Big Types In Little Runtime

Supplemental material

Michael M. Vitousek Cameron Swords Jeremy G. Siek
Indiana University, USA
{mvitouse,cswords,jsiek}@indiana.edu

A. Appendix: Additional semantics

Figure A.1 shows the translation from $\lambda^{\star}_{\rightarrow}$ to $\lambda^{\Downarrow}_{\ell}$ including the insertion of origin markers, and is otherwise identical to Figure 3. Similarly,Figure A.2 shows the single-step reduction rules for $\lambda^{\Downarrow}_{\ell}$ with origin markers p included; otherwise it is identical to the rules shown in Figure 4.

Figure A.3 shows the precision relations for $\lambda^{\Downarrow}_{\ell}$ and $\lambda^{\star}_{\rightarrow}$ used in proving the gradual guarantee. Figure A.4 shows related auxiliary precision relations.

Figure A.5 shows the typing rules for $\lambda^{\Downarrow}_{\ell}$ expression contexts.

Figure A.6 shows blame safety predicates.

B. Appendix: Proofs

B.1 Open world soundness

Lemma B.1. *If* $\Gamma(x) = T$*, then* $\lfloor\Gamma\rfloor(x) = \lfloor T\rfloor$.

Proof. Straightforward induction on Γ. □

Lemma B.2. *If* $\Gamma; \Sigma \vdash e : S$ *and for all* $x \in dom(\Gamma)$, $\Gamma(x) = \Gamma'(x)$ *then* $\Gamma'; \Sigma \vdash e : S$.

Proof. Induction on $\Gamma; \Sigma \vdash e : S$. □

Lemma B.3 (Translation preserves types)**.** *For all* Γ, e_s, e, T*, if* $\Gamma \vdash e_s \rightsquigarrow e : T$*, then* $\lfloor\Gamma\rfloor; \emptyset \vdash e : \lfloor T\rfloor$.

Proof. By induction on $\Gamma \vdash e_s \rightsquigarrow e : T$.

Case CINT

$$\frac{}{\Gamma \vdash n \rightsquigarrow n : \mathsf{int}}$$

By TINT, $\lfloor\Gamma\rfloor; \emptyset \vdash n : \mathsf{int}$.

Case CVAR

$$\frac{\Gamma(x) = T}{\Gamma \vdash x \rightsquigarrow x : T}$$

By Lemma B.1, $\lfloor\Gamma\rfloor(x) = \lfloor T\rfloor$.
By TVAR, $\lfloor\Gamma\rfloor; \emptyset \vdash x : \lfloor T\rfloor$.

Case CADD

$$\frac{\begin{array}{c}\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T_1 \quad T_1 \sim \mathsf{int} \quad \mathrm{fresh}(\ell_1) \\ \Gamma \vdash e_{s2} \rightsquigarrow e_2 : T_2 \quad T_2 \sim \mathsf{int} \quad \mathrm{fresh}(\ell_2)\end{array}}{\Gamma \vdash e_{s1} \ + \ e_{s2} \rightsquigarrow (e_1 :: T_1 \Rightarrow^{\ell_1} \mathsf{int}) +^{\Diamond} (e_2 :: T_2 \Rightarrow^{\ell_2} \mathsf{int}) : \mathsf{int}}$$

By the IH, $\lfloor\Gamma\rfloor; \emptyset \vdash e_1 : \mathsf{int}$.
By the IH, $\lfloor\Gamma\rfloor; \emptyset \vdash e_2 : \mathsf{int}$.
By TPLUS, $\lfloor\Gamma\rfloor; \emptyset \vdash e_1 +^{\Diamond} e_2 : \mathsf{int}$.

Case CFUN

$$\frac{\Gamma, f : T_1 \to T_2, x : T_1 \vdash e_s \rightsquigarrow e' : T_2' \quad T_2 \sim T_2'}{\begin{array}{c}\Gamma \vdash \mathtt{fun}\ f\ (x{:}T_1) \to T_2.\ e_s \rightsquigarrow \\ \mathtt{fun}\ f\ x.\ (\mathtt{let}\ x = x{\Downarrow}\langle\lfloor T_1\rfloor; f; \textsc{Arg}\rangle\ \mathtt{in}\ e') : T_1 \to T_2\end{array}}$$

$\boxed{\Gamma \vdash e_s \rightsquigarrow e : T}$

$$\text{(CINT)}\frac{}{\Gamma \vdash n \rightsquigarrow n : \mathsf{int}} \qquad \text{(CVAR)}\frac{\Gamma(x) = T}{\Gamma \vdash x \rightsquigarrow x : T}$$

(CADD)
$$\frac{\begin{array}{c}\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T_1 \quad T_1 \sim \mathsf{int} \quad \mathrm{fresh}(\ell_1) \\ \Gamma \vdash e_{s2} \rightsquigarrow e_2 : T_2 \quad T_2 \sim \mathsf{int} \quad \mathrm{fresh}(\ell_2)\end{array}}{\Gamma \vdash e_{s1} \ + \ e_{s2} \rightsquigarrow (e_1 :: T_1 \Rightarrow^{\ell_1} \mathsf{int}) +^{\Diamond} (e_2 :: T_2 \Rightarrow^{\ell_2} \mathsf{int}) : \mathsf{int}}$$

(CFUN)
$$\frac{\Gamma, f : T_1 \to T_2, x : T_1 \vdash e_s \rightsquigarrow e' : T_2' \quad T_2 \sim T_2'}{\begin{array}{c}\Gamma \vdash \mathtt{fun}\ f\ (x{:}T_1) \to T_2.\ e_s \rightsquigarrow \\ \mathtt{fun}\ f\ x.\ (\mathtt{let}\ x = x{\Downarrow}\langle\lfloor T_1\rfloor; f; \textsc{Arg}\rangle\ \mathtt{in}\ e') : T_1 \to T_2\end{array}}$$

(CAPP)
$$\frac{\begin{array}{ccc}\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T & T \rhd T_1 \to T_2 & \mathrm{fresh}(f) \\ \Gamma \vdash e_{s2} \rightsquigarrow e_2 : T_1' & T_1 \sim T_1' & \mathrm{fresh}(\ell)\end{array}}{\begin{array}{c}\Gamma \vdash e_{s1}\ e_{s2} \rightsquigarrow \mathtt{let}\ f = e_1 :: T \Rightarrow^{\ell} T_1 \to T_2\ \mathtt{in} \\ (f\ (e_2 :: T_1' \Rightarrow^{\ell} T_1)^{\Diamond}){\Downarrow}\langle\lfloor T_2\rfloor; f; \textsc{Res}\rangle : T_2\end{array}}$$

$$\text{(CREF)}\frac{\Gamma \vdash e_s \rightsquigarrow e : T}{\Gamma \vdash \mathtt{ref}\ e_s \rightsquigarrow \mathtt{ref}\ e : \mathsf{ref}\ T}$$

(CDEREF)
$$\frac{\Gamma \vdash e_s \rightsquigarrow e : T \qquad T \rhd \mathsf{ref}\ T_1 \qquad \mathrm{fresh}(x) \qquad \mathrm{fresh}(\ell)}{\Gamma \vdash !e_s \rightsquigarrow \mathtt{let}\ x = e :: T \Rightarrow^{\ell} \mathsf{ref}\ T_1\ \mathtt{in}\ !x^{\Diamond}{\Downarrow}\langle\lfloor T_1\rfloor; x; \textsc{Deref}\rangle : T_1}$$

(CUPDTREF)
$$\frac{\begin{array}{ccc}\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T & T \rhd \mathsf{ref}\ T_1 & \mathrm{fresh}(\ell_1) \\ \Gamma \vdash e_{s2} \rightsquigarrow e_2 : T_1' & T_1 \sim T_1' & \mathrm{fresh}(\ell_2)\end{array}}{\Gamma \vdash e_{s1} := e_{s2} \rightsquigarrow (e_1 :: T \Rightarrow^{\ell_1} \mathsf{ref}\ T_1) :=^{\Diamond} (e_2 :: T_1' \Rightarrow^{\ell_2} T_1) : \mathsf{int}}$$

Figure A.1. Compilation from $\lambda^{\star}_{\rightarrow}$ to $\lambda^{\Downarrow}_{\ell}$ with origin markers.

By TVAR, $\lfloor\Gamma\rfloor, f{:}\to, x{:}\star; \emptyset \vdash x : \star$.
Let us assume that $x \neq f$.
Then by TVAR $\lfloor\Gamma\rfloor, f{:}\to, x{:}\star; \emptyset \vdash f :\to$.
By TCHECK,
$\lfloor\Gamma\rfloor, f{:}\to, x{:}\lfloor T_1\rfloor; \emptyset \vdash x{\Downarrow}\langle\lfloor T_1\rfloor; f; \textsc{Arg}\rangle : \lfloor T_1\rfloor$.
By the IH, $\lfloor\Gamma\rfloor, f{:}\to, x{:}\lfloor T_1\rfloor; \emptyset \vdash e' : \lfloor T_2'\rfloor$.
By Lemma B.2, $\lfloor\Gamma\rfloor, f{:}\to, x{:}\star, x{:}\lfloor T_1\rfloor; \emptyset \vdash e' : \lfloor T_2'\rfloor$.
By TLET,
$\lfloor\Gamma\rfloor, f{:}\to, x{:}\star; \emptyset \vdash \mathtt{let}\ x = x{\Downarrow}\langle\lfloor T_1\rfloor; f; \textsc{Arg}\rangle\ \mathtt{in}\ e' : \lfloor T_2'\rfloor$.
By TSUBSUMP,

$\boxed{\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \varsigma}$

$$
\begin{array}{lrll}
\text{(EFun)} & \langle \texttt{fun}\ f\ x.\ e, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto (\lambda x.e[a/f])], \mathcal{B}\rangle & \text{where } \mathrm{fresh}(a) \\
\text{(EApp)} & \langle a\ v^p, \sigma, \mathcal{B}\rangle \longrightarrow \langle e[v/x], \sigma, \mathcal{B}\rangle & \text{where } \sigma(a) = (\lambda x.e) \\
\\
\text{(ERef)} & \langle \texttt{ref}\ v, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto v], \mathcal{B}\rangle & \text{where } \mathrm{fresh}(a) \\
\text{(EDeref)} & \langle !a^p, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle & \text{where } \sigma(a) = v \\
\text{(EUpdtRef)} & \langle a{:=}^p v, \sigma, \mathcal{B}\rangle \longrightarrow \langle 0, \sigma[a \mapsto v], \mathcal{B}\rangle & \text{where } \sigma(a) = v' \\
\\
\text{(EAdd)} & \langle n_1 +^p n_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle n', \sigma, \mathcal{B}\rangle & \text{where } n' = n_1 + n_2 \\
\\
\text{(ECheckHO)} & \langle v{\Downarrow}\langle S; a; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \varrho(\mathcal{B}, a', \langle a, r\rangle)\rangle & \text{where } \mathit{hastype}(\sigma, v, S), v = a' \\
\text{(ECheckFirst)} & \langle v{\Downarrow}\langle S; a; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle & \text{where } \mathit{hastype}(\sigma, v, S), v \neq a' \\
\text{(ECheckFail)} & \langle v{\Downarrow}\langle S; a; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \mathit{blame}(\sigma, v, a, r, \mathcal{B}) & \text{where } \neg(\mathit{hastype}(\sigma, v, S)) \\
\\
\text{(ECastHO)} & \langle v{::}T_1 \Rightarrow^\ell T_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \varrho(\mathcal{B}, a, [\![T_1 \Rightarrow^\ell T_2]\!])\rangle & \text{where } \mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor), v = a \\
\text{(ECastFirst)} & \langle v{::}T_1 \Rightarrow^\ell T_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle & \text{where } \mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor), v \neq a \\
\text{(ECastFail)} & \langle v{::}T_1 \Rightarrow^\ell T_2, \sigma, \mathcal{B}\rangle \longrightarrow \textsc{Blame}(\{\ell\}) & \text{where } \neg(\mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor))
\end{array}
$$

$$\varrho(\mathcal{B}, a, b) \quad = \quad \mathcal{B}[a \mapsto \mathcal{B}(a) \cup \{b\}]$$

$\boxed{\langle e, \sigma, \mathcal{B}\rangle \longmapsto \varsigma}$

$$\frac{\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \langle e', \sigma', \mathcal{B}'\rangle}{\langle E[e], \sigma, \mathcal{B}\rangle \longmapsto \langle E[e'], \sigma', \mathcal{B}'\rangle} \qquad \frac{\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \textsc{Blame}(\mathcal{L})}{\langle E[e], \sigma, \mathcal{B}\rangle \longmapsto \textsc{Blame}(\mathcal{L})}$$

Figure A.2. Single step reduction with markers attached

$\lfloor\Gamma\rfloor, f{:}\to, x{:}\star; \emptyset \vdash \texttt{let}\ x = x{\Downarrow}\langle\lfloor T_1\rfloor; f; \textsc{Arg}\rangle\ \texttt{in}\ e' : \star$.
By TFun, $\lfloor\Gamma\rfloor; \emptyset \vdash \texttt{fun}\ f\ x.\ (\texttt{let}\ x = x{\Downarrow}\langle\lfloor T_1\rfloor; f; \textsc{Arg}\rangle\ \texttt{in}\ e') :\to$.

Case CCall

$$\frac{\begin{array}{lll}\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T & T \rhd T_1 \to T_2 & \mathrm{fresh}(f) \\ \Gamma \vdash e_{s2} \rightsquigarrow e_2 : T_1' & T_1 \sim T_1' & \mathrm{fresh}(\ell)\end{array}}{\begin{array}{c}\Gamma \vdash e_{s1}\ e_{s2} \rightsquigarrow \texttt{let}\ f = e_1{::}T \Rightarrow^\ell T_1 \to T_2\ \texttt{in} \\ (f\ (e_2{::}T_1' \Rightarrow^\ell T_1)^\Diamond){\Downarrow}\langle\lfloor T_2\rfloor; f; \textsc{Res}\rangle : T_2\end{array}}$$

By the IH, $\lfloor\Gamma\rfloor; \Sigma \vdash e_1 : \lfloor T\rfloor$.
By the IH, $\lfloor\Gamma\rfloor; \Sigma \vdash e_2 : \lfloor T_1'\rfloor$.
By TCast, $\lfloor\Gamma\rfloor; \Sigma \vdash e_2{::}T_1' \Rightarrow^\ell T_1 : \lfloor T_1\rfloor$.
By TSubsump, $\lfloor\Gamma\rfloor; \Sigma \vdash e_2{::}T_1' \Rightarrow^\ell T_1 : \star$.
By Lemma B.2, $\lfloor\Gamma\rfloor, f{:}\to; \Sigma \vdash e_2{::}T_1' \Rightarrow^\ell T_1 : \star$.
By TCast, $\lfloor\Gamma\rfloor; \Sigma \vdash e_1{::}T \Rightarrow^\ell T_1 \to T_2 :\to$.
By TVar, $\lfloor\Gamma\rfloor, f{:}\to; \Sigma \vdash f :\to$.
By TApp, $\lfloor\Gamma\rfloor, f{:}\to; \Sigma \vdash f\ (e_2{::}T_1' \Rightarrow^\ell T_1)^\Diamond : \star$.
By TCheck,
$\lfloor\Gamma\rfloor, f{:}\to; \Sigma \vdash (f\ (e_2{::}T_1' \Rightarrow^\ell T_1)^\Diamond){\Downarrow}\langle\lfloor T_2\rfloor; f; \textsc{Res}\rangle : \lfloor T_2\rfloor$.
By TLet, $\lfloor\Gamma\rfloor, f{:}\to; \Sigma \vdash \texttt{let}\ f = e_1{::}T \Rightarrow^\ell T_1 \to T_2\ \texttt{in}\ (f\ (e_2{::}T_1' \Rightarrow^\ell T_1)^\Diamond){\Downarrow}\langle\lfloor T_2\rfloor; f; \textsc{Res}\rangle : \lfloor T_2\rfloor$.

Case CRef

$$\frac{\Gamma \vdash e_s \rightsquigarrow e : T}{\Gamma \vdash \texttt{ref}\ e_s \rightsquigarrow \texttt{ref}\ e : \mathsf{ref}\ T}$$

By the IH, $\lfloor\Gamma\rfloor; \Sigma \vdash e : \lfloor T\rfloor$.
By TSubsump, $\lfloor\Gamma\rfloor; \Sigma \vdash e : \star$.
By TRef, $\lfloor\Gamma\rfloor; \Sigma \vdash \texttt{ref}\ e : \mathsf{ref}$.

Case CDeref

$$\frac{\Gamma \vdash e_s \rightsquigarrow e : T \qquad T \rhd \mathsf{ref}\ T_1 \qquad \mathrm{fresh}(x) \qquad \mathrm{fresh}(\ell)}{\Gamma \vdash !e_s \rightsquigarrow \texttt{let}\ x = e{::}T \Rightarrow^\ell \mathsf{ref}\ T_1\ \texttt{in}\ !x{\Downarrow}\langle\lfloor T_1\rfloor; x; \textsc{Deref}\rangle : T_1}$$

By the IH, $\lfloor\Gamma\rfloor; \Sigma \vdash e : \lfloor T\rfloor$.
By TCast, $\lfloor\Gamma\rfloor; \Sigma \vdash e_1{::}T \Rightarrow^\ell \mathsf{ref}\ T_1 : \mathsf{ref}$.
By TVar, $\lfloor\Gamma\rfloor, x{:}\mathsf{ref}; \Sigma \vdash x : \mathsf{ref}$.
By TDeref, $\lfloor\Gamma\rfloor, x{:}\mathsf{ref}; \Sigma \vdash !x^\Diamond : \star$.
By TCheck, $\lfloor\Gamma\rfloor, x{:}\mathsf{ref}; \Sigma \vdash !x^\Diamond{\Downarrow}\langle\lfloor T_1\rfloor; x; \textsc{Deref}\rangle : \lfloor T_1\rfloor$
By TLet, $\lfloor\Gamma\rfloor; \Sigma \vdash \texttt{let}\ x = e_1{::}T \Rightarrow^\ell \mathsf{ref}\ T_1\ \texttt{in}\ !x^\Diamond{\Downarrow}\langle\lfloor T_1\rfloor; x; \textsc{Deref}\rangle : \lfloor T_1\rfloor$.

