\}$, and so $T_2 \parallel T_1$ by case (1). Finally, we have $T_1 \parallel T_2$ by Lemma 77.

□

Lemma 79. *If $x{:}T_1 \rightarrow T_2 \parallel T$, then unref $(T) = x{:}T'_1 \rightarrow T'_2$ for some T'_1 and T'_2 such that $T_1 \parallel T'_1$ and $T_2 \parallel T'_2$.*

Proof. By induction on $x{:}T_1 \rightarrow T_2 \parallel T$ with case analysis on the rule applied last to derive $x{:}T_1 \rightarrow T_2 \parallel T$.

Case (Sim_Base), (Sim_Ref), (Sim_RefineL), (Sim_Hoare) and (Sim_RFun): Contradictory.

Case (Sim_Fun): By inversion.

Case (Sim_RefineR): By the IH. □

Lemma 80. *If $\mathsf{Ref}_r\, T_1 \parallel T$, then unref $(T) = \mathsf{Ref}_s\, T'_1$ for some s and T'_1 such that $T_1 \parallel T'_1$.*

Proof. By induction on $\mathsf{Ref}_r\, T_1 \parallel T$ with case analysis on the rule applied last to derive $\mathsf{Ref}_r\, T_1 \parallel T$.

Case (Sim_Base), (Sim_Fun), (Sim_RefineL), (Sim_Hoare) and (Sim_RFun): Contradictory.

Case (Sim_Ref): By inversion.

Case (Sim_RefineR): By the IH. □

Lemma 81. *If $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \parallel T$, then unref $(T) = \{A'_1\}x{:}T'_1\{A'_2\}^{\varrho'}$ for some A'_1, T'_1, A'_2 and ϱ' such that $T_1 \parallel T'_1$.*

Proof. By induction on $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \parallel T$ with case analysis on the rule applied last to derive $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \parallel T$.

Case (Sim_Base), (Sim_Fun), (Sim_Ref), (Sim_RefineL) and (Sim_RFun): Contradictory.

Case (Sim_Hoare): By inversion.

Case (Sim_RefineR): By the IH. □

Lemma 82. *If $\forall r.\, T_1 \parallel T$, then unref $(T) = \forall r.\, T'_1$ for some T'_1 such that $T_1 \parallel T'_1$.*

Proof. By induction on $\forall r.\, T_1 \parallel T$ with case analysis on the rule applied last to derive $\forall r.\, T_1 \parallel T$.

Case (Sim_Base), (Sim_Fun), (Sim_Ref), (Sim_RefineL) and (Sim_Hoare): Contradictory.

Case (Sim_RFun): By inversion.

Case (Sim_RefineR): By the IH. □

Lemma 83. *For any x, e, T_1, and T_2,*

(1) if $[\,e/x\,]\,T_1 \parallel T_2$, then $T_1 \parallel T_2$; and

(2) if $T_1 \parallel [\,e/x\,]\,T_2$, then $T_1 \parallel T_2$.

Proof. Straightforward by induction on the size of each derivation.

1. By case analysis on the rule applied last to derive $[\,e/x\,]\,T_1 \parallel T_2$.

   Case (Sim_Base): Obvious.
   Case (Sim_Fun): By the IHs and (Sim_Fun).
   Case (Sim_Ref): By the IHs and (Sim_Ref).
   Case (Sim_RefineL): By the IH and (Sim_RefineL).
   Case (Sim_RefineR): By the IH and (Sim_RefineR).
   Case (Sim_Hoare): By the IH and (Sim_Hoare).
   Case (Sim_RFun): By the IH and (Sim_RFun).

2. We are given $T_1 \parallel [\,e/x\,]\,T_2$. By Lemma 77, $[\,e/x\,]\,T_2 \parallel T_1$, and so $T_2 \parallel T_1$ by case (1). Finally, we have $T_1 \parallel T_2$ by Lemma 77.

□

Lemma 84. *If $T_1 \equiv T_2$, then*

(1) $T_1 \parallel T$ iff $T_2 \parallel T$; and

(2) $T \parallel T_1$ iff $T \parallel T_2$.

Proof. By induction on $T_1 \equiv T_2$.

Case $T_1 \Rrightarrow T_2$: By definition, it suffices to show that, for any T, T', x, e_1, and e_2, (1) $[\,e_1/x\,]\,T \parallel T'$ iff $[\,e_2/x\,]\,T \parallel T'$ and (2) $T' \parallel [\,e_1/x\,]\,T$ iff $T' \parallel [\,e_2/x\,]\,T$. These are proven by Lemmas 83 and 45.

Case $T_1 \equiv T_3$ and $T_3 \equiv T_2$: By the IHs.

Case $T_2 \equiv T_1$: By the IH. □

Lemma 85.

(1) If $A_1 \equiv A_2$, then $\{A_1\}x{:}T\{A\}^{\varrho} \equiv \{A_2\}x{:}T\{A\}^{\varrho}$ for any x, T, A, and ϱ.

(2) If $T_1 \equiv T_2$, then $\{A_1\}x{:}T_1\{A_2\}^{\varrho} \equiv \{A_1\}x{:}T_2\{A_2\}^{\varrho}$ for any A_1, x, A_2, and ϱ.

(3) If $A_1 \equiv A_2$, then $\{A\}x{:}T\{A_1\}^{\varrho} \equiv \{A\}x{:}T\{A_2\}^{\varrho}$ for any x, T, A, and ϱ.

Proof.

1. By induction on $A_1 \equiv A_2$.

   Case $A_1 \Rrightarrow A_2$: By definition, there exist some A', y, e_1, and e_2 such that $A_1 = [\,e_1/y\,]\,A'$ and $A_2 = [\,e_2/y\,]\,A'$ and $e_1 \longrightarrow e_2$. Suppose that z is some fresh variable. Then, for $i \in \{1, 2\}$, $\{A_i\}x{:}T\{A\}^{\varrho} = \{[\,e_i/y\,]\,A'\}x{:}T\{A\}^{\varrho} = [\,e_i/z\,]\,(\{[\,z/y\,]\,A'\}x{:}T\{A\}^{\varrho})$. Thus, $\{A_1\}x{:}T\{A\}^{\varrho} \Rrightarrow \{A_2\}x{:}T\{A\}^{\varrho}$.
   Case $A_1 \equiv A_3$ and $A_3 \equiv A_2$: By the IHs and Lemma 55 (2).
   Case $A_2 \equiv A_1$: By the IH and Lemma 55 (3).

2. By induction on $T_1 \equiv T_2$.

Case $T_1 \Rrightarrow T_2$: By definition, there exist some T, y, e_1, and e_2 such that $T_1 = [\, e_1/y \,]\, T$ and $T_2 = [\, e_2/y \,]\, T$ and $e_1 \longrightarrow e_2$. Suppose that z is some fresh variable. Then, for $i \in \{1, 2\}$, $\{A_1\}x{:}T_i\{A_2\}^{\varrho} = \{A_1\}x{:}[\, e_i/y \,]\, T\{A_2\}^{\varrho} = [\, e_i/z \,]\, (\{A_1\}x{:}[\, y/z \,]\, T\{A_2\}^{\varrho})$. Thus, $\{A_1\}x{:}T_1\{A\}^{\varrho} \Rrightarrow \{A_2\}x{:}T_2\{A\}^{\varrho}$.

Case $T_1 \equiv T_3$ and $T_3 \equiv T_2$: By the IHs and Lemma 51 (2).

Case $T_2 \equiv T_1$: By the IHs and Lemma 51 (3). □

3. Similarly to case (1).

Lemma 86 (Type and Context Well-Formedness)**.**

(1) If $\Sigma; \gamma; \Gamma \vdash T$*, then* $\Sigma; \gamma \vdash \Gamma$.

(2) If $\Sigma; \gamma; \Gamma \vdash e : T$*, then* $\Sigma; \gamma; \Gamma \vdash T$ *and* $\Sigma; \gamma \vdash \Gamma$.

(3) If $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$*, then* $\Sigma; \gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}$ *and* $\Sigma; \gamma \vdash \Gamma$.

Proof. Straightforward by induction on the derivation of each judgment. We mention only some interesting cases of typing rules.

Case (T_Var): We are given $\Sigma; \gamma; \Gamma \vdash x : T$ and, by inversion, $\Sigma; \gamma \vdash \Gamma$ and $x{:}T \in \Gamma$. Thus, there exist some Γ_1 and Γ_2 such that $\Gamma = \Gamma_1, x{:}T, \Gamma_2$ and $\Sigma; \gamma; \Gamma_1 \vdash T$. By Lemmas 44 (2) and 41 (2), $\Sigma; \gamma; \Gamma \vdash T$.

Case (T_Const) and (T_Op): By inversion, the assumption that $\mathit{ty}\,(k)$ and $\mathit{ty}\,(\mathit{op})$ are well formed for any k and op, and Lemmas 40 (2), 41 (2), 42 (2), 44 (2) and 46 (2).

Case (T_App): We are given $\Sigma; \gamma; \Gamma \vdash e_1\, e_2 : [\, e_2/x \,]\, T_2$ and, by inversion, $\Sigma; \gamma; \Gamma \vdash e_1 : x{:}T_1 \rightarrow T_2$ and $\Sigma; \gamma; \Gamma \vdash e_2 : T_1$. By the IH, $\Sigma; \gamma \vdash \Gamma$ and $\Sigma; \gamma; \Gamma \vdash x{:}T_1 \rightarrow T_2$. Since $\Sigma; \gamma; \Gamma, x{:}T_1 \vdash T_2$ by inversion, we have $\Sigma; \gamma; \Gamma \vdash [\, e_2/x \,]\, T_2$ by Lemma 46 (2).

Case (T_RApp): We are given $\Sigma; \gamma; \Gamma \vdash e_1\{r\} : [\, r/s \,]\, T_1$ and, by inversion, $\Sigma; \gamma; \Gamma \vdash e_1 : \forall s. T_1$ and $r \in \gamma \cup \mathit{regions}\,(\Gamma)$. By the IH, $\Sigma; \gamma \vdash \Gamma$ and $\Sigma; \gamma; \Gamma \vdash \forall s. T_1$. Since $\Sigma; \gamma; \Gamma, s \vdash T_1$ by inversion, we have $\Sigma; \gamma; \Gamma \vdash [\, r/s \,]\, T_1$ by Lemma 50 (2).

Case (CT_Return): We are given $\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{return}\, e : \{[\, e/x \,]\, A_2\}x{:}T\{A_2\}^{\varrho}$ and, by inversion, $\Sigma; \gamma; \Gamma \vdash e : T$ and $\Sigma; \gamma; \Gamma, x{:}T \vdash^{\varrho} A_2$. By the IH, Lemma 46 (3), and (WF_Hoare), we finish. □

Lemma 87. *If* $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, c : \{A_1\}x{:}T\{A_2\}^{\varrho}$*, then* $\mu; \Sigma; \gamma, r; \emptyset \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$.

Proof. By induction on the typing derivation. Without loss of generality, we can suppose that r is fresh.

Case (CT_Return), (CT_Bind), (CT_CBind), (CT_New), (CT_Deref), (CT_Assign), (CT_Assert), (CT_Check), and (CT_Blame): Contradictory.

Case (CT_Weak): By inversion, we have

- $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, c : \{A'_1\}x{:}T\{A'_2\}^{\varrho}$,
- $A'_1 \subseteq A_1$,
- $A_2 \subseteq A'_2$, and
- $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}$.

By the IH, $\mu; \Sigma; \gamma, r; \emptyset \vdash c : \{A'_1\}x{:}T\{A'_2\}^{\varrho \uplus \{r\}}$. Since $r \notin \gamma$ by Lemmas 86 (1) and 43, we have $\Sigma; \gamma, r; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$ by Lemmas 48 (1) and 40 (2). By (CT_Weak), we finish.

Case (CT_LetRegion): By inversion.

Case (CT_Conv): By inversion, we have

- $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, c : \{A'_1\}x{:}T'\{A'_2\}^{\varrho}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}$, and
- $\{A'_1\}x{:}T'\{A'_2\}^{\varrho} \equiv \{A_1\}x{:}T\{A_2\}^{\varrho}$.

By the IH, $\mu; \Sigma; \gamma, r; \emptyset \vdash c : \{A'_1\}x{:}T'\{A'_2\}^{\varrho \uplus \{r\}}$. By Lemmas 40 (2) and 48 (2), $\Sigma; \gamma, r; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$. Since $\{A'_1\}x{:}T'\{A'_2\}^{\varrho \uplus \{r\}} \equiv \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$ by Lemmas 56 and 85, we finish by (CT_Conv). □

Lemma 88.

(1) If $\mu_1 \mid c_1 \longrightarrow \mu_2 \mid c_2$ and $a@r \notin \mathit{dom}\,(\mu_1) \cup \mathit{dom}\,(\mu_2)$, then $\{a@r \mapsto v\} \uplus \mu_1 \mid c_1 \longrightarrow \{a@r \mapsto v\} \uplus \mu_2 \mid c_2$ for any v.

(2) If $a@r \notin \mathit{dom}\,(\mu)$ and $\mu \mid p_1 \hookrightarrow p_2$, then $\{a@r \mapsto v\} \uplus \mu \mid p_1 \hookrightarrow p_2$.

Proof. By induction on the derivations of $\mu_1 \mid c_1 \longrightarrow \mu_2 \mid c_2$ and $\mu \mid p_1 \hookrightarrow p_2$. We mention only interesting cases.

Case (C_Command)/(C_New): We are given $\mu_1 \mid x \Leftarrow \mathsf{ref}_s v'_1; c'_2 \longrightarrow \mu_1 \uplus \{b@s \mapsto v'_1\} \mid x \leftarrow \mathsf{do\,return}\ b@s; c'_2$ for some x, s, v'_1, c'_2, and b such that $b@s \notin \mathit{dom}\,(\mu_1)$. Since $a@r \neq b@s$, we have $\{a@r \mapsto v\} \uplus \mu_1 \mid x \Leftarrow \mathsf{ref}_s v'_1; c'_2 \longrightarrow \mu_1 \uplus \{a@r \mapsto v, b@s \mapsto v'_1\} \mid x \leftarrow \mathsf{do\,return}\ b@s; c'_2$.

Case (P_Comput): We are given $p_1 = \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle$ and $p_2 = \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle$ for some γ', μ'_1, c'_1, μ'_2, and c'_2 such that $\mu \uplus \mu'_1 \mid c'_1 \longrightarrow \mu \uplus \mu'_2 \mid c'_2$. Since we can suppose that $r \notin \gamma'$ without loss of generality, we finish by the IH (case (1)).

□

Lemma 89. *Suppose that $a@r \notin \mathit{dom}\,(\mu)$.*

(1) If $\mu; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma; \Gamma \vdash c : \{A_1\}x{:}T\{A_2\}^{\varrho}$. Moreover, the lengths of the typing derivations are the same.

(2) If $\mu; \Sigma; \gamma \vdash p : T^{\gamma'}$, then $\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma \vdash p : T^{\gamma'}$. Moreover, the lengths of the typing derivations are the same.

Proof. By induction on the derivations with Lemma 88 (2) in the case for (CT_Check). □

Lemma 90. *Suppose that $A \equiv A'$. Then, $\mu \models A$ iff $\mu \models A'$.*

Proof. Straightforward by induction on $A \equiv A'$ with Lemma 37. □

Lemma 91. *If $\mu \models A_1$ and $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\ v : \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu \models [\,v/x\,]\,A_2$.*

Proof. By induction on the typing derivation. We have to consider three cases; other cases are contradictory.

Case (CT_Return): Obvious.

Case (CT_Weak): By inversion, we have $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\ v : \{A'_1\}x{:}T\{A'_2\}^{\varrho}$ and $A'_1 \subseteq A_1$ and $A_2 \subseteq A'_2$ for some A'_1 and A'_2. Since $\mu \models A_1$, $\mu \models A'_1$. Thus, by the IH, $\mu \models [\,v/x\,]\,A'_2$, and so $\mu \models [\,v/x\,]\,A_2$.

Case (CT_Conv): By inversion, we have $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\ v : \{A'_1\}x{:}T'\{A'_2\}^{\varrho}$ and $\{A'_1\}x{:}T'\{A'_2\}^{\varrho} \equiv \{A_1\}x{:}T\{A_2\}^{\varrho}$ for some A'_1, T', and A'_2. By Lemma 56, $A'_1 \equiv A_1$ and $A'_2 \equiv A_2$. By the IH and Lemma 90, we finish (note that $[\,v/x\,]\,A'_2$ and $[\,v/x\,]\,A_2$ are term-closed and $[\,v/x\,]\,A'_2 \equiv [\,v/x\,]\,A_2$ by Lemma 74).

□

Lemma 92. *If*

- $\gamma, \gamma' \vdash (\mu \uplus \mu')\,|_{\gamma' \cup \gamma''} : (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$,
- $\mathit{dom}\,(\Sigma\,|_{\gamma'}) = \emptyset$,
- $\mathit{dom}\,(\mu\,|_{\gamma'}) = \emptyset$,
- $\mathit{dom}\,(\mu') = \mathit{dom}\,(\mu'\,|_{\gamma'})$, *and*
- $\mathit{dom}\,(\Sigma') = \mathit{dom}\,(\Sigma'\,|_{\gamma'})$,

then $\mathit{dom}\,(\mu') = \mathit{dom}\,(\Sigma')$.

Proof. First, we show $\mathit{dom}\,(\mu') \subseteq \mathit{dom}\,(\Sigma')$. Let $a@r \in \mathit{dom}\,(\mu') = \mathit{dom}\,(\mu'\,|_{\gamma'})$. Since $\gamma, \gamma' \vdash (\mu \uplus \mu')\,|_{\gamma' \cup \gamma''} : (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$, we have $a@r \in \mathit{dom}\,((\Sigma, \Sigma')\,|_{\gamma' \cup \gamma''})$. Since $\mathit{dom}\,(\Sigma\,|_{\gamma'}) = \emptyset$ and $r \in \gamma'$ (from $a@r \in \mathit{dom}\,(\mu'\,|_{\gamma'})$), we have $a@r \in \mathit{dom}\,(\Sigma'\,|_{\gamma' \cup \gamma''}) \subseteq \mathit{dom}\,(\Sigma')$.

Next, we show $\mathit{dom}\,(\Sigma') \subseteq \mathit{dom}\,(\mu')$. Let $a@r \in \mathit{dom}\,(\Sigma')$. Since $\mathit{dom}\,(\Sigma') = \mathit{dom}\,(\Sigma'\,|_{\gamma'})$, we have $r \in \gamma'$. Thus, since $\gamma, \gamma' \vdash (\mu \uplus \mu')\,|_{\gamma' \cup \gamma''} : (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$, we have $a@r \in \mathit{dom}\,(\mu \uplus \mu')$. Since $r \in \gamma'$ and $\mathit{dom}\,(\mu\,|_{\gamma'}) = \emptyset$, we have $a@r \in \mathit{dom}\,(\mu')$. □

Lemma 93. *If $\mu; \Sigma; \gamma; \emptyset \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and $\mu \mid c \longrightarrow \mu' \mid c'$, then one of the followings holds:*

- $\mu = \mu'$;
- $\mu' = \mu \uplus \{a@r \mapsto v\}$ *for some a, $r \in \gamma_{\mathtt{w}}$, and v.*

- *there exists some μ'', a, $r \in \gamma_{\mathtt{w}}$, v, and v' such that $\mu = \mu'' \uplus \{a@r \mapsto v\}$ and $\mu' = \mu'' \uplus \{a@r \mapsto v'\}$.*

Proof. Straightforward by strong induction on the typing derivation except for (CT_Bind) and (CT_Assign); the case for (CT_Assign) rests on Lemma 59 (3).

We consider the case for (CT_Bind): we are given $c = y \leftarrow e'_1; c'_2$ for some y, e'_1, and c'_2. By inversion, $\Sigma; \gamma; \emptyset \vdash e'_1 : \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$ and $\emptyset; \Sigma; \gamma; y{:}T' \vdash c'_2 : \{A_3\}x{:}T\{A_2\}^{\varrho_1}$ for some T', A_3, ϱ_1, and ϱ_2 such that $\varrho_1 \cup \varrho_2 = \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$. By case analysis on the computation rule applied to c.

Case (C_Red), (C_RBlame), (C_CBlame), (C_Return), and (C_Region): $\mu = \mu'$ obviously.

Case (C_Comput): We are given $e'_1 = \mathsf{do}\, c'_1$ for some c'_1, and $\mu \mid c'_1 \longrightarrow \mu' \mid c''_1$. By Lemmas 65, 56 and 89, $\mu; \Sigma; \gamma; \emptyset \vdash c'_1 : \{A''_1\}y{:}T''\{A''_3\}^{\varrho_1}$ for some A''_1, T'', and A''_3; the length of its derivation is smaller than that of $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, c'_1 : \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$. Thus, we can apply the IH and so we finish since $\varrho_1 \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$.

□

Lemma 94. *If*

- $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ *and*
- $\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $\mu; \Sigma; \gamma; \emptyset \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
- $\mu \mid c \longrightarrow \mu' \mid c'$,
- $\gamma \vdash \mu'|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} : (\Sigma, \Sigma')^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$, *and*
- $dom\,(\Sigma') = dom\,(\Sigma'|_{{\gamma_{\mathtt{w}}}'})$,

then $\gamma \vdash \mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$.

Proof. It suffices to show what follows.

- We show that $dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}) = dom\,((\Sigma, \Sigma')|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$.

  We first show that
  $$dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}) \subseteq dom\,((\Sigma, \Sigma')|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}).$$
  Let $a@r \in dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. If $a@r \in dom\,(\mu)$, then $a@r \in dom\,(\Sigma)$ since $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$. Otherwise, if $a@r \notin dom\,(\mu)$, then $r \in {\gamma_{\mathtt{w}}}'$ by Lemma 93. Since $\gamma \vdash \mu'|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} : (\Sigma, \Sigma')^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$, we have $a@r \in dom\,((\Sigma, \Sigma')|_{{\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}'}) \subseteq dom\,((\Sigma, \Sigma')|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$.

  Next, we show that
  $$dom\,((\Sigma, \Sigma')|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}) \subseteq dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}).$$
  Let $a@r \in dom\,(\Sigma|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. Since $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $a@r \in dom\,(\mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. Since $dom\,(\mu) \subseteq dom\,(\mu')$ by Lemma 93, have $a@r \in dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. Let $a@r \in dom\,(\Sigma'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. Since $dom\,(\Sigma') = dom\,(\Sigma'|_{{\gamma_{\mathtt{w}}}'})$, we have $a@r \in dom\,(\Sigma'|_{{\gamma_{\mathtt{w}}}'})$. Since $\gamma \vdash \mu'|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} : (\Sigma, \Sigma')^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$, we have $a@r \in dom\,(\mu'|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}) \subseteq dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$.

- We show that, for any $a@r \in dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$, $\Sigma, \Sigma'; \gamma; \emptyset \vdash \mu'(a@r) : (\Sigma, \Sigma')(a@r)$. Let $a@r \in dom\,(\mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. If $r \in {\gamma_{\mathtt{w}}}'$, then we finish since $a@r \in dom\,(\mu'|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'})$ and $\gamma \vdash \mu'|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} : (\Sigma, \Sigma')^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$. Otherwise, if $r \notin {\gamma_{\mathtt{w}}}'$, then $\mu'(a@r) = \mu(a@r)$ and $a@r \in dom\,(\mu)$ (thus, $a@r \in dom\,(\mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$) by Lemma 93. Since $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we finish by Lemma 42 (4).

□

Lemma 95 (Preservation)**.**

(1) If $\Sigma; \gamma; \emptyset \vdash e : T$ and $e \longrightarrow e'$, then $\Sigma; \gamma; \emptyset \vdash e' : T$.

(2) If

- $\mu; \Sigma; \gamma; \emptyset \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$,
- $\mu \models A_1$,
- $\mu \mid c \longrightarrow \mu' \mid c'$,

then there exist some Σ' *and* A'_1 *such that:*

- $\mu'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c' \,:\, \{A'_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$*;*
- $\gamma \vdash \mu'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \,:\, (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$*; and*
- $\mu' \models A'_1$*;*
- $\mathit{dom}\,(\Sigma') \;=\; \mathit{dom}\,(\Sigma'|_{\gamma_{\mathtt{w}}})$*.*

(3) If

- $\mu; \Sigma; \gamma \vdash p \,:\, T^{\gamma''}$*,*
- $\gamma \vdash \mu|_{\gamma''} \,:\, \Sigma^{\gamma''}$*, and*
- $\mu \mid p \hookrightarrow p'$*,*

then $\mu; \Sigma; \gamma \vdash p' \,:\, T^{\gamma''}$*.*

Proof. By strong induction on the lengths of the typing derivations.

1. Since $e \longrightarrow e'$, there exist some E, e_1, and e_2 such that $e \;=\; E[e_1]$ and $e' \;=\; E[e_2]$ and $e_1 \rightsquigarrow e_2$. By case analysis on the typing rule applied last.

Case (T_Var), (T_Const), (T_Abs), (T_Cast), (T_Address), (T_Do), (T_RAbs), (T_Blame), (T_Guard), (T_Exact), and (T_Forget): Contradictory.

Case (T_Op): We are given $\Sigma; \gamma; \emptyset \vdash \mathit{op}(e'_1, \dots, e'_n) \,:\, [\, e'_1/x_1, \dots, e'_n/x_n \,]\, T'$ and, by inversion, $\mathit{ty}\,(\mathit{op}) \;=\; x_1{:}T_1 \rightarrow \dots \rightarrow x_n{:}T_n \rightarrow T'$ and, for any $i \leq n$, $\Sigma; \gamma; \emptyset \vdash e'_i \,:\, [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1} \,]\, T_i$. Since $E[e_1] \;=\; e = \mathit{op}(e'_1, \dots, e'_n)$, there are two cases by case analysis on E.

Case $E \;=\; [\,]$: Since the only reduction rule applicable to $\mathit{op}(e'_1, \dots, e'_n)$ is (R_Op). Thus, $e' \;=\; [\![\mathit{op}]\!](e'_1, \dots, e'_n)$. By the assumption of op, we finish.

Case $E \;=\; \mathit{op}(e'_1, \dots, e'_{i-1}, E', e'_{i+1}, \dots, e'_n)$ where e'_j is a value for any $j \;<\; i$: By the IH, $\Sigma; \gamma; \emptyset \vdash E'[e'_2] \,:\, [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1} \,]\, T_i$. Since $\emptyset; \emptyset; \emptyset \vdash x_1{:}T_1 \rightarrow \dots \rightarrow x_n{:}T_n \rightarrow T$ by the assumption of $\mathit{ty}\,(\mathit{op})$, we have $\Sigma; \gamma; \emptyset \vdash x_1{:}T_1 \rightarrow \dots \rightarrow x_n{:}T_n \rightarrow T$ by Lemmas 40 (2) and 42 (2). For any $j > i$, if

$$\Sigma; \gamma; \emptyset \vdash [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_2]/x_i, e'_{i+1}/x_{i+1}, \dots, e'_{j-1}/x_{j-1} \,]\, T_j,$$

then

$$\Sigma; \gamma; \emptyset \vdash e'_j \,:\, [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_2]/x_i, e'_{i+1}/x_{i+1}, \dots, e'_{j-1}/x_{j-1} \,]\, T_j$$

by (T_Conv), since

$$\begin{array}{rl} & [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_1]/x_i, e'_{i+1}/x_{i+1}, \dots, e'_{j-1}/x_{j-1} \,]\, T_j \\ \equiv & [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_2]/x_i, e'_{i+1}/x_{i+1}, \dots, e'_{j-1}/x_{j-1} \,]\, T_j, \end{array}$$

and then

$$\Sigma; \gamma; \emptyset \vdash [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_2]/x_i, e'_{i+1}/x_{i+1}, \dots, e'_j/x_j \,]\, T_{j+1}$$

by Lemma 46 (2). Thus, since $\Sigma; \gamma; \emptyset \vdash [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_2]/x_i \,]\, T_{i+1}$ by Lemma 46 (2), we have

$$\Sigma; \gamma; \emptyset \vdash e'_j \,:\, [\, e'_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_2]/x_i, e'_{i+1}/x_{i+1}, \dots, e'_{j-1}/x_{j-1} \,]\, T_j$$

for any $j > i$. By (T_Op),

$$\Sigma; \gamma; \emptyset \vdash \mathit{op}(e'_1, \dots, e'_n) \,:\, [\, e_1/x_1, \dots, e'_{i-1}/x_{i-1}, E'[e'_2]/x_i, e'_{i+1}/x_{i+1}, \dots, e'_n/x_n \,]\, T'.$$

By Lemmas 86 (2) and 51 and (T_Conv), we finish.

Case (T_App): We are given $\Sigma; \gamma; \emptyset \vdash e'_1\, e'_2 \,:\, [\, e'_2/x \,]\, T'_2$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e'_1 \,:\, x{:}T'_1 \rightarrow T'_2$ and $\Sigma; \gamma; \emptyset \vdash e'_2 \,:\, T'_1$. Since $E[e_1] \;=\; e = e'_1\, e'_2$, there are three cases by case analysis on E.

Case $E \;=\; [\,]$: By case analysis on the reduction rule applied to $e'_1\, e'_2$. Note that e'_1 and e'_2 are values in the following.

Case (R_Beta): We are given $e'_1 \;=\; \lambda x{:}T''_1.e''$ for some T''_1 and e'' (note we can suppose that the bound variable is x from Lemma 59 (2)), and $e'_1\, e'_2 \;\rightsquigarrow\; [\, e'_2/x \,]\, e''$. By Lemma 61, $\Sigma; \gamma; x{:}T''_1 \vdash e'' \,:\, T''_2$ and $x{:}T''_1 \rightarrow T''_2 \;\equiv\; x{:}T'_1 \rightarrow T'_2$ for some T''_2. By Lemmas 53 and 51, $T'_1 \;\equiv\; T''_1$ and $T''_2 \;\equiv\; T'_2$. By Lemma 86 (2) and its inversion, $\Sigma; \gamma; \emptyset \vdash T''_1$ and $\Sigma; \gamma; x{:}T''_1 \vdash T''_2$. Since $\Sigma; \gamma; \emptyset \vdash e'_2 \,:\, T''_1$ by (T_Conv), $\Sigma; \gamma; \emptyset \vdash [\, e'_2/x \,]\, e'' \,:\, [\, e'_2/x \,]\, T''_2$ by Lemma 46 (4). Since $[\, e'_2/x \,]\, T''_2 \;\equiv\; [\, e'_2/x \,]\, T'_2$ by Lemma 74, we finish by Lemma 86 (2) and (T_Conv).

Case (R_Base): We are given $e'_1 = \langle B \Leftarrow B\rangle^{\ell}$ for some B and ℓ, and $e'_1\, e'_2 \rightsquigarrow e'_2$. By Lemmas 62, 53 and 52, $T'_1 = T'_2 = B$. Thus, we finish since $[\, e'_2/x \,]\, T'_1 = B$.

Case (R_Fun): We are given $e'_1 = \langle y{:}T''_{11} \rightarrow T''_{12} \Leftarrow y{:}T''_{21} \rightarrow T''_{22}\rangle^{\ell}$ for some y, T''_{11}, T''_{12}, T''_{21}, T''_{22}, and ℓ, and $e'_1\, e'_2 \rightsquigarrow \lambda y{:}T''_{11}.\mathsf{let}\, z = \langle T''_{21} \Leftarrow T''_{11}\rangle^{\ell}\, y \,\mathsf{in}\, \langle T''_{12} \Leftarrow [\, z/y \,]\, T''_{22}\rangle^{\ell}\, (e'_2\, z)$ for some fresh variable z. By Lemma 62, $\Sigma;\gamma;\emptyset \vdash y{:}T''_{11} \rightarrow T''_{12}$ and $\Sigma;\gamma;\emptyset \vdash y{:}T''_{21} \rightarrow T''_{22}$ and $y{:}T''_{11} \rightarrow T''_{12} \parallel y{:}T''_{21} \rightarrow T''_{22}$ and $(y{:}T''_{21} \rightarrow T''_{22}) \rightarrow (y{:}T''_{11} \rightarrow T''_{12}) \equiv \mathit{unref}\,(x{:}T'_1 \rightarrow T'_2)$. By inversion, $T''_{11} \parallel T''_{21}$ (and so $T''_{21} \parallel T''_{11}$ by Lemma 77) and $T''_{12} \parallel T''_{22}$.

Since $T'_1 \equiv y{:}T''_{21} \rightarrow T''_{22}$ by Lemmas 53 and 51 (3), we have $\Sigma;\gamma;\emptyset \vdash e'_2 : y{:}T''_{21} \rightarrow T''_{22}$. Thus, by Lemma 44 (4) and (T_App),

$$\Sigma;\gamma;z{:}T''_{21} \vdash e'_2\, z : [\, z/y \,]\, T''_{22}.$$

Since $T''_{12} \parallel [\, z/y \,]\, T''_{22}$ by Lemma 45 (2), we have $\Sigma;\gamma;y{:}T''_{11}, z{:}T''_{21} \vdash \langle T''_{12} \Leftarrow [\, z/y \,]\, T''_{22}\rangle^{\ell} : [\, z/y \,]\, T''_{22} \rightarrow T''_{12}$ by Lemmas 86 (2) and 44 (2). By Lemma 44 (4) and (T_App),

$$\Sigma;\gamma;y{:}T''_{11}, z{:}T''_{21} \vdash \langle T''_{12} \Leftarrow [\, z/y \,]\, T''_{22}\rangle^{\ell}\, (e'_2\, z) : T''_{12}.$$

Since $T''_{21} \parallel T''_{11}$ and $\Sigma;\gamma;\emptyset \vdash T''_{11}$ and $\Sigma;\gamma;\emptyset \vdash T''_{21}$ by inversion, we have $\Sigma;\gamma;y{:}T''_{11} \vdash \langle T''_{21} \Leftarrow T''_{11}\rangle^{\ell}\, y : T''_{21}$. Thus, by (T_Abs) and (T_App),

$$\Sigma;\gamma;y{:}T''_{11} \vdash \mathsf{let}\, z = \langle T''_{21} \Leftarrow T''_{11}\rangle^{\ell}\, y \,\mathsf{in}\, \langle T''_{21} \Leftarrow [\, z/y \,]\, T''_{22}\rangle^{\ell}\, (e'_2\, z) : T''_{12}.$$

By (T_Abs),

$$\Sigma;\gamma;\emptyset \vdash \lambda y{:}T''_{11}.\mathsf{let}\, z = \langle T''_{21} \Leftarrow T''_{11}\rangle^{\ell}\, y \,\mathsf{in}\, \langle T''_{21} \Leftarrow [\, z/y \,]\, T''_{22}\rangle^{\ell}\, (e'_2\, z) : y{:}T''_{11} \rightarrow T''_{12}.$$

Since $[\, e'_2/x \,]\, (y{:}T''_{11} \rightarrow T''_{12}) = y{:}T''_{11} \rightarrow T''_{12}$, we have $y{:}T''_{11} \rightarrow T''_{12} \equiv [\, e'_2/x \,]\, T'_2$ by Lemmas 53 and 74. Thus, we finish by Lemma 86 (2) and (T_Conv).

Case (R_Forget): We are given $e'_1 = \langle T''_1 \Leftarrow \{y{:}T''_2 \mid c''_2\}\rangle^{\ell}$ for some T''_1, y, T''_2, c''_2, and ℓ, and $e'_1\, e'_2 \rightsquigarrow \langle T''_1 \Leftarrow T''_2\rangle^{\ell}\, e'_2$. By Lemma 62, $T''_1 \parallel \{y{:}T''_2 \mid c''_2\}$ and $\Sigma;\gamma;\emptyset \vdash T''_1$ and $\Sigma;\gamma;\emptyset \vdash \{y{:}T''_2 \mid c''_2\}$ and $\{y{:}T''_2 \mid c''_2\} \rightarrow T''_1 \equiv x{:}T'_1 \rightarrow T'_2$. Since $T''_1 \parallel T''_2$ by Lemma 78 (1), and $\Sigma;\gamma;\emptyset \vdash T''_2$ by inversion, and $\Sigma;\gamma;\emptyset \vdash e'_2 : T''_2$ by Lemmas 53 and 51 (3) and (T_Conv) and (T_Forget), we have

$$\Sigma;\gamma;\emptyset \vdash \langle T''_1 \Leftarrow T''_2\rangle^{\ell}\, e'_2 : T''_1$$

by (T_Cast) and (T_App). Since $[\, e'_2/x \,]\, T''_1 = T''_1$, we have $T''_1 \equiv [\, e'_2/x \,]\, T'_2$ by Lemma 74. By Lemma 86 (2) and (T_Conv), $\Sigma;\gamma;\emptyset \vdash \langle T''_1 \Leftarrow T''_2\rangle^{\ell}\, e'_2 : [\, e'_2/x \,]\, T'_2$.

Case (R_PreCheck): We are given $e'_1 = \langle \{y{:}T''_1 \mid c''_1\} \Leftarrow T''_2\rangle^{\ell}$ for some y, T''_1, c''_1, T''_2, and ℓ such that T''_2 is not a refinement type, and $e'_1\, e'_2 \rightsquigarrow \langle\!\langle \{y{:}T''_1 \mid c''_1\}, \langle T''_1 \Leftarrow T''_2\rangle^{\ell}\, e'_2 \rangle\!\rangle^{\ell}$. By Lemma 62, $\{y{:}T''_1 \mid c''_1\} \parallel T''_2$ and $\Sigma;\gamma;\emptyset \vdash \{y{:}T''_1 \mid c''_1\}$ and $\Sigma;\gamma;\emptyset \vdash T''_2$ and $T''_2 \rightarrow \{y{:}T''_1 \mid c''_1\} \equiv x{:}T'_1 \rightarrow T'_2$. Since $T''_1 \parallel T''_2$ by Lemma 78 (2), and $\Sigma;\gamma;\emptyset \vdash T''_1$ by inversion, we have

$$\Sigma;\gamma;\emptyset \vdash \langle T''_1 \Leftarrow T''_2\rangle^{\ell}\, e'_2 : T''_1$$

by (T_Catt) and (T_App). By (T_WCheck), we finish.

