Signature Restriction for Polymorphic Algebraic Effects (Supplementary Material)

Taro Sekiyama

National Institute of Informatics & SOKENDAI

This is the supplementary material for "Signature Restriction for Polymorphic Algebraic Effects" accepted at ICFP 2020, providing the full definitions of the language, the polymorphic type system, and the type-and-effect system and the full proofs of the properties presented in the paper.

1 Definition

1.1 Syntax

$$
\begin{array}{llll}
\textbf{Variables}\quad x, y, z, f, k & \textbf{Type variables}\quad \alpha, \beta, \gamma & \textbf{Effect operations}\quad \mathsf{op} & \\
\textbf{Base types}\quad \iota & ::= & \mathsf{bool} \mid \mathsf{int} \mid \ldots \\
\textbf{Types}\quad A, B, C, D & ::= & \alpha \mid \iota \mid A \rightarrow B \mid \forall\, \alpha.\, A \mid A \times B \mid A + B \mid A\ \mathsf{list} \\
\textbf{Constants}\quad c & ::= & \mathsf{true} \mid \mathsf{false} \mid 0 \mid + \mid \ldots \\
\textbf{Terms}\quad M & ::= & x \mid c \mid \lambda x.M \mid M_1\, M_2 \mid \#\mathsf{op}(M) \mid \mathsf{handle}\, M\, \mathsf{with}\, H \mid \\
 & & (M_1, M_2) \mid \pi_1 M \mid \pi_2 M \mid \\
 & & \mathsf{inl}\, M \mid \mathsf{inr}\, M \mid \mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \rightarrow M_1;\ \mathsf{inr}\, y \rightarrow M_2 \mid \\
 & & \mathsf{nil} \mid \mathsf{cons}\, M \mid \mathsf{case}\, M\, \mathsf{of}\, \mathsf{nil} \rightarrow M_1;\ \mathsf{cons}\, x \rightarrow M_2 \mid \mathsf{fix}\, f.\lambda x.M \\
\textbf{Handlers}\quad H & ::= & \mathsf{return}\, x \rightarrow M \mid H; \mathsf{op}(x, k) \rightarrow M \\
\textbf{Values}\quad v & ::= & c \mid \lambda x.M \mid (v_1, v_2) \mid \mathsf{inl}\, v \mid \mathsf{inr}\, v \mid \mathsf{nil} \mid \mathsf{cons}\, v \\
\textbf{Typing contexts}\quad \Gamma & ::= & \emptyset \mid \Gamma, x : A \mid \Gamma, \alpha \\
\textbf{Evaluation contexts}\quad E & ::= & [] \mid E\, M_2 \mid v_1\, E \mid \#\mathsf{op}(E) \mid \mathsf{handle}\, E\, \mathsf{with}\, H \mid \\
 & & (E, M_2) \mid (v_1, E) \mid \pi_1 E \mid \pi_2 E \mid \\
 & & \mathsf{inl}\, E \mid \mathsf{inr}\, E \mid \mathsf{case}\, E\, \mathsf{of}\, \mathsf{inl}\, x \rightarrow M_1;\ \mathsf{inr}\, y \rightarrow M_2 \mid \\
 & & \mathsf{cons}\, E \mid \mathsf{case}\, E\, \mathsf{of}\, \mathsf{nil} \rightarrow M_1;\ \mathsf{cons}\, x \rightarrow M_2
\end{array}
$$

Convention 1. *This work follows the conventions as below.*

- *We write* $\boldsymbol{\alpha}^I$ *for* $\boldsymbol{\alpha} = \alpha_1, \cdots, \alpha_n$ *with* $I = \{1, ..., n\}$. *We often omit index sets (I and J) if they are not important: for example, we often abbreviate* $\boldsymbol{\alpha}^I$ *to* $\boldsymbol{\alpha}$. *We apply this bold-font notation to other syntax categories as well; for example,* $\boldsymbol{A}^I$ *denotes a sequence of types.*
- *We write* $\{s\}$ *to view the sequence* s *as a set by ignoring the order.*
- *We write* $\forall\, \boldsymbol{\alpha}^I.\, A$ *for* $\forall \alpha_1. \ldots \forall \alpha_n.\, A$ *with* $I = \{1, ..., n\}$. *We may omit index sets* ($\forall\, \boldsymbol{\alpha}.\, A$). *We write* $\forall\, \boldsymbol{\alpha}^I.\, \boldsymbol{A}^J$ *for a sequence of types* $\forall\, \boldsymbol{\alpha}^I.\, A_1,\ \ldots,\ \forall\, \boldsymbol{\alpha}^I.\, A_n$ *with* $J = \{1, \ldots, n\}$.
- *We write* Γ_1, Γ_2 *for the concatenation of* Γ_1 *and* Γ_2*, and* $x : A$ *and* $\boldsymbol{\alpha}$ *for* $(\emptyset, x : A)$, $(\emptyset, \boldsymbol{\alpha})$*, respectively.*
- *We write* H^{return} *for the return clause in* H *and* $H(\mathsf{op})$ *for the operation clause of* op *in* H.

Definition 1 (Domain of typing contexts)**.** *We define* $dom(\Gamma)$ *as follows.*

$$
\begin{array}{lcl}
dom(\emptyset) & \stackrel{\text{def}}{=} & \emptyset \\
dom(\Gamma, x : A) & \stackrel{\text{def}}{=} & dom(\Gamma) \cup \{x\} \\
dom(\Gamma, \alpha) & \stackrel{\text{def}}{=} & dom(\Gamma) \cup \{\alpha\}
\end{array}
$$

Definition 2 (Free type variables and type substitution in types)**.** *Free type variables $ftv(A)$ in a type A and type substitution $B[\boldsymbol{A}/\boldsymbol{\alpha}]$ of types $\boldsymbol{A}$ for type variables $\boldsymbol{\alpha}$ in B are defined as usual. Type A is closed if and only if $ftv(A)$ is empty.*

Assumption 1. *We suppose that each constant c is assigned a first-order closed type $ty(c)$ of the form $\iota \rightarrow \ldots \rightarrow \iota_n \rightarrow \iota_{n+1}$. We also suppose that, for any ι, there exists the set $\mathbb{K}_\iota$ of constants of ι. For any constant c, $ty(c) = \iota$ if and only if $c \in \mathbb{K}_\iota$. The function ζ gives a denotation to pairs of constants. In particular, for any constants c_1 and c_2: (1) $\zeta(c_1, c_2)$ is defined if and only if $ty(c_1) = \iota_0 \rightarrow A$ and $ty(c_2) = \iota_0$ for some ι_0 and A; and (2) if $\zeta(c_1, c_2)$ is defined, $\zeta(c_1, c_2)$ is a constant and $ty(\zeta(c_1, c_2)) = A$ where $ty(c_1) = \iota_0 \rightarrow A$.*

Definition 3 (Polarity of type variable occurrence)**.** *The positive and negative occurrences of a type variable in a type A are defined by induction on A, as follows.*

- *The occurrence of α in type α is positive.*
- *The positive (resp. negative) occurrences of α in $A \rightarrow B$ are the negative (resp. positive) occurrences of α in A and the positive (resp. negative) occurrences of α in B.*
- *The positive (resp. negative) occurrences of α in $\forall \beta. A$, where β is supposed to be distinct from α, are the positive (resp. negative) occurrences of α in A.*
- *The positive (resp. negative) occurrences of α in $A \times B$ are the positive (resp. negative) occurrences of α in A and those in B.*
- *The positive (resp. negative) occurrences of α in $A + B$ are the positive (resp. negative) occurrences of α in A and those in B.*
- *The positive (resp. negative) occurrences of α in $A\,\mathsf{list}$ are the positive (resp. negative) occurrences of α in A.*

The strictly positive occurrences of a type variable in a type A are defined by induction on A, as follows.

- *The occurrence of α in type α is strictly positive.*
- *The strictly positive occurrences of α in $A \rightarrow B$ are the strictly positive occurrences of α in B.*
- *The strictly positive occurrences of α in $\forall \beta. A$, where β is supposed to be distinct from α, are the strictly positive occurrences of α in A.*
- *The strictly positive occurrences of α in $A \times B$ are the strictly positive occurrences of α in A and those in B.*
- *The strictly positive occurrences of α in $A + B$ are the strictly positive occurrences of α in A and those in B.*
- *The strictly positive occurrences of α in $A\,\mathsf{list}$ are the strictly positive occurrences of α in A.*

Definition 4 (Type signature)**.** *Each effect operation op is assigned a type signature $ty(\mathsf{op})$ of the form $\forall \alpha_1. \ldots \forall \alpha_n. A \hookrightarrow B$ for some n, where $\alpha_1, \ldots, \alpha_n$ are bound in the domain type A and codomain type B. It may be abbreviated to $\forall \boldsymbol{\alpha}^I. A \hookrightarrow B$ or, more simply, to $\forall \boldsymbol{\alpha}. A \hookrightarrow B$. We suppose that $\forall \alpha_1. \ldots \forall \alpha_n. A \hookrightarrow B$ is closed, i.e., $ftv(A), ftv(B) \subseteq \{\alpha_1, \cdots, \alpha_n\}$.*

Definition 5 (Operations satisfying signature restriction)**.** *An operation op having type signature $ty(\mathsf{op}) = \forall \boldsymbol{\alpha}. A \hookrightarrow B$ satisfies the signature restriction if and only if:*

- *the occurrences of each type variable of $\boldsymbol{\alpha}$ in A are only negative or strictly positive; and*
- *the occurrences of each type variable of $\boldsymbol{\alpha}$ in B are only positive.*

1.2 Semantics

Definition 6 (op-free evaluation contexts)**.** *Evaluation context E is op-free, written $\mathsf{op} \notin E$, if and only if, there exist no E_1, E_2, and H such that $E = E_1[\mathsf{handle}\, E_2 \,\mathsf{with}\, H]$ and H has an operation clause for op.*

Definition 7. *Relations $\longrightarrow$ and $\rightsquigarrow$ are the smallest relations satisfying the rules in Figure 1.*

Definition 8 (Multi-step evaluation)**.** *Binary relation $\longrightarrow^*$ over terms is the reflexive and transitive closure of $\longrightarrow$.*

Definition 9 (Nonreducible terms)**.** *We write $M \not\longrightarrow$ if there exists no term M' such that $M \longrightarrow M'$.*

Reduction rules $\boxed{M_1 \rightsquigarrow M_2}$

$$
\begin{array}{rcll}
c\ v & \rightsquigarrow & \zeta(c, v) & \text{R\_Const} \\
(\lambda x.M)\ v & \rightsquigarrow & M[v/x] & \text{R\_Beta} \\
\mathsf{handle}\ v\ \mathsf{with}\ H & \rightsquigarrow & M[v/x] & \text{R\_Return} \\
 & & (\text{where } H^{\mathsf{return}} = \mathsf{return}\ x \rightarrow M) & \\
\mathsf{handle}\ E[\#\mathsf{op}(v)]\ \mathsf{with}\ H & \rightsquigarrow & M[v/x][\lambda y.\mathsf{handle}\ E[y]\ \mathsf{with}\ H/k] & \text{R\_Handle} \\
 & & (\text{where } \mathsf{op} \notin E \text{ and } H(\mathsf{op}) = \mathsf{op}(x,k) \rightarrow M) & \\
\pi_1(v_1, v_2) & \rightsquigarrow & v_1 & \text{R\_Proj1} \\
\pi_2(v_1, v_2) & \rightsquigarrow & v_2 & \text{R\_Proj2} \\
\mathsf{case}\ \mathsf{inl}\ v\ \mathsf{of}\ \mathsf{inl}\ x \rightarrow M_1;\ \mathsf{inr}\ y \rightarrow M_2 & \rightsquigarrow & M_1[v/x] & \text{R\_CaseL} \\
\mathsf{case}\ \mathsf{inr}\ v\ \mathsf{of}\ \mathsf{inl}\ x \rightarrow M_1;\ \mathsf{inr}\ y \rightarrow M_2 & \rightsquigarrow & M_2[v/y] & \text{R\_CaseR} \\
\mathsf{case}\ \mathsf{nil}\ \mathsf{of}\ \mathsf{nil} \rightarrow M_1;\ \mathsf{cons}\ x \rightarrow M_2 & \rightsquigarrow & M_1 & \text{R\_Nil} \\
\mathsf{case}\ \mathsf{cons}\ v\ \mathsf{of}\ \mathsf{nil} \rightarrow M_1;\ \mathsf{cons}\ x \rightarrow M_2 & \rightsquigarrow & M_2[v/x] & \text{R\_Cons} \\
\mathsf{fix}\ f.\lambda x.M & \rightsquigarrow & (\lambda x.M)[\mathsf{fix}\ f.\lambda x.M/f] & \text{R\_Fix}
\end{array}
$$

Evaluation rules $\boxed{M_1 \longrightarrow M_2}$

$$
\frac{M_1 \rightsquigarrow M_2}{E[M_1] \longrightarrow E[M_2]}\ \text{E\_Eval}
$$

Figure 1: Semantics.

1.3 Typing

Definition 10. *Well-formedness judgment* $\vdash \Gamma$ *is the smallest relations satisfying the rules in Figure 3. We write* $\Gamma \vdash A$ *if and only if* $ftv(A) \subseteq dom(\Gamma)$ *and* $\vdash \Gamma$ *is derived. Type containment judgment* $\Gamma \vdash A \sqsubseteq B$ *is the least relation satisfying the rules in Figure 2. Typing judgments* $\Gamma \vdash M : A$ *and* $\Gamma \vdash H : A \Rightarrow B$ *are the smallest relations satisfying the rules in Figure 4.*

Type containment $\boxed{\Gamma \vdash A \sqsubseteq B}$

$$\frac{\vdash \Gamma}{\Gamma \vdash A \sqsubseteq A}\ \textsc{C\_Refl} \qquad \frac{\Gamma \vdash A \sqsubseteq C \quad \Gamma \vdash C \sqsubseteq B}{\Gamma \vdash A \sqsubseteq B}\ \textsc{C\_Trans} \qquad \frac{\Gamma \vdash B_1 \sqsubseteq A_1 \quad \Gamma \vdash A_2 \sqsubseteq B_2}{\Gamma \vdash A_1 \to A_2 \sqsubseteq B_1 \to B_2}\ \textsc{C\_Fun}$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash \forall \alpha.\, A \sqsubseteq A[B/\alpha]}\ \textsc{C\_Inst} \qquad \frac{\vdash \Gamma \quad \alpha \notin \mathit{ftv}(A)}{\Gamma \vdash A \sqsubseteq \forall \alpha.\, A}\ \textsc{C\_Gen} \qquad \frac{\Gamma, \alpha \vdash A \sqsubseteq B}{\Gamma \vdash \forall \alpha.\, A \sqsubseteq \forall \alpha.\, B}\ \textsc{C\_Poly}$$

$$\frac{\Gamma \vdash A_1 \sqsubseteq B_1 \quad \Gamma \vdash A_2 \sqsubseteq B_2}{\Gamma \vdash A_1 \times A_2 \sqsubseteq B_1 \times B_2}\ \textsc{C\_Prod} \qquad \frac{\Gamma \vdash A_1 \sqsubseteq B_1 \quad \Gamma \vdash A_2 \sqsubseteq B_2}{\Gamma \vdash A_1 + A_2 \sqsubseteq B_1 + B_2}\ \textsc{C\_Sum} \qquad \frac{\Gamma \vdash A \sqsubseteq B}{\Gamma \vdash A\,\mathsf{list} \sqsubseteq B\,\mathsf{list}}\ \textsc{C\_List}$$

$$\frac{\vdash \Gamma \quad \alpha \notin \mathit{ftv}(A)}{\Gamma \vdash \forall \alpha.\, A \to B \sqsubseteq A \to \forall \alpha.\, B}\ \textsc{C\_DFun} \qquad \frac{\vdash \Gamma}{\Gamma \vdash \forall \alpha.\, A \times B \sqsubseteq (\forall \alpha.\, A) \times (\forall \alpha.\, B)}\ \textsc{C\_DProd}$$

$$\frac{\vdash \Gamma}{\Gamma \vdash \forall \alpha.\, A + B \sqsubseteq (\forall \alpha.\, A) + (\forall \alpha.\, B)}\ \textsc{C\_DSum} \qquad \frac{\vdash \Gamma}{\Gamma \vdash \forall \alpha.\, A\,\mathsf{list} \sqsubseteq (\forall \alpha.\, A)\,\mathsf{list}}\ \textsc{C\_DList}$$

Figure 2: Type containment.

Well-formedness $\boxed{\vdash \Gamma}$

$$\frac{}{\vdash \emptyset}\ \textsc{WF\_Empty} \qquad \frac{x \notin \mathit{dom}(\Gamma) \quad \Gamma \vdash A}{\vdash \Gamma, x : A}\ \textsc{WF\_ExtVar} \qquad \frac{\alpha \notin \mathit{dom}(\Gamma) \quad \vdash \Gamma}{\vdash \Gamma, \alpha}\ \textsc{WF\_ExtTyVar}$$

Figure 3: Well-formedness.

