Step-Indexed Syntactic Logical Relations for Recursive and Quantified Types

Amal Ahmed
Harvard University
amal@eecs.harvard.edu

March 2006

Abstract

We present a proof technique, based on syntactic logical relations, for showing contextual equivalence of expressions in a λ-calculus with recursive types and impredicative universal and existential types. We show that for recursive and polymorphic types, the method is both sound and complete with respect to contextual equivalence, while for existential types, it is sound but incomplete. Our development builds on the step-indexed PER model of recursive types presented by Appel and McAllester. We have discovered that a direct proof of transitivity of that model does not go through, leaving the "PER" status of the model in question. We show how to extend the Appel-McAllester model to obtain a logical relation that we can prove is transitive, as well as sound and complete with respect to contextual equivalence. We then augment this model to support relational reasoning in the presence of quantified types.

Step-indexed relations are indexed not just by types, but also by the number of steps available for future evaluation. This stratification is essential for handling various circularities, from recursive functions, to recursive types, to impredicative polymorphism. The resulting construction is more elementary than existing logical relations which require complex machinery such as domain theory, admissibility, syntactic minimal invariance, and $\top\top$-closure.

Contents

1 Introduction

Proving equivalence of programs is important for verifying the correctness of compiler optimizations and other program transformations, as well as for establishing that program behavior is independent of the representation of an abstract type. This representation independence principle guarantees that if one implementation of an abstraction is exchanged for another, client modules will not be able to detect a difference.

Program equivalence is generally defined in terms of *contextual equivalence*. We say that two programs are contextually equivalent if they have the same observable behavior when placed in any program context C. Unfortunately, proving contextual equivalence is difficult in general, since it involves quantification over *all* possible contexts. As a result, there's been much work on finding tractable techniques for proving contextual equivalence. Many of these are based on the method of *logical relations*.

Logical relations specify relations on well-typed terms via structural induction on the syntax of types. Thus, for instance, logically related functions take logically related arguments to related results, while logically related pairs consist of components that are related pairwise. Logical relations may be based on denotational models (e.g. [1, 2, 3]) or on the operational semantics of a language [4, 5, 6, 7]. The latter are also known as syntactic logical relations [8] and it is this flavor that is the focus of this paper.

To prove the soundness of a logical relation, one must prove the Fundamental Property (also called the Basic Lemma) which says that any well-typed term is related to itself. For simple type systems, it is fairly straightforward to prove the Fundamental Property in the absence of nontermination. The addition of recursive functions, however, complicates matters: establishing the Fundamental Property now requires proving additional "unwinding" lemmas [9, 6, 7, 10] which show that in any terminating computation a recursively defined function is approximated by its finite unrollings. More challenging still is the addition of recursive types and impredicative quantified types[1] since the logical relation can no longer be defined by induction on types. Thus, showing the existence of a relational interpretation of recursive types requires proving a nontrivial *minimal invariance* property [3, 10, 8, 11, 12].

Appel and McAllester [13] proposed a radically different solution to the problem of recursive types. They defined *intensional* types, based on the operational semantics of the language, that are indexed by the number of available (future) execution steps. This extra information is sufficient to solve recursive equations on types. Appel and McAllester also presented a PER (relational) model of recursive types, which we build on in this paper. The advantage of step-indexed logical relations is that they avoid complex machinery like domain theory, admissibility, and syntactic minimal invariance. The approach is promising since unary step-indexed models have scaled well to advanced features like impredicative quantified types and general references (i.e., mutable references that can store functions, recursive types, other references, and even impredicative quantified types) [14, 15].

Appel and McAllester proved the Fundamental Property for their PER model of equi-recursive types, and conjectured that their model was sound with respect to contextual equivalence. We show that their claim is correct — to be precise, we show soundness for a calculus with iso-recursive types, but the essence of the model is the same.

We discovered, however, that the expected proof of transitivity for the Appel-McAllester model does not go through. To definitively show that their model is not transitive we tried to find a counterexample, but could not. Thus, we note that the transitivity of the Appel-McAllester model remains an open problem.

In Section 2 we consider a λ-calculus with iso-recursive types and present a sound and complete logical relation for the language. We also show how a direct proof of transitivity of the Appel-McAllester model fails, and discuss some of the peculiarities of the step-indexed approach. In Section 3 we extend the logical relation to support quantified types. Specifically, we present a logical relation for a language with recursive and polymorphic types that is both sound and complete with respect to contextual equivalence, while for a language that also has existential types, we show a logical relation that is sound but incomplete. Proofs of all lemmas in the paper and several examples to illustrate the use of our logical relation are given in the appendix.

[1] A quantified type such as $\forall\alpha.\,\tau$ is impredicative if α may be instantiated with *any* type, including $\forall\alpha.\,\tau$ itself.

$$
\begin{array}{llll}
\textit{Types} & \tau & ::= & \mathsf{bool} \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \alpha \mid \mu\alpha.\,\tau \\
\textit{Expressions} & e & ::= & x \mid \mathtt{tt} \mid \mathtt{ff} \mid \mathtt{if}\, e_0, e_1, e_2 \mid \langle e_1, e_2\rangle \mid \mathtt{let}\,\langle x_1, x_2\rangle = e_1\,\mathtt{in}\, e_2 \mid \\
 & & & \lambda x.\, e \mid e_1\, e_2 \mid \mathtt{fold}\, e \mid \mathtt{unfold}\, e \\
\textit{Values} & v & ::= & \mathtt{tt} \mid \mathtt{ff} \mid \langle v_1, v_2\rangle \mid \lambda x.\, e \mid \mathtt{fold}\, v
\end{array}
$$

$$
\textit{Eval Ctxts} \quad E \quad ::= \quad [\cdot] \mid \mathtt{if}\, E, e_1, e_2 \mid \mathtt{let}\,\langle x_1, x_2\rangle = E\,\mathtt{in}\, e \mid E\, e \mid v\, E \mid \mathtt{fold}\, E \mid \mathtt{unfold}\, E
$$

$$
\begin{array}{lrcl}
(\mathsf{iftrue}) & \mathtt{if}\,\mathtt{tt}, e_1, e_2 & \longmapsto & e_1 \\
(\mathsf{iffalse}) & \mathtt{if}\,\mathtt{ff}, e_1, e_2 & \longmapsto & e_2 \\
(\mathsf{letpair}) & \mathtt{let}\,\langle x_1, x_2\rangle = \langle v_1, v_2\rangle\,\mathtt{in}\, e & \longmapsto & e[v_1/x_1][v_2/x_2] \\
(\mathsf{app}) & (\lambda x.\, e)\, v & \longmapsto & e[v/x] \\
(\mathsf{unfold}) & \mathtt{unfold}\,(\mathtt{fold}\, v) & \longmapsto & v \\
(\mathsf{ctxt}) & \dfrac{e \longmapsto e'}{E[e] \longmapsto E[e']} & &
\end{array}
$$

Figure 1: λ^{rec} Syntax and Operational Semantics

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

$$
(\mathsf{Var})\ \frac{}{\Gamma \vdash x : \Gamma(x)} \qquad (\mathsf{Fn})\ \frac{\Gamma, x{:}\tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x.\, e : \tau_1 \to \tau_2} \qquad (\mathsf{App})\ \frac{\Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\, e_2 : \tau_2}
$$

$$
(\mathsf{Fold})\ \frac{\Gamma \vdash e : \tau[\mu\alpha.\,\tau/\alpha]}{\Gamma \vdash \mathtt{fold}\, e : \mu\alpha.\,\tau} \qquad (\mathsf{Unfold})\ \frac{\Gamma \vdash e : \mu\alpha.\,\tau}{\Gamma \vdash \mathtt{unfold}\, e : \tau[\mu\alpha.\,\tau/\alpha]}
$$

Figure 2: λ^{rec} Static Semantics (Selected Rules)

2 Recursive Types

We consider a call-by-value λ-calculus with iso-recursive types (dubbed the λ^{rec}-calculus). Figure 1 presents the syntax and small-step operational semantics for the language, which supports booleans and pairs in addition to recursive types. We define the operational semantics for λ^{rec} as a relation between closed terms e. We use evaluation contexts to lift the primitive rewriting rules to a standard, left-to-right, innermost-to-outermost, call-by-value interpretation of the language. We say that a term e is irreducible ($\mathit{irred}(e)$) if e is a value ($\mathit{val}(e)$) or if e is a "stuck" expression to which no operational rule applies. We also use $e \Downarrow$ as an abbreviation for $\exists e'.\, e \longmapsto^* e' \wedge \mathit{val}(e')$.

Typing judgments in λ^{rec} have the form $\Gamma \vdash e : \tau$ where the context Γ is defined as follows:

$$
\textit{Value Context} \quad \Gamma \quad ::= \quad \bullet \mid \Gamma, x{:}\tau \ .
$$

Thus, Γ is used to track the set of variables in scope, along with their (closed) types. There may be at most one occurrence of a variable x in Γ. The λ^{rec} static semantics is entirely conventional (see, e.g., [17]) so we only show selected rules in Figure 2. We use the abbreviated judgment $\vdash e : \tau$ when the value context is empty.

Theorem 2.1 (λ^{rec} Safety)

If $\bullet \vdash e : \tau$ and $e \longmapsto^* e'$, then either e' is a value, or there exists an e'' such that $e' \longmapsto e''$.

2.1 λ^{rec}: Contextual Equivalence

A context C is an expression with a single hole $[\cdot]$ in it. Typing judgments for contexts have the form $\Gamma_1 \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, where $(\Gamma \triangleright \tau)$ indicates the type of the hole — that is, if $\Gamma \vdash e : \tau$, then $\Gamma_1 \vdash C[e] : \tau_1$.

Definition 2.2 (λ^{rec} **Contextual Approximation** $\preceq^{ctx}$ **& Equivalence** $\simeq^{ctx}$)

If $\Gamma \vdash e : \tau$ *and* $\Gamma \vdash e' : \tau$*, we write* $\Gamma \vdash e \preceq^{ctx} e' : \tau$ *to mean*

$$\forall C, \tau_1.\ \bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge\ C[e] \Downarrow \implies C[e'] \Downarrow \ .$$

Two terms are contextually equivalent if they contextually approximate one another:

$$\Gamma \vdash e \simeq^{ctx} e' : \tau \quad \stackrel{\text{def}}{=} \quad \Gamma \vdash e \preceq^{ctx} e' : \tau \ \wedge\ \Gamma \vdash e' \preceq^{ctx} e : \tau \ .$$

2.2 λ^{rec}: Logical Relation

Our step-indexed logical relation for λ^{rec} is based on the PER model for equi-recursive types presented by Appel and McAllester [13] (henceforth AM). The latter claimed, but did not prove, that their PER model was sound with respect to contextual equivalence. We have proved that this is indeed the case. However, "PER" may be somewhat of misnomer for the AM model since the status of transitivity is unclear, as we shall show.

$$\begin{array}{rcl}
Rel_\tau & \stackrel{\text{def}}{=} & \{\chi \in 2^{Nat \times CValues \times CValues} \mid \quad \forall (j, v, v') \in \chi.\ \ \bullet \vdash v' : \tau \ \wedge \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad \forall i \leq j.\ (i, v, v') \in \chi\} \\
\lfloor \chi \rfloor_k & \stackrel{\text{def}}{=} & \{(j, v, v') \mid\ j < k \ \wedge\ (j, v, v') \in \chi\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{RV}\,[\![\alpha]\!]\rho & = & \rho^{\mathsf{sem}}(\alpha) \\
\mathcal{RV}\,[\![\mathsf{bool}]\!]\rho & = & \{(k, v, v') \mid\ \vdash v' : \mathsf{bool} \ \wedge \\
 & & \qquad (v = v' = \mathtt{tt} \ \vee\ v = v' = \mathtt{ff})\} \\
\mathcal{RV}\,[\![\tau_1 \times \tau_2]\!]\rho & = & \{(k, \langle v_1, v_2\rangle, \langle v_1', v_2'\rangle) \mid\ \vdash \langle v_1', v_2'\rangle : (\tau_1 \times \tau_2)^{[\rho]} \ \wedge \\
 & & \qquad (k, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\rho \wedge (k, v_2, v_2') \in \mathcal{RV}\,[\![\tau_2]\!]\rho\} \\
\mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\rho & = & \{(k, \lambda x.\, e, \lambda x.\, e') \mid\ \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]} \ \wedge \\
 & & \qquad \forall j < k, v, v'. \\
 & & \qquad\quad (j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\rho \implies \\
 & & \qquad\quad (j, e[v/x], e'[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\rho\} \\
\mathcal{RV}\,[\![\mu\alpha.\, \tau]\!]\rho & = & \{(k, \mathtt{fold}\, v, \mathtt{fold}\, v') \mid\ \vdash \mathtt{fold}\, v' : (\mu\alpha.\, \tau)^{[\rho]} \ \wedge \\
 & & \qquad \forall j < k. \\
 & & \qquad\quad \text{let } \chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau]\!]\rho \rfloor_{j+1} \text{ in} \\
 & & \qquad\quad (j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\rho[\alpha \mapsto (\chi,\ \ (\mu\alpha.\, \tau)^{[\rho]}\ )]\} \\
\mathcal{RC}\,[\![\tau]\!]\,\rho & = & \{(k, e, e') \mid\ \forall j < k, e_f. \\
 & & \qquad\quad e \longmapsto^j e_f \wedge \mathit{irred}(e_f) \implies \\
 & & \qquad\quad \exists e_f'.\ e' \longmapsto^* e_f' \ \wedge\ (k - j, e_f, e_f') \in \mathcal{RV}\,[\![\tau]\!]\rho\} \\
\mathcal{RG}\,[\![\bullet]\!] & = & \{(k, \emptyset, \emptyset)\} \\
\mathcal{RG}\,[\![\Gamma, x{:}\tau]\!] & = & \{(k, \gamma[x \mapsto v], \gamma'[x \mapsto v']) \mid\ (k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!] \wedge (k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\emptyset\}
\end{array}$$

$$\begin{array}{rcl}
\Gamma \vdash e \leq e' : \tau & \stackrel{\text{def}}{=} & \Gamma \vdash e : \tau \ \wedge\ \Gamma \vdash e' : \tau \ \wedge \\
 & & \forall k \geq 0.\ \forall \gamma, \gamma'. \\
 & & \quad (k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!] \implies (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\emptyset \\
\Gamma \vdash e \sim e' : \tau & \stackrel{\text{def}}{=} & \Gamma \vdash e \leq e' : \tau \ \wedge\ \Gamma \vdash e' \leq e : \tau
\end{array}$$

Figure 3: λ^{rec} Relational Model (Shaded $\notin$ Appel-McAllester)

In both models, the relational interpretation $\mathcal{RV}\,[\![\tau]\!]$ of a type τ is a set of triples of the form (k, v, v') where k is a natural number (called the *approximation index* or *step index*), and v and v' are (closed) values. Intuitively, $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]$ says that in any computation running for no more than k steps, v approximates v' at the type τ. Our model differs from the AM model in that whenever $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]$, we additionally

require that $\bullet \vdash v' : \tau$. This additional constraint enables us to prove the transitivity of our logical relation. Moreover, restricting the model to terms that are well-typed seems essential for completeness with respect to contextual equivalence, as others have also noted [12]. We defer an explanation of why we don't also require $\bullet \vdash v : \tau$ till Section 2.3.

Figure 3 gives the definition of our logical relation; shaded parts of the definitions have no analog in the AM model. We use the meta-variable χ to denote sets of tuples of the form (k, v, v'), where v and v' are closed values ($v, v' \in \mathit{CValues}$). For any set χ, we define the k-approximation of the set (written $\lfloor \chi \rfloor_k$) as the subset of its elements whose indices are less than k.

We define Rel_τ (where τ is a closed syntactic type) as the set of those sets $\chi \in 2^{\mathit{Nat} \times \mathit{CValues} \times \mathit{CValues}}$ that have the following two properties: if $(k, v, v') \in \chi$, then v' must be well-typed with type τ, and χ must be closed with respect to a decreasing step-index.

We use the meta-variable ρ to denote type substitutions. These are partial maps from type variables α to pairs (χ, τ) where χ is the semantic substitution for α and τ (a closed syntactic type) is the syntactic substitution for α. We note that our definitions ensure that if $\rho(\alpha) = (\chi, \tau)$ then $\chi \in \mathit{Rel}_\tau$. Since types in λ^{rec} may contain free type variables, the interpretation of a type τ is parametrized by a type substitution ρ such that $\mathit{FTV}(\tau) \subseteq \mathit{dom}(\rho)$. We use the following abbreviations:

- Let $\rho(\alpha) = (\chi, \tau)$. Then $\rho^{\mathsf{sem}}(\alpha) = \chi$ and $\rho^{\mathsf{syn}}(\alpha) = \tau$.
- Let $\rho = \{\alpha_1 \mapsto (\chi_1, \tau_1), \ldots, \alpha_n \mapsto (\chi_n, \tau_n)\}$.
  Then $\tau^{[\rho]}$ is an abbreviation for $\tau[\tau_1/\alpha_1, \tau_2/\alpha_2, \ldots, \tau_n/\alpha_n]$.

Next, we consider the relational interpretation $\mathcal{RV}[\![\tau]\!]\rho$ of each type τ. In each case, note that if $(k, v, v') \in \mathcal{RV}[\![\tau]\!]\rho$ then $\vdash v' : (\tau)^{[\rho]}$.

Booleans. Two values are related at the type bool for any number of steps $k \geq 0$, if they are both $\mathtt{tt}$ or both $\mathtt{ff}$.

Pairs. The pairs $\langle v_1, v_2 \rangle$ and $\langle v_1', v_2' \rangle$ are related at type $\tau_1 \times \tau_1$ for k steps if v_i and v_i' are related for k steps at the type τ_i (for $i \in \{1, 2\}$).

Functions. Since functions are suspended computations, their interpretation is given in terms of the interpretation of types as computations (see below). Two functions are related if they map related arguments to related results. Specifically, $\lambda x.\, e$ and $\lambda x.\, e'$ are related at the type $\tau_1 \to \tau_2$ for k steps if, at some point in the future, when there are $j < k$ steps left to execute, and there are arguments v_a and v_a' that are related at the type τ_1 for j steps, then $e[v_a/x]$ and $e'[v_a'/x]$ are related as computations of type τ_2 for j steps.

Recursive Types. One would expect the values $\mathtt{fold}\, v$ and $\mathtt{fold}\, v'$ to be related at the type $\mu\alpha.\, \tau$ for k steps if v and v' are related at the type $\tau[\mu\alpha.\, \tau/\alpha]$ for $j < k$ steps. We show that the latter is equivalent to what is required by the definition in Figure 3. Note that by the definition of $\lfloor \cdot \rfloor_k$

$$(j, v, v') \in \mathcal{RV}[\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\rho \;\Leftrightarrow\; (j, v, v') \in \lfloor \mathcal{RV}[\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\rho \rfloor_{j+1} \;.$$

We prove a type substitution lemma (see Appendix B.7) that allows us to conclude that if $\chi = \lfloor \mathcal{RV}[\![\mu\alpha.\, \tau]\!]\rho \rfloor_{j+1}$ then:

$$\lfloor \mathcal{RV}[\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\rho \rfloor_{j+1} \;=\; \lfloor \mathcal{RV}[\![\tau]\!]\rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})] \rfloor_{j+1} \;.$$

Hence,

$$\begin{array}{ll}
(j, v, v') \in \mathcal{RV}[\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\rho & \\
\quad \Leftrightarrow (j, v, v') \in \lfloor \mathcal{RV}[\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\rho \rfloor_{j+1} & \text{by } \lfloor \cdot \rfloor_k \\
\quad \Leftrightarrow (j, v, v') \in \lfloor \mathcal{RV}[\![\tau]\!]\rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})] \rfloor_{j+1} & \text{by type subst} \\
\quad \Leftrightarrow (j, v, v') \in \mathcal{RV}[\![\tau]\!]\rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})] & \text{by } \lfloor \cdot \rfloor_k
\end{array}$$

which is exactly what is required by the definition of $\mathcal{RV}[\![\mu\alpha.\, \tau]\!]\rho$.

Computations. Two closed expressions e and e' are related as computations of type τ for k steps as follows. If e steps to an irreducible term e_f in $j < k$ steps, then e' must also step to some irreducible e'_f. Furthermore, both e_f and e'_f must be values that are related for the remaining $k - j$ steps.

What is surprising about this definition is that e must terminate in $j < k$ steps, while e' may terminate in *any* number of steps, say i. Hence, i may be greater than k. This has ramifications for transitivity in the AM model and we shall return to this point shortly.

Logical Relation. If $\Gamma \vdash e : \tau$ and $\Gamma \vdash e' : \tau$, then we write $\Gamma \vdash e \leq e' : \tau$ to mean that for all $k \geq 0$, if γ and γ' are mappings from variables x to closed values that are related for k steps at Γ, then $\gamma(e)$ and $\gamma'(e')$ are related for k steps as computations of type τ. We say e and e' are logically equivalent, written $\Gamma \vdash e \sim e' : \tau$, if they logically approximate one another.

We now have to prove that each type τ is a valid type — that is, that the relational interpretation of τ belongs to Rel_τ (i.e., $\mathcal{RV}\,[\![\tau]\!]\,\rho \in Rel_{\tau[\rho]}$). This involves showing well-typedness and closure under decreasing step-index (see Appendix B.6).

Next, we prove a number of nontrivial lemmas (see Appendix B.7 and B.8). Specifically, we prove that the logical relation defined in Figure 3 has the compatibility and substitutivity properties (see e.g., [9]). These allow us to show that the λ^{rec} typing rules preserve the logical relation, and hence prove the following lemma.

Lemma 2.3 (λ^{rec} Fundamental Property / Reflexivity)

If $\Gamma \vdash e : \tau$, *then* $\Gamma \vdash e \leq e : \tau$.

2.3 Transitivity and the Appel-McAllester Model

Let us ignore the shaded parts of Figure 3 and try to prove the following lemma with the resulting definitions.

Proposed Lemma (Transitivity: Appel-McAllester)
If $\Gamma \vdash e_1 \leq e_2 : \tau$ and $\Gamma \vdash e_2 \leq e_3 : \tau$, then $\Gamma \vdash e_1 \leq e_3 : \tau$.

Proof Attempt: Suppose $k \geq 0$ and $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.
Show $(k, \gamma(e_1), \gamma'(e_3)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$. Suppose $j < k$, $\gamma(e_1) \longmapsto^j e_{f_1}$, and $\mathit{irred}(e_{f_1})$.
Show $\exists e_{f_3}.\gamma'(e_3) \longmapsto^* e_{f_3} \wedge (k - j, e_{f_1}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.
Instantiate $\Gamma \vdash e_1 \leq e_2 : \tau$ with $k \geq 0$ and $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.
Hence, $(k, \gamma(e_1), \gamma'(e_2)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Instantiate this with $j < k$, $\gamma(e_1) \longmapsto^j e_{f_1}$, and $\mathit{irred}(e_{f_1})$.
Hence, $\exists e_{f_2}, i$ such that $i \geq 0$, $\gamma'(e_2) \longmapsto^i e_{f_2}$, and $(k - j, e_{f_1}, e_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.
Now we need to use the premise $\Gamma \vdash e_2 \leq e_3 : \tau$. But what should we instantiate this with? We consider two ways we could proceed.

(i) Instantiate $\Gamma \vdash e_2 \leq e_3 : \tau$ with k, γ, γ'. Note that $k \geq 0$ and $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$. Hence, $(k, \gamma(e_2), \gamma'(e_3)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Problem: We could instantiate this with i and e_{f_2}, but at that point we are stuck since we cannot show $i < k$ (since i may be greater than k), and we cannot show $\gamma(e_2) \longmapsto^i e_{f_2}$ (we only have $\gamma'(e_2) \longmapsto^i e_{f_2}$).

(ii) Instantiate $\Gamma \vdash e_2 \leq e_3 : \tau$ with $i + 1$, γ', γ'.
Problem: We cannot show $(i + 1, \gamma', \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$. All we know is that $(k, \gamma, \gamma') \in \Gamma$, where i may be greater than k.

We note that if we restrict our attention to closed terms e_1, e_2, e_3, then the above lemma can be proved. In the case of open terms, however, the status of transitivity of the AM model is unclear as we have been unable to find a counterexample.

There are several things one could attempt in order to rectify the above problem with the AM model (unshaded parts of Figure 3). One problem we encountered was that i may be greater than k. To get around

this, we could change the definition of $(k, e, e') \in \mathcal{RC}[\![\tau]\!]$ to require that e' must terminate in less than k steps. Unfortunately, if we step back and examine the resulting meaning of $\Gamma \vdash e_1 \sim e_2 : \tau$, we see that the latter now requires that both e_1 and e_2 must terminate in *exactly the same number of steps*. Clearly such a logical relation would not be very useful (unless we are concerned with reasoning about timing leaks in an information-flow setting). Other formulations involving the use of not one, but two step-indices (where the second bounds the number of steps in which e' must terminate) also lead to models where both terms are required to terminate in exactly the same number of steps.

Since we want a logical relation that considers programs equivalent modulo the number of steps they take, we will not change the definition of $\mathcal{RC}[\![\tau]\!]$. Instead we fix the problem with transitivity by moving to a typed setting where $(k, v, v') \in \mathcal{RV}[\![\tau]\!]\,\emptyset$ implies $\vdash v' : \tau$. Assuming the definitions in Figure 3, including the shaded parts, let us again try to prove transitivity.

Lemma 2.4 (λ^{rec} : Transitivity)

(Our model: Figure 3, including shaded parts)
If $\Gamma \vdash e_1 \leq e_2 : \tau$ *and* $\Gamma \vdash e_2 \leq e_3 : \tau$, *then* $\Gamma \vdash e_1 \leq e_3 : \tau$.

Proof

We start at the point where we got stuck before. Now from $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]$ we can conclude that $\vdash \gamma' : \Gamma$. By reflexivity (Fundamental Property, Lemma 2.3) it follows that $\vdash \gamma' \leq \gamma' : \Gamma$. Hence, we can show that for all $z \geq 0$, $(z, \gamma', \gamma') \in \mathcal{RG}[\![\Gamma]\!]$ holds. Now we may instantiate $\Gamma \vdash e_2 \leq e_3 : \tau$ above with $i+1$ since we know that $(i+1, \gamma', \gamma') \in \mathcal{RG}[\![\Gamma]\!]$. The rest of the proof is relatively straightforward and is given in Appendix B.10. □

Seemingly Asymmetric Well-Typedness Requirement. The definitions in Figure 3 may have left the reader with the impression that we only require terms on one side of our logical relation to be well-typed. This, however, is not the case. In particular, notice that in the definition of $\Gamma \vdash e \leq e' : \tau$, we require that *both* e and e' be well-typed. However, once we have picked a step-index k (i.e., once we have moved under the $\forall k$ quantifier), there is an asymmetry in the model in that when $(k, e, e') \in \mathcal{RC}[\![\tau]\!]$, k pertains (as a bound) only to e and not to e'. As a result of this asymmetry, when working with a specific k (in the definition of $\mathcal{RV}[\![\tau]\!]$) we do not need to know that v has type τ in the limit, while the converse is true of v'. Hence, at the value interpretation level $\mathcal{RV}[\![\tau]\!]$, we chose only to require $\vdash v' : \tau$. One could add the requirement $\vdash v : \tau$ in the interest of symmetry, but it would simply lead to additional proof obligations being shuffled around. It would also complicate definitions when we get to quantified types as Rel_τ would have to be replaced by Rel_{τ_1,τ_2} (since in the presence of quantified types we wish to relate values of different types).

2.4 λ^{rec}: Soundness

To prove that our logical relation is sound with respect to contextual equivalence, we first define what it means for two contexts to be logically related.

Definition 2.5 (λ^{rec} Logical Relation: Contexts)

$$\Gamma_1 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \stackrel{\text{def}}{=} \forall e, e'.\ \Gamma \vdash e \leq e' : \tau \implies \Gamma_1 \vdash C[e] \leq C'[e'] : \tau_1$$

Next, we prove the compatibility lemmas for contexts, which allows us to prove the following.

Lemma 2.6 (λ^{rec} Reflexivity: Contexts)

If $\Gamma_1 \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, *then* $\Gamma_1 \vdash C \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$.

Theorem 2.7 (λ^{rec} Soundness: $\leq \ \subseteq \ \preceq^{ctx}$)

If $\Gamma \vdash e \leq e' : \tau$ *then* $\Gamma \vdash e \preceq^{ctx} e' : \tau$.

Proof

Suppose $\bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ and $C[e] \Downarrow$. Hence, there exist v_f, k such that $C[e] \longmapsto^k v_f$. We must show $C[e'] \Downarrow$.
Applying Lemma 2.6 to $\bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, we have $\bullet \vdash C \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$.
Instantiate this with $\Gamma \vdash e \leq e' : \tau$. Hence, $\bullet \vdash C[e] \leq C[e'] : \tau_1$.
Instantiate this with $k+1 \geq 0$ and $(k+1, \emptyset, \emptyset) \in \mathcal{RG}[\![\bullet]\!]$.
Hence, $(k+1, C[e], C[e']) \in \mathcal{RC}[\![\tau_1]\!]\emptyset$.
Instantiate this with $k < k+1$, $C[e] \longmapsto^k v_f$, and $\mathit{irred}(v_f)$.
Hence, exists v'_f such that $C[e'] \longmapsto^* v'_f$. Hence, $C[e'] \Downarrow$. □

2.5 λ^{rec}: Completeness

To show that our logical relation is complete with respect to contextual equivalence, we make use of the notion of *ciu-equivalence* introduced by Mason and Talcott [18]. Two closed terms of the same closed type are said to be ciu-equivalent if they have the same termination behavior in any evaluation context E (a *u*se of the term). The relation is extended to open terms via closing substitutions (i.e., *c*losed *i*nstantiations). We note that evaluation contexts E are a simply a subset of general contexts C and that only closed terms can be placed in an evaluation context.

Definition 2.8 (λ^{rec} **Ciu Approximation** $\preceq^{ciu}$ **& Equivalence** $\simeq^{ciu}$)

Let $\Gamma \vdash e : \tau$ *and* $\Gamma \vdash e' : \tau$.

$$\Gamma \vdash e \preceq^{ciu} e' : \tau \quad \stackrel{\text{def}}{=} \quad \forall \gamma, E, \tau_1.\ \bullet \vdash \gamma : \Gamma \ \wedge\ \bullet \vdash E : (\bullet \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge\ E[\gamma(e)] \Downarrow \implies E[\gamma(e')] \Downarrow$$

$$\Gamma \vdash e \simeq^{ciu} e' : \tau \quad \stackrel{\text{def}}{=} \quad \Gamma \vdash e \preceq^{ciu} e' : \tau \ \wedge\ \Gamma \vdash e' \preceq^{ciu} e : \tau$$

Theorem 2.9 (λ^{rec} **:** $\preceq^{ctx} \ \subseteq \ \preceq^{ciu}$)

If $\Gamma \vdash e \preceq^{ctx} e' : \tau$ *then* $\Gamma \vdash e \preceq^{ciu} e' : \tau$.

To prove that two ciu-equivalent terms are logically related, we will need the following lemma which shows that our logical relation respects ciu equivalence. Pitts [9] proves a similar property which he calls "equivalence-respecting".

Lemma 2.10 (λ^{rec} **Equivalence-Respecting: Closed Values**)

If $(k, v_1, v_2) \in \mathcal{RV}[\![\tau]\!]\emptyset$ *and* $\bullet \vdash v_2 \preceq^{ciu} v_3 : \tau$, *then* $(k, v_1, v_3) \in \mathcal{RV}[\![\tau]\!]\emptyset$.

Proof

By induction on k and nested induction on the structure of the (closed) type τ. □

Theorem 2.11 (λ^{rec} **:** $\preceq^{ciu} \ \subseteq \ \leq$)

If $\Gamma \vdash e \preceq^{ciu} e' : \tau$ *then* $\Gamma \vdash e \leq e' : \tau$.

Proof

Suppose $k \geq 0$ and $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]$. Show $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\![\tau]\!]\emptyset$. Suppose $j < k$, $\gamma(e) \longmapsto^j e_f$, and $\mathit{irred}(e_f)$.
Show $\exists e''_f.\ \gamma'(e') \longmapsto^* e''_f \ \wedge\ (k-j, e_f, e''_f) \in \mathcal{RV}[\![\tau]\!]\emptyset$.
From $\Gamma \vdash e \preceq^{ciu} e' : \tau$, we have $\Gamma \vdash e : \tau$. Applying Lemma 2.3 to $\Gamma \vdash e : \tau$, we have $\Gamma \vdash e \leq e : \tau$. Instantiate this with $k \geq 0$ and $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]$. Hence, $(k, \gamma(e), \gamma'(e)) \in \mathcal{RC}[\![\tau]\!]\emptyset$. Instantiate this

with $j < k$, $\gamma(e) \longmapsto^{j} e_f$, and $\mathit{irred}(e_f)$. Hence, $\exists e'_f$ such that $\gamma'(e) \longmapsto^{*} e'_f$ and $(k-j, e_f, e'_f) \in \mathcal{RV}[\![\tau]\!]\emptyset$. Hence, $e_f \equiv v_f$ and $e'_f \equiv v'_f$. Hence, $\gamma'(e) \Downarrow v'_f$.

Instantiate $\Gamma \vdash e \preceq^{ciu} e' : \tau$ with $\vdash \gamma' : \Gamma$ (follows from $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]$), and $\bullet \vdash [\cdot] : (\bullet \triangleright \tau) \rightsquigarrow \tau$, and $\gamma'(e) \Downarrow$. Hence, $\exists v''_f$ such that $\gamma'(e') \longmapsto^{*} v''_f$.

Remains to show: $(k-j, v_f, v''_f) \in \mathcal{RV}[\![\tau]\!]\emptyset$.

This follows from Lemma 2.10 applied to $(k-j, v_f, v'_f) \in \mathcal{RV}[\![\tau]\!]\emptyset$ and $v'_f \preceq^{ciu} v''_f : \tau$ (which follows from $\Gamma \vdash e \preceq^{ciu} e' : \tau$ and $\gamma'(e) \Downarrow v'_f$ and $\gamma'(e') \Downarrow v''_f$). □

3 Type Abstraction

We now extend λ^{rec} with impredicative universal and existential types; we call the extended language the $\lambda^{\forall\exists}$-calculus. (Note that in Section 3.4 we will consider the $\lambda^{\forall}$-calculus which is the extension of λ^{rec} with only universal types.) The syntactic extensions to support quantified types are as follows:

$$\begin{array}{lrcl} \textit{Types} & \tau & ::= & \ldots \mid \forall\alpha.\,\tau \mid \exists\alpha.\,\tau \\ \textit{Values} & v & ::= & \ldots \mid \Lambda.\,e \mid \mathtt{pack}\,v \\ \textit{Expressions} & e & ::= & \ldots \mid e\,[\,] \mid \mathtt{unpack}\,e_1\,\mathtt{as}\,x\,\mathtt{in}\,e_2 \end{array}$$

Note that terms are not decorated with types (which was also the case for λ^{rec}). Here we let the vestigial operators remain in the untyped syntax in order to preserve the operational semantics. For instance, the term $\Lambda.\,e$ is a suspended computation (normally written $\Lambda\alpha.e$); $e\,[\,]$ runs the suspended computation. We extend the λ^{rec} operational semantics as follows:

$$\begin{array}{lrcl} \textit{Evaluation Contexts} \quad E & ::= & \ldots \mid E\,[\,] \mid \mathtt{unpack}\,E\,\mathtt{as}\,x\,\mathtt{in}\,e & \\ \textsf{(inst)} & (\Lambda.\,e)\,[\,] & \longmapsto & e \\ \textsf{(unpack)} & \mathtt{unpack}\,(\mathtt{pack}\,v)\,\mathtt{as}\,x\,\mathtt{in}\,e & \longmapsto & e[v/x] \end{array}$$

$\boxed{\Delta; \Gamma \vdash e : \tau}$

$$\textsf{(All)}\ \frac{\Delta, \alpha; \Gamma \vdash e : \tau}{\Delta; \Gamma \vdash \Lambda.\,e : \forall\alpha.\,\tau} \qquad \textsf{(Inst)}\ \frac{\Delta; \Gamma \vdash e : \forall\alpha.\,\tau \qquad \Delta \vdash \tau_1}{\Delta; \Gamma \vdash e\,[\,] : \tau[\tau_1/\alpha]} \qquad \textsf{(Pack)}\ \frac{\Delta \vdash \tau_1 \qquad \Delta; \Gamma \vdash e : \tau[\tau_1/\alpha]}{\Delta; \Gamma \vdash \mathtt{pack}\,e : \exists\alpha.\,\tau}$$

$$\textsf{(Unpack)}\ \frac{\Delta; \Gamma \vdash e_1 : \exists\alpha.\,\tau_1 \qquad \Delta \vdash \tau_2 \qquad \Delta, \alpha; \Gamma, x : \tau_1 \vdash e_2 : \tau_2}{\Delta; \Gamma \vdash \mathtt{unpack}\,e_1\,\mathtt{as}\,x\,\mathtt{in}\,e_2 : \tau_2}$$

Figure 4: $\lambda^{\forall\exists}$ Static Semantics

$\lambda^{\forall\exists}$ typing judgments have the form $\Delta; \Gamma \vdash e : \tau$, where the context Γ is as before, and the context Δ is defined as follows:

$$\textit{Type Context} \quad \Delta \quad ::= \quad \bullet \mid \Delta, \alpha\ .$$

The type context Δ is used to track the set of type variables in scope. We modify the typing rules in Figure 2 by adding Δ to each typing judgment. Figure 4 gives the typing rules for the additional terms in $\lambda^{\forall\exists}$. We prove soundness of the $\lambda^{\forall\exists}$ typing rules, show that value and type substitution hold, and prove type safety.

Theorem 3.1 **($\lambda^{\forall\exists}$ Safety)**

If $\bullet; \bullet \vdash e : \tau$ and $e \longmapsto^{*} e'$, then either e' is a value, or there exists an e'' such that $e' \longmapsto e''$.

3.1 $\lambda^{\forall\exists}$: Contextual Equivalence

Typing judgments for contexts C now have the form $\Delta_1;\Gamma_1 \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ (where $(\Delta;\Gamma \triangleright \tau)$ represents the type of the hole) indicating that whenever $\Delta;\Gamma \vdash e : \tau$, then $\Delta_1;\Gamma_1 \vdash C[e] : \tau_1$.

Definition 3.2 ($\lambda^{\forall\exists}$ **Contextual Approximation** $\preceq^{ctx}$)

If $\Delta;\Gamma \vdash e : \tau$ *and* $\Delta;\Gamma \vdash e' : \tau$, *then we write* $\Delta;\Gamma \vdash e \preceq^{ctx} e' : \tau$ *to mean*

$$\forall C, \tau_1.\ \bullet;\bullet \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge\ C[e]\Downarrow \implies C[e']\Downarrow\ .$$

3.2 $\lambda^{\forall\exists}$: Logical Relation and Soundness

In this section, we present a logical relation for $\lambda^{\forall\exists}$ and prove it sound with respect to contextual equivalence. (Note, however, that this logical relation is not complete with respect to contextual equivalence. We will discuss properties required for completeness in Section 3.4.)

As in the case of λ^{rec}, the relational interpretation of a type $\mathcal{RV}\,[\![\tau]\!]\,\rho$ in $\lambda^{\forall\exists}$ is a set of triples of the form (k, v, v'). We define Rel_τ as before (see Figure 3), so that every set χ in Rel_τ must be closed under decreasing step index, and the second value of each tuple in χ must be well-typed with type τ.

The relational interpretation of universal and existential types is given in Figure 5. Two values $\mathtt{pack}\,v$ and $\mathtt{pack}\,v'$ are related at the type $\exists\alpha.\,\tau$ for k steps if there exists a syntactic type τ_2 and a semantic interpretation $\chi \in Rel_{\tau_2}$ such that for all $j < k$, $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$. Here we only pick a type τ_2 for the second value v' while the type of v is left unrestricted. Intuitively, this suffices because when showing logical equivalence of two terms $(\Delta;\Gamma \vdash e \sim e' : \tau)$, we pick a type for v' while proving $\Delta;\Gamma \vdash e \leq e' : \tau$ and we pick a type for v while proving $\Delta;\Gamma \vdash e' \leq e : \tau$. The relational interpretation of universal types is the dual of existential types.

$$\begin{array}{rcl}
\mathcal{RV}\,[\![\forall\alpha.\,\tau]\!]\rho & = & \{(k, \Lambda.\,e, \Lambda.\,e') \mid \vdash \Lambda.\,e' : (\forall\alpha.\,\tau)^{[\rho]} \ \wedge \\
& & \qquad \forall\tau_2, \chi.\ \chi \in Rel_{\tau_2} \implies \\
& & \qquad\quad \forall j < k.\ (j, e, e') \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]\} \\
\\
\mathcal{RV}\,[\![\exists\alpha.\,\tau]\!]\rho & = & \{(k, \mathtt{pack}\,v, \mathtt{pack}\,v') \mid \vdash \mathtt{pack}\,v' : (\exists\alpha.\,\tau)^{[\rho]} \ \wedge \\
& & \qquad \exists\tau_2, \chi.\ \chi \in Rel_{\tau_2} \ \wedge \\
& & \qquad\quad \forall j < k.\ (j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{RD}\,[\![\bullet]\!] & = & \{\emptyset\} \\
\mathcal{RD}\,[\![\Delta, \alpha]\!] & = & \{\rho[\alpha \mapsto (\chi, \tau_2)]) \mid \rho \in \mathcal{RD}\,[\![\Delta]\!] \ \wedge\ \chi \in Rel_{\tau_2}\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{RG}\,[\![\bullet]\!]\rho & = & \{(k, \emptyset, \emptyset)\} \\
\mathcal{RG}\,[\![\Gamma, x{:}\tau]\!]\rho & = & \{(k, \gamma[x \mapsto v], \gamma'[x \mapsto v']) \mid (k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\rho \wedge (k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\rho\}
\end{array}$$

$$\begin{array}{rcl}
\Delta;\Gamma \vdash e \leq e' : \tau & \stackrel{\text{def}}{=} & \Delta;\Gamma \vdash e : \tau \ \wedge\ \Delta;\Gamma \vdash e' : \tau \ \wedge \\
& & \forall k \geq 0.\ \forall\rho, \gamma, \gamma'.\ \rho \in \mathcal{RD}\,[\![\Delta]\!] \ \wedge\ (k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\rho \implies \\
& & \qquad (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\rho
\end{array}$$

Figure 5: $\lambda^{\forall\exists}$ Relational Model

The relational interpretation of types as computations $\mathcal{RC}\,[\![\tau]\!]$ is defined exactly as before (see Figure 3). The definition of the logical relation $\Delta;\Gamma \vdash e \leq e' : \tau$ appears in Figure 5.

We prove that each type τ is a valid type: $\mathcal{RV}\,[\![\tau]\!]\,\rho \in Rel_{\tau^{[\rho]}}$. Specifically, we have to show well-typedness and closure under decreasing step-index.

To show the Fundamental Property of the logical relation, we prove the new set of compatibility lemmas, as well as value and type substitutivity. Thus, we can prove the following lemma.

Lemma 3.3 ($\lambda^{\forall\exists}$ **Fundamental Property / Reflexivity)**

If $\Delta;\Gamma \vdash e:\tau$ *then* $\Delta;\Gamma \vdash e \leq e:\tau$.

Next, we prove that the logical relation in Figure 5 is sound with respect to contextual equivalence. The overall proof structure is the same as for λ^{rec}.

Theorem 3.4 ($\lambda^{\forall\exists}$ **:** $\leq \subseteq \preceq^{ctx}$)

If $\Delta;\Gamma \vdash e \leq e' : \tau$ *then* $\Delta;\Gamma \vdash e \preceq^{ctx} e' : \tau$.

3.3 Example: Simple Existential Packages

For lack of space, we present only one simple example (from Sumii and Pierce[19]) to illustrate the use of our logical relation to prove contextual equivalence. Additional examples involving existential packages, recursive types, and higher-order functions are given in Appendix D.

Example: Consider the following existential packages e and e' of type τ:

$$e \;=\; \mathtt{pack}\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle \qquad e' \;=\; \mathtt{pack}\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle \qquad \tau \;=\; \exists\alpha.\, \alpha \times (\alpha \to \mathsf{bool})$$

Show $\bullet;\bullet \vdash e \sim e' : \tau$. We only show $\bullet;\bullet \vdash e \leq e' : \tau$. $\bullet;\bullet \vdash e' \leq e : \tau$ is symmetric.
Suppose $k \geq 0$. Unwinding definitions, we must show $(k, e, e') \in \mathcal{RV}\,[\![\tau]\!]$
$\equiv (k, \mathtt{pack}\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle, \mathtt{pack}\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\exists\alpha.\, \alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset$.
Take $\tau_2 = \mathsf{bool}$ and $\chi = \{(k', 1, \mathtt{tt}) \mid\ k' \geq 0\}$.
Note that $\chi \in Rel_{\mathsf{bool}}$ (from defn of χ). Suppose $j < k$.
Show $(j, \langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle, \langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which follows from:

- $\vdash \langle \mathtt{tt}, \lambda x.\, \neg x\rangle : (\alpha \times (\alpha \to \mathsf{bool}))[\mathsf{bool}/\alpha]$
- $(j, 1, \mathtt{tt}) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv\ (j, 1, \mathtt{tt}) \in \chi$ (by defn of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
  which follows from defn of χ.
- $(j, (\lambda x.\, x \overset{\text{int}}{=} 0), (\lambda x.\, \neg x)) \in \mathcal{RV}\,[\![\alpha \to \mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which follows from:
  First, note that $\vdash \lambda x.\, \neg x : (\alpha \to \mathsf{bool})[\mathsf{bool}/\alpha] \;\equiv\; \vdash \lambda x.\, \neg x : \mathsf{bool} \to \mathsf{bool}$.
  Next, suppose $i < j$, and $(i, v_1, v_1') \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
  Note that $\mathcal{RV}\,[\![\alpha]\!]\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \equiv \chi$ by defn of $\mathcal{RV}\,[\![\alpha]\!]\rho$. Hence, $(i, v_1, v_1') \in \chi$.
  Then, from defn of χ, $v_1 = 1$ and $v_1' = \mathtt{tt}$.
  Show: $(i, (x \overset{\text{int}}{=} 0)[v_1/x], (\neg x)[v_1'/x]) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv (i, v_1 \overset{\text{int}}{=} 0, \neg v_1') \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv (i, 1 \overset{\text{int}}{=} 0, \neg \mathtt{tt}) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
  Note that $(1 \overset{\text{int}}{=} 0) \longmapsto^1 \mathtt{ff}$ and $(\neg \mathtt{tt}) \longmapsto^* \mathtt{ff}$.
  Hence, remains to show: $(i-1, \mathtt{ff}, \mathtt{ff}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which is immediate.

3.4 $\lambda^{\forall}$: Completeness

The $\lambda^{\forall\exists}$ logical relation presented in Section 3.2 is sound but not complete with respect to contextual equivalence. In this section, we present an outline of the desired completeness proof in order to illustrate where the proof gets stuck and to motivate changes to the earlier logical relation that might make it complete with respect to contextual equivalence. With a minor modification to the logical relation from Section 3.2, we are able to show completeness in the presence of recursive and polymorphic types, but not for existential types (i.e., for the language $\lambda^{\forall}$, which extends λ^{rec} with only universal types).

We start by trying to establish completeness for $\lambda^{\forall\exists}$ in a manner similar to that for λ^{rec}. As for λ^{rec}, we rely on the notion of ciu-equivalence, which we define for $\lambda^{\forall\exists}$ as follows.

Definition 3.5 ($\lambda^{\forall\exists}$ **Ciu Approximation** $\preceq^{ciu}$)

Let $\Delta;\Gamma \vdash e : \tau$ *and* $\Delta;\Gamma \vdash e' : \tau$. *If* δ *is a mapping from type variables* α *to closed syntactic types* τ, *we write* $\delta \models \Delta$ *whenever* $dom(\delta) = \Delta$.

$$\Delta;\Gamma \vdash e \preceq^{ciu} e' : \tau \quad \stackrel{\text{def}}{=} \quad \forall \delta, \gamma, E, \tau_1.\ \delta \models \Delta \ \wedge\ \vdash \gamma : \delta(\Gamma) \ \wedge\ \bullet;\bullet \vdash E : (\bullet;\bullet \triangleright \delta(\tau)) \rightsquigarrow \tau_1 \ \wedge\ E[\gamma(e)] \Downarrow \implies E[\gamma(e')] \Downarrow$$

To prove completeness as before, we must show (1) that two contextually equivalent terms are ciu equivalent, and (2) that two ciu equivalent terms are logically related. It is straightforward to prove the first lemma:

Theorem 3.6 ($\lambda^{\forall\exists}$ **:** $\preceq^{ctx} \subseteq \preceq^{ciu}$)

If $\Delta;\Gamma \vdash e \preceq^{ctx} e' : \tau$ *then* $\Delta;\Gamma \vdash e \preceq^{ciu} e' : \tau$.

However, the proof of the second lemma (which states that two ciu equivalent terms are logically related) fails to go through. To see why, let us return to the proof of completeness of λ^{rec}, specifically to Lemma 2.10 which establishes that the relational value interpretation $\mathcal{RV}[\![\tau]\!]$ is equivalence-respecting: if $(k, v_1, v_2) \in \mathcal{RV}[\![\tau]\!]\emptyset$ and $\bullet \vdash v_2 \preceq^{ciu} v_3 : \tau$, then $(k, v_1, v_3) \in \mathcal{RV}[\![\tau]\!]\emptyset$. The proof of that lemma requires induction on k and nested induction on the structure of the closed type τ. In the case of $\lambda^{\forall\exists}$, when we get to the proof of the corresponding lemma, τ may have free type variables. Thus, one of the cases we must consider for the inner induction is $\tau = \alpha$. Assuming that $\rho(\alpha) = (\chi, \tau_\alpha)$, we will be required to show that if $(k, v_1, v_2) \in \mathcal{RV}[\![\alpha]\!]\rho \equiv \rho^{\mathsf{sem}}(\alpha) \equiv \chi$ and $\vdash v_2 \preceq^{ciu} v_3 : \alpha^{[\rho]}$ (where $\alpha^{[\rho]} \equiv \tau_\alpha$), then $(k, v_1, v_3) \in \chi$. This is where the proof for $\lambda^{\forall\exists}$ gets stuck. Note, however, that $\chi \in \mathit{Rel}_{\tau_\alpha}$. Thus, for the above proof to go through for $\lambda^{\forall\exists}$, we must add this requirement directly to the definition of Rel_τ. Hence, every set χ in Rel_τ must satisfy the *equivalence-respecting* property (in addition to closure under decreasing step-index and well-typedness of the second value of each tuple in χ).

A more informal justification for this change is that in the presence of quantified types, we can instantiate a type variable with a relational interpretation of our own choosing. Thus, we have to show that the relation we pick satisfies certain properties, one of which is that it must be equivalence-respecting.

The modified definition of Rel_τ is given below. It makes use of a notion of ciu-equivalence restricted to closed values. With the exception of the definition of Rel_τ, the logical relation is now defined exactly as in Figure 5.

$$v \prec^{ciu} v' : \tau \quad \stackrel{\text{def}}{=} \quad \forall E, \tau_1.\ \bullet;\bullet \vdash E : (\bullet;\bullet \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge\ E[v] \Downarrow \implies E[v'] \Downarrow$$

$$\begin{aligned} \mathit{Rel}_\tau \quad \stackrel{\text{def}}{=} \quad \{\chi \in 2^{Nat \times CValues \times CValues} \mid\ & \\ & \forall (j, v, v') \in \chi.\ \vdash v' : \tau \ \wedge \\ & \qquad \forall i \leq j.\ (i, v, v') \in \chi \ \wedge \\ & \qquad (\forall v''.\ v' \prec^{ciu} v'' : \tau \implies (j, v, v'') \in \chi)\} \end{aligned}$$

As before, we now prove that each type τ is a valid type ($\mathcal{RV}[\![\tau]\!]\rho \in \mathit{Rel}_{\tau^{[\rho]}}$), but now in addition to showing well-typedness and closure under decreasing step-index, we must also show that $\mathcal{RV}[\![\tau]\!]\rho$ is equivalence-respecting. Unfortunately, this property does not hold for existential types. (For details of how the proof fails, see Appendix E.2, proof of Lemma E.1, the case for existential types.)