Case CUpdt

$$\frac{\begin{array}{lll}\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T & T \rhd \mathsf{ref}\ T_1 & \mathrm{fresh}(\ell_1) \\ \Gamma \vdash e_{s2} \rightsquigarrow e_2 : T_1' & T_1 \sim T_1' & \mathrm{fresh}(\ell_2)\end{array}}{\Gamma \vdash e_{s1}{:=}e_{s2} \rightsquigarrow (e_1{::}T \Rightarrow^{\ell_1} \mathsf{ref}\ T_1){:=}^\Diamond(e_2{::}T_1' \Rightarrow^{\ell_2} T_1) : \mathsf{int}}$$

By the IH, $\lfloor\Gamma\rfloor; \Sigma \vdash e_1 : \lfloor T\rfloor$.
By TCast, $\lfloor\Gamma\rfloor; \Sigma \vdash e_1{::}T \Rightarrow^{\ell_1} \mathsf{ref}\ T_1 : \mathsf{ref}$.
By the IH, $\lfloor\Gamma\rfloor; \Sigma \vdash e_2 : \lfloor T_1'\rfloor$.
By TCast, $\lfloor\Gamma\rfloor; \Sigma \vdash e_2{::}T_1' \Rightarrow^{\ell_2} T_1 : \lfloor T_1\rfloor$.
By TSubsump, $\lfloor\Gamma\rfloor; \Sigma \vdash e_2{::}T_1' \Rightarrow^{\ell_2} T_1 : \star$.
By TUpdt, $\lfloor\Gamma\rfloor; \Sigma \vdash (e_1{::}T \Rightarrow^{\ell_1} \mathsf{ref}\ T_1){:=}^\Diamond(e_2{::}T_1' \Rightarrow^{\ell_2} T_1) : \mathsf{int}$

□

Lemma B.4 (Inversion). *Suppose* $\Gamma; \Sigma \vdash e : S$. *Then*

- *If* $e = \texttt{fun}\ f\ x.\ e'$, *then* $\Gamma, f{:}\to, x{:}\star; \Sigma \vdash e' : \star$ *and* $S \in \{\star, \to\}$.
- *If* $e = e_1\ e_2^\Diamond$, *then* $\Gamma; \Sigma \vdash e_1 :\to$ *and* $\Gamma; \Sigma \vdash e_2 : \star$ *and* $S = \star$.
- *If* $e = e_1\ e_2^\blacklozenge$, *then* $\Gamma; \Sigma \vdash e_1 : \star$ *and* $\Gamma; \Sigma \vdash e_2 : \star$ *and* $S = \star$.
- *If* $e = \texttt{ref}\ e'$, *then* $\Gamma; \Sigma \vdash e' : \star$ *and* $S \in \{\star, \mathsf{ref}\}$.
- *If* $e = !e'^\Diamond$, *then* $\Gamma; \Sigma \vdash e' : \mathsf{ref}$ *and* $S = \star$.
- *If* $e = !e'^\blacklozenge$, *then* $\Gamma; \Sigma \vdash e' : \star$ *and* $S = \star$.
- *If* $e = e_1{:=}^\Diamond e_2$, *then* $\Gamma; \Sigma \vdash e_1 : \mathsf{ref}$ *and* $\Gamma; \Sigma \vdash e_2 : \star$ *and* $S \in \{\star, \mathsf{int}\}$.
- *If* $e = e_1{:=}^\blacklozenge e_2$, *then* $\Gamma; \Sigma \vdash e_1 : \star$ *and* $\Gamma; \Sigma \vdash e_2 : \star$ *and* $S \in \{\star, \mathsf{int}\}$.
- *If* $e = e_1 +^\Diamond e_2$, *then* $\Gamma; \Sigma \vdash e_1 : \mathsf{int}$ *and* $\Gamma; \Sigma \vdash e_2 : \mathsf{int}$ *and* $S \in \{\star, \mathsf{int}\}$.
- *If* $e = e_1 +^\blacklozenge e_2$, *then* $\Gamma; \Sigma \vdash e_1 : \star$ *and* $\Gamma; \Sigma \vdash e_2 : \star$ *and* $S \in \{\star, \mathsf{int}\}$.
- *If* $e = e'{::}T_1 \Rightarrow^\ell T_2$, *then* $\Gamma; \Sigma \vdash e' : \lfloor T_1\rfloor$ *and* $T_1 \sim T_2$ *and* $S \in \{\star, \lfloor T_2\rfloor\}$.

$\boxed{e_s \sqsubseteq e_s}$

$$\text{(PEVAR)}\quad x \sqsubseteq x \qquad \text{(PEINT)}\quad n \sqsubseteq n$$

$$\text{(PEFUN)}\ \frac{T_{11} \sqsubseteq T_{21} \qquad T_{12} \sqsubseteq T_{22} \qquad e_{s1} \sqsubseteq e_{s2}}{\texttt{fun}\ f\ (x{:}T_{11}) \to T_{12}.\ e_{s1} \sqsubseteq \texttt{fun}\ f\ (x{:}T_{21}) \to T_{22}.\ e_{s2}}$$

$$\text{(PEAPP)}\ \frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11}\ e_{s12} \sqsubseteq e_{s21}\ e_{s22}} \qquad \text{(PEADD)}\ \frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11}\ +\ e_{s12} \sqsubseteq e_{s21}\ +\ e_{s22}}$$

$$\text{(PEREF)}\ \frac{e_{s1} \sqsubseteq e_{s2}}{\texttt{ref}\ e_{s1} \sqsubseteq \texttt{ref}\ e_{s2}} \qquad \text{(PEDEREF)}\ \frac{e_{s1} \sqsubseteq e_{s2}}{!e_{s1} \sqsubseteq !e_{s2}} \qquad \text{(PESET)}\ \frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11} := e_{s12} \sqsubseteq e_{s21} := e_{s22}}$$

$\boxed{e \sqsubseteq e}$

$$\text{(PVAR)}\quad x \sqsubseteq x \qquad \text{(PINT)}\quad n \sqsubseteq n \qquad \text{(PADDR)}\quad a \sqsubseteq a$$

$$\text{(PFUN)}\ \frac{e_1 \sqsubseteq e_2}{\texttt{fun}\ f\ x.\ e_1 \sqsubseteq \texttt{fun}\ f\ x.\ e_2}$$

$$\text{(PAPP)}\ \frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22}}{e_{11}\ e_{12} \sqsubseteq e_{21}\ e_{22}} \qquad \text{(PADD)}\ \frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22}}{e_{11}\ +\ e_{12} \sqsubseteq e_{21}\ +\ e_{22}}$$

$$\text{(PREF)}\ \frac{e_1 \sqsubseteq e_2}{\texttt{ref}\ e_1 \sqsubseteq \texttt{ref}\ e_2} \qquad \text{(PDEREF)}\ \frac{e_1 \sqsubseteq e_2}{!e_1 \sqsubseteq !e_2} \qquad \text{(PSET)}\ \frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22}}{e_{11} := e_{12} \sqsubseteq e_{21} := e_{22}}$$

$$\text{(PCHECK)}\ \frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22} \qquad S_1 \sqsubseteq S_2}{e_{11}\Downarrow\langle S_1; e_{12}; r\rangle \sqsubseteq e_{21}\Downarrow\langle S_2; e_{22}; r\rangle}$$

$$\text{(PCAST)}\ \frac{e_1 \sqsubseteq e_2 \qquad T_{11} \sqsubseteq T_{21} \qquad T_{12} \sqsubseteq T_{22}}{e_1{::}T_{11} \Rightarrow^{\ell} T_{12} \sqsubseteq e_2{::}T_{21} \Rightarrow^{\ell} T_{22}}$$

$$\text{(PLET)}\ \frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22}}{\texttt{let}\ x = e_{11}\ \texttt{in}\ e_{12} \sqsubseteq \texttt{let}\ x = e_{21}\ \texttt{in}\ e_{22}}$$

Figure A.3. Expression precision

- *If* $e = e_1\Downarrow\langle S'; e_2; r\rangle$*, then* $\Gamma; \Sigma \vdash e_1 : \star$ *and* $\Gamma; \Sigma \vdash e_2 : \star$ *and* $S \in \{\star, S'\}$.
- *If* $e = a$*, then* $\Sigma(a) = S'$ *and* $S \in \{\star, S'\}$.

Proof. Induction on $\Gamma; \Sigma \vdash e : S$. □

Lemma B.5 (Heap weakening)**.** *If* $\Gamma; \Sigma \vdash e : S$ *and* $\Sigma' \sqsubseteq \Sigma$*, then* $\Gamma; \Sigma' \vdash e : S$.

Proof. By induction on $\Gamma; \Sigma \vdash e : S$. Only interesting case:

Case TADDR Since $a \in dom(\Sigma)$, and $\Sigma' \sqsubseteq \Sigma$, $\Sigma'(a) = \Sigma(a)$. Therefore $\Gamma; heapenv' \vdash e : \Sigma(a)$.

□

Lemma B.6 (Substitution)**.** *If* $\Gamma, x : S; \Sigma \vdash e : S'$ *and* $\Gamma; \Sigma \vdash v : S$*, then* $\Gamma; \Sigma \vdash e[v/x] : S'$.

$\boxed{S \sqsubseteq S}$

$$S \sqsubseteq \star \quad \mathsf{int} \sqsubseteq \mathsf{int} \quad \mathsf{ref} \sqsubseteq \mathsf{ref} \quad \to\sqsubseteq\to$$

$\boxed{\Gamma \sqsubseteq \Gamma}$

$$\frac{\forall x \in dom(\Gamma),\ \Gamma(x) \sqsubseteq \Gamma'(x)}{\Gamma \sqsubseteq \Gamma'}$$

$\boxed{\sigma \sqsubseteq \sigma}$

$$\frac{\forall a \in dom(\sigma),\ \sigma(x) \sqsubseteq_h \sigma'(x)}{\sigma \sqsubseteq \sigma'}$$

$\boxed{h \sqsubseteq_h h}$

$$\frac{v \sqsubseteq v'}{v \sqsubseteq_h v'} \qquad \frac{e \sqsubseteq e'}{(\lambda x.e) \sqsubseteq_h (\lambda x.e')}$$

Figure A.4. Auxiliary precision relations

Proof. By induction on $\Gamma, x : S; \Sigma \vdash e : S'$. □

Lemma B.7 (Runtime types are sound)**.** *If* $\emptyset; \Sigma \vdash v : \star$ *and* $\Sigma \vdash \sigma$ *and* $hastype(\sigma, v, S)$*, then* $\emptyset; \Sigma \vdash v : S$.

Proof. By inversion on $hastype(\sigma, v, S)$.

Case $\dfrac{}{hastype(\sigma, n, \mathsf{int})}$
By TINT, $\emptyset; \Sigma \vdash n : \mathsf{int}$

Case $\dfrac{}{hastype(\sigma, v, \star)}$
Immediate.

Case $\dfrac{\sigma(a) = (\lambda x.e, \rho)}{hastype(\sigma, a, \to)}$
Since $\Sigma \vdash \sigma$, $\Sigma \vdash (\lambda x.e) : \Sigma(a)$.
By inversion on $\Sigma \vdash (\lambda x.e) : \Sigma(a)$, $\Sigma(a) = \to$.
By TADDR, $\emptyset; \Sigma \vdash a : \to$.

Case $\dfrac{\sigma(a) = v}{hastype(\sigma, a, \mathsf{ref})}$
Since $\Sigma \vdash \sigma$, $\Sigma \vdash v : \Sigma(a)$.
By inversion on $\Sigma \vdash v : \Sigma(a)$, $\Sigma(a) = \mathsf{ref}$.
By TADDR, $\emptyset; \Sigma \vdash a : \mathsf{ref}$.

□

Lemma B.8 (Heap extension)**.** *If* $\Sigma \vdash \sigma$ *and* $\Sigma[a \mapsto S] \vdash h : S$ *and* $a \notin dom(\Sigma)$*, then* $\Sigma[a \mapsto S] \vdash \sigma[a \mapsto h]$.

Proof. Suppose $a' \in \Sigma[a \mapsto S]$. If $a = a'$, then immediately $\Sigma[a \mapsto S] \vdash \sigma(a') : \Sigma[a \mapsto S](a')$.
If $a \neq a'$, then $\Sigma \vdash \sigma(a') : \Sigma(a')$. Cases on $\sigma(a')$.

Case $\sigma(a') = v, \Sigma(a') = \mathsf{ref}$. Have that $\emptyset; \Sigma \vdash \sigma(a') : \star$. By Lemma B.5, $\emptyset; \Sigma[a \mapsto S] \vdash \sigma(a') : \star$. Thus $\Sigma[a \mapsto S] \vdash \sigma(a') : \Sigma(a')$. Since $a \neq a'$, $\Sigma[a \mapsto S] \vdash \sigma(a') : \Sigma[a \mapsto S](a')$.

Case $\sigma(a') = (\lambda a.e), \Sigma(a') = \to$. Have that $\emptyset, x{:}\star; \Sigma \vdash e : \star$. By Lemma B.5, $\emptyset, x{:}\star; \Sigma[a \mapsto S] \vdash e : \star$. Thus $\Sigma[a \mapsto S] \vdash \sigma(a') : \Sigma(a')$. Since $a \neq a'$, $\Sigma[a \mapsto S] \vdash \sigma(a') : \Sigma[a \mapsto S](a')$.

Thus for all $a' \in \Sigma[a \mapsto S]$, have $\Sigma[a \mapsto S] \vdash \sigma(a') : \Sigma[a \mapsto S](a')$, so by THEAP, $\Sigma[a \mapsto S] \vdash \sigma[a \mapsto h]$. □

$\boxed{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma;S}$

$$\text{(CxHole)}\ \frac{}{\vdash \Box : \Gamma;S \Rightarrow \Gamma;S} \qquad \text{(CxSubsump)}\ \frac{\vdash \mathcal{C} : \Gamma;S_1 \Rightarrow \Gamma';S_2}{\vdash \mathcal{C} : \Gamma;S_1 \Rightarrow \Gamma';\star}$$

$$\text{(CxAddL)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star \qquad \Gamma';\emptyset \vdash e : \star}{\vdash \mathcal{C} \ +^{\blacklozenge}\ e : \Gamma;S \Rightarrow \Gamma';\mathsf{int}} \qquad \text{(CxAddR)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star \qquad \Gamma';\emptyset \vdash e : \star}{\vdash e \ +^{\blacklozenge}\ \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\mathsf{int}}$$

$$\text{(CxFun)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma', f\colon \to, x\colon \star;\star}{\vdash \mathtt{fun}\ f\ x.\ \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\to} \qquad \text{(CxAppL)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star \qquad \Gamma';\emptyset \vdash e : \star}{\vdash \mathcal{C}\ e^{\blacklozenge} : \Gamma;S \Rightarrow \Gamma';\star}$$

$$\text{(CxAppR)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star \qquad \Gamma';\emptyset \vdash e : \star}{\vdash e\ \mathcal{C}^{\blacklozenge} : \Gamma;S \Rightarrow \Gamma';\star}$$

$$\text{(CxRef)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star}{\vdash \mathtt{ref}\ \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\mathsf{ref}} \qquad \text{(CxDerefL)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star \qquad \Gamma';\emptyset \vdash e : \star}{\vdash \mathcal{C} :=^{\blacklozenge} e : \Gamma;S \Rightarrow \Gamma';\mathsf{int}}$$

$$\text{(CxDerefR)}\ \frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star \qquad \Gamma';\emptyset \vdash e : \star}{\vdash e :=^{\blacklozenge} \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\mathsf{int}}$$

Figure A.5. Context typing

$\boxed{L\ \mathsf{safe}\ \ell}$

$$\text{(LInt)}\ \frac{q \neq \ell}{\mathsf{int}^q\ \mathsf{safe}\ \ell} \qquad \text{(LBot)}\ \frac{\ell_1 \neq \ell_2}{\bot^{\ell_1}\ \mathsf{safe}\ \ell_2} \qquad \text{(LDyn)}\ \frac{}{\star\ \mathsf{safe}\ \ell}$$

$$\text{(LFun)}\ \frac{q \neq \ell \qquad L_1\ \mathsf{safe}\ \ell \qquad L_2\ \mathsf{safe}\ \ell}{L_1 \to^q L_2\ \mathsf{safe}\ \ell} \qquad \text{(LRef)}\ \frac{q \neq \ell \qquad L\ \mathsf{safe}\ \ell}{\mathsf{ref}^q\ L\ \mathsf{safe}\ \ell}$$