Term typing $\boxed{\Gamma \vdash M : A}$

$$\frac{\vdash \Gamma \quad x : A \in \Gamma}{\Gamma \vdash x : A}\ \textsc{T\_Var} \qquad \frac{\vdash \Gamma}{\Gamma \vdash c : ty(c)}\ \textsc{T\_Const} \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \to B}\ \textsc{T\_Abs}$$

$$\frac{\Gamma \vdash M_1 : A \to B \quad \Gamma \vdash M_2 : A}{\Gamma \vdash M_1\, M_2 : B}\ \textsc{T\_App} \quad \frac{\Gamma, \alpha \vdash M : A}{\Gamma \vdash M : \forall\, \alpha.\, A}\ \textsc{T\_Gen} \quad \frac{\Gamma \vdash M : A \quad \Gamma \vdash A \sqsubseteq B \quad \Gamma \vdash B}{\Gamma \vdash M : B}\ \textsc{T\_Inst}$$

$$\frac{ty\,(\mathsf{op}) \ =\ \forall\, \boldsymbol{\alpha}.\, A \hookrightarrow B \quad \Gamma \vdash M : A[\boldsymbol{C}/\boldsymbol{\alpha}] \quad \Gamma \vdash \boldsymbol{C}}{\Gamma \vdash \#\mathsf{op}(M) : B[\boldsymbol{C}/\boldsymbol{\alpha}]}\ \textsc{T\_Op} \qquad \frac{\Gamma \vdash M : A \quad \Gamma \vdash H : A \Rightarrow B}{\Gamma \vdash \mathsf{handle}\ M\ \mathsf{with}\ H : B}\ \textsc{T\_Handle}$$

$$\frac{\Gamma \vdash M_1 : A \quad \Gamma \vdash M_2 : B}{\Gamma \vdash (M_1, M_2) : A \times B}\ \textsc{T\_Pair} \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_1 M : A}\ \textsc{T\_Proj1} \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_2 M : B}\ \textsc{T\_Proj2}$$

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash B}{\Gamma \vdash \mathsf{inl}\ M : A + B}\ \textsc{T\_InL} \qquad \frac{\Gamma \vdash M : B \quad \Gamma \vdash A}{\Gamma \vdash \mathsf{inr}\ M : A + B}\ \textsc{T\_InR}$$

$$\frac{\Gamma \vdash M : A + B \quad \Gamma, x : A \vdash M_1 : C \quad \Gamma, y : B \vdash M_2 : C}{\Gamma \vdash \mathsf{case}\ M\ \mathsf{of}\ \mathsf{inl}\ x \to M_1;\ \mathsf{inr}\ y \to M_2 : C}\ \textsc{T\_Case}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \mathsf{nil} : A\ \mathsf{list}}\ \textsc{T\_Nil} \qquad \frac{\Gamma \vdash M : A \times A\ \mathsf{list}}{\Gamma \vdash \mathsf{cons}\ M : A\ \mathsf{list}}\ \textsc{T\_Cons}$$

$$\frac{\Gamma \vdash M : A\ \mathsf{list} \quad \Gamma \vdash M_1 : B \quad \Gamma, x : A \times A\ \mathsf{list} \vdash M_2 : B}{\Gamma \vdash \mathsf{case}\ M\ \mathsf{of}\ \mathsf{nil}\ \to M_1;\ \mathsf{cons}\ x \to M_2 : B}\ \textsc{T\_CaseList} \qquad \frac{\Gamma, f : A \to B, x : A \vdash M : B}{\Gamma \vdash \mathsf{fix}\, f.\lambda x.M : A \to B}\ \textsc{T\_Fix}$$

Handler typing $\boxed{\Gamma \vdash H : A \Rightarrow B}$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \mathsf{return}\ x \to M : A \Rightarrow B}\ \textsc{TH\_Return}$$

$$\frac{\Gamma \vdash H : A \Rightarrow B \quad ty\,(\mathsf{op}) \ =\ \forall\, \boldsymbol{\alpha}.\, C \hookrightarrow D \quad \Gamma, \boldsymbol{\alpha}, x : C, k : D \to B \vdash M : B}{\Gamma \vdash H; \mathsf{op}(x, k) \to M : A \Rightarrow B}\ \textsc{TH\_Op}$$

Figure 4: Typing.

$$\begin{array}{llll}\textbf{Effects} & \epsilon & ::= & \{\mathsf{op}_1, \cdots, \mathsf{op}_n\} \\ \textbf{Types} & A, B, C, D & ::= & \alpha \mid \iota \mid A \rightarrow^{\epsilon} B \mid \forall\, \alpha.\, A \mid A \times B \mid A + B \mid A\ \mathsf{list}\end{array}$$

Figure 5: Type language for the effect-and-type system.

Type containment $\boxed{\Gamma \vdash A \sqsubseteq B}$

$$\frac{\Gamma \vdash B_1 \sqsubseteq A_1 \quad \Gamma \vdash A_2 \sqsubseteq B_2}{\Gamma \vdash A_1 \rightarrow^{\epsilon} A_2 \sqsubseteq B_1 \rightarrow^{\epsilon} B_2}\ \text{C\_FunEff} \qquad \frac{\vdash \Gamma \quad \alpha \notin \mathit{ftv}(A) \quad \mathit{SR}\,(\epsilon)}{\Gamma \vdash \forall\, \alpha.\, A \rightarrow^{\epsilon} B \sqsubseteq A \rightarrow^{\epsilon} \forall\, \alpha.\, B}\ \text{C\_DFunEff}$$

Figure 6: Change from Figure 2 for type containment of the effect-and-type system. It gets rid of (C_Fun) and (C_DFun) instead of adding (C_FunEff) and (C_DFunEff).

1.4 Type-and-effect System

The type language for the type-and-effect system is shown Figure 5. Figure 6 describes only the change of the type containment rules from those of the polymorphic type system.

Definition 11 (Effects satisfying signature restriction)**.** *The predicate $\mathit{SR}\,(\epsilon)$ holds if and only if, for any $\mathsf{op} \in \epsilon$ such that $\mathit{ty}\,(\mathsf{op}) = \forall\, \boldsymbol{\alpha}.\, A \hookrightarrow B$:*

- *the occurrences of each type variable of $\boldsymbol{\alpha}$ in A are only negative or strictly positive;*
- *the occurrences of each type variable of $\boldsymbol{\alpha}$ in B are only positive; and*
- *for any function type $C \rightarrow^{\epsilon'} D$ occurring at a strictly positive position in A, if $\{\boldsymbol{\alpha}\} \cap \mathit{ftv}(D) \neq \emptyset$, then $\mathit{SR}\,(\epsilon')$.*

Definition 12. *Typing judgments $\Gamma \vdash M : A \,|\, \epsilon$ and $\Gamma \vdash H : A \,|\, \epsilon \Rightarrow B \,|\, \epsilon'$ are the smallest relations satisfying the rules in Figure 7.*

Term typing $\boxed{\Gamma \vdash M : A \mid \epsilon}$

$$\frac{\vdash \Gamma \quad x : A \in \Gamma}{\Gamma \vdash x : A \mid \epsilon}\ \textsc{Te\_Var} \qquad \frac{\vdash \Gamma}{\Gamma \vdash c : ty(c) \mid \epsilon}\ \textsc{Te\_Const}$$

$$\frac{\Gamma, x : A \vdash M : B \mid \epsilon'}{\Gamma \vdash \lambda x.M : A \rightarrow^{\epsilon'} B \mid \epsilon}\ \textsc{Te\_Abs} \qquad \frac{\Gamma \vdash M_1 : A \rightarrow^{\epsilon'} B \mid \epsilon \quad \Gamma \vdash M_2 : A \mid \epsilon \quad \epsilon' \subseteq \epsilon}{\Gamma \vdash M_1\, M_2 : B \mid \epsilon}\ \textsc{Te\_App}$$

$$\frac{\Gamma, \alpha \vdash M : A \mid \epsilon \quad SR\,(\epsilon)}{\Gamma \vdash M : \forall\, \alpha.\, A \mid \epsilon}\ \textsc{Te\_Gen} \qquad \frac{\Gamma \vdash M : A \mid \epsilon \quad \Gamma \vdash A \sqsubseteq B \quad \Gamma \vdash B}{\Gamma \vdash M : B \mid \epsilon}\ \textsc{Te\_Inst}$$

$$\frac{ty\,(\mathsf{op}) \ = \ \forall\, \boldsymbol{\alpha}.\, A \hookrightarrow B \quad \mathsf{op} \in \epsilon \quad \Gamma \vdash M : A[\boldsymbol{C}/\boldsymbol{\alpha}] \mid \epsilon \quad \Gamma \vdash \boldsymbol{C}}{\Gamma \vdash \#\mathsf{op}(M) : B[\boldsymbol{C}/\boldsymbol{\alpha}] \mid \epsilon}\ \textsc{Te\_Op}$$

$$\frac{\Gamma \vdash M : A \mid \epsilon \quad \Gamma \vdash H : A \mid \epsilon \Rightarrow B \mid \epsilon'}{\Gamma \vdash \mathsf{handle}\, M\, \mathsf{with}\, H : B \mid \epsilon'}\ \textsc{Te\_Handle}$$

$$\frac{\Gamma \vdash M_1 : A \mid \epsilon \quad \Gamma \vdash M_2 : B \mid \epsilon}{\Gamma \vdash (M_1, M_2) : A \times B \mid \epsilon}\ \textsc{Te\_Pair} \qquad \frac{\Gamma \vdash M : A \times B \mid \epsilon}{\Gamma \vdash \pi_1 M : A \mid \epsilon}\ \textsc{Te\_Proj1} \qquad \frac{\Gamma \vdash M : A \times B \mid \epsilon}{\Gamma \vdash \pi_2 M : B \mid \epsilon}\ \textsc{Te\_Proj2}$$

$$\frac{\Gamma \vdash M : A \mid \epsilon \quad \Gamma \vdash B}{\Gamma \vdash \mathsf{inl}\, M : A + B \mid \epsilon}\ \textsc{Te\_InL} \qquad \frac{\Gamma \vdash M : B \mid \epsilon \quad \Gamma \vdash A}{\Gamma \vdash \mathsf{inr}\, M : A + B \mid \epsilon}\ \textsc{Te\_InR}$$

$$\frac{\Gamma \vdash M : A + B \mid \epsilon \quad \Gamma, x : A \vdash M_1 : C \mid \epsilon \quad \Gamma, y : B \vdash M_2 : C \mid \epsilon}{\Gamma \vdash \mathsf{case}\, M\, \mathsf{of}\, \mathsf{inl}\, x \rightarrow M_1;\, \mathsf{inr}\, y \rightarrow M_2 : C \mid \epsilon}\ \textsc{Te\_Case}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \mathsf{nil} : A\, \mathsf{list} \mid \epsilon}\ \textsc{Te\_Nil} \qquad \frac{\Gamma \vdash M : A \times A\, \mathsf{list} \mid \epsilon}{\Gamma \vdash \mathsf{cons}\, M : A\, \mathsf{list} \mid \epsilon}\ \textsc{Te\_Cons}$$

$$\frac{\Gamma \vdash M : A\, \mathsf{list} \mid \epsilon \quad \Gamma \vdash M_1 : B \mid \epsilon \quad \Gamma, x : A \times A\, \mathsf{list} \vdash M_2 : B \mid \epsilon}{\Gamma \vdash \mathsf{case}\, M\, \mathsf{of}\, \mathsf{nil} \rightarrow M_1;\, \mathsf{cons}\, x \rightarrow M_2 : B \mid \epsilon}\ \textsc{Te\_CaseList}$$

$$\frac{\Gamma, f : A \rightarrow^{\epsilon} B, x : A \vdash M : B \mid \epsilon}{\Gamma \vdash \mathsf{fix}\, f.\lambda x.M : A \rightarrow^{\epsilon} B \mid \epsilon'}\ \textsc{Te\_Fix} \qquad \frac{\Gamma \vdash M : A \mid \epsilon' \quad \epsilon' \subseteq \epsilon}{\Gamma \vdash M : A \mid \epsilon}\ \textsc{Te\_Weak}$$

Handler typing $\boxed{\Gamma \vdash H : A \mid \epsilon \Rightarrow B \mid \epsilon'}$

$$\frac{\Gamma, x : A \vdash M : B \mid \epsilon' \quad \epsilon \subseteq \epsilon'}{\Gamma \vdash \mathsf{return}\, x \rightarrow M : A \mid \epsilon \Rightarrow B \mid \epsilon'}\ \textsc{THe\_Return}$$

$$\frac{\Gamma \vdash H : A \mid \epsilon \Rightarrow B \mid \epsilon' \quad ty\,(\mathsf{op}) \ = \ \forall\, \boldsymbol{\alpha}.\, C \hookrightarrow D \quad \Gamma, \boldsymbol{\alpha}, x : C, k : D \rightarrow^{\epsilon'} B \vdash M : B \mid \epsilon'}{\Gamma \vdash H; \mathsf{op}(x, k) \rightarrow M : A \mid \epsilon \uplus \{\mathsf{op}\} \Rightarrow B \mid \epsilon'}\ \textsc{THe\_Op}$$

Figure 7: Typing of the effect-and-type system.

2 Proofs

2.1 Soundness of the Type System

Lemma 1 (Weakening). *Suppose that* $\vdash \Gamma_1, \Gamma_2$. *Let* Γ_3 *be a typing context such that* $dom(\Gamma_2) \cap dom(\Gamma_3) = \emptyset$.

1. *If* $\vdash \Gamma_1, \Gamma_3$, *then* $\vdash \Gamma_1, \Gamma_2, \Gamma_3$.
2. *If* $\Gamma_1, \Gamma_3 \vdash A$, *then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash A$.
3. *If* $\Gamma_1, \Gamma_3 \vdash A \sqsubseteq B$, *then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash A \sqsubseteq B$.
4. *If* $\Gamma_1, \Gamma_3 \vdash M : A$, *then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash M : A$.
5. *If* $\Gamma_1, \Gamma_3 \vdash H : A \Rightarrow B$, *then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash H : A \Rightarrow B$.

Proof. By (mutual) induction on the derivations of the judgments. □

Lemma 2 (Type substitution). *Suppose that* $\Gamma_1 \vdash A$.

1. *If* $\vdash \Gamma_1, \alpha, \Gamma_2$, *then* $\vdash \Gamma_1, \Gamma_2\,[A/\alpha]$.
2. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash B$, *then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash B[A/\alpha]$.
3. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash B \sqsubseteq C$, *then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash B[A/\alpha] \sqsubseteq C[A/\alpha]$.
4. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash M : B$, *then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash M : B[A/\alpha]$.
5. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash H : B \Rightarrow C$, *then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash H : B[A/\alpha] \Rightarrow C[A/\alpha]$.

Proof. Straightforward by (mutual) induction on the derivations of the judgments. Note that the cases for (T_Op) and (TH_Op) depend on Definition 4, which states that, for any op, if $ty\,(\mathsf{op}) = \forall \boldsymbol{\beta}.\, C \hookrightarrow D$, $ftv(C) \cup ftv(D) \subseteq \{\boldsymbol{\beta}\}$. □

Lemma 3.

1. *If* $\vdash \Gamma_1, x : A, \Gamma_2$, *then* $\vdash \Gamma_1, \Gamma_2$.
2. *If* $\Gamma_1, x : A, \Gamma_2 \vdash B$, *then* $\Gamma_1, \Gamma_2 \vdash B$.
3. *If* $\Gamma_1, x : A, \Gamma_2 \vdash B \sqsubseteq C$, *then* $\Gamma_1, \Gamma_2 \vdash B \sqsubseteq C$.

Proof. By induction on the derivations of the judgments. □

Lemma 4 (Term substitution). *Suppose that* $\Gamma_1 \vdash M : A$.

1. *If* $\Gamma_1, x : A, \Gamma_2 \vdash M' : B$, *then* $\Gamma_1, \Gamma_2 \vdash M'[M/x] : B$.
2. *If* $\Gamma_1, x : A, \Gamma_2 \vdash H : B \Rightarrow C$, *then* $\Gamma_1, \Gamma_2 \vdash H[M/x] : B \Rightarrow C$.

Proof. By mutual induction on the typing derivations with Lemma 3. The case for (T_Var) uses Lemma 1 (4). □

Definition 13. *The function unqualify returns the type obtained by removing all the* $\forall$*s at the top-level from a given type, defined as follows.*

$$\begin{array}{lcl} unqualify(\forall \alpha.\, A) & \stackrel{\text{def}}{=} & unqualify(A) \\ unqualify(A) & \stackrel{\text{def}}{=} & A \quad (\text{if } A \neq \forall \alpha.\, B \text{ for any } \alpha \text{ and } B) \end{array}$$

Lemma 5. *Suppose* $\Gamma \vdash A \sqsubseteq B$. *If* $unqualify(A)$ *is not a type variable, then* $unqualify(B)$ *is not either.*

Proof. By induction on the type containment derivation. Only the interesting case is for (C_Inst). In that case, we are given $\Gamma \vdash \forall \alpha.\, C \sqsubseteq C[D/\alpha]$ ($A = \forall \alpha.\, C$ and $B = C[D/\alpha]$) for some α, C, and D, and, by inversion, $\Gamma \vdash D$. It is easy to see, if $unqualify(\forall \beta.\, C) = unqualify(C)$ is not a type variable, then $unqualify(C[D/\beta])$ is not either. □

Lemma 6. *Suppose that $\Gamma \vdash A \sqsubseteq B$ and unqualify(A) is not a type variable.*

1. *If unqualify$(B) = \iota$, then unqualify$(A) = \iota$.*
2. *If unqualify$(B) = B_1 \rightarrow B_2$, then unqualify$(A) = A_1 \rightarrow A_2$ for some A_1 and A_2.*
3. *If unqualify$(B) = B_1 \times B_2$, then unqualify$(A) = A_1 \times A_2$ for some A_1 and A_2.*
4. *If unqualify$(B) = B_1 + B_2$, then unqualify$(A) = A_1 + A_2$ for some A_1 and A_2.*
5. *If unqualify$(B) = B' \, \mathsf{list}$, then unqualify$(A) = A' \, \mathsf{list}$ for some A'.*

Proof. By induction on the type containment derivation. The case for (C_Trans) is shown by the IHs and Lemma 5. In the case for (C_Inst), we are given $\Gamma \vdash \forall \alpha. C \sqsubseteq C[D/\alpha]$ for some α, C, and D ($A = \forall \alpha. C$ and $B = C[D/\alpha]$). Since *unqualify*$(\forall \alpha. C)$ = *unqualify*(C) is not a type variable, it is easy to see that the top type constructor of *unqualify*(C) is the same as that of *unqualify*$(C[D/\alpha])$. Proving the other cases is straightforward. □

Lemma 7. *If $\Gamma \vdash v : A$, then unqualify(A) is not a type variable.*

Proof. By induction on the typing derivation for v. We can show the case for (T_Inst) by the IH and Lemma 5. □

Lemma 8 (Canonical forms)**.** *Suppose that $\Gamma \vdash v : A$.*

1. *If unqualify$(A) = \iota$, then $v = c$ for some c.*
2. *If unqualify$(A) = B \rightarrow C$, then $v = c$ for some c, or $v = \lambda x.M$ for some x and M.*
3. *If unqualify$(A) = B \times C$, then $v = (v_1, v_2)$ for some v_1 and v_2.*
4. *If unqualify$(A) = B + C$, then $v = \mathsf{inl}\, v'$ or $v = \mathsf{inr}\, v'$ for some v'.*
5. *If unqualify$(A) = B \, \mathsf{list}$, then $v = \mathsf{nil}$ or $v = \mathsf{cons}\, v'$ for some v'.*

Proof. Straightforward by induction on the typing derivation for v. Only the interesting case is for (T_Inst). In the case, we are given, by inversion, $\Gamma \vdash v : B$ and $\Gamma \vdash B \sqsubseteq A$ and $\Gamma \vdash A$ for some B. By Lemma 7, *unqualify*(B) is not a type variable. Thus, by Lemma 6 and the IH, we finish. □

Definition 14. *We use the metavariable Δ for ranging over typing contexts that consist of only type variables. Formally, they are defined by the following syntax.*

$$\Delta ::= \emptyset \mid \Delta, \alpha$$

Lemma 9 (Type containment inversion: function types)**.** *If $\Gamma \vdash \forall \boldsymbol{\alpha_1}^{I_1}. A_1 \rightarrow A_2 \sqsubseteq \forall \boldsymbol{\alpha_2}^{I_2}. B_1 \rightarrow B_2$, then there exist $\boldsymbol{\alpha_{11}}^{I_{11}}$, $\boldsymbol{\alpha_{12}}^{I_{12}}$, $\boldsymbol{\beta}^{J}$, and $\boldsymbol{C}^{I_{11}}$ such that*

- $\{\boldsymbol{\alpha_1}^{I_1}\} = \{\boldsymbol{\alpha_{11}}^{I_{11}}\} \uplus \{\boldsymbol{\alpha_{12}}^{I_{12}}\}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta}^{J} \vdash \boldsymbol{C}^{I_{11}}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash B_1 \sqsubseteq \forall \boldsymbol{\beta}^{J}. A_1[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}. \forall \boldsymbol{\beta}^{J}. A_2[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_2$, *and*
- *type variables in $\{\boldsymbol{\beta}^{J}\}$ do not appear free in A_1 and A_2.*

Proof. By induction on the type containment derivation. Throughout the proof, we use the fact of $\vdash \Gamma$ for applying (C_Refl); it is shown easily by induction on the type containment derivation.