Thus, the following lemma holds for the $\lambda^{\forall}$-calculus (λ^{rec} extended with universal types), but not for $\lambda^{\forall\exists}$.

Lemma 3.7 ($\lambda^{\forall}$ **Equivalence-Respecting)**

Let $\rho \in \mathcal{RD}[\![\Delta]\!]$ *and* $\Delta \vdash \tau$.
If $(k, v_1, v_2) \in \mathcal{RV}[\![\tau]\!]\rho$ *and* $v_2 \prec^{ciu} v_3 : \tau^{[\rho]}$, *then* $(k, v_1, v_3) \in \mathcal{RV}[\![\tau]\!]\rho$.

Note that the change in the definition of Rel_τ does not affect the proof of the fundamental theorem (for $\lambda^{\forall}$) or the proof of soundness with respect to contextual equivalence, which are proved exactly as before.

Since our relational interpretation of existential types fails to be equivalence-respecting, our logical relation is incomplete with respect to contextual equivalence in the presence of existential types. However, the relational interpretations of all the other types in $\lambda^{\forall\exists}$ (i.e., all types in $\lambda^{\forall}$) are equivalence-respecting. Thus, we are able to prove completeness with respect to contextual equivalence for the language $\lambda^{\forall}$.

Theorem 3.8 $(\lambda^{\forall}: \preceq^{ctx} \subseteq \preceq^{ciu} \subseteq \leq)$

If $\Delta; \Gamma \vdash e \preceq^{ctx} e' : \tau$ *then* $\Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau$.
If $\Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau$ *then* $\Delta; \Gamma \vdash e \leq e' : \tau$.

4 Related Work and Conclusion

Logical relations were first developed for denotational semantics of typed λ-calculi (e.g., [1, 2]). Early examples of the use of logical relations based on operational semantics include Tait's [4] proof of strong normalization of the simply typed λ-calculus, and Girard's method of reducibility candidates [5] used to prove normalization for System F.

Pitts [7, 6, 9] developed syntactic logical relations for a λ-calculus with recursive functions and quantified types (but no recursive types). To support recursive functions without using denotational techniques, Pitts makes use of $\top\top$-closure (or biorthogonality [12]). Relations that are $\top\top$-closed can be immediately shown to be equivalence-respecting and admissible [9]. We note that Pitts' logical relations do not support recursive types; at the end of [9], he poses syntactic logical relations for recursive types as an open problem in need of a fresh idea for further progress.

In this paper, we have shown that it is possible to construct a logical relation that is sound and complete with respect to contextual equivalence for a language with recursive functions, recursive types, and polymorphism, without the use of biorthogonality or $\top\top$-closure. For existential types, however, our logical relation is sound but not complete. We conjecture that it should be possible to combine the $\top\top$-closure and step-indexing techniques to obtain a sound and complete logical relation for a language with recursive and polymorphic types as well as existential types.

Birkedal and Harper [10] and Crary and Harper [8] extended syntactic logical relations with recursive types (the latter also support polymorphic types, but not existential types) by adapting Pitts' minimal invariance [3] technique for use in a purely syntactic setting. Melliès and Vouillon [12, 11] construct a realizability model of a language with recursive types and polymorphism based on intuitions from the ideal model of types [20]. They also present a relational model based on an orthogonality relation between quadruples of terms and contexts [12]. We note that to show completeness, they too must move to a typed setting. An issue that merits further investigation is the relationship between the different notions of approximation — i.e., syntactic projections [8], interval types [12], and step counts.

Contextual equivalence may also be proved using bisimulations. Sumii and Pierce [19] present a bisimulation for recursive and quantified types. Using their examples as a point of comparison (see Appendix D) we show that our logical relations are somewhat easier to use when proving contextual equivalence. Also, unlike logical relations, Sumii and Pierce note that their bisimulation cannot be used to derive free theorems [21] based only on types.

We have presented a step-indexed logical relation for recursive and impredicative quantified types. The construction is far more elementary than that of existing logical relations for such types. In future work, we intend to investigate the combination of $\top\top$-closure with step-indexing to obtain a logical relation for $\lambda^{\forall\exists}$ that is sound as well as complete with respect to contextual equivalence. We also hope to scale these techniques up to support dynamically allocated (ML-style) mutable references.

References

[1] Plotkin, G.D.: Lambda-definability and logical relations. Memorandum SAI–RM–4, University of Edinburgh, Edinburgh, Scotland (1973)

[2] Statman, R.: Logical relations and the typed λ-calculus. Information and Control **65**(2–3) (1985) 85–97

[3] Pitts, A.M.: Relational properties of domains. Information and Computation **127**(2) (1996) 66–90

[4] Tait, W.W.: Intensional interpretations of functionals of finite type i. Journal of Symbolic Logic **32**(2) (1967) 198–212

[5] Girard, J.Y.: Interprétation Fonctionnelle et Élimination des Coupures de l'Arithmétique d'Ordre Supérieur. Thèse de doctorat d'état, Université Paris VII, Paris, France (1972)

[6] Pitts, A.M.: Parametric polymorphism and operational equivalence. Mathematical Structures in Computer Science **10** (2000) 321–359

[7] Pitts, A.M.: Existential types: Logical relations and operational equivalence. Lecture Notes in Computer Science **1443** (1998) 309–326

[8] Crary, K., Harper, R.: Syntactic logical relations over polymorphic and recursive types. Draft (2000)

[9] Pitts, A.M.: Typed operational reasoning. In Pierce, B.C., ed.: Advanced Topics in Types and Programming Languages. MIT Press (2005)

[10] Birkedal, L., Harper, R.: Relational interpretations of recursive types in an operational setting. In: Theoretical Aspects of Computer Software (TACS). (1997)

[11] Melliès, P.A., Vouillon, J.: Semantic types: A fresh look at the ideal model for types. In: POPL, Venice, Italy. (2004)

[12] Melliès, P.A., Vouillon, J.: Recursive polymorphic types and parametricity in an operational framework. In: LICS, Chicago, Illinois. (2005)

[13] Appel, A.W., McAllester, D.: An indexed model of recursive types for foundational proof-carrying code. ACM TOPLAS **23**(5) (2001) 657–683

[14] Ahmed, A., Appel, A.W., Virga, R.: An indexed model of impredicative polymorphism and mutable references. Available at `http:// www.cs.princeton.edu/~appel/papers/impred.pdf` (2003)

[15] Ahmed, A.J.: Semantics of Types for Mutable State. PhD thesis, Princeton University (2004)

[16] Ahmed, A.: Step-indexed syntactic logical relations for recursive and quantified types. Technical Report TR-01-06, Harvard University (2006)

[17] Pierce, B.C.: Types and Programming Languages. MIT Press (2002)

[18] Mason, I.A., Talcott, C.L.: Equivalence in functional languages with effects. Journal of Functional Programming **1**(3) (1991) 287–327

[19] Sumii, E., Pierce, B.C.: A bisimulation for type abstraction and recursion. In: POPL, Long Beach, California. (2005) 63–74

[20] MacQueen, D., Plotkin, G., Sethi, R.: An ideal model for recursive polymophic types. Information and Computation **71**(1/2) (1986) 95–130

[21] Wadler, P.: Theorems for free! In: ACM Symposium on Functional Programming Languages and Computer Architecture (FPCA), London (1989)

Appendix: Formal Development

The following appendices present a formal development of the calculi, relational models, and proofs described in the main body of this technical report, as well as additional examples.

In Appendix A, we present the Appel-McAllester model [13] and show how a direct proof of transitivity fails to go through. In Appendix B, we present a logical relation for (iso-)recursive types and show that the relation is transitive, as well as sound and complete with respect to contextual equivalence. In Appendix C, we present a logical relation for a language with recursive, polymorphic, and existential types that is sound but incomplete with respect to contextual equivalence. Appendix D presents a number of examples involving existential packages, higher-order functions, universal types and contravariant recursive types. In Appendix E we present a slight modification of the logical relation from Appendix C and show that in the absence of existential types it is sound and complete with respect to contextual equivalence.

A Appel-McAllester Indexed PER Model (Equi-Recursive Types)

This section gives all the relevant definitions for the Appel-McAllester model (using notational conventions from [13]) and summarizes the lemmas that should hold of the model. Section A.1 illustrates how a direct proof of transitivity fails to go through.

$$
\begin{array}{lrcl}
\textit{Expressions} & e & ::= & x \mid \mathbf{0} \mid \langle e_1, e_2 \rangle \mid \pi_1(e) \mid \pi_2(e) \mid \lambda x.\, e \mid e_1\, e_2 \\
\textit{Values} & v & ::= & x \mid \mathbf{0} \mid \langle v_1, v_2 \rangle \mid \lambda x.\, e \\
\textit{Types} & \tau & ::= & \bot \mid \mathsf{int} \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \mu F
\end{array}
$$

Figure 6: Appel-McAllester: Syntax

$$
\frac{e_1 \longmapsto e_1'}{e_1\, e_2 \longmapsto e_1'\, e_2} \qquad \frac{e_2 \longmapsto e_2'}{(\lambda x.\, e_1)\, e_2 \longmapsto \lambda x.\, e_1\, e_2'} \qquad \frac{}{(\lambda x.\, e)\, v \longmapsto e[v/x]}
$$

$$
\frac{e_1 \longmapsto e_1'}{\langle e_1, e_2 \rangle \longmapsto \langle e_1', e_2 \rangle} \qquad \frac{e_2 \longmapsto e_2'}{\langle v_1, e_2 \rangle \longmapsto \langle v_1, e_2' \rangle} \qquad \frac{}{\pi_1 \langle v_1, v_2 \rangle \longmapsto v_1} \qquad \frac{}{\pi_2 \langle v_1, v_2 \rangle \longmapsto v_2}
$$

Figure 7: Appel-McAllester: Operational Semantics

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

$$
(\mathsf{Var})\ \frac{}{\Gamma \vdash x : \Gamma(x)} \qquad (\mathsf{Zero})\ \frac{}{\Gamma \vdash \mathbf{0} : \mathsf{int}}
$$

$$
(\mathsf{Fun})\ \frac{\Gamma, x{:}\tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x.\, e : \tau_1 \to \tau_2} \qquad (\mathsf{App})\ \frac{\Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\, e_2 : \tau_2}
$$

$$
(\mathsf{Pair})\ \frac{\Gamma \vdash e_1 : \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash \langle e_1, e_2 \rangle : \tau_1 \times \tau_2} \qquad (\mathsf{Proj1})\ \frac{\Gamma \vdash e : \tau_1 \times \tau_2}{\Gamma \vdash \pi_1(e) : \tau_1} \qquad (\mathsf{Proj2})\ \frac{\Gamma \vdash e : \tau_1 \times \tau_2}{\Gamma \vdash \pi_2(e) : \tau_2}
$$

$$
(\mathsf{Fold})\ \frac{\Gamma \vdash e : F(\mu F)}{\Gamma \vdash e : \mu F} \qquad (\mathsf{Unfold})\ \frac{\Gamma \vdash e : \mu F}{\Gamma \vdash e : F(\mu F)}
$$

Figure 8: Appel-McAllester: Static Semantics

$$
\begin{array}{rcl}
\bot & \equiv & \{\} \\
\mathsf{int} & \equiv & \{(k, \mathbf{0}, \mathbf{0})\} \\
\tau_1 \times \tau_2 & \equiv & \{(k, \langle v_1, v_2\rangle, \langle v_1', v_2'\rangle) \mid \forall j < k.\ (j, v_1, v_1') \in \tau_1 \wedge (j, v_2, v_2') \in \tau_2\} \\
\tau_1 \to \tau_2 & \equiv & \{(k, \lambda x.\, e, \lambda x.\, e') \mid \forall j < k, v, v'.\ (j, v, v') \in \tau_1 \implies e[v/x] \leq e'[v'/x] :_j \tau_2\} \\
\mu F & \equiv & \{(k, v, v') \mid (k, v, v') \in F^{k+1}(\bot)\}
\end{array}
$$

$$
\begin{array}{rcl}
e \leq e' :_k \tau & \equiv & \forall j < k, e_f.\ e \longmapsto^j e_f \wedge \mathit{irred}(e_f) \implies \\
& & \qquad \exists e_f'.\ e' \longmapsto^* e_f' \wedge (k - j, e_f, e_f') \in \tau
\end{array}
$$

$$
\begin{array}{rcl}
\gamma \leq \gamma' :_k \Gamma & \equiv & \mathit{dom}(\gamma) = \mathit{dom}(\gamma') = \mathit{dom}(\Gamma) \wedge \\
& & \forall x \in \mathit{dom}(\Gamma).\ \gamma(x) \leq \gamma'(x) :_k \Gamma(x)
\end{array}
$$

$$
\Gamma \vDash e \leq e' : \tau \quad \equiv \quad \forall k \geq 0.\ \forall \gamma, \gamma'.\ \gamma \leq \gamma' :_k \Gamma \implies \gamma(e) \leq \gamma'(e') :_k \tau
$$

$$
\Gamma \vDash e \sim e' : \tau \quad \equiv \quad \Gamma \vDash e \leq e' : \tau \ \wedge\ \Gamma \vDash e' \leq e : \tau
$$

Figure 9: Appel-McAllester: Indexed PER Model [13]

$\boxed{\Gamma \vDash e \sim e' : \tau}$

$$
(\textit{Reflexivity})\ \frac{\Gamma \vDash e : \tau}{\Gamma \vDash e \sim e : \tau} \qquad (\textit{Symmetry})\ \frac{\Gamma \vDash e \sim e' : \tau}{\Gamma \vDash e' \sim e : \tau} \qquad (\textit{Transitivity})\ \frac{\Gamma \vDash e_1 \sim e_2 : \tau \qquad \Gamma \vDash e_2 \sim e_3 : \tau}{\Gamma \vDash e_1 \sim e_3 : \tau}
$$

$$
(\textit{Substitutivity})\ \frac{\Gamma \vDash v \sim v' : \tau_1 \qquad \Gamma, x{:}\tau_1 \vDash e \sim e' : \tau_2}{\Gamma \vDash e[v/x] \sim e'[v'/x] : \tau_2}
$$

(*Compatibility Properties*)

$$
(\mathsf{Var})\ \frac{\Gamma(x) = \tau}{\Gamma \vDash x \sim x : \tau} \qquad (\mathsf{Zero})\ \frac{}{\Gamma \vDash \mathbf{0} \sim \mathbf{0} : \mathsf{int}}
$$

$$
(\mathsf{Fun})\ \frac{\Gamma, x{:}\tau_1 \vDash e \sim e' : \tau_2}{\Gamma \vDash \lambda x.\, e \sim \lambda x.\, e' : \tau_1 \to \tau_2} \qquad (\mathsf{App})\ \frac{\Gamma \vDash e_1 \sim e_1' : \tau_1 \to \tau_2 \qquad \Gamma \vDash e_2 \sim e_2' : \tau_1}{\Gamma \vDash e_1\, e_2 \sim e_1'\, e_2' : \tau_2}
$$

$$
(\mathsf{Pair})\ \frac{\Gamma \vDash e_1 \sim e_1' : \tau_1 \qquad \Gamma \vDash e_2 \sim e_2' : \tau_2}{\Gamma \vDash \langle e_1, e_2\rangle \sim \langle e_1', e_2'\rangle : \tau_1 \times \tau_2}
$$

$$
(\mathsf{Proj1})\ \frac{\Gamma \vDash e \sim e' : \tau_1 \times \tau_2}{\Gamma \vDash \pi_1(e) \sim \pi_1(e') : \tau_1} \qquad (\mathsf{Proj2})\ \frac{\Gamma \vDash e \sim e' : \tau_1 \times \tau_2}{\Gamma \vDash \pi_2(e) \sim \pi_2(e') : \tau_2}
$$

$$
(\mathsf{Fold})\ \frac{\Gamma \vDash e \sim e' : F(\mu F)}{\Gamma \vDash e \sim e' : \mu F} \qquad (\mathsf{Unfold})\ \frac{\Gamma \vDash e \sim e' : \mu F}{\Gamma \vDash e \sim e' : F(\mu F)}
$$

Note: $\sim$ is an equivalence relation if it satisfies the reflexivity, symmetry and transitivity properties. It is a congruence relation if it satisfies the substitutivity and compatibility properties.

Figure 10: Appel-McAllester: Properties Required of $\sim$

A.1 Appel-McAllester: Proof of Transitivity Fails

With the exception of transitivity, all of the lemmas shown in Figure 10 are directly provable in the Appel-McAllester model [13]. A direct proof of transitivity, however, does not go through.

Proposed Lemma (Transitivity)
If $\Gamma \vDash e_1 \leq e_2 : \tau$ *and* $\Gamma \vDash e_2 \leq e_3 : \tau$ *then* $\Gamma \vDash e_1 \leq e_3 : \tau$.

Proof Attempt: We are required to show $\Gamma \vDash e_1 \leq e_3 : \tau$.
Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $\gamma \leq \gamma' :_k \Gamma$.

We are required to show that $\gamma(e_1) \leq \gamma'(e_3) :_k \tau$.
Consider arbitrary j, e_{f_1} such that

- $j < k$,
- $\gamma(e_1) \longmapsto^j e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

We are required to show that $\exists e_{f_3}.\ \gamma'(e_3) \longmapsto^* e_{f_3} \ \wedge\ (k-j, e_{f_1}, e_{f_3}) \in \tau$.
Instantiate $\Gamma \vDash e_1 \leq e_2 : \tau$ with k, γ, γ'. Note that

- $k \geq 0$, and
- $\gamma \leq \gamma' :_k \Gamma$.

Hence, $\gamma(e_1) \leq \gamma'(e_2) :_k \tau$.
Instantiate this with j, e_{f_1}. Note that

- $j < k$,
- $\gamma(e_1) \longmapsto^j e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exist e_{f_2}, i, such that

- $i \geq 0$,
- $\gamma'(e_2) \longmapsto^i e_{f_2}$, and
- $\mathit{irred}(e_{f_2})$.

Now we would like to use the second hypothesis $\Gamma \vDash e_2 \leq e_3 : \tau$.
But what index should we instantiate this with? There are two possible ways to proceed.

(i) Instantiate $\Gamma \vDash e_2 \leq e_3 : \tau$ with k, γ, and γ'. Note that

- $k \geq 0$, and
- $\gamma \leq \gamma' :_k \Gamma$.

Hence, $\gamma(e_2) \leq \gamma'(e_3) :_k \tau$.

Problem: We could instantiate this with i and e_{f2}. But at that point we are stuck since:

- we cannot show $i < k$, as i may be greater than k, and
- we cannot show $\gamma(e_2) \longmapsto^i e_{f2}$, as we only have $\gamma'(e_2) \longmapsto^i e_{f2}$.

(ii) Instantiate $\Gamma \vDash e_2 \leq e_3 : \tau$ with some z such that $z > i$, γ', and γ'.

Problem: We cannot show $\gamma' \leq \gamma' :_z \Gamma$. All we know is that $\gamma \leq \gamma' :_k \Gamma$, where $z > i$ and i may be greater than k.

B Iso-Recursive Types

$$
\begin{array}{llll}
\textit{Types} & \tau & ::= & \mathsf{bool} \mid \tau_1 \to \tau_2 \mid \alpha \mid \mu\alpha.\,\tau \\
\textit{Expressions} & e & ::= & x \mid \mathtt{tt} \mid \mathtt{ff} \mid \mathtt{if}\, e_0, e_1, e_2 \mid \\
 & & & \lambda x.\, e \mid e_1\, e_2 \mid \mathtt{fold}\, e \mid \mathtt{unfold}\, e \\
\textit{Values} & v & ::= & x \mid \mathtt{tt} \mid \mathtt{ff} \mid \lambda x.\, e \mid \mathtt{fold}\, v
\end{array}
$$

Figure 1: λ^{rec} Syntax

$$
\textit{Evaluation Contexts} \quad E \quad ::= \quad [\cdot] \mid \mathtt{if}\, E, e_1, e_2 \mid E\, e \mid v\, E \mid \mathtt{fold}\, E \mid \mathtt{unfold}\, E
$$

$$
\begin{array}{lrcl}
(\mathsf{iftrue}) & \mathtt{if}\, \mathtt{tt}, e_1, e_2 & \longmapsto & e_1 \\
(\mathsf{iffalse}) & \mathtt{if}\, \mathtt{ff}, e_1, e_2 & \longmapsto & e_2 \\
(\mathsf{app}) & (\lambda x.\, e)\, v & \longmapsto & e[v/x] \\
(\mathsf{unfold}) & \mathtt{unfold}\, (\mathtt{fold}\, v) & \longmapsto & v \\
(\mathsf{ctxt}) & \multicolumn{3}{c}{\dfrac{e \longmapsto e'}{E[e] \longmapsto E[e']}}
\end{array}
$$

Figure 2: λ^{rec} Operational Semantics

Notation The notation $e \longmapsto e'$ denotes a single operational step. We write $e \longmapsto^j e'$ to denote that there exists a chain of j steps of the form $e \longmapsto e_1 \longmapsto \ldots \longmapsto e_j$ where e_j is e'. A term e is irreducible (written $\mathit{irred}(e)$) if it has no successor in the step relation — that is, if e is a value (written $\mathit{val}(e)$) or if e is a "stuck" expression (such as $\mathtt{tt}(e')$) to which no operational rule applies. We also use the following abbreviations.

$$
\begin{array}{rcl}
e \longmapsto^* e' & \stackrel{\text{def}}{=} & \exists k \geq 0.\ e \longmapsto^k e' \\
e \Downarrow e' & \stackrel{\text{def}}{=} & e \longmapsto^* e' \wedge \mathit{val}(e') \\
e \Downarrow & \stackrel{\text{def}}{=} & \exists e'.\, e \Downarrow e' \\
e \Uparrow & \stackrel{\text{def}}{=} & \forall k \geq 0.\, \exists e'.\, e \longmapsto^k e'
\end{array}
$$

Type Context $\Delta \quad ::= \quad \bullet \mid \Delta, \alpha$

$\boxed{\Delta \vdash \tau}$

$$(\mathsf{VarTy})\ \frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad (\mathsf{BoolTy})\ \frac{}{\Delta \vdash \mathsf{bool}} \qquad (\mathsf{FnTy})\ \frac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 \to \tau_2} \qquad (\mathsf{RecTy})\ \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \mu\alpha.\,\tau}$$

Figure 3: λ^{rec} Static Semantics I

Value Context $\Gamma \quad ::= \quad \bullet \mid \Gamma, x{:}\tau \qquad\qquad$ *where* $\bullet \vdash \tau$

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

$$(\mathsf{True})\ \frac{}{\Gamma \vdash \mathtt{tt} : \mathsf{bool}} \qquad (\mathsf{False})\ \frac{}{\Gamma \vdash \mathtt{ff} : \mathsf{bool}} \qquad (\mathsf{If})\ \frac{\Gamma \vdash e_0 : \mathsf{bool} \qquad \Gamma \vdash e_1 : \tau \qquad \Gamma \vdash e_2 : \tau}{\Gamma \vdash \mathtt{if}\, e_0, e_1, e_2 : \tau}$$

$$(\mathsf{Var})\ \frac{}{\Gamma \vdash x : \Gamma(x)} \qquad (\mathsf{Fn})\ \frac{\Gamma, x{:}\tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x.\, e : \tau_1 \to \tau_2} \qquad (\mathsf{App})\ \frac{\Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\, e_2 : \tau_2}$$

$$(\mathsf{Fold})\ \frac{\Gamma \vdash e : \tau[\mu\alpha.\,\tau/\alpha]}{\Gamma \vdash \mathtt{fold}\, e : \mu\alpha.\,\tau} \qquad (\mathsf{Unfold})\ \frac{\Gamma \vdash e : \mu\alpha.\,\tau}{\Gamma \vdash \mathtt{unfold}\, e : \tau[\mu\alpha.\,\tau/\alpha]}$$

Figure 4: λ^{rec} Static Semantics II

B.1 λ^{rec} Unary Model

Notation

- We write $\mathcal{V}\,[\![\tau]\!]$ for the semantic interpretation of types as values, $\mathcal{C}\,[\![\tau]\!]$ for the interpretation of types as computations, and $\mathcal{G}\,[\![\Gamma]\!]$ for the interpretation of contexts as substitutions (Figure 5).
- We use the metavariable σ to range over sets of tuples of the form (k, v) where k is a natural number and v is a closed value — i.e., $k \in \mathit{Nat}$ and $v \in \mathit{CValues}$.
- We use δ for mappings from type variables α to sets $\sigma \in 2^{\mathit{Nat} \times \mathit{CValues}}$.

$$\mathit{Type} \stackrel{\text{def}}{=} \{\sigma \in 2^{\mathit{Nat}\times\mathit{CValues}} \mid \forall (j,v) \in \sigma.\ \forall i \leq j.\ (i,v) \in \sigma\}$$

$$\lfloor \sigma \rfloor_k \stackrel{\text{def}}{=} \{(j,v) \mid j < k \ \wedge\ (j,v) \in \sigma\}$$

$$\begin{array}{rcl}
\mathcal{V}\,[\![\alpha]\!]\,\delta & = & \delta(\alpha) \\
\mathcal{V}\,[\![\mathsf{bool}]\!]\,\delta & = & \{(k,v) \mid v = \mathtt{tt} \ \vee\ v = \mathtt{ff}\} \\
\mathcal{V}\,[\![\tau_1 \to \tau_2]\!]\,\delta & = & \{(k, \lambda x.\, e) \mid \forall j < k, v. \\
 & & \qquad (j,v) \in \mathcal{V}\,[\![\tau_1]\!]\,\delta \implies \\
 & & \qquad (j, e[v/x]) \in \mathcal{C}\,[\![\tau_2]\!]\,\delta\} \\
\mathcal{V}\,[\![\mu\alpha.\,\tau]\!]\,\delta & = & \{(k, \mathtt{fold}\, v) \mid \forall j < k. \\
 & & \qquad \text{let } \sigma = \lfloor \mathcal{V}\,[\![\mu\alpha.\,\tau]\!]\,\delta \rfloor_{j+1} \text{ in} \\
 & & \qquad (j,v) \in \mathcal{V}\,[\![\tau]\!]\,\delta[\alpha \mapsto \sigma]\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{C}\,[\![\tau]\!]\,\delta & = & \{(k,e) \mid \forall j < k, e_f. \\
 & & \qquad e \longmapsto^j e_f \wedge \mathit{irred}(e_f) \implies \\
 & & \qquad (k-j, e_f) \in \mathcal{V}\,[\![\tau]\!]\,\delta\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{G}\,[\![\bullet]\!] & = & \{(k, \emptyset)\} \\
\mathcal{G}\,[\![\Gamma, x:\tau]\!] & = & \{(k, \gamma[x \mapsto v]) \mid \\
 & & \qquad (k,\gamma) \in \mathcal{G}\,[\![\Gamma]\!] \wedge (k,v) \in \mathcal{V}\,[\![\tau]\!]\,\emptyset\}
\end{array}$$

$$[\![\Gamma \vdash e : \tau]\!] = \forall k \geq 0.\ \forall \gamma.\ (k,\gamma) \in \mathcal{G}\,[\![\Gamma]\!] \implies (k, \gamma(e)) \in \mathcal{C}\,[\![\tau]\!]\,\emptyset$$

Figure 5: λ^{rec} Step-Indexed Unary Model

$$\begin{array}{rcl}
\mathcal{D}\,[\![\bullet]\!] & = & \{\emptyset \mid \mathbf{True}\} \\
\mathcal{D}\,[\![\Delta, \alpha]\!] & = & \{\delta[\alpha \mapsto \sigma] \mid \delta \in \mathcal{D}\,[\![\Delta]\!] \ \wedge\ \sigma \in \mathit{Type}\}
\end{array}$$

Figure 6: λ^{rec} Step-Indexed Unary Model (Additional Notation for Proofs)

B.2 λ^{rec} Relational (PER) Model

Notation

- We write $\mathcal{RV}\,[\![\tau]\!]$ for the relational interpretation of types as values, $\mathcal{RC}\,[\![\tau]\!]$ for the relational interpretation of types as computations, and $\mathcal{RG}\,[\![\Gamma]\!]$ for the relational interpretation of contexts as substitutions (Figure 7).
- We use the metavariable χ to range over sets of tuples of the form (k, v, v') where k is a natural number and v, v' are closed values — i.e., $k \in \mathit{Nat}$ and $v, v' \in \mathit{CValues}$.
- We use ρ for mappings from type variables α to pairs (χ, τ) of sets $\chi \in 2^{\mathit{Nat} \times \mathit{CValues} \times \mathit{CValues}}$ and syntactic types τ.
- If $\rho(\alpha) = (\chi, \tau)$, the notation $\rho^{\mathsf{sem}}(\alpha)$ denotes χ, while $\rho^{\mathsf{syn}}(\alpha)$ denotes τ.
- If $\mathit{dom}(\gamma) = \mathit{dom}(\Gamma)$, we use $\vdash \gamma : \Gamma$ as shorthand for $\forall x \in \mathit{dom}(\Gamma).\ \bullet \vdash \gamma(x) : \Gamma(x)$.
- If $\rho = \{\alpha_1 \mapsto (\chi_1, \tau_1), \ldots, \alpha_n \mapsto (\chi_n, \tau_n)\}$, the notation $\tau^{[\rho]}$ is an abbreviation for $\tau[\tau_1/\alpha_1, \tau_2/\alpha_2, \ldots, \tau_n/\alpha_n]$.

$$Rel_\tau \stackrel{\text{def}}{=} \{\chi \in 2^{Nat \times CValues \times CValues} \mid \forall (j,v,v') \in \chi. \; \bullet \vdash v' : \tau \;\wedge\; \forall i \leq j.\ (i,v,v') \in \chi\}$$

$$\lfloor \chi \rfloor_k \stackrel{\text{def}}{=} \{(j,v,v') \mid j < k \;\wedge\; (j,v,v') \in \chi\}$$

$$\begin{array}{rcl}
\mathcal{RV}\,[\![\alpha]\!]\,\rho & = & \rho^{\mathsf{sem}}(\alpha) \\
\mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho & = & \{(k,v,v') \mid \bullet \vdash v' : \mathsf{bool} \;\wedge\; (v = v' = \mathtt{tt} \;\vee\; v = v' = \mathtt{ff})\} \\
\mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho & = & \{(k, \lambda x.\, e, \lambda x.\, e') \mid \bullet \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]} \;\wedge\; \forall j < k, v, v'. \\
 & & \quad (j,v,v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho \implies (j, e[v/x], e'[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho\} \\
\mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\rho & = & \{(k, \mathtt{fold}\,v, \mathtt{fold}\,v') \mid \bullet \vdash \mathtt{fold}\,v' : (\mu\alpha.\,\tau)^{[\rho]} \;\wedge\; \forall j < k. \\
 & & \quad \text{let } \chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\rho \rfloor_{j+1} \text{ in} \\
 & & \quad (j,v,v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi,\ (\mu\alpha.\,\tau)^{[\rho]})]\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{RC}\,[\![\tau]\!]\,\rho & = & \{(k,e,e') \mid \forall j < k, e_f. \\
 & & \quad e \longmapsto^j e_f \wedge \mathit{irred}(e_f) \implies \exists e'_f.\ e' \longmapsto^* e'_f \wedge (k-j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau]\!]\,\rho\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{RG}\,[\![\bullet]\!] & = & \{(k, \emptyset, \emptyset)\} \\
\mathcal{RG}\,[\![\Gamma, x : \tau]\!] & = & \{(k, \gamma[x \mapsto v], \gamma'[x \mapsto v']) \mid \\
 & & \quad (k,\gamma,\gamma') \in \mathcal{RG}\,[\![\Gamma]\!] \wedge (k,v,v') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset\}
\end{array}$$

$$\begin{array}{rcl}
\Gamma \vdash e \leq e' : \tau & \stackrel{\text{def}}{=} & \Gamma \vdash e : \tau \;\wedge\; \Gamma \vdash e' : \tau \;\wedge\; \forall k \geq 0.\ \forall \gamma, \gamma'. \\
 & & \quad (k,\gamma,\gamma') \in \mathcal{RG}\,[\![\Gamma]\!] \implies (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset
\end{array}$$

$$\Gamma \vdash e \sim e' : \tau \stackrel{\text{def}}{=} \Gamma \vdash e \leq e' : \tau \;\wedge\; \Gamma \vdash e' \leq e : \tau$$

Figure 7: λ^{rec} Step-Indexed Relational Model (Shaded = Not in Appel-McAllester)

$$\begin{array}{rcl}
\mathcal{RD}\,[\![\bullet]\!] & = & \{\emptyset\} \\
\mathcal{RD}\,[\![\Delta, \alpha]\!] & = & \{\rho[\alpha \mapsto (\chi, \tau)] \mid \rho \in \mathcal{RD}\,[\![\Delta]\!] \;\wedge\; \chi \in \mathit{Rel}_\tau\}
\end{array}$$

Figure 8: λ^{rec} Step-Indexed Relational Model (Additional Notation for Proofs)

B.3 λ^{rec} Contexts and Contextual Equivalence

$$\begin{array}{lrcl} \textit{Contexts} & C & ::= & [\cdot] \mid \mathtt{if}\, C, e_1, e_2 \mid \mathtt{if}\, e_0, C, e_2 \mid \mathtt{if}\, e_0, e_1, C \mid \\ & & & \lambda x.\, C \mid C\, e \mid e\, C \mid \mathtt{fold}\, C \mid \mathtt{unfold}\, C \end{array}$$

Figure 9: λ^{rec} Syntax - Contexts

$\boxed{\Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau'}$

$$(\mathsf{C\text{-}id})\ \frac{}{\Gamma' \vdash [\cdot] : (\Gamma \triangleright \tau) \rightsquigarrow \tau}\ (\Gamma' \supseteq \Gamma) \qquad (\mathsf{C\text{-}if1})\ \frac{\Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \mathsf{bool} \qquad \Gamma' \vdash e_1 : \tau' \qquad \Gamma' \vdash e_2 : \tau'}{\Gamma' \vdash \mathtt{if}\, C, e_1, e_2 : (\Gamma \triangleright \tau) \rightsquigarrow \tau'}$$

$$(\mathsf{C\text{-}if2})\ \frac{\Gamma' \vdash e_0 : \mathsf{bool} \qquad \Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau' \qquad \Gamma' \vdash e_2 : \tau'}{\Gamma' \vdash \mathtt{if}\, e_0, C, e_2 : (\Gamma \triangleright \tau) \rightsquigarrow \tau'}$$

$$(\mathsf{C\text{-}if3})\ \frac{\Gamma' \vdash e_0 : \mathsf{bool} \qquad \Gamma' \vdash e_1 : \tau' \qquad \Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau'}{\Gamma' \vdash \mathtt{if}\, e_0, e_1, C : (\Gamma \triangleright \tau) \rightsquigarrow \tau'} \qquad (\mathsf{C\text{-}fn})\ \frac{\Gamma', x : \tau_1 \vdash C : (\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2}{\Gamma' \vdash \lambda x.\, C : (\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)}$$

$$(\mathsf{C\text{-}app1})\ \frac{\Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2) \qquad \Gamma' \vdash e : \tau_1}{\Gamma' \vdash C\, e : (\Gamma \triangleright \tau) \rightsquigarrow \tau_2} \qquad (\mathsf{C\text{-}app2})\ \frac{\Gamma' \vdash e : \tau_1 \to \tau_2 \qquad \Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1}{\Gamma' \vdash e\, C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_2}$$

$$(\mathsf{C\text{-}fold})\ \frac{\Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau'[\mu\alpha.\, \tau'/\alpha]}{\Gamma' \vdash \mathtt{fold}\, C : (\Gamma \triangleright \tau) \rightsquigarrow \mu\alpha.\, \tau'} \qquad (\mathsf{C\text{-}unfold})\ \frac{\Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \mu\alpha.\, \tau'}{\Gamma' \vdash \mathtt{unfold}\, C : (\Gamma \triangleright \tau) \rightsquigarrow \tau'[\mu\alpha.\, \tau'/\alpha]}$$

$$(\mathsf{C\text{-}ctxt})\ \frac{\Gamma' \vdash C : (\Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau' \qquad \Gamma_1 \vdash C_1 : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1}{\Gamma' \vdash C[C_1[\cdot]] : (\Gamma \triangleright \tau) \rightsquigarrow \tau'}$$

$\boxed{\Gamma' \vdash C[e] : \tau'}$

$$(\mathsf{C\text{-}exp})\ \frac{\Gamma' \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau' \qquad \Gamma \vdash e : \tau}{\Gamma' \vdash C[e] : \tau'}$$

Figure 10: λ^{rec} Static Semantics - Contexts

Definition B.1 (Contextual Approximation ($\preceq^{ctx}$) and Equivalence ($\simeq^{ctx}$))

Let e and e' be expressions such that $\Gamma \vdash e : \tau$ and $\Gamma \vdash e' : \tau$.

$$\Gamma \vdash e \preceq^{ctx} e' : \tau \quad \stackrel{\text{def}}{=} \quad \forall C, \tau_1.\ \bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge\ C[e] \Downarrow \implies C[e'] \Downarrow$$

$$\Gamma \vdash e \simeq^{ctx} e' : \tau \quad \stackrel{\text{def}}{=} \quad \begin{array}{l} \Gamma \vdash e \preceq^{ctx} e' : \tau \ \wedge \\ \Gamma \vdash e' \preceq^{ctx} e : \tau \end{array}$$

Figure 11: λ^{rec} Contextual Approximation and Equivalence

Note: To prove that our logical relation ($\leq$) is sound with respect to contextual equivalence ($\preceq^{ctx}$) (see Section B.11), we first define what it means for two contexts to be logically related as follows:

$$\Gamma_1 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \quad \stackrel{\text{def}}{=} \quad \forall e, e'.\ \Gamma \vdash e \leq e' : \tau \implies \Gamma_1 \vdash C[e] \leq C'[e'] : \tau_1$$

$$\Gamma_1 \vdash C \sim C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \quad \stackrel{\text{def}}{=} \quad \begin{array}{l} \Gamma_1 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge \\ \Gamma_1 \vdash C' \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \end{array}$$

Figure 12: λ^{rec} Step-Indexed Logical Relation: Contexts

B.4 λ^{rec} Evaluation Contexts and Ciu Equivalence

- The syntax of λ^{rec} evaluation contexts E is given in Figure 2.
- Note that evaluation contexts E are simply a subset of general contexts C and that only closed terms can be placed in an evaluation context. Hence, typing judgments for evaluation contexts have the form $\Gamma_1 \vdash (\bullet \triangleright \tau) \rightsquigarrow \tau_1$.

Definition B.2 (Ciu Approximation ($\preceq^{ciu}$) and Equivalence ($\simeq^{ciu}$))

Let e and e' be expressions such that $\Gamma \vdash e : \tau$ and $\Gamma \vdash e' : \tau$.

$$\Gamma \vdash e \preceq^{ciu} e' : \tau \quad \stackrel{\text{def}}{=} \quad \forall \gamma, E, \tau_1. \; \vdash \gamma : \Gamma \;\wedge\; \bullet \vdash E : (\bullet \triangleright \tau) \rightsquigarrow \tau_1 \;\wedge\; E[\gamma(e)] \Downarrow \implies E[\gamma(e')] \Downarrow$$

$$\Gamma \vdash e \simeq^{ciu} e' : \tau \quad \stackrel{\text{def}}{=} \quad \Gamma \vdash e \preceq^{ciu} e' : \tau \;\wedge\; \Gamma \vdash e' \preceq^{ciu} e : \tau$$

Figure 13: λ^{rec} Ciu Approximation and Equivalence

B.5 λ^{rec} Proofs: Type Soundness and Substitution

Lemma B.3 (λ^{rec} **Valid Type:** $\mathcal{V}\,[\![\tau]\!]\,\delta \in \mathit{Type}$)

Let $\delta \in \mathcal{D}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau$.
Then $\mathcal{V}\,[\![\tau]\!]\,\delta \in \mathit{Type}$.

Proof

By the definition of *Type*, it suffices to show:

$$\forall (k, v) \in \mathcal{V}\,[\![\tau]\!]\,\delta.\ \forall j \leq k.\ (j, v) \in \mathcal{V}\,[\![\tau]\!]\,\delta$$

The proof is by induction on the derivation $\Delta \vdash \tau$. □

Lemma B.4 (λ^{rec} **Safety**)

If $\bullet \vdash e : \tau$ *and* $e \longmapsto^* e'$, *then either* e' *is a value, or there exists an* e'' *such that* $e' \longmapsto e''$.

Proof

Prove the soundness of each typing rule using the unary indexed model of λ^{rec} (Figure 5). □

Lemma B.5 (λ^{rec} **Substitution**)

If $\Gamma \vdash v : \tau_1$ *and* $\Gamma, x : \tau_1 \vdash e : \tau_2$,
then $\Gamma \vdash e[v/x] : \tau_2$.

Proof

□

B.6 λ^{rec} Proofs: Validity of Pers

Lemma B.6 (λ^{rec} Per Values Well-Typed)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau$.
If $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$,
then $\bullet \vdash v' : \tau^{[\rho]}$.

Proof

By induction on the derivation $\Delta \vdash \tau$.

We only show the (VarTy) case.

In each of the remaining cases, the result is immediate from the definition of $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, which requires that $\bullet \vdash v' : \tau^{[\rho]}$.

Case (VarTy) $\dfrac{\alpha \in \Delta}{\Delta \vdash \alpha}$:

Note that $\alpha^{[\rho]} \equiv \rho^{\mathsf{syn}}(\alpha)$.
Hence, we are required to show that $\bullet \vdash v' : \rho^{\mathsf{syn}}(\alpha)$.
Note that from $(k, v, v') \in \mathcal{RV}\,[\![\alpha]\!]\,\rho$ it follows that $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.
Note that from $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\alpha \in \Delta$ it follows that there exists τ such that

- $\rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_\tau$, and
- $\rho^{\mathsf{syn}}(\alpha) \equiv \tau$.

By the definition of Rel_τ, since $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_\tau$, it follows that $\bullet \vdash v' : \tau$.
Hence, $\bullet \vdash v' : \rho^{\mathsf{syn}}(\alpha)$.

□

Lemma B.7 (λ^{rec} Per Value-Context Substitutions Well-Typed)

If $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
then $\vdash \gamma' : \Gamma$.

Proof

By induction on Γ.

Case $\Gamma = \bullet$:
From $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\bullet]\!]$ we conclude that $\gamma = \gamma' = \emptyset$.
Hence, we are required to show that $\bullet \vdash \emptyset : \bullet$, which follows trivially.

Case $\Gamma = \Gamma_1, x : \tau$, where $\bullet \vdash \tau$:
From $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma_1, x : \tau]\!]$ we conclude that there exist γ_1, γ_1', v, and v' such that

- $\gamma \equiv \gamma_1[x \mapsto v]$,
- $\gamma' \equiv \gamma_1'[x \mapsto v']$,
- $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]$, and
- $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

Hence, we are required to show that $\vdash \gamma_1'[x \mapsto v'] : \Gamma_1, x : \tau$,
which follows from

- $\vdash \gamma_1' : \Gamma_1$,
  which follows from the induction hypothesis applied to $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]$, and
- $\bullet \vdash v' : \tau$,
  which follows from Lemma B.6 applied to $\bullet \vdash \tau$ and $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

□

Lemma B.8 (λ^{rec} Per Types Downward Closed)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau$.
If $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$ *and* $j \leq k$,
then $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

Proof

The proof is by induction on the derivation $\Delta \vdash \tau$.

Case (VarTy) $\dfrac{\alpha \in \Delta}{\Delta \vdash \alpha}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\alpha]\!]\,\rho$, it follows that $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.
We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\alpha]\!]\,\rho$
$\equiv (j, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.

Note that

- $\rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$,
  which follows from $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, $\alpha \in \Delta$, and the definition of $\mathcal{RD}\,[\![\Delta]\!]$.

Hence, by the definition of $\mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$, since $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$ and $j \leq k$, it follows that $(j, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.

Case (BoolTy) $\dfrac{}{\Delta \vdash \mathsf{bool}}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$ it follows that

- $\bullet \vdash v' : \mathsf{bool}$, and
- either $v = v' = \mathtt{tt}$ or $v = v' = \mathtt{ff}$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$,
which follows from

- $\bullet \vdash v' : \mathsf{bool}$, and
- $v = v' = \mathtt{tt} \;\vee\; v = v' = \mathtt{ff}$.

Case (FnTy) $\dfrac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 \to \tau_2}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$ it follows that $v \equiv \lambda x.\, e$ and $v' \equiv \lambda x.\, e'$.
Note that

(A) $\bullet \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]}$, and

(B) $\forall i < k, v_1, v_1'.\ (i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho \implies (i, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$
$\equiv (j, \lambda x.\, e, \lambda x.\, e') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$.

(C) Consider arbitrary, i, v_1, v_1' such that

- $i < j$, and
- $(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

Instantiate **(B)** with i, v_1, and v_1'. Note that

- $i < k$, which follows from $i < j$ and $j \leq k$, and
- $(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

Hence, $(i, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.

From **(A)** and **(C)** it follows that $(j, \lambda x.\, e, \lambda x.\, e') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$.

Case (RecTy) $\dfrac{\Delta, \alpha \vdash \tau_1}{\Delta \vdash \mu\alpha.\,\tau_1}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$ it follows that $v \equiv \mathtt{fold}\,v_1$ and $v' \equiv \mathtt{fold}\,v_1'$.
Note that

(A) $\bullet \vdash \mathtt{fold}\,v_1' : (\mu\alpha.\,\tau_1)^{[\rho]}$, and

(B) $\forall i < k.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho \rfloor_{i+1}$ in
$(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$
$\equiv (j, \mathtt{fold}\,v_1, \mathtt{fold}\,v_1') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$.

(C) Consider arbitrary i such that

- $i < j$.

Let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho \rfloor_{i+1}$.
Instantiate **(B)** with i, noting that

- $i < k$, which follows from $i < j$ and $j \leq k$.

Hence, $(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]$.

From **(A)**, and **(C)** it follows that $(j, \mathtt{fold}\,v_1, \mathtt{fold}\,v_1') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$.

□

Lemma B.9 (λ^{rec} Per Value Contexts Downward Closed)

Let $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.
If $j \leq k$, *then* $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Proof

Proof by induction on Γ.

Case $\Gamma = \bullet$:

We are required to show that $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\bullet]\!]$.
Note that $\gamma = \gamma' = \emptyset$, which follows from $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\bullet]\!]$.
Hence, we are required to show that $(j, \emptyset, \emptyset) \in \mathcal{RG}\,[\![\bullet]\!]$, which follows trivially.

Case $\Gamma = \Gamma_1, x : \tau$, where $\bullet \vdash \tau$:

From $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma_1, x : \tau]\!]$, we conclude that there exist γ_1, γ_1', v, and v' such that

- $\gamma \equiv \gamma_1[x \mapsto v]$,
- $\gamma' \equiv \gamma_1'[x \mapsto v']$,
- $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]$, and
- $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

Hence, we are required to show that $(j, \gamma_1[x \mapsto v], \gamma_1'[x \mapsto v']) \in \mathcal{RG}\,[\![\Gamma_1, x : \tau]\!]$,
which follows from

- $(j, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]$,
  which follows from the induction hypothesis applied to $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]$ and $j \leq k$, and
- $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$,
  which follows from Lemma B.8 applied to
  - $\emptyset \in \mathcal{RD}\,[\![\bullet]\!]$,
  - $\bullet \vdash \tau$,
  - $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset \in \mathit{Rel}_\tau$, and
  - $j \leq k$.

□

Lemma B.10 **(λ^{rec} Valid Per: $\mathcal{RV}\,[\![\tau]\!]\,\rho \in Rel_{\tau^{[\rho]}}$)**

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\Delta \vdash \tau$.
Then $\mathcal{RV}\,[\![\tau]\!]\,\rho \in Rel_{\tau^{[\rho]}}$.

Proof

By the definition of $Rel_{\tau^{[\rho]}}$, it suffices to show:

$$\forall (k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho.\ \ \bullet \vdash v' : \tau^{[\rho]}\ \ \wedge \\ \forall j \leq k.\ (j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$$

Consider arbitrary $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

- Applying Lemma B.6 to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, $\Delta \vdash \tau$, and $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$ it follows that $\bullet \vdash v' : \tau^{[\rho]}$.
- Consider arbitrary $j \leq k$.

  Applying Lemma B.8 to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, $\Delta \vdash \tau$, $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, and $j \leq k$ it follows that $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

□

B.7 λ^{rec} Proofs: Per Type Substitution

Lemma B.11 (λ^{rec} Per Type Substitution: Recursive Types)

Let $\rho \in \mathcal{RD}[\![\Delta]\!]$ *and* $\Delta, \alpha \vdash \tau$.
Let $\chi = \lfloor \mathcal{RV}[\![\mu\alpha.\,\tau]\!]\,\rho \rfloor_{i+1}$.
Then $\lfloor \mathcal{RV}[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} = \lfloor \mathcal{RV}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1}$.

Proof

We are required to show that for all $k \leq i$, v, and v',

$$(k, v, v') \in \lfloor \mathcal{RV}[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} \text{ iff } (k, v, v') \in \lfloor \mathcal{RV}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1}$$

The proof is by induction on i and nested induction on $\Delta, \alpha \vdash \tau$.