$\boxed{\mathcal{B} \vdash b\ \mathsf{safe}\ \ell}$

$$\text{(SfLType)}\ \frac{L\ \mathsf{safe}\ \ell}{\mathcal{B} \vdash L\ \mathsf{safe}\ \ell} \qquad \text{(SfRef)}\ \frac{\forall b \in \mathcal{B}(a) \setminus \{\langle a, r\rangle\},\ \mathcal{B} \vdash b\ \mathsf{safe}\ \ell}{\mathcal{B} \vdash \langle a, r\rangle\ \mathsf{safe}\ \ell}$$

$\boxed{\mathcal{B} \vdash \sigma\ \mathsf{safe}\ \ell}$

$$\text{(SfEmpHeap)}\ \frac{}{\mathcal{B} \vdash \cdot\ \mathsf{safe}\ \ell}$$

$$\text{(SfHeapCell)}\ \frac{\mathcal{B} \vdash v\ \mathsf{safe}\ \ell \qquad \mathcal{B} \vdash \sigma\ \mathsf{safe}\ \ell}{\mathcal{B} \vdash \sigma[a \mapsto v]\ \mathsf{safe}\ \ell}$$

$$\text{(SfHeapClosure)}\ \frac{\mathcal{B} \vdash e\ \mathsf{safe}\ \ell \qquad \mathcal{B} \vdash \sigma\ \mathsf{safe}\ \ell}{\mathcal{B} \vdash \sigma[a \mapsto (\lambda x.e)]\ \mathsf{safe}\ \ell}$$

$\boxed{\mathcal{B} \vdash e\ \mathsf{safe}\ \ell}$

$$\text{(SfCast)}\ \frac{\mathcal{B} \vdash e\ \mathsf{safe}\ \ell_2 \qquad [\![T_1 \Rightarrow^{\ell_1} T_2]\!]\ \mathsf{safe}\ \ell_2}{\mathcal{B} \vdash e\colon\colon T_1 \Rightarrow^{\ell_1} T_2\ \mathsf{safe}\ \ell_2}$$

$$\text{(SfCheck)}\ \frac{\mathcal{B} \vdash e_1\ \mathsf{safe}\ \ell \qquad \mathcal{B} \vdash e_2\ \mathsf{safe}\ \ell}{\mathcal{B} \vdash e_1 \Downarrow \langle S; e_2; r\rangle\ \mathsf{safe}\ \ell}$$

$$\text{(SfAddr)}\ \frac{\forall b \in \mathcal{B}(a),\ \mathcal{B} \vdash b\ \mathsf{safe}\ \ell}{\mathcal{B} \vdash a\ \mathsf{safe}\ \ell}$$

$$\text{(SfVar)}\ \frac{}{\mathcal{B} \vdash x\ \mathsf{safe}\ \ell} \qquad \text{(SfApp)}\ \frac{\mathcal{B} \vdash e_1\ \mathsf{safe}\ \ell \qquad \mathcal{B} \vdash e_2\ \mathsf{safe}\ \ell}{\mathcal{B} \vdash e_1\ e_2\ \mathsf{safe}\ \ell}$$

Figure A.6. Blame safety predicates

Lemma B.9 (Preservation)**.** *If* $\emptyset;\Sigma \vdash e : S$ *and* $\Sigma \vdash \sigma$ *and* $\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \langle e', \sigma', \mathcal{B}'\rangle$*, then* $\emptyset;\Sigma' \vdash e' : S$ *and* $\Sigma' \vdash \sigma'$ *and* $\Sigma' \sqsubseteq \Sigma$*.*

Proof. By induction on $\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \langle e', \sigma', \mathcal{B}'\rangle$.

Case EFun With fresh(a),

$$\langle \mathtt{fun}\ f\ x.\ e, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto (\lambda x.e[a/f])], \mathcal{B}\rangle$$

By Lemma B.4, $\emptyset, f\colon \to, x\colon\star;\Sigma \vdash e' : \star$ and $S \in \{\star, \to\}$.
Since a fresh, $\Sigma[a \mapsto \to] \sqsubseteq \Sigma$.
By Lemma B.5, $\emptyset, f\colon \to, x\colon\star;\Sigma[a \mapsto \to] \vdash e' : \star$
By TAddr, $\emptyset, x\colon\star;\Sigma[a \mapsto \to] \vdash a :\to$
By Lemma B.6, $\emptyset, x\colon\star;\Sigma[a \mapsto \to] \vdash e[a/f] : \star$
By THClosure, $\Sigma[a \mapsto \to] \vdash (\lambda x.e[a/f]) :\to$.
By Lemma B.8, $\Sigma[a \mapsto \to] \vdash \sigma[a \mapsto (\lambda x.e[a/f])]$.
By TAddr, $\emptyset;\Sigma[a \mapsto \to] \vdash a :\to$.
By TSubsump, $\emptyset;\Sigma[a \mapsto \to] \vdash a : \star$.
Since $S \in \{\star, \to\}$, theorem satisfied.

Case EApp Where $\sigma(a) = (\lambda x.e)$,

$$\langle a\ v^p, \sigma, \mathcal{B}\rangle \longrightarrow \langle e[v/x], \sigma, \mathcal{B}\rangle$$

By Lemma B.4, $\emptyset;\Sigma \vdash v : \star$ and $S = \star$.
By inversion on $\Sigma \vdash \sigma$, $\Sigma \vdash (\lambda x.e) : S'$ for some S'.
By further inversion, $S' = \to$ and $\emptyset, x\colon\star;\Sigma \vdash e : \star$.
By Lemma B.6, $\emptyset;\Sigma \vdash e[a/x] : \star$, which satisfies the theorem.

Case ERef With fresh(a),

$$\langle \mathtt{ref}\ v, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto v], \mathcal{B}\rangle$$

By Lemma B.4, $\emptyset;\Sigma \vdash v : \star$ and $S \in \{\star, \mathsf{ref}\}$.
Since a fresh, $\Sigma[a \mapsto \mathsf{ref}] \sqsubseteq \Sigma$.
By Lemma B.5, $\emptyset;\Sigma[a \mapsto \mathsf{ref}] \vdash v : \star$
By THRef, $\Sigma[a \mapsto \to] \vdash v :\to$.
By Lemma B.8, $\Sigma[a \mapsto \mathsf{ref}] \vdash \sigma[a \mapsto v]$.
By TAddr, $\emptyset;\Sigma[a \mapsto \mathsf{ref}] \vdash a : \mathsf{ref}$.
By TSubsump, $\emptyset;\Sigma[a \mapsto \mathsf{ref}] \vdash a : \star$.
Since $S \in \{\star, \mathsf{ref}\}$, theorem satisfied.

Case EDeref With $\sigma(a) = v$,

$$\langle !a^p, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle$$

...

By Lemma B.4, $S = \star$.
By inversion on $\Sigma \vdash \sigma$, $\Sigma \vdash v : S'$ for some S'.
By further inversion, $S' = \mathsf{ref}$ and $\emptyset;\Sigma \vdash v : \star$, which satisfies the theorem.

Case EUpdtRef With $\sigma(a) = v'$,

$$\langle a :=^p v, \sigma, \mathcal{B}\rangle \longrightarrow \langle 0, \sigma[a \mapsto v], \mathcal{B}\rangle$$

By Lemma B.4, $\emptyset; \Sigma \vdash v : \star$ and $S \in \{\star, \mathsf{int}\}$.
By THREF, $\Sigma \vdash v : \mathsf{ref}$. By inversion on $\Sigma \vdash \sigma$, $\Sigma \vdash v' : S'$ for some S'.
By further inversion, $S' = \mathsf{ref}$, and thus $\Sigma(a) = \mathsf{ref}$.
By THEAP, $\Sigma \vdash \sigma[a \mapsto v]$.
By TINT, $\emptyset; \Sigma \vdash 0 : \mathsf{int}$.
By TSUBSUMP, $\emptyset; \Sigma \vdash 0 : \star$.
Since $S \in \{\star, \mathsf{int}\}$, theorem satisfied.

Case EADD With $n' = n_1 + n_2$,

$$\langle n_1 \ +^p \ n_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle n', \sigma, \mathcal{B}\rangle$$

By Lemma B.4, $S \in \{\star, \mathsf{int}\}$.
By TINT, $\emptyset; \Sigma \vdash n' : \mathsf{int}$.
By TSUBSUMP, $\emptyset; \Sigma \vdash n' : \star$.
Since $S \in \{\star, \mathsf{int}\}$, theorem satisfied.

Cases ECHECKFIRST and ECHECKHO With $\mathit{hastype}(\sigma, v, S)$, and for some $\mathcal{B}'$,

$$\langle v \Downarrow \langle S'; a; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}'\rangle$$

By Lemma B.4, $\emptyset; \Sigma \vdash v : \star$ and $\emptyset; \Sigma \vdash a : \star$ and $S \in \{\star, S'\}$.
By Lemma B.7, $\emptyset; \Sigma \vdash v : S'$. By TSUBSUMP, $\emptyset; \Sigma \vdash v : \star$.
Since $S \in \{\star, S'\}$, theorem satisfied.

Case ECHECKFAIL is vacuous.

Cases ECASTFIRST and ECASTHO With $\mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor)$, and for some $\mathcal{B}'$,

$$\langle v{::}T_1 \Rightarrow^{\ell} T_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}'\rangle$$

By Lemma B.4, $\emptyset; \Sigma \vdash v : \lfloor T_1 \rfloor$ and $S \in \{\star, \lfloor T_2 \rfloor\}$.
By TSUBSUMP, $\emptyset; \Sigma \vdash v : \star$.
By Lemma B.7, $\emptyset; \Sigma \vdash v : \lfloor T_2 \rfloor$. By TSUBSUMP, $\emptyset; \Sigma \vdash v : \star$.
Since $S \in \{\star, \lfloor T_2 \rfloor\}$, theorem satisfied.

Case ECASTFAIL is vacuous.

□

Lemma B.10 (Canonical forms)**.** *If $\emptyset; \Sigma \vdash v : S$ and $\Sigma \vdash \sigma$, then*

- *If $S = \mathsf{int}$, then $v = n$.*
- *If $S = \rightarrow$, then $v = a$ and $\sigma(a) = (\lambda x.e)$.*
- *If $S = \mathsf{ref}$, then $v = a$ and $\sigma(a) = v'$.*
- *If $S = \star$, then $\exists S'$, $S \neq \star$, such that $\emptyset; \Sigma \vdash v : S'$.*

Proof. By induction on $\emptyset; \Sigma \vdash v : S$. Most cases vacuous.

Case TSUBSUMP

$$\frac{\Gamma; \Sigma \vdash v : S'}{\Gamma; \Sigma \vdash v : \star}$$

If $S \neq \star$, case is vacuous. If $S' = \star$, then apply the IH with $\Gamma; \Sigma \vdash v : S'$.
Otherwise, $S' \neq \star$, and theorem satisfied.

Case TINT

$$\Gamma; \Sigma \vdash n : \mathsf{int}$$

If $S \neq \mathsf{int}$, case is vacuous. If $S = \mathsf{int}$, then $v = n$.

Case TADDR

$$\frac{\Sigma(a) = S'}{\Gamma; \Sigma \vdash a : S'}$$

Since $\Sigma \vdash \sigma$, $\Sigma \vdash \sigma(a) : S'$.
Subcases on $\sigma(a)$.

Subcase $\sigma(a) = (\lambda x.e)$
Then $S' = \rightarrow$. If $S \neq \rightarrow$, case is vacuous. Otherwise, theorem satisfied.

Subcase $\sigma(a) = v$
Then $S' = \mathsf{ref}$. If $S \neq \mathsf{ref}$, case is vacuous. Otherwise, theorem satisfied.

□

Lemma B.11 (Progress)**.** *If $\emptyset; \Sigma \vdash e : S$ and $\Sigma \vdash \sigma$, then either:*

- *$\langle e, \sigma, \mathcal{B}\rangle \longmapsto \langle e', \sigma', \mathcal{B}\rangle$, or*
- *$\langle e, \sigma, \mathcal{B}\rangle \longmapsto$ BLAME$(\mathcal{L})$, or*
- *$e = v$, or*
- *$\langle e, \sigma, \mathcal{B}\rangle$ stuck ⧫.*

Proof. By induction on $\emptyset; \Sigma \vdash e : S$.

Case TVAR is vacuous.
Cases TADDR and TINT have $e = v$.
Case TSUBSUMP

$$\frac{\Gamma; \Sigma \vdash e : S}{\Gamma; \Sigma \vdash e : \star}$$

Immediate from the IH.

Case TADD

$$\frac{\Gamma; \Sigma \vdash e_1 : \mathsf{int} \quad \Gamma; \Sigma \vdash e_2 : \mathsf{int}}{\Gamma; \Sigma \vdash e_1 \ +^{\diamond} \ e_2 : \mathsf{int}}$$

By the IH, for both e_1 and e_2, either they are a value, they step (to either blame or another expression), or they are stuck (blaming ⧫). If either steps to another expression, then e steps. If either steps to blame, then e steps to the same blame. If either is stuck by ⧫, then e is stuck by ⧫. Otherwise, e_1 and e_2 are values.
If e_1 is a value, then by Lemma B.10, $e_1 = n_1$.
If e_2 is a value, then by Lemma B.10, $e_2 = n_2$.
Then by EADD, $\langle e_1 \ +^{\diamond} \ e_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle n, \sigma, \mathcal{B}\rangle$, where $n = n_1 + n_2$.

Case TADD-DYN

$$\frac{\Gamma; \Sigma \vdash e_1 : \star \quad \Gamma; \Sigma \vdash e_2 : \star}{\Gamma; \Sigma \vdash e_1 \ +^{\blacklozenge} \ e_2 : \mathsf{int}}$$

By the IH, for both e_1 and e_2, either they are a value, they step (to either blame or another expression), or they are stuck (blaming ⧫). If either steps to another expression, then e steps. If either steps to blame, then e steps to the same blame. If either is stuck by ⧫, then e is stuck by ⧫. Otherwise, e_1 and e_2 are values.
If e_1 is a value, then either $e_1 = n$ or $e_1 = a$. If $e_1 = a$, then $\langle e_1 \ +^{\blacklozenge} \ e_2, \sigma, \mathcal{B}\rangle$ stuck ⧫. Suppose that $e_1 = n_1$. If e_2 is a value, then either $e_2 = n$ or $e_2 = a$. If $e_2 = a$, then $\langle e_1 \ +^{\blacklozenge} \ e_2, \sigma, \mathcal{B}\rangle$ stuck ⧫. Suppose that $e_2 = n_2$. Then by EADD, $\langle e_1 \ +^{\blacklozenge} \ e_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle n, \sigma, \mathcal{B}\rangle$, where $n = n_1 + n_2$.

Case TFUN

$$\frac{\Gamma, x : \star, f :\rightarrow; \Sigma \vdash e : \star}{\Gamma; \Sigma \vdash \mathtt{fun}\ f\ x.\ e :\rightarrow}$$

Immediately have by EFUN that $\langle \mathtt{fun}\ f\ x.\ e, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto (\lambda x.e[a/f])], \mathcal{B}\rangle$ for fresh a.

Case TAPP

$$\frac{\Gamma; \Sigma \vdash e_1 :\rightarrow \quad \Gamma; \Sigma \vdash e_2 : \star}{\Gamma; \Sigma \vdash e_1\ e_2^{\diamond} : \star}$$

By the IH, for both e_1 and e_2, either they are a value, they step (to either blame or another expression), or they are stuck (blaming ⧫). If either steps to another expression, then e steps. If either steps to blame, then e steps to the same blame. If either is stuck by ⧫, then e is stuck by ⧫. Otherwise, e_1 and e_2 are values.
If e_1 is a value, then by Lemma B.10, $v = a$ and $\sigma(a) = (\lambda x.e')$.
Then, with e_2 a value, by EAPP $\langle e_1\ e_2^{\diamond}, \sigma, \mathcal{B}\rangle \longrightarrow \langle e'[e_2/x], \sigma, \mathcal{B}\rangle$.

Case TAPP-DYN

$$\frac{\Gamma;\Sigma \vdash e_1 : \star \quad \Gamma;\Sigma \vdash e_2 : \star}{\Gamma;\Sigma \vdash e_1\ e_2^{\blacklozenge} : \star}$$

By the IH, for both e_1 and e_2, either they are a value, they step (to either blame or another expression), or they are stuck (blaming $\blacklozenge$). If either steps to another expression, then e steps. If either steps to blame, then e steps to the same blame. If either is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e_1 and e_2 are values. Suppose that e_2 is a value.
If e_1 is a value, then either $e_1 = n$ or $e_1 = a$. If $e_1 = n$, then $\langle e_1\ e_2^{\blacklozenge}, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$. Suppose that $e_1 = a$.
By Lemma B.10, $\exists S', S' \neq \star$, such that $\Gamma;\Sigma \vdash e_1 : S'$.
By Lemma B.4, $\Sigma(a) = S'$.
Since $\Sigma \vdash \sigma, \Sigma \vdash \sigma(a) : \Sigma(a)$.
Cases on $\sigma(a)$: if $\sigma(a) = v$, then $\langle e_1\ e_2^{\blacklozenge}, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$.
If $\sigma(a) = (\lambda x.e')$, then by EAPP, $\langle e_1\ e_2^{\blacklozenge}, \sigma, \mathcal{B}\rangle \longrightarrow \langle e'[e_2/x], \sigma, \mathcal{B}\rangle$.

Case TREF

$$\frac{\Gamma;\Sigma \vdash e' : \star}{\Gamma;\Sigma \vdash \mathtt{ref}\ e' : \mathsf{ref}}$$

By the IH, either e' is a value, it steps (to either blame or another expression), or it is stuck (blaming $\blacklozenge$). If it to another expression, then e steps. If it steps to blame, then e steps to the same blame. If it is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e' is a value. Suppose that e' is a value.
Immediately have by by EREF that $\langle \mathtt{ref}\ e', \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto e], \mathcal{B}\rangle$ for fresh a.