Case (C_Refl): We have $\boldsymbol{\alpha_1}^{I_1} = \boldsymbol{\alpha_2}^{I_2}$ and $A_1 = B_1$ and $A_2 = B_2$. Let $\boldsymbol{\alpha_{12}}^{I_{12}}$ and $\boldsymbol{\beta}^{J}$ be the empty sequence, $\boldsymbol{\alpha_{11}}^{I_{11}} = \boldsymbol{\alpha_1}^{I_1}$, and $\boldsymbol{C}^{I_{11}} = \boldsymbol{\alpha_1}^{I_1}$. We have to show that

- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash B_1 \sqsubseteq A_1$ and
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash A_2 \sqsubseteq B_2$.

They are derived by (C_Refl).

Case (C_Trans): By inversion, we have $\Gamma \vdash \forall \boldsymbol{\alpha_1}^{I_1}.\, A_1 \rightarrow A_2 \sqsubseteq D$ and $\Gamma \vdash D \sqsubseteq \forall \boldsymbol{\alpha_2}^{I_2}.\, B_1 \rightarrow B_2$ for some D. By Lemma 6, $D = \forall \boldsymbol{\alpha_3}^{I_3}.\, D_1 \rightarrow D_2$ for some $\boldsymbol{\alpha_3}^{I_3}$, D_1, and D_2. By the IH on $\Gamma \vdash \forall \boldsymbol{\alpha_1}^{I_1}.\, A_1 \rightarrow A_2 \sqsubseteq \forall \boldsymbol{\alpha_3}^{I_3}.\, D_1 \rightarrow D_2$, there exist $\boldsymbol{\alpha_{11}}^{I_{11}}$, $\boldsymbol{\alpha_{12}}^{I_{12}}$, $\boldsymbol{C_1}^{I_{11}}$, and $\boldsymbol{\beta_1}^{J_1}$ such that

- $\{\boldsymbol{\alpha_1}^{I_1}\} = \{\boldsymbol{\alpha_{11}}^{I_{11}}\} \uplus \{\boldsymbol{\alpha_{12}}^{I_{12}}\}$,
- $\Gamma, \boldsymbol{\alpha_3}^{I_3}, \boldsymbol{\beta_1}^{J_1} \vdash \boldsymbol{C_1}^{I_{11}}$,
- $\Gamma, \boldsymbol{\alpha_3}^{I_3} \vdash D_1 \sqsubseteq \forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C_1}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$,
- $\Gamma, \boldsymbol{\alpha_3}^{I_3} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_2[\boldsymbol{C_1}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq D_2$, and
- type variables in $\boldsymbol{\beta_1}^{J_1}$ do not appear free in A_1 and A_2.

By the IH on $\Gamma \vdash \forall \boldsymbol{\alpha_3}^{I_3}.\, D_1 \rightarrow D_2 \sqsubseteq \forall \boldsymbol{\alpha_2}^{I_2}.\, B_1 \rightarrow B_2$, there exist $\boldsymbol{\alpha_{31}}^{I_{31}}$, $\boldsymbol{\alpha_{32}}^{I_{32}}$, $\boldsymbol{C_3}^{I_{31}}$, and $\boldsymbol{\beta_3}^{J_3}$ such that

- $\{\boldsymbol{\alpha_3}^{I_3}\} = \{\boldsymbol{\alpha_{31}}^{I_{31}}\} \uplus \{\boldsymbol{\alpha_{32}}^{I_{32}}\}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta_3}^{J_3} \vdash \boldsymbol{C_3}^{I_{31}}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash B_1 \sqsubseteq \forall \boldsymbol{\beta_3}^{J_3}.\, D_1[\boldsymbol{C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}]$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{32}}^{I_{32}}.\forall \boldsymbol{\beta_3}^{J_3}.\, D_2[\boldsymbol{C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}] \sqsubseteq B_2$, and
- type variables in $\boldsymbol{\beta_3}^{J_3}$ do not appear free in D_1 and D_2.

We show the conclusion by letting $\boldsymbol{C}^{I_{11}} = \boldsymbol{C_1[C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}]^{I_{11}}$ and $\boldsymbol{\beta}^{J} = \boldsymbol{\alpha_{32}}^{I_{32}}, \boldsymbol{\beta_3}^{J_3}, \boldsymbol{\beta_1}^{J_1}$. We have to show that

- $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_{32}}^{I_{32}}, \boldsymbol{\beta_3}^{J_3}, \boldsymbol{\beta_1}^{J_1} \vdash \boldsymbol{C_1[C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}]^{I_{11}}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash B_1 \sqsubseteq \forall \boldsymbol{\alpha_{32}}^{I_{32}}.\forall \boldsymbol{\beta_3}^{J_3}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$, and
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}.\forall \boldsymbol{\alpha_{32}}^{I_{32}}.\forall \boldsymbol{\beta_3}^{J_3}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_2[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_2$.

The first requirement is shown by $\Gamma, \boldsymbol{\alpha_3}^{I_3}, \boldsymbol{\beta_1}^{J_1} \vdash \boldsymbol{C_1}^{I_{11}}$ and $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta_3}^{J_3} \vdash \boldsymbol{C_3}^{I_{31}}$ and Lemma 1 (2) and Lemma 2 (2).

Next, we show the second requirement. Since $\Gamma, \boldsymbol{\alpha_3}^{I_3} \vdash D_1 \sqsubseteq \forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C_1}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$ and $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta_3}^{J_3} \vdash \boldsymbol{C_3}^{I_{31}}$, we have $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_3}^{I_3}, \boldsymbol{\beta_3}^{J_3} \vdash D_1 \sqsubseteq \forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C_1}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$ and $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_{32}}^{I_{32}}, \boldsymbol{\beta_3}^{J_3} \vdash \boldsymbol{C_3}^{I_{31}}$ by Lemma 1 (3) and (2), respectively. Thus, by Lemma 2 (3),

$$\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_{32}}^{I_{32}}, \boldsymbol{\beta_3}^{J_3} \vdash D_1[\boldsymbol{C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}] \sqsubseteq \forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$$

(note that we can suppose that $\boldsymbol{\alpha_{31}}^{I_{31}}$ do not appear free in A_1). By (C_Poly),

$$\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_{32}}^{I_{32}} \vdash \forall \boldsymbol{\beta_3}^{J_3}.\, D_1[\boldsymbol{C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}] \sqsubseteq \forall \boldsymbol{\beta_3}^{J_3}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}].$$

Since $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash B_1 \sqsubseteq \forall \boldsymbol{\beta_3}^{J_3}.\, D_1[\boldsymbol{C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}]$, we have

$$\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_{32}}^{I_{32}} \vdash B_1 \sqsubseteq \forall \boldsymbol{\beta_3}^{J_3}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C_{01}}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$$

by Lemma 1 (3) and (C_Trans). Since we can suppose that $\boldsymbol{\alpha_{32}}^{I_{32}}$ do not appear free in B_1, we have

$$\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash B_1 \sqsubseteq \forall \boldsymbol{\alpha_{32}}^{I_{32}}.\forall \boldsymbol{\beta_3}^{J_3}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_1[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}]$$

by (C_Gen), (C_Poly), and (C_Trans).

Finally, we show the third requirement. Since $\Gamma, \boldsymbol{\alpha_3}^{I_3} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_2[\boldsymbol{C_1}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq D_2$ and $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta_3}^{J_3} \vdash \boldsymbol{C_3}^{I_{31}}$, we have $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_3}^{I_3}, \boldsymbol{\beta_3}^{J_3} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_2[\boldsymbol{C_1}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq D_2$ and $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_{32}}^{I_{32}}, \boldsymbol{\beta_3}^{J_3} \vdash \boldsymbol{C_3}^{I_{31}}$ by Lemma 1 (3) and (2), respectively. Thus, by Lemma 2 (3),

$$\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\alpha_{32}}^{I_{32}}, \boldsymbol{\beta_3}^{J_3} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_2[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq D_2[\boldsymbol{C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}]$$

(note that we can suppose that $\boldsymbol{\alpha_{31}}^{I_{31}}$ do not appear free in A_2). By (C_Poly),

$$\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{32}}^{I_{32}}.\forall \boldsymbol{\beta_3}^{J_3}.\forall \boldsymbol{\alpha_{12}}^{I_{12}}.\forall \boldsymbol{\beta_1}^{J_1}.\, A_2[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq \forall \boldsymbol{\alpha_{32}}^{I_{32}}.\forall \boldsymbol{\beta_3}^{J_3}.\, D_2[\boldsymbol{C_3}^{I_{31}}/\boldsymbol{\alpha_{31}}^{I_{31}}]$$

Since $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{32}}^{I_{32}}. \forall \boldsymbol{\beta_3}^{J_3}. D_2[\boldsymbol{C_3}^{I_{31}} / \boldsymbol{\alpha_{31}}^{I_{31}}] \sqsubseteq B_2$, we have

$$\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{32}}^{I_{32}}. \forall \boldsymbol{\beta_3}^{J_3}. \forall \boldsymbol{\alpha_{12}}^{I_{12}}. \forall \boldsymbol{\beta_1}^{J_1}. A_2[\boldsymbol{C}^{I_{11}} / \boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_2$$

by (C_Trans). Thus, by permutating $\forall$s on the left-hand side,

$$\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}. \forall \boldsymbol{\alpha_{32}}^{I_{32}}. \forall \boldsymbol{\beta_3}^{J_3}. \forall \boldsymbol{\beta_1}^{J_1}. A_2[\boldsymbol{C}^{I_{11}} / \boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_2.$$

Case (C_Fun): Obvious by inversion.

Case (C_Inst): We have $\boldsymbol{\alpha_1}^{I_1} = \alpha, \boldsymbol{\alpha_2}^{I_2}$ and $B_1 = A_1[C/\alpha]$ and $B_2 = A_2[C/\alpha]$ for some C such that $\Gamma \vdash C$. We show the conclusion by letting $\boldsymbol{\alpha_{11}}^{I_{11}} = \alpha, \boldsymbol{\alpha_2}^{I_2}$, $\boldsymbol{C}^{I_{11}} = C, \boldsymbol{\alpha_2}^{I_2}$, and $\boldsymbol{\alpha_{12}}^{I_{12}}$ and $\boldsymbol{\beta}^J$ be the empty sequence. We have to show that

- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash C$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash A_1[C/\alpha] \sqsubseteq A_1[C/\alpha]$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash A_2[C/\alpha] \sqsubseteq A_2[C/\alpha]$.

The first is shown by Lemma 1 (1). The second is by (C_Refl). The third is by (C_Refl).

Case (C_Gen): We have $\boldsymbol{\alpha_2}^{I_2} = \alpha, \boldsymbol{\alpha_1}^{I_1}$ and $A_1 = B_1$ and $A_2 = B_2$ and $\alpha \notin \mathit{ftv}(\forall \boldsymbol{\alpha_1}^{I_1}. A_1 \rightarrow A_2)$. We show the conclusion by letting $\boldsymbol{\alpha_{11}}^{I_{11}} = \boldsymbol{\alpha_1}^{I_1}$, $\boldsymbol{C}^{I_{11}} = \boldsymbol{\alpha_1}^{I_1}$, and $\boldsymbol{\alpha_{12}}^{I_{12}}$ and $\boldsymbol{\beta}^J$ be the empty sequence. We have to show that

- $\Gamma, \alpha, \boldsymbol{\alpha_1}^{I_1} \vdash A_1 \sqsubseteq A_1$ and
- $\Gamma, \alpha, \boldsymbol{\alpha_1}^{I_1} \vdash A_2 \sqsubseteq A_2$.

They are derived by (C_Refl).

Case (C_Poly): We have $\boldsymbol{\alpha_1}^{I_1} = \alpha, \boldsymbol{\alpha_{01}}^{I_{01}}$ and $\boldsymbol{\alpha_2}^{I_2} = \alpha, \boldsymbol{\alpha_{02}}^{I_{02}}$ and, by inversion, $\Gamma, \alpha \vdash \forall \boldsymbol{\alpha_{01}}^{I_{01}}. A_1 \rightarrow A_2 \sqsubseteq \forall \boldsymbol{\alpha_{02}}^{I_{02}}. B_1 \rightarrow B_2$. By the IH, there exist some $\boldsymbol{\alpha_{011}}^{I_{011}}$, $\boldsymbol{\alpha_{12}}^{I_{12}}$, $\boldsymbol{\beta}^J$, and $\boldsymbol{C_0}^{I_{011}}$ such that

- $\{\boldsymbol{\alpha_{01}}^{I_{01}}\} = \{\boldsymbol{\alpha_{011}}^{I_{011}}\} \uplus \{\boldsymbol{\alpha_{12}}^{I_{12}}\}$,
- $\Gamma, \alpha, \boldsymbol{\alpha_{02}}^{I_{02}}, \boldsymbol{\beta}^J \vdash \boldsymbol{C_0}^{I_{011}}$,
- $\Gamma, \alpha, \boldsymbol{\alpha_{02}}^{I_{02}} \vdash B_1 \sqsubseteq \forall \boldsymbol{\beta}^J. A_1[\boldsymbol{C_0}^{I_{011}} / \boldsymbol{\alpha_{011}}^{I_{011}}]$,
- $\Gamma, \alpha, \boldsymbol{\alpha_{02}}^{I_{02}} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}}. \forall \boldsymbol{\beta}^J. A_2[\boldsymbol{C_0}^{I_{011}} / \boldsymbol{\alpha_{011}}^{I_{011}}] \sqsubseteq B_2$, and
- type variables in $\boldsymbol{\beta}^J$ do not appear free in A_1 and B_1.

We can prove the conclusion by letting $\boldsymbol{\alpha_{11}}^{I_{11}} = \alpha, \boldsymbol{\alpha_{011}}^{I_{011}}$ and $\boldsymbol{C}^{I_{11}} = \alpha, \boldsymbol{C_0}^{I_{011}}$.

Case (C_DFun): It is found that, for some α, $\boldsymbol{\alpha_1}^{I_1} = \alpha$ and $\boldsymbol{\alpha_2}^{I_2}$ is the empty sequence and $B_1 = A_1$ and $B_2 = \forall \alpha. A_2$. We show the conclusion by letting $\boldsymbol{\alpha_{12}}^{I_{12}} = \alpha$ and $\boldsymbol{\alpha_{11}}^{I_{11}}$, $\boldsymbol{C}^{I_{11}}$, and $\boldsymbol{\beta}^J$ be the empty sequence. It suffices to show that $\Gamma \vdash A_1 \sqsubseteq A_1$ and $\Gamma \vdash \forall \alpha. A_2 \sqsubseteq \forall \alpha. A_2$, which are derived by (C_Refl).

Case (C_Prod), (C_Sum), (C_List), (C_DProd), (C_DSum), and (C_DList): Contradictory.

□

Lemma 10. *If $\Gamma \vdash A_1 \rightarrow A_2 \sqsubseteq B_1 \rightarrow B_2$, then $\Gamma \vdash B_1 \sqsubseteq A_1$ and $\Gamma \vdash A_2 \sqsubseteq B_2$.*

Proof. By Lemma 9, $\Gamma \vdash B_1 \sqsubseteq \forall \boldsymbol{\alpha}. A_1$ and $\Gamma \vdash \forall \boldsymbol{\alpha}. A_2 \sqsubseteq B_2$ for some [< X >] such that type variables in $\boldsymbol{\alpha}$ do not appear free in A_1 and A_2. Since $\Gamma \vdash \forall \boldsymbol{\alpha}. A_1 \sqsubseteq A_1$ by (C_Inst) (we can substitute any type, e.g., $\forall \beta. \beta$, for $\boldsymbol{\alpha}$), we have $\Gamma \vdash B_1 \sqsubseteq A_1$ by (C_Trans). Since $\Gamma \vdash A_2 \sqsubseteq \forall \boldsymbol{\alpha}. A_2$ by (C_Gen), we have $\Gamma \vdash A_2 \sqsubseteq B_2$. □

Lemma 11 (Value inversion: constants)**.** *If $\Gamma \vdash c : A$, then $\Gamma \vdash \mathit{ty}(c) \sqsubseteq A$.*

Proof. By induction on the typing derivation for c. There are only three typing rules that can be applied to c.

Case (T_Const): By (C_Refl).

Case (T_GEN): We are given $\Gamma \vdash c : \forall \alpha. B$ (i.e., $A = \forall \alpha. B$) and, by inversion, $\Gamma, \alpha \vdash c : B$. By the IH, $\Gamma, \alpha \vdash ty(c) \sqsubseteq B$. By (C_POLY), $\Gamma \vdash \forall \alpha. ty(c) \sqsubseteq \forall \alpha. B$. Since $ty(c)$ is closed, we have $\Gamma \vdash ty(c) \sqsubseteq \forall \alpha. ty(c)$ by (C_GEN). Thus, by (C_TRANS), we have the conclusion.

Case (T_INST): By the IH and (C_TRANS).

□

Lemma 12 (Progress). *If $\Delta \vdash M : A$, then:*

- *$M \longrightarrow M'$ for some M';*
- *M is a value; or*
- *$M = E[\#\mathsf{op}(v)]$ for some E, op, and v such that $\mathsf{op} \notin E$.*

Proof. By induction on the typing derivation for M. We proceed by case analysis on the typing rule applied last to derive $\Delta \vdash M : A$.