Case (R_Ref): We are given $e'_1 = \langle \mathsf{Ref}_r\, T''_1 \Leftarrow \mathsf{Ref}_r\, T''_2\rangle^{\ell}$ for some r, T''_1, T''_2, and ℓ, and $e'_1\, e'_2 \rightsquigarrow T''_1 \Leftarrow^{\ell} T''_2 : e'_2$. By Lemma 62, $\mathsf{Ref}_r\, T''_1 \parallel \mathsf{Ref}_r\, T''_2$ and $\Sigma;\gamma;\emptyset \vdash \mathsf{Ref}_r\, T''_1$ and $\Sigma;\gamma;\emptyset \vdash \mathsf{Ref}_r\, T''_2$ $\mathsf{Ref}_r\, T''_2 \rightarrow \mathsf{Ref}_r\, T''_1 \equiv x{:}T'_1 \rightarrow T'_2$. Since $T'_1 \equiv \mathsf{Ref}_r\, T''_2$ by Lemmas 53 and 51 (3), we have $\Sigma;\gamma;\emptyset \vdash e'_2 : \mathsf{Ref}_r\, T''_2$ by (T_Conv). Since $T''_1 \parallel T''_2$ by inversion of $\mathsf{Ref}_r\, T''_1 \parallel \mathsf{Ref}_r\, T''_2$, we have, by (T_Guard),

$$\Sigma;\gamma;\emptyset \vdash T''_1 \Leftarrow^{\ell} T''_2 : e'_2 : \mathsf{Ref}_r\, T''_1.$$

Since $\mathsf{Ref}_r\, T''_1 = [\, e'_2/x \,]\, (\mathsf{Ref}_r\, T''_1) \equiv [\, e'_2/x \,]\, T'_2$ by Lemmas 53 and 74, we finish by Lemma 86 (2) and (T_Conv).

Case (R_RefFail): By Lemma 86 (2) and (T_Blame).

Case (R_RFun): We are given $e'_1 = \langle \forall r.\, T''_1 \Leftarrow \forall r.\, T''_2\rangle^{\ell}$ for some r, T''_1, T''_2 and ℓ, and $e'_1\, e'_2 \rightsquigarrow \lambda r.\langle T''_1 \Leftarrow T''_2\rangle^{\ell}\, (e'_2\{r\})$. Without loss of generality ,we can suppose that r is fresh. By Lemma 62, $\forall r.\, T''_1 \parallel \forall r.\, T''_2$ and $\Sigma;\gamma;\emptyset \vdash \forall r.\, T''_1$ and $\Sigma;\gamma;\emptyset \vdash \forall r.\, T''_2$ and $\forall r.\, T''_2 \rightarrow \forall r.\, T''_1 \equiv x{:}T'_1 \rightarrow T'_2$. By inversion, $T''_1 \parallel T''_2$ and $\Sigma;\gamma;r \vdash T''_1$ and $\Sigma;\gamma;r \vdash T''_2$. Since $\Sigma;\gamma;r \vdash e'_2 : \forall r.\, T''_2$ by Lemmas 53 and 51 (3) and (T_Conv), we have $\Sigma;\gamma;r \vdash e'_2\{r\} : [\, r/r \,]\, T''_2 = T''_2$ by (T_RApp), and so

$$\Sigma;\gamma;\emptyset \vdash \lambda r.\langle T''_1 \Leftarrow T''_2\rangle^{\ell}\, (e'_2\{r\}) : \forall r.\, T''_1$$

by (T_Cast), (T_App), and (T_RAbs). Since $\forall r.\, T''_1 = [\, e'_2/x \,]\, (\forall r.\, T''_1) \equiv [\, e'_2/x \,]\, T'_2$ by Lemma 74, we finish by Lemma 86 (2) and (T_Conv).

Case (R_Hoare): We are given $e'_1 = \langle \{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1} \Leftarrow \{A_{21}\} y{:}T''_2 \{A_{22}\}^{\varrho_2} \rangle^\ell$ for some A_{11}, y, A_{12}, A_{21}, T''_2, A_{22}, and ℓ such that $\varrho_2 \subseteq \varrho_1$, and

$$e'_1\; e'_2 \rightsquigarrow \mathsf{do}\,\mathsf{assert}\,(A_{21})^\ell; z \leftarrow e'_2; \mathsf{let}\, y = \langle T''_1 \Leftarrow T''_2 \rangle^\ell\, z; \mathsf{assert}\,(A_{12})^\ell; \mathsf{return}\, y$$

for some fresh variable z. Without loss of generality, we can suppose that y is fresh. By Lemma 62,

- $\{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1} \parallel \{A_{21}\} y{:}T''_2 \{A_{22}\}^{\varrho_2}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_{21}\} y{:}T''_2 \{A_{22}\}^{\varrho_2}$, and
- $\{A_{21}\} y{:}T''_2 \{A_{22}\}^{\varrho_2} \rightarrow \{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1} \equiv x{:}T'_1 \rightarrow T'_2$.

By inversion, $T''_1 \parallel T''_2$ and $\Sigma; \gamma; y{:}T''_1 \vdash^{\varrho_1} A_{12}$ and $\Sigma; \gamma; \emptyset \vdash T''_1$ and $\Sigma; \gamma; \emptyset \vdash^{\varrho_2} A_{21}$ and $\Sigma; \gamma; \emptyset \vdash T''_2$. By (T_Cast) and (T_App), $\Sigma; \gamma; z{:}T''_2 \vdash \langle T''_1 \Leftarrow T''_2 \rangle^\ell\, z : T''_1$. By (CT_Return), (CT_Assert), (T_Do), (CT_Bind), and Lemma 44,

$$\emptyset; \Sigma; \gamma; z{:}T''_2 \vdash \mathsf{let}\, y = \langle T''_1 \Leftarrow T''_2 \rangle^\ell\, z; \mathsf{assert}\,(A_{12})^\ell; \mathsf{return}\, y : \{\top\} y{:}T''_1 \{A_{12}\}^{\varrho_1}.$$

Since $\Sigma; \gamma; \emptyset \vdash e'_2 : \{A_{21}\} y{:}T''_2 \{A_{22}\}^{\varrho_2}$ by Lemmas 53 and 51 (3) and (T_Conv), and $\varrho_2 \subseteq \varrho_1$, we have

$$\emptyset; \Sigma; \gamma; \emptyset \vdash z \leftarrow e'_2; \mathsf{let}\, y = \langle T''_1 \Leftarrow T''_2 \rangle^\ell\, z; \mathsf{assert}\,(A_{12})^\ell; \mathsf{return}\, y : \{A_{21}\} y{:}T''_1 \{A_{12}\}^{\varrho_1}$$

by (CT_Weak) and (CT_Bind). By (CT_Assert) and (CT_Weak),

$$\emptyset; \Sigma; \gamma; \emptyset \vdash \mathsf{assert}\,(A_{21})^\ell; z \leftarrow e'_2; \mathsf{let}\, y = \langle T''_1 \Leftarrow T''_2 \rangle^\ell\, z; \mathsf{assert}\,(A_{12})^\ell; \mathsf{return}\, y : \{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1}.$$

Since

$$\Sigma; \gamma; \emptyset \vdash \mathsf{do}\,\mathsf{assert}\,(A_{21})^\ell; z \leftarrow e'_2; \mathsf{let}\, y = \langle T''_1 \Leftarrow T''_2 \rangle^\ell\, z; \mathsf{assert}\,(A_{12})^\ell; \mathsf{return}\, y : \{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1}$$

by (T_Do), and $\{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1} = [\, e'_2/x \,] (\{A_{11}\} y{:}T''_1 \{A_{12}\}^{\varrho_1}) \equiv [\, e'_2/x \,]\, T'_2$ by Lemmas 53 and 74, we finish by Lemma 86 (2) and (T_Conv).

Case (R_HoareFail): By Lemma 86 (2) and (T_Blame).

Case $E = E'\, e'_2$: By the IH and (T_App).

Case $E = e'_1\, E'$ where e'_1 is a value: By the IH and (T_App), $\Sigma; \gamma; \emptyset \vdash e'_1\, E'[e'_2] : [\, E'[e'_2]/x \,]\, T'_1$. Since $[\, E'[e'_2]/x \,]\, T'_2 \equiv [\, E'[e'_1]/x \,]\, T'_1$, we finish by Lemma 86 (2) and (T_Conv).

Case (T_Eq): We are given $\Sigma; \gamma; \emptyset \vdash e'_1 =\!= e'_2 : \mathsf{bool}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e'_1 : \mathsf{Ref}_r\, T'_1$ and $\Sigma; \gamma; \emptyset \vdash e'_2 : \mathsf{Ref}_s\, T'_2$ and $T'_1 \parallel T'_2$. Since $E[e_1] = e = e'_1 =\!= e'_2$, there are three cases we have to consider by case analysis on E.

Case $E = [\,]$: By case analysis on the reduction rule applied to $e'_1 =\!= e'_2$. Note that e'_1 and e'_2 are values in the following.

Case (R_Eq): We are given $\mathit{ungrd}\,(e'_1) = \mathit{ungrd}\,(e'_2)$ and $e'_1 =\!= e'_2 \rightsquigarrow \mathsf{true}$. By (T_Const) (and (T_Forget) if necessary), we finish.

Case (R_NEq): We are given $\mathit{ungrd}\,(e'_1) \neq \mathit{ungrd}\,(e'_2)$ and $e'_1 =\!= e'_2 \rightsquigarrow \mathsf{false}$. By (T_Const) (and (T_Forget) if necessary), we finish.

Case $E = E' =\!= e'_2$: By the IH and (T_Eq).

Case $E = e'_1 =\!= E'$ where e'_1 is a value: By the IH and (T_Eq).

Case (T_REq): We are given $\Sigma; \gamma; \emptyset \vdash r =\!= s : \mathsf{bool}$. Since $E[e_1] = e = (r =\!= s)$, we have $E = [\,]$ and $e_1 = (r =\!= s)$. The reduction rules applicable to $r =\!= s$ are only (R_REq) and (R_RNEq). Thus, e_2 is a Boolean value, so we finish by (T_Const) (and (T_Forget) if Boolean values are given types with refinements).

Case (T_RApp): We are given $\Sigma; \gamma; \emptyset \vdash e'_1\{r\} : [\, r/s \,]\, T'$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e'_1 : \forall s. T'$ and $r \in \gamma$. Since $E[e_1] = e = e'_1\{r\}$, there are two cases we have to consider by case analysis on E.

Case $E = [\,]$: We can suppose that e'_1 is a value since the reduction rule applicable to $e'_1\{r\}$ is only (R_RBeta). By Lemma 59 (5), $e'_1 = \lambda s. e''_1$ for some e''_1. Thus, we are given $e'_1\{r\} \rightsquigarrow [\, r/s \,]\, e''_1$. By Lemma 66, $\Sigma; \gamma; s \vdash e''_1 : T''$ for some T'' such that $\forall s. T'' \equiv \forall s. T'$. By Lemma 75, $[\, r/s \,]\, T'' \equiv [\, r/s \,]\, T'$. Since $\Sigma; \gamma; \emptyset \vdash [\, r/s \,]\, e''_1 : [\, r/s \,]\, T''$ by Lemma 50 (4), $\Sigma; \gamma; \emptyset \vdash [\, r/s \,]\, e''_1 : [\, r/s \,]\, T'$ by Lemma 86 (2) and (T_Conv).

Case $E = E'\{r\}$: By the IH and (T_RApp).

Case (T_WCheck): We are given $\Sigma; \gamma; \emptyset \vdash \langle\!\langle \{x{:}T' \mid c'\}, e' \rangle\!\rangle^\ell : \{x{:}T' \mid c'\}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash \{x{:}T' \mid c'\}$ and $\Sigma; \gamma; \emptyset \vdash e' : T'$. Since $E[e_1] = e$, there are two cases we have to consider by case analysis on E.

Case $E = [\,]$: Since the reduction rule applicable to e is only (R_Check), we can suppose that e' is a value and we are given $\langle\!\langle \{x{:}T' \mid c'\}, e' \rangle\!\rangle^{\ell} \rightsquigarrow \langle \{x{:}T' \mid c'\}, \nu\emptyset.\langle \emptyset \mid c' \rangle, e' \rangle^{\ell}$. By inversion of $\Sigma; \gamma; \emptyset \vdash \{x{:}T' \mid c'\}$, we have $\emptyset; \Sigma; \gamma; x{:}T' \vdash c' \ : \ \{\top\}\mathsf{bool}\{\top\}^{\langle \emptyset, \emptyset \rangle}$, and so $\emptyset; \Sigma; \gamma; \emptyset \vdash [\, e'/x \,]\, c' \ : \ \{\top\}\mathsf{bool}\{\top\}^{\langle \emptyset, \emptyset \rangle}$ by Lemma 46 (5). Thus, since $\gamma \vdash \emptyset \ : \ \Sigma^{\emptyset}$, we finish by (PT) and (T_ACheck).

Case $E = \langle\!\langle \{x{:}T' \mid c'\}, E' \rangle\!\rangle^{\ell}$: By the IH and (T_WCheck).

Case (T_ACheck): We are given $\Sigma; \gamma; \emptyset \vdash \langle \{x{:}T' \mid c'_1\}, p'_2, v' \rangle^{\ell} \ : \ \{x{:}T' \mid c'_1\}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash \{x{:}T' \mid c'_1\}$,
- $\emptyset; \Sigma; \gamma \vdash p'_2 \ : \ \mathsf{bool}^{\emptyset}$,
- $\Sigma; \gamma; \emptyset \vdash v' \ : \ T'$, and
- $\emptyset \mid \nu\emptyset.\langle \emptyset \mid [\, v'/x \,]\, c'_1 \rangle \hookrightarrow^{*} p_2$.

Since $E[e_1] = e$, it is found that $E = [\,]$. By case analysis on the reduction rule applied to e.

Case (R_Checking): We are given $e \rightsquigarrow \langle \{x{:}T' \mid c'_1\}, p''_2, v' \rangle^{\ell}$ for some p''_2 such that $\emptyset \mid p'_2 \hookrightarrow p''_2$. Since $\gamma \vdash \emptyset \ : \ \Sigma^{\emptyset}$, we have $\emptyset; \Sigma; \gamma \vdash p''_2 \ : \ \mathsf{bool}^{\emptyset}$ by the IH (case (3)), Thus, by (T_ACheck), we finish.

Case (R_Blame): By Lemma 86 (2) and (T_Blame).

Case (R_OK): By (T_Exact).

Case (R_Fail): By Lemma 86 (2) and (T_Blame).

Case (T_Conv): By the IH and (T_Conv).

2. By case analysis on the typing rule applied last.

Case (CT_Return): We are given $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, e' \ : \ \{[\, e'/x \,]\, A_1\}x{:}T\{A_1\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e' \ : \ T$ and $\Sigma; \gamma; x{:}T \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A_1$. By case analysis on the computation rule applicable to c.

Case (C_Red): We are given $e' = E'[e'_1]$ and $e'_1 \rightsquigarrow e'_2$ and $\mu \mid c \longrightarrow \mu \mid \mathsf{return}\, E'[e'_2]$ for some E', e'_1, and e'_2. By the IH (case (1)), $\Sigma; \gamma; \emptyset \vdash E'[e'_2] \ : \ T$. By (CT_Return), we have

$$\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, E'[e'_2] \ : \ \{[\, E'[e'_2]/x \,]\, A_1\}x{:}T\{A_1\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Since $e' \longrightarrow E'[e'_2]$, we have $[\, E'[e'_2]/x \,]\, A_1 \equiv [\, e'/x \,]\, A_1$. Thus, by Lemma 86 (3) and (CT_Conv),

$$\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, E'[e'_2] \ : \ \{[\, e'/x \,]\, A_1\}x{:}T\{A_1\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Case (C_RBlame): By Lemma 86 (3) and (CT_Blame).

Case (CT_Bind): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow e'_1; c'_2 \ : \ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e'_1 \ : \ \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$,
- $\emptyset; \Sigma; \gamma; y{:}T' \vdash c'_2 \ : \ \{A_3\}x{:}T\{A_2\}^{\varrho_2}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, and
- $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle = \varrho_1 \cup \varrho_2$

for some y, T', A_3, ϱ_1, and ϱ_2. By case analysis on the computation rule applicable to c.

Case (C_Red): By the IH (case (1)) and (CT_Bind).

Case (C_Comput): We are given $e'_1 = \mathsf{do}\, c'_1$ and $\mu \mid c'_1 \longrightarrow \mu' \mid c''_1$ and $\mu \mid c \longrightarrow \mu' \mid y \leftarrow \mathsf{do}\, c''_1; c'_2$ for some c'_1 and c''_1. Since $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, c'_1 \ : \ \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$, we have $\emptyset; \Sigma; \gamma; \emptyset \vdash c'_1 \ : \ \{A''_1\}y{:}T''\{A''_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$ for some A''_1, T'', A''_3, ${\gamma_{\mathtt{r}}}''$, and ${\gamma_{\mathtt{w}}}''$ such that $\{A''_1\}y{:}T''\{A''_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle} \equiv \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$, by Lemma 65. By Lemma 89 (1), $\mu; \Sigma; \gamma; \emptyset \vdash c'_1 \ : \ \{A''_1\}y{:}T''\{A''_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$. By Lemma 56, we have $A''_1 \equiv A_1$ and $T'' \equiv T'$ and $A''_3 \equiv A_3$ and $\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle = \varrho_1$. Since $\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle = \varrho_1 \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$ and $\gamma \vdash \mu\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ : \ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $\gamma \vdash \mu\,|_{{\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{w}}}''} \ : \ \Sigma^{{\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{w}}}''}$ by Lemma 70. Since $\mu \models A_1$, we have $\mu \models A''_1$ by Lemma 90. Since the length of the derivation of $\mu; \Sigma; \gamma; \emptyset \vdash c'_1 \ : \ \{A''_1\}y{:}T''\{A''_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$ is smaller than that of $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, c'_1 \ : \ \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$ by Lemmas 65 and 89 (1), we can apply the IH: there exist some Σ' and A'_1 such that

* $\mu'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c'_1 \ : \ \{A'_1\}y{:}T''\{A''_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$,
* $\gamma \vdash \mu'\,|_{{\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{w}}}''} \ : \ (\Sigma, \Sigma')^{{\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{w}}}''}$,
* $\mu' \models A'_1$, and
* $\mathit{dom}\,(\Sigma') = \mathit{dom}\,(\Sigma'\,|_{{\gamma_{\mathtt{w}}}''})$.

Since $\Sigma, \Sigma'; \gamma; \emptyset \vdash^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle} A_1'$ by Lemma 86 (3), and $\gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \subseteq \gamma$ by Lemmas 86 (3) and 39, we have $\Sigma, \Sigma'; \gamma; \emptyset \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A_1'$ by Lemma 48 (2), and so $\Sigma, \Sigma'; \gamma; \emptyset \vdash \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ by Lemmas 42 (2) and (3) and (WF_Hoare). Since $\{A_1'\}y{:}T''\{A_3''\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle} \equiv \{A_1'\}y{:}T'\{A_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$ by Lemmas 85 (2) and (3), and $\Sigma, \Sigma'; \gamma; \emptyset \vdash \{A_1'\}y{:}T'\{A_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$ by Lemmas 42 (2) and (3) and (WF_Hoare), we have $\mu'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c_1' : \{A_1'\}y{:}T'\{A_3\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$ by (CT_Conv). By Lemma 42 (5) and (CT_CBind), we have

$$\mu'; \Sigma, \Sigma'; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1''; c_2' : \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Since ${\gamma_{\mathtt{w}}}'' \subseteq \gamma_{\mathtt{w}}$, we have $dom\,(\Sigma') = dom\,(\Sigma' \,|_{\gamma_{\mathtt{w}}})$. Thus, it suffices to show that $\gamma \vdash \mu' \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, which is proven by Lemma 94.

Case (C_RBlame): By Lemma 86 (3) and (CT_Blame).

Case (C_CBlame): By Lemma 86 (3) and (CT_Blame).

Case (C_Return): We are given $e_1' = \mathsf{do}\, \mathsf{return}\, v_1'$ for some v_1' and $\mu \mid c \longrightarrow \mu \mid [\, v_1'/y \,]\, c_2'$. By Lemmas 65 and 56, $\emptyset; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1' : \{A_1''\}y{:}T''\{A_3''\}^{\varrho_1}$ for some A_1'', T'', and A_3'' such that $A_1 \equiv A_1''$ and $T' \equiv T''$ and $A_3 \equiv A_3''$. By Lemmas 60 and 86 (3) and (T_Conv), we have $\Sigma; \gamma; \emptyset \vdash v_1' : T'$. By Lemma 46 (5), $\emptyset; \Sigma; \gamma; \emptyset \vdash [\, v_1'/y \,]\, c_2' : \{[\, v_1'/y \,]\, A_3\}x{:}T\{A_2\}^{\varrho_2}$. By Lemma 89 (1),

$$\mu; \Sigma; \gamma; \emptyset \vdash [\, v_1'/y \,]\, c_2' : \{[\, v_1'/y \,]\, A_3\}x{:}T\{A_2\}^{\varrho_2}.$$

Since $A_1 \equiv A_1''$ and $\mu \models A_1$, we have $\mu \models A_1''$ by Lemma 90. Since $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1' : \{A_1''\}y{:}T''\{A_3''\}^{\varrho_1}$ by Lemma 89 (1), we have $\mu \models [\, v_1'/y \,]\, A_3''$ by Lemma 91. Since $\{A_1''\}y{:}T''\{A_3''\}^{\varrho_1} \equiv \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$ from Lemma 65, we have $[\, v_1'/y \,]\, A_3'' \equiv [\, v_1'/y \,]\, A_3$ by Lemmas 74 and 56. By Lemma 90,

$$\mu \models [\, v_1'/y \,]\, A_3.$$

Note that we let Σ' be empty.

Case (C_Region): We are given $e_1' = \mathsf{do}\, \nu r.\, c_1'$ and $\mu \mid c \longrightarrow \mu \mid \nu r.\, x \leftarrow \mathsf{do}\, c_1'; c_2'$ for some r and c_1' such that $r \notin \mathit{frv}\,(c_2')$. Without loss of generality, we can suppose that $r \notin \gamma$. By Lemmas 65 and 56, $\emptyset; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1' : \{A_1''\}y{:}T''\{A_3''\}^{\varrho_1}$ for some A_1'', T'', and A_3'' such that $A_1 \equiv A_1''$ and $T' \equiv T''$ and $A_3 \equiv A_3''$. By Lemmas 87 and 89 (1), $\mu; \Sigma; \gamma, r; \emptyset \vdash c_1' : \{A_1''\}y{:}T''\{A_3''\}^{\varrho_1 \uplus \{r\}}$. By Lemma 40 (5), $\emptyset; \Sigma; \gamma, r; y{:}T' \vdash c_2' : \{A_3\}x{:}T\{A_2\}^{\varrho_2}$, and by Lemmas 40 (2) and 48 (1), $\Sigma; \gamma, r; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \uplus \{r\}}$. Thus, by Lemma 86 (3), (CT_CBind), and (CT_LetRegion), $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, y \leftarrow \mathsf{do}\, c_1'; c_2' : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$.

Case (CT_CBind): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1'; c_2' : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\mu; \Sigma; \gamma; \emptyset \vdash c_1' : \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $\emptyset; \Sigma; \gamma; y{:}T' \vdash c_2' : \{A_3\}x{:}T\{A_2\}^{\varrho_2}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, and
- $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \cup \varrho_2 = \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$.

By case analysis on the computation rule applicable to c.

Case (C_Red): Contradictory.

Case (C_Comput): We are given $\mu \mid c_1' \longrightarrow \mu' \mid c_1''$ for some c_1''. Since $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have $\gamma \vdash \mu \,|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} : \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$ from $\gamma \vdash \mu \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and Lemma 70. Thus, by the IH, there exist some Σ' and A_1' such that

- $\mu'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c_1'' : \{A_1'\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $\gamma \vdash \mu' \,|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} : (\Sigma, \Sigma')^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$,
- $\mu' \models A_1'$,
- $dom\,(\Sigma') = dom\,(\Sigma' \,|_{\gamma_{\mathtt{w}1}})$.

Since $\Sigma, \Sigma'; \gamma; \emptyset \vdash^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle} A_1'$ by Lemma 86 (3), and $\gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \subseteq \gamma$ by Lemmas 86 (3) and 39, we have $\Sigma, \Sigma'; \gamma; \emptyset \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A_1'$ by Lemma 48 (2), and so $\Sigma, \Sigma'; \gamma; \emptyset \vdash \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ by Lemmas 42 (2) and (3) and (WF_Hoare). By Lemma 42 (5) and (CT_CBind), we have

$$\mu'; \Sigma, \Sigma'; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1''; c_2' : \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Since $\gamma_{\mathtt{w}1} \subseteq \gamma_{\mathtt{w}}$, we have $dom\,(\Sigma') = dom\,(\Sigma' \,|_{\gamma_{\mathtt{w}}})$. Thus, it suffices to show that $\gamma \vdash \mu' \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, which is proven by Lemma 94.

Case (C_RBlame): Contradictory.

Case (C_CBlame): By Lemma 86 (3) and (CT_Blame).

Case (C_Return): We are given $c'_1 \ = \ \mathsf{return}\, v'_1$ for some v'_1, and $\mu \mid c \longrightarrow \mu \mid [\, v'_1/y \,]\, c'_2$. Since $\Sigma; \gamma; \emptyset \vdash v'_1 \ : \ T'$ by Lemma 60, we have

$$\emptyset; \Sigma; \gamma; \emptyset \vdash [\, v'_1/y \,]\, c'_2 \ : \ [\, v'_1/y \,] (\{A_3\} x{:}\, T\{A_2\}^{\varrho_2}) = \{[\, v'_1/y \,]\, A_3\} x{:}\, T\{A_2\}^{\varrho_2}$$

by Lemma 46 (5). Since $\varrho_2 \ \subseteq \ \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have

$$\mu; \Sigma; \gamma; \emptyset \vdash [\, v'_1/y \,]\, c'_2 \ : \ \{[\, v'_1/y \,]\, A_3\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$$

by Lemmas 48 (3) and 89 (1). Since $\mu \models A_1$, we have $\mu \models [\, v'_1/y \,]\, A_3$ by Lemma 91. Thus, we finish.

Case (C_Region): We are given $c'_1 \ = \ \nu r.\, c''_1$ for some r and c''_1. Without loss of generality, we can suppose that r is fresh. We have $\mu \mid c \longrightarrow \mu \mid \nu r.\, y \leftarrow \mathsf{do}\, c''_1; c'_2$. By Lemma 87, $\mu; \Sigma; \gamma, r; \emptyset \vdash c''_1 \ : \ \{A_1\} y{:}\, T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \uplus \{r\}}$. By Lemma 40 (5), $\emptyset; \Sigma; \gamma, r; y{:}\, T' \ \vdash \ c'_2 \ : \ \{A_3\} x{:}\, T\{A_2\}^{\varrho_2}$. By Lemmas 40 (3) and 48 (1), $\Sigma; \gamma, r; \emptyset \vdash \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \uplus \{r\}}$. Thus, by (T_CBind),

$$\mu; \Sigma; \gamma, r; \emptyset \vdash y \leftarrow \mathsf{do}\, c''_1; c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \uplus \{r\}}.$$

By Lemma 86 (3) and (CT_LetRegion),

$$\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, y \leftarrow \mathsf{do}\, c''_1; c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Case (CT_New): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \Leftarrow \mathsf{ref}_r\, e'_1; c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e'_1 \ : \ T'$,
- $\emptyset; \Sigma; \gamma; y{:}\mathsf{Ref}_r\, T' \vdash c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \rangle}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$, and
- $\gamma_{\mathtt{w}} \ = \ {\gamma_{\mathtt{w}}}' \cup \{r\}$.

By case analysis on the computation rule applicable to c.

Case (C_Red): By the IH (case (1)) and (CT_New).

Case (C_RBlame): By Lemma 86 (3) and (CT_Blame).

Case (C_Command)/(C_New): We can suppose that e'_1 is a value. We are given $\mu \mid c \longrightarrow \mu \uplus \{a@r \ \mapsto \ e'_1\} \mid y \leftarrow \mathsf{do}\,\mathsf{return}\, a@r; c'_2$ for some a such that $a@r \ \notin \ \mathit{dom}\,(\mu)$.
We show that $a@r \ \notin \ \mathit{dom}\,(\Sigma)$. If $a@r \ \in \ \mathit{dom}\,(\Sigma)$, then, since $r \ \in \ {\gamma_{\mathtt{w}}}' \cup \{r\} = \gamma_{\mathtt{w}}$ and $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ : \ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $a@r \ \in \ \mathit{dom}\,(\mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}) \subseteq \mathit{dom}\,(\mu)$, which is contradictory since $a@r \ \notin \ \mathit{dom}\,(\mu)$.
Thus, since $\Sigma; \gamma; \emptyset \ \vdash \ \mathsf{Ref}_r\, T'$ by Lemma 86 (3), we have $\Sigma, a@r{:}\, T'; \gamma; \emptyset \ \vdash \ \mathsf{Ref}_r\, T'$ by Lemma 42 (2). By (T_Address), $\Sigma, a@r{:}\, T'; \gamma; \emptyset \ \vdash \ a@r \ \ : \ \mathsf{Ref}_r\, T'$. Since $\Sigma, a@r{:}\, T'; \gamma; y{:}\mathsf{Ref}_r\, T' \ \vdash^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle} \ A_1$ by Lemmas 86 (3), 42 (2) and 44 (3), we have

$$\mu \uplus \{a@r \ \mapsto \ e'_1\}; \Sigma, a@r{:}\, T'; \gamma; \emptyset \vdash \mathsf{return}\, a@r \ : \ \{A_1\} y{:}\mathsf{Ref}_r\, T'\{A_1\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$$

by (CT_Return). Since $\emptyset; \Sigma, a@r{:}\, T'; \gamma; y{:}\mathsf{Ref}_r\, T' \ \vdash \ c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \rangle}$ by Lemma 42 (5), and $\Sigma, a@r{:}\, T'; \gamma; \emptyset \vdash \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$ by Lemma 42 (3), we have

$$\mu \uplus \{a@r \ \mapsto \ e'_1\}; \Sigma, a@r{:}\, T'; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\,\mathsf{return}\, a@r; c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$$

by (CT_CBind).
Since $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ : \ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and $\Sigma, a@r{:}\, T'; \gamma; \emptyset \vdash e'_1 \ : \ T'$ and $r \ \in \ \gamma_{\mathtt{w}}$, we have

$$\gamma \vdash (\mu \uplus \{a@r \ \mapsto \ e'_1\})|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ : \ (\Sigma, a@r{:}\, T')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$$

by Lemma 42 (4).
Since $\mu \models A_1$, we have

$$\mu \uplus \{a@r \ \mapsto \ e'_1\} \models A_1$$

by Lemma 88.
Finally, since $r \ \in \ \gamma_{\mathtt{w}}$,

$$\mathit{dom}\,(a@r{:}\, T') \ = \ \mathit{dom}\,((a@r{:}\, T')|_{\gamma_{\mathtt{w}}}).$$

Case (CT_Deref): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \Leftarrow {!e'_1}; c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e'_1 \ : \ \mathsf{Ref}_r\, T'$,
- $\emptyset; \Sigma; \gamma; y{:}\, T' \vdash c'_2 \ : \ \{A_1\} x{:}\, T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}} \rangle}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_1\} x{:}\, T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}$, and

- $\gamma_{\mathtt{r}} = {\gamma_{\mathtt{r}}}' \cup \{r\}$.

By case analysis on the computation rule applicable to c.

Case (C_Red): By the IH (case (1)) and (CT_Deref).

Case (C_RBlame): By Lemma 86 (3) and (CT_Blame).

Case (C_Command)/(C_Deref): We are given $e'_1 = a@r$ (the region r is identified from Lemma 59 (3)) and $\mu \mid c \longrightarrow \mu \mid y \leftarrow \mathsf{do\,return}\,\mu(a@r); c'_2$. Since $\Sigma; \gamma; \emptyset \vdash a@r \ :\ \mathsf{Ref}_r\, T'$, we have

- $a@r{:}T'' \in \Sigma$,
- $\Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_r\, T''$, and
- $\mathsf{Ref}_r\, T'' \equiv \mathsf{Ref}_r\, T'$

for some T'' by Lemma 63. Since $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ :\ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and $r \in {\gamma_{\mathtt{r}}}' \cup \{r\} = \gamma_{\mathtt{r}}$, we have $\Sigma; \gamma; \emptyset \vdash \mu(a@r) \ :\ T''$. Since $\Sigma; \gamma; \emptyset \vdash \mu(a@r) \ :\ T'$ by Lemmas 54 and 86 (2) and (T_Conv), and $\Sigma; \gamma; y{:}T' \vdash^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle} A_1$ by Lemma 44 (3), we have

$$\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\,\mu(a@t) \ :\ \{A_1\}y{:}T'\{A_1\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}$$

by (CT_Return). By (T_CBind),

$$\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do\,return}\,\mu(a@r); c'_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}.$$

Case (C_Command)/(C_GuardDeref): We are given $e'_1 = T'_1 \Leftarrow^{\ell} T'_2 : v'_1$ and

$$\mu \mid c \longrightarrow \mu \mid y \leftarrow \mathsf{do}\,(z \Leftarrow !v'_1; \mathsf{return}\,\langle T'_1 \Leftarrow T'_2 \rangle^{\ell}\, z); c'_2$$

for some T'_1, ℓ, T'_2, v'_1, and a fresh variable z. Since $\Sigma; \gamma; \emptyset \vdash T'_1 \Leftarrow^{\ell} T'_2 : v'_1 \ :\ \mathsf{Ref}_r\, T'$, we have $\Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_r\, T'_1$ and $\Sigma; \gamma; \emptyset \vdash v'_1 \ :\ \mathsf{Ref}_r\, T'_2$ and $T'_1 \parallel T'_2$ and $T'_1 \equiv T'$ by Lemmas 64 and 54. By Lemma 86 (2), $\Sigma; \gamma; \emptyset \vdash T'_1$ and $\Sigma; \gamma; \emptyset \vdash T'_2$. Thus, by Lemmas 44 (2) and (3), (T_Cast), (T_App), and (CT_Return),

$$\mu; \Sigma; \gamma; z{:}T'_2 \vdash \mathsf{return}\,\langle T'_1 \Leftarrow T'_2 \rangle^{\ell}\, z \ :\ \{A_1\}y{:}T'_1\{A_1\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}.$$

By (CT_Deref),

$$\mu; \Sigma; \gamma; \emptyset \vdash z \Leftarrow !v'_1; \mathsf{return}\,\langle T'_1 \Leftarrow T'_2 \rangle^{\ell}\, z \ :\ \{A_1\}y{:}T'_1\{A_1\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}.$$

Since $T'_1 \equiv T'$, we have $\mu; \Sigma; \gamma; \emptyset \vdash z \Leftarrow !v'_1; \mathsf{return}\,\langle T'_1 \Leftarrow T'_2 \rangle^{\ell}\, z \ :\ \{A_1\}y{:}T'\{A_1\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}$ by Lemmas 85 (2) and 86 (2) and (CT_Conv). By (CT_CBind),

$$\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\,(z \Leftarrow !v'_1; \mathsf{return}\,\langle T'_1 \Leftarrow T'_2 \rangle^{\ell}\, z); c'_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}.$$

Case (CT_Assign): We are given $\mu; \Sigma; \gamma; \emptyset \vdash y \Leftarrow e'_1 {:=} e'_2; c'_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e'_1 \ :\ \mathsf{Ref}_r\, T'$,
- $\Sigma; \gamma; \emptyset \vdash e'_2 \ :\ T'$,
- $\emptyset; \Sigma; \gamma; y{:}\mathsf{unit} \vdash c'_2 \ :\ \{\top\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \rangle}$,
- $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$, and
- $\gamma_{\mathtt{w}} = {\gamma_{\mathtt{w}}}' \cup \{r\}$.

By case analysis on the computation rule applicable to c.

Case (C_Red): By the IH (case (1)) and (CT_Assign).

Case (C_RBlame): By Lemma 86 (3) and (CT_Blame).

Case (C_Command)/(C_Assign): We can suppose that e'_2 is a value. We are given $e'_1 = a@r$ (note that the region r is identified by Lemma 59 (3)) and

$$\mu' \uplus \{a@r \mapsto v'\} \mid c \longrightarrow \mu' \uplus \{a@r \mapsto e'_2\} \mid y \leftarrow \mathsf{do\,return}\,(); c'_2$$

for some μ' and v' such that $\mu = \mu' \uplus \{a@r \mapsto v'\}$. Since $\Sigma; \gamma; \emptyset \vdash a@r \ :\ \mathsf{Ref}_r\, T'$, we have

- $a@r{:}T'' \in \Sigma$,
- $\Sigma; \gamma; \emptyset \vdash \mathsf{Ref}_r\, T''$, and
- $\mathsf{Ref}_r\, T'' \equiv \mathsf{Ref}_r\, T'$

for some T'' by Lemma 63. Since $\Sigma;\gamma;\emptyset \vdash e'_2 \,:\, T'$, and $T' \,\equiv\, T''$ by Lemmas 54 and 51 (3), and $\Sigma;\gamma;\emptyset \vdash T''$ by inversion of $\Sigma;\gamma;\emptyset \vdash \mathsf{Ref}_r\, T''$, we have $\Sigma;\gamma;\emptyset \vdash e'_2 \,:\, T''$ by (T_Conv). Thus, since $\gamma \vdash \mu|_{\gamma_{\mathtt{r}}\cup\gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}}\cup\gamma_{\mathtt{w}}}$ and $r \,\in\, {\gamma_{\mathtt{w}}}' \cup \{r\} = \gamma_{\mathtt{w}}$, we have

$$\gamma \vdash (\mu' \uplus \{a@r \,\mapsto\, e'_2\})|_{\gamma_{\mathtt{r}}\cup\gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}}\cup\gamma_{\mathtt{w}}}.$$

By (WF_EmptyAssert), we have $\Sigma;\gamma;y{:}\mathsf{unit} \vdash^{\langle\gamma_{\mathtt{r}},{\gamma_{\mathtt{w}}}'\cup\{r\}\rangle} \top$. Thus, by (T_Const) and (CT_Return),

$$\mu' \uplus \{a@r \,\mapsto\, e'_2\};\Sigma;\gamma;\emptyset \vdash \mathsf{return}\,() \,:\, \{\top\}y{:}\mathsf{unit}\{\top\}^{\langle\gamma_{\mathtt{r}},{\gamma_{\mathtt{w}}}'\cup\{r\}\rangle}.$$

By (CT_CBind),

$$\mu' \uplus \{a@r \,\mapsto\, e'_2\};\Sigma;\gamma;\emptyset \vdash y \leftarrow \mathsf{do}\,\mathsf{return}\,();\, c'_2 \,:\, \{\top\}x{:}\,T\{A_2\}^{\langle\gamma_{\mathtt{r}},{\gamma_{\mathtt{w}}}'\cup\{r\}\rangle}.$$

Since $\mu' \uplus \{a@r \,\mapsto\, e'_2\} \models \top$, we finish.