Case (VarTy) $\dfrac{\beta \in \Delta}{\Delta, \alpha \vdash \beta}$:

Case $\beta = \alpha$:

$$\begin{array}{lllll}
 & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\alpha]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} & \text{Note that } k \leq i \\
\Leftrightarrow & (k,v,v') & \in & \mathcal{RV}[\![\alpha]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] & \text{by defn of } \lfloor\cdot\rfloor_{i+1} \\
\Leftrightarrow & (k,v,v') & \in & \chi & \text{by defn of } \mathcal{RV}[\![\alpha]\!] \\
\Leftrightarrow & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\mu\alpha.\,\tau]\!]\,\rho \rfloor_{i+1} & \text{by premise } \chi = \lfloor \mathcal{RV}[\![\mu\alpha.\,\tau]\!]\,\rho \rfloor_{i+1} \\
\Leftrightarrow & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\alpha[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1} & \text{by substitution}
\end{array}$$

Case $\beta \neq \alpha$:

$$\begin{array}{lllll}
 & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\beta]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} & \\
\Leftrightarrow & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\beta]\!]\,\rho \rfloor_{i+1} & \text{since } \alpha \notin FTV(\beta) \\
\Leftrightarrow & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\beta[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1} & \text{by substitution}
\end{array}$$

Case (BoolTy) $\dfrac{}{\Delta, \alpha \vdash \mathsf{bool}}$:

$$\begin{array}{lllll}
 & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\mathsf{bool}]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} & \text{Note that } k \leq i \\
\Leftrightarrow & (k,v,v') & \in & \mathcal{RV}[\![\mathsf{bool}]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] & \text{by defn of } \lfloor\cdot\rfloor_{i+1} \\
\Leftrightarrow & (k,v,v') & \in & \mathcal{RV}[\![\mathsf{bool}]\!]\,\rho & \text{since } \alpha \notin FTV(\mathsf{bool}) \\
\Leftrightarrow & (k,v,v') & \in & \mathcal{RV}[\![\mathsf{bool}[\mu\alpha.\,\tau/\alpha]]\!]\,\rho & \text{by substitution} \\
\Leftrightarrow & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\mathsf{bool}[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1} & \text{by defn of } \lfloor\cdot\rfloor_{i+1} \text{ since } k \leq i
\end{array}$$

Case (FnTy) $\dfrac{\Delta, \alpha \vdash \tau_1 \qquad \Delta, \alpha \vdash \tau_2}{\Delta, \alpha \vdash \tau_1 \to \tau_2}$:

$$\begin{array}{lllll}
 & (k,v,v') & \in & \lfloor \mathcal{RV}[\![\tau_1 \to \tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} & \text{Note that } k \leq i \\
\Leftrightarrow & (k,v,v') & \in & \mathcal{RV}[\![\tau_1 \to \tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] & \text{by defn of } \lfloor\cdot\rfloor_{i+1} \\
\Leftrightarrow & (k,\lambda x.\,e,\lambda x.\,e') & \in & \mathcal{RV}[\![\tau_1 \to \tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] & \text{since } v \equiv \lambda x.\,e \text{ and } v' \equiv \lambda x.\,e' \\
\equiv & \bullet \vdash \lambda x.\,e' : (\tau_1 \to \tau_2)^{[\rho]}[((\mu\alpha.\,\tau)^{[\rho]})/\alpha] \wedge & & & \\
 & \forall j < k, v_1, v_1'. & & & \textbf{(A)} \\
 & \quad (j, v_1, v_1') \in \mathcal{RV}[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \implies & & & \text{by defn of } \mathcal{RV}[\![\tau_1 \to \tau_2]\!] \\
 & \quad (j, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] & & & \\
\Leftrightarrow & \bullet \vdash \lambda x.\,e' : (\tau_1[\mu\alpha.\,\tau/\alpha] \to \tau_2[\mu\alpha.\,\tau/\alpha])^{[\rho]} \wedge & & & \\
 & \forall j < k, v_1, v_1'. & & & \textbf{(B)} \\
 & \quad (j, v_1, v_1') \in \mathcal{RV}[\![\tau_1[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \implies & & & \text{see proof of } \textbf{(A)} \Leftrightarrow \textbf{(B)} \text{ below} \\
 & \quad (j, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}[\![\tau_2[\mu\alpha.\,\tau/\alpha]]\!]\,\rho & & & \\
\equiv & (k,\lambda x.\,e,\lambda x.\,e') & \in & \mathcal{RV}[\![\tau_1[\mu\alpha.\,\tau/\alpha] \to \tau_2[\mu\alpha.\,\tau/\alpha]]\!]\,\rho & \\
\Leftrightarrow & (k,v,v') & \in & \mathcal{RV}[\![\tau_1[\mu\alpha.\,\tau/\alpha] \to \tau_2[\mu\alpha.\,\tau/\alpha]]\!]\,\rho & \text{since } v \equiv \lambda x.\,e \text{ and } v' \equiv \lambda x.\,e' \\
\Leftrightarrow & (k,v,v') & \in & \mathcal{RV}[\![(\tau_1 \to \tau_2)[\mu\alpha.\,\tau/\alpha]]\!]\,\rho & \text{by substitution} \\
\Leftrightarrow & (k,v,v') & \in & \lfloor \mathcal{RV}[\![(\tau_1 \to \tau_2)[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1} & \text{by defn of } \lfloor\cdot\rfloor_{i+1} \text{ since } k \leq i
\end{array}$$

Proof: (A) ⇒ (B)

The proof is in 2 parts.

I. From the first conjunct of **(A)** we have $\bullet \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]}[((\mu\alpha.\,\tau)^{[\rho]})/\alpha]$.
Hence, $\bullet \vdash \lambda x.\, e' : (\tau_1[(\mu\alpha.\,\tau)^{[\rho]}/\alpha] \to \tau_2[(\mu\alpha.\,\tau)^{[\rho]}/\alpha])^{[\rho]}$, which follows by substitution.
We are required to show that $\bullet \vdash \lambda x.\, e' : (\tau_1[\mu\alpha.\,\tau/\alpha] \to \tau_2[\mu\alpha.\,\tau/\alpha])^{[\rho]}$,
which follows by substitution.

II. Consider arbitrary j, v_1, v_1' such that

- $j < k$, and
- $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau/\alpha]]\!]\,\rho$.

Note that $(j, v_1, v_1') \in \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1}$,
which follows from the definition of $\lfloor\cdot\rfloor_k$ and $j < i+1$,
which follows from $j < k \leq i$.
Applying the induction hypothesis to $\Delta, \alpha \vdash \tau_1$, we conclude that

$$\lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} = \lfloor \mathcal{RV}\,[\![\tau_1[\mu\tau.\,\alpha/\alpha]]\!]\,\rho \rfloor_{i+1}$$

Hence, $(j, v_1, v_1') \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1}$.
Hence, $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Instantiate the second conjunct of **(A)** with j, v_1, and v_1'. Note that

- $j < k$, and
- $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]$.

Hence, $(j, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]$.
We are required to show that $(j, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2[\mu\tau.\,\alpha/\alpha]]\!]\,\rho$.
Consider arbitrary j' and e_f such that

- $j' < j$,
- $e[v_1/x] \longmapsto^{j'} e_f$, and
- $\mathit{irred}(e_f)$.

Instantiate $(j, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]$ with j' and e_f. Note that

- $j' < j$,
- $e[v_1/x] \longmapsto^{j'} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, there exists e_f' such that

- $e'[v_1'/x] \longmapsto^{*} e_f'$, and
- $(j - j', e_f, e_f') \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]$.

Note that $(j - j', e_f, e_f') \in \lfloor \mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1}$,
which follows from the definition of $\lfloor\cdot\rfloor_k$ and $j - j' < i+1$,
which follows from $j < k \leq i$.
Applying the induction hypothesis to $\Delta, \alpha \vdash \tau_2$, we conclude that

$$\lfloor \mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} = \lfloor \mathcal{RV}\,[\![\tau_2[\mu\tau.\,\alpha/\alpha]]\!]\,\rho \rfloor_{i+1}$$

Hence, $(j - j', e_f, e_f') \in \lfloor \mathcal{RV}\,[\![\tau_2[\mu\tau.\,\alpha/\alpha]]\!]\,\rho \rfloor_{i+1}$.
Hence, $(j - j', e_f, e_f') \in \mathcal{RV}\,[\![\tau_2[\mu\tau.\,\alpha/\alpha]]\!]\,\rho$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Let $e_f' = e_f'$.
We are required to show that

- $e'[v_1'/x] \longmapsto^{*} e_f'$,
  which follows from above, and

- $(j - j', e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2[\mu\tau.\,\alpha/\alpha]]\!]\,\rho$,
  which follows from above.

Proof: (B) $\Rightarrow$ (A)

Analogous to proof of **(A) $\Rightarrow$ (B)**.

Case $(\mathsf{RecTy})\ \dfrac{\Delta, \alpha, \beta \vdash \tau_1}{\Delta, \alpha \vdash \mu\beta.\,\tau_1}$:

$$
\begin{array}{lllll}
 & (k, v, v') & \in & \lfloor \mathcal{RV}\,[\![\mu\beta.\,\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]\rfloor_{i+1} & \text{Note that } k \leq i \\
\Leftrightarrow & (k, v, v') & \in & \mathcal{RV}\,[\![\mu\beta.\,\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] & \text{by defn of } \lfloor\cdot\rfloor_{i+1} \\
\Leftrightarrow & (k, \mathtt{fold}\,v_1, \mathtt{fold}\,v'_1) & \in & \mathcal{RV}\,[\![\mu\beta.\,\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] & \text{since } v \equiv \mathtt{fold}\,v,\ v' \equiv \mathtt{fold}\,v'_1 \\
\equiv & \bullet \vdash \mathtt{fold}\,v'_1 : (\mu\beta.\,\tau_1)^{[\rho]}[((\mu\alpha.\,\tau)^{[\rho]})/\alpha] \wedge & & & \\
 & \forall j < k. & & & \\
 & \quad \text{let } \chi' = \lfloor \mathcal{RV}\,[\![\mu\beta.\,\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]\rfloor_{j+1} \text{ in} & & & \textbf{(A)} \\
 & \quad (j, v_1, v'_1) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]}), & & & \text{by defn of } \mathcal{RV}\,[\![\mu\beta.\,\tau_1]\!] \\
 & \qquad\qquad \beta \mapsto (\chi', (\mu\beta.\,\tau_1)^{[\rho]}[((\mu\alpha.\,\tau)^{[\rho]})/\alpha])] & & & \\
\Leftrightarrow & \bullet \vdash \mathtt{fold}\,v'_1 : (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]} \wedge & & & \\
 & \forall j < k. & & & \textbf{(B)} \\
 & \quad \text{let } \chi' = \lfloor \mathcal{RV}\,[\![\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])]\!]\,\rho\rfloor_{j+1} \text{ in} & & & \text{see proof of } \textbf{(A)} \Leftrightarrow \textbf{(B)} \text{ below} \\
 & \quad (j, v_1, v'_1) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau/\alpha]]\!]\,\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})] & & & \\
\equiv & (k, \mathtt{fold}\,v_1, \mathtt{fold}\,v'_1) & \in & \mathcal{RV}\,[\![\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])]\!]\,\rho & \\
\Leftrightarrow & (k, v, v') & \in & \mathcal{RV}\,[\![\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])]\!]\,\rho & \text{since } v \equiv \mathtt{fold}\,v_1,\ v' \equiv \mathtt{fold}\,v'_1 \\
\Leftrightarrow & (k, v, v') & \in & \mathcal{RV}\,[\![(\mu\beta.\,\tau_1)[\mu\alpha.\,\tau/\alpha]]\!]\,\rho & \text{by substitution} \\
\Leftrightarrow & (k, v, v') & \in & \lfloor \mathcal{RV}\,[\![(\mu\beta.\,\tau_1)[\mu\alpha.\,\tau/\alpha]]\!]\,\rho\rfloor_{i+1} & \text{by defn of } \lfloor\cdot\rfloor_{i+1} \text{ since } k \leq i
\end{array}
$$

Proof: (A) $\Rightarrow$ (B)

The proof is in 2 parts.

I. From the first conjunct of **(A)** we have $\bullet \vdash \mathtt{fold}\,v'_1 : (\mu\beta.\,\tau_1)^{[\rho]}[((\mu\alpha.\,\tau)^{[\rho]})/\alpha]$.
Hence, $\bullet \vdash \mathtt{fold}\,v'_1 : (\mu\beta.\,(\tau_1[((\mu\alpha.\,\tau)^{[\rho]})/\alpha]))^{[\rho]}$, which follows by substitution.
We are required to show that $\bullet \vdash \mathtt{fold}\,v'_1 : (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]}$,
which follows by substitution.

II. Consider arbitrary j such that

- $j < k$

Let $\chi' = \lfloor \mathcal{RV}\,[\![\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])]\!]\,\rho\rfloor_{j+1}$.
Hence, $\chi' = \lfloor \mathcal{RV}\,[\![(\mu\beta.\,\tau_1)[\mu\alpha.\,\tau/\alpha]]\!]\,\rho\rfloor_{j+1}$, which follows by substitution.
Note that $j + 1 < i + 1$, which follows from $j < k$ and $k \leq i$.
Hence, applying the induction hypothesis to $\Delta, \alpha \vdash \mu\beta.\,\tau_1$, we conclude that

$$\lfloor \mathcal{RV}\,[\![\mu\beta.\,\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]\rfloor_{j+1} = \lfloor \mathcal{RV}\,[\![(\mu\beta.\,\tau_1)[\mu\alpha.\,\tau/\alpha]]\!]\,\rho\rfloor_{j+1}.$$

Instantiate the second conjunct of **(A)** with j, noting that

- $j < k$.

Note that $\chi' = \lfloor \mathcal{RV}\,[\![\mu\beta.\,\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \mu\alpha.\,\tau)]\rfloor_{j+1}$.
Hence, $(j, v_1, v'_1) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]}), \beta \mapsto (\chi', (\mu\beta.\,\tau_1)^{[\rho]}[((\mu\alpha.\,\tau)^{[\rho]})/\alpha])]$
$\equiv \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]}), \beta \mapsto (\chi', (\mu\beta.\,(\tau_1[((\mu\alpha.\,\tau)^{[\rho]})/\alpha]))^{[\rho]})]$
$\equiv \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]}), \beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})]$
which follows by substitution.
Hence, $(j, v_1, v'_1) \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]}), \beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})]\rfloor_{i+1}$,
which follows from the definition $\lfloor\cdot\rfloor_k$ and $j < i + 1$.
Hence, $(j, v_1, v'_1) \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]}), \alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})]\rfloor_{i+1}$.
Note that $\Delta, \alpha, \beta \vdash \tau_1$ iff $\Delta, \beta, \alpha \vdash \tau_1$.
Also note that $\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})] \in \mathcal{RD}\,[\![\Delta, \beta]\!]$, which follows from

- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and

- $\chi' \in Rel_{(\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]}}$, which follows from

  $\mathcal{RV}\,[\![\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])]\!]\,\rho \in Rel_{(\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]}}$,
  which follows from Lemma B.10 applied to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\Delta \vdash \mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])$
  $\Rightarrow \lfloor \mathcal{RV}\,[\![\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])]\!]\,\rho \rfloor_{j+1} \in Rel_{(\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]}}$,
  which follows from the definition of $\lfloor\cdot\rfloor_k$
  $\Rightarrow \chi' \in Rel_{(\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]}}$,
  which follows from $\chi' = \lfloor \mathcal{RV}\,[\![\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha])]\!]\,\rho \rfloor_{j+1}$.

Applying the induction hypothesis to

- $\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})] \in \mathcal{RD}\,[\![\Delta, \beta]\!]$,
- $\Delta, \beta, \alpha \vdash \tau_1$, and
- $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})] \rfloor_{i+1}$,
  which follows from $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\rho \rfloor_{i+1}$ since $\beta \notin FTV(\mu\alpha.\,\tau)$,

we conclude that

$$\begin{aligned}&\lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]}), \alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1}\\ &\quad = \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau/\alpha]]\!]\,\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})] \rfloor_{i+1}\end{aligned}$$

Hence, $(j, v_1, v_1') \in \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau/\alpha]]\!]\,\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})] \rfloor_{i+1}$.
Hence, $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau/\alpha]]\!]\,\rho[\beta \mapsto (\chi', (\mu\beta.\,(\tau_1[\mu\alpha.\,\tau/\alpha]))^{[\rho]})]$, which follows from the definition of $\lfloor\cdot\rfloor_k$.

Proof: (B) $\Rightarrow$ (A)
Analogous to proof of **(A) $\Rightarrow$ (B)**.

□

B.8 λ^{rec} Proofs: Fundamental Property of the Logical Relation

The Fundamental Property of a logical relation holds if the latter is a congruence — that is, if it satisfies the compatibility and substitutivity properties.

Lemma B.12 (λ^{rec} Compatibility-True)

$\Gamma \vdash \mathtt{tt} \leq \mathtt{tt} : \mathsf{bool}$.

Proof

The proof is in 2 parts.

I. We are required to show $\Gamma \vdash \mathtt{tt} : \mathsf{bool}$, which is immediate.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(\mathtt{tt}), \gamma'(\mathtt{tt})) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset$
$\equiv (k, \mathtt{tt}, \mathtt{tt}) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{tt} \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Since $\mathtt{tt}$ is a value, we have $\mathit{irred}(\mathtt{tt})$.
Hence, $j = 0$ and $e_f \equiv \mathtt{tt}$.
Let $e'_f = \mathtt{tt}$.
We are required to show that

- $\mathtt{tt} \longmapsto^{*} \mathtt{tt}$,
  which is immediate, and
- $(k - 0, \mathtt{tt}, \mathtt{tt}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$,
  which follows from
  - $\bullet \vdash \mathtt{tt} : \mathsf{bool}$, and
  - $\mathtt{tt} = \mathtt{tt} = \mathtt{tt}$.

□

Lemma B.13 (λ^{rec} Compatibility-False)

$\Gamma \vdash \mathtt{ff} \leq \mathtt{ff} : \mathsf{bool}$.

Proof

The proof is in 2 parts.

I. We are required to show $\Gamma \vdash \mathtt{ff} : \mathsf{bool}$, which is immediate.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(\mathtt{ff}), \gamma'(\mathtt{ff})) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset$
$\equiv (k, \mathtt{ff}, \mathtt{ff}) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{ff} \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Since $\mathtt{ff}$ is a value, we have $\mathit{irred}(\mathtt{ff})$.
Hence, $j = 0$ and $e_f \equiv \mathtt{ff}$.
Let $e'_f = \mathtt{ff}$.
We are required to show that

- $\mathtt{ff} \longmapsto^{*} \mathtt{ff}$,
  which is immediate, and
- $(k - 0, \mathtt{ff}, \mathtt{ff}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$,
  which follows from
  - $\bullet \vdash \mathtt{ff} : \mathsf{bool}$, and
  - $\mathtt{ff} = \mathtt{ff} = \mathtt{ff}$.

□

Lemma B.14 (λ^{rec} Compatibility-If)

If $\Gamma \vdash e_0 \leq e_0' : \mathsf{bool}$, $\Gamma \vdash e_1 \leq e_1' : \tau$, *and* $\Gamma \vdash e_2 \leq e_2' : \tau$,
then $\Gamma \vdash \mathtt{if}\, e_0, e_1, e_2 \leq \mathtt{if}\, e_0', e_1', e_2' : \tau$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Gamma \vdash \mathtt{if}\, e_0, e_1, e_2 : \mathsf{bool}$, which follows from
  - $\Gamma \vdash e_0 : \mathsf{bool}$, which follows from $\Gamma \vdash e_0 \leq e_0' : \mathsf{bool}$,
  - $\Gamma \vdash e_1 : \tau$, which follows from $\Gamma \vdash e_1 \leq e_1' : \tau$, and
  - $\Gamma \vdash e_2 : \tau$, which follows from $\Gamma \vdash e_2 \leq e_2' : \tau$.
- $\Gamma \vdash \mathtt{if}\, e_0', e_1', e_2' : \mathsf{bool}$, which follows analogously.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(\mathtt{if}\, e_0, e_1, e_2), \gamma'(\mathtt{if}\, e_0', e_1', e_2')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$
$\equiv (k, \mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2), \mathtt{if}\, \gamma'(e_0'), \gamma'(e_1'), \gamma'(e_2')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2) \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_0 and e_{f_0} such that

- $\gamma(e_0) \longmapsto^{j_0} e_{f_0}$,
- $\mathit{irred}(e_{f_0})$, and
- $j_0 \leq j$.

Instantiate the second conjunct of $\Gamma \vdash e_0 \leq e_0' : \mathsf{bool}$ with k, γ, and γ'.
Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(e_0), \gamma'(e_0')) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset$.
Instantiate this with j_0, e_{f_0}. Note that

- $j_0 < k$, which follows from $j_0 \leq j$ and $j < k$,
- $\gamma(e_0) \longmapsto^{j_0} e_{f_0}$, and
- $\mathit{irred}(e_{f_0})$.

Hence, there exists e_{f_0}' such that

- $\gamma'(e_0') \longmapsto^* e_{f_0}'$, and
- $(k - j_0, e_{f_0}, e_{f_0}') \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$.

Hence, either $e_{f_0} \equiv e_{f_0}' \equiv \mathtt{tt}$ or $e_{f_0} \equiv e_{f_0}' \equiv \mathtt{ff}$.

Case $e_{f_0} \equiv e'_{f_0} \equiv \mathtt{tt}$:

Note that

$$\begin{aligned}\gamma(\mathtt{if}\, e_0, e_1, e_2) &\equiv \mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{j_0} \mathtt{if}\, e_{f_0}, \gamma(e_1), \gamma(e_2)\\ &\equiv \mathtt{if}\, \mathtt{tt}, \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{1} \gamma(e_1)\\ &\longmapsto^{j_1} e_{f_1}\end{aligned}$$

where $\mathit{irred}(e_{f_1})$ and $e_{f_1} \equiv e_f$ and $j = j_0 + 1 + j_1$.

Instantiate the second conjunct of $\Gamma \vdash e_1 \leq e'_1 : \tau$ with $k - j_0 - 1$, γ, and γ'. Note that

- $k - j_0 - 1 \geq 0$, which follows from $j_0 < k$, and
- $(k - j_0 - 1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
  which follows from Lemma B.9 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$ and $k - j_0 - 1 \leq k$.

Hence, $(k - j_0 - 1, \gamma(e_1), \gamma'(e'_1)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.

Instantiate this with j_1 and e_{f_1}. Note that

- $j_1 < k - j_0 - 1$, which follows from $j_1 = j - j_0 - 1$ and $j < k$,
- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e'_1) \longmapsto^{*} e'_{f_1}$, and
- $(k - j_0 - 1 - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$
  $\equiv (k - j, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$, since $j = j_0 + 1 + j_1$.

Let $e'_f = e'_{f_1}$.

We are required to show

- $\gamma'(\mathtt{if}\, e'_0, e'_1, e'_2) \longmapsto^{*} e'_{f_1}$,
  which follows from

$$\begin{aligned}\gamma'(\mathtt{if}\, e'_0, e'_1, e'_2) &\equiv \mathtt{if}\, \gamma'(e'_0), \gamma'(e'_1), \gamma'(e'_2)\\ &\longmapsto^{*} \mathtt{if}\, e'_{f_0}, \gamma'(e'_1), \gamma'(e'_2)\\ &\equiv \mathtt{if}\, \mathtt{tt}, \gamma'(e'_1), \gamma'(e'_2)\\ &\longmapsto^{1} \gamma'(e'_1)\\ &\longmapsto^{*} e'_{f_1}\end{aligned}$$

  and
- $(k - j, e_f, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$
  $\equiv (k - j, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$,
  which follows from above.

Case $e_{f_0} \equiv e'_{f_0} \equiv \mathtt{ff}$:

Note that

$$\begin{aligned}\gamma(\mathtt{if}\, e_0, e_1, e_2) &\equiv \mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{j_0} \mathtt{if}\, e_{f_0}, \gamma(e_1), \gamma(e_2)\\ &\equiv \mathtt{if}\, \mathtt{ff}, \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{1} \gamma(e_2)\\ &\longmapsto^{j_2} e_{f_2}\end{aligned}$$

where $\mathit{irred}(e_{f_2})$ and $e_{f_2} \equiv e_f$ and $j = j_0 + 1 + j_2$.

Instantiate the second conjunct of $\Gamma \vdash e_2 \leq e'_2 : \tau$ with $k - j_0 - 1$, γ, and γ'. Note that

- $k - j_0 - 1 \geq 0$, which follows from $j_0 < k$, and
- $(k - j_0 - 1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
  which follows from Lemma B.9 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$ and $k - j_0 - 1 \leq k$.

Hence, $(k - j_0 - 1, \gamma(e_2), \gamma'(e'_2)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.

Instantiate this with j_2 and e_{f_2}. Note that

- $j_2 < k - j_0 - 1$, which follows from $j_2 = j - j_0 - 1$ and $j < k$,

- $\gamma(e_2) \longmapsto^{j_2} e_{f_2}$, and
- $\mathit{irred}(e_{f_2})$.

Hence, there exists e'_{f_2} such that

- $\gamma'(e'_2) \longmapsto^{*} e'_{f_2}$, and
- $(k - j_0 - 1 - j_2, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$
  $\equiv (k - j, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$, since $j = j_0 + 1 + j_2$

.

Let $e'_f = e'_{f_2}$.
We are required to show

- $\gamma'(\texttt{if}\, e'_0, e'_1, e'_2) \longmapsto^{*} e'_{f_2}$,
  which follows from
  $$\begin{aligned}\gamma'(\texttt{if}\, e'_0, e'_1, e'_2) &\equiv \texttt{if}\, \gamma'(e'_0), \gamma'(e'_1), \gamma'(e'_2)\\ &\longmapsto^{*} \texttt{if}\, e'_{f_0}, \gamma'(e'_1), \gamma'(e'_2)\\ &\equiv \texttt{if}\, \texttt{ff}, \gamma'(e'_1), \gamma'(e'_2)\\ &\longmapsto^{1} \gamma'(e'_2)\\ &\longmapsto^{*} e'_{f_2}\end{aligned}$$
  and
- $(k - j, e_f, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$
  $\equiv (k - j, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$,
  which follows from above.

□

Lemma B.15 (λ^{rec} Compatibility-Var)

$\Gamma \vdash x \leq x : \Gamma(x)$.

Proof

The proof is in 2 parts.

I. We are required to show $\Gamma \vdash x : \Gamma(x)$, which is immediate.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(x), \gamma'(x)) \in \mathcal{RC}\,[\![\Gamma(x)]\!]\,\emptyset$.
Consider arbitrary j, e_f such that

- $j < k$,
- $\gamma(x) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Since $\gamma(x)$ is a value, we have $\mathit{irred}(\gamma(x))$.
Hence, $j = 0$ and $e_f \equiv \gamma(x)$.
Let $e'_f = \gamma'(x)$.
We are required to show that

- $\gamma'(x) \longmapsto^{*} \gamma'(x)$,
  which is immediate, and
- $(k - 0, \gamma(x), \gamma'(x)) \in \mathcal{RV}\,[\![\Gamma(x)]\!]\,\emptyset$,
  which follows from $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

□

Lemma B.16 (λ^{rec} Compatibility-Fn)

If $\Gamma, x : \tau \vdash e \leq e' : \tau_2$,
then $\Gamma \vdash \lambda x.\, e \leq \lambda x.\, e' : \tau_1 \to \tau_2$.

Proof

The proof is in 2 parts.

I. We are required to show $\Gamma \vdash \lambda x.\, e : \tau_1 \to \tau_2$ and $\Gamma \vdash \lambda x.\, e' : \tau_1 \to \tau_2$,
which follow (respectively) from $\Gamma, x : \tau_1 \vdash e : \tau_2$ and $\Gamma, x : \tau_1 \vdash e' : \tau_2$,
which follow from $\Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(\lambda x.\, e), \gamma'(\lambda x.\, e')) \in \mathcal{RC}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$
$\equiv (k, \lambda x.\, \gamma(e), \lambda x.\, \gamma'(e')) \in \mathcal{RC}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\lambda x.\, \gamma(e) \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Since $\lambda x.\, \gamma(e)$ is a value, we have $\mathit{irred}(\lambda x.\, \gamma(e))$.
Hence, $j = 0$ and $e_f \equiv \lambda x.\, \gamma(e)$.
Let $e'_f = \lambda x.\, \gamma'(e')$.
We are required to show that

- $\lambda x.\, \gamma'(e') \longmapsto^* \lambda x.\, \gamma'(e')$,
  which is immediate, and
- $(k - 0, \lambda x.\, \gamma(e), \lambda x.\, \gamma'(e')) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$
  $\equiv (k, \lambda x.\, \gamma(e), \lambda x.\, \gamma'(e'))$
  $\in \{(k, \lambda x.\, e, \lambda x.\, e') \mid \bullet \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\emptyset]} \ \wedge$
  $\forall j < k, v_1, v'_1.$
  $(j, v_1, v'_1) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset \implies$
  $(j, e[v_1/x], e'[v'_1/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset\}$,
  which follows from

  - $\bullet \vdash \lambda x.\, \gamma'(e') : \tau_1 \to \tau_2$,
    which follows from

    - Note that $\Gamma, x : \tau_1 \vdash e' : \tau_2$, which follows from $\Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$.
      Hence, we have $\Gamma \vdash \lambda x.\, e' : \tau_1 \to \tau_2$.
      Note that $\vdash \gamma' : \Gamma$, which follows from Lemma B.7 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.
      Note that $\bullet \vdash \gamma'(\lambda x.\, e') : \tau_1 \to \tau_2$, which follows from Lemma B.5 applied to $\vdash \gamma' : \Gamma$ and $\Gamma \vdash \lambda x.\, e' : \tau_1 \to \tau_2$.
      Hence, $\bullet \vdash \lambda x.\, \gamma'(e') : \tau_1 \to \tau_2$.

  - $\forall j < k, v_1, v_1 \ldots$.
    Consider arbitrary j, v_1, v'_1 such that

    - $j < k$, and

- $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

We are required to show that $(j, \gamma(e)[v_1/x], \gamma'(e')[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
Instantiate the second conjunct of $\Gamma, x : \tau \vdash e \leq e' : \tau_2$ with j, $\gamma[x \mapsto v_1]$, and $\gamma'[x \mapsto v_1']$.
Note that

- $j \geq 0$, and
- $(j, \gamma[x \mapsto v_1], \gamma'[x \mapsto v_1']) \in \mathcal{RG}\,[\![\Gamma, x : \tau_1]\!]$, which follows from
  - $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
    which follows from Lemma B.9 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$ and $j \leq k$, and
  - $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$,
    which follows from above.

Hence, $(j, \gamma[x \mapsto v_1](e), \gamma'[x \mapsto v_1'](e')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
Thus, $(j, \gamma(e)[x/v_1], \gamma'(e')[x/v_1']) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.

□

Lemma B.17 **(λ^{rec} Compatibility-App)**

If $\Gamma \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$, *and* $\Gamma \vdash e_2 \leq e_2' : \tau_1$,
then $\Gamma \vdash e_1\, e_2 \leq e_1'\, e_2' : \tau_2$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Gamma \vdash e_1\, e_2 : \tau_2$,
  which follows from
  - $\Gamma \vdash e_1 : \tau_1 \to \tau_2$,
    which follows from $\Gamma \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$, and
  - $\Gamma \vdash e_2 : \tau_1$,
    which follows from $\Gamma \vdash e_2 \leq e_2' : \tau_1$.
- $\Gamma \vdash e_1'\, e_2' : \tau_2$, which follows analogously.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(e_1\, e_2), \gamma'(e_1'\, e_2')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$
$\equiv (k, \gamma(e_1)\,\gamma(e_2), \gamma'(e_1')\,\gamma'(e_2')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\gamma(e_1)\gamma(e_2) \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Gamma \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$ with k, γ, and γ'. Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(e_1), \gamma'(e_1')) \in \mathcal{RC}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j$ and $j < k$,
- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e_{f_1}' such that

- $\gamma'(e_1') \longmapsto^* e_{f_1}'$, and
- $(k - j_1, e_{f_1}, e_{f_1}') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.

Hence, $e_{f_1} \equiv \lambda x.\, e_{f_{11}}$ and $e'_{f_1} \equiv \lambda x.\, e'_{f_{11}}$.
Note that

$$\begin{aligned}\gamma(e_1\, e_2) &\equiv \gamma(e_1)\, \gamma(e_2)\\ &\longmapsto^{j_1} e_{f_1}\, \gamma(e_2)\\ &\equiv (\lambda x.\, e_{f_{11}})\, \gamma(e_2)\\ &\longmapsto^{j-j_1} e_f\end{aligned}$$

Hence, by inspection of the operational semantics it follows that there exist j_2 and e_{f_2} such that

- $\gamma(e_2) \longmapsto^{j_2} e_{f_2}$,
- $\mathit{irred}(e_{f_2})$, and
- $j_2 \leq j - j_1$.

Instantiate the second conjunct of $\Gamma \vdash e_2 \leq e'_2 : \tau_1$ with $k - j_1$, γ, and γ'. Note that

- $k - j_1 \geq 0$, which follows from $j_1 < k$, and
- $(k - j_1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
  which follows from Lemma B.9 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$ and $k - j_1 \leq k$.

Hence, $(k - j_1, \gamma(e_2), \gamma'(e'_2)) \in \mathcal{RC}\,[\![\tau_1]\!]\,\emptyset$.
Instantiate this with j_2 and e_{f_2}. Note that

- $j_2 < k - j_1$, which follows from $j_2 \leq j - j_1$ and $j < k$,
- $\gamma(e_2) \longmapsto^{j_2} e_{f_2}$, and
- $\mathit{irred}(e_{f_2})$.

Hence, there exists e'_{f_2} such that

- $\gamma'(e'_2) \longmapsto^{*} e'_{f_2}$, and
- $(k - j_1 - j_2, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

Hence, $e_{f_2} \equiv v_{f_2}$ and $e'_{f_2} \equiv v'_{f_2}$.
Note that

$$\begin{aligned}\gamma(e_1\, e_2) &\equiv \gamma(e_1)\, \gamma(e_2)\\ &\longmapsto^{j_1} e_{f_1}\, \gamma(e_2)\\ &\equiv (\lambda x.\, e_{f_{11}})\, \gamma(e_2)\\ &\longmapsto^{j_2} (\lambda x.\, e_{f_{11}})\, e_{f_2}\\ &\equiv (\lambda x.\, e_{f_{11}})\, v_{f_2}\\ &\longmapsto^{1} e_{f_{11}}[v_{f_2}/x]\\ &\longmapsto^{j_3} e_f\end{aligned}$$

and $\mathit{irred}(e_f)$, where $j = j_1 + j_2 + 1 + j_3$.
Instantiate the second conjunct of $(k - j_1, \lambda x.\, e_{f_{11}}, \lambda x.\, e'_{f_{11}}) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$ with $k - j_1 - j_2 - 1$, v_{f_2}, and v'_{f_2}. Note that

- $k - j_1 - j_2 - 1 < k - j_1$, and
- $(k - j_1 - j_2 - 1, v_{f_2}, v'_{f_2}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$,
  which follows from Lemma B.8 applied to
  - $\emptyset \in \mathcal{RD}\,[\![\bullet]\!]$,
  - $\bullet \vdash \tau_1$,
  - $(k - j_1 - j_2, v_{f_2}, v'_{f_2}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$, and
  - $k - j_1 - j_2 - 1 \leq k - j_1 - j_2$.

Hence, $(k - j_1 - j_2 - 1, e_{f_{11}}[v_{f_2}/x], e'_{f_{11}}[v'_{f_2}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
Instantiate this with j_3 and e_f. Note that

- $j_3 < k - j_1 - j_2 - 1$, which follows from $j_3 = j - j_1 - j_2 - 1$ and $j < k$,
- $e_{f_{11}}[v_{f_2}/x] \longmapsto^{j_3} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, there exists e'_f such that

- $e'_{f_{11}}[v'_{f_2}/x] \longmapsto^* e'_f$, and
- $(k - j_1 - j_2 - 1 - j_3, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$
  $\equiv (k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$, since $j = j_1 + j_2 + 1 + j_3$.

Pick $e'_f = e'_f$.
We are required to show that

- $\gamma'(e'_1\, e'_2) \longmapsto^* e'_f$,
  which follows from

$$\begin{array}{rl} \gamma'(e'_1\, e'_2) & \equiv \gamma'(e'_1)\,\gamma'(e'_2) \\ & \longmapsto^* e'_{f_1}\,\gamma'(e'_2) \\ & \equiv (\lambda x.\, e'_{f_{11}})\,\gamma'(e'_2) \\ & \longmapsto^* (\lambda x.\, e'_{f_{11}})\, e'_{f_2} \\ & \equiv (\lambda x.\, e'_{f_{11}})\, v'_{f_2} \\ & \longmapsto^1 e'_{f_{11}}[v'_{f_2}/x] \\ & \longmapsto^* e'_f \end{array}$$

  and
- $(k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$,
  which follows from above.

□

Lemma B.18 (λ^{rec} Compatibility-Fold)

If $\Gamma \vdash e \leq e' : \tau[\mu\alpha.\,\tau/\alpha]$,
then $\Gamma \vdash \mathtt{fold}\, e \leq \mathtt{fold}\, e' : \mu\alpha.\,\tau$.

Proof

The proof is in 2 parts.

I. We are required to show $\Gamma \vdash \mathtt{fold}\, e : \mu\alpha.\,\tau$ and $\Gamma \vdash \mathtt{fold}\, e' : \mu\alpha.\,\tau$,
which follow (respectively) from $\Gamma \vdash e : \tau[\mu\alpha.\,\tau/\alpha]$ and $\Gamma \vdash e' : \tau[\mu\alpha.\,\tau/\alpha]$,
which follow from $\Gamma \vdash e \leq e' : \tau[\mu\alpha.\,\tau/\alpha]$.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(\mathtt{fold}\, e), \gamma'(\mathtt{fold}\, e')) \in \mathcal{RC}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset$
$\equiv (k, \mathtt{fold}\,\gamma(e), \mathtt{fold}\,\gamma'(e')) \in \mathcal{RC}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{fold}\,\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Gamma \vdash e \leq e' : \tau[\mu\alpha.\,\tau/\alpha]$ with k, γ, and γ'.
Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j < k$,
- $\gamma(e) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e') \longmapsto^{*} e'_{f_1}$, and
- $(k - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset$.

Hence, $e_{f_1} \equiv v_{f_1}$ and $e'_{f_1} \equiv v'_{f_1}$.
Note that

$$\begin{aligned}\gamma(\mathtt{fold}\, e) &\equiv \mathtt{fold}\,\gamma(e)\\ &\longmapsto^{j_1} \mathtt{fold}\, e_{f_1}\\ &\equiv \mathtt{fold}\, v_{f_1}\\ &\longmapsto^{j-j_1} e_f\end{aligned}$$

Since $\mathtt{fold}\, v_{f_1}$ is a value, we have $\mathit{irred}(\mathtt{fold}\, v_{f_1})$.
Hence, $j - j_1 = 0$ (and $j = j_1$) and $e_f \equiv \mathtt{fold}\, v_{f_1}$.
Let $e'_f = \mathtt{fold}\, v'_{f_1}$.
We are required to show that

- $\texttt{fold}\,\gamma'(e') \longmapsto^* e'_f$
  $\equiv \texttt{fold}\,\gamma'(e') \longmapsto^* \texttt{fold}\,v'_{f_1}$
  which follows from above, and
- $(k-j, e_f, e'_f) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset$
  $\equiv (k-j, \texttt{fold}\,v_{f_1}, \texttt{fold}\,v'_{f_1})$
  $\in \{(k, \texttt{fold}\,v, \texttt{fold}\,v') \mid$
  $\bullet \vdash \texttt{fold}\,v' : (\mu\alpha.\,\tau)^{[\emptyset]} \wedge$
  $\forall j < k.$
  let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset \rfloor_{j+1}$ in
  $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\emptyset]})]\}$
  which follows from
  - $\bullet \vdash \texttt{fold}\,v'_{f_1} : (\mu\alpha.\,\tau)^{[\emptyset]}$
    Note that $\bullet \vdash v'_{f_1} : \tau[\mu\alpha.\,\tau/\alpha]$, which follows from $(k-j, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset$.
    Hence, $\bullet \vdash \texttt{fold}\,v'_{f_1} : \mu\alpha.\,\tau$.
  - $\forall i < k-j.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset \rfloor_{i+1}$ in $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\emptyset]})]$.
    Consider arbitrary i such that
    - $i < k-j$.

    Let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset \rfloor_{i+1}$.
    We are required to show that $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\emptyset]})]$.
    Applying Lemma B.8 to
    - $\emptyset \in \mathcal{RD}\,[\![\bullet]\!]$,
    - $\bullet \vdash \tau[\mu\alpha.\,\tau/\alpha]$,
    - $(k-j, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset$, and
    - $i \leq k-j$,

    we conclude that $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset$.
    Hence, $(i, v_{f_1}, v'_{f_1}) \in \lfloor \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset \rfloor_{i+1}$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
    Applying Lemma B.11 to $\bullet \vdash \mu\alpha.\,\tau$ and $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset \rfloor_{i+1}$ we conclude that $\lfloor \mathcal{RV}\,[\![\tau]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\emptyset]})] \rfloor_{i+1} = \lfloor \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset \rfloor_{i+1}$.
    Hence, $(i, v_{f_1}, v'_{f_1}) \in \lfloor \mathcal{RV}\,[\![\tau]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\emptyset]})] \rfloor_{i+1}$.
    Hence, $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\emptyset]})]$, which follows from the definition of $\lfloor\cdot\rfloor_k$.

□

Lemma B.19 (λ^{rec} Compatibility-Unfold)

If $\Gamma \vdash e \leq e' : \mu\alpha.\,\tau$,
then $\Gamma \vdash \mathtt{unfold}\, e \leq \mathtt{unfold}\, e' : \tau[\mu\alpha.\,\tau/\alpha]$.

Proof

The proof is in 2 parts.

I. We are required to show $\Gamma \vdash \mathtt{unfold}\, e : \tau[\mu\alpha.\,\tau/\alpha]$ and $\Gamma \vdash \mathtt{unfold}\, e' : \tau[\mu\alpha.\,\tau/\alpha]$,
which follow (respectively) from $\Gamma \vdash e : \mu\alpha.\,\tau$ and $\Gamma \vdash e' : \mu\alpha.\,\tau$,
which follow from $\Gamma \vdash e \leq e' : \mu\alpha.\,\tau$.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(\mathtt{unfold}\, e), \gamma'(\mathtt{unfold}\, e')) \in \mathcal{RC}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset$
$\equiv (k, \mathtt{unfold}\,\gamma(e), \mathtt{unfold}\,\gamma'(e')) \in \mathcal{RC}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\emptyset$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{unfold}\,\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Gamma \vdash e \leq e' : \mu\alpha.\,\tau$ with k, γ, and γ'. Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j < k$,
- $\gamma(e) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e') \longmapsto^{*} e'_{f_1}$, and
- $(k - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\emptyset$.

Hence, $e_{f_1} \equiv \mathtt{fold}\, v_{f_{11}}$ and $e'_{f_1} \equiv \mathtt{fold}\, v'_{f_{11}}$.
Note that

$$\begin{aligned}\gamma(\mathtt{unfold}\, e) &\equiv \mathtt{unfold}\,\gamma(e)\\ &\longmapsto^{j_1} \mathtt{unfold}\, e_{f_1}\\ &\equiv \mathtt{unfold}\,(\mathtt{fold}\, v_{f_{11}})\\ &\longmapsto^{1} v_{f_{11}} \longmapsto^{j-j_1-1} e_f\end{aligned}$$

Since $v_{f_{11}}$ is a value, we have $\mathit{irred}(v_{f_{11}})$.

Hence, $j - j_1 - 1 = 0$ (and $j = j_1 + 1$) and $e_f \equiv v_{f_{11}}$.
Furthermore, note that

$$\begin{aligned}\gamma'(\mathtt{unfold}\, e') &\equiv \mathtt{unfold}\, \gamma'(e') \\ &\longmapsto^* \mathtt{unfold}\, e'_{f_1} \\ &\equiv \mathtt{unfold}\, (\mathtt{fold}\, v'_{f_{11}}) \\ &\longmapsto^1 v'_{f_{11}}\end{aligned}$$

Since $v'_{f_{11}}$ is a value, we have $\mathit{irred}(v'_{f_{11}})$.
Let $e'_f = v'_{f_{11}}$.
We are required to show that

- $\mathtt{unfold}\, \gamma'(e') \longmapsto^* e'_f$
  $\equiv \mathtt{unfold}\, \gamma'(e') \longmapsto^* v'_{f_{11}}$
  which follows from above, and
- $(k - j, e_f, e'_f) \in \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \emptyset$
  $\equiv (k - j, v_{f_{11}}, v'_{f_{11}}) \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \emptyset$,
  which we conclude as follows:
  From $(k - j_1, e_{f_1}, e'_{f_1}) \equiv (k - j_1, \mathtt{fold}\, v_{f_{11}}, \mathtt{fold}\, v'_{f_{11}}) \in \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \emptyset$, we have
  - $\bullet \vdash \mathtt{fold}\, v'_{f_{11}} : (\mu\alpha.\, \tau)^{[\emptyset]}$, and
  - $\forall i < k - j_1.$ let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \emptyset \rfloor_{i+1}$ in $(i, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau]\!]\, \emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\emptyset]})]$.

  Instantiate $\forall i < k - j_1.$ let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \emptyset \rfloor_{i+1}$ in $(i, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau]\!]\, \emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\emptyset]})]$ with $k - j$.
  Note that
  - $k - j < k - j_1$, which follows from $j = j_1 + 1$.

  Let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \emptyset \rfloor_{k-j+1}$.
  Hence, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau]\!]\, \emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\emptyset]})]$.
  Hence, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \lfloor \mathcal{RV}\, [\![\tau]\!]\, \emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\emptyset]})] \rfloor_{k-j+1}$, which follows from the definition of $\lfloor \cdot \rfloor_k$.
  Applying Lemma B.11 to $\emptyset \in \mathcal{RD}\, [\![\bullet]\!]$, $\bullet \vdash \mu\alpha.\, \tau$, and $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \emptyset \rfloor_{k-j+1}$, we conclude that
  $\lfloor \mathcal{RV}\, [\![\tau]\!]\, \emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\emptyset]})] \rfloor_{k-j+1} = \lfloor \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \emptyset \rfloor_{k-j+1}$.
  Hence, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \lfloor \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \emptyset \rfloor_{k-j+1}$.
  Thus, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \emptyset$, which follows from the definition of $\lfloor \cdot \rfloor_k$.

□

Lemma B.20 (λ^{rec} Substitutivity)

If $\Gamma \vdash v \leq v' : \tau_1$ *and* $\Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$,
then $\Gamma \vdash e[v/x] \leq e'[v'/x] : \tau_2$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Gamma \vdash e[v/x] : \tau_2$,
  which follows from Lemma B.5 applied to
  - $\Gamma \vdash v : \tau_1$,
    which follows from $\Gamma \vdash v \leq v' : \tau_1$, and
  - $\Gamma, x : \tau_1 \vdash e : \tau_2$,
    which follows from $\Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$.
- $\Gamma \vdash e'[v'/x] : \tau_2$, which follows analogously.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(e[v/x]), \gamma'(e'[v'/x])) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
Instantiate the second conjunct of $\Gamma \vdash v \leq v' : \tau_1$ with k, γ, and γ'. Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(v), \gamma'(v')) \in \mathcal{RC}\,[\![\tau_1]\!]\,\emptyset$.
Instantiate this with 0 and $\gamma(v)$.
Note that $\gamma(v)$ is a value. Hence,

- $\gamma(v) \longmapsto^0 \gamma(v)$, and
- $\mathit{irred}(\gamma(v))$.

Hence, there exists e'_f such that

- $\gamma'(v') \longmapsto^* e'_f$, and
- $(k - 0, \gamma(v), e'_f) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

Since $\gamma'(v')$ is a value, it follows that $\gamma'(v') \longmapsto^0 \gamma'(v')$. Hence $e'_f \equiv \gamma'(v')$.
Thus, $(k - 0, \gamma(v), e'_f) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$
$\equiv (k, \gamma(v), \gamma'(v')) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.
Instantiate the second conjunct of $\Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$ with k, $\gamma[x \mapsto \gamma(v)]$, and $\gamma'[x \mapsto \gamma'(v')]$.
Note that

- $k \geq 0$, and
- $(k, \gamma[x \mapsto \gamma(v)], \gamma'[x \mapsto \gamma'(v')]) \in \mathcal{RG}\,[\![\Gamma, x : \tau_1]\!]$,
  which follows from
  - $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$, and
  - $(k, \gamma(v), \gamma'(v')) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$, which follows from above.

Hence, $(k, \gamma[x \mapsto \gamma(v)](e), \gamma'[x \mapsto \gamma'(v')](e') \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$
$\equiv (k, \gamma(e[\gamma(v)/x]), \gamma'(e'[\gamma'(v')/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$
$\equiv (k, \gamma(e[v/x]), \gamma'(e'[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.

□

B.9 λ^{rec} Proofs: Reflexivity

Lemma B.21 (λ^{rec} Reflexivity)

If $\Gamma \vdash e : \tau$, *then* $\Gamma \vdash e \leq e : \tau$.

Proof

By induction on the derivation $\Gamma \vdash e : \tau$.

Each case follows from the corresponding compatibility lemma (i.e., Lemmas B.12 through B.19). $\square$

B.10 λ^{rec} Proofs: Transitivity

Lemma B.22 (λ^{rec} **Transitivity: Closed Terms)**

Let $\bullet \vdash \tau$.

(A) *If* $(k, v_1, v_2) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$ *and* $\forall z \geq 0.\ (z, v_2, v_3) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$, *then* $(k, v_1, v_3) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

(B) *If* $(k, e_1, e_2) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$ *and* $\forall z \geq 0.\ (z, e_2, e_3) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$, *then* $(k, e_1, e_3) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.

Proof

We simultaneously prove both **(A)** and **(B)** by induction on k and nested induction on the structure of the (closed) type τ.

(A) Case $k = 0$:

Case $(\mathsf{BoolTy})\ \dfrac{}{\bullet \vdash \mathsf{bool}}$:

We have as premises

(1) $(0, v_1, v_2) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$, and

(2) $\forall z \geq 0.\ (z, v_2, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$.

Hence, from **(1)** it follows that $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$.

Instantiate **(2)** with 0, noting that $0 \geq 0$.

Hence, $(0, v_2, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$.

From the latter it follows that $(v_2 = v_3 = \mathtt{tt}) \vee (v_2 = v_3 = \mathtt{ff})$.

We are required to show $(0, v_1, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$,

which follows from

- $\bullet \vdash v_3 : \mathsf{bool}$,
  which follows from $(0, v_2, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$.
- $(v_1 = v_3 = \mathtt{tt}) \vee (v_1 = v_3 = \mathtt{ff})$,
  which follows from $(v_1 = v_2 = v_3 = \mathtt{tt}) \vee (v_1 = v_2 = v_3 = \mathtt{ff})$,
  which follows from
  - $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$, and
  - $(v_2 = v_3 = \mathtt{tt}) \vee (v_2 = v_3 = \mathtt{ff})$.

Case $(\mathsf{FnTy})\ \dfrac{\bullet \vdash \tau_1 \qquad \bullet \vdash \tau_2}{\bullet \vdash \tau_1 \to \tau_2}$:

We have as premises

(1) $(0, v_1, v_2) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$, and

(2) $\forall z \geq 0.\ (z, v_2, v_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.

Hence, from **(1)** it follows that $v_1 \equiv \lambda x.\, e_1$ and $v_2 \equiv \lambda x.\, e_2$.

Instantiate **(2)** with 0, noting that $0 \geq 0$.

Hence, $(0, v_2, v_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.

From the latter it follows that $v_3 \equiv \lambda x.\, e_3$.

We are required to show $(0, \lambda x.\, e_1, \lambda x.\, e_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$,

which follows from

- $\bullet \vdash \lambda x.\, e_3 : (\tau_1 \to \tau_2)^{[\emptyset]}$,
  which follows from $(0, \lambda x.\, e_2, \lambda x.\, e_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.
- $\forall j < 0, v, v'.\ (j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset \implies (j, e_1[v/x], e_3[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$,
  which follows trivially since there is no j such that $0 \leq j < 0$.

Case $(\mathsf{RecTy})\ \dfrac{\bullet, \alpha \vdash \tau_1}{\bullet \vdash \mu\alpha.\,\tau_1}$:

We have as premises

(1) $(0, v_1, v_2) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset$, and

(2) $\forall z \geq 0.\ (z, v_2, v_3) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset$.

Hence, from **(1)** it follows that $v_1 \equiv \mathtt{fold}\, v_{11}$ and $v_2 \equiv \mathtt{fold}\, v_{22}$.

Instantiate **(2)** with 0, noting that $0 \geq 0$.

Hence, $(0, v_2, v_3) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset$.

From the latter it follows that $v_3 \equiv \mathtt{fold}\, v_{33}$.

We are required to show $(0, \mathtt{fold}\, v_{11}, \mathtt{fold}\, v_{33}) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset$, which follows from

- $\bullet \vdash \mathtt{fold}\, v_{33} : (\mu\alpha.\,\tau_1)^{[\emptyset]}$,
  which follows from $(0, \mathtt{fold}\, v_{22}, \mathtt{fold}\, v_{33}) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset$.
- $\forall j < 0.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset \rfloor_{j+1}$ in$(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]$,
  which follows trivially since there is no j such that $0 \leq j < 0$.

Case $k > 0$:

Case $(\mathsf{BoolTy})\ \dfrac{}{\bullet \vdash \mathsf{bool}}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$, and

(2) $\forall z \geq 0.\ (z, v_2, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$.

Hence, from **(1)** it follows that $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$.

Instantiate **(2)** with 0, noting that $0 \geq 0$.

Hence, $(0, v_2, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$.

From the latter it follows that $(v_2 = v_3 = \mathtt{tt}) \vee (v_2 = v_3 = \mathtt{ff})$.

We are required to show $(k, v_1, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$,

which follows from

- $\bullet \vdash v_3 : \mathsf{bool}$,
  which follows from $(0, v_2, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$.
- $(v_1 = v_3 = \mathtt{tt}) \vee (v_1 = v_3 = \mathtt{ff})$,
  which follows from $(v_1 = v_2 = v_3 = \mathtt{tt}) \vee (v_1 = v_2 = v_3 = \mathtt{ff})$,
  which follows from
  - $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$, and
  - $(v_2 = v_3 = \mathtt{tt}) \vee (v_2 = v_3 = \mathtt{ff})$.