Case (T_VAR): Contradictory.

Case (T_CONST), (T_ABS), and (T_NIL): Obvious.

Case (T_ABS): Obvious.

Case (T_APP): We are given

- $M = M_1\, M_2$,
- $\Delta \vdash M_1\, M_2 : A$,
- $\Delta \vdash M_1 : B \to A$, and
- $\Delta \vdash M_2 : B$

for some M_1, M_2, and B. By case analysis on the behavior of M_1. We have three cases to consider by the IH.

Case $M_1 \longrightarrow M_1'$ for some M_1': We have $M \longrightarrow M_1'\, M_2$.

Case $M_1 = E_1[\#\mathsf{op}(v)]$ for some E_1, op, and v such that $\mathsf{op} \notin E_1$: We have the third case in the conclusion by letting $E = E_1\, M_2$.

Case $M_1 = v_1$ for some v_1: By case analysis on the behavior of M_2 with the IH.

Case $M_2 \longrightarrow M_2'$ for some M_2': We have $M \longrightarrow v_1\, M_2'$.

Case $M_2 = E_2[\#\mathsf{op}(v)]$ for some E_2, op, and v such that $\mathsf{op} \notin E_2$: We have the third case in the conclusion by letting $E = v_1\, E_2$.

Case $M_2 = v_2$ for some v_2: By Lemma 8 on v_1, we have two cases to consider.

Case $v_1 = c_1$: Since $\Delta \vdash c_1 : B \to A$, we have $\Delta \vdash ty(c_1) \sqsubseteq B \to A$ by Lemma 11. By Lemma 6 (2), it is found that $ty(c_1) = \iota \to C$ for some ι and C. Since $\Delta \vdash \iota \to C \sqsubseteq B \to A$, we have $\Delta \vdash B \sqsubseteq \iota$ for some $\boldsymbol{\gamma}^{I_0}$ by Lemma 10. Since $\Delta \vdash v_2 : B$, $unqualify(B)$ is not a type variable by Lemma 7. Thus, since $\Delta \vdash B \sqsubseteq \iota$, it is found that $unqualify(B) = \iota$ by Lemma 6. Since $\Delta \vdash v_2 : B$, we have $v_2 = c_2$ for some c_2 by Lemma 8. Since $\Delta \vdash c_2 : B$, we have $\Delta \vdash ty(c_2) \sqsubseteq B$ by Lemma 11. Since $unqualify(B) = \iota$, we have $ty(c_2) = \iota$ by Lemma 6. Thus, $\zeta(c_1, c_2)$ is defined, and $M = c_1\, c_2 \longrightarrow \zeta(c_1, c_2)$ by (R_CONST)/(E_EVAL).

Case $v_1 = \lambda x.M'$: By (R_BETA)/(E_EVAL), $M = (\lambda x.M')\, v_2 \longrightarrow M'[v_2/x]$.

Case (T_GEN): By the IH.

Case (T_INST): By the IH.

Case (T_OP): We are given

- $M = \#\mathsf{op}(M')$,

- $ty\,(\mathsf{op}) = \forall\, \boldsymbol{\alpha}.\, A' \hookrightarrow B'$,
- $\Delta \vdash \#\mathsf{op}(M') : B'[\boldsymbol{C}/\boldsymbol{\alpha}]$, and
- $\Delta \vdash M' : A'[\boldsymbol{C}/\boldsymbol{\alpha}]$

for some op, M', $\boldsymbol{\alpha}$, A', B', and $\boldsymbol{C}$. By case analysis on the behavior of M' with the IH.

Case $M' \longrightarrow M''$ for some M'': We have $M \longrightarrow \#\mathsf{op}(M'')$.

Case $M' = E'[\#\mathsf{op}'(v)]$ for some E', op', and v such that $\mathsf{op}' \notin E'$: We have the third case in the conclusion by letting $E = \#\mathsf{op}(E')$.

Case $M' = v$ for some v: We have the third case in the conclusion by letting $E = []$.

Case (T_Handle): We are given

- $M = \mathsf{handle}\, M'\, \mathsf{with}\, H$,
- $\Delta \vdash M' : B$, and
- $\Delta \vdash H : B \Rightarrow A$

for some M', H, and B. By case analysis on the behavior of M' with the IH.

Case $M' \longrightarrow M''$ for some M'': We have $M \longrightarrow \mathsf{handle}\, M''\, \mathsf{with}\, H$.

Case $M' = E'[\#\mathsf{op}(v)]$ for some E', op, and v such that $\mathsf{op} \notin E'$: If handler H contains an operation clause $\mathsf{op}(x, k) \rightarrow M''$, then we have $M \longrightarrow M''[v/x][\lambda y.\mathsf{handle}\, E'[y]\, \mathsf{with}\, H/k]$ by (R_Handle)/(E_Eval).

Otherwise, if H contains no operation clause for op, we have the third case in the conclusion by letting $E = \mathsf{handle}\, E'\, \mathsf{with}\, H$.

Case $M' = v$ for some v: By (R_Return)/(E_Eval).

Case (T_Pair): We are given

- $M = (M_1, M_2)$,
- $\Delta \vdash M_1 : B_1$, and
- $\Delta \vdash M_2 : B_2$

for some M_1, M_2, B_1, and B_2. By case analysis on the behavior of M_1 with the IH.

Case $M_1 \longrightarrow M_1'$ for some M_1': We have $M = (M_1', M_2)$.

Case $M_1 = E_1[\#\mathsf{op}(v)]$ for some E_1, op, and v such that $\mathsf{op} \notin E_1$: We have the third case in the conclusion by letting $E = (E_1, M_2)$.

Case $M_1 = v_1$ for some v_1: By case analysis on the behavior of M_2 with the IH.

Case $M_2 \longrightarrow M_2'$: We have $M_2 \longrightarrow (v_1, M_2')$.

Case $M_2 = E_2[\#\mathsf{op}(v)]$ for some E_2, op, and v such that $\mathsf{op} \notin E_2$: We have the third case in the conclusion by letting $E = (v_1, E_2)$.

Case $M_2 = v_2$: We have the second case in the conclusion since $M = (v_1, v_2)$.

Case (T_Proj1): We are given

- $M = \pi_1 M'$ and
- $\Delta \vdash M' : A \times B$

for some M' and B. By case analysis on the behavior of M' with the IH.

Case $M' \longrightarrow M''$ for some M'': We have $M \longrightarrow \pi_1 M''$.

Case $M' = E'[\#\mathsf{op}(v)]$ for some E', op, and v such that $\mathsf{op} \notin E'$: We have the third case in the conclusion by letting $E = \pi_1 E'$.

Case $M' = v'$ for some v': Since $\Delta \vdash M' : A \times B$ (i.e., $\Delta \vdash v' : A \times B$), we have $v' = (v_1, v_2)$ for some v_1 and v_2 by Lemma 8. By (R_Proj1)/(E_Eval), we finish.

Case (T_Proj2): Similarly to the case for (T_Proj1).

Case (T_InL), (T_InR), and (T_Cons): Similarly to the case for (T_Pair).

Case (T_Case): We are given

- $M = \mathsf{case}\, M'\, \mathsf{of\, inl}\, x \rightarrow M_1; \mathsf{inr}\, y \rightarrow M_2$ and
- $\Delta \vdash M' : B + C$

for some M', M_1, M_2, x, y, B, and C. By case analysis on the behavior of M' wit the IH.

Case $M' \longrightarrow M''$ for some M'': We have $M \longrightarrow \mathsf{case}\, M''\, \mathsf{of\, inl}\, x \rightarrow M_1; \mathsf{inr}\, y \rightarrow M_2$.

Case $M' = E'[\#\mathsf{op}(v)]$ for some E', op, and v such that $\mathsf{op} \notin E'$: We have the third case in the conclusion by letting $E = \mathsf{case}\, E'\, \mathsf{of\, inl}\, x \rightarrow M_1; \mathsf{inr}\, y \rightarrow M_2$.

Case $M' = v$ for some v: By Lemma 8, $v = \mathsf{inl}\, v'$ or $v = \mathsf{inr}\, v'$ for some v'. We finish by (R_CaseL)/(E_Eval) or (R_CaseR)/(E_Eval).

Case (T_CaseList): Similar to the case for (T_Case).

Case (T_Fix): By (R_Fix)/(E_Eval).

□

Lemma 13.

1. *If* $\Gamma \vdash M : A$*, then* $\Gamma \vdash A$*.*
2. *If* $\Gamma \vdash H : A \Rightarrow B$*, then* $\Gamma \vdash B$*.*

Proof. Straightforward by mutual induction on the typing derivations. The case for (T_Op) depends on Lemma 2 and Definition 4, which states that, for op such that $\mathit{ty}(\mathsf{op}) = \forall \boldsymbol{\alpha}. A \hookrightarrow B$, $\mathit{ftv}(B) \subseteq \{\boldsymbol{\alpha}\}$. □

Lemma 14 (Value inversion: lambda abstractions)**.** *If* $\Gamma \vdash \lambda x.M : A$*, then* $\Gamma, \boldsymbol{\alpha}, x : B \vdash M : C$ *and* $\Gamma \vdash \forall \boldsymbol{\alpha}. B \rightarrow C \sqsubseteq A$ *for some* $\boldsymbol{\alpha}$*,* B*, and* C*.*

Proof. By induction on the typing derivation for $\lambda x.M$. There are only three typing rules that can be applied to $\lambda x.M$.

Case (T_Abs): We have $A = B \rightarrow C$ and let $\boldsymbol{\alpha}$ be the empty sequence. We have the conclusion by inversion and (C_Refl).

Case (T_Gen): We are given $\Gamma \vdash \lambda x.M : \forall \beta. D$ (i.e., $A = \forall \beta. D$) and, by inversion, $\Gamma, \beta \vdash \lambda x.M : D$. By the IH, $\Gamma, \beta, \boldsymbol{\gamma}^I, x : B \vdash M : C$ and $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I. B \rightarrow C \sqsubseteq D$ for some $\boldsymbol{\gamma}^I$, B, and C. We show the conclusion by letting $\boldsymbol{\alpha} = \beta, \boldsymbol{\gamma}^I$. It suffices to show that $\Gamma \vdash \forall \beta. \forall \boldsymbol{\gamma}^I. B \rightarrow C \sqsubseteq \forall \beta. D$, which is derived from $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I. B \rightarrow C \sqsubseteq D$ with (C_Poly).

Case (T_Inst): By the IH and (C_Trans).

□

Lemma 15 (Value inversion: pairs)**.** *If* $\Gamma \vdash (M_1, M_2) : A$*, then* $\Gamma, \boldsymbol{\alpha} \vdash M_1 : B_1$ *and* $\Gamma, \boldsymbol{\alpha} \vdash M_2 : B_2$ *and* $\Gamma \vdash \forall \boldsymbol{\alpha}. B_1 \times B_2 \sqsubseteq A$ *for some* $\boldsymbol{\alpha}$*,* B_1*, and* B_2*.*

Proof. By induction on the typing derivation for (M_1, M_2). There are only three typing rules that can be applied to (M_1, M_2).

Case (T_Pair): Obvious by (C_Refl).

Case (T_Gen): We are given $\Gamma \vdash (M_1, M_2) : \forall \beta.\, C$ (i.e., $A = \forall \beta.\, C$) and, by inversion, $\Gamma, \beta \vdash (M_1, M_2) : C$. By the IH, $\Gamma, \beta, \boldsymbol{\gamma}^I \vdash M_1 : B_1$ and $\Gamma, \beta, \boldsymbol{\gamma}^I \vdash M_2 : B_2$ $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I.\, B_1 \times B_2 \sqsubseteq C$ for some $\boldsymbol{\gamma}^I$, B_1, and B_2. We show the conclusion by letting $\boldsymbol{\alpha} = \beta, \boldsymbol{\gamma}^I$. It suffices to show that $\Gamma \vdash \forall \beta. \forall \boldsymbol{\gamma}^I.\, B_1 \times B_2 \sqsubseteq \forall \beta.\, C$, which is derived from $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I.\, B_1 \times B_2 \sqsubseteq C$ with (C_Poly).

Case (T_Inst): By the IH and (C_Trans).

□

Lemma 16 (Value inversion: left injections)**.** *If $\Gamma \vdash \mathsf{inl}\, M : A$, then $\Gamma, \boldsymbol{\alpha} \vdash M : B$ and $\Gamma \vdash \forall \boldsymbol{\alpha}.\, B + C \sqsubseteq A$ for some $\boldsymbol{\alpha}$, B, and C.*

Proof. By induction on the typing derivation for $\mathsf{inl}\, M$. There are only three typing rules that can be applied to $\mathsf{inl}\, M$.

Case (T_InL): Obvious by (C_Refl).

Case (T_Gen): We are given $\Gamma \vdash \mathsf{inl}\, M : \forall \beta.\, D$ (i.e., $A = \forall \beta.\, D$) and, by inversion, $\Gamma, \beta \vdash \mathsf{inl}\, M : D$. By the IH, $\Gamma, \beta, \boldsymbol{\gamma}^I \vdash M : B$ and $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I.\, B + C \sqsubseteq D$ for some $\boldsymbol{\gamma}^I$, B, and C. We show the conclusion by letting $\boldsymbol{\alpha} = \beta, \boldsymbol{\gamma}^I$. It suffices to show that $\Gamma \vdash \forall \beta. \forall \boldsymbol{\gamma}^I.\, B + C \sqsubseteq \forall \beta.\, D$, which is derived from $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I.\, B + C \sqsubseteq D$ with (C_Poly).

Case (T_Inst): By the IH and (C_Trans).

□

Lemma 17 (Value inversion: right injections)**.** *If $\Gamma \vdash \mathsf{inr}\, M : A$, then $\Gamma, \boldsymbol{\alpha} \vdash M : C$ and $\Gamma \vdash \forall \boldsymbol{\alpha}.\, B + C \sqsubseteq A$ for some $\boldsymbol{\alpha}$, B, and C.*

Proof. Similarly to the proof of Lemma 16. □

Lemma 18 (Value inversion: cons)**.** *If $\Gamma \vdash \mathsf{cons}\, M : A$, then $\Gamma, \boldsymbol{\alpha} \vdash M : B \times B\, \mathsf{list}$ and $\Gamma \vdash \forall \boldsymbol{\alpha}.\, B\, \mathsf{list} \sqsubseteq A$ for some $\boldsymbol{\alpha}$ and B.*

Proof. By induction on the typing derivations for $\mathsf{cons}\, M$. There are only three typing rules that can be applied to $\mathsf{cons}\, M$.

Case (T_Cons): Obvious by (C_Refl).

Case (T_Gen): We are given $\Gamma \vdash \mathsf{cons}\, M : \forall \beta.\, C$ (i.e., $A = \forall \beta.\, C$) and, by inversion, $\Gamma, \beta \vdash \mathsf{cons}\, M : C$. By the IH, $\Gamma, \beta, \boldsymbol{\gamma}^I \vdash M : B \times B\, \mathsf{list}$ and $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I.\, B\, \mathsf{list} \sqsubseteq C$ for some $\boldsymbol{\gamma}^I$ and B. We show the conclusion by letting $\boldsymbol{\alpha} = \beta, \boldsymbol{\gamma}^I$. It suffices to show that $\Gamma \vdash \forall \beta. \forall \boldsymbol{\gamma}^I.\, B\, \mathsf{list} \sqsubseteq \forall \beta.\, C$, which is derived from $\Gamma, \beta \vdash \forall \boldsymbol{\gamma}^I.\, B\, \mathsf{list} \sqsubseteq C$ with (C_Poly).

Case (T_Inst): By the IH and (C_Trans).

□

Lemma 19. *If $ty\,(\mathsf{op}) = \forall \boldsymbol{\alpha}^I.\, A \hookrightarrow B$ and $\Gamma \vdash \#\mathsf{op}(v) : C$, then*

- $\Gamma, \boldsymbol{\beta}^J \vdash \boldsymbol{D}^I$,
- $\Gamma, \boldsymbol{\beta}^J \vdash v : A[\boldsymbol{D}^I / \boldsymbol{\alpha}^I]$, *and*
- $\Gamma \vdash \forall \boldsymbol{\beta}^J.\, B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq C$

for some $\boldsymbol{\beta}^J$ and $\boldsymbol{D}^I$.

Proof. By induction on the typing derivation for $\#\mathsf{op}(v)$. There are only three typing rules that can be applied to $\#\mathsf{op}(v)$.

Case (T_Op): We have $C = B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I]$ and $\Gamma \vdash \boldsymbol{D}^I$ and $\Gamma \vdash v : A[\boldsymbol{D}^I / \boldsymbol{\alpha}^I]$ for some $\boldsymbol{D}^I$. We have the conclusion by letting $\boldsymbol{\beta}^J$ be the empty sequence; note that $\Gamma \vdash B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I]$ by (C_Refl).

Case (T_Gen): We are given $C = \forall \beta.\, C_0$ and, by inversion, $\Gamma, \beta \vdash \texttt{\#op}(v) : C_0$ for some β and C_0. By the IH, there exist some $\boldsymbol{\beta_0}^{J_0}$ and $\boldsymbol{D}^I$ such that

- $\Gamma, \beta, \boldsymbol{\beta_0}^{J_0} \vdash \boldsymbol{D}^I$,
- $\Gamma, \beta, \boldsymbol{\beta_0}^{J_0} \vdash v : A[\boldsymbol{D}^I / \boldsymbol{\alpha}^I]$ and
- $\Gamma, \beta \vdash \forall \boldsymbol{\beta_0}^{J_0}.\, B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq C_0$.

We show the conclusion by letting $\boldsymbol{\beta}^J = \beta, \boldsymbol{\beta_0}^{J_0}$. It suffices to show $\Gamma \vdash \forall \beta. \forall \boldsymbol{\beta_0}^{J_0}.\, B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq \forall \beta.\, C_0$, which is proven from $\Gamma, \beta \vdash \forall \boldsymbol{\beta_0}^{J_0}.\, B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq C_0$ with (C_Poly).

Case (T_Inst): By the IH and (C_Trans).

□

Lemma 20. *If* $\Gamma, \boldsymbol{\alpha}^I \vdash E[M] : A$, *then*

- $\Gamma, \boldsymbol{\alpha}^I, \boldsymbol{\beta}^J \vdash M : B$ *and*
- $\Gamma, y : \forall \boldsymbol{\alpha}^I. \forall \boldsymbol{\beta}^J.\, B, \boldsymbol{\alpha}^I \vdash E[y] : A$ *for any* $y \notin dom(\Gamma)$

for some $\boldsymbol{\beta}^J$ *and* B.