Case (C_Command)/(C_GuardAssign): We can suppose that e'_2 is a value. We are given $e'_1 \,=\, T'_1 \Leftarrow^{\ell} T'_2 : v'_1$ and

$$\mu \mid c \,\longrightarrow\, \mu \mid y \leftarrow \mathsf{do}\,(z \Leftarrow v'_1 :=(\langle T'_2 \Leftarrow T'_1\rangle^{\ell}\, e'_2);\mathsf{return}\,());\, c'_2$$

for some T'_1, ℓ, T'_2, v'_1, and a fresh variable z. Since $\Sigma;\gamma;\emptyset \vdash T'_1 \Leftarrow^{\ell} T'_2 : v'_1 \,:\, \mathsf{Ref}_r\, T'$, we have

- $\Sigma;\gamma;\emptyset \vdash \mathsf{Ref}_r\, T'_1$,
- $\Sigma;\gamma;\emptyset \vdash v'_1 \,:\, \mathsf{Ref}_r\, T'_2$,
- $T'_1 \parallel T'_2$, and
- $T'_1 \,\equiv\, T'$

by Lemmas 64 and 54. By Lemma 86 (2) and inversion, we have $\Sigma;\gamma;\emptyset \vdash T'_1$ and $\Sigma;\gamma;\emptyset \vdash T'_2$. Since $\Sigma;\gamma;\emptyset \vdash e'_2 \,:\, T'_1$ by (T_Conv), and $\Sigma;\gamma;z{:}\mathsf{unit},y{:}\mathsf{unit} \vdash^{\langle\gamma_{\mathtt{r}},{\gamma_{\mathtt{w}}}'\cup\{r\}\rangle} \top$ by (WF_EmptyAssert), and $T'_2 \parallel T'_1$ by Lemma 77, we have

$$\mu;\Sigma;\gamma;\emptyset \vdash z \Leftarrow v'_1 :=\langle T'_2 \Leftarrow T'_1\rangle^{\ell}\, e'_2;\mathsf{return}\,() \,:\, \{\top\}y{:}\mathsf{unit}\{\top\}^{\langle\gamma_{\mathtt{r}},{\gamma_{\mathtt{w}}}'\cup\{r\}\rangle}$$

by (T_Cast), (T_App), (T_Const), (CT_Return), and (CT_Assign). Thus, we have

$$\mu;\Sigma;\gamma;\emptyset \vdash y \leftarrow \mathsf{do}\,(z \Leftarrow v'_1 :=\langle T'_2 \Leftarrow T'_1\rangle^{\ell}\, e'_2;\mathsf{return}\,());\, c'_2 \,:\, \{\top\}x{:}\,T\{A_2\}^{\langle\gamma_{\mathtt{r}},{\gamma_{\mathtt{w}}}'\cup\{r\}\rangle}$$

by (CT_CBind).

Case (CT_Weak): By the IH, Lemma 42 (3), and (CT_Weak).

Case (CT_Assert): We are given $\mu;\Sigma;\gamma;\emptyset \vdash \mathsf{assert}\,(c'_1)^{\ell};\, c'_2 \,:\, \{A_1\}x{:}\,T\{A_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle}$ and, by inversion, $\emptyset;\Sigma;\gamma;\emptyset \vdash c'_2 \,:\, \{A_1, c'_1\}x{:}\,T\{A_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle}$. The computation rule applicable to c is only (C_Assert). Thus, we are given $\mu \mid c \,\longrightarrow\, \mu \mid \langle\mathsf{assert}\,(c'_1), \nu\emptyset.\langle\emptyset \mid c'_1\rangle\rangle^{\ell};\, c'_2$. By Lemmas 86 (3) and 89 (1), $\mu;\Sigma;\gamma;\emptyset \vdash c'_1 \,:\, \{A_1\}\mathsf{bool}\{\top\}^{\langle\gamma_{\mathtt{r}},\emptyset\rangle}$. Since $\gamma \vdash \emptyset \,:\, \Sigma^{\emptyset}$ and $\mu \models A_1$, we finish by (PT) and (CT_Check).

Case (CT_Check): We are given $\mu;\Sigma;\gamma;\emptyset \vdash \langle\mathsf{assert}\,(c'_1), p'_2\rangle^{\ell};\, c'_3 \,:\, \{A_1\}x{:}\,T\{A_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle}$ and, by inversion,

- $\emptyset;\Sigma;\gamma;\emptyset \vdash c'_3 \,:\, \{A_1, c'_1\}x{:}\,T\{A_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle}$,
- $\mu;\Sigma;\gamma \vdash p'_2 \,:\, \mathsf{bool}^{\gamma_{\mathtt{r}}}$, and
- $\mu \mid \nu\emptyset.\langle\emptyset \mid c'_1\rangle \hookrightarrow^{*} p'_2$.

By case analysis on the computation rule applicable to c.

Case (C_CBlame) and (C_Fail): By Lemma 86 (3) and (CT_Blame).

Case (C_Checking): We are given $\mu \mid p'_2 \,\hookrightarrow\, \nu\gamma'.\langle\mu' \mid c'\rangle$ for some γ', μ', and c'. Since $\gamma \vdash \mu|_{\gamma_{\mathtt{r}}\cup\gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}}\cup\gamma_{\mathtt{w}}}$, we have $\gamma \vdash \mu|_{\gamma_{\mathtt{r}}} \,:\, \Sigma^{\gamma_{\mathtt{r}}}$ by Lemma 70. Thus, we can apply the IH (case (3)). By (CT_Check), we finish.

Case (C_OK): We are given $p'_2 \,=\, \nu\gamma'.\langle\mu' \mid \mathsf{return}\,\mathsf{true}\rangle$ for some γ' and μ', and $\mu \mid c \,\longrightarrow\, \mu \mid c'_3$. By Lemma 89 (1),

$$\mu;\Sigma;\gamma;\emptyset \vdash c'_3 \,:\, \{A_1, c'_1\}x{:}\,T\{A_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle}.$$

Since $\mu \models A_1$ and $\mu \mid \nu\emptyset.\langle\emptyset \mid c'_1\rangle \hookrightarrow^{*} \nu\gamma'.\langle\mu' \mid \mathsf{return}\,\mathsf{true}\rangle$, we have $\mu \models A_1, c'_1$.

Case (CT_Blame) and (CT_LetRegion): Contradictory.

Case (CT_Conv): By the IH and (CT_Conv).

3. We are given $\mu;\Sigma;\gamma \vdash \nu\gamma'.\langle\mu' \mid c'\rangle \,:\, T^{\gamma''}$ for some γ', μ', and c'. By inversion of the typing derivation,

- $\gamma,\gamma' \vdash \mu' \,:\, (\Sigma,\Sigma')^{\gamma'}$,

- $dom\,(\mu') \;=\; dom\,(\Sigma')$,
- $\mu \uplus \mu'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c' \;:\; \{A_1\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$, and
- $\mu \uplus \mu' \models A_1$

for some Σ', A_1, and x. Without loss of generality, we can suppose that $dom\,(\mu\,|_{\gamma'}) \;=\; \emptyset$ and $dom\,(\Sigma\,|_{\gamma'}) \;=\; \emptyset$. By case anlaysis on the rule applied to evaluate p.

Case (P_Comput): We are given $\mu \uplus \mu' \mid c' \longrightarrow \mu \uplus \mu'' \mid c''$ for some μ'' and c''. Since $dom\,(\mu\,|_{\gamma'}) \;=\; \emptyset$, we have $((\mu|_{\gamma''}) \uplus \mu')|_{\gamma' \cup \gamma''} \;=\; (\mu \uplus \mu')|_{\gamma' \cup \gamma''}$. Thus, by Lemma 72,

$$\gamma, \gamma' \vdash (\mu \uplus \mu')|_{\gamma' \cup \gamma''} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma''}.$$

Thus, by the the IH (case (2)), there exist some Σ'' and A_1'' such that

- $\mu \uplus \mu''; \Sigma, \Sigma', \Sigma''; \gamma, \gamma'; \emptyset \vdash c'' \;:\; \{A_1''\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$,
- $\gamma, \gamma' \vdash (\mu \uplus \mu'')|_{\gamma' \cup \gamma''} \;:\; (\Sigma, \Sigma', \Sigma'')^{\gamma' \cup \gamma''}$,
- $\mu \uplus \mu'' \models A_1''$, and
- $dom\,(\Sigma'') \;=\; dom\,(\Sigma''\,|_{\gamma'})$.

By (PT), it suffices to show that (1) $dom\,(\mu'') \;=\; dom\,(\Sigma', \Sigma'')$ and (2) $\gamma, \gamma' \vdash \mu'' \;:\; (\Sigma, \Sigma', \Sigma'')^{\gamma'}$.

- We show $dom\,(\mu'') \;=\; dom\,(\Sigma', \Sigma'')$. By Lemma 92, it suffices to show that (a) $dom\,(\mu'') \;=\; dom\,(\mu''\,|_{\gamma'})$ and (b) $dom\,(\Sigma', \Sigma'') \;=\; dom\,((\Sigma', \Sigma'')\,|_{\gamma'})$.
  Since $dom\,(\mu') \;=\; dom\,(\mu'\,|_{\gamma'})$ by Lemma 71, we have $dom\,(\mu'') \;=\; dom\,(\mu''\,|_{\gamma'})$ by Lemma 93.
  Since $dom\,(\mu') \;=\; dom\,(\Sigma')$, we have $dom\,(\Sigma') \;=\; dom\,(\Sigma'\,|_{\gamma'})$. Since $dom\,(\Sigma'') \;=\; dom\,(\Sigma''\,|_{\gamma'})$, we have $dom\,(\Sigma', \Sigma'') \;=\; dom\,((\Sigma', \Sigma'')\,|_{\gamma'})$.
- We show $\gamma, \gamma' \vdash \mu'' \;:\; (\Sigma, \Sigma', \Sigma'')^{\gamma'}$. Since $dom\,(\mu'') \;=\; dom\,(\mu''\,|_{\gamma'})$ (from the discussion above) and $\gamma, \gamma' \vdash (\mu \uplus \mu'')|_{\gamma' \cup \gamma''} \;:\; (\Sigma, \Sigma', \Sigma'')^{\gamma' \cup \gamma''}$, it suffices to show that

$$dom\,(\mu'') \;=\; dom\,((\Sigma, \Sigma', \Sigma'')\,|_{\gamma'}).$$

  Since $dom\,(\Sigma\,|_{\gamma'}) \;=\; \emptyset$, it suffices to show that $dom\,(\mu'') \;=\; dom\,((\Sigma', \Sigma'')\,|_{\gamma'})$, which is shown by $dom\,(\mu'') \;=\; dom\,(\Sigma', \Sigma'')$ (from the discussion above) and $dom\,(\mu'') \;=\; dom\,(\mu''\,|_{\gamma'})$.

Case (P_Region): We are given $\mu \mid \nu\gamma'.\langle \mu' \mid \nu r''.\, c'' \rangle \hookrightarrow \nu\gamma', r'.\langle \mu'' \mid c'' \rangle$ where $c' \;=\; \nu r''.\, c''$ for some r'' and c''. Without loss of generality, we can suppose that $r'' \notin \gamma' \cup \gamma$ and $dom\,((\Sigma, \Sigma')\,|_{\{r''\}}) \;=\; \emptyset$. By Lemma 87, we have $\mu \uplus \mu'; \Sigma, \Sigma'; \gamma, \gamma', r''; \emptyset \vdash c'' \;:\; \{A_1\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle \uplus \{r''\}}$. Since $dom\,((\Sigma, \Sigma')\,|_{\gamma' \cup \{r''\}}) \;=\; dom\,((\Sigma, \Sigma')\,|_{\gamma'})$, we have $\gamma, \gamma', r'' \vdash \mu' \;:\; (\Sigma, \Sigma')^{\gamma' \cup \{r''\}}$ by Lemma 40 (4), so we finish by (PT).

□

Lemma 96. *If*

- $\mu; \Sigma; \gamma; \emptyset \vdash c \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma, \gamma \rangle}$,
- $\gamma \vdash \mu \;:\; \Sigma^{\gamma}$,
- $\mu \models A_1$*, and*
- $\emptyset \mid \nu\gamma.\langle \mu \mid c \rangle \hookrightarrow^{*} \nu\gamma'.\langle \mu' \mid \mathsf{return}\, v' \rangle$,

then $\mu' \models [\, v'/x \,]\, A_2$.

Proof. By induction on the length of the computation sequence starting from $\nu\gamma.\langle \mu \mid c \rangle$.

Case 0: By Lemma 91.

Case $i+1$: We are given $\emptyset \mid \nu\gamma.\langle \mu \mid c \rangle \hookrightarrow p$ and $\emptyset \mid p \hookrightarrow^{*} \nu\gamma'.\langle \mu' \mid \mathsf{return}\, v' \rangle$ for some p. By case analysis on the rule applied to $\nu\gamma.\langle \mu \mid c \rangle$.

Case (P_Comput): We are given $\mu \mid c \longrightarrow \mu' \mid c'$ for some μ' and c'. Since $\gamma \vdash \mu \;:\; \Sigma^{\gamma}$, we have $dom\,(\mu) \;=\; dom\,(\Sigma\,|_{\gamma})$, and so $\mu \;=\; \mu|_{\gamma}$. Thus, we can apply Lemma 95 (2). Then, there exist some Σ' and A_1' such that

- ∗ $\mu'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c' \;:\; \{A_1'\}x{:}T\{A_2\}^{\langle \gamma, \gamma \rangle}$,
- ∗ $\gamma \vdash \mu'\,|_{\gamma} \;:\; (\Sigma, \Sigma')^{\gamma}$, and

- $\mu' \models A_1'$.

  By Lemma 93, $\mathit{dom}\,(\mu') = \mathit{dom}\,(\mu'\,|_{\gamma})$. By the IH, we finish.

Case (P_Region): We are given $\emptyset \mid \nu\gamma.\langle \mu \mid \nu r'.\, c' \rangle \hookrightarrow \nu\gamma, r'.\langle \mu \mid c' \rangle$ for some r' and c' such that $c = \nu r'.\, c'$. Without loss of generality, we can suppose that $\mathit{dom}\,(\Sigma \mid_{\{r'\}}) = \emptyset$. By Lemma 87, $\mu; \Sigma; \gamma, r'; \emptyset \vdash c' : \{A_1\} x{:}T\{A_2\}^{\langle \gamma, \gamma \rangle \uplus \{r'\}}$. Thus, by the IH, it suffices to show that $\gamma, r' \vdash \mu : \Sigma^{\gamma \uplus \{r'\}}$. By Lemma 42 (4), it suffices to show that $\mathit{dom}\,(\mu) = \mathit{dom}\,(\Sigma\,|_{\gamma \cup \{r'\}})$. Since $\gamma \vdash \mu : \Sigma^{\gamma}$, we have $\mathit{dom}\,(\mu) = \mathit{dom}\,(\Sigma\,|_{\gamma})$. Thus, it suffices to show that $\mathit{dom}\,(\Sigma\,|_{\gamma}) = \mathit{dom}\,(\Sigma\,|_{\gamma \cup \{r'\}})$. Since $\mathit{dom}\,(\Sigma\,|_{\{r'\}}) = \emptyset$, we finish.

□

Theorem 1 (Type Soundness)**.** *Suppose that $\emptyset; \emptyset; \{r\}; \emptyset \vdash c : \{\top\} x{:}T\{A_2\}^{\langle \{r\}, \{r\} \rangle}$. Let $p = \nu\emptyset.\langle \emptyset \mid \nu r.\, c \rangle$. Then, one of the followings holds:*

- *there is an infinite computation sequence starting with p;*
- *$\emptyset \mid p \hookrightarrow^{*} \nu\gamma.\langle \mu \mid \Uparrow\ell \rangle$ for some γ, μ, and ℓ; or*
- *$\emptyset \mid p \hookrightarrow^{*} \nu\gamma.\langle \mu \mid \mathsf{return}\, v \rangle$ for some γ, μ, and v such that $\models v : T$ and $\mu \models [\, v/x \,]\, A_2$.*

Proof. Suppose that p terminates under the empty store. By (CT_Weak), (CT_LetRegion), and (PT), $\emptyset; \emptyset; \emptyset \vdash p : T^{\emptyset}$. By Lemmas 73 (3) and 95 (3), there exist some γ and μ such that $\emptyset \mid p \hookrightarrow^{*} \nu\gamma.\langle \mu \mid c \rangle$ where $c = \mathsf{return}\, v$ for some v, or $c = \Uparrow\ell$ for some ℓ. $\models v : T$ is shown by inversion of (PT) and Lemmas 60 and 68. $\mu \models [\, v/x \,]\, A_2$ is shown by Lemma 96. □

2.3 Assertion Elimination

Lemma 97. *Suppose that* $r \notin \gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}$.

(1) If $\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma; \emptyset \vdash c : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ *and* $\mu \uplus \{a@r \mapsto v\} \mid c \longrightarrow \mu' \mid c'$*, then there exists some* μ'' *such that* $\mu' = \mu'' \uplus \{a@r \mapsto v\}$ *and* $\mu \mid c \longrightarrow \mu'' \mid c$.

(2) If $\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma \vdash p : T^{\gamma_{\mathtt{r}}}$ *and* $\mu \uplus \{a@r \mapsto v\} \mid p \hookrightarrow p'$*, then* $\mu \mid p \hookrightarrow p'$.

Proof. By strong induction on the lengths of the typing derivations with case analysis on the typing rule and computation rule applied last to c. We mention only interesting cases.

Case (CT_BIND)/(C_COMPUT): We are given

- $c = y \leftarrow \mathsf{do}\, c_1'; c_2'$,
- $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, c_1' : \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $\emptyset; \Sigma; \gamma; y{:}T' \vdash c_2' : \{A_3\}x{:}T\{A_2\}^{\varrho_2}$, and
- $\mu \uplus \{a@r \mapsto v\} \mid c_1' \longrightarrow \mu' \mid c_1''$

for some y, c_1', c_2', T', A_3, $\gamma_{\mathtt{r}1}$, $\gamma_{\mathtt{w}1}$, ϱ_2, and c_1'' such that $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \cup \varrho_2 = \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$. By Lemmas 65, 56 and 89, $\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma; \emptyset \vdash c_1' : \{A_1''\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ for some A_1'', T'', and A_3''; the length of its derivation is smaller than that of $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, c_1' : \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$. Thus, we can apply the IH. Since $r \notin \gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}$ and $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, $r \notin \gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}$. Thus, by the IH, there exists some μ'' such that $\mu' = \mu'' \uplus \{a@r \mapsto v\}$ and $\mu \mid c_1' \longrightarrow \mu'' \mid c_1''$, and so $\mu \mid c \longrightarrow \mu'' \mid y \leftarrow \mathsf{do}\, c_1''; c_2'$ by (C_COMPUT).

Case (CT_DEREF)/(C_COMMAND)/(C_DEREF): We are given

$$\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma; \emptyset \vdash y \Leftarrow !b@s; c_2 : \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{t\}, \gamma_{\mathtt{w}} \rangle}$$

and, by inversion, $\Sigma; \gamma; \emptyset \vdash b@s : \mathsf{Ref}_t\, T'$ and $\gamma_{\mathtt{r}} = {\gamma_{\mathtt{r}}}' \cup \{t\}$. Since (C_COMMAND)/(C_DEREF) is applied, we have $\mu \uplus \{a@r \mapsto v\} \mid c \longrightarrow \mu \uplus \{a@r \mapsto v\} \mid y \leftarrow \mathsf{do\, return}\, (\mu \uplus \{a@r \mapsto v\})(b@s); c_2$. By Lemmas 63 and 54, $s = t$. Since $r \notin {\gamma_{\mathtt{r}}}' \cup \{t\}$, we have $r \neq s$. Thus, $a@r \neq b@s$. Then, by (C_COMMAND)/(C_DEREF), $\mu \mid c \longrightarrow \mu \mid y \leftarrow \mathsf{do\, return}\, \mu(b@s); c_2$.

Case (CT_ASSIGN)/(C_COMMAND)/(C_ASSIGN): We are given

$$\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma; \emptyset \vdash y \Leftarrow b@s := v'; c_2 : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{t\} \rangle}$$

and, by inversion, $\Sigma; \gamma; \emptyset \vdash b@s : \mathsf{Ref}_t\, T'$ and $\gamma_{\mathtt{w}} = {\gamma_{\mathtt{w}}}' \cup \{t\}$. By Lemmas 63 and 54, $s = t$. Since $r \notin {\gamma_{\mathtt{r}}}' \cup \{t\}$, we have $r \neq s$. Thus, $a@r \neq b@s$. Since (C_COMMAND)/(C_ASSIGN) is applied, there exists some v'' and μ'' such that $\mu = \mu'' \uplus \{b@s \mapsto v''\}$ and $\mu \uplus \{a@r \mapsto v\} \mid c \longrightarrow \mu'' \uplus \{a@r \mapsto v, b@s \mapsto v'\} \mid y \leftarrow \mathsf{do\, return}\, (); c_2$. Then, by (C_COMMAND)/(C_ASSIGN), $\mu \mid c \longrightarrow \mu'' \uplus \{b@s \mapsto v'\} \mid y \leftarrow \mathsf{do\, return}\, (); c_2$.

□

Lemma 98. *If* $\Sigma; \gamma; \emptyset \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$ *and* $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ *and* $\mu \models A$*, then* $\mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \models A$.

Proof. By induction on the derivation of $\Sigma; \gamma; \emptyset \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$, it suffices to show that, if $\emptyset; \Sigma; \gamma; \emptyset \vdash c : \{A'\}T\{\top\}^{\langle \gamma_{\mathtt{r}}, \emptyset \rangle}$ and $\mu \models A', c$, then $\mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \models c$. By Lemma 89, $\mu; \Sigma; \gamma; \emptyset \vdash c : \{A'\}T\{\top\}^{\langle \gamma_{\mathtt{r}}, \emptyset \rangle}$. Since $\mu \models A'$, we have $\mu; \Sigma; \gamma \vdash \nu\emptyset.\langle \emptyset \mid c \rangle : T^{\gamma_{\mathtt{r}}}$ by (PT). Since $\mu \models c$ and $\gamma \vdash \mu|_{\gamma_{\mathtt{r}}} : \Sigma^{\gamma_{\mathtt{r}}}$ by Lemma 70, it is straightforward to show $\mu|_{\gamma_{\mathtt{r}}} \models c$ by induction on the number of the computation steps of $\nu\emptyset.\langle \emptyset \mid c \rangle$ with Lemmas 97 and 95 (3). □

Lemma 99. *If* $\Sigma \subseteq \Sigma'$, $\gamma \subseteq \gamma'$, $\Gamma \subseteq \Gamma'$*, and* $\Sigma'; \gamma'; \Gamma' \vdash \langle \mu, \sigma \rangle^{\varrho}$*, then* $\Sigma; \gamma; \Gamma \vdash \langle \mu, \sigma \rangle^{\varrho}$.

Proof. Suppose that $\Sigma'; \gamma'; \Gamma' \vdash \langle \mu, \sigma \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. By definition, there exist some Σ'' and γ'' such that

- $\Sigma' \subseteq \Sigma''$,
- $\gamma' \subseteq \gamma''$,
- for any $s \in \gamma'$, $s \notin \mathit{dom}\,(\sigma)$;
- for any $s \in \Gamma'$, $\sigma(s) \in \gamma''$,
- for any $x{:}T \in \Gamma'$, $\Sigma''; \gamma''; \emptyset \vdash \sigma(x) : \sigma(T)$, and

- $\gamma'' \vdash \mu \,:\, \Sigma''^{\sigma(\gamma_{\mathtt{r}})\cup\sigma(\gamma_{\mathtt{w}})}$.

Since $\Sigma \subseteq \Sigma'$, $\gamma \subseteq \gamma'$, and $\Gamma \subseteq \Gamma'$, we have $\Sigma; \gamma; \Gamma \vdash \langle \mu, \sigma \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. □

Lemma 100. *If $\Sigma \subseteq \Sigma'$, $\gamma \subseteq \gamma'$, $\Gamma \subseteq \Gamma'$, and $\Sigma; \gamma; \Gamma \vdash \gamma_1 \,\mathsf{disj}\, \gamma_2$, then $\Sigma'; \gamma'; \Gamma' \vdash \gamma_1 \,\mathsf{disj}\, \gamma_2$.*

Proof. Suppose that $\Sigma; \gamma; \Gamma \vdash \gamma_1 \,\mathsf{disj}\, \gamma_2$. Let σ be a substitution such that $\Sigma'; \gamma'; \Gamma' \vdash \sigma$. By definition, it suffices to show that $\sigma(\gamma_1) \cap \sigma(\gamma_2) = \emptyset$. By Lemma 99, we have $\Sigma; \gamma; \Gamma \vdash \sigma$. Since $\Sigma; \gamma; \Gamma \vdash \gamma_1 \,\mathsf{disj}\, \gamma_2$, we finish. □

Lemma 101. *Suppose that $r \notin \gamma \cup \mathit{regions}\,(\Gamma)$.*

(1) If $\Sigma; \gamma; \Gamma \vdash T_1 \sim T_2$, then $\Sigma; \gamma, r; \Gamma \vdash T_1 \sim T_2$.

(2) If $\Sigma; \gamma; \Gamma \vdash^{\varrho} A_1 \sim A_2$, then $\Sigma; \gamma, r; \Gamma \vdash^{\varrho} A_1 \sim A_2$.

(3) If $\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \,:\, T$, then $\Sigma; \gamma, r; \Gamma \vdash e_1 \sim e_2 \,:\, T$.

(4) If $\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma, r; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$.

(5) If $\Sigma; \gamma \vdash C^{\mathtt{c}}_{\mathtt{n1}} \sim C^{\mathtt{c}}_{\mathtt{n2}} \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}$, then $\Sigma; \gamma, r \vdash C^{\mathtt{c}}_{\mathtt{n1}} \sim C^{\mathtt{c}}_{\mathtt{n2}} \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}$.

(6) If $\mu; \Sigma; \gamma \vdash p_1 \sim p_2 \,:\, T^{\gamma'}$, then $\mu; \Sigma; \gamma, r \vdash p_1 \sim p_2 \,:\, T^{\gamma'}$.

(7) If $\gamma \vdash \mu_1 \sim \mu_2 \,:\, \Sigma^{\gamma'}$, then $\gamma, r \vdash \mu_1 \sim \mu_2 \,:\, \Sigma^{\gamma'}$.

Proof. By induction on the derivations (well typedness on the left-hand sides are shown by Lemma 40). We mention only interesting cases.

Case (AEC_ElimAssert): We are given $\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{assert}\,(c_{11})^{\ell}; c_{12} \sim c_{22} \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$ and, by inversion,

- $\emptyset; \Sigma; \gamma; \Gamma \vdash c_{12} \sim c_{22} \,:\, \{A_1, c_{11}\}x{:}T\{A_2\}^{\varrho}$,
- $A'_1 \subseteq A_1$,
- $\varrho' \subseteq \varrho$,
- $\Sigma; \gamma; \Gamma \vdash^{\varrho'} A'_1, c_{11}$, and
- for any μ' and σ', if $\Sigma; \gamma; \Gamma \vdash \langle \mu', \sigma' \rangle^{\varrho'}$ and $\mu' \models \sigma'(A'_1)$, then $\mu' \models \sigma'(c_{11})$.

By the IH, we have $\emptyset; \Sigma; \gamma, r; \Gamma \vdash c_{12} \sim c_{22} \,:\, \{A_1, c_{11}\}x{:}T\{A_2\}^{\varrho}$. By Lemma 40, $\Sigma; \gamma, r; \Gamma \vdash^{\varrho'} A'_1, c_{11}$. Thus, by (AEC_ElimAssert), it suffices to show that, for any σ' and μ', if $\Sigma; \gamma, r; \Gamma \vdash \langle \mu', \sigma' \rangle^{\varrho'}$ and $\mu' \models \sigma'(A'_1)$, then $\mu' \models \sigma'(c_{11})$. Let σ' and μ' be a substitution and a store such that $\Sigma; \gamma, r; \Gamma \vdash \langle \mu', \sigma' \rangle^{\varrho'}$ and $\mu' \models \sigma'(A'_1)$. By Lemma 99, $\Sigma; \gamma; \Gamma \vdash \langle \mu', \sigma' \rangle^{\varrho'}$. Thus, by the inversion of the derivation, $\mu' \models \sigma'(c_{11})$.

Case (AEC_Frame): We are given $\mu; \Sigma; \gamma; \Gamma \vdash y \leftarrow \mathsf{do}\, c_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim c_2 \,:\, \{A_1, A\}x{:}T\{A_2, A\}^{\varrho}$ and, by inversion,

- $\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\langle \gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}} \rangle \subseteq \varrho$,
- $\Sigma; \gamma; \Gamma \vdash^{\langle {\gamma_{\mathtt{r}}}', \emptyset \rangle} A$, and
- $\Sigma; \gamma; \Gamma \vdash {\gamma_{\mathtt{r}}}' \,\mathsf{disj}\, \gamma_{\mathtt{w}}$

for some fresh y. By the IH, $\mu; \Sigma; \gamma, r; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. By Lemma 42 (3), $\Sigma; \gamma, r; \Gamma \vdash^{\langle {\gamma_{\mathtt{r}}}', \emptyset \rangle} A$. Thus, by (AEC_Frame), it suffices to show that $\Sigma; \gamma, r; \Gamma \vdash {\gamma_{\mathtt{r}}}' \,\mathsf{disj}\, \gamma_{\mathtt{w}}$, which is shown by Lemma 100.

□

Lemma 102. *Suppose that $r \notin \gamma \cup \mathit{regions}\,(\Gamma_1) \cup \mathit{regions}\,(\Gamma_2)$.*

(1) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash T_1 \sim T_2$, then $\Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash T_1 \sim T_2$.

(2) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash^{\varrho} A_1 \sim A_2$, then $\Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash^{\varrho} A_1 \sim A_2$.

(3) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash e_1 \sim e_2 \,:\, T$, then $\Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash e_1 \sim e_2 \,:\, T$.

(4) If $\mu; \Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma; \Gamma_1, r, \Gamma_2 \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$.

Proof. Similarly to Lemma 101 except for use of Lemma 41 instead of Lemma 40. □

Lemma 103. *Suppose that $\Sigma; \gamma_1; \Gamma_1 \vdash T$ and x is a fresh variable.*

(1) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash T_1 \sim T_2$, then $\Sigma; \gamma; \Gamma_1, x{:}T, \Gamma_2 \vdash T_1 \sim T_2$.

(2) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash^{\varrho} A_1 \sim A_2$, then $\Sigma; \gamma; \Gamma_1, x{:}T, \Gamma_2 \vdash^{\varrho} A_1 \sim A_2$.

(3) If $\Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash e_1 \sim e_2 \ :\ T'$, then $\Sigma; \gamma; \Gamma_1, x{:}T, \Gamma_2 \vdash e_1 \sim e_2 \ :\ T'$.

(4) If $\mu; \Sigma; \gamma; \Gamma_1, \Gamma_2 \vdash c_1 \sim c_2 \ :\ \{A_1\}y{:}T'\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma; \Gamma_1, x{:}T, \Gamma_2 \vdash c_1 \sim c_2 \ :\ \{A_1\}y{:}T'\{A_2\}^{\varrho}$.

Proof. Similarly to Lemma 101 with Lemma 44. □

Lemma 104. *Suppose that $a@r \notin dom\,(\Sigma)$. Let T be a type.*

(1) If $\Sigma; \gamma; \Gamma \vdash T_1 \sim T_2$, then $\Sigma, a@r{:}T; \gamma; \Gamma \vdash T_1 \sim T_2$.

(2) If $\Sigma; \gamma; \Gamma \vdash^{\varrho} A_1 \sim A_2$, then $\Sigma, a@r{:}T; \gamma; \Gamma \vdash^{\varrho} A_1 \sim A_2$.

(3) If $\Sigma; \gamma; \Gamma \vdash e_1 \sim e_2 \ :\ T$, then $\Sigma, a@r{:}T; \gamma; \Gamma \vdash e_1 \sim e_2 \ :\ T$.

(4) If $\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu; \Sigma, a@r{:}T; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}$.

(5) If $\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}$, then $\Sigma, a@r{:}T; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}$.

(6) If $\mu; \Sigma; \gamma \vdash p_1 \sim p_2 \ :\ T^{\gamma'}$, then $\mu; \Sigma, a@r{:}T; \gamma \vdash p_1 \sim p_2 \ :\ T^{\gamma'}$.

(7) If $\gamma \vdash \mu_1 \sim \mu_2 \ :\ (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and $a@r \notin dom\,(\Sigma')$ and $r \notin \gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}$, then $\gamma \vdash \mu_1 \sim \mu_2 \ :\ (\Sigma, a@r{:}T, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$.

Proof. Similarly to Lemma 101 with Lemma 42. □

Lemma 105. *If $\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}$, then $\varrho \subseteq \varrho'$.*

Proof. Straightforward by induction on the derivation of $\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\varrho'}$. □

Lemma 106. *Suppose that $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \subseteq \langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle$ and ${\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \subseteq \gamma$.*

(1) If $\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$.

(2) If $\Sigma; \gamma \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\Sigma; \gamma, r \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle} \Rightarrow \{A'_1\}y{:}T'\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$.

(3) If $\mu; \Sigma; \gamma \vdash p_1 \sim p_2 \ :\ T^{\gamma_{\mathtt{r}}}$, then $\mu; \Sigma; \gamma \vdash p_1 \sim p_2 \ :\ T^{{\gamma_{\mathtt{r}}}'}$.

Proof. By induction on the derivations with Lemma 48. We mention only interesting cases.

Case (AEC_Frame): We are given $\mu; \Sigma; \gamma; \Gamma \vdash y \leftarrow \mathsf{do}\, c_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim c_2 \ :\ \{A_1, A\}x{:}T\{A_2, A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$,
- $\langle {\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{r}}}''', {\gamma_{\mathtt{w}}}'' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $\Sigma; \gamma; \Gamma \vdash^{\langle {\gamma_{\mathtt{r}}}''', \emptyset \rangle} A$, and
- $\Sigma; \gamma; \Gamma \vdash {\gamma_{\mathtt{r}}}''' \,\mathsf{disj}\, {\gamma_{\mathtt{w}}}''$

for some fresh variable y. Since $\langle {\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{r}}}''', {\gamma_{\mathtt{w}}}'' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \subseteq \langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle$, we finish by the IH and (AEC_Frame). The well typedness of c_1 at $\{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$ is shown by Lemma 48.

Case (AEC_RegionNEq2): We are given

$$\mu; \Sigma; \gamma; \Gamma \vdash \nu r.\ C^{\mathsf{c}}_{\mathtt{n}1}\,[\,\mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathtt{not}\,(r == s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true};\, c'_1\,] \sim \nu r.\ C^{\mathsf{c}}_{\mathtt{n}2}\,[\,\mathsf{let}\, y = \mathsf{true};\, c_2\,] \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$$

and, by inversion,

- $s \in \gamma$,
- $\Sigma; \gamma, r; \emptyset \vdash \{A'_1\}x{:}T'\{A'_2\}^{\varrho' \uplus \{r\}}$.

- $\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\Sigma; \gamma, r \vdash C^{\mathtt{c}}_{\mathtt{n1}} \sim C^{\mathtt{c}}_{\mathtt{n2}} \,:\, \{A'_1\}x{:}T'\{A'_2\}^{\varrho' \uplus \{r\}} \Rightarrow \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \uplus \{r\}}$, and
- $\mu; \Sigma; \gamma, r; y{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(r \mathrel{==} s)\} \vdash c_1 \sim c_2 \,:\, \{A'_1\}x{:}T'\{A'_2\}^{\varrho' \uplus \{r\}}$,

Since $r \notin \gamma$, we have $r \notin {\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'$. Since $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \subseteq \langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle$, we have $\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \uplus \{r\} \subseteq \langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \uplus \{r\}$. By the IH ((2)),

$$\Sigma; \gamma, r \vdash C^{\mathtt{c}}_{\mathtt{n1}} \sim C^{\mathtt{c}}_{\mathtt{n2}} \,:\, \{A'_1\}x{:}T'\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \uplus \{r\}} \Rightarrow \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \uplus \{r\}}.$$

By Lemma 48 (1),

$$\Sigma; \gamma; \emptyset \vdash \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}.$$

Since $\varrho' \uplus \{r\} \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle \uplus \{r\}$ by Lemma 105, we have $\varrho' \uplus \{r\} \subseteq \langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \uplus \{r\}$. Thus, by the IH,

$$\mu; \Sigma; \gamma, r; y{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(r \mathrel{==} s)\} \vdash c_1 \sim c_2 \,:\, \{A'_1\}x{:}T'\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \uplus \{r\}}.$$

Since $\Sigma; \gamma, r; \emptyset \vdash \{A'_1\}x{:}T'\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \uplus \{r\}}$ by Lemma 48 (1), we finish by (AEC_RegionNEq2).

□

Lemma 107. *Suppose that $a@r \notin dom\,(\mu)$.*

(1) If $\mu; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$. Moreover, the lengths of the two derivations are the same.

(2) If $\mu; \Sigma; \gamma \vdash p_1 \sim p_2 \,:\, T^{\gamma'}$, then $\mu \uplus \{a@r \mapsto v\}; \Sigma; \gamma \vdash p_1 \sim p_2 \,:\, T^{\gamma'}$. Moreover, the lengths of the two derivations are the same.

Proof. Straightforward by induction on the derivations with Lemma 89 for ensuring well typedness of the left-hand side. □

Lemma 108. *If $\Sigma; \gamma_1; \Gamma_1 \vdash e_1 \,:\, T$ and $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e_1/x\,]\,\Gamma_2 \vdash \langle \mu, \sigma \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and $\sigma(e_1)$ is a value, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash \langle \mu, \sigma \uplus \{x \mapsto \sigma(e_1)\} \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$.*

Proof. Suppose that $\Sigma; \gamma_1; \Gamma_1 \vdash e_1 \,:\, T$ and $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e_1/x\,]\,\Gamma_2 \vdash \langle \mu, \sigma \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. By definition, there exist some Σ' and γ' such that

- $\Sigma \subseteq \Sigma'$,
- $\gamma_1, \gamma_2 \subseteq \gamma'$,
- for any $r \in (\gamma_1, \gamma_2)$, $r \notin dom\,(\sigma)$,
- for any $r \in (\Gamma_1, [\,e_1/x\,]\,\Gamma_2)$, $\sigma(s) \in \gamma'$,
- for any $y{:}T' \in (\Gamma_1, [\,e_1/x\,]\,\Gamma_2)$, $\Sigma'; \gamma'; \emptyset \vdash \sigma(y) \,:\, \sigma(T')$,
- $\gamma' \vdash \mu \,:\, {\Sigma'}^{\sigma(\gamma_{\mathtt{r}}) \cup \sigma(\gamma_{\mathtt{w}})}$, and
- σ maps term variables to values.