Case $(\mathsf{FnTy})\ \dfrac{\bullet \vdash \tau_1 \qquad \bullet \vdash \tau_2}{\bullet \vdash \tau_1 \to \tau_2}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$, and

(2) $\forall z \geq 0.\ (z, v_2, v_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.

Hence, from **(1)** it follows that $v_1 \equiv \lambda x.\, e_1$ and $v_2 \equiv \lambda x.\, e_2$.

Instantiate **(2)** with 0, noting that $0 \geq 0$.

Hence, $(0, v_2, v_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.

From the latter it follows that $v_3 \equiv \lambda x.\, e_3$.

We are required to show $(k, \lambda x.\, e_1, \lambda x.\, e_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$,

which follows from

- $\bullet \vdash \lambda x.\, e_3 : (\tau_1 \to \tau_2)^{[\emptyset]}$,
  which follows from $(0, \lambda x.\, e_2, \lambda x.\, e_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.
- $\forall j < k, v, v'.\ (j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset \implies (j, e_1[v/x], e_3[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$:
  Consider arbitrary j, v, v' such that
  - $j < k$, and

- $(j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

Instantiate **(1)** with j, v, and v'. Note that

- $j < k$, and
- $(j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

Hence, $(j, e_1[v/x], e_2[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
Applying Lemma B.6 to $\bullet \vdash \tau_1$ and $(j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$, we conclude that $\bullet \vdash v' : \tau_1^{[\emptyset]}$.
Hence, by reflexivity (Lemma B.21) we conclude that $\bullet \vdash v' \leq v' : \tau_1$.
Hence, unwinding definitions, we have $\forall z \geq 0.\ (z, v', v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.
Consider arbitrary z' such that $z' \geq 0$.
Instantiate **(2)** with $z' + 1$.
Hence, $(z' + 1, \lambda x.\, e_2, \lambda x.\, e_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$.
Instantiate this with z', v', and v'. Note that

- $z' < z' + 1$, and
- $(z', v', v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$,
  which follows from $\forall z \geq 0.\ (z, v', v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$,
  which follows from above.

Hence, $(z', e_2[v'/x], e_3[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
Thus, $\forall z' \geq 0.\ (z', e_2[v'/x], e_3[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
Applying induction hypothesis **(B)** to $(j, e_1[v/x], e_2[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$ and $\forall z' \geq 0.\ (z', e_2[v'/x], e_3[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$, we conclude that $(j, e_1[v/x], e_3[v'/x]) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$.

Case $(\mathsf{RecTy})\ \dfrac{\bullet, \alpha \vdash \tau_1}{\bullet \vdash \mu\alpha.\, \tau_1}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset$, and

(2) $\forall z \geq 0.\ (z, v_2, v_3) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset$.

Hence, from **(1)** it follows that $v_1 \equiv \texttt{fold}\, v_{11}$ and $v_2 \equiv \texttt{fold}\, v_{22}$.
Instantiate **(2)** with 0, noting that $0 \geq 0$.
Hence, $(0, v_2, v_3) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset$.
From the latter it follows that $v_3 \equiv \texttt{fold}\, v_{33}$.
We are required to show $(k, \texttt{fold}\, v_{11}, \texttt{fold}\, v_{33}) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset$, which follows from

- $\bullet \vdash \texttt{fold}\, v_{33} : (\mu\alpha.\, \tau_1)^{[\emptyset]}$,
  which follows from $(0, \texttt{fold}\, v_{22}, \texttt{fold}\, v_{33}) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset$.
- $\forall j < k.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$ in $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})]$:
  Consider arbitrary j such that
  - $j < k$.

  Let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$.
  Note that from **(1)** we have
  - $\bullet \vdash \texttt{fold}\, v_{22} : (\mu\alpha.\, \tau)^{[\emptyset]}$, and
  - $\forall j < k.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$ in $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})]$.

  Instantiate $\forall j < k.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$ in $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})]$ with j and χ. Note that
  - $j < k$, and
  - $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$.

  Hence, $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})]$.
  Hence, $(j, v_{11}, v_{22}) \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})] \rfloor_{j+1}$, which follows from the definition of $\lfloor \cdot \rfloor_k$.
  Applying Lemma B.11 to $\bullet \vdash \mu\alpha.\, \tau_1$ and χ, we conclude that $\lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})] \rfloor_{j+1} = \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\, \tau_1/\alpha]]\!]\,\emptyset \rfloor_{j+1}$.

Hence, $(j, v_{11}, v_{22}) \in \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset \rfloor_{j+1}$.
Hence, $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Consider arbitrary z' such that $z' \geq 0$.
Instantiate **(2)** with $z' + 1$.
Hence, $(z' + 1, \texttt{fold}\, v_{22}, \texttt{fold}\, v_{33}) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset$, from which we have

- $\bullet \vdash \texttt{fold}\, v_{33} : (\mu\alpha.\,\tau)^{[\emptyset]}$, and
- $\forall j < z' + 1.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset \rfloor_{j+1} \implies (j, v_{22}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]$.

Instantiate $\forall j < z' + 1.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset \rfloor_{j+1}$ in $(j, v_{22}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]$ with z'. Note that

- $z' < z' + 1$.

Let $\chi' = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset \rfloor_{z'+1}$.
Hence, $(z', v_{22}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi', (\mu\alpha.\,\tau_1)^{[\emptyset]})]$.
Hence, $(z', v_{22}, v_{33}) \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi', (\mu\alpha.\,\tau_1)^{[\emptyset]})] \rfloor_{z'+1}$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Applying Lemma B.11 to $\bullet \vdash \mu\alpha.\,\tau_1$ and χ', we conclude that
$\lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi', (\mu\alpha.\,\tau_1)^{[\emptyset]})] \rfloor_{z'+1} = \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset \rfloor_{z'+1}$.
Hence, $(z', v_{22}, v_{33}) \in \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset \rfloor_{z'+1}$.
Hence, $(z', v_{22}, v_{33}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Thus, $\forall z' \geq 0.\ (z', v_{22}, v_{33}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$.
Applying the induction hypothesis **(A)** to $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$ and $\forall z' \geq 0.\ (z', v_{22}, v_{33}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$ — noting that we can apply the induction hypothesis here since $j < k$ — we conclude that $(j, v_{11}, v_{33} \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$.
Hence, $(j, v_{11}, v_{33} \in \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset \rfloor_{j+1}$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Applying Lemma B.11 to $\bullet \vdash \mu\alpha.\,\tau_1$ and $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset \rfloor_{j+1}$, we conclude that
$\lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})] \rfloor_{j+1} = \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset \rfloor_{j+1}$.
Hence, $(j, v_{11}, v_{33}) \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})] \rfloor_{j+1}$.
Hence, $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]$, which follows from the definition of $\lfloor\cdot\rfloor_k$.

(B) Case $k = 0$:

We are required to show $(0, e_1, e_3) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$, which is immediate from the definition of $\mathcal{RC}\,[\![\tau]\!]\,\emptyset$.

Case $k > 0$:

We have as premises

(1) $(k, e_1, e_2) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$, and

(2) $\forall z \geq 0.\ (z, e_2, e_3) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

Consider arbitrary j_1 and e_{f_1} such that

- $j_1 < k$,
- $e_1 \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Instantiate **(1)** with j_1 and e_{f_1}. Note that

- $j_1 < k$,
- $e_1 \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e_{f_2} such that

- $e_2 \longmapsto^{*} e_{f_2}$, and
- $(k - j_1, e_{f_1}, e_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

Hence, there exists $j_2 \geq 0$ such that $e_2 \longmapsto^{j_2} e_{f_2}$.
Consider arbitrary z' such that $z' \geq 0$.
Instantiate **(2)** with $z' + 1 + j_2$. Note that

- $z' + 1 + j_2 \geq 0$.

Hence, $(z' + 1 + j_2, e_2, e_3) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Instantiate this with j_2 and e_{f_2}. Note that

- $j_2 < z' + 1 + j_2$,
- $e_2 \longmapsto^{j_2} e_{f_2}$, and
- $\mathit{irred}(e_{f_2})$.

Hence, there exists e_{f_3} such that

- $e_3 \longmapsto^* e_{f_3}$, and
- $(z' + 1 + j_2 - j_2, e_{f_2}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$
  $\equiv (z' + 1, e_{f_2}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

Applying Lemma B.8 to $\bullet \vdash \tau$, we conclude that $\mathcal{RV}\,[\![\tau]\!]\,\emptyset \in \mathit{Rel}_\tau$.
By the definition of Rel_τ together with $(z'+1, e_{f_2}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$ and $z' \leq z'+1$, we conclude that $(z', e_{f_2}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.
Thus, $\forall z' \geq 0.\ (z', e_{f_2}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.
Pick $e'_f = e_{f_3}$.
We are required to show

- $e_3 \longmapsto^* e_{f_3}$,
  which follows from above, and
- $(k - j_1, e_{f_1}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$,
  which follows from **(A)** applied to $(k - j_1, e_{f_1}, e_{f_2} \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$ and $\forall z' \geq 0.\ (z', e_{f_2}, e_{f_3}) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$,

□

Lemma B.23 (λ^{rec} Transitivity)

If $\Gamma \vdash e_1 \leq e_2 : \tau$ *and* $\Gamma \vdash e_2 \leq e_3 : \tau$,
then $\Gamma \vdash e_1 \leq e_3 : \tau$.

Proof

The proof is in 2 parts.

I. We are required to show $\Gamma \vdash e_1 : \tau$ and $\Gamma \vdash e_3 : \tau$,
which follow (respectively) from $\Gamma \vdash e_1 \leq e_2 : \tau$ and $\Gamma \vdash e_2 \leq e_3 : \tau$.

II. Consider arbitrary k, γ, γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(e_1), \gamma'(e_3)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Consider arbitrary j_1, e_{f_1} such that

- $j_1 < k$,
- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Instantiate the second conjunct of $\Gamma \vdash e_1 \leq e_2 : \tau$ with k, γ, and γ'. Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(e_1), \gamma'(e_2)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Consider arbitrary z' such that $z' \geq 0$.
Applying Lemma B.7 to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$, we conclude that $\vdash \gamma' : \Gamma$.
Hence, by reflexivity (Lemma B.21) we conclude that $\forall x \in \mathit{dom}(\Gamma).\bullet \vdash \gamma'(x) \leq \gamma'(x) : \Gamma(x)$.
Hence, unwinding several definitions, we have $\forall z \geq 0.\ (z, \gamma', \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.
Hence, $(z', \gamma', \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.
Instantiate the second conjunct of $\Gamma \vdash e_2 \leq e_3 : \tau$ with z', γ', and γ'. Note that

- $z' \geq 0$, and
- $(z', \gamma', \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$, which follows from above.

Hence, $(z', \gamma'(e_2), \gamma'(e_3)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Thus, $\forall z' \geq 0.\ (z', \gamma'(e_2), \gamma'(e_3)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Applying Lemma B.22 **(B)** to $\bullet \vdash \tau$, $(k, \gamma(e_1), \gamma'(e_2)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$, and $\forall z' \geq 0.\ (z', \gamma'(e_2), \gamma'(e_3)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$, we conclude that $(k, \gamma(e_1), \gamma'(e_3)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.

□

B.11 λ^{rec} Proofs: Soundness w.r.t. Contextual Equivalence

In this section, we show that $\leq \subseteq \preceq^{ctx}$.

Lemma B.24 (λ^{rec} Context Compatibility: Id)

If $\Gamma_0 \supseteq \Gamma$,
then $\Gamma_0 \vdash [\cdot] \leq [\cdot] : (\Gamma \triangleright \tau) \rightsquigarrow \tau$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Gamma_0 \vdash [e] \leq [e'] : \tau \ \equiv \ \Gamma_0 \vdash e \leq e' : \tau$.
Consider arbitrary k, γ_0, and γ_0' such that

- $k \geq 0$, and
- $(k, \gamma_0, \gamma_0') \in \mathcal{RG}\,[\![\Gamma_0]\!]$.

We are required to show that $(k, \gamma_0(e), \gamma_0'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Let $\gamma = \gamma_0|_{dom(\Gamma)}$ and $\gamma' = \gamma_0'|_{dom(\Gamma)}$. Note that

- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
  which follows from $(k, \gamma_0, \gamma_0') \in \mathcal{RG}\,[\![\Gamma_0]\!]$ and $\Gamma_0 \supseteq \Gamma$, and
- $(k, \gamma_0(e), \gamma_0'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$
  $\equiv (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$,
  which follows from $FV(e) \subseteq dom(\Gamma)$ and $FV(e') \subseteq dom(\Gamma)$.

Hence, it suffices to show that $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Instantiate the second conjunct of $\Gamma \vdash e \leq e' : \tau$ with k, γ, and γ'. Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
  which follows from above.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$. □

Lemma B.25 (λ^{rec} Context Compatibility: If1)

If $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \mathsf{bool}$, $\Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, *and* $\Gamma_0 \vdash e_3 \leq e_3' : \tau_0$,
then $\Gamma_0 \vdash \mathtt{if}\, C, e_2, e_3 \leq \mathtt{if}\, C', e_2', e_3' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that
$\Gamma_0 \vdash \mathtt{if}\, C[e], e_2, e_3 \leq \mathtt{if}\, C'[e'], e_2', e_3' : \tau_0$.

Instantiate $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \mathsf{bool}$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_0 \vdash C[e] \leq C'[e'] : \mathsf{bool}$.

Applying Lemma B.14 to

- $\Gamma_0 \vdash C[e] \leq C'[e'] : \mathsf{bool}$,
- $\Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, and
- $\Gamma_0 \vdash e_3 \leq e_3' : \tau_0$,

we conclude that $\Gamma_0 \vdash \mathtt{if}\, C[e], e_2, e_3 \leq \mathtt{if}\, C'[e'], e_2', e_3' : \tau_0$. □

Lemma B.26 (λ^{rec} Context Compatibility: If2)

If $\Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$, $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$, *and* $\Gamma_0 \vdash e_3 \leq e_3' : \tau_0$,
then $\Gamma_0 \vdash \mathtt{if}\, e_1, C, e_3 \leq \mathtt{if}\, e_1', C', e_3' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that
$\Gamma_0 \vdash \mathtt{if}\, e_1, C[e], e_3 \leq \mathtt{if}\, e_1', C'[e'], e_3' : \tau_0$.

Instantiate $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$.

Applying Lemma B.14 to

- $\Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$,
- $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$, and
- $\Gamma_0 \vdash e_3 \leq e_3' : \tau_0$,

we conclude that $\Gamma_0 \vdash \mathtt{if}\, e_1, C[e], e_3 \leq \mathtt{if}\, e_1', C'[e'], e_3' : \tau_0$. □

Lemma B.27 (λ^{rec} Context Compatibility: If3)

If $\Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$, $\Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, *and* $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$,
then $\Gamma_0 \vdash \mathtt{if}\, e_1, e_2, C \leq \mathtt{if}\, e_1', e_2', C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that
$\Gamma_0 \vdash \mathtt{if}\, e_1, e_2, C[e] \leq \mathtt{if}\, e_1', e_2', C'[e'] : \tau_0$.

Instantiate $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$.

Applying Lemma B.14 to

- $\Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$,
- $\Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, and
- $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$,

we conclude that $\Gamma_0 \vdash \mathtt{if}\, e_1, e_2, C[e] \leq \mathtt{if}\, e_1', e_2', C'[e'] : \tau_0$. □

Lemma B.28 (λ^{rec} Context Compatibility: Fn)

If $\Gamma_0, x : \tau_1 \vdash C \leq C' : (\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2$,
then $\Gamma_0 \vdash \lambda x.\, C \leq \lambda x.\, C' : (\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)$.

Proof

Consider arbitrary e and e' such that

- $\Gamma, x : \tau_1 \vdash e \leq e' : \tau$.

We are required to show that $\Gamma_0 \vdash \lambda x.\, C[e] \leq \lambda x.\, C'[e'] : \tau_1 \to \tau_2$.

Instantiate $\Gamma_0, x : \tau_1 \vdash C \leq C' : (\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2$ with e and e', noting that $\Gamma, x : \tau_1 \vdash e \leq e' : \tau$.

Hence, $\Gamma_0, x : \tau_1 \vdash C[e] \leq C'[e'] : \tau_2$.

Applying Lemma B.16 to $\Gamma_0, x : \tau_1 \vdash C[e] \leq C'[e'] : \tau_2$, we conclude that $\Gamma_0 \vdash \lambda x.\, C[e] \leq \lambda x.\, C'[e'] : \tau_1 \to \tau_2$. □

Lemma B.29 (λ^{rec} Context Compatibility: App1)

If $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)$, *and* $\Gamma_0 \vdash e_2 \leq e_2' : \tau_1$,
then $\Gamma_0 \vdash C\, e_2 \leq C'\, e_2' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_2$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Gamma_0 \vdash (C[e])\, e_2 \leq (C'[e'])\, e_2' : \tau_2$.

Instantiate $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1 \to \tau_2$.

Applying Lemma B.17 to

- $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1 \to \tau_2$, and
- $\Gamma_0 \vdash e_2 \leq e_2' : \tau_1$,

we conclude that $\Gamma_0 \vdash (C[e])\, e_2 \leq (C'[e'])\, e_2' : \tau_2$. □

Lemma B.30 (λ^{rec} Context Compatibility: App2)

If $\Gamma_0 \vdash e \leq e' : \tau_1 \to \tau_2$, *and* $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$,
then $\Gamma_0 \vdash e\, C \leq e'\, C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_2$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Gamma_0 \vdash e_1\, (C[e]) \leq e_1'\, (C'[e']) : \tau_2$.

Instantiate $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1$.

Applying Lemma B.17 to

- $\Gamma_0 \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$, and
- $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1$,

we conclude that $\Gamma_0 \vdash e_1\, (C[e]) \leq e_1'\, (C'[e']) : \tau_2$. □

Lemma B.31 (λ^{rec} Context Compatibility: Fold)

If $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1[\mu\alpha.\, \tau_1/\alpha]$,
then $\Gamma_0 \vdash \mathtt{fold}\, C \leq \mathtt{fold}\, C' : (\Gamma \triangleright \tau) \rightsquigarrow (\mu\alpha.\, \tau_1)$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Gamma_0 \vdash \mathtt{fold}\, C[e] \leq \mathtt{fold}\, C'[e'] : \mu\alpha.\, tau_1$.

Instantiate $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1[\mu\alpha.\, \tau_1/\alpha]$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1[\mu\alpha.\, \tau_1/\alpha]$.

Applying Lemma B.18 to $\Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1[\mu\alpha.\, \tau_1/\alpha]$, we conclude that $\Gamma_0 \vdash \mathtt{fold}\, C[e] \leq \mathtt{fold}\, C'[e'] : \mu\alpha.\, \tau_1$. □

Lemma B.32 (λ^{rec} Context Compatibility: Unfold)

If $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow (\mu\alpha.\,\tau_1)$,
then $\Gamma_0 \vdash \mathtt{unfold}\, C \leq \mathtt{unfold}\, C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1[\mu\alpha.\,\tau_1/\alpha]$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Gamma_0 \vdash \mathtt{unfold}\, C[e] \leq \mathtt{unfold}\, C'[e'] : \tau_1[\mu\alpha.\,\tau_1/\alpha]$.

Instantiate $\Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \mu\alpha.\,\tau_1$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_0 \vdash C[e] \leq C'[e'] : \mu\alpha.\,\tau_1$.

Applying Lemma B.19 to $\Gamma_0 \vdash C[e] \leq C'[e'] : \mu\alpha.\,\tau_1$, we conclude that $\Gamma_0 \vdash \mathtt{fold}\, C[e] \leq \mathtt{fold}\, C'[e'] : \tau_1[\mu\alpha.\,\tau_1/\alpha]$. □

Lemma B.33 (λ^{rec} Context Compatibility: ctxt)

If $\Gamma_0 \vdash C_0 \leq C_0' : (\Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0$, *and* $\Gamma_1 \vdash C_1 \leq C_1' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$,
then $\Gamma_0 \vdash C_0[C_1[\cdot]] \leq C_0'[C_1'[\cdot]] : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Gamma_0 \vdash C_0[C_1[e]] \leq C_0'[C_1'[e']] : \tau_0$.

Instantiate $\Gamma_1 \vdash C_1 \leq C_1' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.

Hence, $\Gamma_1 \vdash C_1[e] \leq C_1'[e'] : \tau_1$.

Instantiate $\Gamma_0 \vdash C_0 \leq C_0' : (\Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0$ with $C_1[e]$ and $C_1'[e']$, noting that $\Gamma_1 \vdash C_1[e] \leq C_1'[e'] : \tau_1$.

Hence, $\Gamma_0 \vdash C_0[C_1[e]] \leq C_0'[C_1'[e']] : \tau_0$. □

Lemma B.34 (λ^{rec} Context Reflexivity)

If $\Gamma_1 \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, *then* $\Gamma_1 \vdash C \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$.

Proof

By induction on the derivation $\Gamma_1 \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$.

Each case follows from the corresponding compatibility lemma (i.e., Lemmas B.24 through B.32). □

Lemma B.35 ($\lambda^{\mathsf{rec}} : \ \leq \ \subseteq \ \preceq^{ctx}$)

If $\Gamma \vdash e \leq e' : \tau$, *then* $\Gamma \vdash e \preceq^{ctx} e' : \tau$.

Proof

Consider arbitrary C and τ_1 such that

- $\bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, and
- $C[e] \Downarrow$.

Hence, there exists some value v_f and some k such that

- $C[e] \longmapsto^k v_f$.

We are required to show that $C[e'] \Downarrow$.
Note that $\bullet \vdash C \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, which follows from Lemma B.34 applied to $\bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$.
Instantiate $\bullet \vdash C \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ with e and e', noting that $\Gamma \vdash e \leq e' : \tau$.
Hence, $\bullet \vdash C[e] \leq C[e'] : \tau_1$.
Instantiate this with $k+1$, $\emptyset$, and $\emptyset$. Note that

- $k + 1 \geq 0$, and
- $(k+1, \emptyset, \emptyset) \in \mathcal{RG}\,[\![\bullet]\!]$.

Hence, $(k+1, C[e], C[e']) \in \mathcal{RC}\,[\![\tau_1]\!]\,\emptyset$.
Instantiate this with k and v_f. Note that

- $k < k + 1$,
- $C[e] \longmapsto^k v_f$, and
- $\mathit{irred}(v_f)$, which follows from the fact that v_f is value.

Hence, there exists v'_f such that

- $C[e'] \longmapsto^* v'_f$, and
- $(k + 1 - k, v_f, v'_f) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

Hence, $C[e'] \Downarrow v'_f$. □

B.12 λ^{rec} Proofs: Completeness w.r.t. Contextual Equivalence

In this section, we show that $\preceq^{ctx} \subseteq \preceq^{ciu} \subseteq \leq$.

Lemma B.36 (λ^{rec} : $\preceq^{ctx}$ Congruence)

If $\Gamma \vdash e \preceq^{ctx} e' : \tau$ *and* $\Gamma_1 \vdash C_1 : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$,
then $\Gamma_1 \vdash C_1[e] \preceq^{ctx} C_1[e'] : \tau_1$.

Proof

Consider arbitrary C and τ_0 such that

- $\bullet \vdash C : (\Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0$, and
- $C[C_1[e]] \Downarrow$.

We are required to show that $C[C_1[e']] \Downarrow$.
Instantiate $\Gamma \vdash e \preceq^{ctx} e' : \tau$ with $C[C_1[\cdot]]$ and τ_0. Note that

- $\bullet \vdash C[C_1[\cdot]] : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0$, which follows using the (C-ctxt) rule:

$$(\mathsf{C\text{-}ctxt})\ \frac{\bullet \vdash C : (\Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0 \qquad \Gamma_1 \vdash C_1 : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1}{\bullet \vdash C[C_1[\cdot]] : (\Gamma \triangleright \tau) \rightsquigarrow \tau_0}$$

- $C[C_1[e]] \Downarrow$.

Hence, $C[C_1[e']] \Downarrow$. □

Lemma B.37 (λ^{rec} : $\preceq^{ctx} \subseteq \preceq^{ciu}$)

If $\Gamma \vdash e \preceq^{ctx} e' : \tau$
then $\Gamma \vdash e \preceq^{ciu} e' : \tau$.

Proof

Consider arbitrary γ, E, and τ_1 such that

- $\vdash \gamma : \Gamma$,
- $\bullet \vdash E : \tau \rightsquigarrow \tau_1$, and
- $E[\gamma(e)] \Downarrow$.

If $\gamma = \{x_1 \mapsto v_1, x_2 \mapsto v_2, \ldots, x_n \mapsto v_n\}$, then let $C_\gamma = (\lambda x_1.\, \lambda x_2.\, \ldots \lambda x_n.\, [\cdot])\, v_1\, v_2\, \ldots\, v_n$.
Note that $\bullet \vdash C_\gamma : (\Gamma \triangleright \tau) \rightsquigarrow \tau$. This follows (assuming $\Gamma = x_1{:}\tau_1, \ldots, x_n{:}\tau_n$) from:

$$\dfrac{\dfrac{x_1{:}\tau_1, \ldots, x_n{:}\tau_n \vdash [\cdot] : (\Gamma \triangleright \tau) \rightsquigarrow \tau}{\bullet \vdash \lambda(x_1, \ldots, x_n).\, [\cdot] : (\Gamma \triangleright \tau) \rightsquigarrow (\tau_1, \ldots, \tau_n) \to \tau} \qquad \bullet \vdash (v_1, \ldots, v_n) : (\tau_1, \ldots, \tau_n)}{\bullet \vdash (\lambda(x_1, \ldots, x_n).\, [\cdot])\, (v_1, \ldots, v_n) : (\Gamma \triangleright \tau) \rightsquigarrow \tau}$$

Note that

- $\bullet \vdash C_\gamma[e] \preceq^{ctx} C_\gamma[e'] : \tau$,
  which follows from Lemma B.36 applied to $\Gamma \vdash e \preceq^{ctx} e' : \tau$ and $\bullet \vdash C_\gamma : (\Gamma \triangleright \tau) \rightsquigarrow \tau$.

Instantiate this with E and τ_1. Note that

- $\bullet \vdash E : (\bullet \triangleright \tau) \rightsquigarrow \tau_1$,
  which is immediate from $\bullet \vdash E : \tau \rightsquigarrow \tau_1$, and
- $E[C_\gamma[e]] \Downarrow$, which follows from
  - $E[C_\gamma[e]] \longmapsto^* E[\gamma(e)]$,
    which follows from the operational semantics and an examination of C_γ, and
  - $E[\gamma(e)] \Downarrow$,
    which follows from above.

Hence, $E[C_\gamma[e']] \Downarrow$.

By the operational semantics, it must be that $E[C_\gamma[e']] \longmapsto^* E[\gamma(e')]$.

Hence, it must be that $E[\gamma(e')] \Downarrow$.

□

Lemma B.38 **(λ^{rec} Equivalence-Respecting: Closed Values)**

Let $\bullet \vdash \tau$.
If $(k, v_1, v_2) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$ *and* $\bullet \vdash v_2 \preceq^{ciu} v_3 : \tau$,
then $(k, v_1, v_3) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

Proof

By induction on k and nested induction on the structure of the (closed) type τ.

Case $(\mathsf{BoolTy})\ \dfrac{}{\bullet \vdash \mathsf{bool}}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$, and

(2) $\bullet \vdash v_2 \preceq^{ciu} v_3 : \mathsf{bool}$.

Hence, from **(1)** it follows that $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$.

From **(2)** it follows that $\bullet \vdash v_3 : \mathsf{bool}$. Hence, either $v_3 = \mathtt{tt}$ or $v_3 = \mathtt{ff}$.

We show that $v_2 = v_3$ by contradiction:

- Suppose $v_2 \neq v_3$. Then, either $v_2 = \mathtt{tt} \ \wedge\ v_3 = \mathtt{ff}$, or $v_2 = \mathtt{ff} \ \wedge\ v_3 = \mathtt{tt}$.

  Case $v_2 = \mathtt{tt} \ \wedge\ v_3 = \mathtt{ff}$:

  Instantiate **(2)** with $\emptyset$, $\mathtt{if}\,[\cdot], \mathtt{tt}, \mathtt{diverge}$, and bool. Note that

  - $\bullet \vdash \emptyset : \bullet$,
  - $\bullet \vdash \mathtt{if}\,[\cdot], \mathtt{tt}, \mathtt{diverge} : \mathsf{bool} \rightsquigarrow \mathsf{bool}$, and
  - $\mathtt{if}\,[v_2], \mathtt{tt}, \mathtt{diverge} \Downarrow$, since $v_2 = \mathtt{tt}$.

  Hence, $\mathtt{if}\,v_3, \mathtt{tt}, \mathtt{diverge} \Downarrow \ \equiv\ \mathtt{if}\,\mathtt{ff}, \mathtt{tt}, \mathtt{diverge} \Downarrow$, since $v_3 = \mathtt{ff}$.
  But clearly, $\mathtt{if}\,\mathtt{ff}, \mathtt{tt}, \mathtt{diverge} \longmapsto \mathtt{diverge}$ and $\mathtt{diverge} \Uparrow$. Hence, we have a contradiction.

  Case $v_2 = \mathtt{ff} \ \wedge\ v_3 = \mathtt{tt}$:

  Instantiate **(2)** with $\emptyset$, $\mathtt{if}\,[\cdot], \mathtt{diverge}, \mathtt{tt}$, and bool. Note that

  - $\bullet \vdash \emptyset : \bullet$,
  - $\bullet \vdash \mathtt{if}\,[\cdot], \mathtt{diverge}, \mathtt{tt} : \mathsf{bool} \rightsquigarrow \mathsf{bool}$, and
  - $\mathtt{if}\,[v_2], \mathtt{diverge}, \mathtt{tt} \Downarrow$, since $v_2 = \mathtt{ff}$.

  Hence, $\mathtt{if}\,v_3, \mathtt{diverge}, \mathtt{tt} \Downarrow \ \equiv\ \mathtt{if}\,\mathtt{tt}, \mathtt{diverge}, \mathtt{tt} \Downarrow$, since $v_3 = \mathtt{tt}$.
  But clearly, $\mathtt{if}\,\mathtt{tt}, \mathtt{diverge}, \mathtt{tt} \longmapsto \mathtt{diverge}$ and $\mathtt{diverge} \Uparrow$. Hence, we have a contradiction.

  Thus, it must be that $v_2 = v_3$.

We are required to show that $(k, v_1, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset$,
which follows from

- $\bullet \vdash v_3 : \mathsf{bool}$,
  which follows from $\bullet \vdash v_2 \preceq^{ctx} v_3 : \mathsf{bool}$.
- $(v_1 = v_3 = \mathtt{tt}) \vee (v_1 = v_3 = \mathtt{ff})$,
  which follows from $(v_1 = v_2 = v_3 = \mathtt{tt}) \vee (v_1 = v_2 = v_3 = \mathtt{ff})$,
  which follows from
  - $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$, and
  - $(v_2 = v_3 = \mathtt{tt}) \vee (v_2 = v_3 = \mathtt{ff})$.

Case $(\mathsf{FnTy})\ \dfrac{\bullet \vdash \tau_1 \qquad \bullet \vdash \tau_2}{\bullet \vdash \tau_1 \to \tau_2}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$, and
(2) $\bullet \vdash v_2 \preceq^{ciu} v_3 : \tau_1 \to \tau_2$.

Hence, from **(1)** it follows that $v_1 \equiv \lambda x.\, e_1$ and $v_2 \equiv \lambda x.\, e_2$.
From **(2)** it follows that $\bullet \vdash v_3 : \tau_1 \to \tau_2$. Hence, $v_3 \equiv \lambda x.\, e_3$.
We are required to show that $(k, \lambda x.\, e_1, \lambda x.\, e_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\emptyset$,
which follows from

- $\bullet \vdash \lambda x.\, e_3 : (\tau_1 \to \tau_2)^{[\emptyset]}$,
  which follows from **(2)**.
- $\forall j < k, v_{11}, v'_{11}.\ (j, v_{11}, v'_{11}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset \implies (j, e_1[v_{11}/x], e_3[v'_{11}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$:
  Consider arbitrary j, v_{11}, v'_{11} such that
  - $j < k$, and
  - $(j, v_{11}, v'_{11}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

  We are required to show that $(j, e_1[v_{11}/x], e_3[v'_{11}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
  Consider arbitrary i and $e_{f_{11}}$ such that
  - $i < j$,
  - $e_1[v_{11}/x] \longmapsto^i e_{f_{11}}$, and
  - $\mathit{irred}(e_{f_{11}})$.

  We are required to show that $\exists e'_f.\ e_3[v'_{11}/x] \longmapsto^* e'_f \ \wedge\ (j - i, e_{f_{11}}, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$.
  Instantiate the second conjunct of **(1)** with j, v_{11}, and v'_{11}. Note that
  - $j < k$, and
  - $(j, v_{11}, v'_{11}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

  Hence, $(j, e_1[v_{11}/x], e_2[v'_{11}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\emptyset$.
  Instantiate this with i and $e_{f_{11}}$. Note that
  - $i < j$,
  - $e_1[v_{11}/x] \longmapsto^i e_{f_{11}}$, and
  - $\mathit{irred}(e_{f_{11}})$.

  Hence, there exists $e_{f_{22}}$ such that
  - $e_2[v'_{11}/x] \longmapsto^* e_{f_{22}}$, and
  - $(j - i, e_{f_{11}}, e_{f_{22}}) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$.

  Hence, $e_{f_{11}} \equiv v_{f_{11}}$ and $e_{f_{22}} \equiv v_{f_{22}}$.
  Instantiate **(2)** with $\emptyset$, $[\cdot]\,v'_{11}$, and τ_2. Note that
  - $\bullet \vdash \emptyset : \bullet$,
  - $\bullet \vdash [\cdot]\,v'_{11} : (\tau_1 \to \tau_2) \rightsquigarrow \tau_2$, and
  - $(\lambda x.\, e_2)\,v'_{11} \Downarrow$,
    which follows from $(\lambda x.\, e_2)\,v'_{11} \longmapsto^1 e_2[v'_{11}/x]$ and $e_2[v'_{11}/x] \longmapsto^* v_{f_{22}}$,
    which follow from above.

  Hence, there exists $v_{f_{33}}$ such that $(\lambda x.\, e_3)\,v'_{11} \Downarrow v_{f_{33}}$.
  By the operational semantics, it must be that $(\lambda x.\, e_3)\,v'_{11} \longmapsto^1 e_3[v'_{11}/x]$.
  Hence, it must be that $e_3[v'_{11}/x] \Downarrow v_{f_{33}}$.
  We show that $\bullet \vdash v_{f_{22}} \preceq^{ciu} v_{f_{33}} : \tau_2$:

- Consider arbitrary γ_0, E_0 and τ_0 such that
  - $\bullet\gamma_0 : \bullet$, from which it follows that $\gamma_0 = \emptyset$,
  - $\bullet \vdash E_0 : \tau_2 \rightsquigarrow \tau_0$, and
  - $E_0[v_{f_{22}}] \Downarrow$.

  We are required to show that $E_0[v_{f_{33}}] \Downarrow$.
  Instantiate **(2)** with $\emptyset$, $E_0[[\cdot]\, v'_{11}]$, and τ_0. Note that
  - $\bullet \vdash \emptyset : \bullet$,
  - $\bullet \vdash E_0[[\cdot]\, v'_{11}] : (\tau_1 \to \tau_2) \rightsquigarrow \tau_0$, and
  - $E_0[[\lambda x.\, e_2]\, v'_{11}] \longmapsto^1 E_0[e_2[v'_{11}/x]] \longmapsto^* E_0[v_{f_{22}}] \Downarrow$.

  Hence, $E_0[[\lambda x.\, e_3]\, v'_{11}] \Downarrow$.
  By the operational semantics, it must be that $E_0[[\lambda x.\, e_3]\, v'_{11}] \longmapsto^1 E_0[e_3[v'_{11}/x]] \longmapsto^* E_0[v_{f_{33}}]$.
  Hence, it must be that $E_0[v_{f_{33}}] \Downarrow$.

Take $e'_f = v_{f_{33}}$.
We are required to show
- $e_3[v'_{11}/x] \longmapsto^* v_{f_{33}}$,
  which follows from above, and
- $(j - i, e_{f_{11}}, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$,
  which follows from the induction hypothesis applied to $\bullet \vdash \tau_2$, $(j - i, v_{f_{11}}, v_{f_{22}}) \in \mathcal{RV}\,[\![\tau_2]\!]\,\emptyset$, and $\bullet \vdash v_{f_{22}} \preceq^{ciu} v_{f_{33}} : \tau_2$.

Case (RecTy) $\dfrac{\bullet, \alpha \vdash \tau_1}{\bullet \vdash \mu\alpha.\, \tau_1}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset$, and
(2) $\bullet \vdash v_2 \preceq^{ciu} v_3 : \mu\alpha.\, \tau_1$.

Hence, from **(1)** it follows that $v_1 \equiv \mathtt{fold}\, v_{11}$ and $v_2 \equiv \mathtt{fold}\, v_{22}$.
From **(2)** it follows that $\bullet \vdash v_3 : \mu\alpha.\, \tau_1$. Hence, $v_3 \equiv \mathtt{fold}\, v_{33}$.
We are required to show that $(k, \mathtt{fold}\, v_{11}, \mathtt{fold}\, v_{33}) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset$,
which follows from

- $\bullet \vdash \mathtt{fold}\, v_{33} : (\mu\alpha.\, \tau_1)^{[\emptyset]}$,
  which follows from **(2)**.
- $\forall j < k.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$ in $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})]$:
  Consider arbitrary j such that
  - $j < k$

  Let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$.
  We are required to show that $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\emptyset]})]$.
  Instantiate the second conjunct of **(1)** with j. Note that
  - $j < k$, and
  - $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\emptyset \rfloor_{j+1}$.

Hence, $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]$.
Note that $(j, v_{11}, v_{22}) \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto \chi, (\mu\alpha.\,\tau_1)^{[\emptyset]}]\rfloor_{j+1}$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Applying Lemma B.11 to $\bullet \vdash \mu\alpha.\,\tau_1$ and χ, we conclude that $\lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]\rfloor_{j+1} = \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset\rfloor_{j+1}$.
Hence, $(j, v_{11}, v_{22}) \in \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset\rfloor_{j+1}$.
Hence, $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
We show that $\bullet \vdash v_{22} \preceq^{ciu} v_{33} : \tau_1[\mu\alpha.\,\tau_1/\alpha]$:

- Consider arbitrary γ_0, E_0 and τ_0 such that
  - $\bullet\gamma_0 : \bullet$, from which it follows that $\gamma_0 = \emptyset$,
  - $\bullet \vdash E_0 : \tau_1[\mu\alpha.\,\tau_1/\alpha] \rightsquigarrow \tau_0$, and
  - $E_0[v_{22}] \Downarrow$.

  We are required to show that $E_0[v_{33}] \Downarrow$.
  Instantiate **(2)** with $\emptyset$, $E_0[\texttt{unfold}\,[\cdot]]$, and τ_0. Note that
  - $\bullet \vdash \emptyset : \bullet$,
  - $\bullet \vdash E_0[\texttt{unfold}\,[\cdot]] : \mu\alpha.\,\tau_1 \rightsquigarrow \tau_0$, and
  - $E_0[\texttt{unfold}\,[\texttt{fold}\,v_{22}]] \longmapsto^1 E_0[v_{22}] \Downarrow$.

  Hence, $E_0[\texttt{unfold}\,[\texttt{fold}\,v_{33}]] \Downarrow$.
  By the operational semantics, it must be that $E_0[\texttt{unfold}\,[\texttt{fold}\,v_{33}]] \longmapsto^1 E_0[v_{33}]$.
  Hence, it must be that $E_0[v_{33}] \Downarrow$.

Applying the induction hypothesis to $\bullet \vdash \tau_1[\mu\alpha.\,\tau_1/\alpha]$, $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$, and $\bullet \vdash v_{22} \preceq^{ciu} v_{33} : \tau_1[\mu\alpha.\,\tau_1/\alpha]$, we conclude that $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset$.
Hence, $(j, v_{11}, v_{33}) \in \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset\rfloor_{j+1}$, which follows from the definition of $\lfloor\cdot\rfloor_k$.
Applying Lemma B.11 to $\bullet \vdash \mu\alpha.\,\tau_1$ and $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\emptyset\rfloor_{j+1}$, we conclude that $\lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]\rfloor_{j+1} = \lfloor \mathcal{RV}\,[\![\tau_1[\mu\alpha.\,\tau_1/\alpha]]\!]\,\emptyset\rfloor_{j+1}$.
Hence, $(j, v_{11}, v_{33}) \in \lfloor \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]\rfloor_{j+1}$.
Hence, $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\emptyset]})]$, which follows from the definition of $\lfloor\cdot\rfloor_k$.

□

Lemma B.39 (λ^{rec} : $\preceq^{ciu} \subseteq \leq$)

If $\Gamma \vdash e \preceq^{ciu} e' : \tau$
then $\Gamma \vdash e \leq e' : \tau$.

Proof

Consider arbitrary k, γ, and γ' such that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

We are required to show that $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Consider arbitrary j and e_f such that

- $j < k$,
- $\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Note that $\Gamma \vdash e \leq e : \tau$, which follows from Lemma B.21 applied to $\Gamma \vdash e : \tau$.
Instantiate $\Gamma \vdash e \leq e : \tau$ with k, γ, and γ'. Note that

- $k \geq 0$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(e), \gamma'(e)) \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$.
Instantiate this with j and e_f. Note that

- $j < k$,
- $\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, there exists e'_f such that

- $\gamma'(e) \longmapsto^{*} e'_f$, and
- $(k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$.

Note that $e_f \equiv v_f$ and $e'_f \equiv v'_f$.
Hence, $\gamma'(e) \Downarrow v'_f$.
Instantiate $\Gamma \vdash e \preceq^{ciu} e' : \tau$ with γ', $[\cdot]$, and τ. Note that

- $\vdash \gamma' : \Gamma$,
  which follows from Lemma B.7 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
- $\bullet \vdash [\cdot] : \tau \rightsquigarrow \tau$, and
- $\gamma'(e) \Downarrow$.

Hence, there exists v_f'' such that $\gamma'(e') \Downarrow v_f''$.

Let $e_f'' = v_f''$.

We are required to show that

- $\gamma'(e') \longmapsto^* v_f''$,
  which follows from above, and
- $(k - j, v_f, v_f'') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$,
  which follows from Lemma B.38 applied to
  - $\bullet \vdash \tau$,
  - $(k - j, v_f, v_f') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset$, and
  - $v_f' \preceq^{ciu} v_f'' : \tau$,
    which follows from
    - Consider arbitrary E_1 and τ_1 such that
      - $\bullet \vdash E_1 : \tau \rightsquigarrow \tau_1$, and
      - $E_1[v_f'] \Downarrow$.

      We are required to show that $E_1[v_f''] \Downarrow$.

      Instantiate $\Gamma \vdash e \preceq^{ciu} e' : \tau$ with γ', E_1, and τ_1. Note that
      - $\vdash \gamma' : \Gamma$,
        which follows from Lemma B.7 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$,
      - $\bullet \vdash E_1 : \tau \rightsquigarrow \tau_1$, and
      - $E_1[\gamma'(e)] \Downarrow$,
        which follows from
        - $E_1[\gamma'(e)] \longmapsto^* E_1[v_f]$,
          which follows from $\gamma'(e) \longmapsto^* v_f$, and
        - $E_1[v_f] \Downarrow$,
          which follows from above.

      Hence, $E_1[\gamma'(e')] \Downarrow$.

      By the operational semantics, it must be that $E_1[\gamma'(e')] \longmapsto^* E_1[v_f'']$, which follows from $\gamma'(e') \longmapsto^* v_f''$ above.

      Hence, it must be that $E_1[v_f''] \Downarrow$.

□

C Quantified Types

$$
\begin{array}{llll}
\textit{Types} & \tau & ::= & \mathsf{bool} \mid \tau_1 \to \tau_2 \mid \alpha \mid \mu\alpha.\,\tau \mid \forall\alpha.\,\tau \mid \exists\alpha.\,\tau \\
\textit{Expressions} & e & ::= & x \mid \mathtt{tt} \mid \mathtt{ff} \mid \mathtt{if}\, e_0, e_1, e_2 \mid \\
 & & & \lambda x.\, e \mid e_1\, e_2 \mid \mathtt{fold}\, e \mid \mathtt{unfold}\, e \mid \\
 & & & \Lambda.\, e \mid e\,[\,] \mid \mathtt{pack}\, e \mid \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, e_2 \\
\textit{Values} & v & ::= & x \mid \mathtt{tt} \mid \mathtt{ff} \mid \lambda x.\, e \mid \mathtt{fold}\, v \mid \Lambda.\, e \mid \mathtt{pack}\, v
\end{array}
$$

Figure 1: $\lambda^{\forall\exists}$ Syntax

$$
\begin{array}{llll}
\textit{Evaluation Contexts} & E & ::= & [\cdot] \mid \mathtt{if}\, E, e_1, e_2 \mid E\, e \mid v\, E \mid \mathtt{fold}\, E \mid \mathtt{unfold}\, E \mid \\
 & & & E\,[\,] \mid \mathtt{pack}\, E \mid \mathtt{unpack}\, E\, \mathtt{as}\, x\, \mathtt{in}\, e
\end{array}
$$

$$
\begin{array}{lrcl}
\textsf{(iftrue)} & \mathtt{if}\, \mathtt{tt}, e_1, e_2 & \longmapsto & e_1 \\
\textsf{(iffalse)} & \mathtt{if}\, \mathtt{ff}, e_1, e_2 & \longmapsto & e_2 \\
\textsf{(app)} & (\lambda x.\, e)\, v & \longmapsto & e[v/x] \\
\textsf{(unfold)} & \mathtt{unfold}\, (\mathtt{fold}\, v) & \longmapsto & v \\
\textsf{(inst)} & (\Lambda.\, e)\,[\,] & \longmapsto & e \\
\textsf{(unpack)} & \mathtt{unpack}\, (\mathtt{pack}\, v)\, \mathtt{as}\, x\, \mathtt{in}\, e & \longmapsto & e[v/x] \\
\textsf{(ctxt)} & \dfrac{e \longmapsto e'}{E[e] \longmapsto E[e']} & &
\end{array}
$$

Figure 2: $\lambda^{\forall\exists}$ Operational Semantics

Notation The notation $e \longmapsto e'$ denotes a single operational step. We write $e \longmapsto^j e'$ to denote that there exists a chain of j steps of the form $e \longmapsto e_1 \longmapsto \ldots \longmapsto e_j$ where e_j is e'. A term e is irreducible if it has no successor in the step relation, that is, $\mathit{irred}(e)$ if e is a value or if e is a "stuck" expression (such as $\mathtt{tt}(e')$) to which no operational rule applies. We also use the following abbreviations.

$$
\begin{array}{rcl}
e \longmapsto^* e' & \stackrel{\text{def}}{=} & \exists k \geq 0.\, e \longmapsto^k e' \\
e \Downarrow e' & \stackrel{\text{def}}{=} & e \longmapsto^* e' \wedge \mathit{irred}(e') \\
e \Downarrow & \stackrel{\text{def}}{=} & \exists e'.\, e \Downarrow e' \\
e \Uparrow & \stackrel{\text{def}}{=} & \forall k \geq 0.\, \exists e'.\, e \longmapsto^k e'
\end{array}
$$

$$\textit{Type Context} \quad \Delta \quad ::= \quad \bullet \mid \Delta, \alpha$$

$\boxed{\Delta \vdash \tau}$

$$(\mathsf{VarTy})\ \frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad (\mathsf{BoolTy})\ \frac{}{\Delta \vdash \mathsf{bool}} \qquad (\mathsf{FnTy})\ \frac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 \to \tau_2} \qquad (\mathsf{RecTy})\ \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \mu\alpha.\,\tau}$$

$$(\mathsf{AllTy})\ \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \forall\alpha.\,\tau} \qquad (\mathsf{ExTy})\ \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \exists\alpha.\,\tau}$$

Figure 3: $\lambda^{\forall\exists}$ Static Semantics I

$$\begin{array}{lllll} \textit{Type Context} & \Delta & ::= & \bullet \mid \Delta, \alpha \\ \textit{Value Context} & \Gamma & ::= & \bullet \mid \Gamma, x{:}\tau \end{array}$$

$\boxed{\Delta; \Gamma \vdash e : \tau}$

$$(\mathsf{True})\ \frac{}{\Delta; \Gamma \vdash \mathtt{tt} : \mathsf{bool}} \qquad (\mathsf{False})\ \frac{}{\Delta; \Gamma \vdash \mathtt{ff} : \mathsf{bool}} \qquad (\mathsf{If})\ \frac{\Delta; \Gamma \vdash e_0 : \mathsf{bool} \qquad \Delta; \Gamma \vdash e_1 : \tau \qquad \Delta; \Gamma \vdash e_2 : \tau}{\Delta; \Gamma \vdash \mathtt{if}\, e_0, e_1, e_2 : \tau}$$

$$(\mathsf{Var})\ \frac{}{\Delta; \Gamma \vdash x : \Gamma(x)} \qquad (\mathsf{Fn})\ \frac{\Delta; \Gamma, x{:}\tau_1 \vdash e : \tau_2}{\Delta; \Gamma \vdash \lambda x.\, e : \tau_1 \to \tau_2} \qquad (\mathsf{App})\ \frac{\Delta; \Gamma \vdash e_1 : \tau_1 \to \tau_2 \qquad \Delta; \Gamma \vdash e_2 : \tau_1}{\Delta; \Gamma \vdash e_1\, e_2 : \tau_2}$$

$$(\mathsf{Fold})\ \frac{\Delta; \Gamma \vdash e : \tau[\mu\alpha.\,\tau/\alpha]}{\Delta; \Gamma \vdash \mathtt{fold}\, e : \mu\alpha.\,\tau} \qquad (\mathsf{Unfold})\ \frac{\Delta; \Gamma \vdash e : \mu\alpha.\,\tau}{\Delta; \Gamma \vdash \mathtt{unfold}\, e : \tau[\mu\alpha.\,\tau/\alpha]}$$

$$(\mathsf{All})\ \frac{\Delta, \alpha; \Gamma \vdash e : \tau}{\Delta; \Gamma \vdash \Lambda.\, e : \forall\alpha.\,\tau} \qquad (\mathsf{Inst})\ \frac{\Delta; \Gamma \vdash e : \forall\alpha.\,\tau \qquad \Delta \vdash \tau_1}{\Delta; \Gamma \vdash e\,[\,] : \tau[\tau_1/\alpha]} \qquad (\mathsf{Pack})\ \frac{\Delta \vdash \tau_1 \qquad \Delta; \Gamma \vdash e : \tau[\tau_1/\alpha]}{\Delta; \Gamma \vdash \mathtt{pack}\, e : \exists\alpha.\,\tau}$$

$$(\mathsf{Unpack})\ \frac{\Delta; \Gamma \vdash e_1 : \exists\alpha.\,\tau_1 \qquad \Delta \vdash \tau_2 \qquad \Delta, \alpha; \Gamma, x : \tau_1 \vdash e_2 : \tau_2}{\Delta; \Gamma \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, e_2 : \tau_2}$$

Figure 4: $\lambda^{\forall\exists}$ Static Semantics II

C.1 $\lambda^{\forall\exists}$ Unary Model

Notation

- We write $\mathcal{V}[\![\tau]\!]$ for the semantic interpretation of types as values, $\mathcal{C}[\![\tau]\!]$ for the interpretation of types as computations, $\mathcal{G}[\![\Gamma]\!]$ for the interpretation of value contexts as value substitutions, and $\mathcal{D}[\![\Delta]\!]$ for the interpretation of type contexts as type substitutions (Figure 5).
- We use the metavariable σ to range over sets of tuples of the form (k, v) where k is a natural number and v is a closed value — i.e., $k \in \mathit{Nat}$ and $v \in \mathit{CValues}$.
- We use δ for mappings from type variables α to sets $\sigma \in 2^{\mathit{Nat} \times \mathit{CValues}}$.