Case TDEREF

$$\frac{\Gamma;\Sigma \vdash e' : \mathsf{ref}}{\Gamma;\Sigma \vdash !e'^{\Diamond} : \star}$$

By the IH, either e' is a value, it steps (to either blame or another expression), or it is stuck (blaming $\blacklozenge$). If it to another expression, then e steps. If it steps to blame, then e steps to the same blame. If it is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e' is a value. Suppose that e' is a value.
By Lemma B.10, $v = a$ and $\sigma(a) = v'$.
By EDEREF, $\langle !e'^{\Diamond}, \sigma, \mathcal{B}\rangle \longrightarrow \langle v', \sigma, \mathcal{B}\rangle$.

Case TDEREF-DYN

$$\frac{\Gamma;\Sigma \vdash e' : \star}{\Gamma;\Sigma \vdash !e'^{\blacklozenge} : \star}$$

By the IH, either e' is a value, it steps (to either blame or another expression), or it is stuck (blaming $\blacklozenge$). If it to another expression, then e steps. If it steps to blame, then e steps to the same blame. If it is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e' is a value. Suppose that e' is a value.
If e' is a value, then either $e' = n$ or $e' = a$. If $e' = n$, then $\langle !e'^{\blacklozenge}, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$. Suppose that $e' = a$.
By Lemma B.10, $\exists S', S' \neq \star$, such that $\Gamma;\Sigma \vdash e' : S'$.
By Lemma B.4, $\Sigma(a) = S'$.
Since $\Sigma \vdash \sigma, \Sigma \vdash \sigma(a) : \Sigma(a)$.
Cases on $\sigma(a)$: if $\sigma(a) = (\lambda x.e')$, then $\langle !e'^{\blacklozenge}, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$.
If $\sigma(a) = v$, then by EDEREF, $\langle !e'^{\blacklozenge}, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle$.

Case TUPDTREF

$$\frac{\Gamma;\Sigma \vdash e_1 : \mathsf{ref} \quad \Gamma;\Sigma \vdash e_2 : \star}{\Gamma;\Sigma \vdash e_1 {:=}^{\Diamond} e_2 : \mathsf{int}}$$

By the IH, for both e_1 and e_2, either they are a value, they step (to either blame or another expression), or they are stuck (blaming $\blacklozenge$). If either steps to another expression, then e steps. If either steps to blame, then e steps to the same blame. If either is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e_1 and e_2 are values.
If e_1 is a value, then by Lemma B.10, $v = a$ and $\sigma(a) = v$.
Then, with e_2 a value, by EUPDTREF $\langle e_1 {:=}^{\Diamond} e_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle 0, \sigma[a \mapsto e_2], \mathcal{B}\rangle$.

Case TUPDTREF-DYN

$$\frac{\Gamma;\Sigma \vdash e_1 : \star \quad \Gamma;\Sigma \vdash e_2 : \star}{\Gamma;\Sigma \vdash e_1 {:=}^{\blacklozenge} e_2 : \mathsf{int}}$$

By the IH, for both e_1 and e_2, either they are a value, they step (to either blame or another expression), or they are stuck (blaming $\blacklozenge$). If either steps to another expression, then e steps. If either steps to blame, then e steps to the same blame. If either is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e_1 and e_2 are values. Suppose that e_2 is a value.
If e_1 is a value, then either $e_1 = n$ or $e_1 = a$. If $e_1 = n$, then $\langle e_1 {:=}^{\blacklozenge} e_2, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$. Suppose that $e_1 = a$.
By Lemma B.10, $\exists S', S' \neq \star$, such that $\Gamma;\Sigma \vdash e_1 : S'$.
By Lemma B.4, $\Sigma(a) = S'$.
Since $\Sigma \vdash \sigma, \Sigma \vdash \sigma(a) : \Sigma(a)$.
Cases on $\sigma(a)$: if $\sigma(a) = (\lambda x.e')$, then $\langle e_1 {:=}^{\blacklozenge} e_2, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$.
If $\sigma(a) = v$, then by EUPDTREF, $\langle e_1 {:=}^{\blacklozenge} e_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle 0, \sigma[a \mapsto e_2], \mathcal{B}\rangle$.

Case TCHECK

$$\frac{\Gamma;\Sigma \vdash e_1 : \star \quad \Gamma;\Sigma \vdash e_2 : \mathit{tagtype}(r)}{\Gamma;\Sigma \vdash e_1 \Downarrow \langle S; e_2; r\rangle : S}$$

By the IH, for both e_1 and e_2, either they are a value, they step (to either blame or another expression), or they are stuck (blaming $\blacklozenge$). If either steps to another expression, then e steps. If either steps to blame, then e steps to the same blame. If either is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e_1 and e_2 are values.
By definition of *tagtype*, either $\Gamma;\Sigma \vdash e_2 :\rightarrow$ or $\Gamma;\Sigma \vdash e_2 :$ ref. In either case, by Lemma B.10 have that $e_2 = a$.
Let $\mathcal{B}'$ be defined as $\mathcal{B}$ if $e_1 = n$, and $\varrho(\mathcal{B}, a', \langle a, r\rangle)$ if $e_1 = a'$.
We proceed by subcases on $\mathit{hastype}(\sigma, e_1, S)$.

Subcase $\mathit{hastype}(\sigma, v, S)$.
Then we have $\langle e_1 \Downarrow \langle S; e_2; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \langle e_1, \sigma, \mathcal{B}'\rangle$ by ECHECKFIRST (if $e_1 = n$) or ECHECKHO (if $e_1 = a'$).

Subcase $\neg(\mathit{hastype}(\sigma, v, S))$.
Then by ECHECKBLAME,
$\langle e_1 \Downarrow \langle S; e_2; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \mathit{blame}(\sigma, v, a, \mathcal{B},)$.

Case TCAST

$$\frac{\Gamma;\Sigma \vdash e' : \lfloor T_1 \rfloor \quad T_1 \sim T_2}{\Gamma;\Sigma \vdash e' :: T_1 \Rightarrow^{\ell} T_2 : \lfloor T_2 \rfloor}$$

By the IH, either e' is a value, it steps (to either blame or another expression), or it is stuck (blaming $\blacklozenge$). If it to another expression, then e steps. If it steps to blame, then e steps to the same blame. If it is stuck by $\blacklozenge$, then e is stuck by $\blacklozenge$. Otherwise, e' is a value. Suppose that e' is a value.
Let $\mathcal{B}'$ be defined as $\mathcal{B}$ if $e_1 = n$, and $\varrho(\mathcal{B}, a', [\![T_1 \Rightarrow^{\ell} T_2]\!])$ if $e_1 = a$.
We proceed by subcases on $\mathit{hastype}(\sigma, e', \lfloor T_2 \rfloor)$.

Subcase $\mathit{hastype}(\sigma, e_1, \lfloor T_2 \rfloor)$. Then we have $\langle e' :: T_1 \Rightarrow^{\ell} T_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle e', \sigma, \mathcal{B}'\rangle$ by ECASTFIRST (if $e_1 = n$) or ECASTHO (if $e_1 = a$).

Subcase $\neg(\mathit{hastype}(\sigma, v, S))$. Then by ECHECKBLAME, $\langle e_1 \Downarrow \langle S; e_2; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow$ BLAME$(\{\ell\})$.

□

Lemma B.12 (Composition). *If* $\vdash \mathcal{C} : \Gamma; S \Rightarrow \Gamma'; S'$ *and* $\Gamma;\emptyset \vdash e : S$, *then* $\Gamma;\emptyset \vdash C[e] : S'$.

Proof. By induction on $\vdash \mathcal{C} : \Gamma; S \Rightarrow \Gamma'; S'$.

Case CXHOLE

$$\frac{}{\vdash \Box : \Gamma;S \Rightarrow \Gamma;S}$$

Since $\Box[e] = e$, have that $\Gamma;\emptyset \vdash e : S$.

Case CXSUBSUMP

$$\frac{\vdash \mathcal{C} : \Gamma;S_1 \Rightarrow \Gamma';S_2}{\vdash \mathcal{C} : \Gamma;S_1 \Rightarrow \Gamma';\star}$$

By the IH, $\Gamma;\emptyset \vdash \mathcal{C}[e] : S_2$. By TSUBSUMP, $\Gamma;\emptyset \vdash \mathcal{C}[e] : \star$

Case CXADDL

$$\frac{\vdash \mathcal{C} : \Gamma;S \Rightarrow \Gamma';\star \qquad \Gamma';\emptyset \vdash e' : \star}{\vdash \mathcal{C} \ +^{\blacklozenge}\ e' : \Gamma;S \Rightarrow \Gamma';\mathsf{int}}$$

By the IH, $\Gamma;\emptyset \vdash \mathcal{C}[e] : \star$. By TADD-DYN, $\Gamma;\emptyset \vdash \mathcal{C}[e] +^{\blacklozenge} e' : \mathsf{int}$.

Remaining cases are similar. □

Lemma B.13 (Open world soundness)**.** *If* $\Gamma \vdash e_s \rightsquigarrow e : T$ *and* $\vdash \mathcal{C} : \lfloor\Gamma\rfloor;\lfloor T\rfloor \Rightarrow \emptyset;S$*, then* $\emptyset;\emptyset \vdash \mathcal{C}[e] : S$ *and either:*

- $\langle \mathcal{C}[e], \emptyset, \emptyset\rangle \longrightarrow^* \langle v, \sigma, \mathcal{B}\rangle$ *and* $\emptyset;\Sigma \vdash v : S$ *and* $\Sigma \vdash \sigma$*, or*
- $\langle \mathcal{C}[e], \emptyset, \emptyset\rangle \longrightarrow^* \textsc{Blame}(\mathcal{L})$*, or*
- $\langle \mathcal{C}[e], \emptyset, \emptyset\rangle \longrightarrow^* \langle e', \sigma, \mathcal{B}\rangle$ *and* $\langle e', \sigma, \mathcal{B}\rangle$ *stuck* $\blacklozenge$*, or*
- *for all* ς *such that* $\langle \mathcal{C}[e], \emptyset, \emptyset\rangle \longrightarrow^* \varsigma$*, have that* $\varsigma = \langle e', \sigma, \mathcal{B}\rangle$ *and exists* ς' *such that* $\langle e', \sigma, \mathcal{B}\rangle \longrightarrow \varsigma'$.

Proof. By Lemma B.3, $\lfloor\Gamma\rfloor;\emptyset \vdash e : \lfloor T\rfloor$. By Lemma B.12, $\emptyset;\emptyset \vdash \mathcal{C}[e] : S$.
Suppose that for all ς such that $\langle \mathcal{C}[e], \emptyset, \emptyset\rangle \longrightarrow^* \varsigma$, have that $\varsigma = \langle e', \sigma, \mathcal{B}\rangle$ and exists ς' such that $\langle e', \sigma, \mathcal{B}\rangle \longrightarrow \varsigma'$. Then the theorem is satisfied.
Otherwise, there exists some ς such that $\varsigma \neq \langle e', \sigma, \mathcal{B}\rangle$ or there is no ς' such that $\langle e', \sigma, \mathcal{B}\rangle \longrightarrow \varsigma'$.
If $\varsigma \neq \langle e', \sigma, \mathcal{B}\rangle$, then $\varsigma = \textsc{Blame}(\mathcal{L})$.
Otherwise, $\langle \mathcal{C}[e], \emptyset, \emptyset\rangle \longrightarrow^* \langle e', \sigma, \mathcal{B}\rangle$ and $\langle e', \sigma, \mathcal{B}\rangle \not\longrightarrow \varsigma'$. By repeating Lemma B.9, $\emptyset;\Sigma \vdash e' : S$ and $\Sigma \vdash \sigma$. By Lemma B.11, either $e' = v$ or $\langle e', \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$. □

B.2 Blame

Lemma B.14. *For all* T_1, T_2, ℓ*,* $[\![T_1 \Leftrightarrow^{\ell} T_2]\!]$ *safe iff* $T_1 = T_2$.

Proof. First we prove that if $T_1 = T_2$, then $[\![T_1 \Leftrightarrow^{\ell} T_2]\!]$ safe ℓ by trivial induction on $T_1 <:_b T_2$.

Example Case $T_{11} \to T_{12} = T_{21} \to T_{22}$
Have $[\![T_{11} \to T_{12} \Leftrightarrow^{\ell} T_{21} \to T_{22}]\!] = [\![T_{21} \Leftrightarrow^{\ell} T_{11}]\!] \to^{\epsilon} [\![T_{12} \Leftrightarrow^{\ell} T_{22}]\!]$.
By IH, $[\![T_{21} \Leftrightarrow^{\ell} T_{11}]\!]$ safe ℓ since $T_{21} = T_{11}$.
By IH, $[\![T_{12} \Leftrightarrow^{\ell} T_{22}]\!]$ safe ℓ since $T_{12} = T_{22}$.
Hence $[\![T_{21} \Leftrightarrow^{\ell} T_{11}]\!] \to^{\epsilon} [\![T_{12} \Leftrightarrow^{\ell} T_{22}]\!]$ safe ℓ.

Next we prove that if $[\![T_1 \Leftrightarrow^{\ell} T_2]\!]$ safe , then $T_1 = T_2$ by induction on $[\![T_1 \Leftrightarrow^{\ell} T_2]\!]$ safe

Case LINT

$$\frac{q \neq \ell}{\mathsf{int}^q \ \mathsf{safe}\ \ell}$$

There are three ℓ-labeled casts that compile to int^q:
Subcase $[\![\mathsf{int} \Leftrightarrow^{\ell} \mathsf{int}]\!]$:
Have that $\mathsf{int} = \mathsf{int}$.
Subcases $[\![\mathsf{int} \Leftrightarrow^{\ell} \star]\!]$ and $[\![\star \Leftrightarrow^{\ell} \mathsf{int}]\!]$:
Then $q = \ell$, which is contradictory.

Case LBOT is vacuous.

Case LDYN

$$\frac{}{\star \ \mathsf{safe}\ \ell}$$

The only ℓ-labeled cast that compiles to $\star$ is $\star \Leftrightarrow^{\ell} \star$. Have that $\star = \star$.

Case LFUNC

$$\frac{q \neq \ell \qquad L_1 \ \mathsf{safe}\ \ell \qquad L_2 \ \mathsf{safe}\ \ell}{L_1 \to^q L_2 \ \mathsf{safe}\ \ell}$$

There are three ℓ-labeled casts that compile to $L_1 \to^q L_2$:
Subcase $[\![T_1 \to T_2 \Leftrightarrow^{\ell} T_3 \to T_4]\!]$:
Then $L_1 = [\![T_3 \Leftrightarrow^{\ell} T_1]\!]$ and $L_2 = [\![T_2 \Leftrightarrow^{\ell} T_4]\!]$.
By the IH, $T_3 = T_1$.
By the IH, $T_2 = T_4$.
Thus $T_1 \to T_2 = T_3 \to T_4$.
Subcases $[\![T_1 \to T_2 \Leftrightarrow^{\ell} \star]\!]$ and $[\![\star \Leftrightarrow^{\ell} T_1 \to T_2]\!]$:
Then $q = \ell$, which is contradictory.

Case LREF

$$\frac{q \neq \ell \qquad L \ \mathsf{safe}\ \ell}{\mathsf{ref}^q \ L \ \mathsf{safe}\ \ell}$$

There are three ℓ-labeled casts that compile to $\mathsf{ref}^q\ L$:
Subcase $[\![\mathsf{ref}\ T_1 \Leftrightarrow^{\ell} \mathsf{ref}\ T_2]\!]$:
Then $L = [\![T_2 \Leftrightarrow^{\ell} T_1]\!]$.
By the IH, $T_1 = T_2$.
Thus $\mathsf{ref}\ T_1 = \mathsf{ref}\ T_2$.
Subcases $[\![\mathsf{ref}\ T \Leftrightarrow^{\ell} \star]\!]$ and $[\![\star \Leftrightarrow^{\ell} T_1 \to T_2]\!]$:
Then $q = \ell$, which is contradictory.

□

Lemma B.15. *For all* T_1, T_2, ℓ*,* $T_1 <:_b T_2$ *iff* $[\![T_1 \Rightarrow^{\ell} T_2]\!]$ *safe* ℓ.

Proof. First we prove that if $T_1 <:_b T_2$, then $[\![T_1 \Rightarrow^{\ell} T_2]\!]$ safe ℓ by induction on $T_1 <:_b T_2$.

Case SINTDYN

$$\frac{}{\mathsf{int} <:_b \star}$$

$[\![\mathsf{int} \Rightarrow^{\ell} \star]\!] = \mathsf{int}^{\epsilon}$, and int^{ϵ} safe ℓ.

Case SFUNCDYN

$$\frac{T_1 \to T_2 <:_b \star \to \star}{T_1 \to T_2 <:_b \star}$$

Have $[\![T_1 \to T_2 \Rightarrow^{\ell} \star]\!] = [\![\star \Rightarrow^{\ell} T_1]\!] \to^{\epsilon} [\![T_2 \Rightarrow^{\ell} T_1]\!]$.
Also, $[\![T_1 \to T_2 \Rightarrow^{\ell} \star \to \star]\!] = [\![\star \Rightarrow^{\ell} T_1]\!] \to^{\epsilon} [\![T_2 \Rightarrow^{\ell} T_1]\!]$.
By the IH, $[\![T_1 \to T_2 \Rightarrow^{\ell} \star \to \star]\!]$ safe ℓ.