To show that $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash \langle \mu, \sigma \uplus \{x \mapsto \sigma(e_1)\} \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, it suffices to prove that, for any $z{:}T'' \in (x{:}T, \Gamma_2)$,

$$\Sigma'; \gamma'; \emptyset \vdash (\sigma \uplus \{x \mapsto \sigma(e_1)\})(z) \,:\, (\sigma \uplus \{x \mapsto \sigma(e_1)\})(T'')$$

(note that $\sigma(e_1)$ is a value).

If $z = x$, then we have to show $\Sigma'; \gamma'; \emptyset \vdash \sigma(e_1) \,:\, \sigma(T)$. Since $\Sigma; \gamma_1; \Gamma_1 \vdash e_1 \,:\, T$, we have $\Sigma'; \gamma_1; \Gamma_1 \vdash e_1 \,:\, T$ by Lemma 42 (4). Let $\Gamma_3 = r'_1, ..., r'_n$ where $r'_1, ..., r'_n$ are fresh region variables and n is the number of region variables bound in Γ_1. By Lemma 41, we have $\Sigma'; \gamma_1; \Gamma_3, \Gamma_1 \vdash e_1 \,:\, T$. By Lemma 50 (4), we can substitute region variables bound in Γ_3 for ones bound in Γ_1. Thus, by Lemma 40 with $\gamma' \supseteq \gamma_1$ (note that region variables in $\gamma' \setminus \gamma_1$ do not occur by the substitution above) and Lemma 50 (4) (to rename region variables bound in Γ_3 to ones in γ'), and Lemma 46 (4), we have $\Sigma'; \gamma'; \emptyset \vdash \sigma(e_1) \,:\, T$.

Otherwise, if $z{:}T'' \in \Gamma_2$, then it suffices to show that $\Sigma'; \gamma'; \emptyset \vdash \sigma(z) \,:\, (\sigma \uplus \{x \mapsto \sigma(e_1)\})(T'')$. Since $z{:}([\,e_1/x\,]\,T'') \in [\,e_1/x\,]\,\Gamma_2$, we have $\Sigma'; \gamma'; \emptyset \vdash \sigma(z) \,:\, \sigma([\,e_1/x\,]\,T'')$. Since $\sigma([\,e_1/x\,]\,T'') = (\sigma \uplus \{x \mapsto \sigma(e_1)\})(T'')$, we finish. □

Lemma 109. *If $\Sigma; \gamma_1; \Gamma_1 \vdash e_1 \,:\, T$ and $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash \gamma'_1 \;\mathsf{disj}\; \gamma'_2$ and e_1 is a value or a variable, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\,e_1/x\,]\,\Gamma_2 \vdash \gamma'_1 \;\mathsf{disj}\; \gamma'_2$.*

Proof. Similarly to Lemma 100 with Lemma 108; note that, for any closing value substitution σ, $\sigma(e_1)$ is a value by Lemma 1. □

Lemma 110. *Suppose that $\Sigma; \gamma_1; \Gamma_1 \vdash e_1 \sim e_2 : T$ and e_1 is a value or a variable.*

(1) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash T_1 \sim T_2$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash [\, e_1/x \,] T_1 \sim [\, e_2/x \,] T_2$.

(2) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash^{\varrho} A_1 \sim A_2$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash^{\varrho} [\, e_1/x \,] A_1 \sim [\, e_2/x \,] A_2$.

(3) If $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash e'_1 \sim e'_2 : T'$, then $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash [\, e_1/x \,] e'_1 \sim [\, e_2/x \,] e'_2 : [\, e_1/x \,] T'$.

(4) If $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash c_1 \sim c_2 : \{A_1\}y{:}T\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash [\, e_1/x \,] c_1 \sim [\, e_2/x \,] c_2 : [\, e_1/x \,] (\{A_1\}y{:}T\{A_2\}^{\varrho})$.

Proof. By induction on the derivations with Lemma 46. We mention only interesting cases.

Case (AETm_Var): We are given $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash y \sim y : T'$. If $x = y$, then it suffices to show that $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash e_1 \sim e_2 : T$. Since $\Sigma; \gamma_1; \Gamma_1 \vdash e_1 \sim e_2 : T$, we finish by Lemmas 101 (3), 102 (3) and 103 (3).

Case (AEC_ElimAssert): We are given $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash \mathsf{assert}\,(c_{11})^{\ell}; c_{12} \sim c_{22} : \{A_1\}x{:}T\{A_2\}^{\varrho}$ and, by inversion,

- $\emptyset; \Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash c_{12} \sim c_{22} : \{A_1, c_{11}\}x{:}T\{A_2\}^{\varrho}$,
- $A'_1 \subseteq A_1$,
- $\varrho' \subseteq \varrho$,
- $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash^{\varrho'} A'_1, c_{11}$, and
- for any μ' and σ', if $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash \langle \mu', \sigma' \rangle^{\varrho'}$ and $\mu' \models \sigma'(A'_1)$, then $\mu' \models \sigma'(c_{11})$.

By the IH, we have $\emptyset; \Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash [\, e_1/x \,] c_{12} \sim [\, e_2/x \,] c_{22} : [\, e_1/x \,] (\{A_1, c_{11}\}x{:}T\{A_2\}^{\varrho})$. By Lemma 46 (3), $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash^{\varrho'} [\, e_1/x \,] (A'_1, c_{11})$. Since $A'_1 \subseteq A_1$, we have $[\, e_1/x \,] A'_1 \subseteq [\, e_1/x \,] A_1$. Thus, by (AEC_ElimAssert), it suffices to show that, for any σ' and μ', if $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash \langle \mu', \sigma' \rangle^{\varrho'}$ and $\mu' \models \sigma'([\, e_1/x \,] A'_1)$, then $\mu' \models \sigma'([\, e_1/x \,] c_{11})$. Let σ' and μ' be a substitution and a store such that $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash \langle \mu', \sigma' \rangle^{\varrho'}$ and $\mu' \models \sigma'([\, e_1/x \,] A'_1)$. Since $\sigma(e_1)$ is a value (by Lemma 1 if e_1 is a value), we have $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash \langle \mu', \sigma' \uplus \{x \mapsto \sigma'(e_1)\} \rangle^{\varrho'}$ by Lemma 108. Since $\sigma'([\, e_1/x \,] A'_1) = (\sigma' \uplus \{x \mapsto \sigma'(e_1)\})(A'_1)$ and $\sigma'([\, e_1/x \,] c_{11}) = (\sigma' \uplus \{x \mapsto \sigma'(e_1)\})(c_{11})$, we have $\mu' \models \sigma'([\, e_1/x \,] c_{11})$ by the inversion of the derivation.

Case (AEC_Frame): We are given $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash y \leftarrow \mathsf{do}\, c'_1; \mathsf{assert}\,(A')^{\ell}; \mathsf{return}\, y \sim c_2 : \{A'_1, A'\}x{:}T\{A'_2, A'\}^{\varrho}$ and, by inversion,

- $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash c'_1 \sim c_2 : \{A'_1\}x{:}T\{A'_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\langle \gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}} \rangle \subseteq \varrho$,
- $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash^{\langle {\gamma_{\mathtt{r}}}', \emptyset \rangle} A'$, and
- $\Sigma; \gamma_1, \gamma_2; \Gamma_1, x{:}T, \Gamma_2 \vdash {\gamma_{\mathtt{r}}}' \,\mathsf{disj}\, \gamma_{\mathtt{w}}$

for some fresh y. By the IH, $\mu; \Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash [\, e_1/x \,] c'_1 \sim [\, e_2/x \,] c_2 : [\, e_1/x \,] (\{A'_1\}x{:}T\{A'_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle})$. By Lemma 46 (3), $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash^{\langle {\gamma_{\mathtt{r}}}', \emptyset \rangle} A'$. By Lemma 109, $\Sigma; \gamma_1, \gamma_2; \Gamma_1, [\, e_1/x \,] \Gamma_2 \vdash {\gamma_{\mathtt{r}}}' \,\mathsf{disj}\, \gamma_{\mathtt{w}}$. Thus, we finish by (AEC_Frame).

□

Lemma 111. *If $r \in \gamma$ and $\Sigma; \gamma; \Gamma_1, [\, r/s \,] \Gamma_2 \vdash \langle \mu, \sigma \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \langle \mu, \sigma \uplus \{s \mapsto r\} \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$.*

Proof. Suppose that $r \in \gamma$ and $\Sigma; \gamma; \Gamma_1, [\, r/s \,] \Gamma_2 \vdash \langle \mu, \sigma \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. By definition, there exist some Σ' and γ' such that

- $\Sigma \subseteq \Sigma'$,
- $\gamma \subseteq \gamma'$,
- for any $t \in \gamma$, $t \notin \mathit{dom}\,(\sigma)$,
- for any $t \in (\Gamma_1, [\, r/s \,] \Gamma_2)$, $\sigma(t) \in \gamma'$,
- for any $y{:}T' \in (\Gamma_1, [\, r/s \,] \Gamma_2)$, $\Sigma'; \gamma'; \emptyset \vdash \sigma(y) : \sigma(T')$, and
- $\gamma' \vdash \mu : {\Sigma'}^{\sigma(\gamma_{\mathtt{r}}) \cup \sigma(\gamma_{\mathtt{w}})}$.

To show that $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \langle \mu, \sigma \uplus \{s \mapsto r\}\rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, it suffices to prove that (1) $(\sigma \uplus \{s \mapsto r\})(s) = r \in \gamma$ and (2) for any $z{:}T'' \in \Gamma_2$,

$$\Sigma'; \gamma'; \emptyset \vdash (\sigma \uplus \{s \mapsto r\})(z) \,:\, (\sigma \uplus \{s \mapsto r\})(T'').$$

Since $r \in \gamma$ by the assumption, we show (2) in what follows. Let $z{:}T'' \in \Gamma_2$. Since $z{:}([\,r/s\,]\,T'') \in [\,r/s\,]\,\Gamma_2$, we have $\Sigma'; \gamma'; \emptyset \vdash \sigma(z) \,:\, \sigma([\,r/s\,]\,T'')$. Since $\sigma(z) = (\sigma \uplus \{s \mapsto r\})(z)$ and $\sigma([\,r/s\,]\,T'') = (\sigma \uplus \{s \mapsto r\})(T'')$, we finish. □

Lemma 112. *If $r \in \gamma$ and $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \gamma_1 \mathrel{\mathsf{disj}} \gamma_2$, then $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,\gamma_1 \mathrel{\mathsf{disj}} [\,r/s\,]\,\gamma_2$.*

Proof. Suppose that $r \in \gamma$ and $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \gamma_1 \mathrel{\mathsf{disj}} \gamma_2$. Let σ be a substitution such that $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash \sigma$. By definition, it suffices to show that $\sigma([\,r/s\,]\,\gamma_1) \cap \sigma([\,r/s\,]\,\gamma_2) = \emptyset$. By Lemma 111, $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \sigma \uplus \{s \mapsto r\}$. Since $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \gamma_1 \mathrel{\mathsf{disj}} \gamma_2$, we have $(\sigma \uplus \{s \mapsto r\})(\gamma_1) \cap (\sigma \uplus \{s \mapsto r\})(\gamma_2) = \emptyset$. Since $r \notin \mathit{dom}(\sigma)$ by $r \in \gamma$ and definition of σ, we have $(\sigma \uplus \{s \mapsto r\})(\gamma_i) = \sigma([\,r/s\,]\,\gamma_i)$ for $i \in \{1, 2\}$. Thus, we finish. □

Lemma 113. *Suppose that $r \in \gamma$.*

(1) If $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash T_1 \sim T_2$, then $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,T_1 \sim [\,r/s\,]\,T_2$.

(2) If $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash^{\varrho} A_1 \sim A_2$, then $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash^{[\,r/s\,]\,\varrho} [\,r/s\,]\,A_1 \sim [\,r/s\,]\,A_2$.

(3) If $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash e_1 \sim e_2 \,:\, T'$, then $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,e_1 \sim [\,r/s\,]\,e_2 \,:\, [\,r/s\,]\,T'$.

(4) If $\mu; \Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\mu; \Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,c_1 \sim [\,r/s\,]\,c_2 \,:\, [\,r/s\,]\,(\{A_1\}x{:}T\{A_2\}^{\varrho})$.

Proof. Similarly to Lemma 110 with Lemmas 50, 111, 112 and 49. We mention only the case for (AEC_RegionNEq1). We are given $\mu; \Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \nu t.\, \mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathtt{not}\,(t =\!= u)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c_1' \sim \nu t.\, \mathsf{let}\, y = \mathsf{true}; c_2' \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$ and, by inversion,

- $u \in \gamma \cup \mathit{regions}\,(\Gamma_1, s, \Gamma_2)$,
- $\Sigma; \gamma; \Gamma_1, s, \Gamma_2 \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}$, and
- $\mu; \Sigma; \gamma, t; \Gamma_1, s, \Gamma_2, y{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(t =\!= u)\} \vdash c_1' \sim c_2' \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{t\}}$.

Without loss of generality, we can suppose that $t \neq r$ and $t \neq s$. By the IH,

$$\mu; \Sigma; \gamma, t; \Gamma_1, [\,r/s\,]\,\Gamma_2, y{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(t =\!= [\,r/s\,]\,u)\} \vdash [\,r/s\,]\,c_1' \sim [\,r/s\,]\,c_2' \,:\, [\,r/s\,]\,(\{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{t\}}).$$

If $s = u$, then $[\,r/s\,]\,u \in \gamma$ since $r \in \gamma$; otherwise, if $s \neq u$, then $[\,r/s\,]\,u \in \gamma \cup \mathit{regions}\,(\Gamma_1, \Gamma_2)$ since $u \in \gamma \cup \mathit{regions}\,(\Gamma_1, s, \Gamma_2)$. Thus, $[\,r/s\,]\,u \in \gamma \cup \mathit{regions}\,(\Gamma_1, [\,r/s\,]\,u)$. Since $\Sigma; \gamma; \Gamma_1, [\,r/s\,]\,\Gamma_2 \vdash [\,r/s\,]\,(\{A_1\}x{:}T\{A_2\}^{\varrho})$ by Lemma 50 (2), we finish by (AEC_RegionNEq1). □

Lemma 114. *(1) If $\Sigma; \gamma; \Gamma \vdash T_1 \sim B$, then $T_1 = B$.*

(2) If $\Sigma; \gamma; \Gamma \vdash B \sim T_2$, then $T_2 = B$.

Proof. By case analysis on the rule applied last. □

Lemma 115. *(1) If $\Sigma; \gamma; \Gamma \vdash T_1 \sim x{:}T_{21} \to T_{22}$, then $T_1 = x{:}T_{11} \to T_{12}$ for some T_{11} and T_{12}.*

(2) If $\Sigma; \gamma; \Gamma \vdash x{:}T_{11} \to T_{12} \sim T_2$, then $T_2 = x{:}T_{21} \to T_{22}$ for some T_{21} and T_{22}.

(3) If $\Sigma; \gamma; \Gamma \vdash x{:}T_{11} \to T_{12} \sim x{:}T_{21} \to T_{22}$, then $\Sigma; \gamma; \Gamma \vdash T_{11} \sim T_{21}$ and $\Sigma; \gamma; \Gamma, x{:}T_{11} \vdash T_{12} \sim T_{22}$.

Proof. By case analysis on the rule applied last. □

Lemma 116. *(1) If $\Sigma; \gamma; \Gamma \vdash T_1 \sim \mathsf{Ref}_r\, T_2'$, then $T_1 = \mathsf{Ref}_r\, T_1'$ for some T_1'.*

(2) If $\Sigma; \gamma; \Gamma \vdash \mathsf{Ref}_r\, T_1' \sim T_2$, then $T_2 = \mathsf{Ref}_r\, T_2'$ for some T_2'.

(3) If $\Sigma; \gamma; \Gamma \vdash \mathsf{Ref}_r\, T_1 \sim \mathsf{Ref}_r\, T_2$, then $\Sigma; \gamma; \Gamma \vdash T_1 \sim T_2$.

Proof. By case analysis on the rule applied last. □

Lemma 117. *(1) If $\Sigma; \gamma; \Gamma \vdash T_1 \sim \{x{:}T_2' \mid c_2'\}$, then $T_1 = \{x{:}T_1' \mid c_1'\}$ for some T_1' and c_1'.*

(2) If $\Sigma; \gamma; \Gamma \vdash \{x{:}T_1' \mid c_1'\} \sim T_2$, then $T_2 = \{x{:}T_2' \mid c_2'\}$ for some T_2' and c_2'.

(3) If $\Sigma; \gamma; \Gamma \vdash \{x{:}T_1 \mid c_1\} \sim \{x{:}T_2 \mid c_2\}$, then $\Sigma; \gamma; \Gamma \vdash T_1 \sim T_2$ and $\emptyset; \Sigma; \gamma; \Gamma, x{:}T_1 \vdash c_1 \sim c_2 \,:\, \{\top\}\mathsf{bool}\{\top\}^{\langle \emptyset, \emptyset \rangle}$.

Proof. By case analysis on the rule applied last. □

Lemma 118. *(1) If $\Sigma;\gamma;\Gamma \vdash T_1 \sim \{A_{21}\}x{:}T_2'\{A_{22}\}^\varrho$, then $T_1 = \{A_{11}\}x{:}T_1'\{A_{12}\}^\varrho$ for some A_{11}, T_1', and A_{12}.*

(2) If $\Sigma;\gamma;\Gamma \vdash \{A_{11}\}x{:}T_1'\{A_{12}\}^\varrho \sim T_2$, then $T_2 = \{A_{21}\}x{:}T_2'\{A_{22}\}^\varrho$ for some A_{21}, T_2', and A_{22}.

(3) If $\Sigma;\gamma;\Gamma \vdash \{A_{11}\}x{:}T_1\{A_{12}\}^\varrho \sim \{A_{21}\}x{:}T_2\{A_{22}\}^\varrho$, then

- $\Sigma;\gamma;\Gamma \vdash^\varrho A_{11} \sim A_{21}$,
- $\Sigma;\gamma;\Gamma \vdash T_1 \sim T_2$, *and*
- $\Sigma;\gamma;\Gamma, x{:}T_1 \vdash^\varrho A_{12} \sim A_{22}$.

Proof. By case analysis on the rule applied last. □

Lemma 119. *(1) If $\Sigma;\gamma;\Gamma \vdash T_1 \sim \forall r.T_2'$, then $T_1 = \forall r.T_1'$ for some T_1'.*

(2) If $\Sigma;\gamma;\Gamma \vdash \forall r.T_1' \sim T_2$, then $T_2 = \forall r.T_2'$ for some T_2'.

(3) If $\Sigma;\gamma;\Gamma \vdash \forall r.T_1 \sim \forall r.T_2$, then $\Sigma;\gamma;\Gamma, r \vdash T_1 \sim T_2$.

Proof. By case analysis on the rule applied last. □

Lemma 120. *(1) If $\Sigma;\gamma;\Gamma \vdash e_1 \sim k : T$, then $e_1 = k$.*

(2) If $\Sigma;\gamma;\Gamma \vdash k \sim e_2 : T$, then $e_2 = k$.

Proof. Straightforward by induction on the derivation with Lemmas 51, 102 (3), 103 (3) and 58. □

Lemma 121. *(1) If $\Sigma;\gamma;\Gamma \vdash e_1 \sim \lambda x{:}T_{21}'.e_2' : T$, then $e_1 = \lambda x{:}T_{11}'.e_1'$ for some T_{11}' and e_1'.*

(2) If $\Sigma;\gamma;\Gamma \vdash \lambda x{:}T_{11}'.e_1' \sim e_2 : T$, then $e_2 = \lambda x{:}T_{21}'.e_2'$ for some T_{21}' and e_2'.

(3) If $\Sigma;\gamma;\Gamma \vdash \lambda x{:}T_{11}.e_1 \sim \lambda x{:}T_{21}.e_2 : T$, then there exists some T_{12} such that

- $\Sigma;\gamma;\Gamma, x{:}T_{11} \vdash e_1 \sim e_2 : T_{12}$,
- $\Sigma;\gamma;\Gamma \vdash T_{11} \sim T_{21}$, *and*
- $x{:}T_{11} \rightarrow T_{12} \equiv \mathit{unref}\,(T)$.

Proof. Straightforward by induction on the derivation with Lemmas 51, 102 (3), 103 (3) and 58. □

Lemma 122. *(1) If $\Sigma;\gamma;\Gamma \vdash e_1 \sim \langle T_{21} \Leftarrow T_{22}\rangle^\ell : T$, then $e_1 = \langle T_{11} \Leftarrow T_{12}\rangle^\ell$ for some T_{11} and T_{12}.*

(2) If $\Sigma;\gamma;\Gamma \vdash \langle T_{11} \Leftarrow T_{12}\rangle^\ell \sim e_2 : T$, then $e_2 = \langle T_{21} \Leftarrow T_{22}\rangle^\ell$ for some T_{21} and T_{22}.

(3) If $\Sigma;\gamma;\Gamma \vdash \langle T_{11} \Leftarrow T_{12}\rangle^\ell \sim \langle T_{21} \Leftarrow T_{22}\rangle^\ell : T$, then

- $\Sigma;\gamma;\Gamma \vdash T_{11} \sim T_{21}$,
- $\Sigma;\gamma;\Gamma \vdash T_{12} \sim T_{22}$, *and*
- $T_{12} \rightarrow T_{11} \equiv \mathit{unref}\,(T)$.

Proof. Straightforward by induction on the derivation with Lemmas 51, 102 (3), 103 (3) and 58. □

Lemma 123.
- *If $\Sigma;\gamma;\Gamma \vdash e_1 \sim a@r : T$, then $e_1 = a@r$.*
- *If $\Sigma;\gamma;\Gamma \vdash a@r \sim e_2 : T$, then $e_2 = a@r$.*
- *If $\Sigma;\gamma;\Gamma \vdash a@r \sim a@r : T$, then there exists some T' such that $a@r{:}T' \in \Sigma$ and $\mathsf{Ref}_r\,T' \equiv \mathit{unref}\,(T)$.*

Proof. Straightforward by induction on the derivation with Lemmas 51, 102 (3), 103 (3) and 58. □

Lemma 124. *(1) If $\Sigma;\gamma;\Gamma \vdash e_1 \sim (T_{21} \Leftarrow^\ell T_{22} : v_2) : T$, then $e_1 = T_{11} \Leftarrow^\ell T_{12} : v_1$ for some T_{11}, T_{12}, and v_1.*

(2) If $\Sigma;\gamma;\Gamma \vdash (T_{11} \Leftarrow^\ell T_{12} : v_1) \sim e_2 : T$, then $e_2 = T_{21} \Leftarrow^\ell T_{22} : v_2$ for some T_{21}, T_{22}, and v_2.

(3) If $\Sigma;\gamma;\Gamma \vdash (T_{11} \Leftarrow^\ell T_{12} : v_1) \sim (T_{21} \Leftarrow^\ell T_{22} : v_2) : T$, then there exists some r such that

- $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \,:\, \mathsf{Ref}_r\, T_{12}$,
- $\Sigma; \gamma; \emptyset \vdash T_{11} \sim T_{21}$,
- $\Sigma; \gamma; \emptyset \vdash T_{12} \sim T_{22}$, *and*
- $\mathsf{Ref}_r\, T_{11} \,\equiv\, \mathit{unref}\,(T)$.

Proof. Straightforward by induction on the derivation with Lemmas 51, 102 (3), 103 (3) and 58. □

Lemma 125. *(1) If* $\Sigma; \gamma; \Gamma \vdash e_1 \sim \lambda r.e_2' \,:\, T$, *then* $e_1 \,=\, \lambda r.e_1'$ *for some* e_1'.

(2) If $\Sigma; \gamma; \Gamma \vdash \lambda r.e_1' \sim e_2 \,:\, T$, *then* $e_2 \,=\, \lambda r.e_2'$ *for some* e_2'.

(3) If $\Sigma; \gamma; \Gamma \vdash \lambda r.e_1 \sim \lambda r.e_2 \,:\, T$, *then there exists some* T' *such that* $\Sigma; \gamma; \Gamma, r \vdash e_1 \sim e_2 \,:\, T'$ *and* $\forall r.T' \,\equiv\, \mathit{unref}\,(T)$.

Proof. Straightforward by induction on the derivation with Lemmas 51, 102 (3), 103 (3) and 58. □

Lemma 126. *(1) If* $\Sigma; \gamma; \Gamma \vdash e_1 \sim \mathsf{do}\, c_2 \,:\, T$, *then* $e_1 \,=\, \mathsf{do}\, c_1$ *for some* c_1.

(2) If $\Sigma; \gamma; \Gamma \vdash \mathsf{do}\, c_1 \sim e_2 \,:\, T$, *then* $e_2 \,=\, \mathsf{do}\, c_2$ *for some* c_2.

(3) If $\Sigma; \gamma; \Gamma \vdash \mathsf{do}\, c_1 \sim \mathsf{do}\, c_2 \,:\, T$, *then there exists some* A_1, x, T', A_2, *and* ϱ *such that* $\emptyset; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T'\{A_2\}^{\varrho}$ *and* $\{A_1\}x{:}T'\{A_2\}^{\varrho} \,\equiv\, \mathit{unref}\,(T)$. *Moreover, the length of the derivation of* $\emptyset; \Sigma; \gamma; \Gamma \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T'\{A_2\}^{\varrho}$ *is smaller than that of* $\Sigma; \gamma; \Gamma \vdash \mathsf{do}\, c_1 \sim \mathsf{do}\, c_2 \,:\, T$.

Proof. Straightforward by induction on the derivation with Lemmas 51, 102 (3), 103 (3) and 58. □

Lemma 127. *(1)* $\Sigma; \gamma; \Gamma \vdash e_1 \sim v_2 \,:\, T$, *then* e_1 *is a value.*

(2) $\Sigma; \gamma; \Gamma \vdash v_1 \sim e_2 \,:\, T$, *then* e_2 *is a value.*

Proof. By Lemmas 120, 121, 122, 123, 124, 125 and 126. □

Lemma 128. *(1)* $\Sigma; \gamma; \Gamma \vdash e_1 \sim E_2[\Uparrow\ell] \,:\, T$, *then* $e_1 \,=\, E_1[\Uparrow\ell]$ *for some* E_1.

(2) $\Sigma; \gamma; \Gamma \vdash E_1[\Uparrow\ell] \sim e_2 \,:\, T$, *then* $e_2 \,=\, E_2[\Uparrow\ell]$ *for some* E_2.

Proof. Straightforward by induction on the derivation. □

Lemma 129. *(1) If* $\mu; \Sigma; \gamma \vdash p_1 \sim \nu\gamma'.\langle \mu_2 \mid c_2 \rangle \,:\, T^{\gamma''}$, *then* $p_1 \,=\, \nu\gamma'.\langle \mu_1 \mid c_1 \rangle$ *for some* μ_1 *and* c_1.

(2) If $\mu; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu_1 \mid c_1 \rangle \sim p_2 \,:\, T^{\gamma''}$, *then* $p_2 \,=\, \nu\gamma'.\langle \mu_2 \mid c_2 \rangle$ *for some* μ_2 *and* c_2.

(3) If $\mu; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu_1 \mid c_1 \rangle \sim \nu\gamma'.\langle \mu_2 \mid c_2 \rangle \,:\, T^{\gamma_{\mathtt{r}}''}$, *then there exist some* Σ' *and* A_1 *such that*

- $\gamma, \gamma' \vdash \mu_1 \sim \mu_2 \,:\, (\Sigma, \Sigma')^{\gamma'}$ *and*
- $\mu \uplus \mu_1; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$

Proof. Straightforward by inversion of the derivation. □

Lemma 130. *If* $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \,:\, \mathsf{Ref}_r\, T$, *then* $\mathit{ungrd}\,(v_1) \,=\, \mathit{ungrd}\,(v_2)$.

Proof. By structural induction on v_1. From well-typedness of v_1, there are two cases we have to consider by Lemma 59 (3). If $v_1 = a@r$ for some a, we finish by Lemma 123. Otherwise, if $v_1 \,=\, T_{11} \Leftarrow^{\ell} T_{12} : v_1'$ for some T_{11}, T_{12}, ℓ, and v_1', then, by Lemma 124, there exist some T_{21}, T_{22}, ℓ, v_2', and s such that $v_2 \,=\, T_{21} \Leftarrow^{\ell} T_{22} : v_2'$ and $\Sigma; \gamma; \emptyset \vdash v_1' \sim v_2' \,:\, \mathsf{Ref}_s\, T_{12}$. Since $\mathit{ungrd}\,(v_1) \,=\, \mathit{ungrd}\,(v_1')$ and $\mathit{ungrd}\,(v_2) \,=\, \mathit{ungrd}\,(v_2')$ and $\mathit{ungrd}\,(v_1') \,=\, \mathit{ungrd}\,(v_2')$ by the IH, we have $\mathit{ungrd}\,(v_1) \,=\, \mathit{ungrd}\,(v_2)$. □

Lemma 131. *If*

- $\gamma \vdash \mu|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$,
- $\mu \models A$,
- $\Sigma; \gamma; \emptyset \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$, *and*
- *for any* μ' *and* σ', *if* $\Sigma; \gamma; \emptyset \vdash \langle \mu', \sigma' \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ *and* $\mu' \models \sigma'(A)$, *then* $\mu' \models \sigma'(c)$,

then $\mu \models c$.

Proof. By Lemma 88, it suffices to show that $(\mu\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}) \models c$. Form the assumption, it suffices to show that:

$$\Sigma; \gamma; \emptyset \vdash \langle \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}, \emptyset \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$$
$$\mu\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \models A$$

Since $\Sigma; \gamma; \emptyset \vdash^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle} A$ and $\mu \models A$, we have $\mu\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \models A$ by Lemma 98. We show that $\Sigma; \gamma; \emptyset \vdash \langle \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}, \emptyset \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. Since $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $\Sigma; \gamma; \emptyset \vdash \langle \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}, \emptyset \rangle^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. □

Lemma 132. *Suppose that* $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ *and* $\mu_1 \models A_1$.

(1) If $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \Uparrow\ell : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$*, then* $c_1 = \Uparrow\ell$ *or there exists some* c_1' *and* A_1' *such that*

- $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid c_1'$ *(the computation does not mutate contents in* μ_1*),*
- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1' \sim \Uparrow\ell : \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$
- $\mu_1 \models A_1'$*, and*
- *the size of* c_1' *is less than* c_1.

(2) If $\mu_1; \Sigma; \gamma; \emptyset \vdash \Uparrow\ell \sim c_2 : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$*, then* $c_2 = \Uparrow\ell$.

Proof. 1. By induction on the derivation of $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \Uparrow\ell : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ with case analysis on the rule applied last.

Case (AEC_Blame): Obvious.

Case (AEC_Weak): By the IH and (AEC_Weak).

Case (AEC_Conv): By the IH, (AEC_Conv), and Lemma 90.

Case (AEC_ElimAssert): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{assert}\,(c_{11})^{\ell'}; c_{12} \sim \Uparrow\ell : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\emptyset; \Sigma; \gamma; \emptyset \vdash c_{12} \sim \Uparrow\ell : \{A_1, c_{11}\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $A_1' \subseteq A_1$,
- $\Sigma; \gamma; \emptyset \vdash^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle} A_1', c_{11}$, and
- for any μ' and σ', if $\Sigma; \gamma; \emptyset \vdash \langle \mu', \sigma' \rangle^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$ and $\mu' \models \sigma'(A_1')$, then $\mu' \models \sigma'(c_{11})$.

By Lemma 107, we have $\mu_1; \Sigma; \gamma; \emptyset \vdash c_{12} \sim \Uparrow\ell : \{A_1, c_{11}\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, so we finish if $\mu_1 \models c_{11}$ is derived. Since $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$. Since $\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have $\gamma \vdash \mu_1\,|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} : \Sigma^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$ by Lemma 70. Since $\mu_1 \models A_1$ and $A_1' \subseteq A_1$, we have $\mu_1 \models A_1'$. Thus, by Lemma 131, we have $\mu_1 \models c_{11}$.

Case (AEC_Frame): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1'; \mathsf{assert}\,(A)^{\ell'}; \mathsf{return}\, y \sim \Uparrow\ell : \{A_1', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1' \sim \Uparrow\ell : \{A_1'\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
- $\langle {\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $\Sigma; \gamma; \emptyset \vdash^{\langle {\gamma_{\mathtt{r}}}'', \emptyset \rangle} A$, and
- $\Sigma; \gamma; \emptyset \vdash {\gamma_{\mathtt{r}}}'' \,\mathsf{disj}\, {\gamma_{\mathtt{w}}}'$

for some fresh y. If $c_1' = \Uparrow\ell$, then we have $\mu_1 \mid c_1 \longrightarrow \mu_1 \mid \Uparrow\ell$ by (C_CBlame). Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \Uparrow\ell \sim \Uparrow\ell : \{A_1', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ by (AEC_Blame), we finish. Otherwise, if $c_1' \neq \Uparrow\ell$, then, by the IH, there exists some c_1'' and A_1'' such that

- $\mu_1 \mid c_1' \longrightarrow^* \mu_1 \mid c_1''$,
- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1'' \sim \Uparrow\ell : \{A_1''\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
- $\mu_1 \models A_1''$, and
- the size of c_1'' is less than c_1'.

By (C_Comput), $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid y \leftarrow \mathsf{do}\, c_1''; \mathsf{assert}\,(A)^{\ell'}; \mathsf{return}\, y$. By (AEC_Frame), $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1''; \mathsf{assert}\,(A)^{\ell'}; \mathsf{return}\, y \sim \Uparrow\ell : \{A_1'', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. Thus, we finish.

2. Straightforward by induction on the derivation of $\mu; \Sigma; \gamma; \Gamma \vdash \Uparrow\ell \sim c_2 : \{A_1\}x{:}T\{A_2\}^{\varrho}$.

□

Lemma 133. *Suppose that $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and $\mu_1 \models A_1$.*

(1) If $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \Uparrow\ell \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid \Uparrow\ell$ where the computation does not mutate contents in μ_1.

(2) If $\mu_1; \Sigma; \gamma; \emptyset \vdash \Uparrow\ell \sim c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid \Uparrow\ell$ where the computation does not mutate contents in μ_2.

Proof. The second case is derived immediately from Lemma 132. We show the first case by induction on the size of c_1. We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \Uparrow\ell \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. If $c_1 = \Uparrow\ell$, then we finish. Otherwise, by Lemma 132, there exists some c_1' and A_1' such that

- $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid c_1'$ (where the computation does not mutate contents in μ_1),
- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1' \sim \Uparrow\ell \;:\; \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\mu_1 \models A_1'$, and
- the size of c_1' is less than c_1.

We finish by the IH. □

Lemma 134. *If $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1 \sim \nu r.\, c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho}$, then:*

- *$\mu; \Sigma; \gamma, r; \emptyset \vdash c_1 \sim c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$; or*
- *there exist $C^{\mathsf{c}}_{\mathtt{n}1}$, $C^{\mathsf{c}}_{\mathtt{n}2}$, c_1', c_2', s, y, z, ℓ, A_1', T', A_2', and ϱ' such that*
  - $c_1 \;=\; C^{\mathsf{c}}_{\mathtt{n}1}\,[\,\mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathsf{not}\,(r =\!= s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true};\, c_1'\,]$,
  - $c_2 \;=\; C^{\mathsf{c}}_{\mathtt{n}2}\,[\,\mathsf{let}\, y = \mathsf{true};\, c_2'\,]$,
  - $s \in \gamma$,
  - $\Sigma; \gamma, r \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1'\}x{:}T'\{A_2'\}^{\varrho' \uplus \{r\}} \Rightarrow \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$,
  - $\mu; \Sigma; \gamma, r; y{:}\{z{:}\mathsf{bool} \mid \mathsf{not}\,(r =\!= s)\} \vdash c_1' \sim c_2' \;:\; \{A_1'\}x{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}$, *and*
  - $\Sigma; \gamma, r; \emptyset \vdash \{A_1'\}x{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}$.

Proof. By induction on the derivation of $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1 \sim \nu r.\, c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\varrho}$.

Case (AEC_Weak): By inversion,

- $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1 \sim \nu r.\, c_2 \;:\; \{A_1'\}x{:}T\{A_2'\}^{\varrho}$,
- $A_1' \subseteq A_1$, and
- $A_2 \subseteq A_2'$.

If $\mu; \Sigma; \gamma; \emptyset \vdash c_1 \sim c_2 \;:\; \{A_1'\}x{:}T\{A_2'\}^{\varrho \uplus \{r\}}$, then we finish by (AEC_Weak). Otherwise, by the IH, we are given

- $c_1 \;=\; C^{\mathsf{c}}_{\mathtt{n}1}\,[\,\mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathsf{not}\,(r =\!= s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true};\, c_1'\,]$,
- $c_2 \;=\; C^{\mathsf{c}}_{\mathtt{n}2}\,[\,\mathsf{let}\, y = \mathsf{true};\, c_2'\,]$,
- $s \in \gamma$,
- $\Sigma; \gamma, r \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1''\}x{:}T''\{A_2''\}^{\varrho'' \uplus \{r\}} \Rightarrow \{A_1'\}x{:}T\{A_2'\}^{\varrho \uplus \{r\}}$,
- $\mu; \Sigma; \gamma, r; y{:}\{z{:}\mathsf{bool} \mid \mathsf{not}\,(r =\!= s)\} \vdash c_1' \sim c_2' \;:\; \{A_1''\}x{:}T''\{A_2''\}^{\varrho'' \uplus \{r\}}$, and
- $\Sigma; \gamma, r; \emptyset \vdash \{A_1''\}x{:}T''\{A_2''\}^{\varrho'' \uplus \{r\}}$.

By (AEC_RegionNEq2), it suffices to show that $\Sigma; \gamma, r \vdash C^{\mathsf{c}}_{\mathtt{n}1} \sim C^{\mathsf{c}}_{\mathtt{n}2} \;:\; \{A_1''\}x{:}T''\{A_2''\}^{\varrho'' \uplus \{r\}} \Rightarrow \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$, which is derived by (AECc_Weak) since $A_1' \subseteq A_1$ and $A_2 \subseteq A_2'$.

Case (AEC_Conv): By the IH, (AEC_Conv), and (AECc_Conv).

Case (AEC_LetRegion): By inversion.

Case (AEC_RegionNEq1): By inversion and (AECc_Hole); we let $C^{\mathsf{c}}_{\mathtt{n}1}$ and $C^{\mathsf{c}}_{\mathtt{n}2}$ be $[\,]$. We can derive $\Sigma; \gamma, r; \emptyset \vdash \{A_1''\}x{:}T''\{A_2''\}^{\varrho'' \uplus \{r\}}$ by Lemmas 40 (2) and 48 (1).