$$\mathit{Type} \stackrel{\text{def}}{=} \{\sigma \in 2^{Nat \times CValues} \mid \forall (j,v) \in \sigma.\ \forall i \leq j.\ (i,v) \in \sigma\}$$

$$\lfloor \sigma \rfloor_k \stackrel{\text{def}}{=} \{(j,v) \mid j < k \ \wedge\ (j,v) \in \sigma\}$$

$$\begin{array}{rcl}
\mathcal{V}\,[\![\alpha]\!]\,\delta & = & \delta(\alpha) \\
\mathcal{V}\,[\![\mathsf{bool}]\!]\,\delta & = & \{(k,v) \mid v = \mathtt{tt} \ \vee\ v = \mathtt{ff}\} \\
\mathcal{V}\,[\![\tau_1 \to \tau_2]\!]\,\delta & = & \{(k, \lambda x.\, e) \mid \forall j < k, v. \\
 & & \qquad (j,v) \in \mathcal{V}\,[\![\tau_1]\!]\,\delta \implies \\
 & & \qquad (j, e[v/x]) \in \mathcal{C}\,[\![\tau_2]\!]\,\delta\} \\
\mathcal{V}\,[\![\mu\alpha.\, \tau]\!]\,\delta & = & \{(k, \mathtt{fold}\, v) \mid \forall j < k. \\
 & & \qquad \text{let } \sigma = \lfloor \mathcal{V}\,[\![\mu\alpha.\, \tau]\!]\,\delta \rfloor_{j+1} \text{ in} \\
 & & \qquad (j,v) \in \mathcal{V}\,[\![\tau]\!]\,\delta[\alpha \mapsto \sigma]\} \\
\mathcal{V}\,[\![\forall\alpha.\, \tau]\!]\,\delta & = & \{(k, \Lambda.\, e) \mid \forall j < k, \sigma. \\
 & & \qquad \sigma \in \mathit{Type} \implies (j,e) \in \mathcal{C}\,[\![\tau]\!]\,\delta[\alpha \mapsto \sigma]\} \\
\mathcal{V}\,[\![\exists\alpha.\, \tau]\!]\,\delta & = & \{(k, \mathtt{pack}\, v) \mid \exists\sigma.\ \sigma \in \mathit{Type} \ \wedge \\
 & & \qquad \forall j < k.\ (j,v) \in \mathcal{V}\,[\![\tau]\!]\,\delta[\alpha \mapsto \sigma]\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{C}\,[\![\tau]\!]\,\delta & = & \{(k,e) \mid \forall j < k, e_f. \\
 & & \qquad e \longmapsto^j e_f \wedge \mathit{irred}(e_f) \implies \\
 & & \qquad (k-j, e_f) \in \mathcal{V}\,[\![\tau]\!]\,\delta\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{D}\,[\![\bullet]\!] & = & \{\emptyset\} \\
\mathcal{D}\,[\![\Delta, \alpha]\!] & = & \{\delta[\alpha \mapsto \sigma] \mid \delta \in \mathcal{D}\,[\![\Delta]\!] \ \wedge\ \sigma \in \mathit{Type}\}
\end{array}$$

$$\begin{array}{rcl}
\mathcal{G}\,[\![\bullet]\!]\,\delta & = & \{(k,\emptyset)\} \\
\mathcal{G}\,[\![\Gamma, x:\tau]\!]\,\delta & = & \{(k, \gamma[x \mapsto v]) \mid \\
 & & \qquad (k,\gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\delta \wedge (k,v) \in \mathcal{V}\,[\![\tau]\!]\,\delta\}
\end{array}$$

$$\begin{array}{rcl}
[\![\Delta; \Gamma \vdash e : \tau]\!] & = & \forall k \geq 0.\ \forall \delta, \gamma. \\
 & & \qquad \delta \in \mathcal{D}\,[\![\Delta]\!] \ \wedge\ (k,\gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\delta \implies \\
 & & \qquad (k, \gamma(e)) \in \mathcal{C}\,[\![\tau]\!]\,\delta
\end{array}$$

Figure 5: $\lambda^{\forall\exists}$ Step-Indexed Unary Model

C.2 $\lambda^{\forall\exists}$ Relational (PER) Model

Notation

- We write $\mathcal{RV}[\![\tau]\!]$ for the relational interpretation of types as values, $\mathcal{RC}[\![\tau]\!]$ for the relational interpretation of types as computations, $\mathcal{RG}[\![\Gamma]\!]$ for the relational interpretation of value contexts as value substitutions, and $\mathcal{RD}[\![\Delta]\!]$ for the interpretation of type contexts as type substitutions (Figures 6-7).
- We use the metavariable χ to range over sets of tuples of the form (k, v, v') where k is a natural number and v,v' are closed values — i.e., $k \in \mathit{Nat}$ and $v, v' \in \mathit{CValues}$.
- We use ρ for mappings from type variables α to pairs (χ, τ) of sets $\chi \in 2^{\mathit{Nat} \times \mathit{CValues} \times \mathit{CValues}}$ and syntactic types τ.
- If $\rho(\alpha) = (\chi, \tau)$, the notation $\rho^{\mathsf{sem}}(\alpha)$ denotes χ, while $\rho^{\mathsf{syn}}(\alpha)$ denotes τ.
- We write $\vdash e : \tau$ as an abbreviation for $\bullet; \bullet \vdash e : \tau$.
- If $\mathit{dom}(\gamma) = \mathit{dom}(\Gamma)$, we use $\Delta \vdash \gamma : \Gamma$ as shorthand for $\forall x \in \mathit{dom}(\Gamma).\ \Delta; \bullet \vdash \gamma(x) : \Gamma(x)$.
- If $\rho = \{\alpha_1 \mapsto (\chi_1, \tau_1), \ldots, \alpha_n \mapsto (\chi_n, \tau_n)\}$, the notation $\tau^{[\rho]}$ is an abbreviation for $\tau[\tau_1/\alpha_1, \tau_2/\alpha_2, \ldots, \tau_n/\alpha_n]$.

$$Rel_\tau \stackrel{\text{def}}{=} \{\chi \in 2^{Nat \times CValues \times CValues} \mid \forall (j, v, v') \in \chi. \vdash v' : \tau \ \wedge \ \forall i \leq j.\ (i, v, v') \in \chi\}$$

$$\lfloor \chi \rfloor_k \stackrel{\text{def}}{=} \{(j, v, v') \mid \ j < k \ \wedge \ (j, v, v') \in \chi\}$$

$$\begin{aligned}
\mathcal{RV}\,[\![\alpha]\!]\,\rho &= \rho^{\mathsf{sem}}(\alpha) \\
\mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho &= \{(k, v, v') \mid \vdash v' : \mathsf{bool} \ \wedge \ (v = v' = \mathtt{tt} \ \vee \ v = v' = \mathtt{ff})\} \\
\mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho &= \{(k, \lambda x.\, e, \lambda x.\, e') \mid \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]} \ \wedge \ \forall j < k, v, v'. \\
&\qquad (j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho \implies (j, e[v/x], e'[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho\} \\
\mathcal{RV}\,[\![\mu\alpha.\, \tau]\!]\,\rho &= \{(k, \mathtt{fold}\, v, \mathtt{fold}\, v') \mid \vdash \mathtt{fold}\, v' : (\mu\alpha.\, \tau)^{[\rho]} \ \wedge \ \forall j < k. \\
&\qquad \text{let } \chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\, \tau]\!]\,\rho \rfloor_{j+1} \text{ in } (j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]\} \\
\mathcal{RV}\,[\![\forall\alpha.\, \tau]\!]\,\rho &= \{(k, \Lambda.\, e, \Lambda.\, e') \mid \vdash \Lambda.\, e' : (\forall\alpha.\, \tau)^{[\rho]} \ \wedge \ \forall \tau_2, \chi. \\
&\qquad \chi \in Rel_{\tau_2} \implies \forall j < k.\ (j, e, e') \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]\} \\
\mathcal{RV}\,[\![\exists\alpha.\, \tau]\!]\,\rho &= \{(k, \mathtt{pack}\, v, \mathtt{pack}\, v') \mid \vdash \mathtt{pack}\, v' : (\exists\alpha.\, \tau)^{[\rho]} \ \wedge \ \exists \tau_2, \chi. \\
&\qquad \chi \in Rel_{\tau_2} \ \wedge \ \forall j < k.\ (j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]\}
\end{aligned}$$

$$\mathcal{RC}\,[\![\tau]\!]\,\rho = \{(k, e, e') \mid \forall j < k, e_f.\ e \longmapsto^j e_f \wedge \mathit{irred}(e_f) \implies \exists e'_f.\ e' \longmapsto^* e'_f \wedge (k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau]\!]\,\rho\}$$

Figure 6: $\lambda^{\forall\exists}$ Step-Indexed Relational Model I

$$
\begin{array}{rcl}
\mathcal{RD}\,[\![\bullet]\!] & = & \{\emptyset\} \\
\mathcal{RD}\,[\![\Delta, \alpha]\!] & = & \{\rho[\alpha \mapsto (\chi, \tau_2)]) \mid \ \rho \in \mathcal{RD}\,[\![\Delta]\!] \ \wedge \ \chi \in Rel_{\tau_2}\}
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{RG}\,[\![\bullet]\!]\,\rho & = & \{(k, \emptyset, \emptyset)\} \\
\mathcal{RG}\,[\![\Gamma, x : \tau]\!]\,\rho & = & \{(k, \gamma[x \mapsto v], \gamma'[x \mapsto v']) \mid \\
 & & \quad (k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho \wedge (k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho\}
\end{array}
$$

$$
\begin{array}{rcl}
\Delta; \Gamma \vdash e \leq e' : \tau & \stackrel{\text{def}}{=} & \Delta; \Gamma \vdash e : \tau \ \wedge \ \Delta; \Gamma \vdash e' : \tau \ \wedge \\
 & & (\forall k \geq 0.\ \forall \rho, \gamma, \gamma'. \\
 & & \quad \rho \in \mathcal{RD}\,[\![\Delta]\!] \ \wedge \ (k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho \implies \\
 & & \quad (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\rho)
\end{array}
$$

$$
\Delta; \Gamma \vdash e \sim e' : \tau \quad \stackrel{\text{def}}{=} \quad \Delta; \Gamma \vdash e \leq e' : \tau \ \wedge \ \Delta; \Gamma \vdash e' \leq e : \tau
$$

Figure 7: $\lambda^{\forall\exists}$ Step-Indexed Relational Model II

C.3 $\lambda^{\forall\exists}$ Contexts and Contextual Equivalence

$$
\begin{array}{rrcl}
\textit{Contexts} & C & ::= & [\cdot] \mid \texttt{if}\, C, e_1, e_2 \mid \texttt{if}\, e_0, C, e_2 \mid \texttt{if}\, e_0, e_1, C \mid \\
& & & \lambda x.\, C \mid C\, e \mid e\, C \mid \texttt{fold}\, C \mid \texttt{unfold}\, C \\
& & & \Lambda.\, C \mid C\, [\,] \mid \texttt{pack}\, C \mid \texttt{unpack}\, C\, \texttt{as}\, x\, \texttt{in}\, e \mid \texttt{unpack}\, e\, \texttt{as}\, x\, \texttt{in}\, C
\end{array}
$$

Figure 8: $\lambda^{\forall\exists}$ Syntax - Contexts

$\boxed{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'}$

$$(\textsf{C-id})\ \frac{}{\Delta';\Gamma' \vdash [\cdot] : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau}\quad (\Delta' \supseteq \Delta, \Gamma' \supseteq \Gamma)$$

$$(\textsf{C-if1})\ \frac{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \mathsf{bool} \qquad \Delta';\Gamma' \vdash e_1 : \tau' \qquad \Delta';\Gamma' \vdash e_2 : \tau'}{\Delta';\Gamma' \vdash \mathtt{if}\, C, e_1, e_2 : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'}$$

$$(\textsf{C-if2})\ \frac{\Delta';\Gamma' \vdash e_0 : \mathsf{bool} \qquad \Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau' \qquad \Delta';\Gamma' \vdash e_2 : \tau'}{\Delta';\Gamma' \vdash \mathtt{if}\, e_0, C, e_2 : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'}$$

$$(\textsf{C-if3})\ \frac{\Delta';\Gamma' \vdash e_0 : \mathsf{bool} \qquad \Delta';\Gamma' \vdash e_1 : \tau' \qquad \Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'}{\Delta';\Gamma' \vdash \mathtt{if}\, e_0, e_1, C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'}$$

$$(\textsf{C-fn})\ \frac{\Delta';\Gamma', x : \tau_1 \vdash C : (\Delta;\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2}{\Delta';\Gamma' \vdash \lambda x.\, C : (\Delta;\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)}$$

$$(\textsf{C-app1})\ \frac{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2) \qquad \Delta';\Gamma' \vdash e : \tau_1}{\Delta';\Gamma' \vdash C\, e : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_2}$$

$$(\textsf{C-app2})\ \frac{\Delta';\Gamma' \vdash e : \tau_1 \to \tau_2 \qquad \Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1}{\Delta';\Gamma' \vdash e\, C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_2} \qquad (\textsf{C-fold})\ \frac{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'[\mu\alpha.\, \tau'/\alpha]}{\Delta';\Gamma' \vdash \mathtt{fold}\, C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \mu\alpha.\, \tau'}$$

$$(\textsf{C-unfold})\ \frac{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \mu\alpha.\, \tau'}{\Delta';\Gamma' \vdash \mathtt{unfold}\, C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'[\mu\alpha.\, \tau'/\alpha]} \qquad (\textsf{C-all})\ \frac{\Delta', \alpha;\Gamma' \vdash C : (\Delta, \alpha;\Gamma \triangleright \tau) \rightsquigarrow \tau_1}{\Delta';\Gamma' \vdash \Lambda.\, C : (\Delta, \alpha;\Gamma \triangleright \tau) \rightsquigarrow \forall\alpha.\, \tau_1}$$

$$(\textsf{C-inst})\ \frac{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \forall\alpha.\, \tau_1 \qquad \Delta' \vdash \tau_2}{\Delta';\Gamma' \vdash C\,[\,] : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow (\tau_1[\tau_2/\alpha])} \qquad (\textsf{C-pack})\ \frac{\Delta' \vdash \tau_2 \qquad \Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1[\tau_2/\alpha]}{\Delta';\Gamma' \vdash \mathtt{pack}\, C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \exists\alpha.\, \tau_1}$$

$$(\textsf{C-unpack1})\ \frac{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \exists\alpha.\, \tau_1 \qquad \Delta \vdash \tau_2 \qquad \Delta', \alpha;\Gamma', x : \tau_1 \vdash e_2 : \tau_2}{\Delta';\Gamma' \vdash \mathtt{unpack}\, C\, \mathtt{as}\, x\, \mathtt{in}\, e_2 : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_2}$$

$$(\textsf{C-unpack2})\ \frac{\Delta';\Gamma' \vdash e_1 : \exists\alpha.\, \tau_1 \qquad \Delta \vdash \tau_2 \qquad \Delta', \alpha;\Gamma', x : \tau_1 \vdash C : (\Delta, \alpha;\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2}{\Delta';\Gamma' \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, C : (\Delta, \alpha;\Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2}$$

$$(\textsf{C-ctxt})\ \frac{\Delta';\Gamma' \vdash C : (\Delta_1;\Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau' \qquad \Delta_1;\Gamma_1 \vdash C_1 : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1}{\Delta';\Gamma' \vdash C[C_1[\cdot]] : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau'}$$

$\boxed{\Delta';\Gamma' \vdash C[e] : \tau'}$

$$(\textsf{C-exp})\ \frac{\Delta';\Gamma' \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau' \qquad \Delta;\Gamma \vdash e : \tau}{\Delta';\Gamma' \vdash C[e] : \tau'}$$

Figure 9: $\lambda^{\forall\exists}$ Static Semantics - Contexts

Definition C.1 (Contextual Approximation ($\preceq^{ctx}$) and Equivalence ($\simeq^{ctx}$))

Let e and e' be expressions such that $\Delta;\Gamma \vdash e : \tau$ and $\Delta;\Gamma \vdash e' : \tau$.

$$\Delta;\Gamma \vdash e \preceq^{ctx} e' : \tau \quad \stackrel{\text{def}}{=} \quad \forall C, \tau_1.\ \bullet;\bullet \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge\ C[e]\Downarrow \implies C[e']\Downarrow$$

$$\Delta;\Gamma \vdash e \simeq^{ctx} e' : \tau \quad \stackrel{\text{def}}{=} \quad \begin{array}{l} \Delta;\Gamma \vdash e \preceq^{ctx} e' : \tau \ \wedge \\ \Delta;\Gamma \vdash e' \preceq^{ctx} e : \tau \end{array}$$

Figure 10: $\lambda^{\forall\exists}$ Contextual Approximation and Equivalence

Note: To prove that our logical relation ($\leq$) is sound with respect to contextual equivalence ($\preceq^{ctx}$) (see Section C.10), we first define what it means for two contexts to be logically related as follows:

$$\Delta_1;\Gamma_1 \vdash C \leq C' : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \quad \stackrel{\text{def}}{=} \quad \forall e, e'.\ \Delta;\Gamma \vdash e \leq e' : \tau \implies \Delta_1;\Gamma_1 \vdash C[e] \leq C'[e'] : \tau_1$$

$$\Delta_1;\Gamma_1 \vdash C \sim C' : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \quad \stackrel{\text{def}}{=} \quad \begin{array}{l} \Delta_1;\Gamma_1 \vdash C \leq C' : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge \\ \Delta_1;\Gamma_1 \vdash C' \leq C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \end{array}$$

Figure 11: $\lambda^{\forall\exists}$ Step-Indexed Logical Relation - Contexts

C.4 $\lambda^{\forall\exists}$ Evaluation Contexts and Ciu Equivalence

- The syntax of $\lambda^{\forall\exists}$ evaluation contexts E is given in Figure 2.
- Note that evaluation contexts E are simply a subset of general contexts C and that only closed terms can be placed in an evaluation context. Hence, typing judgments for evaluation contexts have the form $\Delta_1; \Gamma_1 \vdash (\bullet; \bullet \triangleright \tau) \rightsquigarrow \tau_1$.

Definition C.2 (Ciu Approximation ($\preceq^{ciu}$) and Equivalence ($\simeq^{ciu}$))

Let e and e' be expressions such that $\Delta; \Gamma \vdash e : \tau$ and $\Delta; \Gamma \vdash e' : \tau$.
Let δ be a mapping from type variables α to closed syntactic types τ. We write $\delta \models \Delta$ whenever $dom(\delta) = \Delta$.

$$\begin{array}{lcl} \Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau & \stackrel{\text{def}}{=} & \forall \delta, \gamma, E, \tau_1. \\ & & \quad \delta \models \Delta \ \wedge \\ & & \quad \vdash \gamma : \delta(\Gamma) \ \wedge \\ & & \quad \bullet; \bullet \vdash E : (\bullet; \bullet \triangleright \delta(\tau)) \rightsquigarrow \tau_1 \ \wedge \\ & & \quad E[\gamma(e)] \Downarrow \implies E[\gamma(e')] \Downarrow \end{array}$$

$$\begin{array}{lcl} \Delta; \Gamma \vdash e \simeq^{ciu} e' : \tau & \stackrel{\text{def}}{=} & \Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau \ \wedge \\ & & \Delta; \Gamma \vdash e' \preceq^{ciu} e : \tau \end{array}$$

Figure 12: $\lambda^{\forall\exists}$ Ciu Approximation and Equivalence

C.5 $\lambda^{\forall\exists}$ Proofs: Type Soundness and Substitution

Lemma C.3 **($\lambda^{\forall\exists}$ Valid Type: $\mathcal{V}\,[\![\tau]\!]\,\delta \in \mathit{Type}$)**

Let $\delta \in \mathcal{D}\,[\![\Delta]\!]$ and $\Delta \vdash \tau$.
Then $\mathcal{V}\,[\![\tau]\!]\,\delta \in \mathit{Type}$.

Proof

By the definition of *Type*, it suffices to show:

$$\forall (k, v) \in \mathcal{V}\,[\![\tau]\!]\,\delta.\ \forall j \leq k.\ (j, v) \in \mathcal{V}\,[\![\tau]\!]\,\delta$$

The proof is by induction on the derivation $\Delta \vdash \tau$. □

Lemma C.4 **($\lambda^{\forall\exists}$ Safety)**

If $\bullet; \bullet \vdash e : \tau$ and $e \longmapsto^* e'$, then either e' is a value, or there exists an e'' such that $e' \longmapsto e''$.

Proof

Prove the soundness of each typing rule using the unary indexed model of $\lambda^{\forall\exists}$ (Figure 5). □

Lemma C.5 **($\lambda^{\forall\exists}$ Value Substitution)**

If $\Delta; \Gamma \vdash v : \tau_1$ and $\Delta; \Gamma, x : \tau_1 \vdash e : \tau_2$,
then $\Delta; \Gamma \vdash e[v/x] : \tau_2$.

Proof

□

Lemma C.6 **($\lambda^{\forall\exists}$ Type Substitution)**

If $\Delta \vdash \tau_1$ and $\Delta, \alpha; \Gamma \vdash e : \tau_2$,
then $\Delta; \Gamma[\tau_1/\alpha] \vdash e : \tau_2[\tau_1/\alpha]$.

Proof

□

C.6 $\lambda^{\forall\exists}$ Proofs: Validity of Pers

The goal of this section, is to show that each $\lambda^{\forall\exists}$ type τ is a valid type — that is, $\mathcal{RV}\,[\![\tau]\!]\,\rho \in \mathit{Rel}_{\tau^{[\rho]}}$. Specifically, this involves showing that the relational interpretation of a type τ satisfies the well-typedness requirement and is closed under decreasing step-index.

Lemma C.7 ($\lambda^{\forall\exists}$ Per Values Well-Typed)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau$.
If $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$,
then $\vdash v' : \tau^{[\rho]}$.

Proof

By induction on the derivation $\Delta \vdash \tau$.

We only show the (VarTy) case.

In each of the remaining cases, the result is immediate from the definition of $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, which requires that $\vdash v' : \tau^{[\rho]}$.

Case (VarTy) $\dfrac{\alpha \in \Delta}{\Delta \vdash \alpha}$:

Note that $\alpha^{[\rho]} \equiv \rho^{\mathsf{syn}}(\alpha)$.

Hence, we are required to show that $\vdash v' : \rho^{\mathsf{syn}}(\alpha)$.

Note that from $(k, v, v') \in \mathcal{RV}\,[\![\alpha]\!]\,\rho$ it follows that $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.

Note that from $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\alpha \in \Delta$ it follows that there exists τ such that

- $\rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_\tau$, and
- $\rho^{\mathsf{syn}}(\alpha) \equiv \tau$.

By the definition of Rel_τ, since $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_\tau$, it follows that $\vdash v' : \tau$.

Hence, $\vdash v' : \rho^{\mathsf{syn}}(\alpha)$.

□

Lemma C.8 ($\lambda^{\forall\exists}$ Per Value-Context Substitutions Well-Typed)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \Gamma$.
If $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$,
then $\vdash \gamma' : \Gamma^{[\rho]}$.

Proof

By induction on Γ.

Case $\Gamma = \bullet$:

From $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\bullet]\!]\,\rho$ we conclude that $\gamma = \gamma' = \emptyset$.

Hence, we are required to show that $\vdash \emptyset : \bullet^{[\rho]} \;\equiv\; \vdash \emptyset : \bullet$, which follows trivially.

Case $\Gamma = \Gamma_1, x : \tau$:

From $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma_1, x : \tau]\!]\,\rho$ we conclude that there exist γ_1, γ_1', v, and v' such that

- $\gamma \equiv \gamma_1[x \mapsto v]$,

- $\gamma' \equiv \gamma_1'[x \mapsto v']$,
- $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]\,\rho$, and
- $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

Hence, we are required to show that $\vdash \gamma_1'[x \mapsto v'] : (\Gamma_1, x : \tau)^{[\rho]}$,
which follows from

- $\vdash \gamma_1' : (\Gamma_1)^{[\rho]}$,
  which follows from the induction hypothesis applied to $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]\,\rho$, and
- $\vdash v' : \tau^{[\rho]}$,
  which follows from Lemma C.7 applied to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, $\Delta \vdash \tau$, and $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

□

Lemma C.9 **($\lambda^{\forall\exists}$ Per Types Downward Closed)**

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau$.
If $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$ *and* $j \leq k$,
then $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

Proof

The proof is by induction on the derivation $\Delta \vdash \tau$.

Case (VarTy) $\dfrac{\alpha \in \Delta}{\Delta \vdash \alpha}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\alpha]\!]\,\rho$, it follows that $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.
We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\alpha]\!]\,\rho$
$\equiv (j, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.

Note that

- $\rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$,
  which follows from $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, $\alpha \in \Delta$, and the definition of $\mathcal{RD}\,[\![\Delta]\!]$.

Hence, by the definition of $\mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$, since $(k, v, v') \in \rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$ and $j \leq k$, it follows that $(j, v, v') \in \rho^{\mathsf{sem}}(\alpha)$.

Case (BoolTy) $\dfrac{}{\Delta \vdash \mathsf{bool}}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$ it follows that

- $\vdash v' : \mathsf{bool}$, and
- either $v = v' = \mathtt{tt}$ or $v = v' = \mathtt{ff}$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$,
which follows from

- $\vdash v' : \mathsf{bool}$, and
- $v = v' = \mathtt{tt} \;\vee\; v = v' = \mathtt{ff}$.

Case (FnTy) $\dfrac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 \to \tau_2}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$ it follows that $v \equiv \lambda x.\, e$ and $v' \equiv \lambda x.\, e'$.
Note that

(A) $\vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]}$, and

(B) $\forall i < k, v_1, v_1'.\ (i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho \implies$
$(i, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$
$\equiv (j, \lambda x.\, e, \lambda x.\, e') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$.

(C) Consider arbitrary, i, v_1, v_1' such that

- $i < j$, and
- $(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

Instantiate **(B)** with i, v_1, and v_1'. Note that

- $i < k$, which follows from $i < j$ and $j \leq k$, and
- $(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

Hence, $(i, e[v_1/x], e'[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.

From **(A)** and **(C)** it follows that $(j, \lambda x.\, e, \lambda x.\, e') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$.

Case $(\mathsf{RecTy})\ \dfrac{\Delta, \alpha \vdash \tau_1}{\Delta \vdash \mu\alpha.\,\tau_1}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$ it follows that $v \equiv \mathtt{fold}\,v_1$ and $v' \equiv \mathtt{fold}\,v_1'$.

Note that

(A) $\vdash \mathtt{fold}\,v_1' : (\mu\alpha.\,\tau_1)^{[\rho]}$, and

(B) $\forall i < k.$ let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho \rfloor_{i+1}$ in
$(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\rho]})]$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$
$\equiv (j, \mathtt{fold}\,v_1, \mathtt{fold}\,v_1') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$.

(C) Consider arbitrary i such that

- $i < j$.

Let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho \rfloor_{i+1}$.

Instantiate **(B)** with i, noting that

- $i < k$, which follows from $i < j$ and $j \leq k$.

Hence, $(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\rho]})]$.

From **(A)**, and **(C)** it follows that $(j, \mathtt{fold}\,v_1, \mathtt{fold}\,v_1') \in \mathcal{RV}\,[\![\mu\alpha.\,\tau_1]\!]\,\rho$.

Case $(\mathsf{AllTy})\ \dfrac{\Delta, \alpha \vdash \tau_1}{\Delta \vdash \forall\alpha.\,\tau_1}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\forall\alpha.\,\tau_1]\!]\,\rho$ it follows that $v \equiv \Lambda.\,e$ and $v' \equiv \Lambda.\,e'$.

Note that

(A) $\vdash \Lambda.\,e' : (\forall\alpha.\,\tau_1)^{[\rho]}$, and

(B) $\forall \tau_2, \chi.\ \chi \in Rel_{\tau_2} \implies$
$\forall i < k.\ (i, e, e') \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\forall\alpha.\,\tau_1]\!]\,\rho$
$\equiv (j, \Lambda.\,e, \Lambda.\,e') \in \mathcal{RV}\,[\![\forall\alpha.\,\tau_1]\!]\,\rho$.

(C) Consider arbitrary, τ_2, χ such that

- $\chi \in Rel_{\tau_2}$.

Consider arbitrary i such that

- $i < j$.

Instantiate **(B)** with τ_2, and χ. Note that

- $\chi \in Rel_{\tau_2}$.

Hence, $\forall i < k.\ (i, e, e') \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

Instantiate this with i. Note that

- $i < k$, which follows from $i < j$ and $j \leq k$.

Hence, $(i, e, e') \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

From **(A)** and **(C)** it follows that $(j, \Lambda.\,e, \Lambda.\,e') \in \mathcal{RV}\,[\![\forall\alpha.\,\tau_1]\!]\,\rho$.

Case $(\mathsf{ExTy})\ \dfrac{\Delta, \alpha \vdash \tau_1}{\Delta \vdash \exists\alpha.\,\tau_1}$:

From $(k, v, v') \in \mathcal{RV}\,[\![\exists\alpha.\,\tau_1]\!]\,\rho$ it follows that $v \equiv \mathtt{pack}\,v_1$ and $v' \equiv \mathtt{pack}\,v_1'$.

Note that

(A) $\vdash \mathtt{pack}\,v_1' : (\exists\alpha.\,\tau_1)^{[\rho]}$, and

(B) $\exists \tau_2, \chi.\ \chi \in Rel_{\tau_2}\ \wedge$
$\forall i < k.\ (i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

We are required to show that $(j, v, v') \in \mathcal{RV}\,[\![\exists\alpha.\,\tau_1]\!]\,\rho$
$\equiv (j, \mathtt{pack}\,v_1, \mathtt{pack}\,v_1') \in \mathcal{RV}\,[\![\exists\alpha.\,\tau_1]\!]\,\rho$.

(C) From **(B)** it follows that there exist τ_2 and χ such that

- $\chi \in Rel_{\tau_2}$, and
- $\forall i < k.\ (i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

Consider arbitrary, i such that

- $i < j$.

Instantiate $\forall i < k.\ (i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$ with i. Note that

- $i < k$, which follows from $i < j$ and $j \leq k$.

Hence, $(i, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

From **(A)** and **(C)** it follows that $(j, \texttt{pack}\, v_1, \texttt{pack}\, v_1') \in \mathcal{RV}\,[\![\exists \alpha.\, \tau_1]\!]\,\rho$.

□

Lemma C.10 **($\lambda^{\forall\exists}$ Per Value Contexts Downward Closed)**

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \Gamma$.
If $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ *and* $j \leq k$,
then $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Proof

Proof by induction on Γ.

Case $\Gamma = \bullet$:

We are required to show that $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\bullet]\!]\,\rho$.
Note that $\gamma = \gamma' = \emptyset$, which follows from $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\bullet]\!]\,\rho$.
Hence, we are required to show that $(j, \emptyset, \emptyset) \in \mathcal{RG}\,[\![\bullet]\!]\,\rho$, which follows trivially.

Case $\Gamma = \Gamma_1, x : \tau$:

From $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma_1, x : \tau]\!]\,\rho$, we conclude that there exist γ_1, γ_1', v, and v' such that

- $\gamma \equiv \gamma_1[x \mapsto v]$,
- $\gamma' \equiv \gamma_1'[x \mapsto v']$,
- $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]\,\rho$, and
- $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

Hence, we are required to show that $(j, \gamma_1[x \mapsto v], \gamma_1'[x \mapsto v']) \in \mathcal{RG}\,[\![\Gamma_1, x : \tau]\!]\,\rho$,
which follows from

- $(j, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]\,\rho$,
  which follows from the induction hypothesis applied to $(k, \gamma_1, \gamma_1') \in \mathcal{RG}\,[\![\Gamma_1]\!]\,\rho$ and $j \leq k$, and
- $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$,
  which follows from Lemma C.9 applied to
  - $\rho \in \mathcal{RD}\,[\![\Delta]\!]$,
  - $\Delta \vdash \tau$,
  - $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, and
  - $j \leq k$.

□

Lemma C.11 **($\lambda^{\forall\exists}$ Valid Per: $\mathcal{RV}\,[\![\tau]\!]\,\rho \in Rel_{\tau^{[\rho]}}$)**

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\Delta \vdash \tau$.
Then $\mathcal{RV}\,[\![\tau]\!]\,\rho \in Rel_{\tau^{[\rho]}}$.

Proof

By the definition of $Rel_{\tau^{[\rho]}}$, it suffices to show:

$$\forall (k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho.\ \vdash v' : \tau^{[\rho]}\ \wedge\ \forall j \leq k.\ (j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$$

Consider arbitrary $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

- Applying Lemma C.7 to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, $\Delta \vdash \tau$, and $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, it follows that $\vdash v' : \tau^{[\rho]}$.
- Consider arbitrary $j \leq k$.

  Applying Lemma C.9 to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, $\Delta \vdash \tau$, $(k, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, and $j \leq k$, it follows that $(j, v, v') \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

□

C.7 $\lambda^{\forall\exists}$ Proofs: Per Type Substitution

Lemma C.12 ($\lambda^{\forall\exists}$ Per Type Substitution)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau_1$.
Let $\chi = \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.
Then $\mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})] = \mathcal{RV}\,[\![\tau[\tau_1/\alpha]]\!]\,\rho$.

Proof

□

Lemma C.13 ($\lambda^{\forall\exists}$ Per Type Substitution: Value Contexts)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau_1$.
Let $\chi = \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.
Then $\mathcal{RG}\,[\![\Gamma]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})] = \mathcal{RG}\,[\![\Gamma[\tau_1/\alpha]]\!]\,\rho$.

Proof

□

Lemma C.14 ($\lambda^{\forall\exists}$ Per Type Substitution: Recursive Types)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \mu\alpha.\,\tau$.
Let $\chi = \lfloor \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\rho \rfloor_{i+1}$.
Then $\lfloor \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} = \lfloor \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1}$.

Proof

We are required to show that for all $k \leq i$, v, and v',

$$(k, v, v') \in \lfloor \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau)^{[\rho]})] \rfloor_{i+1} \text{ iff } (k, v, v') \in \lfloor \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho \rfloor_{i+1}$$

The proof is by induction on i and nested induction on $\Delta, \alpha \vdash \tau$. □

C.8 $\lambda^{\forall\exists}$ Proofs: Fundamental Property of the Logical Relation

The Fundamental Property of a logical relation holds if the latter is a congruence — that is, if it satisfies the compatibility and substitutivity properties.

Lemma C.15 ($\lambda^{\forall\exists}$ Compatibility-True)

$\Delta; \Gamma \vdash \mathtt{tt} \leq \mathtt{tt} : \mathsf{bool}$.

Proof

The proof is in 2 parts.

I. We are required to show $\Delta; \Gamma \vdash \mathtt{tt} : \mathsf{bool}$, which is immediate.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\mathtt{tt}), \gamma'(\mathtt{tt})) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\rho$
$\equiv (k, \mathtt{tt}, \mathtt{tt}) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{tt} \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Since $\mathtt{tt}$ is a value, we have $\mathit{irred}(\mathtt{tt})$.
Hence, $j = 0$ and $e_f \equiv \mathtt{tt}$.
Let $e'_f = \mathtt{tt}$.
We are required to show that

- $\mathtt{tt} \longmapsto^* \mathtt{tt}$,
  which is immediate, and
- $(k - 0, \mathtt{tt}, \mathtt{tt}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$,
  which follows from
  - $\vdash \mathtt{tt} : \mathsf{bool}$, and
  - $\mathtt{tt} = \mathtt{tt} = \mathtt{tt}$.

□

Lemma C.16 ($\lambda^{\forall\exists}$ Compatibility-False)

$\Delta; \Gamma \vdash \texttt{ff} \leq \texttt{ff} : \mathsf{bool}$.

Proof

The proof is in 2 parts.

I. We are required to show $\Delta; \Gamma \vdash \texttt{ff} : \mathsf{bool}$, which is immediate.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\texttt{ff}), \gamma'(\texttt{ff})) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\rho$
$\equiv (k, \texttt{ff}, \texttt{ff}) \in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\texttt{ff} \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Since $\texttt{ff}$ is a value, we have $\mathit{irred}(\texttt{ff})$.
Hence, $j = 0$ and $e_f \equiv \texttt{ff}$.
Let $e'_f = \texttt{ff}$.
We are required to show that

- $\texttt{ff} \longmapsto^{*} \texttt{ff}$,
  which is immediate, and
- $(k - 0, \texttt{ff}, \texttt{ff}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$,
  which follows from
  - $\vdash \texttt{ff} : \mathsf{bool}$, and
  - $\texttt{ff} = \texttt{ff} = \texttt{ff}$.

□

Lemma C.17 **($\lambda^{\forall\exists}$ Compatibility-If)**

If $\Delta;\Gamma \vdash e_0 \leq e_0' : \mathsf{bool}$, $\Delta;\Gamma \vdash e_1 \leq e_1' : \tau$, *and* $\Delta;\Gamma \vdash e_2 \leq e_2' : \tau$,
then $\Delta;\Gamma \vdash \mathtt{if}\, e_0, e_1, e_2 \leq \mathtt{if}\, e_0', e_1', e_2' : \tau$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Delta;\Gamma \vdash \mathtt{if}\, e_0, e_1, e_2 : \mathsf{bool}$, which follows from
  - $\Delta;\Gamma \vdash e_0 : \mathsf{bool}$, which follows from $\Delta;\Gamma \vdash e_0 \leq e_0' : \mathsf{bool}$,
  - $\Delta;\Gamma \vdash e_1 : \tau$, which follows from $\Delta;\Gamma \vdash e_1 \leq e_1' : \tau$, and
  - $\Delta;\Gamma \vdash e_2 : \tau$, which follows from $\Delta;\Gamma \vdash e_2 \leq e_2' : \tau$.
- $\Delta;\Gamma \vdash \mathtt{if}\, e_0', e_1', e_2' : \mathsf{bool}$, which follows analogously.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\mathtt{if}\, e_0, e_1, e_2), \gamma'(\mathtt{if}\, e_0', e_1', e_2')) \in \mathcal{RC}[\![\tau]\!]\,\rho$
$\equiv (k, \mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2), \mathtt{if}\, \gamma'(e_0'), \gamma'(e_1'), \gamma'(e_2')) \in \mathcal{RC}[\![\tau]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_0 and e_{f_0} such that

- $\gamma(e_0) \longmapsto^{j_0} e_{f_0}$,
- $\mathit{irred}(e_{f_0})$, and
- $j_0 \leq j$.

Instantiate the second conjunct of $\Delta;\Gamma \vdash e_0 \leq e_0' : \mathsf{bool}$ with k, ρ, γ, and γ'.
Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(e_0), \gamma'(e_0')) \in \mathcal{RC}[\![\mathsf{bool}]\!]\,\rho$.
Instantiate this with j_0, e_{f_0}. Note that

- $j_0 < k$, which follows from $j_0 \leq j$ and $j < k$,
- $\gamma(e_0) \longmapsto^{j_0} e_{f_0}$, and
- $\mathit{irred}(e_{f_0})$.

Hence, there exists e_{f_0}' such that

- $\gamma'(e_0') \longmapsto^{*} e_{f_0}'$, and

- $(k - j_0, e_{f_0}, e'_{f_0}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$.

Hence, either $e_{f_0} \equiv e'_{f_0} \equiv \mathtt{tt}$ or $e_{f_0} \equiv e'_{f_0} \equiv \mathtt{ff}$.

Case $e_{f_0} \equiv e'_{f_0} \equiv \mathtt{tt}$:

Note that

$$\begin{aligned}\gamma(\mathtt{if}\, e_0, e_1, e_2) &\equiv \mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{j_0} \mathtt{if}\, e_{f_0}, \gamma(e_1), \gamma(e_2)\\ &\equiv \mathtt{if}\, \mathtt{tt}, \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{1} \gamma(e_1)\\ &\longmapsto^{j_1} e_{f_1}\end{aligned}$$

where $\mathit{irred}(e_{f_1})$ and $e_{f_1} \equiv e_f$ and $j = j_0 + 1 + j_1$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e_1 \leq e'_1 : \tau$ with $k - j_0 - 1$, ρ, γ, and γ'. Note that

- $k - j_0 - 1 \geq 0$, which follows from $j_0 < k$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k - j_0 - 1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$,
  which follows from Lemma C.10 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ and $k - j_0 - 1 \leq k$.

Hence, $(k - j_0 - 1, \gamma(e_1), \gamma'(e'_1)) \in \mathcal{RC}\,[\![\tau]\!]\,\rho$.

Instantiate this with j_1 and e_{f_1}. Note that

- $j_1 < k - j_0 - 1$, which follows from $j_1 = j - j_0 - 1$ and $j < k$,
- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e'_1) \longmapsto^{*} e'_{f_1}$, and
- $(k - j_0 - 1 - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$
  $\equiv (k - j, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, since $j = j_0 + 1 + j_1$.

Let $e'_f = e'_{f_1}$.

We are required to show

- $\gamma'(\mathtt{if}\, e'_0, e'_1, e'_2) \longmapsto^{*} e'_{f_1}$,
  which follows from

$$\begin{aligned}\gamma'(\mathtt{if}\, e'_0, e'_1, e'_2) &\equiv \mathtt{if}\, \gamma'(e'_0), \gamma'(e'_1), \gamma'(e'_2)\\ &\longmapsto^{*} \mathtt{if}\, e'_{f_0}, \gamma'(e'_1), \gamma'(e'_2)\\ &\equiv \mathtt{if}\, \mathtt{tt}, \gamma'(e'_1), \gamma'(e'_2)\\ &\longmapsto^{1} \gamma'(e'_1)\\ &\longmapsto^{*} e'_{f_1}\end{aligned}$$

  and

- $(k - j, e_f, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$
  $\equiv (k - j, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$,
  which follows from above.

Case $e_{f_0} \equiv e'_{f_0} \equiv \mathtt{ff}$:

Note that

$$\begin{aligned}\gamma(\mathtt{if}\, e_0, e_1, e_2) &\equiv \mathtt{if}\, \gamma(e_0), \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{j_0} \mathtt{if}\, e_{f_0}, \gamma(e_1), \gamma(e_2)\\ &\equiv \mathtt{if}\, \mathtt{ff}, \gamma(e_1), \gamma(e_2)\\ &\longmapsto^{1} \gamma(e_2)\\ &\longmapsto^{j_2} e_{f_2}\end{aligned}$$

where $\mathit{irred}(e_{f_2})$ and $e_{f_2} \equiv e_f$ and $j = j_0 + 1 + j_2$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e_2 \leq e'_2 : \tau$ with $k - j_0 - 1$, ρ, γ, and γ'. Note that

- $k - j_0 - 1 \geq 0$, which follows from $j_0 < k$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and

- $(k - j_0 - 1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$,
  which follows from Lemma C.10 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ and $k - j_0 - 1 \leq k$.

Hence, $(k - j_0 - 1, \gamma(e_2), \gamma'(e_2')) \in \mathcal{RC}\,[\![\tau]\!]\,\rho$.
Instantiate this with j_2 and e_{f_2}. Note that

- $j_2 < k - j_0 - 1$, which follows from $j_2 = j - j_0 - 1$ and $j < k$,
- $\gamma(e_2) \longmapsto^{j_2} e_{f_2}$, and
- $\mathit{irred}(e_{f_2})$.

Hence, there exists e'_{f_2} such that

- $\gamma'(e_2') \longmapsto^* e'_{f_2}$, and
- $(k - j_0 - 1 - j_2, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.
  $\equiv (k - j, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$, since $j = j_0 + 1 + j_2$

Let $e'_f = e'_{f_2}$.
We are required to show

- $\gamma'(\mathtt{if}\, e_0', e_1', e_2') \longmapsto^* e'_{f_2}$,
  which follows from
  $$\begin{aligned}\gamma'(\mathtt{if}\, e_0', e_1', e_2') &\equiv \mathtt{if}\, \gamma'(e_0'), \gamma'(e_1'), \gamma'(e_2') \\ &\longmapsto^* \mathtt{if}\, e'_{f_0}, \gamma'(e_1'), \gamma'(e_2') \\ &\equiv \mathtt{if}\, \mathtt{ff}, \gamma'(e_1'), \gamma'(e_2') \\ &\longmapsto^1 \gamma'(e_2') \\ &\longmapsto^* e'_{f_2}\end{aligned}$$
  and
- $(k - j, e_f, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$
  $\equiv (k - j, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$,
  which follows from above.

□

Lemma C.18 ($\lambda^{\forall\exists}$ Compatibility-Var)

$\Delta; \Gamma \vdash x \leq x : \Gamma(x)$.

Proof

The proof is in 2 parts.

I. We are required to show $\Delta; \Gamma \vdash x : \Gamma(x)$, which is immediate.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(x), \gamma'(x)) \in \mathcal{RC}[\![\Gamma(x)]\!]\,\rho$.
Consider arbitrary j, e_f such that

- $j < k$,
- $\gamma(x) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Since $\gamma(x)$ is a value, we have $\mathit{irred}(\gamma(x))$.
Hence, $j = 0$ and $e_f \equiv \gamma(x)$.
Let $e'_f = \gamma'(x)$.
We are required to show that

- $\gamma'(x) \longmapsto^{*} \gamma'(x)$,
  which is immediate, and
- $(k - 0, \gamma(x), \gamma'(x)) \in \mathcal{RV}[\![\Gamma(x)]\!]\,\rho$,
  which follows from $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$.

□

Lemma C.19 **($\lambda^{\forall\exists}$ Compatibility-Fn)**

If $\Delta; \Gamma, x : \tau \vdash e \leq e' : \tau_2$,
then $\Delta; \Gamma \vdash \lambda x.\, e \leq \lambda x.\, e' : \tau_1 \to \tau_2$.

Proof

The proof is in 2 parts.

I. We are required to show $\Delta; \Gamma \vdash \lambda x.\, e : \tau_1 \to \tau_2$ and $\Delta; \Gamma \vdash \lambda x.\, e' : \tau_1 \to \tau_2$,
which follow (respectively) from $\Delta; \Gamma, x : \tau_1 \vdash e : \tau_2$ and $\Delta; \Gamma, x : \tau_1 \vdash e' : \tau_2$,
which follow from $\Delta; \Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\lambda x.\, e), \gamma'(\lambda x.\, e')) \in \mathcal{RC}\,[\![\tau_1 \to \tau_2]\!]\,\rho$
$\equiv (k, \lambda x.\, \gamma(e), \lambda x.\, \gamma'(e')) \in \mathcal{RC}\,[\![\tau_1 \to \tau_2]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\lambda x.\, \gamma(e) \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Since $\lambda x.\, \gamma(e)$ is a value, we have $\mathit{irred}(\lambda x.\, \gamma(e))$.
Hence, $j = 0$ and $e_f \equiv \lambda x.\, \gamma(e)$.
Let $e'_f = \lambda x.\, \gamma'(e')$.
We are required to show that

- $\lambda x.\, \gamma'(e') \longmapsto^* \lambda x.\, \gamma'(e')$,
  which is immediate, and
- $(k - 0, \lambda x.\, \gamma(e), \lambda x.\, \gamma'(e')) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$
  $\equiv (k, \lambda x.\, \gamma(e), \lambda x.\, \gamma'(e'))$
  $\in \{(k, \lambda x.\, e, \lambda x.\, e') \mid \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]} \ \wedge$
  $\forall j < k, v_1, v'_1.$
  $(j, v_1, v'_1) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho \implies$
  $(j, e[v_1/x], e'[v'_1/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho\}$,
  which follows from
  - $\vdash \lambda x.\, \gamma'(e') : (\tau_1 \to \tau_2)^{[\rho]}$,
    which follows from
    - Note that $\Delta; \Gamma, x : \tau_1 \vdash e' : \tau_2$, which follows from $\Delta; \Gamma, x : \tau_1 \vdash e \leq e' : \tau$.
      Hence, we have $\Delta; \Gamma \vdash \lambda x.\, e' : \tau_1 \to \tau_2$.
      Note that $\bullet; \Gamma^{[\rho]} \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]}$, which follows from Lemma C.6 applied to $\bullet \vdash \rho^{\mathsf{syn}}$ and $\Delta; \Gamma \vdash \lambda x.\, e' : \tau_1 \to \tau_2$.
      Note that $\bullet; \bullet \vdash \gamma' : \Gamma^{[\rho]}$, which follows from Lemma C.8 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.
      Note that $\bullet; \bullet \vdash \gamma'(\lambda x.\, e') : (\tau_1 \to \tau_2)^{[\rho]}$, which follows from Lemma C.5 applied to $\bullet; \bullet \vdash \gamma' : \Gamma^{[\rho]}$ and $\bullet; \Gamma^{[\rho]} \vdash \lambda x.\, e' : (\tau_1 \to \tau_2)^{[\rho]}$.
      Hence, $\bullet; \bullet \vdash \lambda x.\, \gamma'(e') : (\tau_1 \to \tau_2)^{[\rho]}$.

- $\forall j < k, v_1, v_1 \ldots$.
  Consider arbitrary j, v_1, v_1' such that
  - $j < k$, and
  - $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

  We are required to show that $(j, \gamma(e)[v_1/x], \gamma'(e')[v_1'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.
  Instantiate the second conjunct of $\Delta; \Gamma, x : \tau \vdash e \leq e' : \tau_2$ with j, ρ, $\gamma[x \mapsto v_1]$, and $\gamma'[x \mapsto v_1']$. Note that
  - $j \geq 0$,
  - $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
  - $(j, \gamma[x \mapsto v_1], \gamma'[x \mapsto v_1']) \in \mathcal{RG}\,[\![\Gamma, x : \tau_1]\!]\,\rho$, which follows from
    - $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$,
      which follows from Lemma C.10 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ and $j \leq k$, and
    - $(j, v_1, v_1') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$,
      which follows from above.

  Hence, $(j, \gamma[x \mapsto v_1](e), \gamma'[x \mapsto v_1'](e')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.
  Thus, $(j, \gamma(e)[x/v_1], \gamma'(e')[x/v_1']) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.

□

Lemma C.20 **($\lambda^{\forall\exists}$ Compatibility-App)**

If $\Delta;\Gamma \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$, *and* $\Delta;\Gamma \vdash e_2 \leq e_2' : \tau_1$,
then $\Delta;\Gamma \vdash e_1\, e_2 \leq e_1'\, e_2' : \tau_2$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Delta;\Gamma \vdash e_1\, e_2 : \tau_2$, which follows from
  - $\Delta;\Gamma \vdash e_1 : \tau_1 \to \tau_2$,
    which follows from $\Delta;\Gamma \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$, and
  - $\Delta;\Gamma \vdash e_2 : \tau_1$,
    which follows from $\Delta;\Gamma \vdash e_2 \leq e_2' : \tau_1$.
- $\Delta;\Gamma \vdash e_1'\, e_2' : \tau_2$, which follows analogously.

II. Consider arbitrary k, ρ, γ, and γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(e_1\, e_2), \gamma'(e_1'\, e_2')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$
$\equiv (k, \gamma(e_1)\,\gamma(e_2), \gamma'(e_1')\,\gamma'(e_2')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\gamma(e_1)\,\gamma(e_2) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Delta;\Gamma \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$ with k, ρ, γ, and γ'. Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(e_1), \gamma'(e_1')) \in \mathcal{RC}\,[\![\tau_1 \to \tau_2]\!]\,\rho$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j$ and $j < k$,
- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e_{f_1}' such that

- $\gamma'(e_1') \longmapsto^{*} e_{f_1}'$, and
- $(k - j_1, e_{f_1}, e_{f_1}') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$.