Case SREFDYN

$$\frac{\mathsf{ref}\ T <:_b \mathsf{ref}\ \star}{\mathsf{ref}\ T <:_b \star}$$

Have $[\![\mathsf{ref}\ T \Rightarrow^{\ell} \star]\!] = \mathsf{ref}^{\epsilon}\ [\![\star \Rightarrow^{\ell} T]\!]$.
Also, $[\![\mathsf{ref}\ T \Rightarrow^{\ell} \mathsf{ref}\ \star]\!] = \mathsf{ref}^{\epsilon}\ [\![\star \Rightarrow^{\ell} T]\!]$.
By the IH, $[\![\mathsf{ref}\ T \Rightarrow^{\ell} \mathsf{ref}\ \star]\!]$ safe ℓ.

Case SINTINT

$$\frac{}{\mathsf{int} <:_b \mathsf{int}}$$

$[\![\mathsf{int} \Rightarrow^{\ell} \mathsf{int}]\!] = \mathsf{int}^{\epsilon}$, and int^{ϵ} safe ℓ.

Case SFUNCFUNC

$$\frac{T_3 <:_b T_1 \qquad T_2 <:_b T_4}{T_1 \to T_2 <:_b T_3 \to T_4}$$

Have $[\![T_1 \to T_2 \Rightarrow^{\ell} T_3 \to T_4]\!] = [\![T_3 \Rightarrow^{\ell} T_1]\!] \to^{\epsilon} [\![T_2 \Rightarrow^{\ell} T_4]\!]$.

By the IH, $[\![T_3 \Rightarrow^\ell T_1]\!]$ safe ℓ.
By the IH, $[\![T_2 \Rightarrow^\ell T_4]\!]$ safe ℓ.
Therefore $[\![T_3 \Rightarrow^\ell T_1]\!] \to^\epsilon [\![T_2 \Rightarrow^\ell T_1]\!]$ safe ℓ.

Case SREFREF

$$\frac{}{\mathsf{ref}\ T <:_b \mathsf{ref}\ T}$$

Have $[\![\mathsf{ref}\ T \Rightarrow^\ell \mathsf{ref}\ T]\!] = \mathsf{ref}^\epsilon\ [\![T \Leftrightarrow^\ell T]\!]$.
By Lemma B.14, $[\![T \Leftrightarrow^\ell T]\!]$ safe ℓ.
Therefore $\mathsf{ref}^\epsilon\ [\![T \Leftrightarrow^\ell T]\!]$ safe ℓ.

We now prove that if $[\![T_1 \Rightarrow^\ell T_2]\!]$ safe ℓ, then $T_1 <:_b T_2$ by induction on $[\![T_1 \Rightarrow^\ell T_2]\!]$ safe ℓ.

Case LINT

$$\frac{q \neq \ell}{\mathsf{int}^q \text{ safe } \ell}$$

There are three ℓ-labeled casts that compile to int^q:
Subcase $[\![\mathsf{int} \Rightarrow^\ell \mathsf{int}]\!]$:
Have that $\mathsf{int} <:_b \mathsf{int}$.
Subcase $[\![\mathsf{int} \Rightarrow^\ell \star]\!]$:
Have that $\mathsf{int} <:_b \star$.
Subcase $[\![\star \Rightarrow^\ell \mathsf{int}]\!]$:
Then $q = \ell$, which is contradictory.

Case LBOT is vacuous.

Case LDYN

$$\frac{}{\star \text{ safe } \ell}$$

The only ℓ-labeled cast that compiles to $\star$ is $\star \Rightarrow^\ell \star$. Have that $\star <:_b \star$.

Case LFUNC

$$\frac{q \neq \ell \qquad L_1 \text{ safe } \ell \qquad L_2 \text{ safe } \ell}{L_1 \to^q L_2 \text{ safe } \ell}$$

There are three ℓ-labeled casts that compile to $L_1 \to^q L_2$:
Subcase $[\![T_1 \to T_2 \Rightarrow^\ell T_3 \to T_4]\!]$:
Then $L_1 = [\![T_3 \Rightarrow^\ell T_1]\!]$ and $L_2 = [\![T_2 \Rightarrow^\ell T_4]\!]$.
By the IH, $T_3 <:_b T_1$.
By the IH, $T_2 <:_b T_4$.
Thus $T_1 \to T_2 <:_b T_3 \to T_4$.
Subcase $[\![T_1 \to T_2 \Rightarrow^\ell \star]\!]$:
Then $L_1 = [\![\star \Rightarrow^\ell T_1]\!]$ and $L_2 = [\![T_2 \Rightarrow^\ell \star]\!]$.
By the IH, $\star <:_b T_1$.
By the IH, $T_2 <:_b \star$.
Hence $T_1 \to T_2 <:_b \star \to \star$.
Thus $T_1 \to T_2 <:_b \star$.
Subcase $[\![\star \Rightarrow^\ell T_1 \to T_2]\!]$:
Then $q = \ell$, which is contradictory.

Case LREF

$$\frac{q \neq \ell \qquad L \text{ safe } \ell}{\mathsf{ref}^q\ L \text{ safe } \ell}$$

There are three ℓ-labeled casts that compile to $\mathsf{ref}^q\ L$:
Subcase $[\![\mathsf{ref}\ T_1 \Rightarrow^\ell \mathsf{ref}\ T_2]\!]$:
Then $L = [\![T_2 \Leftrightarrow^\ell T_1]\!]$.
By the IH, $T_1 = T_2$.
Thus $\mathsf{ref}\ T_1 <:_b \mathsf{ref}\ T_2$.
Subcase $[\![\mathsf{ref}\ T \Rightarrow^\ell \star]\!]$:
Then $L = [\![\star \Leftrightarrow^\ell T]\!]$.
By the IH, $\star = T$.
Hence $\mathsf{ref}\ T <:_b \mathsf{ref}\ \star$.
Thus $\mathsf{ref}\ T <:_b \star$.
Subcase $[\![\star \Rightarrow^\ell T_1 \to T_2]\!]$:
Then $q = \ell$, which is contradictory.

□

Lemma B.16. *If $\mathcal{B} \vdash b$ safe ℓ, then $\varrho(\mathcal{B}, a, b) \vdash b$ safe ℓ.*

Proof. By induction on $\mathcal{B} \vdash b$ safe ℓ.

Case SFLTYPE

$$\frac{L \text{ safe } \ell}{\mathcal{B} \vdash L \text{ safe } \ell}$$

Since $\mathcal{B}$ not used and L safe ℓ, $\varrho(\mathcal{B}, a, L) \vdash L$ safe ℓ.

Case SFPTR

$$\frac{\forall b' \in \mathcal{B}(a') \setminus \{\langle a', r\rangle\},\ \mathcal{B} \vdash b' \text{ safe } \ell}{\mathcal{B} \vdash \langle a', r\rangle \text{ safe } \ell}$$

Subcases on $a = a'$.
Subcase $a = a'$
Then $\forall b' \in \mathcal{B}(a) \setminus \{\langle a, r\rangle\},\ \mathcal{B} \vdash b'$ safe ℓ.
Have that $b = \langle a', r\rangle$.

$$\begin{aligned}\varrho(\mathcal{B}, a, \langle a, r\rangle))(a) \setminus \{\langle a, r\rangle\} &= (\mathcal{B}(a) \cup \{\langle a, r\rangle\}) \setminus \{\langle a, r\rangle\} \\ &= \mathcal{B}(a) \setminus \{\langle a, r\rangle\}\end{aligned}$$

By the IH, $\forall b' \in \mathcal{B}(a) \setminus \{\langle a, r\rangle\},\ \varrho(\mathcal{B}, a, b) \vdash b'$ safe ℓ.
Therefore, $\varrho(\mathcal{B}, a, b) \vdash b$ safe ℓ.
Subcase $a \neq a'$
Then $\mathcal{B}(a') = \varrho(\mathcal{B}, a, b)(a')$.
By the IH, $\forall b' \in \mathcal{B}(a') \setminus \{\langle a', r\rangle\},\ \varrho(\mathcal{B}, a, b) \vdash b'$ safe ℓ.
Therefore, $\varrho(\mathcal{B}, a, b) \vdash b$ safe ℓ.

□

Lemma B.17. *If $\mathcal{B} \vdash b$ safe ℓ and $\mathcal{B} \vdash b'$ safe ℓ, then $\varrho(\mathcal{B}, a, b') \vdash b$ safe ℓ.*

Proof. By induction on $\mathcal{B} \vdash b$ safe ℓ.

Case SFLTYPE

$$\frac{L \text{ safe } \ell}{\mathcal{B} \vdash L \text{ safe } \ell}$$

Since $\mathcal{B}$ not used and L safe ℓ, $\varrho(\mathcal{B}, a, b') \vdash L$ safe ℓ.

Case SFPTR

$$\frac{\forall b'' \in \mathcal{B}(a') \setminus \{\langle a', r\rangle\},\ \mathcal{B} \vdash b'' \text{ safe } \ell}{\mathcal{B} \vdash \langle a', r\rangle \text{ safe } \ell}$$

Subcases on $a = a'$.
Subcase $a = a'$
Then $\forall b'' \in \mathcal{B}(a) \setminus \{\langle a, r\rangle\},\ \mathcal{B} \vdash b''$ safe ℓ.
By the IH, $\forall b'' \in \mathcal{B}(a) \setminus \{\langle a, r\rangle\},\ \varrho(\mathcal{B}, a, b') \vdash b''$ safe ℓ
By Lemma B.16, $\varrho(\mathcal{B}, a, b') \vdash b'$ safe ℓ.
Therefore, $\varrho(\mathcal{B}, a, b') \vdash b$ safe ℓ.
Subcase $a \neq a'$
Then $\mathcal{B}(a') = \varrho(\mathcal{B}, a, b)(a')$.
By the IH, $\forall b'' \in \mathcal{B}(a') \setminus \{\langle a', r\rangle\},\ \varrho(\mathcal{B}, a, b') \vdash b''$ safe ℓ
Therefore, $\varrho(\mathcal{B}, a, b') \vdash b$ safe ℓ.

□

Lemma B.18. *If $\mathcal{B} \vdash e$ safe ℓ and $\mathcal{B} \vdash b$ safe ℓ, then $\varrho(\mathcal{B}, a, b) \vdash e$ safe ℓ.*

Proof. By straightforward induction on $\mathcal{B} \vdash e$ safe ℓ. Only interesting case:

Case SFADDR

$$\frac{\forall b' \in \mathcal{B}(a'),\ \mathcal{B} \vdash b' \text{ safe } \ell}{\mathcal{B} \vdash a' \text{ safe } \ell}$$

By Lemma B.17, $\forall b' \in \varrho(\mathcal{B}, a, b)(a'),\ \varrho(\mathcal{B}, a, b) \vdash b' \text{ safe } \ell$.
Therefore $\varrho(\mathcal{B}, a, b) \vdash a' \text{ safe } \ell$

□

Lemma B.19. *If $\mathcal{B} \vdash \sigma$ safe ℓ and $\mathcal{B} \vdash b$ safe ℓ, then $\varrho(\mathcal{B}, a, b) \vdash \sigma$ safe ℓ.*

Proof. By straightforward induction on $\mathcal{B} \vdash \sigma \text{ safe } \ell$, using Lemma B.18. □

Lemma B.20. *If $\mathcal{B} \vdash e_1$ safe ℓ and $\mathcal{B} \vdash e_2$ safe ℓ, then $\mathcal{B} \vdash e_1[e_2/x]$ safe.*

Proof. By straightforward induction on $\mathcal{B} \vdash e_1 \text{ safe } \ell$. □

Lemma B.21. *If $\mathcal{B} \vdash e$ safe ℓ and $\mathcal{B} \vdash \sigma$ safe ℓ and $\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \langle e', \sigma', \mathcal{B}'\rangle$, then $\mathcal{B}' \vdash e'$ safe ℓ and $\mathcal{B}' \vdash \sigma'$ safe ℓ.*

Proof. By induction on $\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \langle e', \sigma', \mathcal{B}'\rangle$.

Case EFUN With fresh(a),

$$\langle \texttt{fun}\ f\ x.\ e, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto (\lambda x.e[a/f])], \mathcal{B}\rangle$$

Since $\mathcal{B} \vdash \texttt{fun}\ f\ x.\ e$ safe ℓ, have $\mathcal{B} \vdash e$ safe ℓ.
Since a fresh, $\mathcal{B}(a) = \emptyset$. Thus by SFADDR, $\mathcal{B} \vdash a$ safe ℓ.
By Lemma B.20, $\mathcal{B} \vdash e[a/f]$ safe ℓ.
By SFHEAPCLOSURE, $\mathcal{B} \vdash \sigma[a \mapsto (\lambda x.e[a/f])]$ safe ℓ.

Case EAPP Where $\sigma(a) = (\lambda x.e)$,

$$\langle a\ v^p, \sigma, \mathcal{B}\rangle \longrightarrow \langle e[v/x], \sigma, \mathcal{B}\rangle$$

Since $\mathcal{B} \vdash \sigma$ safe ℓ, $\mathcal{B} \vdash e$ safe ℓ.
By inversion, $\mathcal{B} \vdash v$ safe ℓ.
By Lemma B.20, $\mathcal{B} \vdash e[v/x]$ safe $\mathcal{B}$.

Case EREF With fresh(a),

$$\langle \texttt{ref}\ v, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma[a \mapsto v], \mathcal{B}\rangle$$

Since $\mathcal{B} \vdash \texttt{ref}\ v$ safe ℓ, have $\mathcal{B} \vdash v$ safe ℓ.
Since a fresh, $\mathcal{B}(a) = \emptyset$. Thus by SFADDR, $\mathcal{B} \vdash a$ safe ℓ.
By SFHEAPCELL, $\mathcal{B} \vdash \sigma[a \mapsto v]$ safe ℓ.

Case EDEREF With $\sigma(a) = v$,

$$\langle !a^p, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle$$

Since $\mathcal{B} \vdash \sigma$ safe ℓ, $\mathcal{B} \vdash v$ safe ℓ.

Case EUPDTREF With $\sigma(a) = v'$,

$$\langle a :=^p v, \sigma, \mathcal{B}\rangle \longrightarrow \langle 0, \sigma[a \mapsto v], \mathcal{B}\rangle$$

Since $\mathcal{B} \vdash a :=^p v$ safe ℓ, have $\mathcal{B} \vdash v$ safe ℓ.
By SFHEAPCELL, $\mathcal{B} \vdash \sigma[a \mapsto v]$ safe ℓ.
By SFINT, $\mathcal{B} \vdash 0$ safe ℓ.

Case EADD With $n' = n_1 + n_2$,

$$\langle n_1\ +^p\ n_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle n', \sigma, \mathcal{B}\rangle$$

By SFINT, $\mathcal{B} \vdash n'$ safe ℓ.

Case ECHECKFIRST With *hastype*(σ, v, S) and $v \neq a$,

$$\langle v \Downarrow \langle S'; a; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle$$

By inversion, $\mathcal{B} \vdash v$ safe ℓ.

Case ECHECKHO With *hastype*(σ, a', S),

$$\langle a' \Downarrow \langle S'; a; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \langle a', \sigma, \varrho(\mathcal{B}, a', \langle a, r\rangle)\rangle$$

By inversion $\mathcal{B} \vdash a$ safe ℓ and $\mathcal{B} \vdash a'$ safe ℓ.
Therefore, for all $b \in \mathcal{B}(a)$, $\mathcal{B} \vdash b$ safe ℓ.
Hence $\mathcal{B} \vdash \langle a, r\rangle$ safe ℓ.
By Lemma B.18, $\varrho(\mathcal{B}, a', \langle a, r\rangle) \vdash a'$ safe ℓ.
By Lemma B.19, $\varrho(\mathcal{B}, a', \langle a, r\rangle) \vdash \sigma$ safe ℓ.

Case ECHECKFAIL is vacuous.

Case ECASTFIRST With *hastype*$(\sigma, v, \lfloor T_2 \rfloor)$ and $v \neq a$,

$$\langle v{::}T_1 \Rightarrow^{\ell'} T_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle v, \sigma, \mathcal{B}\rangle$$

By inversion $\mathcal{B} \vdash v$ safe ℓ.

Case ECASTHO With *hastype*$(\sigma, a, \lfloor T_2 \rfloor)$,

$$\langle a{::}T_1 \Rightarrow^{\ell'} T_2, \sigma, \mathcal{B}\rangle \longrightarrow \langle a, \sigma, \varrho(\mathcal{B}, a, [\![T_1 \Rightarrow^{\ell'} T_2]\!])\rangle$$

Immediately, $[\![T_1 \Rightarrow^{\ell'} T_2]\!]$ safe ℓ.
Therefore $\mathcal{B} \vdash [\![T_1 \Rightarrow^{\ell'} T_2]\!]$ safe ℓ.
By inversion $\mathcal{B} \vdash a$ safe ℓ.
By Lemma B.18, $\varrho(\mathcal{B}, a, [\![T_1 \Rightarrow^{\ell'} T_2]\!]) \vdash a$ safe ℓ.
By Lemma B.19, $\varrho(\mathcal{B}, a, [\![T_1 \Rightarrow^{\ell'} T_2]\!]) \vdash \sigma$ safe ℓ.

Case ECASTFAIL is vacuous.