Case (AEC_RegionNEq2): By inversion.

□

Lemma 135. *If*

- $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, C^{\mathsf{c}}_{\mathtt{n1}}[\, c_{11} \,] \sim \nu r.\, C^{\mathsf{c}}_{\mathtt{n2}}[\, c_{21} \,] \;:\; \{A_1\} y{:}T' \{A_3\}^{\varrho_1}$ *and*
- $\emptyset; \Sigma; \gamma, r; y{:}T' \vdash c_{12} \sim c_{22} \;:\; \{A_3\} x{:}T \{A_2\}^{\varrho_2}$,

then $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, y \leftarrow \mathsf{do}\, C^{\mathsf{c}}_{\mathtt{n1}}[\, c_{11} \,]; c_{12} \sim \nu r.\, y \leftarrow \mathsf{do}\, C^{\mathsf{c}}_{\mathtt{n2}}[\, c_{21} \,]; c_{22} \;:\; \{A_1\} x{:}T \{A_2\}^{\varrho_1 \cup \varrho_2}$.

Proof. By Lemma 134, there are two cases we have to consider.

- Suppose that $\mu; \Sigma; \gamma, r; \emptyset \vdash C^{\mathsf{c}}_{\mathtt{n1}}[\, c_{11} \,] \sim C^{\mathsf{c}}_{\mathtt{n2}}[\, c_{21} \,] \;:\; \{A_1\} y{:}T' \{A_3\}^{\varrho_1 \uplus \{r\}}$. Since $\emptyset; \Sigma; \gamma, r; y{:}T' \vdash c_{12} \sim c_{22} \;:\; \{A_3\} x{:}T \{A_2\}^{\varrho_2}$ by Lemma 101 (4), we have

  $$\mu; \Sigma; \gamma, r; \emptyset \vdash y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, c_1 \,]; c'_{12} \sim y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, c_2 \,]; c'_{22} \;:\; \{A_1\} x{:}T \{A_2\}^{\varrho \uplus \{r\}}$$

  by (AEC_CBind). By (AEC_LetRegion), we finish.

- Suppose that

  - $C^{\mathsf{c}}_{\mathtt{n1}}[\, c_{11} \,] \;=\; C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, \mathsf{let}\, z = \langle \{z{:}\mathsf{bool} \mid \mathtt{not}\,(r =\!\!= s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c'_1 \,]$,
  - $C^{\mathsf{c}}_{\mathtt{n2}}[\, c_{21} \,] \;=\; C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, \mathsf{let}\, z = \mathsf{true}; c'_2 \,]$,
  - $s \;\in\; \gamma$,
  - $\Sigma; \gamma, r \vdash C^{\mathsf{c}\prime}_{\mathtt{n1}} \sim C^{\mathsf{c}\prime}_{\mathtt{n2}} \;:\; \{A''_1\} y{:}T'' \{A''_3\}^{\varrho'_1 \uplus \{r\}} \Rightarrow \{A_1\} y{:}T' \{A_3\}^{\varrho_1 \uplus \{r\}}$,
  - $\mu; \Sigma; \gamma, r; z{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(r =\!\!= s)\} \vdash c'_1 \sim c'_2 \;:\; \{A''_1\} y{:}T'' \{A''_3\}^{\varrho'_1 \uplus \{r\}}$, and
  - $\Sigma; \gamma, r; \emptyset \vdash \{A''_1\} y{:}T'' \{A''_3\}^{\varrho'_1 \uplus \{r\}}$.

  Since $\emptyset; \Sigma; \gamma, r; y{:}T' \vdash c'_{12} \sim c'_{22} \;:\; \{A_3\} x{:}T \{A_2\}^{\varrho_2}$ by Lemma 101 (4), we have

  $$\Sigma; \gamma, r \vdash y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n1}}; c'_{12} \sim y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n2}}; c'_{22} \;:\; \{A''_1\} y{:}T'' \{A''_3\}^{\varrho'_1 \uplus \{r\}} \Rightarrow \{A_1\} x{:}T \{A_2\}^{\varrho_1 \cup \varrho_2 \uplus \{r\}}$$

  by (AECc_CBind). Thus, by (AEC_RegionNEq2), we finish.

□

Lemma 136. *If* $\mu; \Sigma; \gamma; \emptyset \vdash C^{\mathsf{c}}_{\mathtt{n1}}[\, \nu r.\, c_1 \,] \sim C^{\mathsf{c}}_{\mathtt{n2}}[\, \nu r.\, c_2 \,] \;:\; \{A_1\} x{:}T \{A_2\}^{\varrho}$, *then* $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, C^{\mathsf{c}}_{\mathtt{n1}}[\, c_1 \,] \sim \nu r.\, C^{\mathsf{c}}_{\mathtt{n2}}[\, c_2 \,] \;:\; \{A_1\} x{:}T \{A_2\}^{\varrho}$.

Proof. By strong induction on the length of derivation of $\mu; \Sigma; \gamma; \emptyset \vdash C^{\mathsf{c}}_{\mathtt{n1}}[\, \nu r.\, c_1 \,] \sim C^{\mathsf{c}}_{\mathtt{n2}}[\, \nu r.\, c_2 \,] \;:\; \{A_1\} x{:}T \{A_2\}^{\varrho}$ with case analysis on the rule applied last to the derivation. Note that $\Sigma; \gamma; \emptyset \vdash \{A_1\} x{:}T \{A_2\}^{\varrho}$ from well typedness of the left-hand side—it is needed to apply (AEC_RegionNEq2).

Case (AEC_Bind): We are given

$$\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, \nu r.\, c_1 \,]; c'_{12} \sim y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, \nu r.\, c_2 \,]; c'_{22} \;:\; \{A_1\} x{:}T \{A_2\}^{\varrho}$$

and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, \nu r.\, c_1 \,] \sim \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, \nu r.\, c_2 \,] \;:\; \{A_1\} y{:}T' \{A_3\}^{\varrho_1}$,
- $\emptyset; \Sigma; \gamma; y{:}T' \vdash c'_{12} \sim c'_{22} \;:\; \{A_3\} x{:}T \{A_2\}^{\varrho_2}$, and
- $\varrho \;=\; \varrho_1 \cup \varrho_2$.

Here, we have $C^{\mathsf{c}}_{\mathtt{n1}} \;=\; y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n1}}; c'_{12}$ and $C^{\mathsf{c}}_{\mathtt{n2}} \;=\; y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n2}}; c'_{22}$. By Lemmas 126 and 56, $\emptyset; \Sigma; \gamma; \emptyset \vdash C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, \nu r.\, c_1 \,] \sim C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, \nu r.\, c_2 \,] \;:\; \{A''_1\} y{:}T'' \{A''_3\}^{\varrho_1}$ $\{A''_1\} y{:}T'' \{A''_3\}^{\varrho_1} \;\equiv\; \{A_1\} y{:}T' \{A_3\}^{\varrho_1}$ for some A''_1, T'', and A''_3; the length of its derivation is smaller than that of $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, \nu r.\, c_1 \,] \sim \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, \nu r.\, c_2 \,] \;:\; \{A_1\} y{:}T' \{A_3\}^{\varrho_1}$. Thus, we can apply the IH: $\emptyset; \Sigma; \gamma; \emptyset \vdash \nu r.\, C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, c_1 \,] \sim \nu r.\, C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, c_2 \,] \;:\; \{A''_1\} y{:}T'' \{A''_3\}^{\varrho_1}$. By (AEC_Conv) and Lemma 107 (1), $\mu; \Sigma; \gamma; \emptyset \vdash \nu r.\, C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, c_1 \,] \sim \nu r.\, C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, c_2 \,] \;:\; \{A_1\} y{:}T' \{A_3\}^{\varrho_1}$. Thus, by Lemma 135, we finish.

Case (AEC_CBind): We are given

$$\mu; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n1}}[\, \nu r.\, c_1 \,]; c'_{12} \sim y \leftarrow \mathsf{do}\, C^{\mathsf{c}\prime}_{\mathtt{n2}}[\, \nu r.\, c_2 \,]; c'_{22} \;:\; \{A_1\} x{:}T \{A_2\}^{\varrho}$$

and, by inversion,

- $\mu;\Sigma;\gamma;\emptyset \vdash C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,\nu r.\, c_1\,] \sim C^{\mathtt{c}\prime}_{\mathtt{n2}}[\,\nu r.\, c_2\,] \,:\, \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$,
- $\emptyset;\Sigma;\gamma;y{:}T' \vdash c'_{12} \sim c'_{22} \,:\, \{A_3\}x{:}T\{A_2\}^{\varrho_2}$, and
- $\varrho \,=\, \varrho_1 \cup \varrho_2$.

Here, we have $C^{\mathtt{c}}_{\mathtt{n1}} \,=\, y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n1}}; c'_{12}$ and $C^{\mathtt{c}}_{\mathtt{n2}} \,=\, y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n2}}; c'_{22}$. By the IH, $\mu;\Sigma;\gamma;\emptyset \vdash \nu r.\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,] \sim \nu r.\, C^{\mathtt{c}\prime}_{\mathtt{n2}}[\,c_2\,] \,:\, \{A_1\}y{:}T'\{A_3\}^{\varrho_1}$. Thus, by Lemma 135, we finish.

Case (AEC_Weak): By the IH and (AEC_Weak).

Case (AEC_Conv): By the IH and (AEC_Conv).

Case (AEC_LetRegion), (AEC_RegionNEq1), and (AEC_RegionNEq2): Obvious since $C^{\mathtt{c}}_{\mathtt{n1}} = C^{\mathtt{c}}_{\mathtt{n2}} = [\,]$.

Case (AEC_Frame): We are given

$$\mu;\Sigma;\gamma;\emptyset \vdash y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,\nu r.\, c_1\,]; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim C^{\mathtt{c}}_{\mathtt{n2}}[\,\nu r.\, c_2\,] \,:\, \{A'_1, A\}x{:}T\{A'_2, A\}^{\varrho}$$

and, by inversion,

- $\mu;\Sigma;\gamma;\emptyset \vdash C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,\nu r.\, c_1\,] \sim C^{\mathtt{c}}_{\mathtt{n2}}[\,\nu r.\, c_2\,] \,:\, \{A'_1\}x{:}T\{A'_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle}$,
- $\langle\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}}\rangle \,\subseteq\, \varrho$,
- $\Sigma;\gamma;\emptyset \vdash^{\langle{\gamma_{\mathtt{r}}}',\emptyset\rangle} A$, and
- $\Sigma;\gamma;\emptyset \vdash {\gamma_{\mathtt{r}}}'\,\mathsf{disj}\,\gamma_{\mathtt{w}}$

for some fresh y. Here, we have $C^{\mathtt{c}}_{\mathtt{n1}} \,=\, y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n1}}; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y$. Without loss of generality, we can suppose that $r \,\notin\, {\gamma_{\mathtt{r}}}'$. By the IH, $\mu;\Sigma;\gamma;\emptyset \vdash \nu r.\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,] \sim \nu r.\, C^{\mathtt{c}}_{\mathtt{n2}}[\,c_2\,] \,:\, \{A'_1\}x{:}T\{A'_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle}$.

Suppose that $\mu;\Sigma;\gamma,r;\emptyset \,\vdash\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,] \,\sim\, C^{\mathtt{c}}_{\mathtt{n2}}[\,c_2\,] \,:\, \{A'_1\}x{:}T\{A'_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle \uplus \{r\}}$. We show that (AEC_Frame) can be applied to derive

$$\mu;\Sigma;\gamma,r;\emptyset \vdash y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,]; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim C^{\mathtt{c}}_{\mathtt{n2}}[\,c_2\,] \,:\, \{A'_1, A\}x{:}T\{A'_2, A\}^{\varrho \uplus \{r\}}.$$

Let σ be a substitution such that $\Sigma;\gamma,r;\emptyset \,\vdash\, \sigma$. Since $\Sigma;\gamma;\emptyset \,\vdash\, \sigma$ by Lemma 99, and $\Sigma;\gamma;\emptyset \,\vdash\, {\gamma_{\mathtt{r}}}'\,\mathsf{disj}\,\gamma_{\mathtt{w}}$, we have $\sigma({\gamma_{\mathtt{r}}}') \cap \sigma(\gamma_{\mathtt{w}}) \,=\, \emptyset$. Since $\Sigma;\gamma;\emptyset \vdash^{\langle{\gamma_{\mathtt{r}}}',\emptyset\rangle} A$, we have ${\gamma_{\mathtt{r}}}' \subseteq \gamma \subseteq \gamma, r$ by Lemma 39 (1). From well typedness of the left-hand side, we have $\gamma_{\mathtt{w}} \subseteq \gamma \subseteq \gamma, r$ by Lemmas 86 (3) and 39 (2). Thus, by definition, $\sigma({\gamma_{\mathtt{r}}}') \,=\, {\gamma_{\mathtt{r}}}'$ and $\sigma(\gamma_{\mathtt{w}}, r) \,=\, \gamma_{\mathtt{w}}, r$. Since $r \,\notin\, {\gamma_{\mathtt{r}}}'$, we have $\sigma({\gamma_{\mathtt{r}}}') \cap \sigma(\gamma_{\mathtt{w}}, r) \,=\, \emptyset$. Since $\langle\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}}\rangle \,\subseteq\, \varrho$, we have $\langle\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}}\rangle \,\uplus\, \{r\} \,\subseteq\, \varrho \,\uplus\, \{r\}$. Thus, (AEC_Frame) can be applied. By (AEC_LetRegion),

$$\mu;\Sigma;\gamma;\emptyset \vdash \nu r.\, (y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,]; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y) \sim \nu r.\, C^{\mathtt{c}}_{\mathtt{n2}}[\,c_2\,] \,:\, \{A'_1, A\}x{:}T\{A'_2, A\}^{\varrho}.$$

Otherwise, by Lemma 134, we are given

- $C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,] \,=\, C^{\mathtt{c}\prime\prime}_{\mathtt{n1}}[\,\mathsf{let}\, z = \langle\{z{:}\mathsf{bool} \mid \mathsf{not}\,(r =\!\!= s)\} \Leftarrow \mathsf{bool}\rangle^{\ell}\, \mathsf{true}; c''_1\,]$,
- $C^{\mathtt{c}}_{\mathtt{n2}}[\,c_2\,] \,=\, C^{\mathtt{c}\prime\prime}_{\mathtt{n2}}[\,\mathsf{let}\, z = \mathsf{true}; c''_2\,]$,
- $s \,\in\, \gamma$,
- $\Sigma;\gamma,r \vdash C^{\mathtt{c}\prime\prime}_{\mathtt{n1}} \sim C^{\mathtt{c}\prime\prime}_{\mathtt{n2}} \,:\, \{A''_1\}x{:}T''\{A''_2\}^{\varrho'' \uplus \{r\}} \Rightarrow \{A'_1\}x{:}T\{A'_2\}^{\langle\gamma_{\mathtt{r}},\gamma_{\mathtt{w}}\rangle \uplus \{r\}}$, and
- $\mu;\Sigma;\gamma,r;z{:}\{z{:}\mathsf{bool} \mid \mathsf{not}\,(r =\!\!= s)\} \vdash c''_1 \sim c''_2 \,:\, \{A''_1\}x{:}T''\{A''_2\}^{\varrho'' \uplus \{r\}}$.

Similarly to the discussion above, we can apply (AECc_Frame) and derive

$$\Sigma;\gamma,r \vdash y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime\prime}_{\mathtt{n1}}; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim C^{\mathtt{c}\prime\prime}_{\mathtt{n2}} \,:\, \{A''_1\}x{:}T''\{A''_2\}^{\varrho'' \uplus \{r\}} \Rightarrow \{A'_1, A\}x{:}T\{A'_2, A\}^{\varrho \uplus \{r\}}.$$

Since $C^{\mathtt{c}}_{\mathtt{n2}}[\,c_2\,] \,=\, C^{\mathtt{c}\prime\prime}_{\mathtt{n2}}[\,\mathsf{let}\, z = \mathsf{true}; c''_2\,]$ and

$$y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,]; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \,=\, y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime\prime}_{\mathtt{n1}}[\,\mathsf{let}\, z = \langle\{z{:}\mathsf{bool} \mid \mathsf{not}\,(r =\!\!= s)\} \Leftarrow \mathsf{bool}\rangle^{\ell}\, \mathsf{true}; c''_1\,]; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y,$$

we have

$$\mu;\Sigma;\gamma;\emptyset \vdash \nu r.\, (y \leftarrow \mathsf{do}\, C^{\mathtt{c}\prime}_{\mathtt{n1}}[\,c_1\,]; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y) \sim \nu r.\, C^{\mathtt{c}}_{\mathtt{n2}}[\,c_2\,] \,:\, \{A'_1, A\}x{:}T\{A'_2, A\}^{\varrho}$$

by (AEC_RegionNEq2).

□

Lemma 137. *Suppose that* $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ *and* $\mu_1 \models A_1$.

(1) If $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \nu r.\, c_2' \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then there exists some c_1' and A_1' such that:

- *$\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid c_1'$ (the computation does not mutate contents in μ_1);*
- *$\mu_1; \Sigma; \gamma; \emptyset \vdash c_1' \sim \nu r.\, c_2' \,:\, \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$;*
- *$\mu_1 \models A_1'$; and*
- *$c_1' = \nu r.\, c_1''$ for some c_1'', or the size of c_1' is less than c_1.*

(2) If $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1' \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $c_2 = \nu r.\, c_2'$ for some c_2'.

Proof. 1. By induction on the derivation of $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \nu r.\, c_2' \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho}$ with case analysis on the rule applied last.

Case (AEC_Weak): By the IH and (AEC_Weak).

Case (AEC_Conv): By the IH, (AEC_Conv), and Lemma 90.

Case (AEC_LetRegion): Obvious.

Case (AEC_ElimAssert): Similarly to the case of (AEC_ElimAssert) in Lemma 132.

Case (AEC_Frame): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1'; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim \nu r.\, c_2' \,:\, \{A_1', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1' \sim \nu r.\, c_2' \,:\, \{A_1'\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
- $\langle {\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $\Sigma; \gamma; \emptyset \vdash^{\langle {\gamma_{\mathtt{r}}}'', \emptyset \rangle} A$, and
- $\Sigma; \gamma; \emptyset \vdash {\gamma_{\mathtt{r}}}'' \;\mathsf{disj}\; {\gamma_{\mathtt{w}}}'$

for some fresh y. By the IH, there exist some c_1'' and A_1'' such that

- $\mu_1 \mid c_1' \longrightarrow^* \mu_1 \mid c_1''$,
- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1'' \sim \nu r.\, c_2' \,:\, \{A_1''\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
- $\mu_1 \models A_1''$, and
- $c_1'' = \nu r.\, c_1'''$ for some c_1''', or the size of c_1'' is less than c_1'.

By (C_Comput), $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid y \leftarrow \mathsf{do}\, c_1''; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y$. If the size of c_1'' is less than c_1', then the size of $y \leftarrow \mathsf{do}\, c_1''; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y$ is less than $y \leftarrow \mathsf{do}\, c_1'; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y$, so we finish by (AEC_Frame). Otherwise, suppose that c_1'' takes the form $\nu r.\, c_1'''$. Then, we have $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid \nu r.\, (y \leftarrow \mathsf{do}\, c_1'''; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y)$ by (C_Region). Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1''' \sim \nu r.\, c_2' \,:\, \{A_1''\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$, we have $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, (\nu r.\, c_1'''); \mathsf{assert}\,(A)^{\ell}; \mathsf{retu}$ $\nu r.\, c_2' \,:\, \{A_1'', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ by (AEC_Frame). By Lemma 136, $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, (y \leftarrow \mathsf{do}\, c_1'''; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y) \sim \nu r.\, c_2' \,:\, \{A_1'', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$. Since $\mu_1 \models A_1''$ and $\mu_1 \models A$ (from $\mu_1 \models A_1', A$), we finish.

2. Straightforward by induction on the derivation of $\mu_1; \Sigma; \gamma; \Gamma \vdash \nu r.\, c_1' \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$

□

Lemma 138. *Suppose that $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and $\mu_1 \models A_1$.*

(1) If $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \nu r.\, c_2' \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then there exists some c_1' and A_1' such that:

- *$\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid \nu r.\, c_1'$ (the computation does not mutate contents in μ_1);*
- *$\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1' \sim \nu r.\, c_2' \,:\, \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$; and*
- *$\mu_1 \models A_1'$.*

(2) If $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1' \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then there exists some c_2' and A_1' such that:

- *$\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid \nu r.\, c_2'$ (the computation does not mutate contents in μ_2);*
- *$\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_1' \sim \nu r.\, c_2' \,:\, \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$; and*
- *$\mu_1 \models A_1'$.*

Proof. The second case is derived immediately from Lemma 137. The first case is shown straightforwardly by induction on the size of c_1 with Lemma 137. □

Lemma 139. *If $\gamma \vdash \mu_1 \sim \mu_2 \,:\, \Sigma^{\gamma'}$ and $\gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \subseteq \gamma'$, then $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$.*

Proof. Obvious. Well formedness of $\mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ is shown by Lemma 70. □

Lemma 140. *If $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}$, then $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ T$.*

Proof. Straightforward by induction on the derivation of $\mu; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}$ with Lemma 127. □

Lemma 141. *Suppose that $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ :\ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and $\mu_1 \models A_1$.*

(1) If $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then there exists some c_1' and A_1' such that

- *$\mu \mid c_1 \longrightarrow^* \mu_1 \mid c_1'$ (the computation does not mutate contents in μ_1),*
- *$\mu_1; \Sigma; \gamma; \emptyset \vdash c_1' \sim \mathsf{return}\, v_2 \ :\ \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,*
- *$\mu_1 \models A_1'$, and*
- *$c_1' \ =\ \mathsf{return}\, v_1$ for some v_1, or the size of c_1' is less than c_1.*

(2) If $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then $c_2 \ =\ \mathsf{return}\, v_2$ for some v_2.

Proof. 1. By induction on the derivation of $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ with case analysis on the rule applied last.

Case (AEC_Return): By inversion and Lemma 127.

Case (AEC_Weak): By the IH and (AEC_Weak).

Case (AEC_Conv): By the IH and (AEC_Conv).

Case (AEC_ElimAssert): Similarly to the case of (AEC_ElimAssert) in Lemma 132.

Case (AEC_Frame): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_1'; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim \mathsf{return}\, v_2 \ :\ \{A_1', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1' \sim \mathsf{return}\, v_2 \ :\ \{A_1'\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
- $\langle {\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}' \rangle \ \subseteq\ \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $\Sigma; \gamma; \emptyset \ \vdash^{\langle {\gamma_{\mathtt{r}}}'', \emptyset \rangle} A$, and
- $\Sigma; \gamma; \emptyset \vdash {\gamma_{\mathtt{r}}}'' \,\mathsf{disj}\, {\gamma_{\mathtt{w}}}'$

for some fresh y. Since $\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \ \subseteq\ \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$ and $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ :\ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $\gamma \vdash \mu_1|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \sim \mu_2|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \ :\ \Sigma^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$ by Lemma 139. Since $\mu_1 \models A_1', A$, we have $\mu_1 \models A_1'$. Thus, we can apply the IH: there exist some c_1'' and A_1'' such that

- $\mu_1 \mid c_1' \longrightarrow^* \mu_1 \mid c_1''$,
- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1'' \sim \mathsf{return}\, v_2 \ :\ \{A_1''\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
- $\mu_1 \models A_1''$, and
- $c_1'' \ =\ \mathsf{return}\, v_1$ for some v_1, or the size of c_1'' is less than c_1'.

By (C_Comput), $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid y \leftarrow \mathsf{do}\, c_1''; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y$. If the size of c_1'' is less than c_1', then the size of $y \leftarrow \mathsf{do}\, c_1''; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y$ is less than $y \leftarrow \mathsf{do}\, c_1'; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y$, so we finish.

In what follows, we suppose that $c_1'' \ =\ \mathsf{return}\, v_1$. Since $\mu_1 \models A_1', A$, we have $\mu_1 \models A$. Thus, $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid \mathsf{return}\, v_1$. Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1''\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$, we have $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ T$ by Lemma 140. By (AEC_Return),

$$\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{[\, v_1/x \,]\, A_2', A\}x{:}T\{A_2', A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1''\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$, we have $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \ :\ \{A_1''\}x{:}T\{A_2'\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$. Since $\mu_1 \models A_1''$, we have $\mu_1 \models [\, v_1/x \,]\, A_2'$ by Lemma 91. Since $\mu_1 \models [\, v_1/x \,]\, A_2', A$, we finish.

2. Straightforward by induction on the derivation of $\mu; \Sigma; \gamma; \Gamma \vdash \mathsf{return}\, v_1 \sim c_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}$ with Lemma 127 in the case of (AEC_Return). □

Lemma 142. *Suppose that $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ :\ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ and $\mu_1 \models A_1$.*

(1) If $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, then there exists some v_1 and A_1' such that

- *$\mu \mid c_1 \longrightarrow^* \mu_1 \mid \mathsf{return}\, v_1$ (the computation does not mutate contents in μ_1),*
- *$\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$, and*

- $\mu_1 \models A'_1$.

(2) If $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$*, then there exists some* v_2 *and* A'_1 *such that*

- $\mu_2 \mid c_2 \longrightarrow^{*} \mu_2 \mid \mathsf{return}\, v_2$ *(the computation does not mutate contents in* μ_2*),*
- $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \;:\; \{A'_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$*, and*
- $\mu_1 \models A'_1$.

Proof. The second case is derived immediately from Lemma 137. The first case is shown straightforwardly by induction on the size of c_1 with Lemma 141. □

Lemma 143. *If*

- $\gamma \vdash \mu_1 \sim \mu_2 \;:\; \Sigma^{\gamma''}$,
- $\gamma, \gamma' \vdash \mu'_1 \sim \mu'_2 \;:\; (\Sigma, \Sigma')^{\gamma'}$,
- $\mathit{dom}\,(\mu'_1) \;=\; \mathit{dom}\,(\Sigma')$*, and*
- $\mathit{dom}\,(\Sigma\,|_{\gamma'}) \;=\; \emptyset$,

then $\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma''} \sim (\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma''} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$.

Proof. Since $\gamma \vdash \mu_1 \sim \mu_2 \;:\; \Sigma^{\gamma''}$ and $\gamma, \gamma' \vdash \mu'_1 \sim \mu'_2 \;:\; (\Sigma, \Sigma')^{\gamma'}$, we have $\mathit{dom}\,(\mu_1) \;=\; \mathit{dom}\,(\mu_2)$ and $\mathit{dom}\,(\mu'_1) \;=\; \mathit{dom}\,(\mu'_2)$. Thus,

$$\mathit{dom}\,((\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma''}) \;=\; \mathit{dom}\,((\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma''}).$$

Since μ_1 and μ'_1 are well formed, we have $\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma''} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$. Thus,

$$\mathit{dom}\,((\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma''}) \;=\; \mathit{dom}\,((\Sigma, \Sigma')\,|_{\gamma' \cup \gamma''}).$$

Since $\gamma \vdash \mu_1 \sim \mu_2 \;:\; \Sigma^{\gamma''}$, for any $a@r \;\in\; \mathit{dom}\,(\mu_1)$, $\Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \mu_1(a@r) \sim \mu_2(a@r) \;:\; \Sigma(a@r)$ by Lemmas 101 (3) and 104 (3). Since $\gamma, \gamma' \vdash \mu'_1 \sim \mu'_2 \;:\; (\Sigma, \Sigma')^{\gamma'}$, for any $a@r \;\in\; \mathit{dom}\,(\mu'_1)$, $\Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \mu'_1(a@r) \sim \mu'_2(a@r) \;:\; (\Sigma, \Sigma')(a@r)$. Thus, by (AES), we have

$$\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma''} \sim (\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma''} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma''}.$$

□

Lemma 144. *If* $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ *and* $\mu_1; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle \sim \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle \;:\; T^{\gamma_{\mathtt{r}}}$*, then* $\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \sim (\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma_{\mathtt{r}}}$ *(where* Σ' *is the store typing context used to type* $\nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle$*).*

Proof. Without loss of generality, we can suppose that $\mathit{dom}\,(\Sigma\,|_{\gamma'}) \;=\; \emptyset$ and $\mathit{dom}\,(\mu_1\,|_{\gamma'}) \;=\; \emptyset$ and $\mathit{dom}\,(\mu_2\,|_{\gamma'}) \;=\; \emptyset$. Since $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}}} \;:\; \Sigma^{\gamma_{\mathtt{r}}}$. Since $\mu_1; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle \sim \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle \;:\; T^{\gamma_{\mathtt{r}}}$, there exist some Σ' such that $\gamma, \gamma' \vdash \mu'_1 \sim \mu'_2 \;:\; (\Sigma, \Sigma')^{\gamma'}$. From well typedness of $\nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle$, $\mathit{dom}\,(\mu'_1) \;=\; \mathit{dom}\,(\Sigma')$. Thus, by Lemma 143,

$$\gamma, \gamma' \vdash ((\mu_1\,|_{\gamma_{\mathtt{r}}}) \uplus \mu'_1)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \sim ((\mu_2\,|_{\gamma_{\mathtt{r}}}) \uplus \mu'_2)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma_{\mathtt{r}}}.$$

Since $\mu_1\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;=\; \mu_1\,|_{\gamma_{\mathtt{r}}}$ and $\mu_2\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;=\; \mu_2\,|_{\gamma_{\mathtt{r}}}$ from $\mathit{dom}\,(\mu_1\,|_{\gamma'}) \;=\; \emptyset$ and $\mathit{dom}\,(\mu_2\,|_{\gamma'}) \;=\; \emptyset$, respectively, we have

$$\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \sim (\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma_{\mathtt{r}}}.$$

□

Lemma 145. *If* $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ *and* $\gamma \vdash \mu'_1\,|_{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'} \sim \mu'_2\,|_{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'} \;:\; (\Sigma, \Sigma')^{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'}$ *and* $\langle \gamma_{\mathtt{r}}', \gamma_{\mathtt{w}}' \rangle \;\subseteq\; \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$ *and* $\mu_i\,|_{\gamma_{\mathtt{w}}'^{c}} \;=\; \mu'_i\,|_{\gamma_{\mathtt{w}}'^{c}}$ *for* $i \in \{1, 2\}$ *and* $\mathit{dom}\,(\Sigma') \;=\; \mathit{dom}\,(\Sigma'\,|_{\gamma_{\mathtt{w}}'})$ *then* $\gamma \vdash \mu'_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu'_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$.

Proof. By definition, it suffices to show the followings.

- We show $\mathit{dom}\,(\mu'_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}) \;=\; \mathit{dom}\,(\mu'_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. Let $a@r \;\in\; \mathit{dom}\,(\mu'_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. If $r \;\in\; \gamma_{\mathtt{w}}'$, then $a@r \;\in\; \mathit{dom}\,(\mu'_1\,|_{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'})$. Since $\gamma \vdash \mu'_1\,|_{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'} \sim \mu'_2\,|_{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'} \;:\; (\Sigma, \Sigma')^{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'}$, we have $a@r \;\in\; \mathit{dom}\,(\mu'_2\,|_{\gamma_{\mathtt{r}}' \cup \gamma_{\mathtt{w}}'}) \subseteq \mathit{dom}\,(\mu'_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. Otherwise, if $r \;\notin\; \gamma_{\mathtt{w}}'$, then $a@r \;\in\; \mathit{dom}\,(\mu_1\,|_{\gamma_{\mathtt{w}}'^{c}})$ since $\mu_1\,|_{\gamma_{\mathtt{w}}'^{c}} \;=\; \mu'_1\,|_{\gamma_{\mathtt{w}}'^{c}}$. Since $r \;\in\; \gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}$ and $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $a@r \;\in\; \mathit{dom}\,(\mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}) \subseteq \mathit{dom}\,(\mu_2\,|_{\gamma_{\mathtt{w}}'^{c}}) = \mathit{dom}\,(\mu'_2\,|_{\gamma_{\mathtt{w}}'^{c}})$. Since $r \;\in\; \gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}$, we have $\mathit{dom}\,(\mu'_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}})$. The converse is shown similarly.

- We show $dom\,(\mu_1'\,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}) \,=\, dom\,((\Sigma, \Sigma')\,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$. Let $a@r \,\in\, dom\,(\mu_1'\,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$. If $r \,\in\, {\gamma_\mathtt{w}}'$, then $a@r \,\in\, dom\,(\mu_1'\,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'})$. Since $\gamma \vdash \mu_1' \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'} \sim \mu_2' \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'} \,:\, (\Sigma, \Sigma')^{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'}$, we have $a@r \,\in\, dom\,((\Sigma, \Sigma') \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'}) \subseteq dom\,((\Sigma, \Sigma') \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$. Conversely, let $a@r \,\in\, dom\,((\Sigma, \Sigma') \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$. If $r \,\in\, {\gamma_\mathtt{w}}'$, then, since $\gamma \vdash \mu_1' \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'} \sim \mu_2' \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'} \,:\, (\Sigma, \Sigma')^{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'}$, we have $a@r \,\in\, dom\,(\mu_1' \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'}) \subseteq dom\,(\mu_1' \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$. Otherwise, suppose that $r \,\notin\, {\gamma_\mathtt{w}}'$. If $a@r \,\in\, dom\,(\Sigma \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$, then, since $\gamma \vdash \mu_1 \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \sim \mu_2 \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \,:\, \Sigma^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}$, we have $a@r \,\in\, dom\,(\mu_1 \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$. Since $\mu_1 \,|_{{\gamma_\mathtt{w}}'^c} \,=\, \mu_1' \,|_{{\gamma_\mathtt{w}}'^c}$, we have $a@r \in dom\,(\mu_1'\,|_{{\gamma_\mathtt{w}}'^c})$. Since $r \,\in\, \gamma_\mathtt{r} \cup \gamma_\mathtt{w}$, we have $a@r \in dom\,(\mu_1'\,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$. Otherwise, if $a@r \in dom\,(\Sigma'\,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$, then contradictory since $a@r \,\in\, dom\,(\Sigma'\,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}) \subseteq dom\,(\Sigma') = dom\,(\Sigma'\,|_{{\gamma_\mathtt{w}}'})$ but $r \,\notin\, {\gamma_\mathtt{w}}'$.

- We show that, for any $a@r \,\in\, dom\,(\mu_1' \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}})$, $\Sigma, \Sigma'; \gamma; \emptyset \vdash \mu_1'(a@r) \sim \mu_2'(a@r) \,:\, (\Sigma, \Sigma')(a@r)$. If $r \,\in\, {\gamma_\mathtt{w}}'$, then, since $\gamma \vdash \mu_1' \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'} \sim \mu_2' \,|_{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'} \,:\, (\Sigma, \Sigma')^{{\gamma_\mathtt{r}}' \cup {\gamma_\mathtt{w}}'}$, we finish. Otherwise, suppose that $r \,\notin\, {\gamma_\mathtt{w}}'$. For $i \in \{1, 2\}$, since $\mu_i \,|_{{\gamma_\mathtt{w}}'^c} \,=\, \mu_i' \,|_{{\gamma_\mathtt{w}}'^c}$, $\mu_i'(a@r) \,=\, \mu_i(a@r)$. Since $r \,\in\, \gamma_\mathtt{r} \cup \gamma_\mathtt{w}$ and $\gamma \vdash \mu_1 \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \sim \mu_2 \,|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \,:\, \Sigma^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}$, we finish by Lemma 104 (3).

□

Lemma 146. *(1) If $\gamma \subseteq \gamma'$ and $\mu|_{\gamma'} \,=\, \mu'|_{\gamma'}$, then $\mu|_{\gamma} \,=\, \mu'|_{\gamma}$.*

(2) If $\gamma \subseteq \gamma'$ and $\mu|_{\gamma^c} \,=\, \mu'|_{\gamma^c}$, then $\mu|_{\gamma'^c} \,=\, \mu'|_{\gamma'^c}$.

Proof. We show the first case—the second case is shown by the first case since $\gamma \,\subseteq\, \gamma'$ implies ${\gamma'}^c \,\subseteq\, \gamma^c$. Suppose that $dom\,(\mu|_\gamma) \,\subseteq\, dom\,(\mu|_{\gamma'})$ and $dom\,(\mu'|_\gamma) \,\subseteq\, dom\,(\mu'|_{\gamma'})$. Then, $\mu|_\gamma \,=\, \mu'|_\gamma$ because

$$\begin{array}{rll} (\mu|_\gamma)(a@r) \,=\, v & \text{iff} & (\mu|_{\gamma'})(a@r) \,=\, v \text{ and } r \,\in\, \gamma \\ & \text{iff} & (\mu'|_{\gamma'})(a@r) \,=\, vtextandr \,\in\, \gamma \quad (\text{since } \mu|_{\gamma'} \,=\, \mu'|_{\gamma'}) \\ & \text{iff} & (\mu'|_\gamma)(a@r) \,=\, v. \end{array}$$

Thus, it suffices to show that, for any μ, γ, and γ', if $\gamma \,\subseteq\, \gamma'$, then $dom\,(\mu|_\gamma) \,\subseteq\, dom\,(\mu|_{\gamma'})$. Let $a@r \,\in\, dom\,(\mu|_\gamma)$. Since $r \,\in\, \gamma \subseteq \gamma'$, we have $a@r \,\in\, dom\,(\mu|_{\gamma'})$. □

Lemma 147. *If $\Sigma; \gamma \vdash C^\mathtt{c}_{\mathtt{n}1} \sim C^\mathtt{c}_{\mathtt{n}2} \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}} \Rightarrow \{A_1'\}y'{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}$ and $\mu; \Sigma; \gamma; \emptyset \vdash c_1 \sim c_2 \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$, then $\mu; \Sigma; \gamma; \emptyset \vdash C^\mathtt{c}_{\mathtt{n}1}\,[\,c_1\,] \sim C^\mathtt{c}_{\mathtt{n}2}\,[\,c_2\,] \,:\, \{A_1'\}y'{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}$*

Proof. By induction on the derivation of $\Sigma; \gamma \vdash C^\mathtt{c}_{\mathtt{n}1} \sim C^\mathtt{c}_{\mathtt{n}2} \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}} \Rightarrow \{A_1'\}y'{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}$.

Case (AECc_Hole): Obvious since we are given $C^\mathtt{c}_{\mathtt{n}1} \,=\, [\,]$ and $C^\mathtt{c}_{\mathtt{n}2} \,=\, [\,]$ and $\{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}} \,=\, \{A_1'\}y{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}$.