Hence, $e_{f_1} \equiv \lambda x.\, e_{f_{11}}$ and $e'_{f_1} \equiv \lambda x.\, e'_{f_{11}}$.
Note that

$$\begin{aligned}\gamma(e_1\, e_2) &\equiv \gamma(e_1)\, \gamma(e_2)\\ &\longmapsto^{j_1} e_{f_1}\, \gamma(e_2)\\ &\equiv (\lambda x.\, e_{f_{11}})\, \gamma(e_2)\\ &\longmapsto^{j-j_1} e_f\end{aligned}$$

Hence, by inspection of the operational semantics it follows that there exist j_2 and e_{f_2} such that

- $\gamma(e_2) \longmapsto^{j_2} e_{f_2}$,
- $\mathit{irred}(e_{f_2})$, and
- $j_2 \leq j - j_1$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e_2 \leq e'_2 : \tau_1$ with $k - j_1$, ρ, γ, and γ'. Note that

- $k - j_1 \geq 0$, which follows from $j_1 < k$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k - j_1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$,
  which follows from Lemma C.10 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ and $k - j_1 \leq k$.

Hence, $(k - j_1, \gamma(e_2), \gamma'(e'_2)) \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho$.
Instantiate this with j_2 and e_{f_2}. Note that

- $j_2 < k - j_1$, which follows from $j_2 \leq j - j_1$ and $j < k$,
- $\gamma(e_2) \longmapsto^{j_2} e_{f_2}$, and
- $\mathit{irred}(e_{f_2})$.

Hence, there exists e'_{f_2} such that

- $\gamma'(e'_2) \longmapsto^{*} e'_{f_2}$, and
- $(k - j_1 - j_2, e_{f_2}, e'_{f_2}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

Hence, $e_{f_2} \equiv v_{f_2}$ and $e'_{f_2} \equiv v'_{f_2}$.
Note that

$$\begin{aligned}\gamma(e_1\, e_2) &\equiv \gamma(e_1)\, \gamma(e_2)\\ &\longmapsto^{j_1} e_{f_1}\, \gamma(e_2)\\ &\equiv (\lambda x.\, e_{f_{11}})\, \gamma(e_2)\\ &\longmapsto^{j_2} (\lambda x.\, e_{f_{11}})\, e_{f_2}\\ &\equiv (\lambda x.\, e_{f_{11}})\, v_{f_2}\\ &\longmapsto^{1} e_{f_{11}}[v_{f_2}/x]\\ &\longmapsto^{j_3} e_f\end{aligned}$$

and $\mathit{irred}(e_f)$, where $j = j_1 + j_2 + 1 + j_3$.
Instantiate the second conjunct of $(k - j_1, \lambda x.\, e_{f_{11}}, \lambda x.\, e'_{f_{11}}) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$ with $k - j_1 - j_2 - 1$, v_{f_2}, and v'_{f_2}. Note that

- $k - j_1 - j_2 - 1 < k - j_1$, and
- $(k - j_1 - j_2 - 1, v_{f_2}, v'_{f_2}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$,
  which follows from Lemma C.9 applied to
  - $\rho \in \mathcal{RD}\,[\![\Delta]\!]$,
  - $\Delta \vdash \tau_1$,
  - $(k - j_1 - j_2, v_{f_2}, v'_{f_2}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$, and
  - $k - j_1 - j_2 - 1 \leq k - j_1 - j_2$.

Hence, $(k - j_1 - j_2 - 1, e_{f_{11}}[v_{f_2}/x], e'_{f_{11}}[v'_{f_2}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.
Instantiate this with j_3 and e_f. Note that

- $j_3 < k - j_1 - j_2 - 1$, which follows from $j_3 = j - j_1 - j_2 - 1$ and $j < k$,
- $e_{f_{11}}[v_{f_2}/x] \longmapsto^{j_3} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, there exists e'_f such that

- $e'_{f_{11}}[v'_{f_2}/x] \longmapsto^* e'_f$, and
- $(k - j_1 - j_2 - 1 - j_3, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$
  $\equiv (k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$, since $j = j_1 + j_2 + 1 + j_3$.

Pick $e'_f = e'_f$.
We are required to show that

- $\gamma'(e'_1\, e'_2) \longmapsto^* e'_f$,
  which follows from

$$\begin{array}{rl}
\gamma'(e'_1\, e'_2) & \equiv \gamma'(e'_1)\,\gamma'(e'_2) \\
& \longmapsto^* e'_{f_1}\,\gamma'(e'_2) \\
& \equiv (\lambda x.\, e'_{f_{11}})\,\gamma'(e'_2) \\
& \longmapsto^* (\lambda x.\, e'_{f_{11}})\, e'_{f_2} \\
& \equiv (\lambda x.\, e'_{f_{11}})\, v'_{f_2} \\
& \longmapsto^1 e'_{f_{11}}[v'_{f_2}/x] \\
& \longmapsto^* e'_f
\end{array}$$

  and

- $(k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$,
  which follows from above.

□

Lemma C.21 **($\lambda^{\forall\exists}$ Compatibility-Fold)**

If $\Delta; \Gamma \vdash e \leq e' : \tau[\mu\alpha.\,\tau/\alpha]$,
then $\Delta; \Gamma \vdash \mathtt{fold}\, e \leq \mathtt{fold}\, e' : \mu\alpha.\,\tau$.

Proof

The proof is in 2 parts.

I. We are required to show $\Delta; \Gamma \vdash \mathtt{fold}\, e : \mu\alpha.\,\tau$ and $\Delta; \Gamma \vdash \mathtt{fold}\, e' : \mu\alpha.\,\tau$,
which follow (respectively) from $\Delta; \Gamma \vdash e : \tau[\mu\alpha.\,\tau/\alpha]$ and $\Delta; \Gamma \vdash e' : \tau[\mu\alpha.\,\tau/\alpha]$,
which follow from $\Delta; \Gamma \vdash e \leq e' : \tau[\mu\alpha.\,\tau/\alpha]$.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\mathtt{fold}\, e), \gamma'(\mathtt{fold}\, e')) \in \mathcal{RC}\,[\![\mu\alpha.\,\tau]\!]\,\rho$
$\equiv (k, \mathtt{fold}\,\gamma(e), \mathtt{fold}\,\gamma'(e')) \in \mathcal{RC}\,[\![\mu\alpha.\,\tau]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{fold}\,\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e \leq e' : \tau[\mu\alpha.\,\tau/\alpha]$ with k, ρ, γ, and γ'.
Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j < k$,
- $\gamma(e) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e') \longmapsto^{*} e'_{f_1}$, and
- $(k - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho$.

Hence, $e_{f_1} \equiv v_{f_1}$ and $e'_{f_1} \equiv v'_{f_1}$.
Note that

$$\begin{aligned}\gamma(\texttt{fold}\, e) &\equiv \texttt{fold}\, \gamma(e) \\ &\longmapsto^{j_1} \texttt{fold}\, e_{f_1} \\ &\equiv \texttt{fold}\, v_{f_1} \\ &\longmapsto^{j-j_1} e_f\end{aligned}$$

Since $\texttt{fold}\, v_{f_1}$ is a value, we have $\mathit{irred}(\texttt{fold}\, v_{f_1})$.
Hence, $j - j_1 = 0$ (and $j = j_1$) and $e_f \equiv \texttt{fold}\, v_{f_1}$.
Let $e'_f = \texttt{fold}\, v'_{f_1}$. We are required to show that

- $\texttt{fold}\, \gamma'(e') \longmapsto^* e'_f$
  $\equiv \texttt{fold}\, \gamma'(e') \longmapsto^* \texttt{fold}\, v'_{f_1}$
  which follows from above, and
- $(k-j, e_f, e'_f) \in \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho$
  $\equiv (k-j, \texttt{fold}\, v_{f_1}, \texttt{fold}\, v'_{f_1})$
  $\in \{(k, \texttt{fold}\, v, \texttt{fold}\, v') \mid$
  $\vdash \texttt{fold}\, v' : (\mu\alpha.\, \tau)^{[\rho]} \wedge$
  $\forall j < k.$
  let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{j+1}$ in
  $(j, v, v') \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]\}$
  which follows from
  - $\vdash \texttt{fold}\, v'_{f_1} : (\mu\alpha.\, \tau)^{[\rho]}$
    Note that $\vdash v'_{f_1} : (\tau[\mu\alpha.\, \tau/\alpha])^{[\rho]}$, which follows from $(k-j, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho$.
    Note that $\vdash v'_{f_1} : (\tau[\mu\alpha.\, \tau/\alpha])^{[\rho]}$
    $\equiv \bullet; \bullet \vdash v'_{f_1} : (\tau[\mu\alpha.\, \tau/\alpha])^{[\rho]}$
    $\equiv \bullet; \bullet \vdash v'_{f_1} : (\tau^{[\rho]}[(\mu\alpha.\, \tau)^{[\rho]}/\alpha])$.
    Hence, $\bullet; \bullet \vdash \texttt{fold}\, v'_{f_1} : (\mu\alpha.\, \tau)^{[\rho]}$.
  - $\forall i < k - j.$ let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{i+1}$ in $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})])$.
    Consider arbitrary i such that
    - $i < k - j$.

    Let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{i+1}$.
    We are required to show that $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]$
    $\equiv (i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]$.
    Applying Lemma C.9 to
    - $\rho \in \mathcal{RD}\, [\![\Delta]\!]$,
    - $\Delta \vdash \tau[\mu\alpha.\, \tau/\alpha]$,
    - $(k-j, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho$, and
    - $i \leq k - j$,

    we conclude that $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho$.
    Hence, $(i, v_{f_1}, v'_{f_1}) \in \lfloor \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho \rfloor_{i+1}$, which follows from the definition of $\lfloor \cdot \rfloor_k$.
    Applying Lemma C.14 to $\rho \in \mathcal{RD}\, [\![\Delta]\!]$, $\Delta \vdash \mu\alpha.\, \tau$, and $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{i+1}$ we conclude that
    $\lfloor \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})] \rfloor_{i+1} = \lfloor \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho \rfloor_{i+1}$.
    Hence, $(i, v_{f_1}, v'_{f_1}) \in \lfloor \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})] \rfloor_{i+1}$.
    Hence, $(i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]$, which follows from the definition of $\lfloor \cdot \rfloor_k$.

□

Lemma C.22 **($\lambda^{\forall\exists}$ Compatibility-Unfold)**

If $\Delta; \Gamma \vdash e \leq e' : \mu\alpha.\,\tau$,
then $\Delta; \Gamma \vdash \mathtt{unfold}\, e \leq \mathtt{unfold}\, e' : \tau[\mu\alpha.\,\tau/\alpha]$.

Proof

The proof is in 2 parts.

I. We are required to show $\Delta; \Gamma \vdash \mathtt{unfold}\, e : \tau[\mu\alpha.\,\tau/\alpha]$ and $\Delta; \Gamma \vdash \mathtt{unfold}\, e' : \tau[\mu\alpha.\,\tau/\alpha]$,
which follow (respectively) from $\Delta; \Gamma \vdash e : \mu\alpha.\,\tau$ and $\Delta; \Gamma \vdash e' : \mu\alpha.\,\tau$,
which follows from $\Delta; \Gamma \vdash e \leq e' : \mu\alpha.\,\tau$.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\mathtt{unfold}\, e), \gamma'(\mathtt{unfold}\, e')) \in \mathcal{RC}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho$
$\equiv (k, \mathtt{unfold}\,\gamma(e), \mathtt{unfold}\,\gamma'(e')) \in \mathcal{RC}\,[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{unfold}\,\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e \leq e' : \mu\alpha.\,\tau$ with k, ρ, γ, and γ'. Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]$.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\mu\alpha.\,\tau]\!]\,\rho$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j < k$,
- $\gamma(e) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e') \longmapsto^{*} e'_{f_1}$, and
- $(k - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\mu\alpha.\,\tau]\!]\,\rho$.

Hence, $e_{f_1} \equiv \texttt{fold}\, v_{f_{11}}$ and $e'_{f_1} \equiv \texttt{fold}\, v'_{f_{11}}$.
Note that

$$\begin{aligned}\gamma(\texttt{unfold}\, e) &\equiv \texttt{unfold}\, \gamma(e)\\ &\longmapsto^{j_1} \texttt{unfold}\, e_{f_1}\\ &\equiv \texttt{unfold}\, (\texttt{fold}\, v_{f_{11}})\\ &\longmapsto^{1} v_{f_{11}} \longmapsto^{j-j_1-1} e_f\end{aligned}$$

Since $v_{f_{11}}$ is a value, we have $\mathit{irred}(v_{f_{11}})$.
Hence, $j - j_1 - 1 = 0$ (and $j = j_1 + 1$) and $e_f \equiv v_{f_{11}}$.
Furthermore, note that

$$\begin{aligned}\gamma'(\texttt{unfold}\, e') &\equiv \texttt{unfold}\, \gamma'(e')\\ &\longmapsto^{*} \texttt{unfold}\, e'_{f_1}\\ &\equiv \texttt{unfold}\, (\texttt{fold}\, v'_{f_{11}})\\ &\longmapsto^{1} v'_{f_{11}}\end{aligned}$$

Since $v'_{f_{11}}$ is a value, we have $\mathit{irred}(v'_{f_{11}})$.
Let $e'_f = v'_{f_{11}}$.
We are required to show that

- $\texttt{unfold}\, \gamma'(e') \longmapsto^{*} e'_f$
  $\equiv \texttt{unfold}\, \gamma'(e') \longmapsto^{*} v'_{f_{11}}$
  which follows from above, and
- $(k - j, e_f, e'_f) \in \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho$
  $\equiv (k - j, v_{f_{11}}, v'_{f_{11}}) \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho$,
  which we conclude as follows:
  From $(k - j_1, e_{f_1}, e'_{f_1}) \equiv (k - j_1, \texttt{fold}\, v_{f_{11}}, \texttt{fold}\, v'_{f_{11}}) \in \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho$, we have
  - $\vdash \texttt{fold}\, v'_{f_{11}} : (\mu\alpha.\, \tau)^{[\rho]}$, and
  - $\forall i < k - j_1.$ let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{i+1}$ in $(i, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau]\!]\, \emptyset[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]$.

  Instantiate $\forall i < k - j_1.$ let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{i+1}$ in $(i, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]$
  with $k - j$. Note that
  - $k - j < k - j_1$, which follows from $j = j_1 + 1$.

  Let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{k-j+1}$.
  Hence, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})]$.
  Hence, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \lfloor \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})] \rfloor_{k-j+1}$, which follows from the definition of $\lfloor \cdot \rfloor_k$.
  Applying Lemma C.14 to $\rho \in \mathcal{RD}\, [\![\Delta]\!]$, $\Delta \vdash \mu\alpha.\, \tau$, and $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau]\!]\, \rho \rfloor_{k-j+1}$, we conclude that
  $\lfloor \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau)^{[\rho]})] \rfloor_{k-j+1} = \lfloor \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho \rfloor_{k-j+1}$.
  Hence, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \lfloor \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho \rfloor_{k-j+1}$.
  Thus, $(k - j, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\, [\![\tau[\mu\alpha.\, \tau/\alpha]]\!]\, \rho$, which follows from the definition of $\lfloor \cdot \rfloor_k$.

□

Lemma C.23 **($\lambda^{\forall\exists}$ Compatibility-All)**

If $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau$,
then $\Delta; \Gamma \vdash \Lambda.\, e \leq \Lambda.\, e' : \forall\alpha.\, \tau$.

Proof

The proof is in 2 parts.

I. We are required to show $\Delta; \Gamma \vdash \Lambda.\, e : \forall\alpha.\, \tau$ and $\Delta; \Gamma \vdash \Lambda.\, e' : \forall\alpha.\, \tau$,
which follow (respectively) from $\Delta, \alpha; \Gamma \vdash e : \tau$ and $\Delta, \alpha; \Gamma \vdash e' : \tau$,
which follow from $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau$.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\Lambda.\, e), \gamma'(\Lambda.\, e')) \in \mathcal{RC}\,[\![\forall\alpha.\, \tau]\!]\,\rho$
$\equiv (k, \Lambda.\, \gamma(e), \Lambda.\, \gamma'(e')) \in \mathcal{RC}\,[\![\forall\alpha.\, \tau]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\Lambda.\, \gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Since $\Lambda.\, \gamma(e)$ is a value, we have $\mathit{irred}(\Lambda.\, \gamma(e))$.
Hence, $j = 0$ and $e_f \equiv \Lambda.\, \gamma(e)$.
Let $e'_f = \Lambda.\, \gamma'(e')$.
We are required to show that

- $\Lambda.\, \gamma'(e') \longmapsto^{*} \Lambda.\, \gamma'(e')$,
  which is immediate, and
- $(k - 0, \Lambda.\, \gamma(e), \Lambda.\, \gamma'(e')) \in \mathcal{RV}\,[\![\forall\alpha.\, \tau]\!]\,\rho$
  $\equiv (k, \Lambda.\, \gamma(e), \Lambda.\, \gamma'(e'))$
  $\in \{(k, \Lambda.\, e, \Lambda.\, e') \mid \vdash \Lambda.\, e' : (\forall\alpha.\, \tau)^{[\rho]} \ \wedge$
  $\forall\tau_2, \chi.$
  $\chi \in \mathit{Rel}_{\tau_2} \implies$
  $\forall j < k.\ (j, e, e') \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]\}$,
  which follows from
  - $\vdash \Lambda.\, \gamma'(e') : (\forall\alpha.\, \tau)^{[\rho]}$,
    which follows from
    - Note that $\Delta, \alpha; \Gamma \vdash e' : \tau$, which follows from $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau$.
      Hence, we have $\Delta; \Gamma \vdash \Lambda.\, e' : \forall\alpha.\, \tau$.
      Note that $\bullet; \Gamma^{[\rho]} \vdash \Lambda.\, e' : (\forall\alpha.\, \tau)^{[\rho]}$, which follows from Lemma C.6 applied to $\bullet \vdash \rho^{\mathsf{syn}}$ and $\Delta; \Gamma \vdash \Lambda.\, e' : \forall\alpha.\, \tau$.
      Note that $\vdash \gamma' : \Gamma^{[\rho]}$, which follows from Lemma C.8 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.
      Note that $\bullet; \bullet \vdash \gamma'(\Lambda.\, e') : (\forall\alpha.\, \tau)^{[\rho]}$, which follows from Lemma C.5 applied to $\vdash \gamma' : \Gamma^{[\rho]}$ and $\bullet; \Gamma^{[\rho]} \vdash \Lambda.\, e' : (\forall\alpha.\, \tau)^{[\rho]}$.
      Hence, $\bullet; \bullet \vdash \Lambda.\, \gamma'(e') : (\forall\alpha.\, \tau)^{[\rho]}$.

- $\forall \tau_2, \chi. \ldots$
  Consider arbitrary τ_2, and χ such that
  - $\chi \in \mathit{Rel}_{\tau_2}$.

  We are required to show that $\forall j < k.\ (j, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.
  Consider arbitrary j such that
  - $j < k$.

  We are required to show that $(j, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.
  Instantiate the second conjunct of the premise $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau$ with j, $\rho[\alpha \mapsto (\chi, \tau_2)]$, γ, and γ'. Note that
  - $j \geq 0$,
  - $\rho[\alpha \mapsto (\chi, \tau_2)] \in \mathcal{RD}\,[\![\Delta, \alpha]\!]$,
    which follows from $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\chi \in \mathit{Rel}_{\tau_2}$, and
  - $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$, which follows from
    - $(j, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$,
      which follows from Lemma C.10 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ and $j \leq k$, and
    - $\alpha \notin \mathit{FTV}(\Gamma)$.

  Hence, $(j, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

□

Lemma C.24 **($\lambda^{\forall\exists}$ Compatibility-Inst)**

If $\Delta; \Gamma \vdash e \leq e' : \forall\alpha.\, \tau$ *and* $\Delta \vdash \tau_1$,
then $\Delta; \Gamma \vdash e\,[\,] \leq e'\,[\,] : \tau[\tau_1/\alpha]$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Delta; \Gamma \vdash e\,[\,] : \tau[\tau_1/\alpha]$, which follows from
  - $\Delta; \Gamma \vdash e : \forall\alpha.\, \tau$,
    which follows from $\Delta; \Gamma \vdash e \leq e' : \forall\alpha.\, \tau$, and
  - $\Delta \vdash \tau_1$.
- $\Delta; \Gamma \vdash e'\,[\,] : \tau[\tau_1/\alpha]$, which follows analogously.

II. Consider arbitrary k, ρ, γ, and γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(e\,[\,]), \gamma'(e'\,[\,])) \in \mathcal{RC}\,[\![\tau[\tau_1/\alpha]]\!]\,\rho$
$\equiv (k, \gamma(e)\,[\,], \gamma'(e')\,[\,]) \in \mathcal{RC}\,[\![\tau[\tau_1/\alpha]]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\gamma(e)\,[\,] \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e \leq e' : \forall\alpha.\, \tau$ with k, ρ, γ, and γ'. Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\forall\alpha.\, \tau]\!]\,\rho$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j$ and $j < k$,
- $\gamma(e) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e') \longmapsto^* e'_{f_1}$, and
- $(k - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\forall\alpha.\, \tau]\!]\,\rho$.

Hence, $e_{f_1} \equiv \Lambda.\, e_{f_{11}}$ and $e'_{f_1} \equiv \Lambda.\, e'_{f_{11}}$.
Note that

$$\begin{aligned}\gamma(e\,[\,]) &\equiv \gamma(e)\,[\,]\\ &\longmapsto^{j_1} e_{f_1}\,[\,]\\ &\equiv (\Lambda.\, e_{f_{11}})\,[\,] \longmapsto^{1} e_{f_{11}}\\ &\longmapsto^{j_2} e_f\end{aligned}$$

and $\mathit{irred}(e_f)$, where $j = j_1 + 1 + j_2$.
Let $\chi = \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.
Instantiate the second conjunct of $(k - j_1, \Lambda.\, e_{f_{11}}, \Lambda.\, e'_{f_{11}}) \in \mathcal{RV}\,[\![\forall\alpha.\,\tau]\!]\,\rho$ with $(\tau_1)^{[\rho]}$, and χ. Note that

- $\chi \in \mathit{Rel}_{(\tau_1)^{[\rho]}}$,
  which follows from $\mathcal{RV}\,[\![\tau_1]\!]\,\rho \in \mathit{Rel}_{(\tau_1)^{[\rho]}}$,
  which in turn follows from Lemma C.11 applied to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\Delta \vdash \tau_1$.

Hence, $\forall i < k - j_1.\ (i, e_{f_{11}}, e'_{f_{11}}) \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$.
Instantiate this with $k - j_1 - 1$, noting that $k - j_1 - 1 < k - j_1$.
Hence, $(k - j_1 - 1, e_{f_{11}}, e'_{f_{11}}) \in \mathcal{RC}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$.
Instantiate this with j_2 and e_f. Note that

- $j_2 < k - j_1 - 1$, which follows from $j_2 = j - j_1 - 1$ and $j < k$,
- $e_{f_{11}} \longmapsto^{j_2} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, there exists e'_f such that

- $e'_{f_{11}} \longmapsto^{*} e'_f$, and
- $(k - j_1 - 1 - j_2, e_f, e'_f) \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$
  $\equiv (k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$, since $j = j_1 + 1 + j_2$.

Pick $e'_f = e'_f$.
We are required to show that

- $\gamma'(e'\,[\,]) \longmapsto^{*} e'_f$,
  which follows from

  $$\begin{aligned}\gamma'(e'\,[\,]) &\equiv \gamma'(e')\,[\,]\\ &\longmapsto^{*} e'_{f_1}\,[\,]\\ &\equiv (\Lambda.\, e'_{f_{11}})\,[\,]\\ &\longmapsto^{1} e'_{f_{11}}\\ &\longmapsto^{*} e'_f\end{aligned}$$

  and
- $(k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau[\tau_1/\alpha]]\!]\,\rho$,
  which follows from Lemma C.12 applied to
  - $\rho \in \mathcal{RD}\,[\![\Delta]\!]$,
  - $\Delta \vdash \tau_1$,
  - $\chi = \mathcal{RV}\,[\![\tau_1]\!]\,\rho$, and
  - $(k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$.

□

Lemma C.25 **($\lambda^{\forall\exists}$ Compatibility-Pack)**

If $\Delta \vdash \tau_1$ *and* $\Delta; \Gamma \vdash e \leq e' : \tau[\tau_1/\alpha]$,
then $\Delta; \Gamma \vdash \mathtt{pack}\, e \leq \mathtt{pack}\, e' : \exists\alpha.\, \tau$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Delta; \Gamma \vdash \mathtt{pack}\, e : \exists\alpha.\, \tau$, which follows from
  - $\Delta \vdash \tau_1$, and
  - $\Delta; \Gamma \vdash e : \tau[\tau_1/\alpha]$,
    which follows from $\Delta; \Gamma \vdash e \leq e' : \tau[\tau_1/\alpha]$.
- $\Delta; \Gamma \vdash \mathtt{pack}\, e' : \exists\alpha.\, \tau$, which follows analogously.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(\mathtt{pack}\, e), \gamma'(\mathtt{pack}\, e')) \in \mathcal{RC}\,[\![\exists\alpha.\, \tau]\!]\,\rho$
$\equiv (k, \mathtt{pack}\, \gamma(e), \mathtt{pack}\, \gamma'(e')) \in \mathcal{RC}\,[\![\exists\alpha.\, \tau]\!]\,\rho$.

Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{pack}\, \gamma(e) \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e \leq e' : \tau[\tau_1/\alpha]$ with k, ρ, γ, and γ'.
Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau[\tau_1/\alpha]]\!]\,\rho$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j < k$,
- $\gamma(e) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e') \longmapsto^* e'_{f_1}$, and
- $(k - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau[\tau_1/\alpha]]\!]\,\rho$.

Hence, $e_{f_1} \equiv v_{f_1}$ and $e'_{f_1} \equiv v'_{f_1}$.
Note that

$$\begin{aligned}\gamma(\mathtt{pack}\, e) &\equiv \mathtt{pack}\, \gamma(e) \\ &\longmapsto^{j_1} \mathtt{pack}\, e_{f_1} \\ &\equiv \mathtt{pack}\, v_{f_1} \\ &\longmapsto^{j-j_1} e_f\end{aligned}$$

Since $\mathtt{pack}\, v_{f_1}$ is a value, we have $\mathit{irred}(\mathtt{pack}\, v_{f_1})$.
Hence, $j - j_1 = 0$ (and $j = j_1$) and $e_f \equiv \mathtt{pack}\, v_{f_1}$.
Let $e'_f = \mathtt{pack}\, v'_{f_1}$. We are required to show that

- $\mathtt{pack}\, \gamma'(e') \longmapsto^* e'_f$
  $\equiv \mathtt{pack}\, \gamma'(e') \longmapsto^* \mathtt{pack}\, v'_{f_1}$
  which follows from above, and
- $(k-j, e_f, e'_f) \in \mathcal{RV}\, [\![\exists \alpha.\, \tau]\!]\, \rho$
  $\equiv (k-j, \mathtt{pack}\, v_{f_1}, \mathtt{pack}\, v'_{f_1})$
  $\in \{(k, \mathtt{pack}\, v, \mathtt{pack}\, v') \mid$
  $\vdash \mathtt{pack}\, v' : (\exists \alpha.\, \tau)^{[\rho]} \ \wedge$
  $\exists \tau_2, \chi.$
  $\chi \in \mathit{Rel}_{\tau_2} \ \wedge$
  $\forall j < k.\ (j, v, v') \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, \tau_2)]\}$
  which follows from
  - $\vdash \mathtt{pack}\, v'_{f_1} : (\exists \alpha.\, \tau)^{[\rho]}$
    Note that $\vdash v'_{f_1} : (\tau[\tau_1/\alpha])^{[\rho]}$, which follows from $(k-j, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau[\tau_1/\alpha]]\!]\, \rho$.
    Note that $\bullet \vdash (\tau_1)^{[\rho]}$, which follows from $\Delta \vdash \tau_1$ and $\rho \in \mathcal{RD}\, [\![\Delta]\!]$.
    Note that $\vdash v'_{f_1} : (\tau[\tau_1/\alpha])^{[\rho]}$
    $\equiv \bullet; \bullet \vdash v'_{f_1} : (\tau[\tau_1/\alpha])^{[\rho]}$
    $\equiv \bullet; \bullet \vdash v'_{f_1} : (\tau^{[\rho]}[(\tau_1)^{[\rho]}/\alpha])$.
    Hence, $\bullet; \bullet \vdash \mathtt{fold}\, v'_{f_1} : (\mu \alpha.\, \tau)^{[\rho]}$, which follows from $\bullet \vdash (\tau_1)^{[\rho]}$ and $\bullet; \bullet \vdash v'_{f_1} : \tau^{[\rho]}[(\tau_1)^{[\rho]}/\alpha]$.
  - $\exists \tau_2, \chi.\ \chi \in \mathit{Rel}_{\tau_2} \ \wedge \ \forall i < k-j.\ (i, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, \tau_2)]$.
    Pick $\tau_2 = (\tau_1)^{[\rho]}$ and $\chi = \mathcal{RV}\, [\![\tau_1]\!]^{[\rho]}$.
    Note that
    - $\chi \in \mathit{Rel}_{(\tau_1)^{[\rho]}}$,
      which follows from Lemma C.11 applied to $\rho \in \mathcal{RD}\, [\![\Delta]\!]$ and $\Delta \vdash \tau_1$.

    Consider arbitrary i such that
    - $i < k - j$.

    We are required to show that $(i, v_{f_1}, v_{f'_1}) \in \mathcal{RV}\, [\![\tau]\!]\, \rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$,
    which follows from Lemma C.12 applied to
    - $\rho \in \mathcal{RD}\, [\![\Delta]\!]$,
    - $\Delta \vdash \tau_1$,
    - $\chi = \mathcal{RV}\, [\![\tau_1]\!]\, \rho$, and
    - $(k-j, v_{f_1}, v'_{f_1}) \in \mathcal{RV}\, [\![\tau[\tau_1/\alpha]]\!]\, \rho$.

□

Lemma C.26 **($\lambda^{\forall\exists}$ Compatibility-Unpack)**

If $\Delta; \Gamma \vdash e_1 \leq e_1' : \exists\alpha.\, \tau_1$, *and* $\Delta \vdash \tau_2$,
and $\Delta, \alpha; \Gamma, x : \tau_1 \vdash e_2 \leq e_2' : \tau_2$,
then $\Delta; \Gamma \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, e_2 \leq \mathtt{unpack}\, e_1'\, \mathtt{as}\, x\, \mathtt{in}\, e_2' : \tau_2$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Delta; \Gamma \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, e_2 : \tau_2$, which follows from
  - $\Delta; \Gamma \vdash e_1 : \exists\alpha.\, \tau_1$,
    which follows from $\Delta; \Gamma \vdash e_1 \leq e_1' : \exists\alpha.\, \tau_1$,
  - $\Delta \vdash \tau_2$, and
  - $\Delta, \alpha; \Gamma, x : \tau_1 \vdash e_2 : \tau_2$,
    which follows from $\Delta, \alpha; \Gamma, x : \tau_1 \vdash e_2 \leq e_2' : \tau_2$.
- $\Delta; \Gamma \vdash \mathtt{unpack}\, e_1'\, \mathtt{as}\, x\, \mathtt{in}\, e_2' : \tau_2$, which follows analogously.

II. Consider arbitrary k, ρ, γ, and γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that
$(k, \gamma(\mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, e_2), \gamma'(\mathtt{unpack}\, e_1'\, \mathtt{as}\, x\, \mathtt{in}\, e_2')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$
$\equiv (k, \mathtt{unpack}\, \gamma(e_1)\, \mathtt{as}\, x\, \mathtt{in}\, \gamma(e_2), \mathtt{unpack}\, \gamma'(e_1')\, \mathtt{as}\, x\, \mathtt{in}\, \gamma'(e_2')) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.
Consider arbitrary j, e_f such that

- $j < k$,
- $\mathtt{unpack}\, \gamma(e_1)\, \mathtt{as}\, x\, \mathtt{in}\, \gamma(e_2) \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Hence, by inspection of the operational semantics, it follows that there exist j_1 and e_{f_1} such that

- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$,
- $\mathit{irred}(e_{f_1})$, and
- $j_1 \leq j$.

Instantiate the second conjunct of $\Delta; \Gamma \vdash e_1 \leq e_1' : \exists\alpha.\, \tau_1$ with k, ρ, γ, and γ'. Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(e_1), \gamma'(e_1')) \in \mathcal{RC}\,[\![\exists\alpha.\, \tau_1]\!]\,\rho$.
Instantiate this with j_1, e_{f_1}. Note that

- $j_1 < k$, which follows from $j_1 \leq j$ and $j < k$,
- $\gamma(e_1) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e'_{f_1} such that

- $\gamma'(e'_1) \longmapsto^* e'_{f_1}$, and
- $(k - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\exists\alpha.\,\tau_1]\!]\,\rho$.

Hence, $e_{f_1} \equiv \mathtt{pack}\, v_{f_{11}}$ and $e'_{f_1} \equiv \mathtt{pack}\, v'_{f_{11}}$.
Note that

$$\begin{aligned}\gamma(\mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, e_2) &\equiv \mathtt{unpack}\, \gamma(e_1)\, \mathtt{as}\, x\, \mathtt{in}\, \gamma(e_2)\\ &\longmapsto^{j_1} \mathtt{unpack}\, e_{f_1}\, \mathtt{as}\, x\, \mathtt{in}\, \gamma(e_2)\\ &\equiv \mathtt{unpack}\, (\mathtt{pack}\, v_{f_{11}})\, \mathtt{as}\, x\, \mathtt{in}\, \gamma(e_2)\\ &\longmapsto^{1} \gamma(e_2)[v_{f_{11}}/x] \longmapsto^{j_2} e_f\end{aligned}$$

where $\mathit{irred}(e_f)$ and $j = j_1 + 1 + j_2$.
From $(k - j_1, \mathtt{pack}\, v_{f_{11}}, \mathtt{pack}\, v'_{f_{11}}) \in \mathcal{RV}\,[\![\exists\alpha.\,\tau_1]\!]\,\rho$, it follows that there exist τ_{22} and χ such that

- $\chi \in \mathit{Rel}_{\tau_{22}}$, and
- $\forall i < k - j_1.\ (i, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$.

Instantiate the latter with $k - j_1 - 1$. Note that $k - j_1 - 1 < k - j_1$.
Hence, $(k - j_1 - 1, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$.x
Instantiate the second conjunct of $\Delta, \alpha; \Gamma, x : \tau_1 \vdash e_2 \leq e'_2 : \tau_2$ with $k - j_1 - 1$, $\rho[\alpha \mapsto (\chi, \tau_{22})]$, $\gamma[x \mapsto v_{f_{11}}]$, and $\gamma'[x \mapsto v'_{f_{11}}]$. Note that

- $k - j_1 - 1 \geq 0$, which follows from $j_1 + 1 + j_2 = j$ and $j < k$,
- $\rho[\alpha \mapsto (\chi, \tau_{22})] \in \mathcal{RD}\,[\![\Delta, \alpha]\!]$,
  which follows from
  - $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
  - $\chi \in \mathit{Rel}_{\tau_{22}}$,
    which follows from above.
- $(k - j_1 - 1, \gamma[x \mapsto v_{f_{11}}], \gamma'[x \mapsto v'_{f_{11}}]) \in \mathcal{RG}\,[\![\Gamma, x : \tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$,
  which follows from
  - $(k - j_1 - 1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$,
    which follows from $(k - j_1 - 1, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ (since $\alpha \notin \mathit{FTV}(\Gamma)$),
    which follows from Lemma C.10 applied to $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$ and $k - j_1 - 1 \leq k$, and
  - $(k - j_1 - 1, v_{f_{11}}, v'_{f_{11}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$,
    which follows from above.

Hence, $(k - j_1 - 1, \gamma[x \mapsto v_{f_{11}}](e_2), \gamma'[x \mapsto v'_{f_{11}}](e'_2)) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$
$\equiv (k - j_1 - 1, \gamma(e_2)[v_{f_{11}}/x], \gamma'(e'_2)[v'_{f_{11}}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$.
Instantiate this with j_2 and e_f. Note that

- $j_2 < k - j_1 - 1$, which follows from $j_2 = j - j_1 - 1$ and $j < k$,
- $\gamma(e_2)[v_{f_{11}}/x] \longmapsto^{j_2} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, there exists e'_f such that

- $\gamma'(e'_2)[v'_{f_{11}}/x] \longmapsto^* e'_f$, and
- $(k - j_1 - 1 - j_2, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$
  $\equiv (k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$, since $j = j_1 + 1 + j_2$.

Pick $e'_f = e'_f$.
We are required to show that

- $\gamma'(\texttt{unpack}\, e_1' \,\texttt{as}\, x \,\texttt{in}\, e_2') \longmapsto^* e_f'$,
  which follows from

$$\begin{array}{l}\gamma'(\texttt{unpack}\, e_1' \,\texttt{as}\, x \,\texttt{in}\, e_2') \equiv \texttt{unpack}\, \gamma'(e_1') \,\texttt{as}\, x \,\texttt{in}\, \gamma'(e_2') \\ \qquad\qquad \longmapsto^* \texttt{unpack}\, e_{f_1}' \,\texttt{as}\, x \,\texttt{in}\, \gamma'(e_2') \\ \qquad\qquad \equiv \texttt{unpack}\, (\texttt{pack}\, v_{f_{11}}') \,\texttt{as}\, x \,\texttt{in}\, \gamma'(e_2') \\ \qquad\qquad \longmapsto^1 \gamma'(e_2')[v_{f_{11}}'/x] \\ \qquad\qquad \longmapsto^* e_f'\end{array}$$

  and

- $(k-j, e_f, e_f') \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$,
  which follows from $(k-j, e_f, e_f') \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, \tau_{22})]$ since $\alpha \notin FTV(\tau_2)$.

□

Lemma C.27 ($\lambda^{\forall\exists}$ Substitutivity: Values)

If $\Delta; \Gamma \vdash v \leq v' : \tau_1$ *and* $\Delta; \Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$,
then $\Delta; \Gamma \vdash e[v/x] \leq e'[v'/x] : \tau_2$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Delta; \Gamma \vdash e[v/x] : \tau_2$, which follows from Lemma C.5 applied to
  - $\Delta; \Gamma \vdash' : \tau_1$,
    which follows from $\Delta; \Gamma \vdash v \leq v' : \tau_1$, and
  - $\Delta; \Gamma, x : \tau_1 \vdash e : \tau_2$,
    which follows from $\Delta; \Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$.
- $\Delta; \Gamma \vdash e'[v'/x] : \tau_2$, which follows analogously.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(e[v/x]), \gamma'(e'[v'/x])) \in \mathcal{RC}[\![\tau_2]\!]\,\rho$.
Instantiate the second conjunct of $\Delta; \Gamma \vdash v \leq v' : \tau_1$ with k, ρ, γ, and γ'. Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(v), \gamma'(v')) \in \mathcal{RC}[\![\tau_1]\!]\,\rho$.
Instantiate this with 0 and $\gamma(v)$.
Note that $\gamma(v)$ is a value. Hence,

- $\gamma(v) \longmapsto^0 \gamma(v)$, and
- $\mathit{irred}(\gamma(v))$.

Hence, there exists e'_f such that

- $\gamma'(v') \longmapsto^* e'_f$, and
- $(k - 0, \gamma(v), e'_f) \in \mathcal{RV}[\![\tau_1]\!]\,\rho$.

Since $\gamma'(v')$ is a value, it follows that $\gamma'(v') \longmapsto^0 \gamma'(v')$. Hence $e'_f \equiv \gamma'(v')$.
Thus, $(k - 0, \gamma(v), e'_f) \in \mathcal{RV}[\![\tau_1]\!]\,\rho$
$\equiv (k, \gamma(v), \gamma'(v')) \in \mathcal{RV}[\![\tau_1]\!]\,\rho$.
Instantiate the second conjunct of $\Delta; \Gamma, x : \tau_1 \vdash e \leq e' : \tau_2$ with k, $\gamma[x \mapsto \gamma(v)]$, and $\gamma'[x \mapsto \gamma'(v')]$.
Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
- $(k, \gamma[x \mapsto \gamma(v)], \gamma'[x \mapsto \gamma'(v')]) \in \mathcal{RG}[\![\Gamma, x : \tau_1]\!]\,\rho$,
  which follows from

- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$, and
- $(k, \gamma(v), \gamma'(v')) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$, which follows from above.

Hence, $(k, \gamma[x \mapsto \gamma(v)](e), \gamma'[x \mapsto \gamma'(v')](e') \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$
$\equiv (k, \gamma(e[\gamma(v)/x]), \gamma'(e'[\gamma'(v')/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$
$\equiv (k, \gamma(e[v/x]), \gamma'(e'[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho.$

□

Lemma C.28 ($\lambda^{\forall\exists}$ Substitutivity: Types)

If $\Delta \vdash \tau_1$ *and* $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau_2$,
then $\Delta; \Gamma[\tau_1/\alpha] \vdash e \leq e' : \tau_2[\tau_1/\alpha]$.

Proof

The proof is in 2 parts.

I. We are required to show

- $\Delta; \Gamma[\tau_1/\alpha] \vdash e : \tau_2[\tau_1/\alpha]$, which follows from Lemma C.6 applied to
  - $\Delta \vdash \tau_1$,
    which we have as a premise, and
  - $\Delta, \alpha; \Gamma \vdash e : \tau_2$,
    which follows from $\Delta, \alpha; \Gamma \vdash e \leq e : \tau_2$.
- $\Delta; \Gamma[\tau_1/\alpha] \vdash e' : \tau_2[\tau_1/\alpha]$, which follows analogously.

II. Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma[\tau_1/\alpha]]\!]\,\rho$.

We are required to show that $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\![\tau_2[\tau_1/\alpha]]\!]\,\rho$.
Consider arbitrary j and e_f such that

- $j < k$,
- $\gamma(e) \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

We are required to show that $\exists e'_f.\ \gamma'(e') \longmapsto^* e'_f \ \wedge\ (k - j, e_f, e'_f) \in \mathcal{RV}[\![\tau_2[\tau_1/\alpha]]\!]\,\rho$.
Let $\chi = \mathcal{RV}[\![\tau_1]\!]\,\rho$.
Instantiate the second conjunct of $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau_2$ with k, $\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$, γ, and γ'.
Note that

- $k \geq 0$,
- $\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})] \in \mathcal{RD}[\![\Delta, \alpha]\!]$,
  which follows from
  - $\rho \in \mathcal{RD}[\![\Delta]\!]$, and
  - $\chi = \mathcal{RV}[\![\tau_1]\!]\,\rho \in \mathit{Rel}_{(\tau_1)^{[\rho]}}$,
    which follows from Lemma C.11 applied to $\rho \in \mathcal{RD}[\![\Delta]\!]$ and $\Delta \vdash \tau_1$.
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$,
  which follows from
  - $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma[\tau_1/\alpha]]\!]\,\rho$,
    which follows from above, and
  - $\mathcal{RG}[\![\Gamma]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})] \ = \ \mathcal{RG}[\![\Gamma[\tau_1/\alpha]]\!]\,\rho$,
    which follows from Lemma C.13 applied to $\rho \in \mathcal{RD}[\![\Delta]\!]$ and $\Delta \vdash \tau_1$, since $\chi = \mathcal{RV}[\![\tau_1]\!]\,\rho$.

Hence, $(k, \gamma(e), \gamma'(e') \in \mathcal{RC}[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$.
Instantiate this with j and e_f. Note that

- $j < k$,
- $\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e'_f)$.

Hence, there exists e'_f such that

- $\gamma'(e') \longmapsto^{*} e'_f$, and
- $(k-j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})]$.

It remains for us to show that $(k-j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2[\tau_1/\alpha]]\!]\,\rho$.

Note that $\mathcal{RV}\,[\![\tau_2]\!]\,\rho[\alpha \mapsto (\chi, (\tau_1)^{[\rho]})] \;=\; \mathcal{RV}\,[\![\tau_2[\tau_1/\alpha]]\!]\,\rho$, which follows from Lemma C.12 applied to $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\Delta \vdash \tau_1$ and $\chi = \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.
Hence, $(k-j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau_2[\tau_1/\alpha]]\!]\,\rho$.

□

C.9 $\lambda^{\forall\exists}$ Proofs: Reflexivity

Lemma C.29 ($\lambda^{\forall\exists}$ Reflexivity)

If $\Delta;\Gamma \vdash e : \tau$, *then* $\Delta;\Gamma \vdash e \leq e : \tau$.

Proof

By induction on the derivation $\Delta;\Gamma \vdash e : \tau$.

Each case follows from the corresponding compatibility lemma (i.e., Lemmas C.15 through C.26). □

C.10 $\lambda^{\forall\exists}$ Proofs: Soundness w.r.t. Contextual Equivalence

In this section, we show that $\leq \subseteq \preceq^{ctx}$.

Lemma C.30 ($\lambda^{\forall\exists}$ Context Compatibility: Id)

If $\Delta_0 \supseteq \Delta$ *and* $\Gamma_0 \supseteq \Gamma$,
then $\Delta_0; \Gamma_0 \vdash [\cdot] \leq [\cdot] : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash [e] \leq [e'] : \tau \;\equiv\; \Delta_0; \Gamma_0 \vdash e \leq e' : \tau$.
Consider arbitrary k, ρ_0, γ_0, and γ_0' such that

- $k \geq 0$,
- $\rho_0 \in \mathcal{RD}[\![\Delta_0]\!]$, and
- $(k, \gamma_0, \gamma_0') \in \mathcal{RG}[\![\Gamma_0]\!]\,\rho_0$.

We are required to show that $(k, \gamma_0(e), \gamma_0'(e')) \in \mathcal{RC}[\![\tau]\!]\,\rho_0$.
Let $\rho = \rho_0|_{dom(\Delta)}$. Note that

- $\rho \in \mathcal{RD}[\![\Delta]\!]$,
  which follows from $\rho_0 \in \mathcal{RD}[\![\Delta_0]\!]$ and $\Delta_0 \supseteq \Delta$.

Let $\gamma = \gamma_0|_{dom(\Gamma)}$ and $\gamma' = \gamma_0'|_{dom(\Gamma)}$. Note that

- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho_0$,
  which follows from $(k, \gamma_0, \gamma_0') \in \mathcal{RG}[\![\Gamma_0]\!]\,\rho_0$ and $\Gamma_0 \supseteq \Gamma$.

Hence, note that

- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$,
  which follows from $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho_0$ since $FTV(\Gamma) \subseteq dom(\Delta)$ and $\rho \in \mathcal{RD}[\![\Delta]\!]$.

Note that

- $(k, \gamma_0(e), \gamma_0'(e')) \in \mathcal{RC}[\![\tau]\!]\,\rho_0$
  $\equiv (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\![\tau]\!]\,\rho_0$,
  which follows from $FV(e) \subseteq dom(\Gamma)$ and $FV(e') \subseteq dom(\Gamma)$
  $\equiv (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\![\tau]\!]\,\rho$,
  which follows from $FTV(\tau) \subseteq dom(\Delta)$ and $\rho \in \mathcal{RD}[\![\Delta]\!]$.

Hence, it suffices to show that $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\![\tau]\!]\,\rho$.
Instantiate the second conjunct of $\Delta; \Gamma \vdash e \leq e' : \tau$ with k, ρ, γ, and γ'. Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}[\![\Delta]\!]$,
  which follows from above, and
- $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]$,
  which follows from above.

Hence, $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\![\tau]\!]\,\rho$. □

Lemma C.31 **($\lambda^{\forall\exists}$ Context Compatibility: If1)**

If $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \mathsf{bool}$, $\Delta_0; \Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, *and* $\Delta_0; \Gamma_0 \vdash e_3 \leq e_3' : \tau_0$, *then* $\Delta_0; \Gamma_0 \vdash \mathtt{if}\, C, e_2, e_3 \leq \mathtt{if}\, C', e_2', e_3' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that
$\Delta_0; \Gamma_0 \vdash \mathtt{if}\, C[e], e_2, e_3 \leq \mathtt{if}\, C'[e'], e_2', e_3' : \tau_0$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \mathsf{bool}$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \mathsf{bool}$.

Applying Lemma C.17 to

- $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \mathsf{bool}$,
- $\Delta_0; \Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, and
- $\Delta_0; \Gamma_0 \vdash e_3 \leq e_3' : \tau_0$,

we conclude that $\Delta_0; \Gamma_0 \vdash \mathtt{if}\, C[e], e_2, e_3 \leq \mathtt{if}\, C'[e'], e_2', e_3' : \tau_0$. □

Lemma C.32 **($\lambda^{\forall\exists}$ Context Compatibility: If2)**

If $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$, $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$, *and* $\Delta_0; \Gamma_0 \vdash e_3 \leq e_3' : \tau_0$, *then* $\Delta_0; \Gamma_0 \vdash \mathtt{if}\, e_1, C, e_3 \leq \mathtt{if}\, e_1', C', e_3' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that
$\Delta_0; \Gamma_0 \vdash \mathtt{if}\, e_1, C[e], e_3 \leq \mathtt{if}\, e_1', C'[e'], e_3' : \tau_0$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$.

Applying Lemma C.17 to

- $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$,
- $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$, and
- $\Delta_0; \Gamma_0 \vdash e_3 \leq e_3' : \tau_0$,

we conclude that $\Delta_0; \Gamma_0 \vdash \mathtt{if}\, e_1, C[e], e_3 \leq \mathtt{if}\, e_1', C'[e'], e_3' : \tau_0$. □

Lemma C.33 ($\lambda^{\forall\exists}$ Context Compatibility: If3)

If $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$, $\Delta_0; \Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, *and* $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$,
then $\Delta_0; \Gamma_0 \vdash \mathtt{if}\, e_1, e_2, C \leq \mathtt{if}\, e_1', e_2', C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that
$\Delta_0; \Gamma_0 \vdash \mathtt{if}\, e_1, e_2, C[e] \leq \mathtt{if}\, e_1', e_2', C'[e'] : \tau_0$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$.

Applying Lemma C.17 to

- $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \mathsf{bool}$,
- $\Delta_0; \Gamma_0 \vdash e_2 \leq e_2' : \tau_0$, and
- $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_0$,

we conclude that $\Delta_0; \Gamma_0 \vdash \mathtt{if}\, e_1, e_2, C[e] \leq \mathtt{if}\, e_1', e_2', C'[e'] : \tau_0$. □

Lemma C.34 ($\lambda^{\forall\exists}$ Context Compatibility: Fn)

If $\Delta_0; \Gamma_0, x : \tau_1 \vdash C \leq C' : (\Delta; \Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2$,
then $\Delta_0; \Gamma_0 \vdash \lambda x.\, C \leq \lambda x.\, C' : (\Delta; \Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma, x : \tau_1 \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash \lambda x.\, C[e] \leq \lambda x.\, C'[e'] : \tau_1 \to \tau_2$.

Instantiate $\Delta_0; \Gamma_0, x : \tau_1 \vdash C \leq C' : (\Delta; \Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2$ with e and e', noting that $\Delta; \Gamma, x : \tau_1 \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0, x : \tau_1 \vdash C[e] \leq C'[e'] : \tau_2$.

Applying Lemma C.19 to $\Delta_0; \Gamma_0, x : \tau_1 \vdash C[e] \leq C'[e'] : \tau_2$, we conclude that $\Delta_0; \Gamma_0 \vdash \lambda x.\, C[e] \leq \lambda x.\, C'[e'] : \tau_1 \to \tau_2$. □

Lemma C.35 ($\lambda^{\forall\exists}$ Context Compatibility: App1)

If $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)$, *and* $\Delta_0; \Gamma_0 \vdash e_2 \leq e_2' : \tau_1$,
then $\Delta_0; \Gamma_0 \vdash C\, e_2 \leq C'\, e_2' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_2$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash (C[e])\, e_2 \leq (C'[e'])\, e_2' : \tau_2$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow (\tau_1 \to \tau_2)$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1 \to \tau_2$.

Applying Lemma C.20 to

- $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1 \to \tau_2$, and
- $\Delta_0; \Gamma_0 \vdash e_2 \leq e_2' : \tau_1$,

we conclude that $\Delta_0; \Gamma_0 \vdash (C[e])\, e_2 \leq (C'[e'])\, e_2' : \tau_2$. □

Lemma C.36 ($\lambda^{\forall\exists}$ Context Compatibility: App2)

If $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$, *and* $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$,
then $\Delta_0; \Gamma_0 \vdash e_1\, C \leq e_1'\, C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_2$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash e_1\, (C[e]) \leq e_1'\, (C'[e']) : \tau_2$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1$.