□

Lemma B.22. *If L safe ℓ, then extract$(\overline{r}, L)$ safe ℓ.*

Proof. By straightforward induction on *extract*$(\overline{r}, L)$, using inversion on the safe relation. □

Lemma B.23. *If $\mathcal{B} \vdash b$ safe ℓ and collectblame$(\overline{r}, \mathcal{B}, b) = \overline{L}$, then $\ell \notin \{label(L) \mid L \in \overline{L}\}$.*

Proof. By induction on *collectblame*$(\overline{r}, \mathcal{B}, b) = \overline{L}$.

Case

$$\frac{extract(\overline{r}, L) = L' \qquad label(L') = \ell'}{collectblame(\overline{r}, \mathcal{B}, L) = \{L'\}}$$

Since $b = L$ and $\mathcal{B} \vdash L$ safe ℓ, L safe ℓ. By Lemma B.22, L' safe ℓ. Therefore $label(L') \neq \ell$.

Case

$$\frac{extract(\overline{r}, L) = L' \qquad label(L') = \epsilon}{collectblame(\overline{r}, \mathcal{B}, L) = \emptyset}$$

Trivially, $\ell \notin \{label(L) \mid L \in \emptyset\}$.

Case

$$\frac{}{collectblame(\overline{r}, \mathcal{B}, \langle a, r\rangle) = \cup_{b' \in \mathcal{B}(a)}\ collectblame((r;\overline{r}), \mathcal{B}, b')}$$

Since $b = \langle a, r\rangle$ and $\mathcal{B} \vdash \langle a, r\rangle$ safe ℓ, $\forall b' \in \mathcal{B}(a)$, $\mathcal{B} \vdash b'$ safe ℓ.
By the IH, for each a', $\ell \notin \{label(L) \mid L \in collectblame((r;\overline{r}), \mathcal{B}, b')\}$.
Hence $\ell \notin \{label(L) \mid L \in \cup_{b' \in \mathcal{B}(a)}\ collectblame((r;\overline{r}), \mathcal{B}, b')\}$.

□

Lemma B.24. *Have that resolve$(\sigma, v, \overline{L}) \subseteq \{label(L) \mid L \in \overline{L}\}$.*

Proof. Straightforward induction on *resolve*$(\sigma, v, \overline{L})$. □

Lemma B.25. *If $\mathcal{B} \vdash a$ safe ℓ and blame$(\sigma, v, a, r, \mathcal{B}) =$ BLAME$(\mathcal{L})$, then $\ell \notin \mathcal{L}$.*

Proof. Have

$$\frac{\overline{L} = \cup_{b \in \mathcal{B}(a)}\ \mathit{collectblame}(r, \mathcal{B}, b) \qquad \mathcal{L} = \mathit{resolve}(\sigma, v, \overline{L})}{\mathit{blame}(\sigma, v, a, r, \mathcal{B}) = \textsc{Blame}(\mathcal{L})}$$

Since $\mathcal{B} \vdash a$ safe ℓ, have that for all $b \in \mathcal{B}(a)$, $\mathcal{B} \vdash b$ safe ℓ.
By Lemma B.23, $\ell \notin \{\mathit{label}(L) \mid L \in \overline{L}\}$.
By Lemma B.24, $\mathcal{L} \subseteq \{\mathit{label}(L) \mid L \in \overline{L}\}$
Therefore $\ell \notin \mathcal{L}$. □

Lemma B.26. *If* $\emptyset; \Sigma \vdash v : \lfloor T_1 \rfloor$ *and* $\Sigma \vdash \sigma$ *and* $[\![T_1 \Rightarrow^{\ell} T_2]\!]$ *safe* ℓ*, then* $\mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor)$.

Proof. By induction on $\emptyset; \Sigma \vdash v : \lfloor T_1 \rfloor$. Most cases vacuous.

Case TInt
Then $T_1 = \mathsf{int}$ and $v = n$. For it to hold that $[\![\mathsf{int} \Rightarrow^{\ell} T_2]\!]$ safe ℓ, then either $T_2 = \mathsf{int}$ or $T_2 = \star$. In either case, $\mathit{hastype}(\sigma, n, \lfloor T_2 \rfloor)$.

Case TAddr
Then $v = a$ and $\lfloor T_1 \rfloor = \Sigma(a)$.
Subcase $\lfloor T_1 \rfloor = \mathsf{ref}$:
Then $\sigma(a) = v$.
For it to hold that $[\![T_1 \Rightarrow^{\ell} T_2]\!]$ safe ℓ with $\lfloor T_1 \rfloor = \mathsf{ref}$, either $\lfloor T_2 \rfloor = \star$ or $\lfloor T_2 \rfloor = \mathsf{ref}$. (This is necessary but not sufficient.) In either case, $\mathit{hastype}(\sigma, a, \lfloor T_2 \rfloor)$.
Subcase $\lfloor T_1 \rfloor = \rightarrow$:
Then $\sigma(a) = (\lambda x.e)$.
For it to hold that $[\![T_1 \Rightarrow^{\ell} T_2]\!]$ safe ℓ with $\lfloor T_1 \rfloor = \rightarrow$, either $\lfloor T_2 \rfloor = \star$ or $\lfloor T_2 \rfloor = \rightarrow$. (This is necessary but not sufficient.) In either case, $\mathit{hastype}(\sigma, a, \lfloor T_2 \rfloor)$.

Case TSubsump
Then $T_1 = \star$. For it to hold that $[\![\star \Rightarrow^{\ell} T_2]\!]$ safe ℓ, we must have $T_2 = \star$. Then we have that $\mathit{hastype}(\sigma, v, \star)$.

□

Lemma B.27. *If* $\emptyset; \Sigma \vdash e : S$ *and* $\Sigma \vdash \sigma$ *and* $\mathcal{B} \vdash e$ *safe* ℓ *and* $\mathcal{B} \vdash \sigma$ *safe* ℓ *and* $\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \varsigma$*, then* $\varsigma \neq \textsc{Blame}(\mathcal{L})$ *with* $\ell \in \mathcal{L}$.

Proof. By induction on $\langle e, \sigma, \mathcal{B}\rangle \longrightarrow \varsigma$. Most cases vacuous.

Case ECheckFail With $\neg(\mathit{hastype}(\sigma, v, S))$,

$$\langle v \Downarrow \langle S; a; r\rangle, \sigma, \mathcal{B}\rangle \longrightarrow \mathit{blame}(\sigma, v, a, r, \mathcal{B})$$

By inversion, $\mathcal{B} \vdash a$ safe ℓ.
Suppose $\mathit{blame}(\sigma, v, a, r, \mathcal{B}) = \textsc{Blame}(\mathcal{L})$.
Then by Lemma B.25, $\ell \notin \mathcal{L}$.

Case ECastFail With $\neg(\mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor))$,

$$\langle v :: T_1 \Rightarrow^{\ell'} T_2, \sigma, \mathcal{B}\rangle \longrightarrow \textsc{Blame}(\{\ell'\})$$

Subcase $\ell \neq \ell'$:
Have immediately that $\ell \notin \{\ell'\}$.
Subcase $\ell = \ell'$:
Since $\mathcal{B} \vdash v :: T_1 \Rightarrow^{\ell} T_2$ safe ℓ, $[\![T_1 \Rightarrow^{\ell} T_2]\!]$ safe ℓ.
By Lemma B.4, $\emptyset; \Sigma \vdash v : \lfloor T_1 \rfloor$.
By Lemma B.26, $\mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor)$. But this contradicts $\neg(\mathit{hastype}(\sigma, v, \lfloor T_2 \rfloor))$.

□

Lemma B.28. *Suppose that* $\emptyset; \emptyset \vdash e : S$ *and that* e *contains a subterm* $e' :: T_1 \Rightarrow^{\ell} T_2$ *containing the only occurrence of* ℓ *in* e*. Then if* $T_1 <:_b T_2$, $\langle e, \emptyset, \emptyset\rangle \not\longrightarrow \textsc{Blame}(\mathcal{L})$ *with* $\ell \in \mathcal{L}$.

Proof. By Lemma B.15, $[\![T_1 \Rightarrow^{\ell} T_2]\!]$ safe ℓ. Since ℓ does not otherwise occur in e, $\emptyset \vdash e$ safe ℓ. Then by applying Lemmas B.9, B.27, and B.21, we have that $\langle e, \emptyset, \emptyset\rangle \not\longrightarrow^{*} \textsc{Blame}(\mathcal{L})$ with $\ell \in \mathcal{L}$. □

B.3 The gradual guarantee

Lemma B.29. *If* $T_1 \sim T_2$ *and* $T_1 \sqsubseteq T_1'$ *and* $T_2 \sqsubseteq T_2'$*, then* $T_1' \sim T_2'$.

Proof. By induction on $T_1 \sim T_2$, and then cases on T_1' and T_2'.

Case $T_{11} \to T_{12} \sim T_{21} \to T_{22}$

$$\frac{T_{11} \sim T_{21} \qquad T_{12} \sim T_{22}}{T_{11} \to T_{12} \sim T_{21} \to T_{22}}$$

Have that T_1' must be either $\star$ or $T_{11}' \to T_{12}'$.
In the former case, theorem holds immediately.
Otherwise, have that $T_{11} \sqsubseteq T_{11}'$ and $T_{12} \sqsubseteq T_{12}'$.
Then have that T_2' must be either $\star$ or $T_{21}' \to T_{22}'$.
In the former case, theorem holds immediately.
Otherwise, have that $T_{21} \sqsubseteq T_{21}'$ and $T_{22} \sqsubseteq T_{22}'$.
Then by the IH, $T_{11}' \sim T_{21}'$ and $T_{12}' \sim T_{22}'$.
Therefore $T_{11}' \to T_{12}' \sim T_{21}' \to T_{22}'$.

Remaining cases are similar. □

Lemma B.30. *If* $T_1 \sqsubseteq T_2$ *and* $T_1 \rhd T_{11} \to T_{12}$ *then* $T_2 \rhd T_{21} \to T_{22}$ *and* $T_{11} \sqsubseteq T_{21}$ *and* $T_{12} \sqsubseteq T_{22}$.

Proof. By cases on $T_1 \sqsubseteq T_2$.

Case $T \sqsubseteq \star$
Then $T_{21} = T_{22} = \star$.
Proceed by subcases on T
Subcase $T = \star$ Then $T_{11} = T_{12} = \star$.
Have $\star \sqsubseteq \star$.
Subcase $T = T_{11}' \to T_{12}'$ Then $T_{11} = T_{11}'$ and $T_{12} = T_{12}'$.
Have $T_{11} \sqsubseteq \star$ and $T_{12} \sqsubseteq \star$.
Other subcases vacuous.

Case $T_{11}' \to T_{12}' \sqsubseteq T_{21}' \to T_{22}'$
Have $T_{11}' \sqsubseteq T_{21}'$ and $T_{12}' \sqsubseteq T_{22}'$
Have $T_{11} = T_{11}'$ and $T_{12} = T_{12}'$ and $T_{21} = T_{21}'$ and $T_{22} = T_{22}'$.

Other subcases vacuous. □

Lemma B.31. *If* $T_1 \sqsubseteq T_2$ *and* $T_1 \rhd \mathsf{ref}\, T_1'$ *then* $T_2 \rhd \mathsf{ref}\, T_2'$ *and* $T_1' \sqsubseteq T_2'$.

Proof. By cases on $T_1 \sqsubseteq T_2$.

Case $T \sqsubseteq \star$
Then $T_2' = \star$.
Proceed by subcases on T
Subcase $T = \star$ Then $T_1' = \star$.
Have $\star \sqsubseteq \star$.
Subcase $T = \mathsf{ref}\, T_1''$ Then $T_1' = T_1''$.
Have $T_1' \sqsubseteq \star$.
Other subcases vacuous.

Case $\mathsf{ref}\, T_1'' \sqsubseteq \mathsf{ref}\, T_2''$
Have $T_1'' \sqsubseteq T_2''$.
Have $T_1'' = T_1'$ and $T_2'' = T_2'$.

Other subcases vacuous. □

Lemma B.32 (Weakening preserves cast insertion)**.** *If* $e_{s1} \sqsubseteq e_{s2}$ *and* $\Gamma_1 \sqsubseteq \Gamma_2$ *and* $\Gamma_1 \vdash e_{s1} \rightsquigarrow e_1 : T_1$*, then* $\Gamma_2 \vdash e_{s2} \rightsquigarrow e_2 : T_2$ *and* $T_1 \sqsubseteq T_2$.

Proof. By induction on $e_{s1} \sqsubseteq e_{s2}$.

Case PEVAR

Since $\Gamma_1 \sqsubseteq \Gamma_2$ and $\Gamma_1(x) = T_1$, have that $\Gamma_2(x) = T_2$ and $T_1 \sqsubseteq T_2$. Therefore $\Gamma_2 \vdash x \rightsquigarrow x : T_2$.

Case PEINT is immediate.

Case PEFUN

$$\frac{T_{11} \sqsubseteq T_{21} \qquad T_{12} \sqsubseteq T_{22} \qquad e_{s1} \sqsubseteq e_{s2}}{\texttt{fun}\ f\ (x{:}T_{11}) \to T_{12}.\ e_{s1} \sqsubseteq \texttt{fun}\ f\ (x{:}T_{21}) \to T_{22}.\ e_{s2}}$$

Immediately, $T_{11} \to T_{12} \sqsubseteq T_{21} \to T_{22}$.
Since $\Gamma_1 \sqsubseteq \Gamma_2$ and $T_{11} \to T_{12} \sqsubseteq T_{21} \to T_{22}$ and $T_{11} \sqsubseteq T_{12}$, have that $\Gamma_1, f : T_{11} \to T_{12}, x : T_{11} \sqsubseteq \Gamma_2, f : T_{21} \to T_{22}, x : T_{21}$.
By inversion, $\Gamma_1, f : T_{11} \to T_{12}, x : T_{11} \vdash e_{s1} \rightsquigarrow e_1 : T'_{12}$ and $T'_{12} \sim T_{12}$.
By the IH, $\Gamma_2, f : T_{21} \to T_{22}, x : T_{21} \vdash e_{s2} \rightsquigarrow e_2 : T'_{22}$ and $T_{12'} \sqsubseteq T'_{22}$.
By Lemma B.29, $T'_{22} \sim T_{22}$.
Therefore by CFUN $\Gamma' \vdash \texttt{fun}\ f\ (x{:}T_{21}) \to T_{22}.\ e_{s2} \rightsquigarrow e : T_{21} \to T_{22}$.

Case PEAPP

$$\frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11}\ e_{s12} \sqsubseteq e_{s21}\ e_{s22}}$$

By inversion, $\Gamma_1 \vdash e_{s11} \rightsquigarrow e_{11} : T_1$.
By the IH, $\Gamma_2 \vdash e_{s21} \rightsquigarrow e_{21} : T_2$ and $T_1 \sqsubseteq T_2$.
By inversion, $T_1 \rhd T_{11} \to T_{12}$.
By Lemma B.30, $T_2 \rhd T_{21} \to T_{22}$ and $T_{11} \sqsubseteq T_{21}$ and $T_{12} \sqsubseteq T_{22}$. By inversion, $\Gamma_1 \vdash e_{s12} \rightsquigarrow e_{12} : T'_{11}$.
By the IH, $\Gamma_2 \vdash e_{s22} \rightsquigarrow e_{22} : T'_{21}$ and $T'_{11} \sqsubseteq T'_{21}$.
By Lemma B.29, $T'_{21} \sim T_{21}$.
By CAPP, $\Gamma_2 \vdash e_{s21}\ e_{s22} \rightsquigarrow e : T_{22}$.

Case PEREF

$$\frac{e_{s1} \sqsubseteq e_{s2}}{\texttt{ref}\ e_{s1} \sqsubseteq \texttt{ref}\ e_{s2}}$$

By inversion, $\Gamma_1 \vdash e_{s1} \rightsquigarrow e_1 : T_1$.
By the IH, $\Gamma_2 \vdash e_{s2} \rightsquigarrow e_2 : T_2$ and $T_1 \sqsubseteq T_2$.
Thus $\mathsf{ref}\ T_1 \sqsubseteq \mathsf{ref}\ T_2$.
By CREF, $\Gamma_2 \vdash \texttt{ref}\ e_{s2} \rightsquigarrow e : \mathsf{ref}\ T_2$.

Case PEDEREF

$$\frac{e_{s1} \sqsubseteq e_{s2}}{!e_{s1} \sqsubseteq !e_{s2}}$$

By inversion, $\Gamma_1 \vdash e_{s1} \rightsquigarrow e_1 : T_1$.
By the IH, $\Gamma_2 \vdash e_{s2} \rightsquigarrow e_2 : T_2$ and $T_1 \sqsubseteq T_2$.
By inversion, $T_1 \rhd \mathsf{ref}\ T'_1$.
By Lemma B.31, $T_2 \rhd \mathsf{ref}\ T'_2$ and $T'_1 \sqsubseteq T'_2$.
By CDEREF, $\Gamma_2 \vdash !e_{s2} \rightsquigarrow e : T'_2$.

Case PESET

$$\frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11} := e_{s12} \sqsubseteq e_{s21} := e_{s22}}$$

By inversion, $\Gamma_1 \vdash e_{s11} \rightsquigarrow e_{11} : T_1$.
By the IH, $\Gamma_2 \vdash e_{s21} \rightsquigarrow e_{21} : T_2$ and $T_1 \sqsubseteq T_2$.
By inversion, $T_1 \rhd \mathsf{ref}\ T'_1$.
By Lemma B.31, $T_2 \rhd \mathsf{ref}\ T'_2$ and $T'_1 \sqsubseteq T'_2$.
By inversion, $\Gamma_1 \vdash e_{s12} \rightsquigarrow e_{12} : T'_1$.
By the IH, $\Gamma_2 \vdash e_{s22} \rightsquigarrow e_{22} : T'_2$ and $T'_1 \sqsubseteq T'_2$.
By inversion, $T_1 \sim T'_1$.
By Lemma B.29, $T_2 \sim T'_2$.
By CUPDTREF, $\Gamma_2 \vdash e_{s21} := e_{s22} \rightsquigarrow e : \mathsf{int}$.