Case (AECc_CBind): We are given $\Sigma; \gamma \vdash z' \leftarrow \mathsf{do}\ C^{\mathtt{c}\prime}_{\mathtt{n}1}; c_1' \sim z' \leftarrow \mathsf{do}\ C^{\mathtt{c}\prime}_{\mathtt{n}2}; c_2' \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}} \Rightarrow \{A_1'\}y'{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}$ and, by inversion,

- $\Sigma; \gamma \vdash C^{\mathtt{c}\prime}_{\mathtt{n}1} \sim C^{\mathtt{c}\prime}_{\mathtt{n}2} \,:\, \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}} \Rightarrow \{A_1'\}z'{:}T_1'\{A_3\}^{\varrho_1}$,
- $\emptyset; \Sigma; \gamma; z'{:}T_1' \vdash c_1' \sim c_2' \,:\, \{A_3\}y'{:}T'\{A_2'\}^{\varrho_2}$, and
- $\varrho' \,\uplus\, \{r\} \,=\, \varrho_1 \cup \varrho_2$.

By the IH,

$$\mu; \Sigma; \gamma; \emptyset \vdash C^{\mathtt{c}\prime}_{\mathtt{n}1}\,[\,c_1\,] \sim C^{\mathtt{c}\prime}_{\mathtt{n}2}\,[\,c_2\,] \,:\, \{A_1'\}z'{:}T_1'\{A_3\}^{\varrho_1}.$$

Thus, by (AEC_CBind),

$$\mu; \Sigma; \gamma; \emptyset \vdash z' \leftarrow \mathsf{do}\ C^{\mathtt{c}\prime}_{\mathtt{n}1}\,[\,c_1\,]; c_1' \sim z' \leftarrow \mathsf{do}\ C^{\mathtt{c}\prime}_{\mathtt{n}2}\,[\,c_2\,]; c_2' \,:\, \{A_1'\}y'{:}T'\{A_2'\}^{\varrho' \uplus \{r\}}.$$

Case (AECc_Weak): By the IH and (AEC_Weak).

Case (AECc_Conv): By the IH and (AEC_Conv).

Case (AECc_Frame): By the IH and (AEC_Frame).

□

Lemma 148. *If $\mu \mid c \longrightarrow \mu' \mid c'$, then $\mu \mid C^\mathtt{c}_\mathtt{n}\,[\,c\,] \longrightarrow \mu' \mid C^\mathtt{c}_\mathtt{n}\,[\,c'\,]$.*

Proof. Straightforward by structural induction on $C^\mathtt{c}_\mathtt{n}$ with (C_Comput). □

Lemma 149.

(1) If $\Sigma; \gamma; \emptyset \vdash e_1 \sim e_2 \,:\, T$ and $e_1 \longrightarrow e_1''$, then there exist some e_1' and e_2' such that

- $e_1'' \longrightarrow^* e_1'$,
- $e_2 \longrightarrow^* e_2'$, *and*
- $\Sigma; \gamma; \emptyset \vdash e_1' \sim e_2' : T$.

(2) If

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim c_2 : \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$,
- $\mu_1 \models A_1$, *and*
- $\mu_1 \mid c_1 \longrightarrow \mu_1'' \mid c_1''$,

then there exist some Σ', A_1', μ_1', c_1', μ_2', *and* c_2' *such that:*

- $\mu_1'' \mid c_1'' \longrightarrow^* \mu_1' \mid c_1'$;
- $\mu_2 \mid c_2 \longrightarrow^* \mu_2' \mid c_2'$;
- $\mu_1'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c_1' \sim c_2' : \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$;
- $\gamma \vdash \mu_1'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2'|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} : (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$;
- $\mu_1' \models A_1'$;
- $dom\,(\Sigma') = dom\,(\Sigma'|_{\gamma_{\mathtt{w}}})$;
- $\mu_i|_{\gamma_{\mathtt{w}}{}^c} = \mu_i'|_{\gamma_{\mathtt{w}}{}^c}$ *for* $i \in \{1, 2\}$;
- *contents of* μ_1'' *and* μ_2 *are mutated only if their addresses are associated with regions in* $\gamma_{\mathtt{w}}$.

(3) If

- $\mu_1; \Sigma; \gamma \vdash p_1 \sim p_2 : T^{\gamma'}$,
- $\gamma \vdash \mu_1|_{\gamma'} \sim \mu_2|_{\gamma'} : \Sigma^{\gamma'}$, *and*
- $\mu_1 \mid p_1 \hookrightarrow p_1''$,

then there exist some p_1' *and* p_2' *such that*

- $\mu_1 \mid p_1'' \hookrightarrow^* p_1'$,
- $\mu_2 \mid p_2 \hookrightarrow^* p_2'$, *and*
- $\mu_1; \Sigma; \gamma \vdash p_1' \sim p_2' : T^{\gamma'}$.

Proof. By strong induction on the length of the derivation of each judgment.

1. Since $e_1 \longrightarrow e_1''$, there exist some E_1, e_1', and e_1''' such that $e_1 = E_1[e_1']$ and $e_1' = E_1[e_1''']$ and $e_1' \rightsquigarrow e_1'''$. By case analysis on the typing rule applied last.

Case (AETm_Var), (AETm_Const), (AETm_Abs), (AETm_Cast), (AETm_Address), (AETm_Do), (AETm_RAbs), (AETm_Blame), (AETm_Guard), (AETm_Exact), and (AETm_Forget): Contradictory.

Case (AETm_Op): We are given $\Sigma; \gamma; \emptyset \vdash op(e_{11}, \ldots, e_{1n}) \sim op(e_{21}, \ldots, e_{2n}) : [\, e_{11}/x_1, \ldots, e_{1n}/x \,]\, T'$ and, by inversion, $ty\,(op) = x_1{:}T_1 \rightarrow \ldots \rightarrow x_n{:}T_n \rightarrow T'$ and, for any i, $\Sigma; \gamma; \emptyset \vdash e_{1i} \sim e_{2i} : [\, e_{11}/x_1, \ldots, e_{1i-1}/x_{i-1} \,]\, T_i$. Since $E_1[e_1'] = e_1 = op(e_{11}, \ldots, e_{1n})$, there are two cases we have to consider by case analysis on E_1.

Case $E_1 = [\,]$: Since the only reduction rule applicable to $op(e_{11}, \ldots, e_{1n})$ is (R_Op). Thus, $e_1''' = [\![op]\!](e_{11}, \ldots, e_{1n})$. By the assumption of op, $e_{1i} = k_i$ for any i. Thus, $e_{2i} = k_i$ for any i by Lemma 120, and so we finish by (AETm_Const) (since $[\![op]\!](k_1, \ldots, k_n)$ is a constant).

Case $E_1 = op(e_{11}, \ldots, e_{1i-1}, E_1', e_{1i+1}, \ldots, e_{1n})$ where e_{1j} is a value for any $j < i$: By the IH, there exist some e_{1i}' and e_{2i}' such that

* $E_1'[e_1'''] \longrightarrow^* e_{1i}'$,
* $e_{2i} \longrightarrow^* e_{2i}'$,
* $\Sigma; \gamma; \emptyset \vdash e_{1i}' \sim e_{2i}' : [\, e_{11}/x_1, \ldots, e_{1i-1}/x_{i-1} \,]\, T_i$.

Since, for any $j > i$, $\Sigma; \gamma; \emptyset \vdash e_{1j} \sim e_{2j} : [\, e_{11}/x_1, \ldots, e_{1i-1}/x_{i-1}, e_{1i}'/x_i, e_{1i+1}/x_{i+1}, \ldots, e_{1j-1}/x_{j-1} \,]\, T_j$ by (AETm_Conv), we finish by (AETm_Op), (AETm_Conv), and Lemma 31.

Case (AETm_App): We are given $\Sigma;\gamma;\emptyset \vdash e_{11}\, e_{12} \sim e_{21}\, e_{22} \ :\ [\, e_{12}/x\,]\, T_2$ and, by inversion, $\Sigma;\gamma;\emptyset \vdash e_{11} \sim e_{21} \ :\ x{:}T_1 \rightarrow T_2$ and $\Sigma;\gamma;\emptyset \vdash e_{12} \sim e_{22} \ :\ T_1$. Since $E_1[e'_1] = e_1 = e_{11}\, e_{12}$, there are three cases we have to consider by case analysis on E_1.

Case $E_1 = [\,]$: By case analysis on the reduction rule applied to $e_{11}\, e_{12}$. Note that e_{11} and e_{12} are values in the following, and so is e_{22} by Lemma 127.

Case (R_Beta): We are given $(\lambda x{:}T'_{11}.e'_{11})\, e_{12} \longrightarrow [\, e_{12}/x\,]\, e'_{11}$. By Lemmas 121 and 53, there exist some T'_{21}, e'_{21}, and T'_{12} such that

- $e_{21} = \lambda x{:}T'_{21}.e'_{21}$,
- $\Sigma;\gamma;x{:}T'_{11} \vdash e'_{11} \sim e'_{21} \ :\ T'_{12}$,
- $\Sigma;\gamma;\emptyset \vdash T'_{11} \sim T'_{21}$,
- $T'_{11} \equiv T_1$, and
- $T'_{12} \equiv T_2$.

Thus, $e_{21}\, e_{22} \longrightarrow [\, e_{22}/x\,]\, e'_{21}$ by (R_Beta). Since $\Sigma;\gamma;\emptyset \vdash e_{12} \sim e_{22} \ :\ T_1$, we have $\Sigma;\gamma;\emptyset \vdash e_{12} \sim e_{22} \ :\ T'_{11}$ by (AETm_Conv). Thus, by Lemma 110, $\Sigma;\gamma;\emptyset \vdash [\, e_{12}/x\,]\, e'_{11} \sim [\, e_{22}/x\,]\, e'_{21} \ :\ [\, e_{12}/x\,]\, T'_{12}$ (note that both e_{12} and e_{22} are values). Since $[\, e_{12}/x\,]\, T'_{12} \equiv [\, e_{12}/x\,]\, T_2$ by Lemma 74, we finish by (AETm_Conv).

Case (R_Base): We are given $\langle B \Leftarrow B\rangle^{\ell}\, e_{12} \longrightarrow e_{12}$. By Lemmas 122, 114, 53 and 52, $e_{21} = \langle B \Leftarrow B\rangle^{\ell}$ and $T_1 = T_2 = B$. Since $e_{21}\, e_{22} \longrightarrow e_{22}$ by (R_Beta), we finish.

Case (R_Fun): We are given

$$\begin{array}{l}\langle y{:}T_{111} \rightarrow T_{112} \Leftarrow y{:}T_{121} \rightarrow T_{122}\rangle^{\ell}\, e_{12} \\ \qquad \longrightarrow \lambda y{:}T_{111}.\mathsf{let}\, z = \langle T_{121} \Leftarrow T_{111}\rangle^{\ell}\, y\, \mathsf{in}\, \langle T_{112} \Leftarrow [\, z/y\,]\, T_{122}\rangle^{\ell}\, (e_{12}\, z)\end{array}$$

By Lemmas 122 and 115,

- $e_{21} = \langle y{:}T_{211} \rightarrow T_{212} \Leftarrow y{:}T_{221} \rightarrow T_{222}\rangle^{\ell}$,
- $\Sigma;\gamma;\emptyset \vdash T_{111} \sim T_{211}$ and $\Sigma;\gamma;y{:}T_{111} \vdash T_{112} \sim T_{212}$,
- $\Sigma;\gamma;\emptyset \vdash T_{121} \sim T_{221}$ and $\Sigma;\gamma;y{:}T_{121} \vdash T_{122} \sim T_{222}$, and
- $x{:}T_1 \rightarrow T_2 \equiv (y{:}T_{121} \rightarrow T_{122}) \rightarrow (y{:}T_{111} \rightarrow T_{112})$

for some T_{211}, T_{212}, T_{221}, and T_{222}. By (R_Fun),

$$e_{21}\, e_{22} \longrightarrow \lambda y{:}T_{211}.\mathsf{let}\, z = \langle T_{221} \Leftarrow T_{211}\rangle^{\ell}\, y\, \mathsf{in}\, \langle T_{212} \Leftarrow [\, z/y\,]\, T_{222}\rangle^{\ell}\, (e_{22}\, z).$$

Let v_1 and v_2 be the right-hand sides of reductions of $e_{11}\, e_{12}$ and $e_{21}\, e_{22}$, respectively. By Lemmas 53 and 74 and (AETm_Conv), it suffices to show that

$$\Sigma;\gamma;\emptyset \vdash v_1 \sim v_2 \ :\ y{:}T_{111} \rightarrow T_{112},$$

which is derived easily, using Lemmas 103 (1) and 110 to derive $\Sigma;\gamma;z{:}T_{121} \vdash [\, z/y\,]\, T_{122} \sim [\, z/y\,]\, T_{222}$.

Case (R_Forget): We are given $\langle T_{11} \Leftarrow \{y{:}T_{12} \mid c_{12}\}\rangle^{\ell}\, e_{12} \longrightarrow \langle T_{11} \Leftarrow T_{12}\rangle^{\ell}\, e_{12}$. By Lemmas 122 and 117,

- $e_{21} = \langle T_{21} \Leftarrow \{y{:}T_{22} \mid c_{22}\}\rangle^{\ell}$,
- $\Sigma;\gamma;\emptyset \vdash T_{11} \sim T_{21}$,
- $\Sigma;\gamma;\emptyset \vdash T_{12} \sim T_{22}$, and
- $x{:}T_1 \rightarrow T_2 \equiv \{y{:}T_{12} \mid c_{12}\} \rightarrow T_{11}$

for some T_{21}, T_{22}, and c_{22}. By (R_Forget), $e_{21}\, e_{22} \longrightarrow \langle T_{21} \Leftarrow T_{22}\rangle^{\ell}\, e_{22}$. By Lemmas 53 and 74 and (AETm_Conv), it suffices to show that

$$\Sigma;\gamma;\emptyset \vdash \langle T_{11} \Leftarrow T_{12}\rangle^{\ell}\, e_{12} \sim \langle T_{21} \Leftarrow T_{22}\rangle^{\ell}\, e_{22} \ :\ T_{11},$$

which is derived by (AETm_Cast) and (AETm_App).

Case (R_PreCheck): We are given $\langle \{y{:}T_{11} \mid c_{11}\} \Leftarrow T_{12}\rangle^{\ell}\, e_{12} \longrightarrow \langle\!\langle \{y{:}T_{11} \mid c_{11}\}, \langle T_{11} \Leftarrow T_{12}\rangle^{\ell}\, e_{12} \rangle\!\rangle^{\ell}$ where T_{12} is not a refinement type. By Lemmas 122 and 117,

- $e_{21} = \langle \{y{:}T_{21} \mid c_{21}\} \Leftarrow T_{22}\rangle^{\ell}$,
- $\Sigma;\gamma;\emptyset \vdash \{y{:}T_{11} \mid c_{11}\} \sim \{y{:}T_{21} \mid c_{21}\}$,
- $\Sigma;\gamma;\emptyset \vdash T_{11} \sim T_{21}$,
- $\Sigma;\gamma;\emptyset \vdash T_{12} \sim T_{22}$,
- $x{:}T_1 \rightarrow T_2 \equiv T_{12} \rightarrow \{y{:}T_{11} \mid c_{11}\}$, and
- T_{22} is not a refinement type

for some T_{21}, T_{22}, and c_{21}. By (R_PreCheck), $e_{21}\,e_{22} \longrightarrow \langle\!\langle\, \{y{:}T_{21} \mid c_{21}\}, \langle T_{21} \Leftarrow T_{22}\rangle^{\ell}\, e_{22}\,\rangle\!\rangle^{\ell}$. By Lemmas 53 and 74 and (AETm_Conv), it suffices to show that

$$\Sigma;\gamma;\Gamma \vdash \langle\!\langle\, \{y{:}T_{11} \mid c_{11}\}, \langle T_{11} \Leftarrow T_{12}\rangle^{\ell}\, e_{12}\,\rangle\!\rangle^{\ell} \sim \langle\!\langle\, \{y{:}T_{21} \mid c_{21}\}, \langle T_{21} \Leftarrow T_{22}\rangle^{\ell}\, e_{22}\,\rangle\!\rangle^{\ell} \;:\; \{y{:}T_{11} \mid c_{11}\},$$

which is derived by (AETm_Cast), (AETm_App), and (AETm_WCheck).

Case (R_Ref): We are given $\langle \mathsf{Ref}_r\, T_{11} \Leftarrow \mathsf{Ref}_r\, T_{12}\rangle^{\ell}\, e_{12} \longrightarrow T_{11} \Leftarrow^{\ell} T_{12} : e_{12}$. By Lemmas 122 and 116,

- $e_{21} \;=\; \langle \mathsf{Ref}_r\, T_{21} \Leftarrow \mathsf{Ref}_r\, T_{22}\rangle^{\ell}$,
- $\Sigma;\gamma;\emptyset \vdash T_{11} \sim T_{21}$,
- $\Sigma;\gamma;\emptyset \vdash T_{12} \sim T_{22}$, and
- $x{:}T_1 \rightarrow T_2 \;\equiv\; \mathsf{Ref}_r\, T_{12} \rightarrow \mathsf{Ref}_r\, T_{11}$

for some T_{21} and T_{22}. By (R_Ref), $e_{21}\,e_{22} \longrightarrow T_{21} \Leftarrow^{\ell} T_{22} : e_{22}$. By Lemmas 53 and 74, (AETm_Conv), it suffices to show that

$$\Sigma;\gamma;\emptyset \vdash T_{11} \Leftarrow^{\ell} T_{12} : e_{12} \sim T_{21} \Leftarrow^{\ell} T_{22} : e_{22} \;:\; \mathsf{Ref}_r\, T_{11},$$

which is derived by (AETm_Guard) since $\Sigma;\gamma;\emptyset \vdash e_{12} \sim e_{22} \;:\; \mathsf{Ref}_r\, T_{12}$ by Lemma 53 (AETm_Conv).

Case (R_RefFail): We are given $\langle \mathsf{Ref}_r\, T_{11} \Leftarrow \mathsf{Ref}_s\, T_{12}\rangle^{\ell}\, e_{12} \longrightarrow \Uparrow\ell$. By inversion of (R_RefFail), $r \neq s$. By Lemmas 122 and 116, $e_{21} \;=\; \langle \mathsf{Ref}_r\, T_{21} \Leftarrow \mathsf{Ref}_s\, T_{22}\rangle^{\ell}$ for some T_{21} and T_{22}. By (R_RefFail), $e_{21} \longrightarrow \Uparrow\ell$. Thus, we finish by (AEC_Blame).

Case (R_RFun): We are given $\langle \forall r.\, T_{11} \Leftarrow \forall r.\, T_{12}\rangle^{\ell}\, e_{12} \longrightarrow \lambda r.\langle T_{11} \Leftarrow T_{12}\rangle^{\ell}\, (e_{12}\{r\})$. By Lemmas 122 and 119,

- $e_{21} \;=\; \langle \forall r.\, T_{21} \Leftarrow \forall r.\, T_{22}\rangle^{\ell}$,
- $\Sigma;\gamma;r \vdash T_{11} \sim T_{21}$,
- $\Sigma;\gamma;r \vdash T_{12} \sim T_{22}$, and
- $x{:}T_1 \rightarrow T_2 \;\equiv\; \forall r.\, T_{12} \rightarrow \forall r.\, T_{11}$

for some T_{21} and T_{22}. By (R_RFun), $e_{21}\,e_{22} \longrightarrow \lambda r.\langle T_{21} \Leftarrow T_{22}\rangle^{\ell}\, (e_{22}\{r\})$. By Lemmas 53 and 74 and (AETm_Conv), it suffices to show that

$$\Sigma;\gamma;\Gamma \vdash \lambda r.\langle T_{11} \Leftarrow T_{12}\rangle^{\ell}\, (e_{12}\{r\}) \sim \lambda r.\langle T_{21} \Leftarrow T_{22}\rangle^{\ell}\, (e_{22}\{r\}) \;:\; \forall r.\, T_{11},$$

which is derived by (AETm_RApp), (AETm_Cast), and (AETm_RAbs) since $\Sigma;\gamma;r \vdash e_{12} \sim e_{22} \;:\; \forall r.\, T_{12}$ by Lemmas 102 (3) and 53 and (AETm_Conv).

Case (R_Hoare): We are given

$$\begin{aligned}&\langle \{A_{111}\}y{:}T_{11}\{A_{112}\}^{\varrho_1} \Leftarrow \{A_{121}\}y{:}T_{12}\{A_{122}\}^{\varrho_2}\rangle^{\ell}\, e_{12}\\ &\quad\longrightarrow \mathsf{do\,assert}\,(A_{121})^{\ell}; z \leftarrow e_{12}; \mathsf{let}\, y = \langle T_{11} \Leftarrow T_{12}\rangle^{\ell}\, z; \mathsf{assert}\,(A_{112})^{\ell}; \mathsf{return}\, y\end{aligned}$$

for some fresh variable z. By inversion of (R_Hoare), $\varrho_2 \subseteq \varrho_1$. By Lemmas 122 and 118,

- $e_{21} \;=\; \langle \{A_{211}\}y{:}T_{21}\{A_{212}\}^{\varrho_1} \Leftarrow \{A_{221}\}y{:}T_{22}\{A_{222}\}^{\varrho_2}\rangle^{\ell}$,
- $\Sigma;\gamma;\emptyset \vdash T_{11} \sim T_{21}$,
- $\Sigma;\gamma;\emptyset \vdash T_{12} \sim T_{22}$,
- $\Sigma;\gamma;\emptyset \vdash^{\varrho_2} A_{121} \sim A_{221}$,
- $\Sigma;\gamma;y{:}T_{11} \vdash^{\varrho_1} A_{112} \sim A_{212}$, and
- $x{:}T_1 \rightarrow T_2 \;\equiv\; \{A_{121}\}y{:}T_{12}\{A_{122}\}^{\varrho_2} \rightarrow \{A_{111}\}y{:}T_{11}\{A_{112}\}^{\varrho_1}$

for some A_{211}, T_{21}, A_{212}, A_{221}, T_{22}, and A_{222}. By (R_Hoare),

$$e_{21}\,e_{22} \longrightarrow \mathsf{do\,assert}\,(A_{221})^{\ell}; z \leftarrow e_{22}; \mathsf{let}\, y = \langle T_{21} \Leftarrow T_{22}\rangle^{\ell}\, z; \mathsf{assert}\,(A_{212})^{\ell}; \mathsf{return}\, y.$$

Let v_1 and v_2 be the right-hand sides of reductions of $e_{11}\,e_{12}$ and $e_{21}\,e_{22}$, respectively. By Lemmas 53 and 74 and (AETm_Conv), it suffices to show that

$$\Sigma;\gamma;\Gamma \vdash v_1 \sim v_2 \;:\; \{A_{111}\}y{:}T_{11}\{A_{112}\}^{\varrho_1},$$

which is derived easily; note that $\varrho_2 \subseteq \varrho_1$ is needed for (AEC_CBind).

(R_HoareFail): We are given

$$\langle \{A_{111}\}y{:}T_{11}\{A_{112}\}^{\varrho_1} \Leftarrow \{A_{121}\}y{:}T_{12}\{A_{122}\}^{\varrho_2}\rangle^{\ell}\, e_{12} \longrightarrow \Uparrow\ell.$$

By inversion of (R_HoareFail), $\varrho_2 \not\subseteq \varrho_1$. By Lemmas 122 and 118, $e_{21} \;=\; \langle \{A_{211}\}y{:}T_{21}\{A_{212}\}^{\varrho_1} \Leftarrow \{A_{221}\}y{:}T_{22}\{A_{222}\}^{\varrho_2}\rangle^{\ell}$ for some A_{211}, T_{21}, A_{212}, A_{221}, T_{22}, and A_{222}. Thus, by (R_HoareFail), $e_{21} \longrightarrow \Uparrow\ell$. By (AEC_Blame), we finish.

Case $E_1 \,=\, E_1'\, e_{12}$: By the IH, there exist some e_{11}' and e_{21}' such that

- $E_1'[e_1'''] \longrightarrow^* \; e_{11}'$,
- $e_{21} \longrightarrow^* \; e_{21}'$, and
- $\Sigma; \gamma; \emptyset \vdash e_{11}' \sim e_{21}' \;:\; x{:}T_1 \rightarrow T_2$.

By (AETm_App) and Lemma 31, we finish.

Case $E_1 \,=\, e_{11}\, E_1'$ where e_{11} is a value: By Lemma 127, e_{21} is a value. By the IH, there exist some e_{12}' and e_{22}' such that

- $E_1'[e_1'''] \longrightarrow^* \; e_{12}'$,
- $e_{22} \longrightarrow^* \; e_{22}'$, and
- $\Sigma; \gamma; \emptyset \vdash e_{12}' \sim e_{22}' \;:\; T_1$.

By (AETm_App), (AETm_Conv), and Lemma 31, we finish.

Case (AETm_Eq): We are given $\Sigma; \gamma; \emptyset \vdash e_{11} == e_{12} \sim e_{21} == e_{22} \;:\; \mathsf{bool}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e_{11} \sim e_{21} \;:\; \mathsf{Ref}_r\, T_1$ and $\Sigma; \gamma; \emptyset \vdash e_{12} \sim e_{22} \;:\; \mathsf{Ref}_s\, T_2$. Since $E_1[e_1'] \,=\, e_1 = (e_{11} == e_{12})$, there are three cases we have to consider by case analysis on E_1.

Case $E_1 \,=\, [\,]$: By case analysis on the reduction rule applied to $e_{11} == e_{12}$. Note that e_{11} and e_{12} are values in the following, and so are e_{21} and e_{22} by Lemma 127.

Case (R_Eq) and (R_NEq): By Lemma 130 and (AETm_Const).

Case $E_1 \,=\, E_1' == e_{12}$: By the IH, there exist some e_{11}' and e_{21}' such that

- $E_1'[e_1'''] \longrightarrow^* \; e_{11}'$,
- $e_{21} \longrightarrow^* \; e_{21}'$, and
- $\Sigma; \gamma; \emptyset \vdash e_{11}' \sim e_{21}' \;:\; \mathsf{Ref}_r\, T_1$.

Thus, we finish by (AETm_Eq) and Lemma 31.

Case $E_1 \,=\, e_{11} == E_1'$ where e_{11} is a value: By Lemma 127, e_{21} is a value. By the IH, there exist some e_{12}' and e_{22}' such that

- $E_1'[e_1'''] \longrightarrow^* \; e_{12}'$,
- $e_{22} \longrightarrow^* \; e_{22}'$, and
- $\Sigma; \gamma; \emptyset \vdash e_{12}' \sim e_{22}' \;:\; \mathsf{Ref}_s\, T_2$.

Thus, we finish by (AETm_Eq) and Lemma 31.

Case (AETm_REq): We are given $\Sigma; \gamma; \emptyset \vdash (r == s) \sim (r == s) \;:\; \mathsf{bool}$. Since the reduction rules applicable to $r == s$ are only (R_REq) and (R_RNEq), we finish by (AETm_Const).

Case (AETm_RApp): We are given $\Sigma; \gamma; \emptyset \vdash e_{11}\{r\} \sim e_{21}\{r\} \;:\; [\,r/s\,]\, T'$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash e_{11} \sim e_{21} \;:\; \forall s. T'$. Since $E_1[e_1'] \,=\, e_1 = e_{11}\{r\}$, there are two cases we have to consider by case analysis on E_1.

Case $E_1 \,=\, [\,]$: Since the only reduction rule applicable to $e_{11}\{r\}$ is (R_RBeta). Thus, we are given [[$e11 = nus.e11'$]] for some s and e_{11}', and $e_{11}\{r\} \longrightarrow [\,r/s\,]\, e_{11}'$. By Lemma 125,

- $e_{21} \,=\, \lambda s. e_{21}'$,
- $\Sigma; \gamma; s \vdash e_{11}' \sim e_{21}' \;:\; T''$, and
- $\forall s. T'' \,\equiv\, \forall s. T'$

for some e_{21}' and T''. By (R_RBeta), $e_{21}\{r\} \longrightarrow [\,r/s\,]\, e_{21}'$. Since $r \,\in\, \gamma$ from well-formedness of e_1, we have $\Sigma; \gamma; \emptyset \vdash [\,r/s\,]\, e_{11}' \sim [\,r/s\,]\, e_{21}' \;:\; [\,r/s\,]\, T''$ by Lemma 113 (3). Since $[\,r/s\,]\, T'' \,\equiv\, [\,r/s\,]\, T'$ by Lemma 75, we finish by (AETm_Conv).

Case $E_1 \,=\, E_1'\{r\}$: By the IH, there exist some e_{11}' and e_{21}' such that

- $E_1'[e_1'''] \longrightarrow^* \; e_{11}'$,
- $e_{21} \longrightarrow^* \; e_{21}'$, and
- $\Sigma; \gamma; \emptyset \vdash E_1'[e_1'''] \sim e_{21}' \;:\; \forall s. T'$.

By (AETm_RApp) and Lemma 31, we finish.

Case (AETm_WCheck): We are given $\Sigma; \gamma; \emptyset \vdash \langle\!\langle\, \{x{:}T_1 \mid c_1\}, e_1'''' \,\rangle\!\rangle^\ell \sim \langle\!\langle\, \{x{:}T_2 \mid c_2\}, e_2'''' \,\rangle\!\rangle^\ell \;:\; \{x{:}T_1 \mid c_1\}$ and, by inversion, $\Sigma; \gamma; \emptyset \vdash \{x{:}T_1 \mid c_1\} \sim \{x{:}T_2 \mid c_2\}$ and $\Sigma; \gamma; \emptyset \vdash e_1'''' \sim e_2'''' \;:\; T_1$. Since $E_1[e_1''''] \,=\, e_1 = \langle\!\langle\, \{x{:}T_1 \mid c_1\}, e_1'''' \,\rangle\!\rangle^\ell$, there are two cases we have to consider by case analysis on E_1.

Case $E_1 \,=\, [\,]$: Since the reduction rule applicable to e_1 is only (R_Check), e_1'''' is a value and

$$\langle\!\langle\, \{x{:}T_1 \mid c_1\}, e_1'''' \,\rangle\!\rangle^\ell \longrightarrow \langle \{x{:}T_1 \mid c_1\}, \nu\emptyset. \langle \emptyset \mid [\, e_1''''/x \,]\, c_1 \rangle, e_1'''' \rangle^\ell.$$

By Lemma 127, e_2'''' is a value. By (R_Check),

$$e_2 \longrightarrow \langle \{x{:}T_2 \mid c_2\}, \nu\emptyset.\langle \emptyset \mid [\, e_2''''/x \,]\, c_2 \rangle, e_2'''' \rangle^{\ell}.$$

Thus, it suffices to show that

$$\Sigma; \gamma; \emptyset \vdash \langle \{x{:}T_1 \mid c_1\}, \nu\emptyset.\langle \emptyset \mid [\, e_1''''/x \,]\, c_1 \rangle, e_1'''' \rangle^{\ell} \sim \langle \{x{:}T_2 \mid c_2\}, \nu\emptyset.\langle \emptyset \mid [\, e_2''''/x \,]\, c_2 \rangle, e_2'''' \rangle^{\ell} \;:\; \{x{:}T_1 \mid c_1\}.$$

Since $\Sigma; \gamma; \emptyset \vdash \{x{:}T_1 \mid c_1\} \sim \{x{:}T_2 \mid c_2\}$, we have $\emptyset; \Sigma; \gamma; x{:}T_1 \vdash c_1 \sim c_2 \;:\; \{\top\}\mathsf{bool}\{\top\}^{\langle \emptyset, \emptyset \rangle}$. By Lemma 110 (4), $\emptyset; \Sigma; \gamma; \emptyset \vdash [\, e_1''''/x \,]\, c_1 \sim [\, e_2''''/x \,]\, c_2 \;:\; \{\top\}\mathsf{bool}\{\top\}^{\langle \emptyset, \emptyset \rangle}$. By (AEP) and (AETm_ACheck), we finish.

Case $E_1 = \langle\!\langle\, \{x{:}T_1 \mid c_1\}, E_1' \,\rangle\!\rangle^{\ell}$: By the IH, there exist some e_1'''' and e_2'''' such that

- $*$ $E_1'[e_1'''] \longrightarrow^* e_1''''$,
- $*$ $e_{21} \longrightarrow^* e_2''''$, and
- $*$ $\Sigma; \gamma; \emptyset \vdash e_1'''' \sim e_2'''' \;:\; T_1$.

By (AETm_WCheck) and Lemma 31, we finish.

Case (AETm_ACheck): We are given $\Sigma; \gamma; \emptyset \vdash \langle \{x{:}T_1 \mid c_1\}, p_1, v_1 \rangle^{\ell} \sim \langle \{x{:}T_2 \mid c_2\}, p_2, v_2 \rangle^{\ell} \;:\; \{x{:}T_1 \mid c_1\}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash \{x{:}T_1 \mid c_1\} \sim \{x{:}T_2 \mid c_2\}$,
- $\emptyset; \Sigma; \gamma \vdash p_1 \sim p_2 \;:\; \mathsf{bool}^{\emptyset}$, and
- $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \;:\; T_1$.

Since $E_1[e_1'] = e_1$, we have $E_1 = [\,]$. By case analysis on the reduction rule applied to e_1.

Case (R_Checking): We are given $\emptyset \mid p_1 \hookrightarrow p_1''$ for some p_1''. Since $\gamma \vdash \emptyset \sim \emptyset \;:\; \emptyset^{\emptyset}$, there exist some p_1' and p_2' such that

- $*$ $\emptyset \mid p_1'' \hookrightarrow^* p_1'$,
- $*$ $\emptyset \mid p_2 \hookrightarrow^* p_2'$, and
- $*$ $\emptyset; \Sigma; \gamma \vdash p_1' \sim p_2' \;:\; \mathsf{bool}^{\emptyset}$

by the IH (case (3)). Thus, we finish by (AETm_ACheck) and (R_Checking), we finish.

Case (R_Blame): We are given $p_1 = \nu\gamma'.\langle \mu_1' \mid \Uparrow\ell' \rangle$ and $e_1 \longrightarrow \Uparrow\ell'$. By Lemma 129, there exist some μ_2', Σ', and A_1' such that

- $*$ $p_2 = \nu\gamma'.\langle \mu_2' \mid c_2' \rangle$,
- $*$ $\gamma, \gamma' \vdash \mu_1' \sim \mu_2' \;:\; (\Sigma, \Sigma')^{\gamma'}$, and
- $*$ $\mu_1'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \Uparrow\ell' \sim c_2' \;:\; \{A_1'\}\mathsf{bool}\{\top\}^{\langle \gamma', \gamma' \rangle}$.

By definition, for $i \in \{1, 2\}$, $\mu_i' = \mu_i \,|_{\gamma'}$. From well typedness of p_1, $\mu_1' \models A_1'$. Thus, by Lemma 133, $\mu_2' \mid c_2' \longrightarrow^* \mu_2' \mid \Uparrow\ell'$ where the computation does not mutate contents in μ_2'. Thus, by (R_Checking)/(P_Comput) and (R_Blame), $e_2 \longrightarrow^* \Uparrow\ell'$. By (AEC_Blame), we finish.

Case (R_OK) and (R_Fail): We are given $p_1 = \nu\gamma'.\langle \mu_1' \mid \mathsf{return}\, v_1 \rangle$ for some γ', μ_1', v_1 such that v_1' is true or false. By Lemma 129, there exist some μ_2', Σ', and A_1' such that

- $*$ $p_2 = \nu\gamma'.\langle \mu_2' \mid c_2' \rangle$,
- $*$ $\gamma, \gamma' \vdash \mu_1' \sim \mu_2' \;:\; (\Sigma, \Sigma')^{\gamma'}$, and
- $*$ $\mu_1'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \mathsf{return}\, v_1' \sim c_2' \;:\; \{A_1'\}\mathsf{bool}\{\top\}^{\langle \gamma', \gamma' \rangle}$.

By definition, for $i \in \{1, 2\}$, $\mu_i' = \mu_i' \,|_{\gamma'}$. From well typedness of p_1, $\mu_1' \models A_1'$. Thus, by Lemma 142, there exist some v_2' and A_1'' such that

- $*$ $\mu_2' \mid c_2' \longrightarrow^* \mu_2' \mid \mathsf{return}\, v_2'$ where the computation does not mutate contents in μ_2', and
- $*$ $\mu_1'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \mathsf{return}\, v_1' \sim \mathsf{return}\, v_2' \;:\; \{A_1''\}\mathsf{bool}\{\top\}^{\langle \gamma', \gamma' \rangle}$.

Since $\Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash v_1' \sim v_2' \;:\; \mathsf{bool}$ by Lemma 140, we have $v_1' = v_2'$ by Lemma 120. If the applied evaluation rule is (R_OK), then, for $i \in \{1, 2\}$, we have $e_i \longrightarrow^* v_i$ by (R_Checking)/(P_Comput) and (R_OK); otherwise, if the applied evaluation rule is (R_Fail), then, for $i \in \{1, 2\}$, we have $e_i \longrightarrow^* \Uparrow\ell$ by (R_Checking)/(P_Comput) and (R_Fail);

Case (AETm_Conv): By the IH and (AETm_Conv).

2. By case analysis on the typing rule applied last.

Case (AEC_Return): If the applied computation rule is (C_Red), then we finish by the IH (case (1)), (C_Red), and (AEC_Return). Otherwise, if (C_RBlame) is applied, then we finish by Lemma 128, (C_RBlame), and (AEC_Blame).

Case (AEC_Bind): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow e_{11}; c_{12} \sim y \leftarrow e_{21}; c_{22} \ :\ \{A_1\}x{:}T\{A_2\}^{\varrho}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e_{11} \sim e_{21} \ :\ \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $\emptyset; \Sigma; \gamma; y{:}T' \vdash c_{12} \sim c_{22} \ :\ \{A_3\}x{:}T\{A_2\}^{\varrho_2}$, and
- $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \cup \varrho_2 \ =\ \varrho$.

By case analysis on the computation rule applied to c_1.

Case (C_Red): By the IH (case (1)), (C_Red), and (AEC_Bind).