Applying Lemma C.20 to

- $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \tau_1 \to \tau_2$, and
- $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1$,

we conclude that $\Delta_0; \Gamma_0 \vdash e_1\, (C[e]) \leq e_1'\, (C'[e']) : \tau_2$. □

Lemma C.37 ($\lambda^{\forall\exists}$ Context Compatibility: Fold)

If $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1[\mu\alpha.\, \tau_1/\alpha]$,
then $\Delta_0; \Gamma_0 \vdash \texttt{fold}\, C \leq \texttt{fold}\, C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow (\mu\alpha.\, \tau_1)$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash \texttt{fold}\, C[e] \leq \texttt{fold}\, C'[e'] : \mu\alpha.\, tau_1$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1[\mu\alpha.\, \tau_1/\alpha]$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1[\mu\alpha.\, \tau_1/\alpha]$.

Applying Lemma C.21 to $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1[\mu\alpha.\, \tau_1/\alpha]$, we conclude that $\Delta_0; \Gamma_0 \vdash \texttt{fold}\, C[e] \leq \texttt{fold}\, C'[e'] : \mu\alpha.\, \tau_1$. □

Lemma C.38 ($\lambda^{\forall\exists}$ Context Compatibility: Unfold)

If $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow (\mu\alpha.\, \tau_1)$,
then $\Delta_0; \Gamma_0 \vdash \mathtt{unfold}\, C \leq \mathtt{unfold}\, C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1[\mu\alpha.\, \tau_1/\alpha]$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash \mathtt{unfold}\, C[e] \leq \mathtt{unfold}\, C'[e'] : \tau_1[\mu\alpha.\, \tau_1/\alpha]$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \mu\alpha.\, \tau_1$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \mu\alpha.\, \tau_1$.

Applying Lemma C.22 to $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \mu\alpha.\, \tau_1$, we conclude that $\Delta_0; \Gamma_0 \vdash \mathtt{unfold}\, C[e] \leq \mathtt{unfold}\, C'[e'] : \tau_1[\mu\alpha.\, \tau_1/\alpha]$. □

Lemma C.39 ($\lambda^{\forall\exists}$ Context Compatibility: All)

If $\Delta_0, \alpha; \Gamma_0 \vdash C \leq C' : (\Delta, \alpha; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$,
then $\Delta_0; \Gamma_0 \vdash \Lambda.\, C \leq \Lambda.\, C' : (\Delta, \alpha; \Gamma \triangleright \tau) \rightsquigarrow \forall\alpha.\, \tau_1$.

Proof

Consider arbitrary e and e' such that

- $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash \Lambda.\, C[e] \leq \Lambda.\, C'[e'] : \forall\alpha.\, \tau_1$.

Instantiate $\Delta_0, \alpha; \Gamma_0 \vdash C \leq C' : (\Delta, \alpha; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$ with e and e', noting that $\Delta, \alpha; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0, \alpha; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1$.

Applying Lemma C.23 to $\Delta_0, \alpha; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1$, we conclude that $\Delta_0; \Gamma_0 \vdash \Lambda.\, C[e] \leq \Lambda.\, C'[e'] : \forall\alpha.\, \tau_1$. □

Lemma C.40 ($\lambda^{\forall\exists}$ Context Compatibility: Inst)

If $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \forall\alpha.\, \tau_1$ *and* $\Delta_0 \vdash \tau_2$,
then $\Delta_0; \Gamma_0 \vdash C\,[\,] \leq C'\,[\,] : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1[\tau_2/\alpha]$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash C[e]\,[\,] \leq C'[e']\,[\,] : \tau_1[\tau_2/\alpha]$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \forall\alpha.\, \tau_1$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \forall\alpha.\, \tau_1$.

Applying Lemma C.23 to $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \forall\alpha.\, \tau_1$ and $\Delta_0 \vdash \tau_2$, we conclude that $\Delta_0; \Gamma_0 \vdash C[e]\,[\,] \leq C'[e']\,[\,] : \tau_1[\tau_2/\alpha]$. □

Lemma C.41 ($\lambda^{\forall\exists}$ Context Compatibility: Pack)

If $\Delta_0 \vdash \tau_2$ *and* $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1[\tau_2/\alpha]$,
then $\Delta_0; \Gamma_0 \vdash \mathtt{pack}\, C \leq \mathtt{pack}\, C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \exists\alpha.\, \tau_1$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash \mathtt{pack}\, C[e] \leq \mathtt{pack}\, C'[e'] : \exists\alpha.\, \tau_1$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1[\tau_2/\alpha]$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1[\tau_2/\alpha]$.

Applying Lemma C.25 to $\Delta_0 \vdash \tau_2$ and $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \tau_1[\tau_2/\alpha]$, we conclude that $\Delta_0; \Gamma_0 \vdash \mathtt{pack}\, C[e] \leq \mathtt{pack}\, C'[e'] : \exists\alpha.\, \tau_1$. □

Lemma C.42 ($\lambda^{\forall\exists}$ Context Compatibility: Unpack1)

If $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \exists\alpha.\, \tau_1$, *and* $\Delta_0 \vdash \tau_2$, *and* $\Delta_0, \alpha; \Gamma_0, x : \tau_1 \vdash e_2 \leq e_2' : \tau_2$,
then $\Delta_0; \Gamma_0 \vdash \mathtt{unpack}\, C\, \mathtt{as}\, x\, \mathtt{in}\, e_2 \leq \mathtt{unpack}\, C'\, \mathtt{as}\, x\, \mathtt{in}\, e_2' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_2$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash \mathtt{unpack}\, (C[e])\, \mathtt{as}\, x\, \mathtt{in}\, e_2 \leq \mathtt{unpack}\, (C'[e'])\, \mathtt{as}\, x\, \mathtt{in}\, e_2' : \tau_2$.

Instantiate $\Delta_0; \Gamma_0 \vdash C \leq C' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \exists\alpha.\, \tau_1$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \exists\alpha.\, \tau_1$.

Applying Lemma C.26 to

- $\Delta_0; \Gamma_0 \vdash C[e] \leq C'[e'] : \exists\alpha.\, \tau_1$,
- $\Delta_0 \vdash \tau_2$, and
- $\Delta_0, \alpha; \Gamma_0, x : \tau_1 \vdash e_2 \leq e_2' : \tau_2$,

we conclude that $\Delta_0; \Gamma_0 \vdash \mathtt{unpack}\, (C[e])\, \mathtt{as}\, x\, \mathtt{in}\, e_2 \leq \mathtt{unpack}\, (C'[e'])\, \mathtt{as}\, x\, \mathtt{in}\, e_2' : \tau_2$. □

Lemma C.43 ($\lambda^{\forall\exists}$ Context Compatibility: Unpack2)

If $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \exists\alpha.\, \tau_1$, *and* $\Delta_0 \vdash \tau_2$, *and* $\Delta_0, \alpha; \Gamma_0, x : \tau_1 \vdash C \leq C' : (\Delta, \alpha; \Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2$, *then* $\Delta_0; \Gamma_0 \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, C \leq \mathtt{unpack}\, e_1'\, \mathtt{as}\, x\, \mathtt{in}\, C' : (\Delta, \alpha; \Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2$.

Proof

Consider arbitrary e and e' such that

- $\Delta, \alpha; \Gamma, x : \tau_1 \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, (C[e]) \leq \mathtt{unpack}\, e_1'\, \mathtt{as}\, x\, \mathtt{in}\, (C'[e']) : \tau_2$.

Instantiate $\Delta_0, \alpha; \Gamma_0, x : \tau_1 \vdash C \leq C' : (\Delta, \alpha; \Gamma, x : \tau_1 \triangleright \tau) \rightsquigarrow \tau_2$ with e and e', noting that $\Delta, \alpha; \Gamma, x : \tau_1 \vdash e \leq e' : \tau$.

Hence, $\Delta_0, \alpha; \Gamma_0, x : \tau_1 \vdash C[e] \leq C'[e'] : \tau_2$.

Applying Lemma C.26 to

- $\Delta_0; \Gamma_0 \vdash e_1 \leq e_1' : \exists\alpha.\, \tau_1$,
- $\Delta_0 \vdash \tau_2$, and
- $\Delta_0, \alpha; \Gamma_0, x : \tau_1 \vdash C[e] \leq C'[e'] : \tau_2$,

we conclude that $\Delta_0; \Gamma_0 \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, x\, \mathtt{in}\, (C[e]) \leq \mathtt{unpack}\, e_1'\, \mathtt{as}\, x\, \mathtt{in}\, (C'[e']) : \tau_2$. □

Lemma C.44 ($\lambda^{\forall\exists}$ Context Compatibility: Ctxt)

If $\Delta_0; \Gamma_0 \vdash C_0 \leq C_0' : (\Delta_1; \Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0$, *and* $\Delta_1; \Gamma_1 \vdash C_1 \leq C_1' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$, *then* $\Delta_0; \Gamma_0 \vdash C_0[C_1[\cdot]] \leq C_0'[C_1'[\cdot]] : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$.

Proof

Consider arbitrary e and e' such that

- $\Delta; \Gamma \vdash e \leq e' : \tau$.

We are required to show that $\Delta_0; \Gamma_0 \vdash C_0[C_1[e]] \leq C_0'[C_1'[e']] : \tau_0$.

Instantiate $\Delta_1; \Gamma_1 \vdash C_1 \leq C_1' : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$ with e and e', noting that $\Delta; \Gamma \vdash e \leq e' : \tau$.

Hence, $\Delta_1; \Gamma_1 \vdash C_1[e] \leq C_1'[e'] : \tau_1$.

Instantiate $\Delta_0; \Gamma_0 \vdash C_0 \leq C_0' : (\Delta_1; \Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0$ with $C_1[e]$ and $C_1'[e']$, noting that $\Delta_1; \Gamma_1 \vdash C_1[e] \leq C_1'[e'] : \tau_1$.

Hence, $\Delta_0; \Gamma_0 \vdash C_0[C_1[e]] \leq C_0'[C_1'[e']] : \tau_0$. □

Lemma C.45 ($\lambda^{\forall\exists}$ Context Reflexivity)

If $\Delta_1; \Gamma_1 \vdash C : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$, *then* $\Delta_1; \Gamma_1 \vdash C \leq C : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$.

Proof

By induction on the derivation $\Delta_1; \Gamma_1 \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$.

Each case follows from the corresponding compatibility lemma (i.e., Lemmas C.30 through C.43). □

Lemma C.46 ($\lambda^{\forall\exists}$ **:** $\leq \subseteq \preceq^{ctx}$)

If $\Delta;\Gamma \vdash e \leq e' : \tau$*, then* $\Delta;\Gamma \vdash e \preceq^{ctx} e' : \tau$.

Proof

Consider arbitrary C and τ_1 such that

- $\bullet;\bullet \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, and
- $C[e] \Downarrow$.

Hence, there exists some value v_f and some k such that

- $C[e] \longmapsto^k v_f$.

We are required to show that $C[e'] \Downarrow$.

Note that $\bullet;\bullet \vdash C \leq C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1$, which follows from Lemma C.45 applied to $\bullet \vdash C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1$.

Instantiate $\bullet;\bullet \vdash C \leq C : (\Delta;\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ with e and e', noting that $\Delta;\Gamma \vdash e \leq e' : \tau$.

Hence, $\bullet;\bullet \vdash C[e] \leq C[e'] : \tau_1$.

Instantiate this with $k+1$, $\emptyset$, $\emptyset$, and $\emptyset$. Note that

- $k+1 \geq 0$,
- $\emptyset \in \mathcal{RD}\,[\![\bullet]\!]$,
- $(k+1,\emptyset,\emptyset) \in \mathcal{RG}\,[\![\bullet]\!]\,\emptyset$.

Hence, $(k+1, C[e], C[e']) \in \mathcal{RC}\,[\![\tau_1]\!]\,\emptyset$.

Instantiate this with k and v_f. Note that

- $k < k+1$,
- $C[e] \longmapsto^k v_f$, and
- $\mathit{irred}(v_f)$, which follows from the fact that v_f is value.

Hence, there exists v'_f such that

- $C[e'] \longmapsto^* v'_f$, and
- $(k+1-k, v_f, v'_f) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$.

Hence, $C[e'] \Downarrow v'_f$. □

D Examples

In this section, we present several examples to illustrate uses of our logical relations method for proving contextual equivalence. The examples are taken directly from Sumii and Pierce [19] so that the reader may compare the use of their bisimulation against the use of our step-indexed logical relation for showing contextual equivalence. These examples involve existential packages, contravariant recursive types, and higher-order functions (Sections D.1–D.5).

In each of the examples that follow, we wish to show that the closed terms e and e' of type τ are contextually equivalent — that is, $\bullet;\bullet \vdash e \simeq^{ctx} e' : \tau$. It suffices to show $\bullet;\bullet \vdash e \sim e' : \tau$.

Recursive Functions

Encoding Fix: Some of the examples that follow (see Sections D.4 and D.5) make use of recursive functions $\mathtt{fix}\, f(x).\, e$ which can be encoded in $\lambda^{\forall\exists}$ as follows:

$$\begin{array}{lcl} \mathtt{Y} & \equiv & \Lambda.\, \lambda f.\, (\lambda x.\, f\, ((\mathtt{unfold}\, x)\, x))\, \mathtt{fold}\, (\lambda x.\, f\, ((\mathtt{unfold}\, x)\, x)) \\ \mathtt{fix}\, f(x).\, e & \equiv & (\mathtt{Y}\, [\,])\, \lambda f.\, \lambda x.\, e \end{array}$$

where we can derive the following rules:

$$(\mathsf{Y})\ \frac{}{\Delta;\Gamma \vdash \mathtt{Y} : \forall\alpha.\, (\alpha \to \alpha) \to \alpha} \qquad (\mathsf{FixTy})\ \frac{\Delta;\Gamma, f : \tau_1 \to \tau_2, x : \tau_1 \vdash e : \tau_2}{\Delta;\Gamma \vdash \mathtt{fix}\, f(x).\, e : \tau_1 \to \tau_2}$$

With the above formulation, the term $\mathtt{fix}\, f(x).\, e$ is not itself a value, but it reduces to a lambda abstraction. Though we could use the above encoding in the examples that follow, the downside is that we would end up having to desugar $\mathtt{fix}\, f(x).\, e$ when establishing the equivalence of recursive functions.

Fix as a Language Primitive: To simplify proving equivalence of recursive functions, we will instead tweak the $\lambda^{\forall\exists}$ calculus slightly, replacing terms $\lambda x.\, e$ with $\mathtt{fix}\, f(x).\, e$ and treating the latter as values in $\lambda^{\forall\exists}$. We will continue to write $\lambda x.\, e$ whenever f does not appear free in e. We modify the (app) rule in the operational semantics as follows.

$$(\mathtt{fix}\, f(x).\, e)\, v \longmapsto e[\mathtt{fix}\, f(x).\, e/f][v/x]$$

We replace the function typing rule (FnTy) with the (FixTy) rule given above. The relational interpretation of function types is modified as follows.

$$\begin{array}{rcll} \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho & = & \{(k, \mathtt{fix}\, f(x).\, e, \mathtt{fix}\, f(x).\, e') \mid & \vdash \mathtt{fix}\, f(x).\, e' : (\tau_1 \to \tau_2)^{[\rho]} \ \wedge \\ & & & \forall j < k, v, v'. \\ & & & \quad (j, v, v') \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho \ \wedge \\ & & & \quad (j, \mathtt{fix}\, f(x).\, e, \mathtt{fix}\, f(x).\, e') \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho \implies \\ & & & \quad (j, e[v/x], e'[v'/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho\} \end{array}$$

We note that all the lemmas pertaining to function types proved in Section C are still provable after appropriate modifications to comply with the (FixTy) rule and the new relational interpretion of function types.

D.1 Simple Existential Packages

Consider the following existential packages e and e' of type τ (see Sumii and Pierce [19], Section 4.1):

$$\begin{array}{lcl} e & = & \mathtt{pack}\,\langle 1, \lambda x.\, x \stackrel{\mathrm{int}}{=} 0\rangle \\ e' & = & \mathtt{pack}\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle \\ \tau & = & \exists\alpha.\, \alpha \times (\alpha \to \mathsf{bool}) \end{array}$$

We are required to show that $\bullet;\bullet \vdash e \sim e' : \tau$. The proof is in two parts.

I. Show $\bullet;\bullet \vdash e \leq e' : \tau$.

Consider arbitrary k, ρ, γ, γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\bullet]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Hence, $\rho = \emptyset$ and $\gamma = \gamma' = \emptyset$.

We are required to show that $(k, e, e') \in \mathcal{RC}\,[\![\tau]\!]\,\emptyset$. (Note that if $k = 0$ we are done.)

Consider arbitrary j and e_f such that

- $j < k$,
- $e \longmapsto^j e_f$, and
- $\mathit{irred}(e_f)$.

Since e is a value, we conclude that $j = 0$ and $e = e_f$. Also, note that e' is a value.

Pick $e'_f = e'$.

Note that $e' \longmapsto^* e'$ and $\mathit{val}(e')$.

It remains for us to show that $(k - 0, e, e') \in \mathcal{RV}\,[\![\tau]\!] \equiv (k, \mathtt{pack}\,\langle 1, \lambda x.\, x \stackrel{\mathrm{int}}{=} 0\rangle, \mathtt{pack}\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\exists\alpha.\, \alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset$.

Note that we already have $\vdash e' : \tau$.

Take $\tau_2 = \mathsf{bool}$ and $\chi = \{(k', 1, \mathtt{tt}) \mid\ k' \geq 0\}$.

Note that $\chi \in \mathit{Rel}_{\mathsf{bool}}$, which follows from the definition of χ.

Consider arbitrary j such that $j < k$.

We are required to show that $(j, \langle 1, \lambda x.\, x \stackrel{\mathrm{int}}{=} 0\rangle, \langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which follows from

- $\vdash \langle \mathtt{tt}, \lambda x.\, \neg x\rangle : (\alpha \times (\alpha \to \mathsf{bool}))[\mathsf{bool}/\alpha]$
  $\equiv\ \vdash \langle \mathtt{tt}, \lambda x.\, \neg x\rangle : \mathsf{bool} \times (\mathsf{bool} \to \mathsf{bool})$, which is follows easily from the static semantics.
- $(j, 1, \mathtt{tt}) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv (j, 1, \mathtt{tt}) \in \chi$ (by the definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
  which in turn follows from our definition of χ.
- $(j, (\lambda x.\, x \stackrel{\mathrm{int}}{=} 0), (\lambda x.\, \neg x)) \in \mathcal{RV}\,[\![\alpha \to \mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which we conclude as follows:
  First, note that $\vdash \lambda x.\, \neg x : (\alpha \to \mathsf{bool})[\mathsf{bool}/\alpha]\ \equiv\ \vdash \lambda x.\, \neg x : \mathsf{bool} \to \mathsf{bool}$, which is immediate.
  Next, consider arbitrary i, v_1, and v'_1 such that

- $i < j$, and
- $(i, v_1, v_1') \in \mathcal{RV}[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.

Note that $\mathcal{RV}[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \equiv \chi$ by definition of $\mathcal{RV}[\![\alpha]\!]\,\rho$.

Hence, $(i, v_1, v_1') \in \chi$.

Then, it must be that $v_1 = 1$ and $v_1' = \mathtt{tt}$, which follows from the definition of χ.

We are required to show that

$$\begin{array}{rcl} (i, (x \overset{\text{int}}{=} 0)[v_1/x], (\neg x)[v_1'/x]) & \in & \mathcal{RC}[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \\ \equiv (i, v_1 \overset{\text{int}}{=} 0, \neg v_1') & \in & \mathcal{RC}[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \\ \equiv (i, 1 \overset{\text{int}}{=} 0, \neg \mathtt{tt}) & \in & \mathcal{RC}[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \end{array}$$

Note that $(1 \overset{\text{int}}{=} 0) \longmapsto^1 \mathtt{ff}$ and $(\neg \mathtt{tt}) \longmapsto^* \mathtt{ff}$.

Hence, it remains for us to show that $(i - 1, \mathtt{ff}, \mathtt{ff}) \in \mathcal{RV}[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which is immediate.

II. Show $\bullet; \bullet \vdash e' \leq e : \tau$.

Consider an arbitrary k such that $k \geq 0$.

Unwinding definitions as in **(I)** above, since e' and e are closed values of closed type, it suffices to show $(k, e', e) \in \mathcal{RV}[\![\tau]\!]\,\emptyset \equiv (k, \mathtt{pack}\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle, \mathtt{pack}\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) \in \mathcal{RV}[\![\exists \alpha.\, \alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset$.

Note that we already have $\vdash e : \tau$.

Take $\tau_2 = \mathsf{int}$ and $\chi = \{(k', \mathtt{tt}, 1) \mid\ k' \geq 0\}$.

Note that $\chi \in \mathit{Rel}_{\mathsf{int}}$, which follows from the definition of χ.

Consider arbitrary j such that $j < k$.

We are required to show that $(j, \langle \mathtt{tt}, \lambda x.\, \neg x\rangle, \langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) \in \mathcal{RV}[\![\alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$, which follows from

- $\vdash \langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle : (\alpha \times (\alpha \to \mathsf{bool}))[\mathsf{int}/\alpha]$
  $\equiv\ \vdash \langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle : \mathsf{int} \times (\mathsf{int} \to \mathsf{bool})$, which follows easily from the static semantics.
- $(j, \mathtt{tt}, 1) \in \mathcal{RV}[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$
  $\equiv (j, \mathtt{tt}, 1) \in \chi$ (by the definition of $\mathcal{RV}[\![\alpha]\!]\,\rho$)
  which in turn follows from our definition of χ.
- $(j, (\lambda x.\, \neg x), (\lambda x.\, x \overset{\text{int}}{=} 0)) \in \mathcal{RV}[\![\alpha \to \mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$, which we conclude as follows:

  First, note that $\vdash \lambda x.\, x \overset{\text{int}}{=} 0 : (\alpha \to \mathsf{bool})[\mathsf{int}/\alpha]\ \equiv\ \vdash \lambda x.\, x \overset{\text{int}}{=} 0 : \mathsf{int} \to \mathsf{bool}$, which is immediate.

  Next, consider arbitrary i, v_1, and v_1' such that

  - $i < j$, and
  - $(i, v_1, v_1') \in \mathcal{RV}[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$.

  Note that $\mathcal{RV}[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \equiv \chi$ by definition of $\mathcal{RV}[\![\alpha]\!]\,\rho$.

  Hence, $(i, v_1, v_1') \in \chi$.

  Then, it must be that $v_1 = \mathtt{tt}$ and $v_1' = 1$, which follows from the definition of χ.

We are required to show that

$$\begin{array}{rcl}(i, (\neg x)[v_1/x], (x \overset{\text{int}}{=} 0)[v_1'/x]) & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \\ \equiv (i, \neg v_1, v_1' \overset{\text{int}}{=} 0) & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \\ \equiv (i, \neg \mathtt{tt}, 1 \overset{\text{int}}{=} 0) & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]\end{array}$$

Note that $(\neg \mathtt{tt}) \longmapsto^1 \mathtt{ff}$ and $(1 \overset{\text{int}}{=} 0) \longmapsto^* \mathtt{ff}$.

Hence, it remains for us to show that $(i-1, \mathtt{ff}, \mathtt{ff}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$, which is immediate.

Discussion The above proof is largely mechanical. The only interesting part of showing that two packages have types $\exists\alpha.\,\tau'$ is the choice of χ and τ_2. This is because we later have to show that $\chi \in \mathit{Rel}_{\tau_2}$. But even the choice of χ is mostly mechanical:

- We decide on the pairs of values (v, v') (such that $\vdash v' : \tau_2$) that must be related at type α — for this particular example, the sets of pairs are $\{(1, \mathtt{tt})\}$ (with $\tau_2 = \mathsf{bool}$), or $\{(\mathtt{tt}, 1)\}$ (with $\tau_2 = \mathsf{int}$), depending on the direction of the proof.
- We define χ, which specifies that each of the above pairs of values is related at every step-index $k' \geq 0$. This is necessary in order to ensure that χ will be closed with respect to a decreasing step-index — i.e., if $(k, v, v') \in \chi$ and $j \leq k$, then $(j, v, v') \in \chi$.

For the set χ defined in this way, it is trivial to show $\chi \in \mathit{Rel}_{\tau_2}$.

Comparison with Sumii-Pierce In comparison, if we use Sumii and Pierce's [19] bisimulation method, we first have to come up with some bisimulation X and then show that X is in fact a valid bisimulation. For the above example, Sumii and Pierce show that we can pick either $X = \{(\emptyset, \mathcal{R}_0), (\Delta, \mathcal{R}_1), (\Delta, \mathcal{R}_2), (\Delta, \mathcal{R}_3), (\Delta, \mathcal{R}_4), (\Delta, \mathcal{R}_5)\}$ or $X = \{(\Delta, \mathcal{R}_5)\}$ where:

$$\begin{array}{rcl}\Delta & = & (\alpha, \mathsf{int}, \mathsf{bool}) \\ \mathcal{R}_0 & = & \{(e, e', \tau)\} \\ \mathcal{R}_1 & = & \mathcal{R}_0 \cup \{(\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle,\ \langle \mathtt{tt}, \lambda x.\, \neg x\rangle,\ \alpha \times (\alpha \to \mathsf{bool}))\} \\ \mathcal{R}_2 & = & \mathcal{R}_1 \cup \{(1, \mathtt{tt}, \alpha)\} \\ \mathcal{R}_3 & = & \mathcal{R}_1 \cup \{(\lambda x.\, x \overset{\text{int}}{=} 0,\ \lambda x.\, \neg x,\ \alpha \to \mathsf{bool})\} \\ \mathcal{R}_4 & = & \mathcal{R}_2 \cup \mathcal{R}_3 \\ \mathcal{R}_5 & = & \mathcal{R}_4 \cup \{(\mathtt{ff}, \mathtt{ff}, \mathsf{bool})\}\end{array}$$

As one would expect, one difference between the bisimulation and logical relations approach is as follows: with the bisimulation, one must specify at the outset which values are related at each type τ_s that is a subexpression of $\tau = \exists\alpha.\,\alpha \times (\alpha \to \mathsf{bool})$, whereas with a logical relation, in the course of the proof, one only has to specify which values are related at the type α.

For this example, once we have chosen X, proving that X is a valid bisimulation seems to require the same level of (largely mechanical) effort as was required for the logical relations proof.

D.2 Functions Generating Packages

Consider the following functions e and e' of type τ, which generate existential packages (see Sumii and Pierce [19], Section 4.3):

$$\begin{array}{lcllcl} e & = & \lambda y.\, e_1 & e_1 & = & \mathtt{pack}\,\langle y, \lambda x.\, x\rangle \\ e' & = & \lambda y.\, e'_1 & e'_1 & = & \mathtt{pack}\,\langle y+1, \lambda x.\, x-1\rangle \\ \tau & = & \mathsf{int} \to \tau_1 & \tau_1 & = & \exists\alpha.\, \alpha \times (\alpha \to \mathsf{int}) \end{array}$$

We are required to show that $\bullet;\bullet \vdash e \sim e' : \tau$. The proof is in two parts.

I. Show $\bullet;\bullet \vdash e \leq e' : \tau$.

Consider an arbitrary $k \geq 0$.

Unwinding definitions, we see that since e and e' are closed values of closed type, it suffices to show that $(k, e, e') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset \equiv (k, \lambda y.\, e_1, \lambda y.\, e'_1) \in \mathcal{RV}\,[\![\mathsf{int} \to \tau_1]\!]\,\emptyset$.

Note that we already have $\vdash \lambda y.\, e'_1 : \mathsf{int} \to \tau_1$.

Consider arbitrary j, v, and v' such that

- $j < k$, and
- $(j, v, v') \in \mathcal{RV}\,[\![\mathsf{int}]\!]\,\emptyset$.

Note that $\vdash v' : \mathsf{int}$, which follows from Lemma C.7 applied to $(j, v, v') \in \mathcal{RV}\,[\![\mathsf{int}]\!]\,\emptyset$.

Also, note that $v = v'$, which follows from the definition of $\mathcal{RV}\,[\![\mathsf{int}]\!]$.

We are required to show that $(j, e_1[v/x], e'_1[v'/x]) \in \mathcal{RC}\,[\![\tau_1]\!]\,\emptyset$
$\equiv (j, \mathtt{pack}\,\langle v, \lambda x.\, x\rangle, \mathtt{pack}\,\langle v'+1, \lambda x.\, x-1\rangle) \in \mathcal{RC}\,[\![\exists\alpha.\, \alpha \times (\alpha \to \mathsf{int})]\!]\,\emptyset$.

Consider arbitrary j_1 and e_{f_1} such that

- $j_1 < j$,
- $\mathtt{pack}\,\langle v, \lambda x.\, x\rangle \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Since $\mathtt{pack}\,\langle v, \lambda x.\, x\rangle$ is a value, we have $j_1 = 0$ and $e_{f_1} = \mathtt{pack}\,\langle v, \lambda x.\, x\rangle$.

Let $e'_{f_1} = \mathtt{pack}\,\langle v'+1, \lambda x.\, x-1\rangle$.

Note that $\mathtt{pack}\,\langle v'+1, \lambda x.\, x-1\rangle \longmapsto^* \mathtt{pack}\,\langle v'+1, \lambda x.\, x-1\rangle$.

Thus, it remains for us to show that $(j - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\emptyset$
$\equiv\ (j, \mathtt{pack}\,\langle v, \lambda x.\, x\rangle, \mathtt{pack}\,\langle v'+1, \lambda x.\, x-1\rangle) \in \mathcal{RV}\,[\![\exists\alpha.\, \alpha \times (\alpha \to \mathsf{int})]\!]\,\emptyset$.

Note that $\vdash \mathtt{pack}\,\langle v'+1, \lambda x.\, x-1\rangle : \exists\alpha.\, \alpha \times (\alpha \to \mathsf{int})$, which follows from the (Pack) rule applied to

- $\bullet \vdash \mathsf{int}$, and
- $\bullet;\bullet \vdash \langle v'+1, \lambda x.\, x-1\rangle : (\alpha \times (\alpha \to \mathsf{int}))[\mathsf{int}/\alpha]$
  $\equiv \bullet;\bullet \vdash \langle v'+1, \lambda x.\, x-1\rangle : \mathsf{int} \times (\mathsf{int} \to \mathsf{int})$, which follows from the static semantics and $\vdash v' : \mathsf{int}$.

Take $\tau_2 = \mathsf{int}$ and $\chi = \{(k', n, n+1) \mid\ k' \geq 0\ \wedge\ \vdash n : \mathsf{int}\}$.

Note that $\chi \in \mathit{Rel}_{\mathsf{int}}$, which follows easily from the definition of χ.

Consider an arbitrary i such that $i < j$.

We are required to show that $(j, \langle v, \lambda x.\, x\rangle, \langle v'+1, \lambda x.\, x-1\rangle) \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \mathsf{int})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$, which follows from

- $\vdash \langle v'+1, \lambda x.\, x-1\rangle : (\alpha \times (\alpha \to \mathsf{int}))[\mathsf{int}/\alpha]$
  $\equiv \ \vdash \langle v'+1, \lambda x.\, x-1\rangle : \mathsf{int} \times (\mathsf{int} \to \mathsf{int})$,
  which follows from the static semantics and $\vdash v' : \mathsf{int}$.

- $(j, v, v'+1) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$
  $\equiv (j, v, v'+1) \in \chi$ (by definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
  $\equiv (j, v, v+1) \in \chi$ (since $v = v'$ above)
  which follows from the definition of χ.

- $(j, \lambda x.\, x, \lambda x.\, x-1) \in \mathcal{RV}\,[\![\alpha \to \mathsf{int}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$, which we conclude as follows:
  First, note that $\vdash \lambda x.\, x-1 : (\alpha \to \mathsf{int})[\mathsf{int}/\alpha] \ \equiv \ \vdash \lambda x.\, x-1 : \mathsf{int} \to \mathsf{int}$, which is immediate.

  Next, consider arbitrary i, v_{11}, and v'_{11} such that

  - $i < j$, and
  - $(i, v_{11}, v'_{11}) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$.

  Note that $\mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \equiv \chi$ by definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$.

  Hence, $(i, v_{11}, v'_{11}) \in \chi$.

  Then, it must be that $v_{11} = n$ and $v'_{11} = n+1$, where $\vdash n : \mathsf{int}$.

  We are required to show that

$$\begin{array}{rcl} (i, x[v_{11}/x], (x-1)[v'_{11}/x]) & \in & \mathcal{RC}\,[\![\mathsf{int}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \\ \equiv (i, v_{11}, v'_{11} - 1) & \in & \mathcal{RC}\,[\![\mathsf{int}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \\ \equiv (i, n, (n+1) - 1) & \in & \mathcal{RC}\,[\![\mathsf{int}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \end{array}$$

  Note that $n \longmapsto^0 n$ and $((n+1)-1) \longmapsto^* n$.

  Hence, it remains for us to show that $(i-0, n, n) \in \mathcal{RV}\,[\![\mathsf{int}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$, which is immediate.

II. Show $\bullet; \bullet \vdash e' \le e : \tau$.

The proof is analogous to that of **(I)**.

Comparison with Sumii-Pierce For this example, Sumii and Pierce must consider an *infinite* bisimulation. They choose the following bisimulation, which they point out is not the minimal one:

$$\begin{array}{rcl} X & = & \{(\Delta, \mathcal{R}) \mid \\ & & \quad \Delta = \{(\beta_i, \mathsf{int}, \mathsf{int}) \mid -n \le i \le n\}, \\ & & \quad \mathcal{R} \subseteq \cup_{-n \le i \le n} \mathcal{R}_i, \\ & & \quad n = 0, 1, 2, \ldots\} \\ \mathcal{R}_i & = & \{(e, e', \mathsf{int} \to \tau_1), \\ & & \quad (e_1[i/y], e'_1[i/y], \tau_1), \\ & & \quad (\langle i, \lambda x.\, x\rangle, \langle i+1, \lambda x.\, x-1\rangle, \beta_i \times (\beta_i \to \mathsf{int})), \\ & & \quad (i, i+1, \beta_i), \\ & & \quad (\lambda x.\, x, \lambda x.\, x-1, \beta_i \to \mathsf{int}), \\ & & \quad (i, i, \mathsf{int})\} \end{array}$$

We note that with the logical relations approach, there is no need to consider an infinite set of types β_i or an infinite set of relations analogous to $\mathcal{R}_i$.

D.3 Higher-Order Functions I

Consider the following higher-order functions e and e' of type τ (see Sumii and Pierce [19], Section 4.5). Note that this example is essentially the "dual" of the example in Section D.1.

$$\begin{array}{lcl} e & = & \lambda f.\, f\,[\,]\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle \\ e' & = & \lambda f.\, f\,[\,]\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle \\ \sigma & = & \forall\alpha.\, (\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1} \\ \tau & = & \sigma \to \mathbf{1} \end{array}$$

We are required to show that $\bullet;\bullet \vdash e \sim e' : \tau$. The proof is in two parts.

I. Show $\bullet;\bullet \vdash e \leq e' : \tau$.

Consider an arbitrary $k \geq 0$.

Unwinding definitions, we see that since e and e' are closed values of closed type, it suffices to show that $(k, e, e') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset \equiv (k, \lambda f.\, f\,[\,]\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle, \lambda f.\, f\,[\,]\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\sigma \to \mathbf{1}]\!]\,\emptyset$.

Note that we already have $\vdash e' : \sigma \to \mathbf{1}$.

Consider arbitrary j, v, and v' such that

- $j < k$, and
- $(j, v, v') \in \mathcal{RV}\,[\![\sigma]\!]\,\emptyset$
  $\equiv (j, v, v') \in \mathcal{RV}\,[\![\forall\alpha.\, (\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset$.

Note that $\vdash v' : \sigma$, which follows from Lemma C.7 applied to $(j, v, v') \in \mathcal{RV}\,[\![\sigma]\!]\,\emptyset$.

Also, note that $v = \Lambda.\, e_1$ and $v' = \Lambda.\, e_1'$, which follows from $(j, v, v') \in \mathcal{RV}\,[\![\forall\alpha.\ \ldots]\!]\,\emptyset$.

We are required to show that
$(j,\ \ (f\,[\,]\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle)[v/f],\ \ (f\,[\,]\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle)[v'/f]) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset$
$\equiv (j,\ \ (v\,[\,])\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle,\ \ (v'\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset$
$\equiv (j,\ \ (\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle,\ \ (\Lambda.\, e_1'\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset$.

Consider arbitrary j_1 and e_{f_1} such that

- $j_1 < j$,
- $((\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

By the operational semantics, it follows that

$$\begin{array}{l} ((\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle) \longmapsto^{1} (e_1\,\langle 1, \lambda x.\, x \stackrel{\text{int}}{=} 0\rangle) \\ \qquad\qquad\qquad\qquad\quad \longmapsto^{j_1 - 1} e_{f_1} \end{array}$$

Hence, by the operational semantics, it follows that there must exist j_{11} and $e_{f_{11}}$ such that

- $e_1 \longmapsto^{j_{11}} e_{f_{11}}$,
- $\mathit{irred}(e_{f_{11}})$, and
- $j_{11} \leq j_1 - 1$.

Take $\tau_2 = \mathsf{bool}$ and $\chi = \{(k', 1, \mathtt{tt}) \mid \ k' \geq 0\}$.
Instantiate the second conjunct of $(j, \Lambda.\, e_1, \Lambda.\, e_1') \in \mathcal{RV}\,[\![\forall\alpha.\, (\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset$ with χ and τ_2.
Note that $\chi \in \mathit{Rel}_{\mathsf{bool}}$, which follows from the definition of χ.
Hence, we have $\forall i < j.\ (i, e_1, e_1') \in \mathcal{RC}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
Instantiate this with j_1 noting that $j_1 < j$.
Hence, we have $(j_1, e_1, e_1') \in \mathcal{RC}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
Instantiate this with j_{11} and $e_{f_{11}}$. Note that

- $j_{11} < j_1$, which follows from $j_{11} \leq j_1 - 1$,
- $e_1 \longmapsto^{j_{11}} e_{f_{11}}$, and
- $\mathit{irred}(e_{f_{11}})$.

Hence, there exists $e'_{f_{11}}$ such that

- $e_1' \longmapsto^* e'_{f_{11}}$ and
- $(j_1 - j_{11}, e_{f_{11}}, e'_{f_{11}}) \in \mathcal{RV}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.

Hence, $e_{f_{11}} = \lambda z.\, e_2$ and $e'_{f_{11}} = \lambda z.\, e_2'$.
Then, by the operational semantics it follows that

$$\begin{aligned}
((\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) &\longmapsto^1 \ (e_1\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) \\
&\longmapsto^{j_{11}} \ (e_{f_{11}}\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) \\
&\equiv \ (\lambda z.\, e_2\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) \\
&\longmapsto^1 \ (e_2[\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle / z]) \\
&\longmapsto^{j_{12}} \ e_{f_1}
\end{aligned}$$

Note that $j_1 = 1 + j_{11} + 1 + j_{12}$.
Let $v_z = \langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle$.
Let $v_z' = \langle \mathtt{tt}, \lambda x.\, \neg x\rangle$.
Instantiate $(j_1 - j_{11}, \lambda z.\, e_2, \lambda z.\, e_2') \in \mathcal{RV}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$ with $j_{12} + 1$, v_z, and v_z'. Note that

- $j_{12} + 1 < j_1 - j_{11}$, which follows from $j_{12} = j_1 - 1 - j_{11} - 1$, and
- $(j_{12} + 1, v_z, v_z') \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv \ (j_{12} + 1,\ \langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle,\ \langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$,
  which follows from
  - $\vdash \langle \mathtt{tt}, \lambda x.\, \neg x\rangle : (\alpha \times (\alpha \to \mathsf{bool}))[\mathsf{bool}/\alpha]$
    $\equiv \ \vdash \langle \mathtt{tt}, \lambda x.\, \neg x\rangle : \mathsf{bool} \times (\mathsf{bool} \to \mathsf{bool})$, which follows from the static semantics.
  - $(j_{12} + 1, 1, \mathtt{tt}) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
    $\equiv (j_{12} + 1, 1, \mathtt{tt}) \in \chi$ (by the definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
    which follows from our choice of χ.

- $(j_{12}+1, \lambda x.\, x \overset{\text{int}}{=} 0, \lambda x.\, \neg x) \in \mathcal{RV}\,[\![\alpha \to \mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which we conclude as follows:

  First, note that $\vdash \lambda x.\, \neg x : (\alpha \to \mathsf{bool})[\mathsf{bool}/\alpha] \;\equiv\; \vdash \lambda x.\, \neg x : \mathsf{bool} \to \mathsf{bool}$, which follows easily from the static semantics.

  Next, consider arbitrary i, v_1, and v_1' such that

  - $i < j_{12} + 1$, and
  - $(i, v_1, v_1') \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.

  Note that $\mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \equiv \chi$ by definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$.

  Hence, $(i, v_1, v_1') \in \chi$.

  Then, it must be that $v_1 = 1$ and $v_1' = \mathtt{tt}$, which follows from the definition of χ.

  We are required to show that

$$\begin{array}{rcl}(i, (x \overset{\text{int}}{=} 0)[v_1/x], (\neg x)[v_1'/x]) & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \\ \equiv (i, v_1 \overset{\text{int}}{=} 0, \neg v_1') & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \\ \equiv (i, 1 \overset{\text{int}}{=} 0, \neg \mathtt{tt}) & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]\end{array}$$

  Note that $(1 \overset{\text{int}}{=} 0) \longmapsto^1 \mathtt{ff}$ and $(\neg \mathtt{tt}) \longmapsto^* \mathtt{ff}$.

  Hence, it remains for us to show that $(i-1, \mathtt{ff}, \mathtt{ff}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which is immediate.

Hence, $(j_{12}+1, e_2[v_z/z], e_2'[v_z'/z]) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
Instantiate this with j_{12} and e_{f_1}. Note that

- $j_{12} < j_{12} + 1$,
- $e_2[v_z/z] \longmapsto^{j_{12}} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e_{f_1}' such that

- $e_2'[v_z'/z] \longmapsto^* e_{f_1}'$, and
- $(j_{12} + 1 - j_{12}, e_{f_1}, e_{f_1}') \in \mathcal{RV}\,[\![\mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv (1, e_{f_1}, e_{f_1}') \in \mathcal{RV}\,[\![\mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.

Hence, $e_{f_1} = \langle\,\rangle$ and $e_{f_1}' = \langle\,\rangle$.
Hence, by the operational semantics we have

$$\begin{array}{rcl}((\Lambda.\, e_1'\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) & \longmapsto^1 & (e_1'\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \\ & \longmapsto^* & (e_{f_{11}}'\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \\ & \equiv & (\lambda z.\, e_2'\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \\ & \longmapsto^1 & (e_2'[\langle \mathtt{tt}, \lambda x.\, \neg x\rangle/z]) \\ & \longmapsto^* & e_{f_1}'\end{array}$$

Take $e_{f_1}' = e_{f_1}' \equiv \langle\,\rangle$. We are required to show

- $(\Lambda.\, e_1'\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle \longmapsto^* e_{f_1}'$,
  which follows from above, and

- $(j - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\mathbf{1}]\!]\,\emptyset$,
  which follows from $e_{f_1} = e'_{f_1} = \langle\,\rangle$.

II. Show $\bullet;\bullet \vdash e' \leq e : \tau$.

The proof is analogous to that of **(I)**.

D.4 Recursive Types

We now consider an example involving contravariant recursive types, that is, recursive types with a negative occurrence. Consider the following existential packages e and e' of type τ (see Sumii and Pierce [19], Section 4.4):

$$\begin{array}{lcl} e & = & \mathtt{pack}\,(\mathtt{fold}\,\langle 0, e_1\rangle) \\ e' & = & \mathtt{pack}\,(\mathtt{fold}\,\langle 0, e_1'\rangle) \end{array}$$

$$\begin{array}{lcl} e_1 & = & \mathtt{fix}\,f(s).\,\langle \mathtt{fold}\,(\langle s+1, f\rangle), \lambda c.\,(s \stackrel{\mathrm{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\,c))\rangle \\ e_1' & = & \mathtt{fix}\,f(s).\,\langle \mathtt{fold}\,(\langle s-1, f\rangle), \lambda c.\,(s \stackrel{\mathrm{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\,c))\rangle \end{array}$$

$$\begin{array}{lcl} \tau & = & \exists\alpha.\,\sigma \\ \sigma & = & \mu\beta.\,\alpha \times (\alpha \to \varphi) \\ \varphi & = & \beta \times (\beta \to \mathsf{bool}) \end{array}$$

We are required to show that $\bullet;\bullet \vdash e \sim e' : \tau$. The proof is in two parts.

I. Show $\bullet;\bullet \vdash e \le e' : \tau$.

Consider an arbitrary $k \ge 0$.

Unwinding definitions, we see that since e and e' are closed values of closed type, it suffices to show that $(k, e, e') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset \equiv (k, \mathtt{pack}\,(\mathtt{fold}\,\langle 0, e_1\rangle), \mathtt{pack}\,(\mathtt{fold}\,\langle 0, e_1'\rangle)) \in \mathcal{RV}\,[\![\exists\alpha.\,\sigma]\!]\,\emptyset$.

Note that we already have $\vdash \mathtt{pack}\,(\mathtt{fold}\,\langle 0, e_1'\rangle) : \exists\alpha.\,\sigma$.

Take $\tau_2 = \mathsf{int}$ and $\chi = \{(k', n, -n) \mid\ k' \ge 0\ \wedge\ \vdash n : \mathsf{int}\ \wedge\ n \ge 0\}$.

Note that $\chi \in \mathit{Rel}_{\mathsf{int}}$, which follows easily from the definition of χ.

Consider an arbitrary i such that $i < j$.

We are required to show that $(i, \mathtt{fold}\,\langle 0, e_1\rangle, \mathtt{fold}\,\langle 0, e_1'\rangle) \in \mathcal{RV}\,[\![\sigma]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$.

Note that we already have $\vdash \mathtt{fold}\,\langle 0, e_1'\rangle : \sigma[\mathsf{int}/\alpha]$.

Consider arbitrary i_1 such that $i_1 < i$.

Let $\chi_\beta = \lfloor \mathcal{RV}\,[\![\sigma]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \rfloor_{i_1+1}$.

We are required to show $(i_1, \langle 0, e_1\rangle, \langle 0, e_1'\rangle) \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \varphi)]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$, which follows from

- $(i_1, 0, 0) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$
  $\equiv (i_1, 0, 0) \in \chi$ (by definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
  which follows from $(i_1, 0, -0) \in \chi$.

- $(i_1, e_1, e_1') \in \mathcal{RV}\,[\![\alpha \to \varphi]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$
  $\equiv (i_1, \mathtt{fix}\,f(s).\,\langle \mathtt{fold}\,(\langle s+1, f\rangle), \lambda c.\,(s \stackrel{\mathrm{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\,c))\rangle,$
  $\mathtt{fix}\,f(s).\,\langle \mathtt{fold}\,(\langle s-1, f\rangle), \lambda c.\,(s \stackrel{\mathrm{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\,c))\rangle)$
  $\in \mathcal{RV}\,[\![\alpha \to \varphi]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$, which we conclude as follows:
  First, note that

  $\vdash \mathtt{fix}\,f(s).\,\langle \mathtt{fold}\,(\langle s-1, f\rangle), \lambda c.\,(s \stackrel{\mathrm{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\,c))\rangle : (\alpha \to \varphi)[\mathsf{int}/\alpha][\sigma[\mathsf{int}/\alpha]/\beta]$
  $\equiv\ \vdash \mathtt{fix}\,f(s).\,\langle \mathtt{fold}\,(\langle s-1, f\rangle), \lambda c.\,(s \stackrel{\mathrm{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\,c))\rangle : \mathsf{int} \to (\sigma[\mathsf{int}/\alpha] \times (\sigma[\mathsf{int}/\alpha] \to \mathsf{bool}))$

  Next, consider arbitrary i_2, v, v' such that

  - $i_2 < i_1$,

- $(i_2, v, v') \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$
  $\equiv (i_2, v, v') \in \chi$, and

- $(i_2, e_1, e_1') \in \mathcal{RV}\,[\![\alpha \to \varphi]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$
  $\equiv (i_2, \mathtt{fix}\, f(s).\, \langle \mathtt{fold}\,(\langle s+1, f\rangle), \lambda c.\, (s \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c))\rangle,$
  $\mathtt{fix}\, f(s).\, \langle \mathtt{fold}\,(\langle s-1, f\rangle), \lambda c.\, (s \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c))\rangle)$
  $\in \mathcal{RV}\,[\![\alpha \to \varphi]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$.

Note that from $(i_2, v, v') \in \chi$, it must be that $v = -v'$, which we conclude from the definition of χ.

We are required to show $(i_2, \langle \mathtt{fold}\,(\langle v+1, e_1\rangle), \lambda c.\, (v \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c))\rangle,$
$\langle \mathtt{fold}\,(\langle v'-1, e_1'\rangle), \lambda c.\, (v' \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c))\rangle)$
$\in \mathcal{RC}\,[\![\beta \times \beta \to \mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$.

Noting that both $v+1$ and $v'-1$ reduce to values in one step, it suffices to show $(i_2 - 1, \langle \mathtt{fold}\,(\langle v+1, e_1\rangle), \lambda c.\, (v \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c))\rangle, \langle \mathtt{fold}\,(\langle v'-1, e_1'\rangle), \lambda c.\, (v' \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c))\rangle)$
$\in \mathcal{RV}\,[\![\beta \times (\beta \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$, which follows from:

- $(i_2 - 1, \mathtt{fold}\,(\langle v+1, e_1\rangle), \mathtt{fold}\,(\langle v'-1, e_1'\rangle)) \in \mathcal{RV}\,[\![\beta]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$
  $\equiv (i_2 - 1, \mathtt{fold}\,(\langle v+1, e_1\rangle), \mathtt{fold}\,(\langle v'-1, e_1'\rangle)) \in \chi_\beta$
  $\equiv (i_2 - 1, \mathtt{fold}\,(\langle v+1, e_1\rangle), \mathtt{fold}\,(\langle v'-1, e_1'\rangle)) \in \lfloor \mathcal{RV}\,[\![\sigma]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \rfloor_{i_1+1}$
  $\equiv (i_2 - 1, \mathtt{fold}\,(\langle v+1, e_1\rangle), \mathtt{fold}\,(\langle v'-1, e_1'\rangle)) \in \mathcal{RV}\,[\![\mu\beta.\, \alpha \times (\alpha \to \varphi)]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$
  which we conclude as follows:
  Consider arbitrary i_3 such that $i_3 < i_2 - 1$.
  Let $\chi_{\beta_1} = \lfloor \mathcal{RV}\,[\![\sigma]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \rfloor_{i_3+1}$. Note that $\chi_{\beta_1} = \lfloor \chi_\beta \rfloor_{i_3+1}$ since $i_3 \le i_1$.
  We are required to show that

  $$(i_3, \langle v+1, e_1\rangle, \langle v'-1, e_1'\rangle) \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \varphi)]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_{\beta_1}, \sigma[\mathsf{int}/\alpha])]$$

  which follows from:

  - $(i_3, v+1, v'-1) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_{\beta_1}, \sigma[\mathsf{int}/\alpha])]$
    $\equiv (i_3, v+1, v'-1) \in \chi$ (by definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
    which follows from $v = -v'$ (from above) and $(i_3, v+1, -v-1) \in \chi$.

  - $(i_3, e_1, e_1') \in \mathcal{RV}\,[\![\alpha \to \varphi]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_{\beta_1}, \sigma[\mathsf{int}/\alpha])]$
    which follows by Lemma C.9 applied to $i_3 \le i_2$ and
    $(i_2, e_1, e_1') \in \mathcal{RV}\,[\![\alpha \to \varphi]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$,
    both of which follow from above.