Proof. By induction on the typing derivation of $\Gamma, \boldsymbol{\alpha}^I \vdash E[M] : A$.

Suppose that $E = []$. Since $\Gamma, \boldsymbol{\alpha}^I \vdash E[M] : A$, we have $\Gamma, \boldsymbol{\alpha}^I \vdash M : A$. We let $\boldsymbol{\beta}^J$ be the empty sequence and $B = A$. It is then trivial that $\Gamma, y : \forall \boldsymbol{\alpha}^I.\, B, \boldsymbol{\alpha}^I \vdash E[y] : A$ by (T_Inst). Note that $\vdash \Gamma$ and $\Gamma \vdash \forall \boldsymbol{\alpha}.\, B$ by Lemma 13.

In what follows, we suppose that $E \neq []$. We proceed by case analysis on the typing rule applied last to derive $\Gamma, \boldsymbol{\alpha}^I \vdash E[M] : A$.

Case (T_Var), (T_Const), (T_Abs), (T_Nil), and (T_Fix): Contradictory with the assumption that $E \neq []$.

Case (T_App): By case analysis on E.

Case $E = E'\, M_2$: By inversion of the typing derivation, we have $\Gamma, \boldsymbol{\alpha}^I \vdash E'[M] : C \to A$ and $\Gamma, \boldsymbol{\alpha}^I \vdash M_2 : C$ for some C. By the IH, (1) $\Gamma, \boldsymbol{\alpha}^I, \boldsymbol{\beta}^J \vdash M : B$ for some $\boldsymbol{\beta}^J$ and B and (2) for any $y \notin dom(\Gamma)$, $\Gamma, y : \forall \boldsymbol{\alpha}^I. \forall \boldsymbol{\beta}^J.\, B, \boldsymbol{\alpha}^I \vdash E'[y] : C \to A$. By Lemma 1 (4) and (T_App), $\Gamma, y : \forall \boldsymbol{\alpha}^I. \forall \boldsymbol{\beta}^J.\, B, \boldsymbol{\alpha}^I \vdash E'[y]\, M_2 : A$, i.e., $\Gamma, y : \forall \boldsymbol{\alpha}^I. \forall \boldsymbol{\beta}^J.\, B, \boldsymbol{\alpha}^I \vdash E[y] : A$.

Case $E = v_1\, E'$: Similarly to the above case.

Case (T_Gen): We have $\Gamma, \boldsymbol{\alpha}^I \vdash E[M] : \forall \gamma.\, A'$ and, by inversion, $\Gamma, \boldsymbol{\alpha}^I, \gamma \vdash E[M] : A'$ for some γ and A' (note $A = \forall \gamma.\, A'$). By the IH, (1) $\Gamma, \boldsymbol{\alpha}^I, \gamma, \boldsymbol{\beta}^J \vdash M : B$ for some $\boldsymbol{\beta}^J$ and B and (2) for any $y \notin dom(\Gamma)$, $\Gamma, y : \forall \boldsymbol{\alpha}^I. \forall \gamma. \forall \boldsymbol{\beta}^J.\, B, \boldsymbol{\alpha}^I, \gamma \vdash E[y] : A'$.

By (T_Gen), $\Gamma, y : \forall \boldsymbol{\alpha}^I. \forall \gamma. \forall \boldsymbol{\beta}^J.\, B, \boldsymbol{\alpha}^I \vdash E[y] : \forall \gamma.\, A'$. Since $A = \forall \gamma.\, A'$, we finish.

Otherwise: By the IH(s) and the corresponding typing rule, as the case for (T_App).

□

Lemma 21. *Suppose that* $\Gamma_1 \vdash A \sqsubseteq B$ *and* $\Gamma_1 \vdash A$.

1. *If* $\Gamma_1, x : B, \Gamma_2 \vdash M : C$, *then* $\Gamma_1, x : A, \Gamma_2 \vdash M : C$.
2. *If* $\Gamma_1, x : B, \Gamma_2 \vdash H : C \Rightarrow D$, *then* $\Gamma_1, x : A, \Gamma_2 \vdash H : C \Rightarrow D$.

Proof. By mutual induction on the typing derivations. □

Lemma 22. *If* $ty\,(\mathsf{op}) = \forall \boldsymbol{\alpha}^I.\, A \hookrightarrow B$ *and* $\Gamma \vdash E[\texttt{\#op}(v)] : C$, *then*

- $\Gamma, \boldsymbol{\beta}^J \vdash \boldsymbol{D}^I$,
- $\Gamma, \boldsymbol{\beta}^J \vdash v : A[\boldsymbol{D}^I / \boldsymbol{\alpha}^I]$, *and*

- *for any* $y \notin dom(\Gamma)$, $\Gamma, y : \forall \boldsymbol{\beta}^J . B\, [\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \vdash E[y] : C$

for some $\boldsymbol{\beta}^J$ *and* $\boldsymbol{D}^I$*.*

Proof. By Lemma 20,

- $\Gamma, \boldsymbol{\beta_1}^{J_1} \vdash \texttt{\#op}(v) : C'$ and
- $\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1} . C' \vdash E[y] : C$ for any $y \notin dom(\Gamma)$

for some $\boldsymbol{\beta_1}^{J_1}$ and C'. By Lemma 19,

- $\Gamma, \boldsymbol{\beta_1}^{J_1}, \boldsymbol{\beta_2}^{J_2} \vdash \boldsymbol{D}^I$,
- $\Gamma, \boldsymbol{\beta_1}^{J_1}, \boldsymbol{\beta_2}^{J_2} \vdash v : A[\boldsymbol{D}^I / \boldsymbol{\alpha}^I]$, and
- $\Gamma, \boldsymbol{\beta_1}^{J_1} \vdash \forall \boldsymbol{\beta_2}^{J_2} . B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq C'$

for some $\boldsymbol{\beta_2}^{J_2}$ and $\boldsymbol{D}^I$.

We show the conclusion by letting $\boldsymbol{\beta}^J = \boldsymbol{\beta_1}^{J_1}, \boldsymbol{\beta_2}^{J_2}$. It suffices to show that, for any $y \notin dom(\Gamma)$,

$$\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1} . \forall \boldsymbol{\beta_2}^{J_2} . B\, [\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \vdash E[y] : C.$$

Since $\Gamma, \boldsymbol{\beta_1}^{J_1} \vdash \forall \boldsymbol{\beta_2}^{J_2} . B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq C'$, we have

$$\Gamma \vdash \forall \boldsymbol{\beta_1}^{J_1} . \forall \boldsymbol{\beta_2}^{J_2} . B[\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \sqsubseteq \forall \boldsymbol{\beta_1}^{J_1} . C'$$

by (C_Poly). Since $\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1} . C' \vdash E[y] : C$, we have

$$\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1} . \forall \boldsymbol{\beta_2}^{J_2} . B\, [\boldsymbol{D}^I / \boldsymbol{\alpha}^I] \vdash E[y] : C.$$

by Lemma 21. □

Lemma 23 (Type containment inversion: product types)**.** *If* $\Gamma \vdash \forall \boldsymbol{\alpha_1}^{I_1} . A_1 \times A_2 \sqsubseteq \forall \boldsymbol{\alpha_2}^{I_2} . B_1 \times B_2$*, then there exist* $\boldsymbol{\alpha_{11}}^{I_{11}}$*,* $\boldsymbol{\alpha_{12}}^{I_{12}}$*,* $\boldsymbol{\beta}^J$*, and* $\boldsymbol{C}^{I_{11}}$ *such that*

- $\{\boldsymbol{\alpha_1}^{I_1}\} = \{\boldsymbol{\alpha_{11}}^{I_{11}}\} \uplus \{\boldsymbol{\alpha_{12}}^{I_{12}}\}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta}^J \vdash \boldsymbol{C}^{I_{11}}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}} . \forall \boldsymbol{\beta}^J . A_1[\boldsymbol{C}^{I_{11}} / \boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_1$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}} . \forall \boldsymbol{\beta}^J . A_2[\boldsymbol{C}^{I_{11}} / \boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_2$*, and*
- *type variables in* $\{\boldsymbol{\beta}^J\}$ *do not appear free in* A_1 *and* A_2*.*

Proof. By induction on the type containment derivation. The proof is similar to that of Lemma 9. □

Lemma 24 (Type containment inversion: sum types)**.** *If* $\Gamma \vdash \forall \boldsymbol{\alpha_1}^{I_1} . A_1 + A_2 \sqsubseteq \forall \boldsymbol{\alpha_2}^{I_2} . B_1 + B_2$*, then there exist* $\boldsymbol{\alpha_{11}}^{I_{11}}$*,* $\boldsymbol{\alpha_{12}}^{I_{12}}$*,* $\boldsymbol{\beta}^J$*, and* $\boldsymbol{C}^{I_{11}}$ *such that*

- $\{\boldsymbol{\alpha_1}^{I_1}\} = \{\boldsymbol{\alpha_{11}}^{I_{11}}\} \uplus \{\boldsymbol{\alpha_{12}}^{I_{12}}\}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta}^J \vdash \boldsymbol{C}^{I_{11}}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}} . \forall \boldsymbol{\beta}^J . A_1[\boldsymbol{C}^{I_{11}} / \boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_1$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall \boldsymbol{\alpha_{12}}^{I_{12}} . \forall \boldsymbol{\beta}^J . A_2[\boldsymbol{C}^{I_{11}} / \boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B_2$*, and*
- *type variables in* $\{\boldsymbol{\beta}^J\}$ *do not appear free in* A_1 *and* A_2*.*

Proof. By induction on the type containment derivation. The proof is similar to that of Lemma 9. □

Lemma 25 (Type containment inversion: list types). *If* $\Gamma \vdash \forall\, \boldsymbol{\alpha_1}^{I_1}.\, A\, \mathsf{list} \sqsubseteq \forall\, \boldsymbol{\alpha_2}^{I_2}.\, B\, \mathsf{list}$*, then there exist* $\boldsymbol{\alpha_{11}}^{I_{11}}$*,* $\boldsymbol{\alpha_{12}}^{I_{12}}$*,* $\boldsymbol{\beta}^{J}$*, and* $\boldsymbol{C}^{I_{11}}$ *such that*

- $\{\boldsymbol{\alpha_1}^{I_1}\} = \{\boldsymbol{\alpha_{11}}^{I_{11}}\} \uplus \{\boldsymbol{\alpha_{12}}^{I_{12}}\}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2}, \boldsymbol{\beta}^{J} \vdash \boldsymbol{C}^{I_{11}}$,
- $\Gamma, \boldsymbol{\alpha_2}^{I_2} \vdash \forall\, \boldsymbol{\alpha_{12}}^{I_{12}}.\, \forall\, \boldsymbol{\beta}^{J}.\, A[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha_{11}}^{I_{11}}] \sqsubseteq B$*, and*
- *type variables in* $\{\boldsymbol{\beta}^{J}\}$ *do not appear free in* A*.*

Proof. By induction on the type containment derivation. The proof is similar to that of Lemma 9. □

Lemma 26. *Suppose that* α *does not appear free in* A*.*

1. *If the occurrences of* β *in* A *are only negative, then* $\Gamma_1, \alpha, \Gamma_2 \vdash A[B/\beta] \sqsubseteq A[\forall\, \alpha.\, B/\beta]$*.*
2. *If the occurrences of* β *in* A *are only positive, then* $\Gamma_1, \alpha, \Gamma_2 \vdash A[\forall\, \alpha.\, B/\beta] \sqsubseteq A[B/\beta]$*.*

Proof. By structural induction on A.

Case $A = \gamma$: If $\gamma = \beta$, then we have to show that $\Gamma_1, \alpha, \Gamma_2 \vdash \forall\, \alpha.\, B \sqsubseteq B$, which is derived by (C_Refl), (C_Inst), and (C_Trans). Note that we do not need to consider the negative case, i.e., to show $\Gamma_1, \alpha, \Gamma_2 \vdash B \sqsubseteq \forall\, \alpha.\, B$, because the occurrence β in β is not negative.

Case $A = \iota$: By (C_Refl).

Case $A = \forall\, \gamma.\, C$: By the IH and (C_Poly) for each case.

Case $A = C \rightarrow D$: By the IHs and (C_Fun) for each case.

Case $A = C \times D$: By the IH and (C_Prod) for each case.

Case $A = C + D$: By the IH and (C_Sum) for each case.

Case $A = C\, \mathsf{list}$: By the IH and (C_List) for each case.

□

Lemma 27. *Suppose that* α *does not appear free in* A*.*

1. *If the occurrences of* β *in* A *are only negative or strictly positive, then* $\Gamma \vdash \forall\, \alpha.\, A[B/\beta] \sqsubseteq A[\forall\, \alpha.\, B/\beta]$*.*
2. *If the occurrences of* β *in* A *are only positive, then* $\Gamma \vdash A[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, A[B/\beta]$*.*

Proof. By induction on A.

Case $A = \gamma$: If $\gamma = \beta$, then we have to show that $\Gamma \vdash \forall\, \alpha.\, B \sqsubseteq \forall\, \alpha.\, B$ in the both cases, which is shown by (C_Refl). Otherwise, if $\gamma \neq \beta$, then we have to show that $\Gamma \vdash \forall\, \alpha.\, \gamma \sqsubseteq \gamma$ and $\Gamma \vdash \gamma \sqsubseteq \forall\, \alpha.\, \gamma$. By the assumption, $\alpha \neq \gamma$. Thus, by (C_Gen), $\Gamma \vdash \gamma \sqsubseteq \forall\, \alpha.\, \gamma$. We also have $\Gamma \vdash \forall\, \alpha.\, \gamma \sqsubseteq \gamma$ by (C_Inst) (the type used for instantiation can be any, e.g., int).

Case $A = \iota$: Similar for the case that $A = \gamma$ and $\gamma \neq \beta$.

Case $A = C \rightarrow D$: We prove the first case. The occurrences of β in $C \rightarrow D$ are only negative or strictly positive. By definition, the occurrences of β in C are only positive. Thus, by the IH, $\Gamma \vdash C[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, C[B/\beta]$. By definition, the occurrences of β in D are only negative or strictly positive. Thus, by the IH, $\Gamma \vdash \forall\, \alpha.\, D[B/\beta] \sqsubseteq D[\forall\, \alpha.\, B/\beta]$. By (C_Fun),

$$\Gamma \vdash (\forall\, \alpha.\, C[B/\beta]) \rightarrow \forall\, \alpha.\, D[B/\beta] \sqsubseteq C[\forall\, \alpha.\, B/\beta] \rightarrow D[\forall\, \alpha.\, B/\beta].$$

By (C_DFun) and (C_Trans),

$$\Gamma \vdash \forall\, \alpha.\, (\forall\, \alpha.\, C[B/\beta]) \rightarrow D[B/\beta] \sqsubseteq C[\forall\, \alpha.\, B/\beta] \rightarrow D[\forall\, \alpha.\, B/\beta]. \tag{1}$$

By (C_INST),

$$\Gamma, \alpha \vdash \forall\, \alpha.\, C[B/\beta] \sqsubseteq C[B/\beta]. \tag{2}$$

By (C_FUN) and (C_POLY) with (2),

$$\Gamma \vdash \forall\, \alpha.\, C[B/\beta] \rightarrow D[B/\beta] \sqsubseteq \forall\, \alpha.\, (\forall\, \alpha.\, C[B/\beta]) \rightarrow D[B/\beta].$$

Thus, by (C_TRANS) with (1),

$$\Gamma \vdash \forall\, \alpha.\, C[B/\beta] \rightarrow D[B/\beta] \sqsubseteq C[\forall\, \alpha.\, B/\beta] \rightarrow D[\forall\, \alpha.\, B/\beta].$$

Next, we prove the second case. The occurrences of β in $C \rightarrow D$ are only positive. By definition, the occurrences of β in C are only negative. Thus, by Lemma 26 (1), $\Gamma, \alpha \vdash C[B/\beta] \sqsubseteq C[\forall\, \alpha.\, B/\beta]$. By definition, the occurrences of β in D are only positive. Thus, by Lemma 26 (2), $\Gamma, \alpha \vdash D[\forall\, \alpha.\, B/\beta] \sqsubseteq D[B/\beta]$. By (C_FUN), (C_POLY), and (C_TRANS),

$$\Gamma \vdash \forall\, \alpha.\, C[\forall\, \alpha.\, B/\beta] \rightarrow D[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, C[B/\beta] \rightarrow D[B/\beta].$$

Since α does not appear free in $A = C \rightarrow D$, we have $\Gamma \vdash C[\forall\, \alpha.\, B/\beta] \rightarrow D[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, C[\forall\, \alpha.\, B/\beta] \rightarrow D[\forall\, \alpha.\, B/\beta]$ by (C_GEN). Thus, by (C_TRANS),

$$\Gamma \vdash C[\forall\, \alpha.\, B/\beta] \rightarrow D[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, C[B/\beta] \rightarrow D[B/\beta].$$

Case $A = \forall\, \gamma.\, C$: By the IH, (C_POLY), and permutation of the top-level $\forall$s for each case.

Case $A = C \times D$: We prove the first case. The occurrences of β in $C \times D$ are only negative or strictly positive. By definition, the occurrences of β in C are only negative or strictly positive. Thus, by the IH, $\Gamma \vdash \forall\, \alpha.\, C[B/\beta] \sqsubseteq C[\forall\, \alpha.\, B/\beta]$. Similarly, we also have $\Gamma \vdash \forall\, \alpha.\, D[B/\beta] \sqsubseteq D[\forall\, \alpha.\, B/\beta]$. By (C_PROD),

$$\Gamma \vdash (\forall\, \alpha.\, C[B/\beta]) \times \forall\, \alpha.\, D[B/\beta] \sqsubseteq C[\forall\, \alpha.\, B/\beta] \times D[\forall\, \alpha.\, B/\beta].$$

By (C_DPROD) and (C_TRANS),

$$\Gamma \vdash \forall\, \alpha.\, (C[B/\beta] \times D[B/\beta]) \sqsubseteq C[\forall\, \alpha.\, B/\beta] \times D[\forall\, \alpha.\, B/\beta].$$

We prove the second case. The occurrences of β in $C \times D$ are only positive. By definition, the occurrences of β in C are only positive. Thus, by the IH, $\Gamma \vdash C[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, C[B/\beta]$. Similarly, we also have $\Gamma \vdash D[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, D[B/\beta]$. By (C_PROD),

$$\Gamma \vdash C[\forall\, \alpha.\, B/\beta] \times D[\forall\, \alpha.\, B/\beta] \sqsubseteq (\forall\, \alpha.\, C[B/\beta]) \times \forall\, \alpha.\, D[B/\beta].$$

By (C_GEN), (C_POLY), (C_INST), (C_PROD), and (C_TRANS), we have $\Gamma \vdash (\forall\, \alpha.\, C[B/\beta]) \times \forall\, \alpha.\, D[B/\beta] \sqsubseteq \forall\, \alpha.\, (C[B/\beta] \times D[B/\beta])$. Thus, by (C_TRANS),

$$\Gamma \vdash C[\forall\, \alpha.\, B/\beta] \times D[\forall\, \alpha.\, B/\beta] \sqsubseteq \forall\, \alpha.\, (C[B/\beta] \times D[B/\beta]).$$

Case $A = C + D$: Similarly to the case that A is a product type; this case uses (C_SUM) and (C_DSUM) instead of (C_PROD) and (C_DPROD).