Case (C_Comput): We are given $e_{11} \ =\ \mathsf{do}\, c_{11}$ and $\mu_1 \mid c_{11} \longrightarrow \mu_1'' \mid c_{11}''$ for some μ_1'' and c_{11}''. Since $\Sigma; \gamma; \emptyset \vdash e_{11} \sim e_{21} \ :\ \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ we have

- $*$ $e_{21} \ =\ \mathsf{do}\, c_{21}$,
- $*$ $\emptyset; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} \ :\ \{A_1''\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $*$ $A_1'' \ \equiv\ A_1$,
- $*$ $T'' \ \equiv\ T'$, and
- $*$ $A_3'' \ \equiv\ A_3$.

for some c_{21}, A_{11}'', T'', and A_3'' by Lemmas 126 and 56. By Lemma 107 (1), $\mu_1; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} \ :\ \{A_1''\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$. Since $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \ \subseteq\ \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have $\gamma \vdash \mu_1 \mid_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \sim \mu_2 \mid_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \ :\ \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$ by Lemma 139. Since $A_1'' \ \equiv\ A_1$ and $\mu_1 \models A_1$, we have $\mu_1 \models A_1''$ by Lemma 90. Since the length of the derivation of $\mu_1; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} \ :\ \{A_1''\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ is smaller than that of $\Sigma; \gamma; \emptyset \vdash \mathsf{do}\, c_{11} \sim \mathsf{do}\, c_{21} \ :\ \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, we can apply the IH: there exist some Σ', A_1', μ_1', c_{11}', μ_2', and c_{21}' such that

- $*$ $\mu_1'' \mid c_{11}'' \longrightarrow^* \mu_1' \mid c_{11}'$,
- $*$ $\mu_2 \mid c_{21} \longrightarrow^* \mu_2' \mid c_{21}'$,
- $*$ $\mu_1'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c_{11}' \sim c_{21}' \ :\ \{A_1'\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $*$ $\gamma \vdash \mu_1' |_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \sim \mu_2' |_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \ :\ (\Sigma, \Sigma')^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$,
- $*$ $\mu_1' \models A_1'$,
- $*$ $\mathit{dom}\,(\Sigma') \ =\ \mathit{dom}\,(\Sigma' |_{\gamma_{\mathtt{w}1}})$, and
- $*$ $\mu_i |_{\gamma_{\mathtt{w}1}{}^c} \ =\ \mu_i' |_{\gamma_{\mathtt{w}1}{}^c}$ for $i \in \{1, 2\}$.

By (C_Comput), $\mu_1 \mid c_1 \longrightarrow^* \mu_1' \mid y \leftarrow \mathsf{do}\, c_{11}'; c_{12}$ and $\mu_2 \mid c_2 \longrightarrow^* \mu_2' \mid y \leftarrow \mathsf{do}\, c_{21}'; c_{22}$. Since $\{A_1'\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle} \ \equiv\ \{A_1'\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ by Lemmas 85 (2) and (3), we have $\mu_1'; \Sigma, \Sigma'; \gamma; \emptyset \vdash c_{11}' \sim c_{21}' \ :\ \{A_1'\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ by (AEC_Conv). By Lemma 104 (4) and (AEC_CBind), we have

$$\mu_1'; \Sigma, \Sigma'; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_{11}'; c_{12} \sim y \leftarrow \mathsf{do}\, c_{21}'; c_{22} \ :\ \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Since $\gamma_{\mathtt{w}1} \ \subseteq\ \gamma_{\mathtt{w}}$, $\mathit{dom}\,(\Sigma') \ =\ \mathit{dom}\,(\Sigma' |_{\gamma_{\mathtt{w}}})$. By Lemma 145,

$$\gamma \vdash \mu_1' |_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2' |_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ :\ (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}.$$

Finally, for $i \in \{1, 2\}$, since $\gamma_{\mathtt{w}1} \ \subseteq\ \gamma_{\mathtt{w}}$ and $\mu_i |_{\gamma_{\mathtt{w}1}{}^c} \ =\ \mu_i' |_{\gamma_{\mathtt{w}1}{}^c}$, we have $\mu_i |_{\gamma_{\mathtt{w}}{}^c} \ =\ \mu_i' |_{\gamma_{\mathtt{w}}{}^c}$ by Lemma 146 (2).

Case (C_RBlame): By Lemma 128, (C_RBlame), and (AEC_Blame).

Case (C_CBlame): By Lemmas 126 and 133, (C_Comput), (C_CBlame), and (AEC_Blame).

Case (C_Return): We are given $e_{11} \ =\ \mathsf{do}\, \mathsf{return}\, v_1$ for some v_1, and $\mu_1 \mid c_1 \longrightarrow \mu_1 \mid [\, v_1/y \,]\, c_{12}$. By Lemmas 126 and 56, we have

- $*$ $e_{21} \ =\ \mathsf{do}\, c_{21}$,
- $*$ $\emptyset; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim c_{21} \ :\ \{A_1''\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $*$ $A_1'' \ \equiv\ A_1$,
- $*$ $T'' \ \equiv\ T'$, and
- $*$ $A_3'' \ \equiv\ A_3$

for some c_{21}, A_1'', T'', and A_3''. By Lemma 107 (1), $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim c_{21} \ :\ \{A_1''\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$. Since $\gamma \vdash \mu_1 |_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \sim \mu_2 |_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \ :\ \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$ by Lemma 139, and $\mu_1 \models A_1''$ by Lemma 90, we have

- $*$ $\mu_2 \mid c_{21} \longrightarrow^* \mu_2 \mid \mathsf{return}\, v_2$ where the computation does not mutate contents in μ_2,
- $*$ $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1'\}y{:}T''\{A_3''\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, and
- $*$ $\mu_1 \models A_1'$

for some v_2 and A_1' by Lemma 142. By (C_Comput) and (C_Return), $\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid [\, v_2/y \,]\, c_{22}$. Since $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ T''$ by Lemma 140, we have $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ T'$ by (AETm_Conv), and so

$$\emptyset; \Sigma; \gamma; \emptyset \vdash [\, v_1/x \,]\, c_{12} \sim [\, v_2/x \,]\, c_{22} \ :\ \{[\, v_1/y \,]\, A_3\}x{:}T\{A_2\}^{\varrho_2}$$

by Lemma 110 (4). Since $\gamma_\mathtt{r} \cup \gamma_\mathtt{w} \subseteq \gamma$ by applying Lemmas 86 (3) and 39 to well typedness of the left-hand side, we have

$$\mu_1; \Sigma; \gamma; \emptyset \vdash [\, v_1/y \,]\, c_{12} \sim [\, v_2/y \,]\, c_{22} \ : \ \{[\, v_1/y \,]\, A_3\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$$

by Lemma 106 (1). Since $\{A'_1\}y{:}T''\{A''_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle} \equiv \{A'_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ by Lemmas 85 (2) and (3), we have $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \ : \ \{A'_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ by (T_Conv). Thus, since $\mu_1 \models A'_1$, we have $\mu_1 \models [\, v_1/x \,]\, A_3$ by Lemma 91.

Case (C_Region): We are given $e_{11} = \nu r.\, c'_{11}$ for some r and c'_{11}, and $\mu_1 \mid c_1 \longrightarrow \mu_1 \mid \nu r.\, y \leftarrow \mathsf{do}\, c'_{11}; c_{12}$. By Lemmas 126 and 56,

- $*$ $e_{21} = \mathsf{do}\, c_{21}$,
- $*$ $\emptyset; \Sigma; \gamma; \emptyset \vdash \nu r.\, c'_{11} \sim c_{21} \ : \ \{A''_1\}y{:}T''\{A''_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $*$ $A''_1 \equiv A_1$,
- $*$ $T'' \equiv T$, and
- $*$ $A''_3 \equiv A_3$

for some c_{21}, A''_1, T'', and A''_3. Since $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle$, we have $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \sim \mu_2|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \ : \ \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$ by Lemma 139. Since $\mu_1 \models A''_1$ by Lemma 90, there exist some c'_{21} and A'_1 such that

- $*$ $\mu_2 \mid c_{21} \longrightarrow^* \mu_2 \mid \nu r.\, c'_2$ where the computation does not mutate contents in μ_2,
- $*$ $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c'_{11} \sim \nu r.\, c'_{21} \ : \ \{A'_1\}y{:}T''\{A''_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, and
- $*$ $\mu_1 \models A'_1$

by Lemma 138. Thus, by (C_Comput) and (C_Region), $\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid \nu r.\, y \leftarrow \mathsf{do}\, c'_{21}; c_{22}$. Thus, it suffices to show that

$$\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, y \leftarrow \mathsf{do}\, c'_{11}; c_{12} \sim \nu r.\, y \leftarrow \mathsf{do}\, c'_{21}; c_{22} \ : \ \{A'_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}.$$

Since $\{A'_1\}y{:}T''\{A''_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle} \equiv \{A'_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ by Lemmas 85 (2) and (3), we have $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c'_{11} \sim \nu r.\, c'_{21} \ : \ \{A'_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ by (AEC_Conv). Thus, $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, \nu r.\, c'_{11}; c_{12} \sim y \leftarrow \mathsf{do}\, \nu r.\, c'_{21}; c_{22} \ : \ \{A'_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ by (AEC_CBind). By Lemma 136, we finish.

Case (AEC_CBind): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c_{11}; c_{12} \sim y \leftarrow \mathsf{do}\, c_{21}; c_{22} \ : \ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \cup \varrho_2}$ and, by inversion,

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} \ : \ \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $\emptyset; \Sigma; \gamma; y{:}T' \vdash c_{12} \sim c_{22} \ : \ \{A_3\}x{:}T\{A_2\}^{\varrho_2}$, and
- $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \cup \varrho_2 = \langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle$.

By case analysis on the computation rule applied to c_1.

Case (C_Comput): We are given $\mu_1 \mid c_{11} \longrightarrow \mu''_1 \mid c''_{11}$ for some μ''_1 and c''_{11}. Since $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle$, we have $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \sim \mu_2|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \ : \ \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$ by Lemma 139. Thus, by the IH, there exist some Σ', A'_1, μ'_1, c'_{11}, μ'_2, and c'_{21} such that

- $*$ $\mu''_1 \mid c''_{11} \longrightarrow^* \mu'_1 \mid c'_{11}$,
- $*$ $\mu_2 \mid c_{21} \longrightarrow^* \mu'_2 \mid c'_{21}$,
- $*$ $\mu'_1; \Sigma, \Sigma'; \gamma; \emptyset \vdash c'_{11} \sim c'_{21} \ : \ \{A'_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$,
- $*$ $\gamma \vdash \mu'_1|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \sim \mu'_2|_{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \ : \ (\Sigma, \Sigma')^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$,
- $*$ $\mu'_1 \models A'_1$,
- $*$ $\mathit{dom}\,(\Sigma') = \mathit{dom}\,(\Sigma'|_{\gamma_{\mathtt{w}1}})$, and
- $*$ $\mu_i|_{\gamma_{\mathtt{w}1}{}^c} = \mu'_i|_{\gamma_{\mathtt{w}1}{}^c}$ for $i \in \{1, 2\}$.

By (C_Comput), $\mu_1 \mid c_1 \longrightarrow^* \mu'_1 \mid y \leftarrow \mathsf{do}\, c'_{11}; c_{12}$ and $\mu_2 \mid c_2 \longrightarrow^* \mu'_2 \mid y \leftarrow \mathsf{do}\, c'_{21}; c_{22}$. By Lemma 104 (4) and (AEC_CBind), we have

$$\mu'_1; \Sigma, \Sigma'; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c'_{11}; c_{12} \sim y \leftarrow \mathsf{do}\, c'_{21}; c_{22} \ : \ \{A'_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}.$$

Since $\gamma_{\mathtt{w}1} \subseteq \gamma_\mathtt{w}$, $\mathit{dom}\,(\Sigma') = \mathit{dom}\,(\Sigma'|_{\gamma_\mathtt{w}})$. By Lemma 145,

$$\gamma \vdash \mu'_1|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \sim \mu'_2|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \ : \ (\Sigma, \Sigma')^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}.$$

Finally, for $i \in \{1, 2\}$, since $\gamma_{\mathtt{w}1} \subseteq \gamma_\mathtt{w}$ and $\mu_i|_{\gamma_{\mathtt{w}1}{}^c} = \mu'_i|_{\gamma_{\mathtt{w}1}{}^c}$, we have $\mu_i|_{\gamma_\mathtt{w}{}^c} = \mu'_i|_{\gamma_\mathtt{w}{}^c}$ by Lemma 146 (2).

Case (C_CBlame): By Lemma 133, (C_Comput), (C_CBlame), and (AEC_Blame).

Case (C_Return): We are given $c_{11} = \mathsf{return}\, v_1$ for some v_1, and $\mu_1 \mid c_1 \longrightarrow \mu_1 \mid [\, v_1/y \,]\, c_{12}$. By Lemma 142, there exists some v_2 and A'_1 such that

- $\mu_2 \mid c_{21} \longrightarrow^* \mu_2 \mid \mathsf{return}\, v_2$ where the computation does not mutate contents of μ_2,
- $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \ :\ \{A_1'\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, and
- $\mu_1 \models A_1'$.

By (C_Comput) and (C_Return), $\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid [\, v_2/y \,]\, c_{22}$. Since $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 \ :\ T'$ by Lemma 140, we have

$$\mu_1; \Sigma; \gamma; \emptyset \vdash [\, v_1/y \,]\, c_{12} \sim [\, v_2/y \,]\, c_{22} \ :\ \{[\, v_1/y \,]\, A_3\}x{:}T\{A_2\}^{\varrho_2}$$

by Lemma 110 (4). Since $\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}} \subseteq \gamma$ by well typedness of the left-hand side, we have

$$\mu_1; \Sigma; \gamma; \emptyset \vdash [\, v_1/y \,]\, c_{12} \sim [\, v_2/y \,]\, c_{22} \ :\ \{[\, v_1/y \,]\, A_3\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$$

by Lemma 106 (1). Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{return}\, v_1 \ :\ \{A_1'\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$ from the well typedness, we have $\mu_1 \models [\, v_1/x \,]\, A_3$ by Lemma 91.

Case (C_Region): We are given $c_{11} = \nu r.\, c_{11}'$ for some r and c_{11}', and $\mu_1 \mid c_1 \longrightarrow \mu_1 \mid \nu r.\, y \leftarrow \mathsf{do}\, c_{11}'; c_{12}$. Since $\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have $\gamma \vdash \mu_1 \,|_{\,\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \sim \mu_2 \,|_{\,\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}} \ :\ \Sigma^{\gamma_{\mathtt{r}1} \cup \gamma_{\mathtt{w}1}}$ by Lemma 139. Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_{11}' \sim c_{21} \ :\ \{A_1\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, there exist some c_{21}' and A_1' such that

- $\mu_2 \mid c_{21} \longrightarrow^* \mu_2 \mid \nu r.\, c_2'$ where the computation does not mutate contents in μ_2,
- $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_{11}' \sim \nu r.\, c_{21}' \ :\ \{A_1'\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, and
- $\mu_1 \models A_1'$

by Lemma 138. Thus, by (C_Comput) and (C_Region), $\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid \nu r.\, y \leftarrow \mathsf{do}\, c_{21}'; c_{22}$. Thus, it suffices to show that

$$\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, y \leftarrow \mathsf{do}\, c_{11}'; c_{12} \sim \nu r.\, y \leftarrow \mathsf{do}\, c_{21}'; c_{22} \ :\ \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c_{11}' \sim \nu r.\, c_{21}' \ :\ \{A_1'\}y{:}T'\{A_3\}^{\langle \gamma_{\mathtt{r}1}, \gamma_{\mathtt{w}1} \rangle}$, we have $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, \nu r.\, c_{11}'; c_{12} \sim y \leftarrow \mathsf{do}\, \nu r.\, c_{21}'; c_{22} \ :\ \{A_1'\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ by (AEC_CBind). By Lemma 136, we finish.

Case (AEC_New): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \Leftarrow \mathsf{ref}_r\, e_{11}; c_{12} \sim y \Leftarrow \mathsf{ref}_r\, e_{21}; c_{22} \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e_{11} \sim e_{21} \ :\ T'$ and
- $\emptyset; \Sigma; \gamma; y{:}\mathsf{Ref}_r\, T' \vdash c_{12} \sim c_{22} \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \rangle}$.

By case analysis on the computation rule applied to c_1.

Case (C_Red): By the IH (case (1)), (C_Red), and (AEC_New).

Case (C_RBlame): By Lemma 128, (C_RBlame), and (AEC_Blame).

Case (C_Command)/(C_New): We can suppose that e_{11} is a value, and so is e_{21} by Lemma 127. We are given $\mu_1 \mid c_1 \longrightarrow \mu_1 \uplus \{a@r \mapsto e_{11}\} \mid y \leftarrow \mathsf{do}\, \mathsf{return}\, a@r; c_{12}$ for some a such that $a@r \notin \mathit{dom}\,(\mu_1)$. Since $\gamma \vdash \mu_1 \,|_{\,\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}} \sim \mu_2 \,|_{\,\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}} \ :\ \Sigma^{\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}}$, it is found that $a@r \notin \mathit{dom}\,(\mu_2)$. Thus, $\mu_2 \mid c_2 \longrightarrow \mu_2 \uplus \{a@r \mapsto e_{21}\} \mid y \leftarrow \mathsf{do}\, \mathsf{return}\, a@r; c_{22}$. By (AETm_Address), (AEC_Return), and (AEC_CBind), we have

$$\mu_1 \uplus \{a@r \mapsto e_{11}\}; \Sigma, a@r{:}T'; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, \mathsf{return}\, a@r; c_{12} \sim y \leftarrow \mathsf{do}\, \mathsf{return}\, a@r; c_{22} \ :\ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, {\gamma_{\mathtt{w}}}' \cup \{r\} \rangle}.$$

Note that $a@r \notin \mathit{dom}\,(\Sigma)$ because $a@r \notin \mathit{dom}\,(\mu_1)$ and $\gamma \vdash \mu_1 \,|_{\,\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2 \,|_{\,\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ :\ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$. Since $\gamma \vdash \mu_1 \,|_{\,\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}} \sim \mu_2 \,|_{\,\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}} \ :\ \Sigma^{\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}}$ and $\Sigma, a@r{:}T'; \gamma; \emptyset \vdash e_{11} \sim e_{21} \ :\ T'$ by Lemma 104 (3), we have

$$\gamma \vdash (\mu_1 \uplus \{a@r \mapsto e_{11}\}) \,|_{\,\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}} \sim (\mu_2 \uplus \{a@r \mapsto e_{21}\}) \,|_{\,\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}} \ :\ (\Sigma, a@r{:}T)^{\gamma_{\mathtt{r}} \cup {\gamma_{\mathtt{w}}}' \cup \{r\}}$$

by Lemma 104 (3). By Lemma 88,

$$\mu_1 \uplus \{a@r \mapsto e_{11}\} \models A_1.$$

Finally, for $i \in \{1, 2\}$,

$$\mu_i \,|_{\,({\gamma_{\mathtt{w}}}' \cup \{r\})^c} = (\mu_i \uplus \{a@r \mapsto e_{i1}\}) \,|_{\,({\gamma_{\mathtt{w}}}' \cup \{r\})^c}.$$

Case (AEC_Deref): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \Leftarrow\, !e_{11}; c_{12} \sim y \Leftarrow\, !e_{21}; c_{22} \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}' \cup \{r\}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e_{11} \sim e_{21} \ :\ \mathsf{Ref}_r\, T'$ and
- $\emptyset; \Sigma; \gamma; y{:}T' \vdash c_{12} \sim c_{22} \ :\ \{A_1\}x{:}T\{A_2\}^{\langle {\gamma_{\mathtt{r}}}', \gamma_{\mathtt{w}} \rangle}$.

By case analysis on the computation rule applied to c_1.

Case (C_Red): By the IH (case (1)), (C_Red), and (AEC_Deref).

Case (C_RBlame): By Lemma 128, (C_RBlame), and (AEC_Blame).

Case (C_Command)/(C_Deref): We are given $e_{11} = a@r$ (the region r is identified from Lemma 59 (3)) and $\mu_1 \mid c_1 \longrightarrow \mu_1 \mid y \leftarrow \mathsf{do\,return}\, \mu_1(a@r); c_{12}$. By Lemma 123, $e_{21} = a@r$. Since $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}}' \cup \{r\} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}}' \cup \{r\} \cup \gamma_{\mathtt{w}}} : \Sigma^{\gamma_{\mathtt{r}}' \cup \{r\} \cup \gamma_{\mathtt{w}}}$, we have $\Sigma; \gamma; \emptyset \vdash \mu_1(a@r) \sim \mu_2(a@r) : \Sigma(a@r)$. By Lemmas 63 and 54 and (AETm_Conv), $\Sigma; \gamma; \emptyset \vdash \mu_1(a@r) \sim \mu_2(a@r) : T'$. Since $\mu_2(a@r)$ is defined, $\mu_2 \mid c_2 \longrightarrow \mu_2 \mid y \leftarrow \mathsf{do\,return}\, \mu_2(a@r); c_{12}$. Thus, we finish by (AEC_Return) and (AEC_CBind).

Case (C_Command)/(C_GuardDeref): Straightforward by Lemma 124.

Case (AEC_Assign): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \Leftarrow e_{11} := e_{12}; c_{13} \sim y \Leftarrow e_{21} := e_{22}; c_{23} : \{A_1\} x{:}T \{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}}' \cup \{r\} \rangle}$ and, by inversion,

- $\Sigma; \gamma; \emptyset \vdash e_{11} \sim e_{21} : \mathsf{Ref}_r\, T'$,
- $\Sigma; \gamma; \emptyset \vdash e_{12} \sim e_{22} : T'$, and
- $\emptyset; \Sigma; \gamma; y{:}\mathsf{unit} \vdash c_{13} \sim c_{23} : \{\top\} x{:}T \{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}}' \rangle}$.

By case analysis on the computation rule applied to c_1.

Case (C_Red): By the IH (case (1)), Lemma 127, (C_Red), and (AEC_Assign).

Case (C_RBlame): By Lemmas 128 and 127, (C_RBlame), and (AEC_Blame).

Case (C_Command)/(C_Assign): We can suppose that e_{12} is a value, and so is e_{22} by Lemma 127. We are given $e_{11} = a@r$ (note that the region r is identified by Lemma 59 (3)) and

$$\mu_1' \uplus \{a@r \mapsto v_1\} \mid c_1 \longrightarrow \mu_1' \uplus \{a@r \mapsto e_{12}\} \mid y \leftarrow \mathsf{do\,return}\,(); c_{13}$$

for some μ_1' and v_1 such that $\mu_1 = \mu_1' \uplus \{a@r \mapsto v_1\}$. By Lemma 123, $e_{21} = a@r$. Since $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}' \cup \{r\}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}' \cup \{r\}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}' \cup \{r\}}$, there exists some μ_2' and v_2 such that $\mu_2 = \mu_2' \uplus \{a@r \mapsto v_2\}$ and $\Sigma; \gamma; \emptyset \vdash v_1 \sim v_2 : \Sigma(a@r)$. Thus, by (C_Command)/(C_Assign),

$$\mu_2 \mid c_2 \longrightarrow \mu_2' \uplus \{a@r \mapsto e_{22}\} \mid y \leftarrow \mathsf{do\,return}\,(); c_{23}.$$

Since $\Sigma; \gamma; \emptyset \vdash e_{12} \sim e_{22} : T'$ and $\Sigma; \gamma; \emptyset \vdash a@r : \mathsf{Ref}_r\, T'$, we have $\Sigma; \gamma; \emptyset \vdash e_{12} \sim e_{22} : \Sigma(a@r)$ by Lemmas 63 and 54 and (AETm_Conv). Thus,

$$\gamma \vdash (\mu_1' \uplus \{a@r \mapsto e_{12}\})|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}' \cup \{r\}} \sim (\mu_2' \uplus \{a@r \mapsto e_{22}\})|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}' \cup \{r\}} : \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}' \cup \{r\}}.$$

Since $\Sigma; \gamma; \emptyset \vdash () \sim () : \mathsf{unit}$ by (AETm_Const), we have

$$\mu_1' \uplus \{a@r \mapsto e_{12}\}; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do\,return}\,(); c_{13} \sim y \leftarrow \mathsf{do\,return}\,(); c_{23} : \{\top\} x{:}T \{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}}' \cup \{r\} \rangle}$$

by (AEC_Return) and (AEC_CBind). Finally, for $i \in \{1, 2\}$,

$$(\mu_i' \uplus \{a@r \mapsto v_i\})|_{(\gamma_{\mathtt{w}}' \cup \{r\})^c} = (\mu_i' \uplus \{a@r \mapsto e_{i2}\})|_{(\gamma_{\mathtt{w}}' \cup \{r\})^c}.$$

Case (C_Command)/(C_GuardAssign): Straightforward by Lemma 124.

Case (AEC_Assert): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{assert}\,(c_{11})^\ell; c_{12} \sim \mathsf{assert}\,(c_{21})^\ell; c_{22} : \{A_1\} x{:}T \{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\emptyset; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} : \{A_1\} \mathsf{bool} \{\top\}^{\langle \gamma_{\mathtt{r}}, \emptyset \rangle}$ and
- $\emptyset; \Sigma; \gamma; \emptyset \vdash c_{12} \sim c_{22} : \{A_1, c_{11}\} x{:}T \{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$.

The computation rule applicable to c is only (C_Assert). Thus, for $i \in \{1, 2\}$,

$$\mu_i \mid \mathsf{assert}\,(c_{i1})^\ell; c_{i2} \longrightarrow \mu_i \mid \langle \mathsf{assert}\,(c_{i1}), \nu\emptyset.\langle \emptyset \mid c_{i1} \rangle \rangle^\ell; c_{i2}.$$

Since $\mu_1; \Sigma; \gamma; \emptyset \vdash c_{11} \sim c_{21} : \{A_1\} \mathsf{bool} \{\top\}^{\langle \gamma_{\mathtt{r}}, \emptyset \rangle}$ by Lemma 107, we have

$$\mu_1; \Sigma; \gamma \vdash \nu\emptyset.\langle \emptyset \mid c_{11} \rangle \sim \nu\emptyset.\langle \emptyset \mid c_{21} \rangle : \mathsf{bool}^{\gamma_{\mathtt{r}}}$$

by (AEP). By (AEC_Check), we finish.

Case (AEC_Check): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash \langle \mathsf{assert}\,(c_{11}), p_1 \rangle^\ell; c_{12} \sim \langle \mathsf{assert}\,(c_{21}), p_2 \rangle^\ell; c_{22} : \{A_1\} x{:}T \{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\mu_1; \Sigma; \gamma \vdash p_1 \sim p_2 : \mathsf{bool}^{\gamma_{\mathtt{r}}}$ and
- $\emptyset; \Sigma; \gamma; \emptyset \vdash c_{12} \sim c_{22} : \{A_1, c_{11}\} x{:}T \{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$.

Since $\mu_1; \Sigma; \gamma \vdash p_1 \sim p_2 : \mathsf{bool}^{\gamma_{\mathtt{r}}}$, there exist some γ', μ_1', c_1', μ_2', c_2', Σ', and A_1' such that

- $p_1 \;=\; \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle$,
- $p_2 \;=\; \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle$,
- $\gamma, \gamma' \vdash \mu'_1 \sim \mu'_2 \;:\; (\Sigma, \Sigma')^{\gamma'}$, and
- $\mu_1 \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c'_1 \sim c'_2 \;:\; \{A'_1\}\mathsf{bool}\{\top\}^{\langle \gamma' \cup \gamma_{\mathtt{r}}, \gamma' \rangle}$

by Lemma 129. From well typedness of p_1, $\mu_1 \uplus \mu'_1 \models A'_1$. By Lemma 144,

$$\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \sim (\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma_{\mathtt{r}}}.$$

We proceed by case analysis on the computation rule applied to c.

Case (C_CBlame): We are given $c'_1 \;=\; \Uparrow\ell'$ and $\mu_1 \mid c_1 \longrightarrow \mu_1 \mid \Uparrow\ell'$ for some ℓ'. Since

- $*$ $\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \sim (\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma_{\mathtt{r}}}$,
- $*$ $\mu_1 \uplus \mu'_1 \models A'_1$, and
- $*$ $\mu_1 \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \Uparrow\ell' \sim c'_2 \;:\; \{A'_1\}\mathsf{bool}\{\top\}^{\langle \gamma' \cup \gamma_{\mathtt{r}}, \gamma' \rangle}$,

we have $\mu_2 \uplus \mu'_2 \mid c'_2 \longrightarrow^* \mu_2 \uplus \mu'_2 \mid \Uparrow\ell'$, where the computation does not mutate contents in $\mu_2 \uplus \mu'_2$, by Lemma 133. Thus, $\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid \Uparrow\ell'$ by (C_Checking)/(P_Comput) and (C_CBlame). By (AEC_Blame), we finish.

Case (C_Checking): Since $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $\gamma \vdash \mu_1\,|_{\gamma_{\mathtt{r}}} \sim \mu_2\,|_{\gamma_{\mathtt{r}}} \;:\; \Sigma^{\gamma_{\mathtt{r}}}$ by Lemma 139. Since $\mu_1; \Sigma; \gamma \;\vdash\; p_1 \;\sim\; p_2 \;:\; \mathsf{bool}^{\gamma_{\mathtt{r}}}$, there exist some p'_1 and p'_2 such that $\mu_1 \mid p_1 \hookrightarrow^* p'_1$ (one or more computation steps) and $\mu_2 \mid p_2 \hookrightarrow^* p'_2$ and $\mu_1; \Sigma; \gamma \vdash p'_1 \sim p'_2 \;:\; \mathsf{bool}^{\gamma_{\mathtt{r}}}$ by the IH (case (3)). Thus, we finish by (C_Checking) and (AEC_Check).

Case (C_OK) and (C_Fail): We are given $c'_1 \;=\; \mathsf{return}\, v_1$ for some v_1 such that v_1 is true or false. Since

- $*$ $\gamma, \gamma' \vdash (\mu_1 \uplus \mu'_1)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \sim (\mu_2 \uplus \mu'_2)\,|_{\gamma' \cup \gamma_{\mathtt{r}}} \;:\; (\Sigma, \Sigma')^{\gamma' \cup \gamma_{\mathtt{r}}}$,
- $*$ $\mu_1 \uplus \mu'_1 \models A'_1$, and
- $*$ $\mu_1 \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \mathsf{return}\, v_1 \sim c'_2 \;:\; \{A'_1\}\mathsf{bool}\{\top\}^{\langle \gamma' \cup \gamma_{\mathtt{r}}, \gamma' \rangle}$,

there exist some v_2 and A''_1 such that

- $*$ $\mu_2 \uplus \mu'_2 \mid c'_2 \longrightarrow^* \mu_2 \uplus \mu'_2 \mid \mathsf{return}\, v_2$ where the computation does not mutate contents in $\mu_2 \uplus \mu'_2$, and
- $*$ $\mu_1 \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \mathsf{return}\, v_1 \sim \mathsf{return}\, v_2 \;:\; \{A''_1\}\mathsf{bool}\{\top\}^{\langle \gamma' \cup \gamma_{\mathtt{r}}, \gamma' \rangle}$

by Lemma 142. By Lemmas 140 and 120, $v_1 \;=\; v_2$.

If $v_1 \;=\; \mathsf{true}$, then, by (C_Checking)/(P_Comput) and (C_OK), $\mu_i \mid c_i \longrightarrow^* \mu_i \mid c_{i2}$ for $i \in \{1, 2\}$. By Lemma 107,

$$\mu_1; \Sigma; \gamma; \emptyset \vdash c_{12} \sim c_{22} \;:\; \{A_1, c_{11}\}x\!:\!T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

From well typedness of c_1, $\mu_1 \mid \nu\emptyset.\langle \emptyset \mid c_{11} \rangle \hookrightarrow^* p_1$. Thus, since $\mu_1 \models A_1$, we have $\mu_1 \models (A_1, c_{11})$, and so we finish.

Otherwise, if $v_1 \;=\; \mathsf{false}$, then, by (C_Checking)/(P_Comput) and (C_Fail), $\mu_i \mid c_i \longrightarrow^* \mu_i \mid \Uparrow\ell$ for $i \in \{1, 2\}$. By (AEC_Blame), we finish.

Case (AEC_Blame), (AEC_LetRegion), (AEC_RegionNEq1), and (AEC_RegionNEq2): Contradictory.

Case (AEC_Weak): By the IH and (AEC_Weak).

Case (AEC_Conv): By the IH and (AEC_Conv).

Case (AEC_ElimAssert): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{assert}\,(c_{11})^{\ell}; c_{12} \sim c_2 \;:\; \{A_1\}x\!:\!T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\emptyset; \Sigma; \gamma; \emptyset \vdash c_{12} \sim c_2 \;:\; \{A_1, c_{11}\}x\!:\!T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $A''_1 \;\subseteq\; A_1$,
- $\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle \;\subseteq\; \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $\Sigma; \gamma; \emptyset \vdash^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle} A''_1, c_{11}$, and
- for any μ' and σ', if $\Sigma; \gamma; \emptyset \vdash \langle \mu', \sigma' \rangle^{\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle}$ and $\mu' \models \sigma'(A''_1)$, then $\mu' \models \sigma'(c_{11})$.

Since $\mu_1; \Sigma; \gamma; \emptyset \;\vdash\; c_{12} \;\sim\; c_2 \;:\; \{A_1, c_{11}\}x\!:\!T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ by Lemma 107, it suffices to show that $\mu_1 \models c_{11}$. Since $\gamma \;\vdash\; \mu_1 \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;\sim\; \mu_2 \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$, we have $\gamma \;\vdash\; \mu_1 \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \;:\; \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$. Since $\langle {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}'' \rangle \;\subseteq\; \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have $\gamma \vdash \mu_1\,|_{{\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{w}}}''} \;:\; \Sigma^{{\gamma_{\mathtt{r}}}'' \cup {\gamma_{\mathtt{w}}}''}$ by Lemma 70. Since $\mu_1 \models A_1$ and $A''_1 \subseteq A_1$, we have $\mu_1 \models A''_1$. Thus, by Lemma 131, $\mu_1 \models c_{11}$.

Case (AEC_Frame): We are given $\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\, c'_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim c_2 \;:\; \{A'_1, A\}x\!:\!T\{A'_2, A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$ and, by inversion,

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c'_1 \sim c_2 \;:\; \{A'_1\}x\!:\!T\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,

- $\langle {\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{r}}}'', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$,
- $\Sigma; \gamma; \emptyset \vdash^{\langle {\gamma_{\mathtt{r}}}'', \emptyset \rangle} A$, and
- $\Sigma; \gamma; \emptyset \vdash {\gamma_{\mathtt{r}}}'' \,\mathsf{disj}\, {\gamma_{\mathtt{w}}}'$

for some fresh y. Since $\mu_1 \models A'_1, A$, we have $\mu_1 \models A'_1$. Since $\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have $\gamma \vdash \mu_1 \,|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \sim \mu_2 \,|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \,:\, \Sigma^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$. By case analysis on the computation rule applied to c_1.

Case (C_Comput): We are given $\mu_1 \mid c'_1 \longrightarrow \mu''_1 \mid c''_1$ for some μ''_1 and c''_1. Since $\mu_1; \Sigma; \gamma; \emptyset \vdash c'_1 \sim c_2 \,:\, \{A'_1\} x{:}T\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$, there exist some Σ''', A'''_1, μ'''_1, c'''_1, μ'''_2, and c'''_2 such that

* $\mu''_1 \mid c''_1 \longrightarrow^* \mu'''_1 \mid c'''_1$,
* $\mu_2 \mid c_2 \longrightarrow^* \mu'''_2 \mid c'''_2$,
* $\mu'''_1; \Sigma, \Sigma'''; \gamma; \emptyset \vdash c'''_1 \sim c'''_2 \,:\, \{A'''_1\} x{:}T\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$,
* $\gamma \vdash \mu'''_1 \,|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \sim \mu'''_2 \,|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \,:\, (\Sigma, \Sigma''')^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$,
* $\mu'''_1 \models A'''_1$,
* $\mathit{dom}\,(\Sigma''') = \mathit{dom}\,(\Sigma''' \,|_{{\gamma_{\mathtt{w}}}'})$, and
* $\mu_i \,|_{{\gamma_{\mathtt{w}}}'^{c}} = \mu'''_i \,|_{{\gamma_{\mathtt{w}}}'^{c}}$ for $i \in \{1, 2\}$

by the IH.
By (C_Comput), $\mu_1 \mid c_1 \longrightarrow^* \mu'''_1 \mid y \leftarrow \mathsf{do}\; c'''_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\; y$. By (AEC_Frame),

$$\mu'''_1; \Sigma, \Sigma'''; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\; c'''_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\; y \sim c'''_2 \,:\, \{A'''_1, A\} x{:}T\{A'_2, A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

By Lemma 145,

$$\gamma \vdash \mu'''_1 \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu'''_2 \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \,:\, (\Sigma, \Sigma''')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}.$$

Since $\mathit{dom}\,(\Sigma''') = \mathit{dom}\,(\Sigma''' \,|_{{\gamma_{\mathtt{w}}}'})$ and ${\gamma_{\mathtt{w}}}' \subseteq \gamma_{\mathtt{w}}$, we have $\mathit{dom}\,(\Sigma''') = \mathit{dom}\,(\Sigma''' \,|_{\gamma_{\mathtt{w}}})$. For $i \in \{1, 2\}$, since ${\gamma_{\mathtt{w}}}' \subseteq \gamma_{\mathtt{w}}$ and $\mu_i \,|_{{\gamma_{\mathtt{w}}}'^{c}} = \mu'''_i \,|_{{\gamma_{\mathtt{w}}}'^{c}}$, we have $\mu_i \,|_{{\gamma_{\mathtt{w}}}^{c}} = \mu'''_i \,|_{{\gamma_{\mathtt{w}}}^{c}}$ by Lemma 146 (2).
We show $\mu'''_1 \models A'''_1, A$. Since $\mu'''_1 \models A'''_1$, it suffices to show that $\mu'''_1 \models A$. By Lemma 88, it suffices to show that $\mu'''_1 \,|_{{\gamma_{\mathtt{r}}}''} \models A$. Since c'_1 and A are well typed and formed, we have ${\gamma_{\mathtt{w}}}', {\gamma_{\mathtt{r}}}'' \subseteq \gamma$. Thus, since $\Sigma; \gamma; \emptyset \vdash {\gamma_{\mathtt{r}}}'' \,\mathsf{disj}\, {\gamma_{\mathtt{w}}}'$, we have ${\gamma_{\mathtt{r}}}'' \cap {\gamma_{\mathtt{w}}}' = \emptyset$. Hence, ${\gamma_{\mathtt{r}}}'' \subseteq {{\gamma_{\mathtt{w}}}'}^{C}$. Since $\mu_1 \,|_{{\gamma_{\mathtt{w}}}'^{c}} = \mu'''_1 \,|_{{\gamma_{\mathtt{w}}}'^{c}}$, we have $\mu_1 \,|_{{\gamma_{\mathtt{r}}}''} = \mu'''_1 \,|_{{\gamma_{\mathtt{r}}}''}$ by Lemma 146 (1). Thus, it suffices to show that $\mu_1 \,|_{{\gamma_{\mathtt{r}}}''} \models A$. Since $\gamma \vdash \mu_1 \,|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \,:\, \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$ from well formedness of μ_1, and ${\gamma_{\mathtt{r}}}'' \subseteq \gamma_{\mathtt{r}}$, we have $\gamma \vdash \mu_1 \,|_{{\gamma_{\mathtt{r}}}''} \,:\, \Sigma^{{\gamma_{\mathtt{r}}}''}$ by Lemma 70. Since $\Sigma; \gamma; \emptyset \vdash^{\langle {\gamma_{\mathtt{r}}}'', \emptyset \rangle} A$ and $\mu_1 \models A$ (from $\mu_1 \models A'_1, A$), we finish by Lemma 98.