Case PEADD

$$\frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11}\ +\ e_{s12} \sqsubseteq e_{s21}\ +\ e_{s22}}$$

By inversion, $\Gamma_1 \vdash e_{s11} \rightsquigarrow e_{11} : T_{11}$.
By the IH, $\Gamma_2 \vdash e_{s21} \rightsquigarrow e_{21} : T_{21}$ and $T_{11} \sqsubseteq T_{21}$.
By inversion, $\Gamma_1 \vdash e_{s12} \rightsquigarrow e_{12} : T_{12}$.
By the IH, $\Gamma_2 \vdash e_{s22} \rightsquigarrow e_{22} : T_{22}$ and $T_{12} \sqsubseteq T_{22}$.
By inversion $T_{11} \sim \mathsf{int}$ and $T_{12} \sim \mathsf{int}$.
By Lemma B.29, $T_{21} \sim \mathsf{int}$ and $T_{22} \sim \mathsf{int}$.
By CADD, $\Gamma_2 \vdash e_{s21}\ +\ e_{s22} \rightsquigarrow e : \mathsf{int}$.

□

Lemma B.33. *If* $T_1 \sqsubseteq T_2$ *then* $\lfloor T_1 \rfloor \sqsubseteq \lfloor T_2 \rfloor$.

Proof. Immediately by cases on $T_1 \sqsubseteq T_2$. □

Lemma B.34 (Cast insertion preserves precision)**.** *If* $\Gamma \vdash e_s \rightsquigarrow e : T$ *and* $\Gamma' \vdash e'_s \rightsquigarrow e' : T'$ *and* $e_s \sqsubseteq e'_s$ *and* $\Gamma \sqsubseteq \Gamma'$*, then* $e \sqsubseteq e'$ *and* $T \sqsubseteq T'$.

Proof. By induction on $e_s \sqsubseteq e'_s$.

Case PEVAR

$$x \sqsubseteq x$$

Since $\Gamma(x) = T$ and $\Gamma \sqsubseteq \Gamma', T \sqsubseteq T'$.
By PVAR, $x \sqsubseteq x$.

Case PEINT

$$n \sqsubseteq n$$

Have $T = T' = \mathsf{int}$.
By PINT, $n \sqsubseteq n$.

Case PEFUN

$$\frac{T_{11} \sqsubseteq T_{21} \qquad T_{12} \sqsubseteq T_{22} \qquad e_{s1} \sqsubseteq e_{s2}}{\texttt{fun}\ f\ (x{:}T_{11}) \to T_{12}.\ e_{s1} \sqsubseteq \texttt{fun}\ f\ (x{:}T_{21}) \to T_{22}.\ e_{s2}}$$

Have $\Gamma \vdash \texttt{fun}\ f\ (x{:}T_{11}) \to T_{12}.\ e_{s1} \rightsquigarrow \texttt{fun}\ f\ x.\ (\texttt{let}\ x = x{\Downarrow}\langle \lfloor T_{11} \rfloor; f; \textsc{Arg} \rangle\ \texttt{in}\ e_1) : T_{11} \to T_{12}$.
Have $\Gamma' \vdash \texttt{fun}\ f\ (x{:}T_{21}) \to T_{22}.\ e_{s1} \rightsquigarrow \texttt{fun}\ f\ x.\ (\texttt{let}\ x = x{\Downarrow}\langle \lfloor T_{21} \rfloor; f; \textsc{Arg} \rangle\ \texttt{in}\ e_2) : T_{21} \to T_{22}$.
Immediately have $T_{11} \to T_{12} \sqsubseteq T_{21} \to T_{22}$.
By inversion, $\Gamma, f : T_{11} \to T_{12}, x : T_{11} \vdash e_{s1} \rightsquigarrow e_1 : T'_{12}$.
By inversion, $\Gamma', f : T_{21} \to T_{22}, x : T_{21} \vdash e_{s2} \rightsquigarrow e_2 : T'_{22}$.
Have that $\Gamma, f : T_{11} \to T_{12}, x : T_{11} \sqsubseteq \Gamma', f : T_{21} \to T_{22}, x : T_{21}$.
By the IH, $e_1 \sqsubseteq e_2$.
By PVAR, $x \sqsubseteq x$ and $f \sqsubseteq f$.
By Lemma B.33, $\lfloor T_{11} \rfloor \sqsubseteq \lfloor T_{21} \rfloor$.
Hence by PCHECK, $x{\Downarrow}\langle \lfloor T_{11} \rfloor; f; \textsc{Arg} \rangle \sqsubseteq x{\Downarrow}\langle \lfloor T_{21} \rfloor; f; \textsc{Arg} \rangle$.
Hence by PLET and PFUN, $e \sqsubseteq e'$.

Case PEAPP

$$\frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11}\ e_{s12} \sqsubseteq e_{s21}\ e_{s22}}$$

Have $\Gamma \vdash e_{s11}\ e_{s12} \rightsquigarrow \texttt{let}\ f = e_{11}{::}T_1 \Rightarrow^{\ell} T_{11} \to T_{12}\ \texttt{in}\ (f\ (e_{12}{::}T'_{11} \Rightarrow^{\ell} T_{11})){\Downarrow}\langle \lfloor T_{12} \rfloor; f; \textsc{Res} \rangle : T_{12}$.
Have that ℓ, f fresh in the cast inserion of $e_{s11}\ e_{s12}$.
Assume without loss of generality that ℓ, f fresh in the cast insertion of $e_{s21}\ e_{s22}$, and select them for use in its translation.
Have $\Gamma' \vdash e_{s21}\ e_{s22} \rightsquigarrow \texttt{let}\ f = e_{21}{::}T_2 \Rightarrow^{\ell} T_{21} \to T_{22}\ \texttt{in}\ (f\ (e_{22}{::}T'_{21} \Rightarrow^{\ell} T_{11})){\Downarrow}\langle \lfloor T_{22} \rfloor; f; \textsc{Res} \rangle : T_{22}$.
By inversion, $\Gamma \vdash e_{s11} \rightsquigarrow e_{11} : T_1$ and $T_1 \rhd T_{11} \to T_{12}$.
By inversion, $\Gamma' \vdash e_{s21} \rightsquigarrow e_{21} : T_2$ and $T_2 \rhd T_{21} \to T_{22}$.
By the IH, $e_{11} \sqsubseteq e_{21}$ and $T_1 \sqsubseteq T_2$.
By Lemma B.30, $T_{11} \sqsubseteq T_{21}$ and $T_{21} \sqsubseteq T_{22}$, and therefore

$T_{11} \to T_{12} \sqsubseteq T_{21} \to T_{22}$.
By inversion, $\Gamma \vdash e_{s12} \rightsquigarrow e_{12} : T'_{11}$.
By inversion, $\Gamma' \vdash e_{s22} \rightsquigarrow e_{22} : T'_{21}$.
By the IH, $e_{12} \sqsubseteq e_{22}$ and $T'_{11} \sqsubseteq T'_{21}$.
By Lemma B.33, $\lfloor T_{11} \rfloor \sqsubseteq \lfloor T_{21} \rfloor$.
By PCAST, PVAR, PAPP, PCHECK, and PLET, $e \sqsubseteq e'$.

Case PEREF

$$\frac{e_{s1} \sqsubseteq e_{s2}}{\texttt{ref}\ e_{s1} \sqsubseteq \texttt{ref}\ e_{s2}}$$

Have $\Gamma \vdash \texttt{ref}\ e_{s1} \rightsquigarrow \texttt{ref}\ e_1 : \mathsf{ref}\ T_1$.
Have $\Gamma' \vdash \texttt{ref}\ e_{s2} \rightsquigarrow \texttt{ref}\ e_2 : \mathsf{ref}\ T_2$.
By inversion, $\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T_1$.
By inversion, $\Gamma' \vdash e_{s2} \rightsquigarrow e_2 : T_2$.
By the IH, $e_1 \sqsubseteq e_2$ and $T_1 \sqsubseteq T_2$.
Therefore $\texttt{ref}\ e_1 \sqsubseteq \texttt{ref}\ e_2$ (by PREF) and $\mathsf{ref}\ T_1 \sqsubseteq \mathsf{ref}\ T_2$.

Case PEDEREF

$$\frac{e_{s1} \sqsubseteq e_{s2}}{!e_{s1} \sqsubseteq !e_{s2}}$$

Have $\Gamma \vdash !e_{s1} \rightsquigarrow \texttt{let}\ x = e_1 :: T_1 \Rightarrow^{\ell} \mathsf{ref}\ T'_1\ \texttt{in}\ !x \Downarrow \langle \lfloor T'_1 \rfloor; x; \text{DEREF} \rangle : T'_1$.
Have that ℓ, x fresh in the cast inserion of $!e_{s1}$.
Assume without loss of generality that ℓ, x fresh in the cast insertion of $!e_{s2}$, and select them for use in its translation.
Have $\Gamma' \vdash !e_{s2} \rightsquigarrow \texttt{let}\ x = e_2 :: T_2 \Rightarrow^{\ell} \mathsf{ref}\ T'_2\ \texttt{in}\ !x \Downarrow \langle \lfloor T'_2 \rfloor; x; \text{DEREF} \rangle : T'_2$.
By inversion, $\Gamma \vdash e_{s1} \rightsquigarrow e_1 : T_1$ and $T_1 \rhd \mathsf{ref}\ T'_1$.
By inversion, $\Gamma' \vdash e_{s2} \rightsquigarrow e_2 : T_2$ and $T_2 \rhd \mathsf{ref}\ T'_2$.
By the IH, $e_1 \sqsubseteq e_2$ and $T_1 \sqsubseteq T_2$.
By Lemma B.31, $T'_1 \sqsubseteq T'_2$, and therefore $\mathsf{ref}\ T'_1 \sqsubseteq \mathsf{ref}\ T'_2$.
By Lemma B.33, $\lfloor T'_1 \rfloor \sqsubseteq \lfloor T'_2 \rfloor$. By PCAST, PVAR, PDEREF, PCHECK, and PLET, $e \sqsubseteq e'$.

Case PESET

$$\frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11} := e_{s12} \sqsubseteq e_{s21} := e_{s22}}$$

Have $\Gamma \vdash e_{s11} := e_{s12} \rightsquigarrow (e_{11} :: T_1 \Rightarrow^{\ell_1} \mathsf{ref}\ T'_1 := e_{12} :: T''_1 \Rightarrow^{\ell_2} T'_1) : \mathsf{int}$.
Have that ℓ_1, ℓ_2 fresh in the cast inserion of $e_{s11} := e_{s12}$.
Assume without loss of generality that ℓ_1, ℓ_2 fresh in the cast insertion of $e_{s21} := e_{s22}$, and select them for use in its translation.
Have $\Gamma' \vdash e_{s21} := e_{s22} \rightsquigarrow (e_{21} :: T_2 \Rightarrow^{\ell_1} \mathsf{ref}\ T'_2 := e_{22} :: T''_2 \Rightarrow^{\ell_2} T'_2) : \mathsf{int}$.
By inversion, $\Gamma \vdash e_{s11} \rightsquigarrow e_{11} : T_1$ and $T_1 \rhd \mathsf{ref}\ T'_1$.
By inversion, $\Gamma' \vdash e_{s21} \rightsquigarrow e_{21} : T_2$ and $T_2 \rhd \mathsf{ref}\ T'_2$.
By the IH, $e_{11} \sqsubseteq e_{21}$ and $T_1 \sqsubseteq T_2$.
By Lemma B.31, $T'_1 \sqsubseteq T'_2$, and therefore $\mathsf{ref}\ T'_1 \sqsubseteq \mathsf{ref}\ T'_2$.
By inversion, $\Gamma \vdash e_{s12} \rightsquigarrow e_{12} : T''_1$.
By inversion, $\Gamma' \vdash e_{s22} \rightsquigarrow e_{22} : T''_2$.
By the IH, $e_{12} \sqsubseteq e_{22}$ and $T''_1 \sqsubseteq T''_2$.
By PCAST and PSET, $e \sqsubseteq e'$.

Case PEADD

$$\frac{e_{s11} \sqsubseteq e_{s21} \qquad e_{s12} \sqsubseteq e_{s22}}{e_{s11}\ +\ e_{s12} \sqsubseteq e_{s21}\ +\ e_{s22}}$$

Have $\Gamma \vdash e_{s11}\ +\ e_{s12} \rightsquigarrow e_{11} :: T_{11} \Rightarrow^{\ell_1} \mathsf{int}\ +\ e_{12} :: T_{12} \Rightarrow^{\ell_2} \mathsf{int} : \mathsf{int}$.
Have that ℓ_1, ℓ_2 fresh in the cast inserion of $e_{s11}\ +\ e_{s12}$.
Assume without loss of generality that ℓ_1, ℓ_2 fresh in the cast insertion of $e_{s21}\ +\ e_{s22}$, and select them for use in its translation.
Have $\Gamma' \vdash e_{s21}\ +\ e_{s22} \rightsquigarrow e_{21} :: T_{21} \Rightarrow^{\ell_1} \mathsf{int}\ +\ e_{22} :: T_{22} \Rightarrow^{\ell_2} \mathsf{int} : \mathsf{int}$.
By inversion, $\Gamma \vdash esrcn_{11} \rightsquigarrow e_{11} : T_{11}$.
By inversion, $\Gamma \vdash esrcn_{21} \rightsquigarrow e_{21} : T_{21}$.
By the IH, $e_{11} \sqsubseteq e_{21}$ and $T_{11} \sqsubseteq T_{21}$.
By inversion, $\Gamma \vdash esrcn_{11} \rightsquigarrow e_{11} : T_{11}$.
By inversion, $\Gamma \vdash esrcn_{21} \rightsquigarrow e_{21} : T_{21}$.
By the IH, $e_{11} \sqsubseteq e_{21}$ and $T_{11} \sqsubseteq T_{21}$.
By PCAST and PADD, $e \sqsubseteq e'$.

□

Lemma B.35. *If $v \sqsubseteq e$, then e is a value.*

Proof. By cases on $v \sqsubseteq e$. The only non-vacuous cases are PADDR and PINT. In both cases, e is a value. □

Lemma B.36. *If $e \sqsubseteq v$, then e is a value.*

Proof. By cases on $e \sqsubseteq v$. The only non-vacuous cases are PADDR and PINT. In both cases, e is a value. □

Lemma B.37 (Preservation of simulation under substitution)**.** *Suppose $e_1 \sqsubseteq e'_1$ and $e_2 \sqsubseteq e'_2$. Then $e_1[e_2/x] \sqsubseteq e'_1[e'_2/x]$.*

Proof. By induction on $e_1 \sqsubseteq e'_1$.

Case PVAR

$$y \sqsubseteq y$$

If $x = y$, then $y[e_2/x] = e_2$ and $y[e'_2/x] = e'_2$, and theorem proved by assumption.
Otherwise, $y[e_2/x] = y$ and $y[e'_2/x] = y$, and we prove by applying PVAR.

Cases PINT and PADDR are trivial.

Case PFUN

$$\frac{e_1 \sqsubseteq e'_1}{\texttt{fun}\ f\ y.\ e_1 \sqsubseteq \texttt{fun}\ f\ y.\ e'_1}$$

If $y = x$, then $\texttt{fun}\ f\ y.\ e_1[e_2/x] = \texttt{fun}\ f\ y.\ e_1$ and $\texttt{fun}\ f\ y.\ e'_1[e'_2/x] = \texttt{fun}\ f\ y.\ e'_1$, and the theorem holds by assumption.
Similar if $f = x$.
Otherwise, $\texttt{fun}\ f\ y.\ e_1[e_2/x] = \texttt{fun}\ f\ y.\ e_1[e_2/x]$ and $\texttt{fun}\ f\ y.\ e'_1[e'_2/x] = \texttt{fun}\ f\ y.\ e'_1[e'_2/x]$.
By the IH, $e_1[e_2/x] \sqsubseteq e'_1[e'_2/x]$.
By PFUN $\texttt{fun}\ f\ y.\ e_1[e_2/x] \sqsubseteq \texttt{fun}\ f\ y.\ e'_1[e'_2/x]$.

Remaining cases are similar. □

Lemma B.38. *Suppose $v_1 \sqsubseteq v_2$ and $\sigma_1 \sqsubseteq \sigma_2$ and $S_1 \sqsubseteq S_2$. If $\mathit{hastype}(\sigma_1, v_1, S_1)$, then $\mathit{hastype}(\sigma_2, v_2, S_2)$.*

Proof. By cases on $\mathit{hastype}(\sigma_1, v_1, S_1)$.

Case $\mathit{hastype}(\sigma_1, n_1, \mathsf{int})$
Since $n_1 \sqsubseteq v_2$, $v_2 = n_2$.
Since $\mathsf{int} \sqsubseteq S_2$, either $S_2 = \mathsf{int}$ or $S_2 = \star$.
In either case, $\mathit{hastype}(\sigma_2, n_2, S_2)$.

Case $\mathit{hastype}(\sigma_1, v_1, \star)$
Since $\star \sqsubseteq S_2$, $S_2 = \star$.
For any σ_2, v_2, $\mathit{hastype}(\sigma_2, v_2, \star)$.