Case $A = C\ \mathsf{list}$: Similarly to the case that A is a product type; this case uses (C_LIST) and (C_DLIST) instead of (C_PROD) and (C_DPROD).

□

Lemma 28 (Subject reduction). *Suppose that all operations satisfy the signature restriction.*

1. *If $\Delta \vdash M_1 : A$ and $M_1 \rightsquigarrow M_2$, then $\Delta \vdash M_2 : A$.*
2. *If $\Delta \vdash M_1 : A$ and $M_1 \longrightarrow M_2$, then $\Delta \vdash M_2 : A$.*

Proof. 1. Suppose that $\Delta \vdash M_1 : A$ and $M_1 \rightsquigarrow M_2$. By induction on the typing derivation for M_1.

Case (T_VAR), (T_OP), (T_PAIR), (T_INL), (T_INR), and (T_CONS): Contradictory because there are no reduction rules that can be applied to M_1.

Case (T_CONST), (T_ABS), and (T_NIL): Contradictory since M_1 is a value and no reduction rules can be applied to values.

Case (T_APP): We have two reduction rules which can be applied to function applications.

Case (R_CONST): We are given

- $M_1 = c_1\, c_2$,
- $M_2 = \zeta(c_1, c_2)$,
- $\Delta \vdash c_1\, c_2 : A$,
- $\Delta \vdash c_1 : B \rightarrow A$, and
- $\Delta \vdash c_2 : B$

for some c_1, c_2, and B. By Lemma 11, $\Delta \vdash ty(c_1) \sqsubseteq B \rightarrow A$. By Lemma 6 and Assumption 1, $ty(c_1) = \iota \rightarrow C$ for some ι and C. Since $\zeta(c_1, c_2)$ is defined, it is found that $ty(c_2) = \iota$ and $ty(\zeta(c_1, c_2)) = C$. Since $\vdash \Delta$ by Lemma 13, we have $\Delta \vdash \zeta(c_1, c_2) : ty(\zeta(c_1, c_2))$. Since $\Delta \vdash \iota \rightarrow ty(\zeta(c_1, c_2)) \sqsubseteq B \rightarrow A$ (recall that $C = ty(\zeta(c_1, c_2))$), we have $\Delta \vdash ty(\zeta(c_1, c_2)) \sqsubseteq A$ by Lemma 10. By (T_INST), we have $\Delta \vdash \zeta(c_1, c_2) : A$.

Case (R_BETA): We are given

- $M_1 = (\lambda x.M)\, v$,
- $M_2 = M[v/x]$,
- $\Delta \vdash (\lambda x.M)\, v : A$,
- $\Delta \vdash \lambda x.M : B \rightarrow A$, and
- $\Delta \vdash v : B$

for some x, M, v, and B. By Lemma 14 $\Delta, \boldsymbol{\alpha}^I, x : B' \vdash M : A'$ and $\Delta \vdash \forall \boldsymbol{\alpha}^I. B' \rightarrow A' \sqsubseteq B \rightarrow A$ for some $\boldsymbol{\alpha}^I$, A', and B'. By Lemma 9, there exist $\boldsymbol{\alpha_1}^{I_1}$, $\boldsymbol{\alpha_2}^{I_2}$, $\boldsymbol{\beta}^J$, and $\boldsymbol{C}^{I_1}$ such that

- $\{\boldsymbol{\alpha}^I\} = \{\boldsymbol{\alpha_1}^{I_1}\} \uplus \{\boldsymbol{\alpha_2}^{I_2}\}$,
- $\Delta, \boldsymbol{\beta}^J \vdash \boldsymbol{C}^{I_1}$,
- $\Delta \vdash B \sqsubseteq \forall \boldsymbol{\beta}^J. B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$,
- $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq A$, and
- type variables in $\boldsymbol{\beta}^J$ do not appear free in A' and B'.

By Lemma 1, $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}^I, x : B' \vdash M : A'$ and $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2} \vdash \boldsymbol{C}^{I_1}$. Thus, by Lemma 2 (4),

$$\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2}, x : B'\,[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}^{I_1}] \vdash M : A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \tag{3}$$

Since $\Delta \vdash v : B$ and $\Delta \vdash B \sqsubseteq \forall \boldsymbol{\beta}^J. B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$, we have

$$\Delta \vdash v : \forall \boldsymbol{\beta}^J. B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$$

by (T_INST) (note that $\Delta \vdash \forall \boldsymbol{\beta}^J. B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$ is shown easily with Lemma 13). By Lemma 1 (4), (C_INST), and (T_INST), we have

$$\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2} \vdash v : B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}^{I_1}].$$

By Lemma 4 (1) with (3),

$$\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2} \vdash M[v/x] : A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}].$$

By (T_GEN) (with permutation of the bindings in the typing context),

$$\Delta \vdash M[v/x] : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}].$$

Since $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq A$, we have $\Delta \vdash M[v/x] : A$ by (T_INST).

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

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

Case (T_Handle): We have two reduction rules which can be applied to handle–with expressions.

Case (R_Return): We are given

- $M_1 = \mathsf{handle}\, v \,\mathsf{with}\, H$,
- $H^{\mathsf{return}} = \mathsf{return}\, x \rightarrow M$,
- $M_2 = M[v/x]$,
- $\Delta \vdash \mathsf{handle}\, v \,\mathsf{with}\, H : A$,
- $\Delta \vdash v : B$,
- $\Delta \vdash H : B \Rightarrow A$

for some v, H, x, M, and B. By inversion of the derivation of $\Delta \vdash H : B \Rightarrow A$, we have $\Delta, x : B \vdash M : A$. By Lemma 4 (1), $\Delta \vdash M[v/x] : A$, which is the conclusion we have to show.

Case (R_Handle): We are given

- $M_1 = \mathsf{handle}\, E[\#\mathsf{op}(v)] \,\mathsf{with}\, H$,
- $\mathsf{op} \notin E$,
- $H(\mathsf{op}) = \mathsf{op}(x, k) \rightarrow M$,
- $M_2 = M[v/x][\lambda y.\mathsf{handle}\, E[y] \,\mathsf{with}\, H/k]$,
- $\Delta \vdash \mathsf{handle}\, E[\#\mathsf{op}(v)] \,\mathsf{with}\, H : A$,
- $\Delta \vdash E[\#\mathsf{op}(v)] : B$,
- $\Delta \vdash H : B \Rightarrow A$

for some E, op, v, H, x, y, k, M, and B. Suppose that $ty\,(\mathsf{op}) = \forall \boldsymbol{\alpha}.\, C \hookrightarrow D$. By inversion of the derivation of $\Delta \vdash H : B \Rightarrow A$, we have $\Delta, \boldsymbol{\alpha}, x : C, k : D \rightarrow A \vdash M : A$.
By Lemma 22, $\Delta, \boldsymbol{\beta}^J \vdash \boldsymbol{C_0}$ and $\Delta, \boldsymbol{\beta}^J \vdash v : C[\boldsymbol{C_0}/\boldsymbol{\alpha}]$ for some $\boldsymbol{\beta}^J$ and $\boldsymbol{C_0}$. Since $\Delta \vdash \forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}$,

$$\Delta, x : C\,[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}], k : D[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow A \vdash M : A \tag{4}$$

by Lemma 2 (4) (note that type variables in $\boldsymbol{\alpha}$ do not appear free in A).
Since $\Delta, \boldsymbol{\beta}^J \vdash v : C[\boldsymbol{C_0}/\boldsymbol{\alpha}]$, we have $\Delta \vdash v : \forall \boldsymbol{\beta}^J.\, C[\boldsymbol{C_0}/\boldsymbol{\alpha}]$ by (T_Gen). By Definition 5, the occurrences of $\boldsymbol{\alpha}$ in the domain type C of the type signature of op are only negative or strictly positive. Thus, we have $\Delta \vdash v : C[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}]$ by Lemma 27 (1) and (T_Inst) (note that we can suppose that $\boldsymbol{\beta}^J$ do not appear free in C). Thus, by applying Lemma 4 (1) to (4), we have

$$\Delta, k : D[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow A \vdash M[v/x] : A. \tag{5}$$

We show that

$$\Delta \vdash \lambda y.\mathsf{handle}\, E[y] \,\mathsf{with}\, H : D[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow A.$$

By Definition 5, the occurrences of $\boldsymbol{\alpha}$ in the codomain type D of the type signature of op are only positive. Thus, we have $\Delta \vdash D[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \sqsubseteq \forall \boldsymbol{\beta}^J.\, D[\boldsymbol{C_0}/\boldsymbol{\alpha}]$ by Lemma 27 (2) (note that we can suppose that $\boldsymbol{\beta}^J$ do not appear free in D). Thus,

$$\Delta, y : D\,[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash y : \forall \boldsymbol{\beta}^J.\, D[\boldsymbol{C_0}/\boldsymbol{\alpha}]$$

by (T_Inst). By Lemma 1 (4) and (C_Inst),

$$\Delta, y : D\,[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}], \boldsymbol{\beta}^J \vdash y : D[\boldsymbol{C_0}/\boldsymbol{\alpha}].$$

By Lemma 22,

$$\Delta, y : \forall \boldsymbol{\beta}^J.\, D\,[\boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash E[y] : B.$$

By Lemma 21,

$$\Delta, y : D\,[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash E[y] : B.$$

Thus, we have

$$\Delta, y : D\,[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash \mathsf{handle}\, E[y] \,\mathsf{with}\, H : A$$

by Lemma 1 (5) and (T_Handle). By (T_Abs),

$$\Delta \vdash \lambda y.\mathsf{handle}\, E[y] \,\mathsf{with}\, H : D[\forall \boldsymbol{\beta}^J.\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow A.$$

By applying Lemma 4 (1) to (5), we have

$$\Delta \vdash M[v/x][\lambda y.\mathsf{handle}\ E[y]\ \mathsf{with}\ H/k] : A,$$

which is what we have to show.

Case (T_Proj1): We have one reduction rule (R_Proj1) which can be applied to projection π_1. Thus, we are given

- $M_1 = \pi_1(v_1, v_2)$,
- $M_2 = v_1$,
- $\Delta \vdash \pi_1(v_1, v_2) : A$,
- $\Delta \vdash (v_1, v_2) : A \times B$

for some v_1, v_2, and B. By Lemma 15, $\Delta, \boldsymbol{\alpha}^I \vdash v_1 : C_1$ and $\Delta, \boldsymbol{\alpha}^I \vdash v_2 : C_2$ and $\Delta \vdash \forall \boldsymbol{\alpha}^I.\, C_1 \times C_2 \sqsubseteq A \times B$ for some $\boldsymbol{\alpha}^I$, C_1, and C_2. By Lemma 23, there exist $\boldsymbol{\alpha_1}^{I_1}$, $\boldsymbol{\alpha_2}^{I_2}$, $\boldsymbol{\beta}^J$, and $\boldsymbol{D}^{I_1}$ such that

- $\{\boldsymbol{\alpha}^I\} = \{\boldsymbol{\alpha_1}^{I_1}\} \uplus \{\boldsymbol{\alpha_2}^{I_2}\}$,
- $\Delta, \boldsymbol{\beta}^J \vdash \boldsymbol{D}^{I_1}$,
- $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq A$,
- $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_2[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq B$, and
- type variables in $\boldsymbol{\beta}^J$ do not appear in C_1 and C_2.

We have to show that

$$\Delta \vdash v_1 : A.$$

Since $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq A$, it suffices to show that

$$\Delta \vdash v_1 : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$$

by (T_Inst). We have $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}^I \vdash v_1 : C_1$ by Lemma 1 (4). By Lemma 2 (4), we have $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2} \vdash v_1 : C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$. By (T_Gen) (and swapping $\boldsymbol{\beta}^J$ and $\boldsymbol{\alpha_2}^{I_2}$ in the typing context $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2}$), we have

$$\Delta \vdash v_1 : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}].$$

Case (T_Proj2): Similar to the case for (T_Proj1).

Case (T_Case): We have two reduction rules which can be applied to case expressions.

Case (R_CaseL): We are given

- $M_1 = \mathsf{case}\,(\mathsf{inl}\ v)\ \mathsf{of}\ \mathsf{inl}\ x \to M_1';\ \mathsf{inr}\ y \to M_2'$,
- $M_2 = M_1'[v/x]$,
- $\Delta \vdash \mathsf{case}\,(\mathsf{inl}\ v)\ \mathsf{of}\ \mathsf{inl}\ x \to M_1';\ \mathsf{inr}\ y \to M_2' : A$,
- $\Delta \vdash \mathsf{inl}\ v : B_1 + B_2$,
- $\Delta, x : B_1 \vdash M_1' : A$, and
- $\Delta, x : B_2 \vdash M_2' : A$

for some v, x, y, M_1',, M_2', B_1, and B_2. By Lemma 16, $\Delta, \boldsymbol{\alpha}^I \vdash v : C_1$ and $\Delta \vdash \forall \boldsymbol{\alpha}^I.\, C_1 + C_2 \sqsubseteq B_1 + B_2$ for some $\boldsymbol{\alpha}^I$, C_1, and C_2. By Lemma 24, there exist $\boldsymbol{\alpha_1}^{I_1}$, $\boldsymbol{\alpha_2}^{I_2}$, $\boldsymbol{\beta}^J$, and $\boldsymbol{D}^{I_1}$ such that

- $\{\boldsymbol{\alpha}^I\} = \{\boldsymbol{\alpha_1}^{I_1}\} \uplus \{\boldsymbol{\alpha_2}^{I_2}\}$,
- $\Delta, \boldsymbol{\beta}^J \vdash \boldsymbol{D}^{I_1}$,
- $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq B_1$,
- $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_2[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq B_2$, and
- type variables in $\boldsymbol{\beta}^J$ do not appear in C_1 and C_2.

We first show that

$$\Delta \vdash v : B_1.$$

Since $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq B_1$, it suffices to show that

$$\Delta \vdash v : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$$

by (T_INST). We have $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}^I \vdash v_1 : C_1$ by Lemma 1 (4). By Lemma 2 (4), we have $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2} \vdash v_1 : C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]$. By (T_GEN) (and swapping $\boldsymbol{\beta}^J$ and $\boldsymbol{\alpha_2}^{I_2}$ in the typing context $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2}$), we have

$$\Delta \vdash v_1 : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C_1[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}].$$

Since $\Delta, x : B_1 \vdash M_1' : A$, we have

$$\Delta \vdash M_1'[v/x] : A$$

by Lemma 4 (1).

Case (R_CASER): Similar to the case for (R_CASER), using Lemma 17 instead of Lemma 16.

Case (T_CASELIST): We have two reduction rules which can be applied to case expressions for lists.

Case (R_NIL): Obvious.

Case (R_CONS): We are given

- $M_1 = \mathsf{case}\,(\mathsf{cons}\,v)\;\mathsf{of}\;\mathsf{nil} \rightarrow M_1';\,\mathsf{cons}\,x \rightarrow M_2'$,
- $M_2 = M_2'[v/x]$,
- $\Delta \vdash \mathsf{case}\,(\mathsf{cons}\,v)\;\mathsf{of}\;\mathsf{nil} \rightarrow M_1';\,\mathsf{cons}\,y \rightarrow M_2' : A$,
- $\Delta \vdash \mathsf{cons}\,v : B\;\mathsf{list}$, and
- $\Delta, x : B \times B\;\mathsf{list} \vdash M_2' : A$

for some v, x, M_1',, M_2', and B. By Lemma 18, $\Delta, \boldsymbol{\alpha}^I \vdash v : C \times C\;\mathsf{list}$ and $\Delta \vdash \forall \boldsymbol{\alpha}^I. C\;\mathsf{list} \sqsubseteq B\;\mathsf{list}$ for some $\boldsymbol{\alpha}^I$ and C. By Lemma 25, there exist $\boldsymbol{\alpha_1}^{I_1}$, $\boldsymbol{\alpha_2}^{I_2}$, $\boldsymbol{\beta}^J$, and $\boldsymbol{D}^{I_1}$ such that

- $\{\boldsymbol{\alpha}^I\} = \{\boldsymbol{\alpha_1}^{I_1}\} \uplus \{\boldsymbol{\alpha_2}^{I_2}\}$,
- $\Delta, \boldsymbol{\beta}^J \vdash \boldsymbol{D}^{I_1}$,
- $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq B$, and
- type variables in $\boldsymbol{\beta}^J$ do not appear in C.

We first show that

$$\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \times C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\;\mathsf{list} \sqsubseteq B \times B\;\mathsf{list}.$$

Since $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq B$, we have

$$\Delta \vdash (\forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}])\;\mathsf{list} \sqsubseteq B\;\mathsf{list}$$

by (C_LIST). We also have

$$\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\;\mathsf{list} \sqsubseteq (\forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}])\;\mathsf{list}$$

by (C_DLIST). Thus, by (C_TRANS), we have

$$\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\;\mathsf{list} \sqsubseteq B\;\mathsf{list}.$$

By (C_PROD),

$$\Delta \vdash (\forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]) \times (\forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\;\mathsf{list}) \sqsubseteq B \times B\;\mathsf{list}.$$

By (C_DPROD) and (C_TRANS), we have

$$\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \times C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\;\mathsf{list} \sqsubseteq B \times B\;\mathsf{list} \tag{6}$$

Next, we show that

$$\Delta \vdash v : B \times B\;\mathsf{list}.$$

By (T_INST) with (6), it suffices to show that

$$\Delta \vdash v : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \times C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\;\mathsf{list}.$$

We have $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}^I \vdash v : C \times C\, \mathsf{list}$ by Lemma 1 (4). By Lemma 2 (4), we have $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2} \vdash v : C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \times C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\, \mathsf{list}$. By (T_Gen) (and swapping $\boldsymbol{\beta}^J$ and $\boldsymbol{\alpha_2}^{I_2}$ in the typing context $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2}$), we have

$$\Delta \vdash v : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J.\, C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \times C[\boldsymbol{D}^{I_1}/\boldsymbol{\alpha_1}^{I_1}]\, \mathsf{list}.$$

Since $\Delta, x : B \times B\, \mathsf{list} \vdash M'_2 : A$, we have

$$\Delta \vdash M'_2[v/x] : A$$

by Lemma 4 (1).