Case (C_CBlame): We are given $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid \Uparrow\ell'$ for some ℓ' by (C_CBlame). By Lemma 133 and (AEC_Blame), we finish.

Case (C_Region): We are given $c'_1 = \nu r.\, c''_1$ for some r and c''_1, and $\mu_1 \mid c_1 \longrightarrow^* \mu_1 \mid \nu r.\, (y \leftarrow \mathsf{do}\; c''_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\; y)$. Since $\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle \subseteq \langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle$, we have $\gamma \vdash \mu_1 \,|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \sim \mu_2 \,|_{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'} \,:\, \Sigma^{{\gamma_{\mathtt{r}}}' \cup {\gamma_{\mathtt{w}}}'}$. Since $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c''_1 \sim c_2 \,:\, \{A'_1\} x{:}T\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$ and $\mu_1 \models A'_1$ (from $\mu_1 \models A'_1, A$), there exist some c''_2 and A''_1 such that

* $\mu_2 \mid c_2 \longrightarrow^* \mu_2 \mid \nu r.\, c''_2$ where the computation does not mutate contents in μ_2,
* $\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, c''_1 \sim \nu r.\, c''_2 \,:\, \{A''_1\} x{:}T\{A'_2\}^{\langle {\gamma_{\mathtt{r}}}', {\gamma_{\mathtt{w}}}' \rangle}$, and
* $\mu_1 \models A''_1$

by Lemma 138. By (AEC_Frame),

$$\mu_1; \Sigma; \gamma; \emptyset \vdash y \leftarrow \mathsf{do}\,(\nu r.\, c''_1); \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\; y \sim \nu r.\, c''_2 \,:\, \{A''_1, A\} x{:}T\{A'_2, A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

By Lemma 136,

$$\mu_1; \Sigma; \gamma; \emptyset \vdash \nu r.\, (y \leftarrow \mathsf{do}\; c''_1; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\; y) \sim \nu r.\, c''_2 \,:\, \{A''_1, A\} x{:}T\{A'_2, A\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}.$$

Since $\mu_1 \models A$ (from $\mu_1 \models A'_1, A$) and $\mu_1 \models A''_1$, we have $\mu_1 \models A''_1, A$.

3. We are given

- $\mu_1; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle \sim \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle \,:\, T^{\gamma''}$,
- $\gamma \vdash \mu_1 \,|_{\gamma''} \sim \mu_2 \,|_{\gamma''} \,:\, \Sigma^{\gamma''}$, and
- $\mu_1 \mid \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle \hookrightarrow p''_1$.

Without loss of generality, we can suppose that $\mathit{dom}\,(\mu_1 \,|_{\gamma'}) = \emptyset$ and $\mathit{dom}\,(\mu_2 \,|_{\gamma'}) = \emptyset$. By inversion of $\mu_1; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu'_1 \mid c'_1 \rangle \sim \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle \,:\, T^{\gamma''}$, there exist some Σ' and A_1 such that

- $\gamma, \gamma' \vdash \mu_1' \sim \mu_2' \ : \ (\Sigma, \Sigma')^{\gamma'}$ and
- $\mu_1 \uplus \mu_1'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash c_1' \sim c_2' \ : \ \{A_1\}\, T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$.

From well typedness of $\nu\gamma'.\langle \mu_1' \mid c_1' \rangle$, we have $\mu_1 \uplus \mu_1' \models A_1$. Since $\gamma \vdash \mu_1|_{\gamma''} \sim \mu_2|_{\gamma''} \ : \ \Sigma^{\gamma''}$ and $\mu_1; \Sigma; \gamma \vdash \nu\gamma'.\langle \mu_1' \mid c_1' \rangle \sim \nu\gamma'.\langle \mu_2' \mid c_2' \rangle \ : \ T^{\gamma''}$, we have

$$\gamma, \gamma' \vdash (\mu_1 \uplus \mu_1')|_{\gamma' \cup \gamma''} \sim (\mu_2 \uplus \mu_2')|_{\gamma' \cup \gamma''} \ : \ (\Sigma, \Sigma')^{\gamma' \cup \gamma''}$$

by Lemma 144. By case analysis on the rule applied to evaluate $\nu\gamma'.\langle \mu_1' \mid c_1' \rangle$.

Case (P_Comput): We are given $\mu_1 \uplus \mu_1' \mid c_1' \longrightarrow \mu_1 \uplus \mu_1''' \mid c_1'''$ for some μ_1''' and c_1'''. By the IH (case (2)), there exist some Σ'', A_1'', μ_1'', c_1'', μ_2'', and c_2'' such that

- $\mu_1 \uplus \mu_1''' \mid c_1''' \longrightarrow^* \mu_1 \uplus \mu_1'' \mid c_1''$,
- $\mu_2 \uplus \mu_2' \mid c_2' \longrightarrow^* \mu_2 \uplus \mu_2'' \mid c_2''$,
- $\mu_1 \uplus \mu_1''; \Sigma, \Sigma', \Sigma''; \gamma, \gamma'; \emptyset \vdash c_1'' \sim c_2'' \ : \ \{A_1''\}\, T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$,
- $\gamma, \gamma' \vdash (\mu_1 \uplus \mu_1'')|_{\gamma' \cup \gamma''} \sim \mu_2 \uplus \mu_2''|_{\gamma' \cup \gamma''} \ : \ (\Sigma, \Sigma', \Sigma'')^{\gamma' \cup \gamma''}$,
- $\mathit{dom}\,(\Sigma'') = \mathit{dom}\,(\Sigma''|_{\gamma'})$, and
- $(\mu_i \uplus \mu_i')|_{\gamma'^c} = (\mu_i \uplus \mu_i'')|_{\gamma'^c}$ for $i \in \{1, 2\}$.

Note that c_1''' and c_2' mutate only references with regions in γ' and μ_1 and μ_2 do not include such addresses. By (AEP), it suffices to show that

$$\gamma, \gamma' \vdash \mu_1'' \sim \mu_2'' \ : \ (\Sigma, \Sigma', \Sigma'')^{\gamma'},$$

which is derived by the followings.

- We show that $\mathit{dom}\,(\mu_1'') = \mathit{dom}\,(\mu_2'')$. let $a@r \in \mathit{dom}\,(\mu_1'')$. If $r \in \gamma'$, then, since $\gamma, \gamma' \vdash (\mu_1 \uplus \mu_1'')|_{\gamma' \cup \gamma''} \sim \mu_2 \uplus \mu_2''|_{\gamma' \cup \gamma''} \ : \ (\Sigma, \Sigma', \Sigma'')^{\gamma' \cup \gamma''}$, we have $a@r \in \mathit{dom}\,((\mu_2 \uplus \mu_2'')|_{\gamma' \cup \gamma''})$. Since $\mathit{dom}\,(\mu_2|_{\gamma'}) = \emptyset$, we have $a@r \in \mathit{dom}\,(\mu_2''|_{\gamma' \cup \gamma''}) \subseteq \mathit{dom}\,(\mu_2'')$. Otherwise, if $r \notin \gamma'$, then, since $(\mu_1 \uplus \mu_1')|_{\gamma'^c} = (\mu_1 \uplus \mu_1'')|_{\gamma'^c}$, we have $a@r \in \mathit{dom}\,(\mu_1')$. However, since $\gamma, \gamma' \vdash \mu_1' \sim \mu_2' \ : \ (\Sigma, \Sigma')^{\gamma'}$, $a@r \in \mathit{dom}\,((\Sigma, \Sigma')|_{\gamma'})$, that is, $r \in \gamma'$, which is contradictory.
  The converse is shown similarly.
- We show that $[\mathit{dom}(mu1'') = \mathit{dom}((Sig, Sig', Sig'')|rset')]$. Let $a@r \in \mathit{dom}\,(\mu_1'')$. If $r \in \gamma'$, then we finish from $\gamma, \gamma' \vdash (\mu_1 \uplus \mu_1'')\,|_{\gamma' \cup \gamma''} \sim \mu_2 \uplus \mu_2''\,|_{\gamma' \cup \gamma''} \ : \ (\Sigma, \Sigma', \Sigma'')^{\gamma' \cup \gamma''}$. Otherwise, if $r \notin \gamma'$, then, since $(\mu_1 \uplus \mu_1')\,|_{\gamma'^c} = (\mu_1 \uplus \mu_1'')\,|_{\gamma'^c}$, we have $a@r \in \mathit{dom}\,(\mu_1')$. However, since $\gamma, \gamma' \vdash \mu_1' \sim \mu_2' \ : \ (\Sigma, \Sigma')^{\gamma'}$, $a@r \in \mathit{dom}\,((\Sigma, \Sigma')|_{\gamma'})$, that is, $r \in \gamma'$, which is contradictory.
  Let $a@r \in \mathit{dom}\,((\Sigma, \Sigma', \Sigma'')\,|_{\gamma'})$. Since $\gamma, \gamma' \vdash (\mu_1 \uplus \mu_1'')\,|_{\gamma' \cup \gamma''} \sim \mu_2 \uplus \mu_2''\,|_{\gamma' \cup \gamma''} \ : \ (\Sigma, \Sigma', \Sigma'')^{\gamma' \cup \gamma''}$ and $\mathit{dom}\,(\mu_1|_{\gamma'}) = \emptyset$, we finish.
- We show that, for any $a@r \in \mathit{dom}\,(\mu_1'')$, $\Sigma, \Sigma', \Sigma''; \gamma, \gamma'; \emptyset \vdash \mu_1''(a@r) \sim \mu_2''(a@r) \ : \ (\Sigma, \Sigma', \Sigma'')(a@r)$, which is derived from $\gamma, \gamma' \vdash (\mu_1 \uplus \mu_1'')|_{\gamma' \cup \gamma''} \sim \mu_2 \uplus \mu_2''|_{\gamma' \cup \gamma''} \ : \ (\Sigma, \Sigma', \Sigma'')^{\gamma' \cup \gamma''}$ since $a@r \in \mathit{dom}\,((\Sigma, \Sigma', \Sigma'')|_{\gamma'})$ and $a@r \in \mathit{dom}\,(\mu_2'')$ from the discussion above.

Case (P_Region): We are given $c_1' = \nu r.\, c_1''$ for some r and c_1''. Without loss of generality, we can suppose that $r \notin \gamma \cup \gamma'$ and $\mathit{dom}\,(\Sigma|_{\{r\}}) = \emptyset$ and $\mathit{dom}\,(\Sigma'|_{\{r\}}) = \emptyset$. By (P_Region), $\mu_1 \mid \nu\gamma'.\langle \mu_1' \mid \nu r.\, c_1'' \rangle \hookrightarrow \nu\gamma', r.\langle \mu_1' \mid c_1'' \rangle$. Since $\mu_1 \uplus \mu_1'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \nu r.\, c_1'' \sim c_2' \ : \ \{A_1\}\, T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$, there exist some c_2'' and A_1'' such that

- $\mu_2 \uplus \mu_2' \mid c_2' \longrightarrow^* \mu_2 \uplus \mu_2' \mid \nu r.\, c_2''$ where the computation does not mutate contents in $\mu_2 \uplus \mu_2'$,
- $\mu_1 \uplus \mu_1'; \Sigma, \Sigma'; \gamma, \gamma'; \emptyset \vdash \nu r.\, c_1'' \sim \nu r.\, c_2'' \ : \ \{A_1''\}\, T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle}$, and
- $\mu_1 \models A_1''$.

By (P_Comput) and (P_Region), $\mu_2 \mid \nu\gamma'.\langle \mu_2' \mid c_2' \rangle \hookrightarrow^* \nu\gamma', r.\langle \mu_2' \mid c_2'' \rangle$. Since $\mathit{dom}\,(\Sigma \mid_{\{r\}}) = \emptyset$ and $\mathit{dom}\,(\Sigma' \mid_{\{r\}}) = \emptyset$, we have $\mathit{dom}\,((\Sigma, \Sigma')\,|_{\gamma'}) = \mathit{dom}\,((\Sigma, \Sigma')\,|_{\gamma' \cup \{r\}})$. Thus, since $\gamma, \gamma' \vdash \mu_1' \sim \mu_2' \ : \ (\Sigma, \Sigma')^{\gamma'}$, we have $\gamma, \gamma', r \vdash \mu_1' \sim \mu_2' \ : \ (\Sigma, \Sigma')^{\gamma' \cup \{r\}}$ by Lemma 101 (3). If $\mu_1 \uplus \mu_1'; \Sigma, \Sigma'; \gamma, \gamma', r; \emptyset \vdash c_1'' \sim c_2'' \ : \ \{A_1''\}\, T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle \uplus \{r\}}$, then we finish by (AEP).

Otherwise, by Lemma 134, there exist $C^{\mathtt{c}'''}_{\mathtt{n}1}$, $C^{\mathtt{c}'''}_{\mathtt{n}2}$, c_1''', c_2''', s, y, z, ℓ, A_1''', x, T''', A_2''', and ϱ''' such that

- $c_1'' = C^{\mathtt{c}'''}_{\mathtt{n}1}[\,\mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathsf{not}\,(r == s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true};\, c_1'''\,]$,
- $c_2'' = C^{\mathtt{c}'''}_{\mathtt{n}2}[\,\mathsf{let}\, y = \mathsf{true};\, c_2'''\,]$,
- $s \in (\gamma, \gamma')$,

- $\Sigma, \Sigma'; \gamma, \gamma', r \vdash C^{\mathsf{c}'''}_{\mathtt{n1}} \sim C^{\mathsf{c}'''}_{\mathtt{n2}} \ : \ \{A'''_1\}x{:}T'''\{A'''_2\}^{\varrho''' \uplus \{r\}} \Rightarrow \{A''_1\}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle \uplus \{r\}}$,
- $\mu_1 \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma', r; y{:}\{z{:}\mathsf{bool} \mid \mathtt{not}\,(r \mathrel{==} s)\} \vdash c'''_1 \sim c'''_2 \ : \ \{A'''_1\}x{:}T'''\{A'''_2\}^{\varrho''' \uplus \{r\}}$, and
- $\Sigma, \Sigma'; \gamma, \gamma', r; \emptyset \vdash \{A'''_1\}x{:}T'''\{A'''_2\}^{\varrho''' \uplus \{r\}}$.

Since $r \notin \gamma \cup \gamma'$ and $s \in (\gamma, \gamma')$, $r \neq s$, so we have $r \mathrel{==} s \rightsquigarrow \mathsf{false}$. Thus, $\mu_1 \uplus \mu'_1 \mid \mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathtt{not}\,(r \mathrel{==} s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c'''_1 \longrightarrow^{*} \mu_1 \uplus \mu'_1 \mid [\mathsf{true}/y]\, c'''_1$. Obviously, $\mu_2 \uplus \mu'_2 \mid \mathsf{let}\, y = \mathsf{true}; c'''_2 \longrightarrow^{*} \mu_2 \uplus \mu'_2 \mid [\mathsf{true}/y]\, c'''_2$. Since $c''_1 = C^{\mathsf{c}'''}_{\mathtt{n1}}[\mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \mathtt{not}\,(r \mathrel{==} s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c'''_1]$ and $c''_2 = C^{\mathsf{c}'''}_{\mathtt{n2}}[\mathsf{let}\, y = \mathsf{true}; c'''_2]$, we have, for $i \in \{1,2\}$ $\mu_i \uplus \mu'_i \mid c''_i \longrightarrow \mu_i \uplus \mu'_i \mid C^{\mathsf{c}'''}_{\mathtt{n}i}[[\mathsf{true}/y]\, c'''_i]$ by Lemma 148, and so

$$\mu_i \mid \nu\gamma'.\langle \mu'_i \mid \nu r.\, c''_i \rangle \hookrightarrow^{*} \nu\gamma', r.\langle \mu'_i \mid C^{\mathsf{c}'''}_{\mathtt{n}i}[[\mathsf{true}/y]\, c'''_i] \rangle$$

by (P_Comput). Since $\Sigma, \Sigma'; \gamma, \gamma', r; \emptyset \vdash \mathsf{true} \sim \mathsf{true} \ : \ \{z{:}\mathsf{bool} \mid \mathtt{not}\,(r \mathrel{==} s)\}$ by (AEC_Const) and (AEC_Exact) (note that true can be typed at $\{z{:}\mathsf{bool} \mid \mathtt{not}\,(r \mathrel{==} s)\}$), we have

$$\mu_1 \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma', r; \emptyset \vdash [\mathsf{true}/y]\, c'''_1 \sim [\mathsf{true}/y]\, c'''_2 \ : \ \{A'''_1\}x{:}T'''\{A'''_2\}^{\varrho''' \uplus \{r\}}$$

by Lemma 110 (4). Note that, since $\Sigma, \Sigma'; \gamma, \gamma', r; \emptyset \vdash \{A'''_1\}x{:}T'''\{A'''_2\}^{\varrho''' \uplus \{r\}}$, y does not occur free in $\{A'''_1\}x{:}T'''\{A'''_2\}^{\varrho''' \uplus \{r\}}$. By Lemma 147,

$$\mu_1 \uplus \mu'_1; \Sigma, \Sigma'; \gamma, \gamma', r; \emptyset \vdash C^{\mathsf{c}'''}_{\mathtt{n1}}[[\mathsf{true}/y]\, c'''_1] \sim C^{\mathsf{c}'''}_{\mathtt{n2}}[[\mathsf{true}/y]\, c'''_2] \ : \ \{A''_1\}T\{\top\}^{\langle \gamma' \cup \gamma'', \gamma' \rangle \uplus \{r\}}.$$

Thus, by (AEP),

$$\mu_1; \Sigma; \gamma \vdash \nu\gamma', r.\langle \mu'_1 \mid C^{\mathsf{c}'''}_{\mathtt{n1}}[[\mathsf{true}/y]\, c'''_1] \rangle \sim \nu\gamma', r.\langle \mu'_2 \mid C^{\mathsf{c}'''}_{\mathtt{n2}}[[\mathsf{true}/y]\, c'''_2] \rangle \ : \ T^{\gamma''}.$$

□

Lemma 150.

(1) If $\Sigma; \gamma; \emptyset \vdash e_1 \sim e_2 \ : \ T$ and $e_2 \longrightarrow e''_2$, then there exist some e'_1 and e'_2 such that

- $e''_2 \longrightarrow^{*} e'_2$,
- $e_1 \longrightarrow^{*} e'_1$, *and*
- $\Sigma; \gamma; \emptyset \vdash e'_1 \sim e'_2 \ : \ T$.

(2) If

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim c_2 \ : \ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$,
- $\gamma \vdash \mu_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ : \ \Sigma^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$,
- $\mu_1 \models A_1$, *and*
- $\mu_2 \mid c_2 \longrightarrow \mu''_2 \mid c''_2$,

then there exist some Σ', A'_1, μ'_1, c'_1, μ'_2, and c'_2 such that:

- $\mu''_2 \mid c''_2 \longrightarrow^{*} \mu'_2 \mid c'_2$;
- $\mu_1 \mid c_1 \longrightarrow^{*} \mu'_1 \mid c'_1$;
- $\mu'_1; \Sigma, \Sigma'; \gamma; \emptyset \vdash c'_1 \sim c'_2 \ : \ \{A'_1\}x{:}T\{A_2\}^{\langle \gamma_{\mathtt{r}}, \gamma_{\mathtt{w}} \rangle}$;
- $\gamma \vdash \mu'_1|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \sim \mu'_2|_{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}} \ : \ (\Sigma, \Sigma')^{\gamma_{\mathtt{r}} \cup \gamma_{\mathtt{w}}}$;
- $\mu'_1 \models A'_1$;
- *dom* $(\Sigma') = $ *dom* $(\Sigma'|_{\gamma_{\mathtt{w}}})$;
- $\mu_i|_{\gamma_{\mathtt{w}}^{c}} = \mu'_i|_{\gamma_{\mathtt{w}}^{c}}$ *for* $i \in \{1,2\}$;
- *contents of μ''_2 and μ_1 are mutated only if their addresses are associated with regions in $\gamma_{\mathtt{w}}$.*

(3) If

- $\mu_1; \Sigma; \gamma \vdash p_1 \sim p_2 \ : \ T^{\gamma'}$,
- $\gamma \vdash \mu_1|_{\gamma'} \sim \mu_2|_{\gamma'} \ : \ \Sigma^{\gamma'}$, *and*
- $\mu_2 \mid p_2 \hookrightarrow p''_2$,

then there exist some p'_1 and p'_2 such that

- $\mu_2 \mid p''_2 \hookrightarrow^* p'_2$,
- $\mu_1 \mid p_1 \hookrightarrow^* p'_1$, *and*
- $\mu_1; \Sigma; \gamma \vdash p'_1 \sim p'_2 \;:\; T^{\gamma'}$.

Proof. Similarly to Lemma 149. □

Lemma 151.

(1) If $\Sigma; \gamma; \emptyset \vdash e_1 \sim e_2 \;:\; T$, then:

- $e_2 \longrightarrow e'_2$ *for some* e'_2*;*
- e_2 *is a value; or*
- $e_2 \;=\; E_2[\Uparrow\ell]$ *for some* E_2 *and* ℓ*.*

(2) Suppose that

- $\mu_1; \Sigma; \gamma; \emptyset \vdash c_1 \sim c_2 \;:\; \{A_1\}x{:}T\{A_2\}^{\langle \gamma_\mathtt{r}, \gamma_\mathtt{w} \rangle}$ *and*
- $\gamma \vdash \mu_1|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \sim \mu_2|_{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}} \;:\; \Sigma^{\gamma_\mathtt{r} \cup \gamma_\mathtt{w}}$.

Let

- $\mu_{21} = \mu_2|_{\gamma_\mathtt{w}{}^c}$ *and*
- $\mu_{22} = \mu_2|_{\gamma_\mathtt{w}}$.

Then, there exist some μ'_{22} and c'_2 such that

- $\mu_{21} \uplus \mu_{22} \mid c_2 \longrightarrow \mu_{21} \uplus \mu'_{22} \mid c'_2$ *for some* μ'_{22} *and* c'_2*, or*
- c_2 *takes one of:*
  (a) $\nu r.\, c'_2$ *for some* c'_2*;*
  (b) $\mathsf{return}\, v_2$ *for some* v_2*; or*
  (c) $\Uparrow\ell$ *for some* ℓ*.*

(3) If $\mu_1; \Sigma; \gamma \vdash p_1 \sim p_2 \;:\; T^{\gamma'}$ and $\gamma \vdash \mu_1|_{\gamma'} \sim \mu_2|_{\gamma'} \;:\; \Sigma^{\gamma'}$, then:

- $\mu \mid p_2 \hookrightarrow p'_2$ *for some* p'_2*; or*
- p'_2 *is*
  (a) $\nu\gamma''.\langle \mu'_2 \mid \mathsf{return}\, v'_2 \rangle$ *for some* γ''*,* μ'_2*, and* v_2*, or*
  (b) $\nu\gamma''.\langle \mu'_2 \mid \Uparrow\ell' \rangle$ *for some* γ''*,* μ'_2*, and* ℓ'*.*

Proof. Similarly to Lemma 149, we show it by lexicographical induction on pairs of the size of $e_1/c_1/p_1$ and the correspoinding derivation. We mention only the case for (AEC_ElimAssert). In that case, we are given $\mu_1; \Sigma; \gamma; \emptyset \vdash \mathsf{assert}\,(c_{11})^\ell; c_{12} \sim c_2 \;:\; \{A_1\}x{:}T\{A_2\}^\varrho$ and, by inversion, $\emptyset; \Sigma; \gamma; \emptyset \vdash c_{12} \sim c_2 \;:\; \{A_1, c_{11}\}x{:}T\{A_2\}^\varrho$. By Lemma 107, $\mu_1; \Sigma; \gamma; \emptyset \vdash c_{12} \sim c_2 \;:\; \{A_1, c_{11}\}x{:}T\{A_2\}^\varrho$. Since the size of c_{12} is less than $\mathsf{assert}\,(c_{11})^\ell; c_{12}$, we finish by the IH. □

Lemma 152. *If $\emptyset; \emptyset; \emptyset; \emptyset \vdash c_1 \sim c_2 \;:\; \{\top\}T\{\top\}^{\langle \emptyset, \emptyset \rangle}$, then $c_1 \Downarrow c_2$.*

Proof. First, we show $c_1 \mid \Uparrow\ell$ iff $c_2 \mid \Uparrow\ell$. Suppose that $c_1 \mid \Uparrow\ell$. Then, we have $\emptyset \mid \nu\emptyset.\langle \emptyset \mid c_1 \rangle \hookrightarrow^* \nu\gamma'.\langle \mu'_1 \mid \Uparrow\ell \rangle$. By (AEP), $\emptyset; \emptyset; \emptyset \vdash \nu\emptyset.\langle \emptyset \mid c_1 \rangle \sim \nu\emptyset.\langle \emptyset \mid c_2 \rangle \;:\; T^\emptyset$. By induction on the number of computation steps of $\nu\emptyset.\langle \emptyset \mid c_1 \rangle$ with Lemma 149 (3), there exist some μ'_2, c'_2, Σ', and A'_1 such that

- $\emptyset \mid \nu\emptyset.\langle \emptyset \mid c_2 \rangle \hookrightarrow^* \nu\gamma'.\langle \mu'_2 \mid c'_2 \rangle$,
- $\mu'_1; \Sigma'; \gamma'; \emptyset \vdash \Uparrow\ell \sim c'_2 \;:\; \{A'_1\}T\{\top\}^{\langle \gamma', \gamma' \rangle}$,
- $\gamma' \vdash \mu'_1 \sim \mu'_2 \;:\; \Sigma'^{\gamma'}$, and
- $\mu'_1 \models A'_1$.

By Lemma 133, we have $\mu'_2 \mid c'_2 \longrightarrow^* \mu'_2 \mid \Uparrow\ell$ where the computation does not mutate contents in μ'_2. Thus, by (P_Comput), $c_2 \mid \Uparrow\ell$. The other direction, i.e., implication from $c_2 \mid \Uparrow\ell$ to $c_1 \mid \Uparrow\ell$, is shown similarly with Lemma 150.

Next, we show $c_1 \mid \mathsf{stuck}$ iff $c_2 \mid \mathsf{stuck}$. Since c_1 is well typed, it does not get stuck by Lemma 73 and Lemma 95. By Lemmas 151 (3) and 150 (3), c_2 also does not get stuck. □

Lemma 153. *If* $\emptyset; \emptyset; \gamma; \Gamma \vdash c_1 \sim c_2 \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$*, then* $\gamma; \Gamma \vdash c_1 =_{\texttt{ctx}} c_2 \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$*.*

Proof. From well typedness of c_1, $\emptyset; \emptyset; \gamma; \Gamma \vdash c_1 \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$. It is easy to show that all term and region variables in c_2 are contained by Γ and γ by induction on the derivation of $\emptyset; \emptyset; \gamma; \Gamma \vdash c_1 \sim c_2 \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$. Since $\sim$ is compatible, we have $\emptyset; \emptyset; \emptyset; \emptyset \vdash K^{\mathrm{c}}[\,c_1\,] \sim K^{\mathrm{c}}[\,c_2\,] \ : \ \{\top\}T'\{\top\}^{\langle\emptyset,\emptyset\rangle}$ for any K^{c} and T' such that $\emptyset; \emptyset; \emptyset; \emptyset \vdash K^{\mathrm{c}}[\,c_1\,] \ : \ \{\top\}T'\{\top\}^{\langle\emptyset,\emptyset\rangle}$. By Lemma 152, $K^{\mathrm{c}}[\,c_1\,] \Downarrow K^{\mathrm{c}}[\,c_2\,]$. □

Lemma 154 (Precondition Assertion Elimination)**.** *Suppose that* $\gamma; \Gamma \vdash c \ : \ \{A_1, c_1\}x{:}T\{A_2\}^{\varrho}$*. Let* c_1 *be a computation such that there exist some* A'_1 *and* ϱ' *such that*

- $A'_1 \subseteq A_1$*,*
- $\varrho' \subseteq \varrho$*,*
- $\gamma; \Gamma \vdash^{\varrho'} A'_1, c_1$*, and*
- *for any* μ *and* σ*, if* $\emptyset; \gamma; \Gamma \vdash \langle \mu, \sigma \rangle^{\varrho'}$ *and* $\mu \models \sigma(A'_1)$*, then* $\mu \models \sigma(c_1)$*.*

Then, $\gamma; \Gamma \vdash \mathsf{assert}\,(c_1)^{\ell}; c =_{\texttt{ctx}} c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$*.*

Proof. Since $\sim$ is compatible, we have $\emptyset; \emptyset; \gamma; \Gamma \vdash c \sim c \ : \ \{A_1, c_1\}x{:}T\{A_2\}^{\varrho}$. By (AEC_ElimAssert), $\emptyset; \emptyset; \gamma; \Gamma \vdash \mathsf{assert}\,(c_1)^{\ell}; c \sim c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$. Thus, by Lemma 153, we finish. □

Lemma 155 (Postcondition Assertion Elimination)**.** *Suppose that* $\gamma; \Gamma \vdash c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$*. Let* c_2 *be a computation such that there exist some* A'_2 *and* ϱ' *such that*

- $A'_2 \subseteq A_2$*,*
- $\varrho' \subseteq \varrho$*,*
- $\gamma; \Gamma, x{:}T \vdash^{\varrho'} A'_2, c_2$*, and*
- *for any* μ *and* σ*, if* $\emptyset; \gamma; \Gamma, x{:}T \vdash \langle \mu, \sigma \rangle^{\varrho'}$ *and* $\mu \models \sigma(A'_2)$*, then* $\mu \models \sigma(c_2)$*.*

Then, $\gamma; \Gamma \vdash x \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(c_2)^{\ell}; \mathsf{return}\, x =_{\texttt{ctx}} c \ : \ \{A_1\}x{:}T\{A_2, c_2\}^{\varrho}$*.*

Proof. Since c is contextually equivalent to $x \leftarrow \mathsf{do}\, c; \mathsf{return}\, x$, it suffices to show that

$$\gamma; \Gamma \vdash x \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(c_2)^{\ell}; \mathsf{return}\, x =_{\texttt{ctx}} x \leftarrow \mathsf{do}\, c; \mathsf{return}\, x \ : \ \{A_1\}x{:}T\{A_2, c_2\}^{\varrho}.$$

By (AETm_Var) and (AEC_Return), we have

$$\emptyset; \emptyset; \gamma; \Gamma, x{:}T \vdash \mathsf{return}\, x \sim \mathsf{return}\, x \ : \ \{A_2, c_2\}x{:}T\{A_2, c_2\}^{\varrho}.$$

By (AEC_ElimAssert),

$$\emptyset; \emptyset; \gamma; \Gamma, x{:}T \vdash \mathsf{assert}\,(c_2)^{\ell}; \mathsf{return}\, x \sim \mathsf{return}\, x \ : \ \{A_2\}x{:}T\{A_2, c_2\}^{\varrho}.$$

Since $\sim$ is compatible, $\emptyset; \emptyset; \gamma; \Gamma \vdash c \sim c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$. Thus, by (AETm_Do) and (AEC_Bind),

$$\emptyset; \emptyset; \gamma; \Gamma \vdash x \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(c_2)^{\ell}; \mathsf{return}\, x \sim x \leftarrow \mathsf{do}\, c; \mathsf{return}\, x \ : \ \{A_1\}x{:}T\{A_2, c_2\}^{\varrho}.$$

Thus, by Lemma 153, we finish. □

Lemma 156 (Semantic Weakening)**.** *Suppose that* $\gamma; \Gamma \vdash c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$*. Let* A'_1 *and* A'_2 *be assertions such that*

- $\gamma; \Gamma \vdash^{\varrho} A'_1$*,*
- $\gamma; \Gamma, x{:}T \vdash^{\varrho} A'_2$*,*
- *for any* μ *and* σ*, if* $\emptyset; \gamma; \Gamma \vdash \langle \mu, \sigma \rangle^{\varrho'}$ *and* $\mu \models \sigma(A'_1)$*, then* $\mu \models \sigma(A_1)$*, and*
- *for any* μ *and* σ*, if* $\emptyset; \gamma; \Gamma, x{:}T \vdash \langle \mu, \sigma \rangle^{\varrho'}$ *and* $\mu \models \sigma(A_2)$*, then* $\mu \models \sigma(A'_2)$*.*

Then, $\gamma; \Gamma \vdash \mathsf{assert}\,(A_1)^{\ell_1}; x \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(A'_2)^{\ell_2}; \mathsf{return}\, x =_{\texttt{ctx}} c \ : \ \{A'_1\}x{:}T\{A'_2\}^{\varrho}$*.*

Proof. Since c is contextually equivalent to $x \leftarrow \mathsf{do}\, c; \mathsf{return}\, x$, it suffices to show that

$$\gamma; \Gamma \vdash \mathsf{assert}\,(A_1)^{\ell_1}; x \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(A_2')^{\ell_2}; \mathsf{return}\, x =_{\texttt{ctx}} x \leftarrow \mathsf{do}\, c; \mathsf{return}\, x \ : \ \{A_1'\}x{:}T\{A_2'\}^{\varrho}$$

By (AETm_Var), (AEC_Return), and (AEC_Weak), we have

$$\emptyset; \emptyset; \gamma; \Gamma, x{:}T \vdash \mathsf{return}\, x \sim \mathsf{return}\, x \ : \ \{A_2, A_2'\}x{:}T\{A_2'\}^{\varrho}.$$

By (AEC_ElimAssert),

$$\emptyset; \emptyset; \gamma; \Gamma, x{:}T \vdash \mathsf{assert}\,(A_2')^{\ell_2}; \mathsf{return}\, x \sim \mathsf{return}\, x \ : \ \{A_2\}x{:}T\{A_2'\}^{\varrho}.$$

Since $\sim$ is compatible, $\emptyset; \emptyset; \gamma; \Gamma \vdash c \sim c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$. Thus, by (AETm_Do), (AEC_Bind), and (AEC_Weak),

$$\emptyset; \emptyset; \gamma; \Gamma \vdash x \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(A_2')^{\ell_2}; \mathsf{return}\, x \sim x \leftarrow \mathsf{do}\, c; \mathsf{return}\, x \ : \ \{A_1', A_1\}x{:}T\{A_2'\}^{\varrho}.$$

By (AEC_ElimAssert),

$$\emptyset; \emptyset; \gamma; \Gamma \vdash \mathsf{assert}\,(A_1)^{\ell_1}; x \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(A_2')^{\ell_2}; \mathsf{return}\, x \sim x \leftarrow \mathsf{do}\, c; \mathsf{return}\, x \ : \ \{A_1'\}x{:}T\{A_2'\}^{\varrho}.$$

Thus, we finish by Lemma 153. □

Lemma 157 (Local Reasoning)**.** *Suppose that* $\gamma; \Gamma \vdash c \ : \ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle}$. *Let A be an assertion such that there exist some ${\gamma_{\texttt{r}}}'$ such that*

- ${\gamma_{\texttt{r}}}' \subseteq \gamma_{\texttt{r}}$,
- $\gamma; \Gamma \vdash^{\langle {\gamma_{\texttt{r}}}', \emptyset \rangle} A$, *and*
- $\emptyset; \gamma; \Gamma \vdash {\gamma_{\texttt{r}}}' \, \mathsf{disj}\, \gamma_{\texttt{w}}$.

Then, $\gamma; \Gamma \vdash y \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y =_{\texttt{ctx}} c \ : \ \{A_1, A\}x{:}T\{A_2, A\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle}$ *for any variable* $y \notin fv\,(A)$.

Proof. Since $\sim$ is compatible, we have $\emptyset; \emptyset; \gamma; \Gamma \vdash c \sim c \ : \ \{A_1\}x{:}T\{A_2\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle}$. By (AEC_Frame), $\emptyset; \emptyset; \gamma; \Gamma \vdash y \leftarrow \mathsf{do}\, c; \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y \sim c \ : \ \{A_1, A\}x{:}T\{A_2, A\}^{\langle \gamma_{\texttt{r}}, \gamma_{\texttt{w}} \rangle}$. Thus, by Lemma 153, we finish. □

Lemma 158 (Recover Contract Information Lost By Assignment)**.** *Suppose that*

- $\gamma; \Gamma \vdash e_1 \ : \ \mathsf{Ref}_r\, T'$,
- $\gamma; \Gamma \vdash e_2 \ : \ T'$,
- $\gamma; \Gamma \vdash^{\langle \gamma_{\texttt{r}}, \emptyset \rangle} A$, *and*
- $\emptyset; \gamma; \Gamma \vdash \gamma_{\texttt{r}}\, \mathsf{disj}\, \{r\}$.

Then,

$$\gamma; \Gamma \vdash y \leftarrow (\mathsf{do}\, x \Leftarrow e_1 := e_2; \mathsf{return}\, ()); \mathsf{assert}\,(A)^{\ell}; \mathsf{return}\, y =_{\texttt{ctx}} x \Leftarrow e_1 := e_2; \mathsf{return}\, () \ : \ \{A\}x{:}T\{A\}^{\langle \gamma_{\texttt{r}}, \{r\} \rangle}.$$

Proof. Since the write effect in $x \Leftarrow e_1 := e_2; \mathsf{return}\, ()$ is $\{r\}$, we finish by Lemma 157. □

Lemma 159. *Let* $s \in \gamma \cup regions\,(\Gamma)$. *Suppose that* $\gamma, r; \Gamma, y{:}\{z{:}\mathsf{bool} \mid \texttt{not}\,(r == s)\} \vdash c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$ *and* $\gamma; \Gamma \vdash \{A_1\}x{:}T\{A_2\}^{\varrho}$. *Then,* $\gamma; \Gamma \vdash \nu r.\, \mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \texttt{not}\,(r == s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c =_{\texttt{ctx}} \nu r.\, \mathsf{let}\, y = \mathsf{true}; c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}$.

Proof. Since $\sim$ is compatible, we have $\emptyset; \emptyset; \gamma, r; \Gamma, y{:}\{z{:}\mathsf{bool} \mid \texttt{not}\,(r == s)\} \vdash c \sim c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho \uplus \{r\}}$. By (AEC_RegionNEq1),

$$\emptyset; \emptyset; \gamma; \Gamma \vdash \nu r.\, \mathsf{let}\, y = \langle \{z{:}\mathsf{bool} \mid \texttt{not}\,(r == s)\} \Leftarrow \mathsf{bool} \rangle^{\ell}\, \mathsf{true}; c \sim \nu r.\, \mathsf{let}\, y = \mathsf{true}; c \ : \ \{A_1\}x{:}T\{A_2\}^{\varrho}.$$

Thus, by Lemma 153, we finish. □