Case $\mathit{hastype}(\sigma_1, a, \to)$
Since $\to \sqsubseteq S_2$, either $S_2 = \to$ or $S_2 = \star$.
Suppose that $S_2 = \to$.
Have that $\sigma_1(a) = (\lambda x.e_1)$.
Since $a \sqsubseteq v_2$, $v_2 = a$.
Since $\sigma_1 \sqsubseteq \sigma_2$, $\sigma_2(a) = (\lambda x.e_2)$.
Therefore $\mathit{hastype}(\sigma_2, a, \to)$. Now suppose $S_2 = \star$.
For any σ_2, v_2, $\mathit{hastype}(\sigma_2, v_2, \star)$.

Case *hastype*$(\sigma_1, a, \mathsf{ref})$

Since $\mathsf{ref} \sqsubseteq S_2$, either $S_2 = \mathsf{ref}$ or $S_2 = \star$.
Suppose that $S_2 = \mathsf{ref}$.
Have that $\sigma_1(a) = v_1'$.
Since $a \sqsubseteq v_2$, $v_2 = a$.
Since $\sigma_1 \sqsubseteq \sigma_2$, $\sigma_2(a) = v_2'$.
Therefore *hastype*$(\sigma_2, a, \mathsf{ref})$. Now suppose $S_2 = \star$.
For any σ_2, v_2, *hastype*$(\sigma_2, v_2, \star)$.

□

Lemma B.39 (Simulation of more precise programs)**.** *Suppose* $e_1 \sqsubseteq e_2$ *and* $\sigma_1 \sqsubseteq \sigma_2$. *If* $\langle e_1, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, *then* $\langle e_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle e_2', \sigma_2', \mathcal{B}_2'\rangle$ *and* $e_1' \sqsubseteq e_2'$ *and* $\sigma_1' \sqsubseteq \sigma_2'$.

Proof. By cases on $e_1 \sqsubseteq e_2$.

Cases PVAR, PINT, PADDR are vacuous.

Case PAPP

$$\frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22}}{e_{11}\ e_{12} \sqsubseteq e_{21}\ e_{22}}$$

Since $\langle e_{11}\ e_{12}, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have that $e_{11} = a$, $e_{12} = v_1$, $\sigma_1(a) = (\lambda x.e_{1h})$, $e_1' = e_{1h}[v_1/x]$, and $\sigma_1' = \sigma_1$.
Since $a \sqsubseteq e_{21}$, $e_{21} = a$.
Since $v_1 \sqsubseteq e_{22}$, by Lemma B.35 $e_{22} = v_2$.
Since $\sigma_1 \sqsubseteq \sigma_2$, $(\lambda x.e_{1h}) \sqsubseteq_h \sigma_2(a)$.
Therefore $\sigma_2(a) = (\lambda x.e_{2h})$ and $e_{1h} \sqsubseteq e_{2h}$.
Hence by EAPP, $\langle e_{21}\ e_{22}, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle e_{2h}[v_2/x], \sigma_2, \mathcal{B}_2\rangle$.
By Lemma B.37, $e_{1h}[v_1/x] \sqsubseteq e_{2h}[v_2/x]$.

Case PFUN

$$\frac{e_1 \sqsubseteq e_2}{\mathtt{fun}\ f\ x.\ e_1 \sqsubseteq \mathtt{fun}\ f\ x.\ e_2}$$

Since $\langle \mathtt{fun}\ f\ x.\ e_1, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have that $e_1' = a$ for fresh a and $\sigma_1' = \sigma_1[a \mapsto (\lambda x.e_1[a/f])]$.
Suppose without loss of generality that a is fresh for the evaluation of both e_1 and e_2.
Then $\langle \mathtt{fun}\ f\ x.\ e_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle a, \sigma_2[a \mapsto (\lambda x.e_2[a/f])], \mathcal{B}_2\rangle$.
Have immediately that $a \sqsubseteq a$.
By Lemma B.37, $e_1[a/f] \sqsubseteq e_2[a/f]$.
Therefore $(\lambda x.e_1[a/f]) \sqsubseteq_h (\lambda x.e_2[a/f])$.
Therefore $\sigma_1[a \mapsto (\lambda x.e_1[a/f])] \sqsubseteq \sigma_2[a \mapsto (\lambda x.e_2[a/f])]$.

Case PREF

$$\frac{e_1 \sqsubseteq e_2}{\mathtt{ref}\ e_1 \sqsubseteq \mathtt{ref}\ e_2}$$

Since $\langle \mathtt{ref}\ e_1, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have that $e_1 = v_1$, $e_1' = a$ for fresh a and $\sigma_1' = \sigma_1[a \mapsto v_1]$.
Suppose without loss of generality that a is fresh for the evaluation of both e_1 and e_2.
By Lemma B.35 $e_2 = v_2$.
Then $\langle \mathtt{ref}\ v_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle a, \sigma_2[a \mapsto v_2], \mathcal{B}_2\rangle$.
Have immediately that $a \sqsubseteq a$.
Have that $v_1 \sqsubseteq_h v_2$.
Therefore $\sigma_1[a \mapsto v_1] \sqsubseteq \sigma_2[a \mapsto v_2]$.

Case PDEREF

$$\frac{e_1 \sqsubseteq e_2}{!e_1 \sqsubseteq !e_2}$$

Since $\langle !e_1, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have $e_1 = a$, $\sigma_1(a) = v_1$, and $\sigma_1' = \sigma_1$.
Since $a \sqsubseteq e_2$, $e_2 = a$.
Since $\sigma_1 \sqsubseteq \sigma_2$, $\sigma_2(a) = h$ and $v_1 \sqsubseteq_h h$.
Therefore $h = v_2$ and $v_1 \sqsubseteq v_2$.
Thus $\langle !e_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle v_2, \sigma_2, \mathcal{B}_2\rangle$.

Case PSET

$$\frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22}}{e_{11} := e_{12} \sqsubseteq e_{21} := e_{22}}$$

Since $\langle e_{11} := e_{12}, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have $e_{11} = a$, $e_{12} = v_1$, $\sigma_1(a) = v_1'$, $e_1' = 0$, and $\sigma_1' = \sigma_1[a \mapsto v_1]$.
Since $a \sqsubseteq e_{21}$, $e_{21} = a$.
By Lemma B.35 $e_{22} = v_2$.
Since $\sigma_1 \sqsubseteq \sigma_2$, $\sigma_2(a) = v_2'$.
Therefore $\langle e_{21} := e_{22}, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle 0, \sigma_2[a \mapsto v_2], \mathcal{B}_2\rangle$.
Immediately have $0 \sqsubseteq 0$.
Since $v_1 \sqsubseteq v_2$, $v_1 \sqsubseteq_h v_2$. Thus, since $\sigma_1 \sqsubseteq \sigma_2$, $\sigma_1[a \mapsto v_1] \sqsubseteq \sigma_2[a \mapsto v_2]$.

Case PCHECK

$$\frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22} \qquad S_1 \sqsubseteq S_2}{e_{11} \Downarrow \langle S_1; e_{12}; r\rangle \sqsubseteq e_{21} \Downarrow \langle S_2; e_{22}; r\rangle}$$

Since $\langle e_{11} \Downarrow \langle S_1; e_{12}; r\rangle, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have that $e_{11} = v_1$, $e_{12} = a$, *hastype*(σ_1, v_1, S_1), $e_1' = v_1$, and $\sigma_1' = \sigma_1$.
By Lemma B.35 $e_{21} = v_2$.
By Lemma B.38, *hastype*(σ_2, v_2, S_2).
Since $a \sqsubseteq e_{22}$, $e_{22} = a$.
Therefore, $\langle v_2 \Downarrow \langle S_2; a; r\rangle, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle v_2, \sigma_2, \mathcal{B}_2'\rangle$ for some $\mathcal{B}_2'$.

Case PCAST

$$\frac{e_1 \sqsubseteq e_2 \qquad T_{11} \sqsubseteq T_{21} \qquad T_{12} \sqsubseteq T_{22}}{e_1 :: T_{11} \Rightarrow^{\ell} T_{12} \sqsubseteq e_2 :: T_{21} \Rightarrow^{\ell} T_{22}}$$

Since $\langle e_1 :: T_{11} \Rightarrow^{\ell} T_{12}, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have that $e_1 = v_1$, *hastype*$(\sigma_1, v_1, \lfloor T_{12}\rfloor)$, $e_1' = v_1$, and $\sigma_1' = \sigma_1$.
By Lemma B.35 $e_2 = v_2$.
By Lemma B.33 $\lfloor T_{12}\rfloor \sqsubseteq \lfloor T_{22}\rfloor$.
By Lemma B.38, *hastype*$(\sigma_2, v_2, \lfloor T_{22}\rfloor)$.
Therefore, $\langle v_2 :: T_{21} \Rightarrow^{\ell} T_{22}, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle v_2, \sigma_2, \mathcal{B}_2'\rangle$ for some $\mathcal{B}_2'$.

Case PADD

$$\frac{e_{11} \sqsubseteq e_{21} \qquad e_{12} \sqsubseteq e_{22}}{e_{11}\ +\ e_{12} \sqsubseteq e_{21}\ +\ e_{22}}$$

Since $\langle e_{11}\ +\ e_{12}, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, have that $e_{11} = n_1$, $e_{12} = n_2$, $e_1' = n'$ where $n' = n_1 + n_2$, and $\sigma_1' = \sigma_1$.
Since $n_1 \sqsubseteq e_{21}$, $e_{21} = n_1$.
Since $n_2 \sqsubseteq e_{22}$, $e_{22} = n_2$.
Therefore, $\langle e_{21}\ +\ e_{22}, \sigma_2, \mathcal{B}_2\rangle \longrightarrow \langle n', \sigma_2, \mathcal{B}_2\rangle$.

□

Lemma B.40. *Suppose* $e_1 \sqsubseteq e_2$ *and* $\sigma_1 \sqsubseteq \sigma_2$. *For any* n, *if* $\langle e_1, \sigma_1, \mathcal{B}_1\rangle \longrightarrow^n \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$, *then* $\langle e_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow^n \langle e_2', \sigma_2', \mathcal{B}_2'\rangle$ *and* $e_1' \sqsubseteq e_2'$ *and* $\sigma_1' \sqsubseteq \sigma_2'$.

Proof. By induction on n.

Case $n = 0$.

Then $e_1' = e_1$ and $\sigma_1' = \sigma_1$. Have that $\langle e_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow^0 \langle e_2, \sigma_2, \mathcal{B}_2\rangle$, so $e_2' = e_2$ and $\sigma_2' = \sigma_2$. Proof completed by assumptions.

Case $n = n' + 1$.

For some $e_1'', \sigma_1'', \mathcal{B}_1''$, $\langle e_1, \sigma_1, \mathcal{B}_1\rangle \longrightarrow^{n'} \langle e_1'', \sigma_1'', \mathcal{B}_1''\rangle$ and $\langle e_1'', \sigma_1'', \mathcal{B}_1''\rangle \longrightarrow \langle e_1', \sigma_1', \mathcal{B}_1'\rangle$. By the IH, $\langle e_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow^{n'} \langle e_2'', \sigma_2'', \mathcal{B}_2''\rangle$ and $e_1'' \sqsubseteq e_2''$ and $\sigma_1'' \sqsubseteq \sigma_2''$. Then by Lemma B.39, $\langle e_2'', \sigma_2'', \mathcal{B}_2''\rangle \longrightarrow \langle e_2', \sigma_2', \mathcal{B}_2'\rangle$ and $e_1' \sqsubseteq e_2'$ and $\sigma_1' \sqsubseteq \sigma_2'$. Finally, have that $\langle e_2, \sigma_2, \mathcal{B}_2\rangle \longrightarrow^n \langle e_2', \sigma_2', \mathcal{B}_2'\rangle$.

□

Definition B.41 (Divergence)**.** *A $\lambda^{\star}_{\rightarrow}$ term e* diverges*, written $e \Uparrow$, if for all $e', \sigma, \mathcal{B}$ such that $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \langle e', \sigma, \mathcal{B}\rangle$, there exists some $e'', \sigma', \mathcal{B}'$ such that $\langle e', \sigma, \mathcal{B}\rangle \longrightarrow \langle e'', \sigma', \mathcal{B}'\rangle$.*

Lemma B.42 (The gradual guarantee)**.** *If $e_s \sqsubseteq e'_s$ and $\emptyset \vdash e_s \rightsquigarrow e : T$, then*

1. *$\emptyset \vdash e'_s \rightsquigarrow e' : T'$, with $T \sqsubseteq T'$, and*
2. *if $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \langle v, \sigma, \mathcal{B}\rangle$, then $\langle e', \emptyset, \emptyset\rangle \longrightarrow^* \langle v', \sigma', \mathcal{B}'\rangle$ with $v \sqsubseteq v'$ and $\sigma \sqsubseteq \sigma'$, and*
3. *if $e \Uparrow$, then $e' \Uparrow$, and*
4. *if $\langle e', \emptyset, \emptyset\rangle \longrightarrow^* \langle v', \sigma', \mathcal{B}'\rangle$, then either $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \langle v, \sigma, \mathcal{B}\rangle$ with $v \sqsubseteq v'$ and $\sigma \sqsubseteq \sigma'$, or $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \textsc{Blame}(\mathcal{L})$, and*
5. *if $e' \Uparrow$, then either $e \Uparrow$ or $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \textsc{Blame}(\mathcal{L})$.*

Proof. We prove part 1 by applying Lemma B.32. From Lemma B.34 we have that $e \sqsubseteq e'$.

Suppose that $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \langle v, \sigma, \mathcal{B}\rangle$. Then by Lemma B.40, $\langle e', \emptyset, \emptyset\rangle \longrightarrow^* \langle v', \sigma', \mathcal{B}'\rangle$ with $v \sqsubseteq v'$ and $\sigma \sqsubseteq \sigma'$, proving part 2.

Now suppose that for all e_1 such that $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \langle e_1, \sigma_1, \mathcal{B}_1\rangle$, there exists some e_2 such that $\langle e_1, \sigma_1, \mathcal{B}_1\rangle \longrightarrow \langle e_2, \sigma_2, \mathcal{B}_2\rangle$. By Lemma B.40, $\langle e', \emptyset, \emptyset\rangle \longrightarrow^* \langle e'_1, \sigma'_1, \mathcal{B}'_1\rangle$ with $e_1 \sqsubseteq e'_1$ and $\sigma_1 \sqsubseteq \sigma'_2$. Then by Lemma B.39, there exists some e'_2 such that $\langle e'_1, \sigma'_1, \mathcal{B}'_1\rangle \longrightarrow \langle e'_2, \sigma'_2, \mathcal{B}'_2\rangle$. Therefore $\langle e', \emptyset, \emptyset\rangle \Uparrow$, proving part 3.

Suppose that $\langle e', \emptyset, \emptyset\rangle \longrightarrow^n \langle v', \sigma, \mathcal{B}\rangle$ for some n. By Lemma B.13, either

1. $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \langle v, \sigma, \mathcal{B}\rangle$ or
2. $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \textsc{Blame}(\mathcal{L})$ or
3. $\langle e, \emptyset, \emptyset\rangle \longrightarrow^* \langle e, \sigma, \mathcal{B}\rangle$ and $\langle e, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$ or
4. $\langle e, \emptyset, \emptyset\rangle \Uparrow$.

Case 2 satisfies the theorem. Case 3 is impossible because e does not contain any $\blacklozenge$-marked terms. Case 4 is impossible because $\langle e, \emptyset, \emptyset\rangle \longrightarrow^n \langle e_n, \sigma_n, \mathcal{B}_n\rangle$ for some e_n, and by Lemma B.40, $e_n \sqsubseteq v'$. By Lemma B.36, e_n is a value, and therefore $\langle e_n, \sigma_n, \mathcal{B}_n\rangle \not\longrightarrow \langle e'_n, \sigma'_n, \mathcal{B}'_n\rangle$. Finally, have that $\langle e, \emptyset, \emptyset\rangle \longrightarrow^n \langle v, \sigma, \mathcal{B}\rangle$, because if this evaluation took m steps with $m < n$, then e_m would not be a value and $e_m \sqsubseteq v'$, which is ruled out by Lemma B.36, and if $m > n$, then e_n would not be a value and $e_n \sqsubseteq v'$, also ruled out by Lemma B.36. This proves part 4.

Finally, suppose that $\langle e', \emptyset, \emptyset\rangle \Uparrow$. For some n, by Lemma B.13, either

1. $\langle e, \emptyset, \emptyset\rangle \longrightarrow^n \langle v, \sigma, \mathcal{B}\rangle$ or
2. $\langle e, \emptyset, \emptyset\rangle \longrightarrow^n \textsc{Blame}(\mathcal{L})$ or
3. $\langle e, \emptyset, \emptyset\rangle \longrightarrow^n \langle e, \sigma, \mathcal{B}\rangle$ and $\langle e, \sigma, \mathcal{B}\rangle$ stuck $\blacklozenge$ or
4. $\langle e, \emptyset, \emptyset\rangle \Uparrow$.

Case 2 satisfies the theorem. Case 3 is impossible because e does not contain any $\blacklozenge$-marked terms. Case 1 is impossible because $\langle e', \emptyset, \emptyset\rangle \longrightarrow^n \langle e'_n, \sigma'_n, \mathcal{B}'_n\rangle$ for some e'_n which is not a value, and by Lemma B.40, $v \sqsubseteq e'_n$. By Lemma B.35, e'_n is a value, resulting in a contradiction. Case 4 satisfies the theorem. This proves part 5. □