Case (T_Fix): We have one reduction rule (R_Fix) which can be applied to the fixed-point operator. The proof is straightforward with Lemma 4 (1) and (T_Abs).

2. Suppose that $\Delta \vdash M_1 : A$ and $M_1 \longrightarrow M_2$. By definition, there exist some E, M'_1, and M'_2 such that $M_1 = E[M'_1]$, $M_2 = E[M'_2]$, and $M'_1 \rightsquigarrow M'_2$. The proof proceeds by induction on the typing derivation of for $M_1 = E[M'_1]$. If $E = []$, then we have the conclusion by the first case. In what follows, we suppose that $E \neq []$. By case analysis on the typing rule applied last to derive $\Delta \vdash E[M'_1] : A$.

Case (T_Var), (T_Const), (T_Abs), (T_Nil), and (T_Fix): Contradictory because E has to be $[]$.

Case (T_App): By case analysis on E.

Case $E = E'\, M$: We are given

- $\Delta \vdash E'[M'_1] : B \rightarrow A$ and
- $\Delta \vdash M : B$

for some B. By the IH, $\Delta \vdash E'[M'_2] : B \rightarrow A$. Since $M_2 = E'[M'_2]\, M$, we have the conclusion by (T_App).

Case $E = v\, E'$: By the IH.

Case (T_Gen): By the IH.

Case (T_Inst): By the IH.

Case (T_Op): By the IH.

Case (T_Handle): By the IH.

Case (T_Pair): By the IH.

Case (T_Proj1): By the IH.

Case (T_Proj2): By the IH.

Case (T_InL): By the IH.

Case (T_InR): By the IH.

Case (T_Case): By the IH.

Case (T_Cons): By the IH.

Case (T_CaseList): By the IH.

□

Theorem 1 (Type Soundness)**.** *Suppose that all operations satisfy the signature restriction. If $\Delta \vdash M : A$ and $M \longrightarrow^* M'$ and $M' \not\longrightarrow$, then:*

- *M' is a value; or*
- *$M' = E[\#\mathsf{op}(v)]$ for some E, op, and v such that $\mathsf{op} \notin E$.*

Proof. By Lemmas 28 and 12. □

2.2 Soundness of the Type-and-effect System

This section show soundness of the type-and-effect system. We may reuse the lemmas proven in Section 2.1 if their statements and proofs do not need change.

Lemma 29 (Weakening)**.** *Suppose that* $\vdash \Gamma_1, \Gamma_2$*. Let* Γ_3 *be a typing context such that* $dom(\Gamma_2) \cap dom(\Gamma_3) = \emptyset$*.*

1. *If* $\vdash \Gamma_1, \Gamma_3$*, then* $\vdash \Gamma_1, \Gamma_2, \Gamma_3$*.*
2. *If* $\Gamma_1, \Gamma_3 \vdash A$*, then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash A$*.*
3. *If* $\Gamma_1, \Gamma_3 \vdash A \sqsubseteq B$*, then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash A \sqsubseteq B$*.*
4. *If* $\Gamma_1, \Gamma_3 \vdash M : A \,|\, \epsilon$*, then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash M : A \,|\, \epsilon$*.*
5. *If* $\Gamma_1, \Gamma_3 \vdash H : A \,|\, \epsilon \Rightarrow B \,|\, \epsilon'$*, then* $\Gamma_1, \Gamma_2, \Gamma_3 \vdash H : A \,|\, \epsilon \Rightarrow B \,|\, \epsilon'$*.*

Proof. By (mutual) induction on the derivations of the judgments. □

Lemma 30 (Type substitution)**.** *Suppose that* $\Gamma_1 \vdash A$*.*

1. *If* $\vdash \Gamma_1, \alpha, \Gamma_2$*, then* $\vdash \Gamma_1, \Gamma_2\,[A/\alpha]$*.*
2. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash B$*, then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash B[A/\alpha]$*.*
3. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash B \sqsubseteq C$*, then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash B[A/\alpha] \sqsubseteq C[A/\alpha]$*.*
4. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash M : B \,|\, \epsilon$*, then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash M : B[A/\alpha] \,|\, \epsilon$*.*
5. *If* $\Gamma_1, \alpha, \Gamma_2 \vdash H : B \,|\, \epsilon \Rightarrow C \,|\, \epsilon'$*, then* $\Gamma_1, \Gamma_2\,[A/\alpha] \vdash H : B[A/\alpha] \,|\, \epsilon \Rightarrow C[A/\alpha] \,|\, \epsilon'$*.*

Proof. Straightforward by (mutual) induction on the derivations of the judgments, as in Lemma 2. □

Lemma 31 (Term substitution)**.** *Suppose that* $\Gamma_1 \vdash M : A \,|\, \epsilon$ *for any* ϵ*.*

1. *If* $\Gamma_1, x\!:\!A, \Gamma_2 \vdash M' : B \,|\, \epsilon$*, then* $\Gamma_1, \Gamma_2 \vdash M'[M/x] : B \,|\, \epsilon$*.*
2. *If* $\Gamma_1, x\!:\!A, \Gamma_2 \vdash H : B \,|\, \epsilon \Rightarrow C \,|\, \epsilon'$*, then* $\Gamma_1, \Gamma_2 \vdash H[M/x] : B \,|\, \epsilon \Rightarrow C \,|\, \epsilon'$*.*

Proof. By mutual induction on the typing derivations as in Lemma 4. □

Lemma 32 (Canonical forms)**.** *Suppose that* $\Gamma \vdash v : A \,|\, \epsilon$*.*

1. *If* $unqualify(A) = \iota$*, then* $v = c$ *for some* c*.*
2. *If* $unqualify(A) = B \rightarrow^{\epsilon'} C$*, then* $v = c$ *for some* c*, or* $v = \lambda x.M$ *for some* x *and* M*.*
3. *If* $unqualify(A) = B \times C$*, then* $v = (v_1, v_2)$ *for some* v_1 *and* v_2*.*
4. *If* $unqualify(A) = B + C$*, then* $v = \mathsf{inl}\, v'$ *or* $v = \mathsf{inr}\, v'$ *for some* v'*.*
5. *If* $unqualify(A) = B\,\mathsf{list}$*, then* $v = \mathsf{nil}$ *or* $v = \mathsf{cons}\, v'$ *for some* v'*.*

Proof. Similarly to Lemma 8. □

Lemma 33 (Type containment inversion: function types)**.** *If* $\Gamma \vdash \forall \boldsymbol{\alpha}_{\mathbf{1}}^{I_1}.\, A_1 \rightarrow^{\epsilon_1} A_2 \sqsubseteq \forall \boldsymbol{\alpha}_{\mathbf{2}}^{I_2}.\, B_1 \rightarrow^{\epsilon_2} B_2$*, then* $\epsilon_1 = \epsilon_2$ *and there exist* $\boldsymbol{\alpha}_{\mathbf{11}}^{I_{11}}$*,* $\boldsymbol{\alpha}_{\mathbf{12}}^{I_{12}}$*,* $\boldsymbol{\beta}^{J}$*, and* $\boldsymbol{C}^{I_{11}}$ *such that*

- $\{\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}\} = \{\boldsymbol{\alpha}_{\mathbf{11}}^{I_{11}}\} \uplus \{\boldsymbol{\alpha}_{\mathbf{12}}^{I_{12}}\}$,
- $\Gamma, \boldsymbol{\alpha}_{\mathbf{2}}^{I_2}, \boldsymbol{\beta}^{J} \vdash \boldsymbol{C}^{I_{11}}$,
- $\Gamma, \boldsymbol{\alpha}_{\mathbf{2}}^{I_2} \vdash B_1 \sqsubseteq \forall \boldsymbol{\beta}^{J}.\, A_1[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha}_{\mathbf{11}}^{I_{11}}]$,
- $\Gamma, \boldsymbol{\alpha}_{\mathbf{2}}^{I_2} \vdash \forall \boldsymbol{\alpha}_{\mathbf{12}}^{I_{12}}.\, \forall \boldsymbol{\beta}^{J}.\, A_2[\boldsymbol{C}^{I_{11}}/\boldsymbol{\alpha}_{\mathbf{11}}^{I_{11}}] \sqsubseteq B_2$,

- *type variables in* $\{\boldsymbol{\beta}^J\}$ *do not appear free in* A_1 *and* A_2*, and*
- *if* $\boldsymbol{\alpha}_{\mathbf{12}}^{I_{12}}$ *or* $\boldsymbol{\beta}^J$ *is not the empty sequence,* $SR(\epsilon_1)$*.*

Proof. Similarly to Lemma 9. ☐

Lemma 34. *If* $\Gamma \vdash A_1 \rightarrow^{\epsilon_1} A_2 \sqsubseteq B_1 \rightarrow^{\epsilon_2} B_2$*, then* $\epsilon_1 = \epsilon_2$ *and* $\Gamma \vdash B_1 \sqsubseteq A_1$ *and* $\Gamma \vdash A_2 \sqsubseteq B_2$*.*

Proof. Similarly to Lemma 10 with Lemma 33. ☐

Lemma 35 (Value inversion: constants)**.** *If* $\Gamma \vdash c : A \,|\, \epsilon$*, then* $\Gamma \vdash ty(c) \sqsubseteq A$*.*

Proof. Similarly to Lemma 11. ☐

Lemma 36 (Progress)**.** *If* $\Delta \vdash M : A \,|\, \epsilon$*, then:*

- $M \longrightarrow M'$ *for some* M'*;*
- M *is a value; or*
- $M = E[\#\mathsf{op}(v)]$ *for some* E*,* op*, and* v *such that* $\mathsf{op} \notin E$ *and* $\mathsf{op} \in \epsilon$*.*

Proof. Similarly to Lemma 12 with the lemmas proven in this section. The case for (Te_Weak) is also straightforward. ☐

Lemma 37 (Value inversion: lambda abstractions)**.** *If* $\Gamma \vdash \lambda x.M : A \,|\, \epsilon$*, then* $\Gamma, \boldsymbol{\alpha}, x\!:\!B \vdash M : C \,|\, \epsilon'$ *and* $\Gamma \vdash \forall \boldsymbol{\alpha}. B \rightarrow^{\epsilon'} C \sqsubseteq A$ *for some* $\boldsymbol{\alpha}$*,* B*,* C*, and* ϵ'*.*

Proof. Similarly to Lemma 14. ☐

Lemma 38 (Value inversion: pairs)**.** *If* $\Gamma \vdash (M_1, M_2) : A \,|\, \epsilon$*, then* $\Gamma, \boldsymbol{\alpha} \vdash M_1 : B_1 \,|\, \epsilon$ *and* $\Gamma, \boldsymbol{\alpha} \vdash M_2 : B_2 \,|\, \epsilon$ *and* $\Gamma \vdash \forall \boldsymbol{\alpha}. B_1 \times B_2 \sqsubseteq A$ *for some* $\boldsymbol{\alpha}$*,* B_1*, and* B_2*.*

Proof. Similarly to Lemma 15. ☐

Lemma 39 (Value inversion: left injections)**.** *If* $\Gamma \vdash \mathsf{inl}\, M : A \,|\, \epsilon$*, then* $\Gamma, \boldsymbol{\alpha} \vdash M : B \,|\, \epsilon$ *and* $\Gamma \vdash \forall \boldsymbol{\alpha}. B + C \sqsubseteq A$ *for some* $\boldsymbol{\alpha}$*,* B*, and* C*.*

Proof. Similarly to Lemma 16. ☐

Lemma 40 (Value inversion: right injections)**.** *If* $\Gamma \vdash \mathsf{inr}\, M : A \,|\, \epsilon$*, then* $\Gamma, \boldsymbol{\alpha} \vdash M : C \,|\, \epsilon$ *and* $\Gamma \vdash \forall \boldsymbol{\alpha}. B + C \sqsubseteq A$ *for some* $\boldsymbol{\alpha}$*,* B*, and* C*.*

Proof. Similarly to the proof of Lemma 17. ☐

Lemma 41 (Value inversion: cons)**.** *If* $\Gamma \vdash \mathsf{cons}\, M : A \,|\, \epsilon$*, then* $\Gamma, \boldsymbol{\alpha} \vdash M : B \times B\,\mathsf{list} \,|\, \epsilon$ *and* $\Gamma \vdash \forall \boldsymbol{\alpha}. B\,\mathsf{list} \sqsubseteq A$ *for some* $\boldsymbol{\alpha}$ *and* B*.*

Proof. Similarly to Lemma 18. ☐

Lemma 42. *If* $ty(\mathsf{op}) = \forall \boldsymbol{\alpha}^I. A \hookrightarrow B$ *and* $\Gamma \vdash \#\mathsf{op}(v) : C \,|\, \epsilon$*, then*

- $\Gamma, \boldsymbol{\beta}^J \vdash \boldsymbol{D}^I$*,*
- $\Gamma, \boldsymbol{\beta}^J \vdash v : A[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \,|\, \epsilon'$*,*
- $\epsilon' \subseteq \epsilon$*,*
- $\mathsf{op} \in \epsilon'$*, and*
- $\Gamma \vdash \forall \boldsymbol{\beta}^J. B[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \sqsubseteq C$*; or*

for some $\boldsymbol{\beta}^J$*,* $\boldsymbol{D}^I$*, and* ϵ'*. Furthermore, if* $\boldsymbol{\beta}^J$ *is not the empty sequence,* $SR(\epsilon')$ *holds.*

Proof. By induction on the typing derivation. There are only five typing rules that can be applied to $\#\mathsf{op}(v)$.

Case (TE_GEN): Straightforward by the IH. Note that $SR(\epsilon)$ by inversion.

Case (TE_INST): Straightforward by the IH and (C_TRANS).

Case (TE_OP): Trivial.

Case (TE_WEAK): By the IH.

$\square$

Lemma 43. *If* $\Gamma, \boldsymbol{\alpha}^I \vdash E[\#\mathsf{op}(v)] : A \mid \epsilon$ *and* $\mathsf{op} \notin E$*, then*

- $\Gamma, \boldsymbol{\alpha}^I, \boldsymbol{\beta}^J \vdash \#\mathsf{op}(v) : B \mid \epsilon'$ *and*
- $\Gamma, y : \forall \boldsymbol{\alpha}^I . \forall \boldsymbol{\beta}^J . B, \boldsymbol{\alpha}^I \vdash E[y] : A \mid \epsilon$ *for any* $y \notin dom(\Gamma)$*, and*
- $\mathsf{op} \in \epsilon$

for some $\boldsymbol{\beta}^J$*,* B*, and* ϵ'*. Furthermore, if* $\boldsymbol{\beta}^J$ *is not the empty sequence, then* $SR(\{\mathsf{op}\})$ *holds.*

Proof. By induction on the typing derivation.

Case (TE_VAR), (TE_CONST), (TE_ABS), (TE_NIL), and (TE_FIX): Contradictory.

Case (TE_APP): By case analysis on E.

Case $E = E' M_2$: By inversion of the typing derivation, we have $\Gamma, \boldsymbol{\alpha}^I \vdash E'[\#\mathsf{op}(v)] : C \to^{\epsilon''} A \mid \epsilon$ and $\Gamma, \boldsymbol{\alpha}^I \vdash M_2 : C \mid \epsilon$ and $\epsilon'' \subseteq \epsilon$ for some C and ϵ''. By the IH,

- $\Gamma, \boldsymbol{\alpha}^I, \boldsymbol{\beta}^J \vdash \#\mathsf{op}(v) : B \mid \epsilon'$,
- $\Gamma, y : \forall \boldsymbol{\alpha}^I . \forall \boldsymbol{\beta}^J . B, \boldsymbol{\alpha}^I \vdash E'[y] : C \to^{\epsilon''} A \mid \epsilon$ for any $y \notin dom(\Gamma)$, and
- $\mathsf{op} \in \epsilon$,
- If $\boldsymbol{\beta}^J$ is not the empty sequence, then $SR(\{\mathsf{op}\})$ holds.

for some $\boldsymbol{\beta}^J$, B, and ϵ'. By Lemma 29 (4) and (TE_APP), $\Gamma, y : \forall \boldsymbol{\alpha}^I . \forall \boldsymbol{\beta}^J . B, \boldsymbol{\alpha}^I \vdash E'[y] M_2 : A \mid \epsilon$, i.e., $\Gamma, y : \forall \boldsymbol{\alpha}^I . \forall \boldsymbol{\beta}^J . B, \boldsymbol{\alpha}^I \vdash E[y] : A \mid \epsilon$.

Case $E = v_1 E'$: Similarly to the above case.

Case (TE_GEN): By the IH. We find $SR(\{\mathsf{op}\})$ by $\mathsf{op} \in \epsilon$ and $SR(\epsilon)$.

Case (TE_INST): By the IH.

Case (TE_OP): If $E = []$, the proof is straightforward by letting $\boldsymbol{\beta}^J$ be the empty sequence, $B = A$, and $\epsilon' = \epsilon$; $\mathsf{op} \in \epsilon$ is found by Lemma 42.

Otherwise, the proof is similar to the case for (TE_APP).

Case (TE_HANDLE): By the IH. We find $\mathsf{op} \in \epsilon$ because the handler does not have an operation clause for op ($\mathsf{op} \notin E$).

Case (TE_WEAK): By the IH.

Otherwise: Similarly to the case for (TE_APP).

$\square$

Lemma 44. *Suppose that* $\Gamma_1 \vdash A \sqsubseteq B$ *and* $\Gamma_1 \vdash A$*.*

1. *If* $\Gamma_1, x : B, \Gamma_2 \vdash M : C \mid \epsilon$*, then* $\Gamma_1, x : A, \Gamma_2 \vdash M : C \mid \epsilon$*.*
2. *If* $\Gamma_1, x : B, \Gamma_2 \vdash H : C \mid \epsilon \Rightarrow D \mid \epsilon'$*, then* $\Gamma_1, x : A, \Gamma_2 \vdash H : C \mid \epsilon \Rightarrow D \mid \epsilon'$*.*

Proof. By mutual induction on the typing derivations. $\square$

Lemma 45. *If* $ty(\mathsf{op}) = \forall \boldsymbol{\alpha}^I . A \hookrightarrow B$ *and* $\Gamma \vdash E[\#\mathsf{op}(v)] : C \mid \epsilon$ *and* $\mathsf{op} \notin E$*, then*

- $\Gamma, \boldsymbol{\beta}^J \vdash \boldsymbol{D}^I$,
- $\Gamma, \boldsymbol{\beta}^J \vdash v : A[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \,|\, \epsilon'$, *and*
- *for any* $y \notin \mathit{dom}(\Gamma)$, $\Gamma, y : \forall \boldsymbol{\beta}^J.\, B\,[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \vdash E[y] : C \,|\, \epsilon$

for some $\boldsymbol{\beta}^J$, $\boldsymbol{D}^I$, *and* ϵ'. *Furthermore, if* $\boldsymbol{\beta}^J$ *is not the empty sequence,* $\mathit{SR}\,(\{\mathsf{op}\})$ *holds.*

Proof. By Lemma 43,

- $\Gamma, \boldsymbol{\beta_1}^{J_1} \vdash \#\mathsf{op}(v) : C' \,|\, \epsilon''$ and
- $\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1}.\, C' \vdash E[y] : C \,|\, \epsilon$ for any $y \notin \mathit{dom}(\Gamma)$, and
- if $\boldsymbol{\beta_1}^{J_1}$ is not the empty sequence, then $\mathit{SR}\,(\{\mathsf{op}\})$ holds

for some $\boldsymbol{\beta_1}^{J_1}$ and C'. By Lemma 42,

- $\Gamma, \boldsymbol{\beta_1}^{J_1}, \boldsymbol{\beta_2}^{J_2} \vdash \boldsymbol{D}^I$,
- $\Gamma, \boldsymbol{\beta_1}^{J_1}, \boldsymbol{\beta_2}^{J_2} \vdash v : A[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \,|\, \epsilon'$,
- $\Gamma, \boldsymbol{\beta_1}^{J_1} \vdash \forall \boldsymbol{\beta_2}^{J_2}.\, B[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \sqsubseteq C'$, and
- if $\boldsymbol{\beta_2}^{J_2}$ is not the empty sequence, $\mathit{SR}\,(\{\mathsf{op}\})$ holds

for some $\boldsymbol{\beta_2}^{J_2}$, $\boldsymbol{D}^I$, and ϵ'.

We show the conclusion by letting $\boldsymbol{\beta}^J = \boldsymbol{\beta_1}^{J_1}, \boldsymbol{\beta_2}^{J_2}$. It suffices to show that, for any $y \notin \mathit{dom}(\Gamma)$,

$$\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1}.\, \forall \boldsymbol{\beta_2}^{J_2}.\, B\,[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \vdash E[y] : C \,|\, \epsilon.$$

Since $\Gamma, \boldsymbol{\beta_1}^{J_1} \vdash \forall \boldsymbol{\beta_2}^{J_2}.\, B[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \sqsubseteq C'$, we have

$$\Gamma \vdash \forall \boldsymbol{\beta_1}^{J_1}.\, \forall \boldsymbol{\beta_2}^{J_2}.\, B[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \sqsubseteq \forall \boldsymbol{\beta_1}^{J_1}.\, C'$$

by (C_Poly). Since $\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1}.\, C' \vdash E[y] : C \,|\, \epsilon$, we have

$$\Gamma, y : \forall \boldsymbol{\beta_1}^{J_1}.\, \forall \boldsymbol{\beta_2}^{J_2}.\, B\,[\boldsymbol{D}^I/\boldsymbol{\alpha}^I] \vdash E[y] : C \,|\, \epsilon.$$

by Lemma 44. ◻

Lemma 46. *If* $\Gamma \vdash v : A \,|\, \epsilon$, *then* $\Gamma \vdash v : A \,|\, \epsilon'$ *for any* ϵ'.

Proof. Straightforward by induction on the typing derivation. ◻

Lemma 47. *Suppose that* α *does not appear free in* A.

1. *Suppose that (1) the occurrences of* β *in* A *are only negative or strictly positive and (2) for any function type* $C \rightarrow^{\epsilon} D$ *occurring at a strictly positive position of* A, *if* $\beta \in \mathit{ftv}(D)$, *then* $\mathit{SR}\,(\epsilon)$. *Then* $\Gamma \vdash \forall \alpha.\, A[B/\beta] \sqsubseteq A[\forall \alpha.\, B/\beta]$.
2. *If the occurrences of* β *in* A *are only positive, then* $\Gamma \vdash A[\forall \alpha.\, B/\beta] \sqsubseteq \forall \alpha.\, A[B/\beta]$.

Proof. By induction on A. The second case is proven by Lemma 26, (C_Poly), (C_Gen), and (C_Trans).

Let us consider the second case. We consider the case that $A = C \rightarrow^{\epsilon} D$ for some C, D, and ϵ; the other cases are shown similarly to Lemma 27. By the IH on C, $\Gamma \vdash C[\forall \alpha.\, B/\beta] \sqsubseteq \forall \alpha.\, C[B/\beta]$.

Now, we show that

$$\Gamma \vdash \forall \alpha.\, (\forall \alpha.\, C[B/\beta]) \rightarrow^{\epsilon} D[B/\beta] \sqsubseteq C[\forall \alpha.\, B/\beta] \rightarrow^{\epsilon} D[\forall \alpha.\, B/\beta]. \tag{7}$$

If $\beta \in \mathit{ftv}(D)$, then $\mathit{SR}\,(\epsilon)$ by the assumption. By the IH on D, $\Gamma \vdash \forall \alpha.\, D[B/\beta] \sqsubseteq D[\forall \alpha.\, B/\beta]$. By (C_FunEff),

$$\Gamma \vdash (\forall \alpha.\, C[B/\beta]) \rightarrow^{\epsilon} \forall \alpha.\, D[B/\beta] \sqsubseteq C[\forall \alpha.\, B/\beta] \rightarrow^{\epsilon} D[\forall \alpha.\, B/\beta].$$

Since $SR(\epsilon)$, we have (7) by (C_DFunEff) and (C_Trans). Otherwise, if $\beta \not\in ftv(D)$, then $\Gamma, \alpha \vdash D[B/\beta] \sqsubseteq D[\forall\, \alpha.\, B/\beta]$ by (C_Refl) because $D[B/\beta] = D[\forall\, \alpha.\, B/\beta] = D$. Thus,

$$\Gamma \vdash \forall\, \alpha.\, (\forall\, \alpha.\, C[B/\beta]) \rightarrow^{\epsilon} D[B/\beta] \sqsubseteq \forall\, \alpha.\, C[\forall\, \alpha.\, B/\beta] \rightarrow^{\epsilon} D[\forall\, \alpha.\, B/\beta]$$

by (C_Poly) and Lemma 29 (3). Since α does not occur in $A = C \rightarrow^{\epsilon} D$, we can have (7) by eliminating the outermost $\forall$ on the RHS type with (C_Inst).

By (C_Inst),

$$\Gamma, \alpha \vdash \forall\, \alpha.\, C[B/\beta] \sqsubseteq C[B/\beta]. \tag{8}$$

By (C_FunEff) and (C_Poly) with (8),

$$\Gamma \vdash \forall\, \alpha.\, C[B/\beta] \rightarrow^{\epsilon} D[B/\beta] \sqsubseteq \forall\, \alpha.\, (\forall\, \alpha.\, C[B/\beta]) \rightarrow^{\epsilon} D[B/\beta].$$

Thus, by (C_Trans) with (7),

$$\Gamma \vdash \forall\, \alpha.\, C[B/\beta] \rightarrow^{\epsilon} D[B/\beta] \sqsubseteq C[\forall\, \alpha.\, B/\beta] \rightarrow^{\epsilon} D[\forall\, \alpha.\, B/\beta].$$

□

Lemma 48 (Subject reduction)**.**

1. *If $\Delta \vdash M_1 : A \,|\, \epsilon$ and $M_1 \rightsquigarrow M_2$, then $\Delta \vdash M_2 : A \,|\, \epsilon$.*
2. *If $\Delta \vdash M_1 : A \,|\, \epsilon$ and $M_1 \longrightarrow M_2$, then $\Delta \vdash M_2 : A \,|\, \epsilon$.*

Proof. 1. By induction on the typing derivation. Most of the cases are similar to Lemma 28. We here focus on the cases that need a treatment specific to the type-and-effect system.

Case (Te_App)/(R_Beta): We are given

- $M_1 \,=\, (\lambda x.M)\, v$,
- $M_2 \,=\, M[v/x]$,
- $\Delta \vdash (\lambda x.M)\, v : A \,|\, \epsilon$,
- $\Delta \vdash \lambda x.M : B \rightarrow^{\epsilon_0} A \,|\, \epsilon$,
- $\Delta \vdash v : B \,|\, \epsilon$, and
- $\epsilon_0 \subseteq \epsilon$

for some x, M, v, B, and ϵ_0. By Lemma 37 $\Delta, \boldsymbol{\alpha}^I, x\!:\!B' \vdash M : A' \,|\, \epsilon'$ and $\Delta \vdash \forall\, \boldsymbol{\alpha}^I.\, B' \rightarrow^{\epsilon'} A' \sqsubseteq B \rightarrow^{\epsilon_0} A$ for some $\boldsymbol{\alpha}^I$, A', B', and ϵ'. By Lemma 33, we find $\epsilon' = \epsilon_0$, and there exist $\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}$, $\boldsymbol{\alpha}_{\mathbf{2}}^{I_2}$, $\boldsymbol{\beta}^J$, and $\boldsymbol{C}^{I_1}$ such that

- $\{\boldsymbol{\alpha}^I\} \,=\, \{\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}\} \uplus \{\boldsymbol{\alpha}_{\mathbf{2}}^{I_2}\}$,
- $\Delta, \boldsymbol{\beta}^J \vdash \boldsymbol{C}^{I_1}$,
- $\Delta \vdash B \sqsubseteq \forall\, \boldsymbol{\beta}^J.\, B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}]$,
- $\Delta \vdash \forall\, \boldsymbol{\alpha}_{\mathbf{2}}^{I_2}.\forall\, \boldsymbol{\beta}^J.\, A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}] \sqsubseteq A$, and
- type variables in $\boldsymbol{\beta}^J$ do not appear free in A' and B', and
- If $\boldsymbol{\alpha}_{\mathbf{2}}^{I_2}$ or $\boldsymbol{\beta}^J$ is not the empty sequence, $SR(\epsilon_0)$.

By Lemma 29, $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}^I, x\!:\!B' \vdash M : A' \,|\, \epsilon'$ and $\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}_{\mathbf{2}}^{I_2} \vdash \boldsymbol{C}^{I_1}$. Thus, by Lemma 30 (4),

$$\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}_{\mathbf{2}}^{I_2}, x\!:\!B'\,[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}^{I_1}] \vdash M : A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}] \,|\, \epsilon' \tag{9}$$

Since $\Delta \vdash v : B \,|\, \epsilon$ and $\Delta \vdash B \sqsubseteq \forall\, \boldsymbol{\beta}^J.\, B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}]$, we have

$$\Delta \vdash v : \forall\, \boldsymbol{\beta}^J.\, B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}] \,|\, \epsilon$$

by (Te_Inst) (note that $\Delta \vdash \forall\, \boldsymbol{\beta}^J.\, B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}_{\mathbf{1}}^{I_1}]$ is shown easily with Lemma 13). By Lemma 29 (4), (C_Inst), and (Te_Inst), we have

$$\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha}_{\mathbf{2}}^{I_2} \vdash v : B'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha}^{I_1}] \,|\, \epsilon.$$

By Lemmas 46 and 31 (1) with (9),

$$\Delta, \boldsymbol{\beta}^J, \boldsymbol{\alpha_2}^{I_2} \vdash M[v/x] : A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \,|\, \epsilon'.$$

By (TE_Gen) (with permutation of the bindings in the typing context),

$$\Delta \vdash M[v/x] : \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \,|\, \epsilon'$$

(note that If $\boldsymbol{\alpha_2}^{I_2}$ or $\boldsymbol{\beta}^J$ is not the empty sequence, $SR(\epsilon')$). Since $\Delta \vdash \forall \boldsymbol{\alpha_2}^{I_2}. \forall \boldsymbol{\beta}^J. A'[\boldsymbol{C}^{I_1}/\boldsymbol{\alpha_1}^{I_1}] \sqsubseteq A$, we have $\Delta \vdash M[v/x] : A \,|\, \epsilon'$ by (TE_Inst). Since $\epsilon' \subseteq \epsilon$, we have

$$\Delta \vdash M[v/x] : A \,|\, \epsilon$$

by (TE_Weak).

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

Case (TE_Handle)/(R_Handle): We are given

- $M_1 = \mathsf{handle}\, E[\#\mathsf{op}(v)]\, \mathsf{with}\, H$,
- $\mathsf{op} \notin E$,
- $H(\mathsf{op}) = \mathsf{op}(x, k) \rightarrow M$,
- $M_2 = M[v/x][\lambda y.\mathsf{handle}\, E[y]\, \mathsf{with}\, H/k]$,
- $\Delta \vdash \mathsf{handle}\, E[\#\mathsf{op}(v)]\, \mathsf{with}\, H : A \,|\, \epsilon$,
- $\Delta \vdash E[\#\mathsf{op}(v)] : B \,|\, \epsilon'$,
- $\Delta \vdash H : B \,|\, \epsilon' \Rightarrow A \,|\, \epsilon$

for some E, op, v, H, x, y, k, M, B, and ϵ'. Suppose that $ty(\mathsf{op}) = \forall \boldsymbol{\alpha}. C \hookrightarrow D$. By inversion of the derivation of $\Delta \vdash H : B \,|\, \epsilon' \Rightarrow A \,|\, \epsilon$, we have $\Delta, \boldsymbol{\alpha}, x : C, k : D \rightarrow^{\epsilon} A \vdash M : A \,|\, \epsilon$.

By Lemma 45,

- $\Delta, \boldsymbol{\beta}^J \vdash \boldsymbol{C_0}$,
- $\Delta, \boldsymbol{\beta}^J \vdash v : C[\boldsymbol{C_0}/\boldsymbol{\alpha}] \,|\, \epsilon_0$,
- $\Gamma, y : \forall \boldsymbol{\beta}^J. D\,[\boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash E[y] : B \,|\, \epsilon'$, and
- if $\boldsymbol{\beta}^J$ is not the empty sequence, $SR(\{\mathsf{op}\})$

for some $\boldsymbol{\beta}^J$, $\boldsymbol{C_0}$, and ϵ_0. Since $\Delta \vdash \forall \boldsymbol{\beta}^J. \boldsymbol{C_0}$,

$$\Delta, x : C\,[\forall \boldsymbol{\beta}^J. \boldsymbol{C_0}/\boldsymbol{\alpha}], k : D[\forall \boldsymbol{\beta}^J. \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow^{\epsilon} A \vdash M : A \,|\, \epsilon \tag{10}$$

by Lemma 30 (4) (note that type variables in $\boldsymbol{\alpha}$ do not appear free in A). Since $\Delta, \boldsymbol{\beta}^J \vdash v : C[\boldsymbol{C_0}/\boldsymbol{\alpha}] \,|\, \epsilon_0$, we have $\Delta \vdash v : \forall \boldsymbol{\beta}^J. C[\boldsymbol{C_0}/\boldsymbol{\alpha}] \,|\, \epsilon_0$ by Lemma 46 and (TE_Gen).

We show that $\Delta \vdash v : C[\forall \boldsymbol{\beta}^J. \boldsymbol{C_0}/\boldsymbol{\alpha}] \,|\, \epsilon_0$. If $\boldsymbol{\beta}^J$ is not empty, then $SR(\{\mathsf{op}\})$. Thus, we have the derivation by Lemma 47 (1) and (TE_Inst) (note that we can suppose that $\boldsymbol{\beta}^J$ do not appear free in C). Otherwise, if $\boldsymbol{\beta}^J$ is empty, we also have it.

By applying Lemmas 46 and 31 (1) to (10), we have

$$\Delta, k : D[\forall \boldsymbol{\beta}^J. \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow^{\epsilon} A \vdash M[v/x] : A \,|\, \epsilon. \tag{11}$$

We show that

$$\Delta \vdash \lambda y.\mathsf{handle}\, E[y]\, \mathsf{with}\, H : D[\forall \boldsymbol{\beta}^J. \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow^{\epsilon} A \,|\, \epsilon''$$

for any ϵ''.

For that, we first show that $\Delta \vdash D[\forall \boldsymbol{\beta}^J. \boldsymbol{C_0}/\boldsymbol{\alpha}] \sqsubseteq \forall \boldsymbol{\beta}^J. D[\boldsymbol{C_0}/\boldsymbol{\alpha}]$. If $\boldsymbol{\beta}^J$ is not empty, then $SR(\{\mathsf{op}\})$. Thus, we have the derivation by Lemma 47 (2) (note that we can suppose that $\boldsymbol{\beta}^J$ do not appear free in D). Otherwise, if $\boldsymbol{\beta}^J$ is empty, we also have it by (C_Refl).

Thus, since $\Gamma, y : \forall \boldsymbol{\beta}^J. D\,[\boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash E[y] : B \,|\, \epsilon'$, we have

$$\Delta, y : D\,[\forall \boldsymbol{\beta}^J. \boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash E[y] : B \,|\, \epsilon'$$

by Lemma 44. Thus, we have

$$\Delta, y : D\,[\forall\, \boldsymbol{\beta}^J .\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \vdash \mathsf{handle}\, E[y]\, \mathsf{with}\, H : A \,|\, \epsilon$$

by Lemma 29 (5) and (Te_Handle). By (Te_Abs),

$$\Delta \vdash \lambda y.\mathsf{handle}\, E[y]\, \mathsf{with}\, H : D[\forall\, \boldsymbol{\beta}^J .\, \boldsymbol{C_0}/\boldsymbol{\alpha}] \rightarrow^{\epsilon} A \,|\, \epsilon''$$

for any ϵ''.

By applying Lemma 31 (1) to (11), we have

$$\Delta \vdash M[v/x][\lambda y.\mathsf{handle}\, E[y]\, \mathsf{with}\, H/k] : A \,|\, \epsilon,$$

which is what we have to show.

Case (Te_Fix)/(R_Fix): By Lemma 31. Note that the fixed-point combinator can be given any effect.

2. Straightforward by induction on the typing derivation.

□

Theorem 2 (Type Soundness)**.** *If $\Delta \vdash M : A \,|\, \emptyset$ and $M \longrightarrow^{*} M'$ and $M' \not\longrightarrow$, then M' is a value.*

Proof. By Lemmas 48 and 36. □