- $(i_2 - 1, \lambda c.\, (v \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c)), \lambda c.\, (v' \overset{\mathsf{int}}{=} \mathtt{fst}\,(\mathtt{unfold}\, c)))$
  $\in \mathcal{RV}\,[\![\beta \to \mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$, which we conclude as follows:
  Consider arbitrary i_3, v_1, and v_1' such that

  - $i_3 < i_2 - 1$ and

  - $(i_3, v_1, v_1') \in \mathcal{RV}\,[\![\beta]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$
    $\equiv (i_3, v_1, v_1') \in \chi_\beta$.

  From the latter and $\chi_\beta = \lfloor \mathcal{RV}\,[\![\sigma]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})] \rfloor_{i_1+1}$, it follows that $v_1 = \mathtt{fold}\, v_{11}$ and $v_1' = \mathtt{fold}\, v_{11}'$. Hence, $(i_3, \mathtt{fold}\, v_{11}, \mathtt{fold}\, v_{11}') \in \mathcal{RV}\,[\![\sigma]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$.

We are required to show that

$(i_3, (v \overset{\text{int}}{=} \texttt{fst}\,(\texttt{unfold}\,v_1)), (v' \overset{\text{int}}{=} \texttt{fst}\,(\texttt{unfold}\,v_1')))$

$\equiv (i_3, (v \overset{\text{int}}{=} \texttt{fst}\,(\texttt{unfold}\,(\texttt{fold}\,v_{11}))), (v' \overset{\text{int}}{=} \texttt{fst}\,(\texttt{unfold}\,(\texttt{fold}\,v_{11}'))))$

$\in \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$

By the operational semantics $(v \overset{\text{int}}{=} \texttt{fst}\,(\texttt{unfold}\,(\texttt{fold}\,v_{11}))) \longmapsto^1 (v \overset{\text{int}}{=} \texttt{fst}\,(v_{11}))$ and $(v' \overset{\text{int}}{=} \texttt{fst}\,(\texttt{unfold}\,(\texttt{fold}\,v_{11}'))) \longmapsto^1 (v' \overset{\text{int}}{=} \texttt{fst}\,(v_{11}'))$.

Instantiating $(i_3, \texttt{fold}\,v_{11}, \texttt{fold}\,v_{11}') \in \mathcal{RV}\,[\![\mu\beta.\,\alpha \times (\alpha \to \varphi)]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int})]$ with $i_3 - 1 < i_3$ it follows that $(i_3 - 1, v_{11}, v_{11}') \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \varphi)]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$.

Hence, it must be that $\texttt{fst}\,(v_{11}) = v_2$ and $\texttt{fst}\,(v_{11}') = v_2'$ such that $v_2 = -v_2'$ which follows from $(i_3 - 1, v_2, v_2') \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{int}), \beta \mapsto (\chi_\beta, \sigma[\mathsf{int}/\alpha])]$ which is equivalent to $(i_3 - 1, v_2, v_2') \in \chi$.

Thus, since $v = -v'$ and $v_2 = -v_2'$, it easily follows that $(v \overset{\text{int}}{=} v_2)$ and $(v' \overset{\text{int}}{=} v_2')$ either both evaluate to `tt` or both evaluate to `ff`.

II. Show $\bullet; \bullet \vdash e' \leq e : \tau$.

The proof is analogous to that of **(I)**.

D.5 Higher-Order Functions II

We now consider a more complicated example involving higher-order functions. The packages e and e' of type τ shown below are implementations of integer multisets with higher-order functions that compute the weighed sum of all the elements. To prove contextual equivalence of e and e' below, Sumii and Pierce (see [19], Section 7) had to adopt a weaker and much more complicated condition for showing the validity of the bisimulation than the intuitive one they proposed initially. In fact, they note that their weaker condition is reminiscent of step-indexed models.

$$
\begin{array}{lcl}
e & = & \mathtt{pack}\,\langle \mathit{nil}, \mathit{add}, \mathit{weigh}\rangle \\
e' & = & \mathtt{pack}\,\langle \mathit{lf}, \mathit{add}', \mathit{weigh}'\rangle \\
\sigma & = & \alpha \times (\mathsf{int} \to \alpha \to \alpha) \times ((\mathsf{int} \to \mathsf{real}) \to \alpha \to \mathsf{real}) \\
\tau & = & \exists\alpha.\,\sigma \\
 & & \\
\mathit{add} & = & \lambda i.\,\mathtt{fix}\,f(s).\,\mathit{cons}(i,s) \\
\mathit{add}' & = & \lambda i.\,\mathtt{fix}\,f(s).\,\mathtt{case}\,s\,\mathtt{of}\,\mathit{lf} \Rightarrow \mathit{node}(i,\mathit{lf},\mathit{lf}) \\
 & & \quad \| \; \mathit{node}(j,s_1,s_2) \Rightarrow \mathtt{if}\; i<j, \mathit{node}(j, f\,s_1, s_2), \mathit{node}(j, s_1, f\,s_2) \\
 & & \\
\mathit{weigh} & = & \lambda g.\,\mathtt{fix}\,f(s).\,\mathtt{case}\,s\,\mathtt{of}\,\mathit{nil} \Rightarrow 0 \\
 & & \quad \| \; \mathit{cons}(j,s_0) \Rightarrow g\,j + f\,s_0 \\
\mathit{weigh}' & = & \lambda g.\,\mathtt{fix}\,f(s).\,\mathtt{case}\,s\,\mathtt{of}\,\mathit{lf} \Rightarrow 0 \\
 & & \quad \| \; \mathit{node}(j,s_1,s_2) \Rightarrow g\,j + f\,s_1 + f\,s_2
\end{array}
$$

We are required to show that $\bullet;\bullet \vdash e \sim e' : \tau$. The proof is in two parts.

I. Show $\bullet;\bullet \vdash e \le e' : \tau$.

Consider an arbitrary $k \ge 0$.

Unwinding definitions, we see that since e and e' are closed values of closed types, it suffices to show that $(k, e, e') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset \equiv (k, \mathtt{pack}\,\langle \mathit{nil}, \mathit{add}, \mathit{weigh}\rangle, \mathtt{pack}\,\langle \mathit{lf}, \mathit{add}', \mathit{weigh}'\rangle) \in \mathcal{RV}\,[\![\exists\alpha.\,\sigma]\!]\,\emptyset$.

Note that we already have $\vdash \mathtt{pack}\,\langle \mathit{lf}, \mathit{add}', \mathit{weigh}'\rangle : \exists\alpha.\,\sigma$.

Let $\chi_0 = \{(k', \mathit{nil}, \mathit{lf}) \mid \; k' \ge 0 \;\wedge\; \vdash \mathit{lf} : \mathsf{intTree}\}$, and
$\chi_{i+1} = \{(k', s, s') \mid \; \exists (k', s_i, s_i') \in \chi_i.\; \exists n.\; \vdash n : \mathsf{int} \;\wedge\; \mathit{add}(n, s_i) \longmapsto^* s \;\wedge\; \mathit{add}'(n, s_i') \longmapsto^* s'\}$.

Take $\tau_2 = \mathsf{intTree}$ and $\chi = \bigcup_{i \ge 0} \chi_i$.

Note that $\chi \in \mathit{Rel}_{\mathsf{intTree}}$, which follows from the definition of χ_i and $\chi = \bigcup_{i \ge 0} \chi_i$.

Consider an arbitrary k_0 such that $k_0 < k$.

We are required to show that $(k_0, \langle \mathit{nil}, \mathit{add}, \mathit{weigh}\rangle, \langle \mathit{lf}, \mathit{add}', \mathit{weigh}'\rangle) \in \mathcal{RV}\,[\![\sigma]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$, which follows from:

- $(k_0, \mathit{nil}, \mathit{lf}) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$
  $\equiv (k_0, \mathit{nil}, \mathit{leaf}) \in \chi$ (by definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
  which follows from $(k_0, \mathit{nil}, \mathit{lf}) \in \chi_0$ and $\chi_0 \subseteq \chi$.

- $(k_0, \mathit{add}, \mathit{add}') \in \mathcal{RV}\,[\![\mathsf{int} \to \alpha \to \alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$, which we conclude as follows:
  Consider arbitrary k_1, v, and v' such that

  - $k_1 < k_0$ and
  - $(k_1, v, v') \in \mathcal{RV}\,[\![\mathsf{int}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Note that from the latter it follows that $v = v'$.

Let $add_1 = \texttt{fix}\, f(s).\, cons(v, s)$, and
$add'_1 = \texttt{fix}\, f(s).\, \texttt{case}\, s\, \texttt{of}\, lf \Rightarrow node(v', lf, lf)$
$\quad \parallel node(j, s_1, s_2) \Rightarrow \texttt{if}\, v' < j, node(j, f\, s_1, s_2), node(j, s_1, f\, s_2)$.

We are required to show that $(k_1, add_1, add'_1) \in \mathcal{RC}\, [\![\alpha \to \alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Note that since add_1 and add'_1 are closed values, it suffices to show that $(k_1, add_1, add'_1) \in \mathcal{RV}\, [\![\alpha \to \alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Consider arbitrary k_2, s, and s' such that

- $k_2 < k_1$,
- $(k_2, s, s') \in \mathcal{RV}\, [\![\alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$
  $\equiv (k_2, s, s') \in \chi$, and
- $(k_2, add_1, add'_1) \in \mathcal{RV}\, [\![\alpha \to \alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

We are required to show that
$(k_2, cons(v, s),$
$\quad \texttt{case}\, s'\, \texttt{of}\, lf \Rightarrow node(v', lf, lf)$
$\qquad \parallel node(j, s_1, s_2) \Rightarrow \texttt{if}\, v' < j, node(j, add'_1\, s_1, s_2), node(j, s_1, add'_1\, s_2))$
$\in \mathcal{RC}\, [\![\alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$,
which is equivalent to showing
$(k_2 + 2, add(v, s), add'(v', s')) \in \mathcal{RC}\, [\![\alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Note that from $(k_2, s, s') \in \chi$, it follows that there exists some i such that $(k_2, s, s') \in \chi_i \subset \chi$.

- If $i = 0$, then from $(k_2, s, s') \in \chi_i$ it follows that $s = nil$ and $s' = lf$.

  By the operational semantics, $add(v, s) \longmapsto^2 s_f \equiv cons(v, s)$ and $add'(v', s') \longmapsto^* s'_f \equiv node(v', lf, lf)$.

  Note that since $v = v'$, it follows that $(k_2, s_f, s'_f) \in \chi_1$.

  Thus, it remains to show that $(k_2, s_f, s'_f) \in \mathcal{RV}\, [\![\alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})] \equiv \chi$, which is immediate from the fact that $(k_2, s_f, s'_f) \in \chi_1 \subset \chi$.

- Else if $i > 0$, then from $(k_2, s, s') \in \chi_i$ it follows that $s = cons(n, s_0)$ and $s' = node(m, s_1, s_2)$.

  By the operational semantics, $add(v, s) \longmapsto^2 s_f$ and $add'(v', s') \longmapsto^* s'_f$.

  Note that since $v = v'$, it follows that $(k_2, s_f, s'_f) \in \chi_{i+1}$.

  Thus, it remains to show that $(k_2, s_f, s'_f) \in \mathcal{RV}\, [\![\alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})] \equiv \chi$, which is immediate fom the fact that $(k_2, s_f, s'_f) \in \chi_{i+1} \subset \chi$.

- $(k_0, weigh, weigh') \in \mathcal{RV}\, [\![((\mathsf{int} \to \mathsf{real}) \to \alpha \to \mathsf{real})]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$, which we conclude as follows:

  Consider arbitrary k_1, g, and g' such that

  - $k_1 < k_0$ and
  - $(k_1, g, g') \in \mathcal{RV}\, [\![\mathsf{int} \to \mathsf{real}]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Let $weigh_1 = \texttt{fix}\, f(s).\, \texttt{case}\, s\, \texttt{of}\, nil \Rightarrow 0$
$\quad \| \; cons(j, s_0) \Rightarrow g\, j + f\, s_0$, and
$weigh'_1 = \texttt{fix}\, f(s).\, \texttt{case}\, s\, \texttt{of}\, lf \Rightarrow 0$
$\quad \| \; node(j, s_1, s_2) \Rightarrow g'\, j + f\, s_1 + f\, s_2$.

We are required to show that $(k_1, weigh_1, weigh'_1) \in \mathcal{RC}\, [\![\alpha \to \mathsf{real}]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Note that since $weigh_1$ and $weigh'_1$ are closed values, it suffices to show $(k_1, weigh_1, weigh'_1) \in \mathcal{RV}\, [\![\alpha \to \mathsf{real}]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Consider arbitrary k_2, s, and s' such that

- $k_2 < k_1$,
- $(k_2, s, s') \in \mathcal{RV}\, [\![\alpha]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$
  $\equiv (k_2, s, s') \in \chi$, and
- $(k_2, weigh_1, weigh'_1) \in \mathcal{RV}\, [\![\alpha \to \mathsf{real}]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

We are required to show that
$(k_2, \texttt{case}\, s\, \texttt{of}\, nil \Rightarrow 0$
$\quad \| \; cons(j, s_0) \Rightarrow g\, j + weigh_1\, s_0,$
$\quad \texttt{case}\, s'\, \texttt{of}\, lf \Rightarrow 0$
$\quad \| \; node(j, s_1, s_2) \Rightarrow g'\, j + weigh'_1\, s_1 + weigh'_1\, s_2)$
$\in \mathcal{RC}\, [\![\mathsf{real}]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Let $e \equiv \texttt{case}\, s\, \texttt{of}\, nil \Rightarrow 0 \; \| \; cons(j, s_0) \Rightarrow g\, j + weigh_1\, s_0$.

Let $e' \equiv \texttt{case}\, s'\, \texttt{of}\, lf \Rightarrow 0 \; \| \; node(j, s_1, s_2) \Rightarrow g'\, j + weigh'_1\, s_1 + weigh'_1\, s_2)$.

Consider arbitrary k_3 and v_f such that

- $k_3 < k_2$,
- $e \longmapsto^{k_3} v_f$, and
- $irred(v_f)$.

It remains to show that there exists v'_f such that $e' \longmapsto^* v'_f$ and $(k_2 - k_3, v_f, v'_f) \in \mathcal{RV}\, [\![\mathsf{real}]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Note that from $(k_2, s, s') \in \chi$, it follows that there exists some i such that $(k_2, s, s') \in \chi_i \subset \chi$.

- If $i = 0$, then from $(k_2, s, s') \in \chi_i$ it follows that $s = nil$ and $s' = lf$.
  Then, by the operational semantics, $e \longmapsto^1 0$. That is, $v_f = 0$ and $k_3 = 1$.
  Furthermore, by the operational semantics, there exists $v'_f = 0$ such that $e' \longmapsto^* v'_f$.
  It remains to show that $(k_2 - 1, 0, 0) \in \mathcal{RV}\, [\![\mathsf{real}]\!]\, \emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$ which is immediate from the definition of $\mathcal{RV}\, [\![\mathsf{real}]\!]$.
- Else if $i > 0$, then from $(k_2, s, s') \in \chi_i$ it follows that:
  - $s = cons(n, s_0)$, where $add(n, s_0) \longmapsto^* cons(n, s_0)$,
  - $s' = node(\ldots)$, where there exists some s'_0 such that $add'(n, s'_0) \longmapsto^* s'$,
  - $(k_2, s_0, s'_0) \in \chi_{i-1} \subset \chi$.

Then, by the operational semantics, $e \longmapsto^1 (g\, n + weigh_1\, s_0) \longmapsto^{k_3 - 1} v_f$.

Suppose that $s'_0 \equiv node(m, s'_{10}, s'_{20})$.

Then, either $n < m$ and $add'(n, s'_0) \equiv add'(n, node(m, s'_{10}, s'_{20}) \longmapsto node(m, add(n, s'_{10}), s'_{20}) \longmapsto^* s'$

or else, $add'(n, s'_0) \equiv add'(n, node(m, s'_{10}, s'_{20}) \longmapsto node(m, s'_{10}, add(n, s'_{20})) \longmapsto^* s'$.

Then, by the operational semantics,

- either there exists v'_{f1} such that $e' \longmapsto^1 (g'\, m + weigh'_1\, ns'_{10} + weigh'_1\, s'_{20}) \longmapsto v'_{f1}$, where $(add(n, s'_{10})) \longmapsto^* ns'_{10}$
- or there exists some v'_{f2} such that $e' \longmapsto^1 (g'\, m + weigh'_1\, s'_{10} + weigh'_1\, ns'_{20}) \longmapsto v'_{f2}$, where $(add(n, s'_{20})) \longmapsto^* ns'_{20}$.

Consider the expression $(g'\, m + weigh'_1\, s'_{10} + weigh'_1\, s'_{20} + g'\, n)$, which evaluates to some v'_f.

Note that it must be that $v'_f \equiv v'_{f1} \equiv v'_{f2}$.

Thus, it remains for us to show that $(k_2 - k_3, v_f, v'_f) \in \mathcal{RV}\,[\![\mathsf{real}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$.

Furthermore note that the expression $(weigh'_1\, s'_0 + g'\, n) \equiv (weigh'_1\, (node(m, s'_{10}, s'_{20})) + g'\, n) \longmapsto^1 (g'\, m + weigh'_1\, s'_{10} + weigh'_1\, s'_{20} + g'\, n)$ and therefore, this must also evaluate to v'_f.

Finally, note that the expressions $(g\, n + weigh_1\, s_0)$ and $(g'\, n + weigh'_1\, s'_0)$ both evaluate to the same value — that is $v_f \equiv v'_f$, which we conclude as follows:

- From $(k_1, g, g') \in \mathcal{RV}\,[\![\mathsf{int} \to \mathsf{real}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$ and $(k_1, n, n) \in \mathcal{RV}\,[\![\mathsf{int}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$ (which is immediate from the definition of $\mathcal{RV}\,[\![\mathsf{int}]\!]$), with appropriate applications of Lemma C.9, it follows that $g\, n$ and $g'\, n$ both evaluate to the same value.
- From $(k_2, weigh_1, weigh'_1) \in \mathcal{RV}\,[\![\alpha \to \mathsf{real}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$ and $(k_2, s_0, s'_0) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})] \equiv \chi$, with appropriate applications of Lemma C.9, it follows that $weigh_1\, s_0$ and $weigh'_1\, s'_0$ both evaluate to the same value.

From $v_f \equiv v'_f$, it immediately follows that $(k_2 - k_3, v_f, v'_f) \in \mathcal{RV}\,[\![\mathsf{real}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{intTree})]$ as we needed to show.

II. Show $\bullet; \bullet \vdash e' \leq e : \tau$.

The proof is analogous to that of **(I)**.

E Completeness and Quantified Types

In this section, we consider completeness of the logical relation for quantified types. As explained in Section 3.4, the proof of completeness fails to go through for the logical relation in Appendix C. In order to obtain a complete logical relation, we modify the logical relation from Appendix C so that the definition of Rel_τ requires that each $\chi \in Rel_\tau$ also be *equivalence-respecting*. Except for the definition of Rel_τ, the logical relation is defined exactly as before.

It turns out, however, that our relational interpretation of existential types fails to satisfy the equivalence-respecting property. Thus, in this section we show that our modified logical relation is sound and complete for a language with recursive and quantified types, but no existential types.

Notation: $\lambda^\forall$ refers to the $\lambda^{\forall\exists}$-calculus minus all terms, typing rules, etc. that have to do with existential types.

Note: Some lemmas in this section hold for $\lambda^{\forall\exists}$, while others only hold for the sub-language $\lambda^\forall$. The lemmas are annotated accordingly.

E.1 $\lambda^{\forall}$ Relational (PER) Model

$$v \prec^{ciu} v' : \tau \quad \stackrel{\text{def}}{=} \quad \forall E, \tau_1.\ \bullet;\bullet \vdash E : (\bullet;\bullet \triangleright \tau) \rightsquigarrow \tau_1 \ \wedge\ E[v] \Downarrow \implies E[v'] \Downarrow$$

$$\begin{aligned} Rel_\tau \quad \stackrel{\text{def}}{=} \quad \{\chi \in 2^{Nat \times CValues \times CValues} \mid\ & \forall (j, v, v') \in \chi. \\ & \vdash v' : \tau \ \wedge \\ & \forall i \leq j.\ (i, v, v') \in \chi \ \wedge \\ & \forall v''.\ v' \prec^{ciu} v'' : \tau \implies (j, v, v'') \in \chi\} \end{aligned}$$

The rest of the model is defined exactly as in Figures 6 and 7 in Appendix C.

Figure 1: $\lambda^{\forall}$ Step-Indexed Relational Model (Complete)

E.2 $\lambda^{\forall}$ Proofs: Validity of Pers

The goal of this section, is to show that each $\lambda^{\forall}$ type τ is a valid type — that is, $\mathcal{RV}[\![\tau]\!]\,\rho \in Rel_{\tau[\rho]}$. Specifically, this involves showing that the relational interpretation of a type τ satisfies the well-typedness requirement, is closed under decreasing step-index, and is *equivalence-respecting*.

Note on Existential Types: It is important to note that *for existential types, the equivalence-respecting property does not hold* (see the proof of Lemma E.1, where we have included the case for existential types in order to show how the proof for existential types breaks down).

Consequences of Existential Types not being Equivalence-Respecting: It is important to note that the equivalence-respecting property of a type is *not* required in order to prove the Fundamental Property of the logical relation (thus we can reuse all lemmas in Section C.8) or to prove soundness with respect to contextual equivalence (thus we can reuse all lemmas in Section C.10). In fact, the equivalence-respecting property is required only in the proof of *completeness* of the logical relation with respect to contextual equivalence (see Lemma E.5 in Section E.3). Thus, since the relational interpretation of existential types is not equivalence-respecting, the logical relation in Section E.1 is not complete with respect to contextual equivalence for existential types. However, if we omit existential types from the language (as we have done by restricting attention to $\lambda^{\forall}$), the logical relation in Section E.1 is both sound and complete with respect to contextual equivalence.

Note on Lemmas and Proofs that Follow: In the rest of Appendix E we will only present lemmas and proofs that are new or different from those in Appendix C. In particular, we note that to prove the fundamental theorem for $\lambda^{\forall}$ and to show soundness of our new logical relation for $\lambda^{\forall}$, we may reuse all of the proofs in Sections C.7 through C.10 without any modifications (other than leaving out lemmas and cases that pertain to existential types). Accordingly, in the proofs that appear in the rest of this section, we have continued to appeal to lemmas from Appendix C where necessary.

Lemma E.1 ($\lambda^\forall$ Per Equivalence-Respecting)

Let $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ *and* $\Delta \vdash \tau$.
If $(k, v_1, v_2) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$ *and* $v_2 \prec^{ciu} v_3 : \tau^{[\rho]}$,
then $(k, v_1, v_3) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

Proof

NOTE: This proof does not go through for existential types.

By induction on k and nested induction on the structure of the derivation $\Delta \vdash \tau$.

Case $(\mathsf{VarTy})\ \dfrac{\alpha \in \Delta}{\Delta \vdash \alpha}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\alpha]\!]\,\rho \ \equiv\ (k, v_1, v_2) \in \rho^{\mathsf{sem}}(\alpha)$, and
(2) $v_2 \prec^{ciu} v_3 : \alpha^{[\rho]} \ \equiv\ v_2 \prec^{ciu} v_3 : \rho^{\mathsf{syn}}(\alpha)$.

We are required to show that $(k, v_1, v_3) \in \mathcal{RV}\,[\![\alpha]\!]\,\rho$
$\equiv (k, v_1, v_3) \in \rho^{\mathsf{sem}}(\alpha)$.

From $\rho \in \mathcal{RD}\,[\![\Delta]\!]$ and $\alpha \in \Delta$, it follows that

- $\rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$.

Hence, by the definition of $\mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$, since $(k, v_1, v_2) \in \rho^{\mathsf{sem}}(\alpha) \in \mathit{Rel}_{\rho^{\mathsf{syn}}(\alpha)}$ and $v_2 \prec^{ciu} v_3 : \rho^{\mathsf{syn}}(\alpha)$, it follows that $(k, v_1, v_3) \in \rho^{\mathsf{sem}}(\alpha)$.

Case $(\mathsf{BoolTy})\ \dfrac{}{\Delta \vdash \mathsf{bool}}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$, and
(2) $v_2 \prec^{ciu} v_3 : \mathsf{bool}^{[\rho]} \ \equiv\ v_2 \prec^{ciu} v_3 : \mathsf{bool}$.

Hence, from **(1)** it follows that $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$.
From **(2)** it follows that $\vdash v_3 : \mathsf{bool}$.
Hence, either $v_3 = \mathtt{tt}$ or $v_3 = \mathtt{ff}$.
We show that $v_2 = v_3$ by contradiction:

- Suppose $v_2 \neq v_3$. Then, either $v_2 = \mathtt{tt} \ \wedge\ v_3 = \mathtt{ff}$, or $v_2 = \mathtt{ff} \ \wedge\ v_3 = \mathtt{tt}$.

  Case $v_2 = \mathtt{tt} \ \wedge\ v_3 = \mathtt{ff}$:
  Instantiate **(2)** with $\mathtt{if}\,[\cdot], \mathtt{tt}, \mathtt{diverge}$ and bool. Note that
  - $\bullet; \bullet \vdash \mathtt{if}\,[\cdot], \mathtt{tt}, \mathtt{diverge} : (\bullet; \bullet \triangleright \mathsf{bool}) \rightsquigarrow \mathsf{bool}$, and
  - $\mathtt{if}\,[v_2], \mathtt{tt}, \mathtt{diverge} \Downarrow$, since $v_2 = \mathtt{tt}$.

  Hence, $\mathtt{if}\,v_3, \mathtt{tt}, \mathtt{diverge} \Downarrow \ \equiv\ \mathtt{if}\,\mathtt{ff}, \mathtt{tt}, \mathtt{diverge} \Downarrow$, since $v_3 = \mathtt{ff}$.
  But clearly, $\mathtt{if}\,\mathtt{ff}, \mathtt{tt}, \mathtt{diverge} \longmapsto \mathtt{diverge}$ and $\mathtt{diverge} \Uparrow$. Hence, we have a contradiction.

  Case $v_2 = \mathtt{ff} \ \wedge\ v_3 = \mathtt{tt}$:
  Instantiate **(2)** with $\mathtt{if}\,[\cdot], \mathtt{diverge}, \mathtt{tt}$ and bool. Note that
  - $\bullet; \bullet \vdash \mathtt{if}\,[\cdot], \mathtt{diverge}, \mathtt{tt} : (\bullet; \bullet \triangleright \mathsf{bool}) \rightsquigarrow \mathsf{bool}$, and
  - $\mathtt{if}\,[v_2], \mathtt{diverge}, \mathtt{tt} \Downarrow$, since $v_2 = \mathtt{ff}$.

  Hence, $\mathtt{if}\,v_3, \mathtt{diverge}, \mathtt{tt} \Downarrow \ \equiv\ \mathtt{if}\,\mathtt{tt}, \mathtt{diverge}, \mathtt{tt} \Downarrow$, since $v_3 = \mathtt{tt}$.
  But clearly, $\mathtt{if}\,\mathtt{tt}, \mathtt{diverge}, \mathtt{tt} \longmapsto \mathtt{diverge}$ and $\mathtt{diverge} \Uparrow$. Hence, we have a contradiction.

Thus, it must be that $v_2 = v_3$.

We are required to show that $(k, v_1, v_3) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\rho$,
which follows from

- $\vdash v_3 : \mathsf{bool}$,
  which follows from $v_2 \prec^{ciu} v_3 : \mathsf{bool}$.
- $(v_1 = v_3 = \mathtt{tt}) \vee (v_1 = v_3 = \mathtt{ff})$,
  which follows from $(v_1 = v_2 = v_3 = \mathtt{tt}) \vee (v_1 = v_2 = v_3 = \mathtt{ff})$,
  which follows from
  - $(v_1 = v_2 = \mathtt{tt}) \vee (v_1 = v_2 = \mathtt{ff})$, and
  - $(v_2 = v_3 = \mathtt{tt}) \vee (v_2 = v_3 = \mathtt{ff})$.

Case $(\mathsf{FnTy})\ \dfrac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 \to \tau_2}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$, and
(2) $v_2 \prec^{ciu} v_3 : (\tau_1 \to \tau_2)^{[\rho]} \;\equiv\; v_2 \prec^{ciu} v_3 : (\tau_1)^{[\rho]} \to (\tau_2)^{[\rho]}$.

Hence, from **(1)** it follows that $v_1 \equiv \lambda x.\, e_1$ and $v_2 \equiv \lambda x.\, e_2$.
From **(2)** it follows that $\vdash v_3 : (\tau_1)^{[\rho]} \to (\tau_2)^{[\rho]}$. Hence, $v_3 \equiv \lambda x.\, e_3$.
We are required to show that $(k, \lambda x.\, e_1, \lambda x.\, e_3) \in \mathcal{RV}\,[\![\tau_1 \to \tau_2]\!]\,\rho$,
which follows from

- $\vdash \lambda x.\, e_3 : (\tau_1 \to \tau_2)^{[\rho]}$,
  which follows from **(2)**.
- $\forall j < k, v_{11}, v'_{11}.\ (j, v_{11}, v'_{11}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho \implies (j, e_1[v_{11}/x], e_3[v'_{11}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$:
  Consider arbitrary j, v_{11}, v'_{11} such that
  - $j < k$, and
  - $(j, v_{11}, v'_{11}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

  We are required to show that $(j, e_1[v_{11}/x], e_3[v'_{11}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.
  Consider arbitrary i and $e_{f_{11}}$ such that
  - $i < j$,
  - $e_1[v_{11}/x] \longmapsto^i e_{f_{11}}$, and
  - $\mathit{irred}(e_{f_{11}})$.

  We are required to show that $\exists e'_f.\ e_3[v'_{11}/x] \longmapsto^* e'_f \ \wedge\ (j - i, e_{f_{11}}, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$.
  Instantiate the second conjunct of **(1)** with j, v_{11}, and v'_{11}. Note that
  - $j < k$, and
  - $(j, v_{11}, v'_{11}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho$.

  Hence, $(j, e_1[v_{11}/x], e_2[v'_{11}/x]) \in \mathcal{RC}\,[\![\tau_2]\!]\,\rho$.
  Instantiate this with i and $e_{f_{11}}$. Note that
  - $i < j$,
  - $e_1[v_{11}/x] \longmapsto^i e_{f_{11}}$, and
  - $\mathit{irred}(e_{f_{11}})$.

  Hence, there exists $e_{f_{22}}$ such that

- $e_2[v'_{11}/x] \longmapsto^* e_{f_{22}}$, and
- $(j-i, e_{f_{11}}, e_{f_{22}}) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$.

Hence, $e_{f_{11}} \equiv v_{f_{11}}$ and $e_{f_{22}} \equiv v_{f_{22}}$.
Instantiate **(2)** with $[\cdot]\,v'_{11}$, and τ_2. Note that

- $\bullet;\bullet \vdash [\cdot]\,v'_{11} : (\bullet;\bullet \triangleright (\tau_1)^{[\rho]} \to (\tau_2)^{[\rho]}) \rightsquigarrow (\tau_2)^{[\rho]}$, and
- $(\lambda x.\, e_2)\,v'_{11} \Downarrow$,
  which follows from $(\lambda x.\, e_2)\,v'_{11} \longmapsto^1 e_2[v'_{11}/x]$ and $e_2[v'_{11}/x] \longmapsto^* v_{f_{22}}$,
  which follow from above.

Hence, there exists $v_{f_{33}}$ such that $(\lambda x.\, e_3)\,v'_{11} \Downarrow v_{f_{33}}$.
By the operational semantics, it must be that $(\lambda x.\, e_3)\,v'_{11} \longmapsto^1 e_3[v'_{11}/x]$.
Hence, it must be that $e_3[v'_{11}/x] \Downarrow v_{f_{33}}$.
We show that $v_{f_{22}} \prec^{ciu} v_{f_{33}} : (\tau_2)^{[\rho]}$:

- Consider arbitrary E_0 and τ_0 such that
  - $\bullet;\bullet \vdash E_0 : (\bullet;\bullet \triangleright (\tau_2)^{[\rho]}) \rightsquigarrow \tau_0$, and
  - $E_0[v_{f_{22}}] \Downarrow$.

  We are required to show that $E_0[v_{f_{33}}] \Downarrow$.
  Instantiate **(2)** with $E_0[[\cdot]\,v'_{11}]$ and τ_0. Note that
  - $\bullet;\bullet \vdash E_0[[\cdot]\,v'_{11}] : (\bullet;\bullet \triangleright (\tau_1)^{[\rho]} \to (\tau_2)^{[\rho]}) \rightsquigarrow \tau_0$, and
  - $E_0[[\lambda x.\, e_2]\,v'_{11}] \longmapsto^1 E_0[e_2[v'_{11}/x]] \longmapsto^* E_0[v_{f_{22}}] \Downarrow$.

  Hence, $E_0[[\lambda x.\, e_3]\,v'_{11}] \Downarrow$.
  By the operational semantics, it must be that $E_0[[\lambda x.\, e_3]\,v'_{11}] \longmapsto^1 E_0[e_3[v'_{11}/x]] \longmapsto^* E_0[v_{f_{33}}]$.
  Hence, it must be that $E_0[v_{f_{33}}] \Downarrow$.

Take $e'_f = v_{f_{33}}$.
We are required to show

- $e_3[v'_{11}/x] \longmapsto^* v_{f_{33}}$,
  which follows from above, and
- $(j-i, e_{f_{11}}, e'_f) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$,
  which follows from the induction hypothesis applied to $\Delta \vdash \tau_2$, with
  - $\rho \in \Delta$,
  - $(j-i, v_{f_{11}}, v_{f_{22}}) \in \mathcal{RV}\,[\![\tau_2]\!]\,\rho$, and
  - $v_{f_{22}} \prec^{ciu} v_{f_{33}} : (\tau_2)^{[\rho]}$.

Case (RecTy) $\dfrac{\Delta, \alpha \vdash \tau_1}{\Delta \vdash \mu\alpha.\, \tau_1}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\rho$, and
(2) $v_2 \prec^{ciu} v_3 : (\mu\alpha.\, \tau_1)^{[\rho]} \;\equiv\; v_2 \prec^{ciu} v_3 : \mu\alpha.\, (\tau_1)^{[\rho]}$.

Hence, from **(1)** it follows that $v_1 \equiv \mathtt{fold}\, v_{11}$ and $v_2 \equiv \mathtt{fold}\, v_{22}$.
From **(2)** it follows that $\vdash v_3 : \mu\alpha.\, (\tau_1)^{[\rho]}$. Hence, $v_3 \equiv \mathtt{fold}\, v_{33}$.
We are required to show that $(k, \mathtt{fold}\, v_{11}, \mathtt{fold}\, v_{33}) \in \mathcal{RV}\,[\![\mu\alpha.\, \tau_1]\!]\,\rho$,
which follows from

- $\vdash \texttt{fold}\, v_{33} : (\mu\alpha.\, \tau_1)^{[\rho]}$,
  which follows from **(2)**.
- $\forall j < k.$ let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho \rfloor_{j+1}$ in $(j, v_{11}, v_{33}) \in \mathcal{RV}\, [\![\tau_1]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\rho]})]$:
  Consider arbitrary j such that

  - $j < k$.

  Let $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho \rfloor_{j+1}$.
  We are required to show that $(j, v_{11}, v_{33}) \in \mathcal{RV}\, [\![\tau_1]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\rho]})]$.
  Instantiate the second conjunct of **(1)** with j. Note that

  - $j < k$, and
  - $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho \rfloor_{j+1}$.

  Hence, $(j, v_{11}, v_{22}) \in \mathcal{RV}\, [\![\tau_1]\!]\, \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\rho]})]$.
  Let $\rho_1 = \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\rho]})]$. Note that $(\tau_1[\mu\alpha.\, \tau_1/\alpha])^{[\rho]} \;\equiv\; (\tau_1)^{[\rho_1]}$.
  We show that $v_{22} \prec^{ciu} v_{33} : (\tau_1)^{[\rho_1]}$
  $\equiv v_{22} \prec^{ciu} v_{33} : (\tau_1[\mu\alpha.\, \tau_1/\alpha])^{[\rho]}$:

  - Consider arbitrary E_0 and τ_0 such that

    - $\bullet; \bullet \vdash E_0 : (\bullet; \bullet \triangleright (\tau_1[\mu\alpha.\, \tau_1/\alpha])^{[\rho]}) \rightsquigarrow \tau_0$, and
    - $E_0[v_{22}] \Downarrow$.

    We are required to show that $E_0[v_{33}] \Downarrow$.
    Instantiate **(2)** with $E_0[\texttt{unfold}\, [\cdot]]$ and τ_0. Note that

    - $\bullet; \bullet \vdash E_0[\texttt{unfold}\, [\cdot]] : (\bullet; \bullet \triangleright (\mu\alpha.\, \tau_1)^{[\rho]}) \rightsquigarrow \tau_0$, and
    - $E_0[\texttt{unfold}\, [\texttt{fold}\, v_{22}]] \longmapsto^1 E_0[v_{22}] \Downarrow$.

    Hence, $E_0[\texttt{unfold}\, [\texttt{fold}\, v_{33}]] \Downarrow$.
    By the operational semantics, it must be that $E_0[\texttt{unfold}\, [\texttt{fold}\, v_{33}]] \longmapsto^1 E_0[v_{33}]$.
    Hence, it must be that $E_0[v_{33}] \Downarrow$.

  Applying the induction hypothesis to $\Delta, \alpha \vdash \tau_1$, with

  - $\rho_1 \in \mathcal{RD}\, [\![\Delta, \alpha]\!]$,
    which follows (since $\rho_1 = \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\rho]})]$) from

    - $\rho \in \mathcal{RD}\, [\![\Delta]\!]$, and
    - $\chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho \rfloor_{j+1} \in \mathit{Rel}_{(\mu\alpha.\, \tau_1)^{[\rho]}}$, which follows from:
      Consider arbitrary $(i, v_0, v_0') \in \chi = \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho \rfloor_{j+1}$.
      Note that we have the three required properties:

      - *well-typedness:* we have $\vdash v_0' : (\mu\alpha.\, \tau_1)^{[\rho]}$,
        which follows fom Lemma C.7 applied to $\rho \in \mathcal{RD}\, [\![\Delta]\!]$, $\Delta \vdash \mu\alpha.\, \tau_1$, and $(i, v_0, v_0') \in \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho$;
      - *closure with respect to decreasing step-index:*
        we have $(i', v_0, v_0') \in \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho \rfloor_{j+1}$ for arbitrary $i' \leq i$,
        which follows from Lemma C.9 applied to $\rho \in \mathcal{RD}\, [\![\Delta]\!]$, $\Delta \vdash \mu\alpha.\, \tau_1$, $(i, v_0, v_0') \in \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho$ and $i' \leq i$;
      - *equivalence-respecting:* we have $(i, v_0, v_0'') \in \lfloor \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho \rfloor_{j+1}$ for arbitrary v_0'' such that $v_0' \prec^{ciu} v_0'' : (\mu\alpha.\, \tau_1)^{[\rho]}$,
        which follows from the outer induction hypothesis, noting that $i < k$ (since $i \leq j < k$), applied to $\rho \in \mathcal{RD}\, [\![\Delta]\!]$, $\Delta \vdash \mu\alpha.\, \tau_1$, $(i, v_0, v_0') \in \mathcal{RV}\, [\![\mu\alpha.\, \tau_1]\!]\, \rho$, and $v_0' \prec^{ciu} v_0'' : (\mu\alpha.\, \tau_1)^{[\rho]}$.

- $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho_1$,
  which follows from above, and
- $v_{22} \prec^{ciu} v_{33} : (\tau_1)^{[\rho_1]}$,
  which follows from above

we conclude that $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho_1$.
Hence, $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, (\mu\alpha.\,\tau_1)^{[\rho]})]$.

Case (AllTy) $\dfrac{\Delta, \alpha \vdash \tau_1}{\Delta \vdash \forall\alpha.\,\tau_1}$:

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\forall\alpha.\,\tau_1]\!]\,\rho$, and
(2) $v_2 \prec^{ciu} v_3 : (\forall\alpha.\,\tau_1)^{[\rho]} \;\equiv\; v_2 \prec^{ciu} v_3 : \forall\alpha.\,(\tau_1)^{[\rho]}$.

Hence, from **(1)** it follows that $v_1 \equiv \Lambda.\,e_{11}$ and $e_2 \equiv \Lambda.\,e_{22}$.
From **(2)** it follows that $\vdash v_3 : \forall\alpha.\,(\tau_1)^{[\rho]}$. Hence, $v_3 \equiv \Lambda.\,e_{33}$.
We are required to show that $(k, \Lambda.\,e_{11}, \Lambda.\,e_{33}) \in \mathcal{RV}\,[\![\forall\alpha.\,\tau_1]\!]\,\rho$,
which follows from

- $\vdash \Lambda.\,e_{33} : (\forall\alpha.\,\tau_1)^{[\rho]}$,
  which follows from **(2)**.
- $\forall\tau_2, \chi.\ \chi \in \mathit{Rel}_{\tau_2} \implies \forall j < k.\ (j, e_{11}, e_{33}) \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$:
  Consider arbitrary τ_2, and χ such that
  - $\chi \in \mathit{Rel}_{\tau_2}$.

  We are required to show that $\forall j < k.\ (j, e_{11}, e_{33}) \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.
  Consider arbitrary j such that
  - $j < k$.

  We are required to show that $(j, e_{11}, e_{33}) \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.
  Consider arbitrary i and $e_{f_{11}}$ such that
  - $i < j$,
  - $e_{11} \longmapsto^{i} e_{f_{11}}$, and
  - $\mathit{irred}(e_{f_{11}})$.

  We are required to show that $\exists e'_f.\ e_{33} \longmapsto^{*} e'_f \ \wedge\ (j - i, e_{f_{11}}, e'_f) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.
  Instantiate the second conjunct of **(1)** with τ_2, and χ. Note that
  - $\chi \in \mathit{Rel}_{\tau_2}$.

  Hence, $\forall j < k.\ (j, e_{11}, e_{22}) \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.
  Instantiate this with j, noting that $j < k$.
  Hence, $(j, e_{11}, e_{22}) \in \mathcal{RC}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.
  Instantiate this with i and $e_{f_{11}}$. Note that
  - $i < j$,
  - $e_{11} \longmapsto^{i} e_{f_{11}}$, and
  - $\mathit{irred}(e_{f_{11}})$.

  Hence, there exists $e_{f_{22}}$ such that
  - $e_{22} \longmapsto^{*} e_{f_{22}}$, and

- $(j-i, e_{f_{11}}, e_{f_{22}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

Hence, $e_{f_{11}} \equiv v_{f_{11}}$ and $e_{f_{22}} \equiv v_{f_{22}}$.
Instantiate **(2)** with $[\cdot]\,[\,]$ and $\tau_1[\tau_2/\alpha]$. Note that

- $\bullet;\bullet \vdash [\cdot]\,[\,] : (\bullet;\bullet \triangleright \forall\alpha.\,(\tau_1)^{[\rho]}) \rightsquigarrow (\tau_1)^{[\rho]}[\tau_2/\alpha]$, and
- $[\Lambda.\,e_{22}]\,[\,] \Downarrow$,
  which follows from $\Lambda.\,e_{22}\,[\,] \longmapsto^1 e_{22}$ and $e_{22} \longmapsto^* v_{f_{22}}$,
  which follow from above.

Hence, there exists $v_{f_{33}}$ such that $\Lambda.\,e_{33}\,[\,] \Downarrow v_{f_{33}}$.
By the operational semantics, it must that $\Lambda.\,e_{33}\,[\,] \longmapsto^1 e_{33}$.
Hence, it must be that $e_{33} \Downarrow v_{f_{33}}$.
Let $\rho_1 = \rho[\alpha \mapsto (\chi, \tau_2)]$.
We show that $v_{f_{22}} \prec^{ciu} v_{f_{33}} : (\tau_1)^{[\rho_1]}$
$\equiv v_{22} \prec^{ciu} v_{33} : (\tau_1[\tau_2/\alpha])^{[\rho]}$:

- Consider arbitrary E_0 and τ_0 such that
  - $\bullet;\bullet \vdash E_0 : (\bullet;\bullet \triangleright (\tau_1[\tau_2/\alpha])^{[\rho]}) \rightsquigarrow \tau_0$, and
  - $E_0[v_{f_{22}}] \Downarrow$.

  We are required to show that $E_0[v_{f_{33}}] \Downarrow$.
  Instantiate **(2)** with $E_0[[\cdot]\,[\,]]$ and τ_0. Note that
  - $\bullet;\bullet \vdash E_0[[\cdot]\,[\,]] : (\bullet;\bullet \triangleright (\forall\alpha.\,\tau_1)^{[\rho]}) \rightsquigarrow \tau_0$, and
  - $E_0[[\Lambda.\,e_{22}]\,[\,]] \longmapsto^1 E_0[e_{22}] \longmapsto^* E_0[v_{f_{22}}] \Downarrow$.

  Hence, $E_0[[\Lambda.\,e_{33}]\,[\,]] \Downarrow$.
  By the operational semantics, it must be that $E_0[[\Lambda.\,e_{33}]\,[\,]] \longmapsto^1 E_0[e_{33}] \longmapsto^* E_0[v_{f_{33}}]$.
  Hence, it must be that $E_0[v_{f_{33}}] \Downarrow$.

Take $e'_f = v_{f_{33}}$.
We are required to show

- $e_{33} \longmapsto^* v_{f_{33}}$,
  which follows from above, and
- $(j-i, v_{f_{11}}, v_{f_{33}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$:
  Applying the induction hypothesis to $\Delta, \alpha \vdash \tau_1$, with
  - $\rho_1 \in \mathcal{RD}\,[\![\Delta, \alpha]\!]$,
    which follows (since $\rho_1 = \rho[\alpha \mapsto (\chi, \tau_2)]$) from
    - $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
    - $\chi \in \mathit{Rel}_{\tau_2}$,
      which follows from above.
  - $(j-i, v_{f_{11}}, v_{f_{22}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho_1$,
    which follows from above, and
  - $v_{f_{22}} \prec^{ciu} v_{f_{33}} : (\tau_1)^{[\rho_1]}$,
    which follows from above

  we conclude that $(j-i, v_{f_{11}}, v_{f_{33}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho_1$.
  Hence, $(j-i, v_{f_{11}}, v_{f_{33}}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

Case $(\mathsf{ExTy})\ \dfrac{\Delta, \alpha \vdash \tau_1}{\Delta \vdash \exists \alpha.\, \tau_1}$:

Note that this case of the proof fails to go through.

We have as premises

(1) $(k, v_1, v_2) \in \mathcal{RV}\,[\![\exists \alpha.\, \tau_1]\!]\,\rho$, and

(2) $v_2 \prec^{ciu} v_3 : (\exists \alpha.\, \tau_1)^{[\rho]} \;\equiv\; v_2 \prec^{ciu} v_3 : \exists \alpha.\, (\tau_1)^{[\rho]}$.

Hence, from **(1)** it follows that $v_1 \equiv \mathtt{pack}\, v_{11}$ and $v_2 \equiv \mathtt{pack}\, v_{22}$.

From **(2)** it follows that $\vdash v_3 : \exists \alpha.\, (\tau_1)^{[\rho]}$. Hence, $v_3 \equiv \mathtt{pack}\, v_{33}$.

We are required to show that $(k, \mathtt{pack}\, v_{11}, \mathtt{pack}\, v_{33}) \in \mathcal{RV}\,[\![\exists \alpha.\, \tau_1]\!]\,\rho$,
which follows from

- $\vdash \mathtt{pack}\, v_{33} : (\exists \alpha.\, \tau_1)^{[\rho]}$,
  which follows from **(2)**.
- $\exists \tau_2, \chi.\ \chi \in \mathit{Rel}_{\tau_2} \ \wedge\ \forall j < k.\ (j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$:
  From the second conjunct of **(1)** it follows that there exist τ_2 and χ such that

  (A) $\chi \in \mathit{Rel}_{\tau_2}$, and

  (B) $\forall j < k.\ (j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

  From **(A)** we have a τ_2 and χ such that $\chi \in \mathit{Rel}_{\tau_2}$.

  Hence, it remains for us to show that $\forall j < k.\ (j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

  Consider arbitrary j such that

  - $j < k$.

  Instantiate **(B)** with j, noting that $j < k$.

  Hence, $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$.

  Let $\rho_1 = \rho[\alpha \mapsto (\chi, \tau_2)]$. Note that $(\tau_1[\tau_2/\alpha])^{[\rho]} \;\equiv\; (\tau_1)^{[\rho_1]}$.

  We are required to show that $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho[\alpha \mapsto (\chi, \tau_2)]$
  $\equiv (j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho_1$.

  We *attempt* to prove the above as follows:

  We can conclude that $(j, v_{11}, v_{33}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho_1$ by applying the induction hypothesis to $\Delta, \alpha \vdash \tau_1$, but we require the following:

  - $\rho_1 \in \mathcal{RD}\,[\![\Delta, \alpha]\!]$,
    which follows (since $\rho_1 = \rho[\alpha \mapsto (\chi, (\mu\alpha.\, \tau_1)^{[\rho]})]$) from
    - $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
    - $\chi \in \mathit{Rel}_{\tau_2}$,
      which follows from above
  - $(j, v_{11}, v_{22}) \in \mathcal{RV}\,[\![\tau_1]\!]\,\rho_1$,
    which follows from above, and
  - $v_{22} \prec^{ciu} v_{33} : (\tau_1)^{[\rho_1]}$,
    Problem: An attempt to prove this gets stuck:
    We wish to show that $v_{22} \prec^{ciu} v_{33} : (\tau_1)^{[\rho_1]}$
    $\equiv v_{22} \prec^{ciu} v_{33} : (\tau_1[\tau_2/\alpha])^{[\rho]}$:
    - Consider arbitrary E_0 and τ_0 such that
      - $\bullet; \bullet \vdash E_0 : (\bullet; \bullet \triangleright (\tau_1[\tau_2/\alpha])^{[\rho]}) \rightsquigarrow \tau_0$, and
      - $E_0[v_{22}] \Downarrow$.

We are required to show that $E_0[v_{33}] \Downarrow$.
We could instantiate **(2)** with $E_0[\texttt{unpack}\,[\cdot]\,\texttt{as}\,x\,\texttt{in}\,x]$ and τ_0. To proceed, the following two conditions should hold:

- **(Z)** $\bullet; \bullet \vdash E_0[\texttt{unpack}\,[\cdot]\,\texttt{as}\,x\,\texttt{in}\,x] : (\bullet; \bullet \triangleright (\exists\alpha.\,\tau_1)^{[\rho]}) \rightsquigarrow \tau_0$.
  Problem: (Z) is false. The result of the unpack is x, which has type $\tau_1^{[\rho]}$ (where $FTV\tau_1^{[\rho]} = \{\alpha\}$). Thus, it is not the case that $\bullet \vdash \tau_1^{[\rho]}$ as required by the premises of the unpack typing rule.
- $E_0[\texttt{unpack}\,[\texttt{pack}\,v_{22}]\,\texttt{as}\,x\,\texttt{in}\,x] \longmapsto^1 E_0[v_{22}] \Downarrow$,
  which follows from the operational semantics.

If **(Z)** were true, we could have proceeded as follows. We could now conclude that $E_0[\texttt{unpack}\,[\texttt{pack}\,v_{33}]\,\texttt{as}\,x\,\texttt{in}\,x] \Downarrow$. Thus, by the operational semantics, it must be that $E_0[\texttt{unpack}\,[\texttt{pack}\,v_{33}]\,\texttt{as}\,x\,\texttt{in}\,x] \longmapsto^1 E_0[v_{33}]$. Hence, it must be that $E_0[v_{33}] \Downarrow$.

However, since **(Z)** does not hold, we cannot conclude that $E_0[v_{33}] \Downarrow$ as required.

□

Lemma E.2 **($\lambda^{\forall}$ Valid Per: $\mathcal{RV}[\![\tau]\!]\rho \in Rel_{\tau^{[\rho]}}$)**

Let $\rho \in \mathcal{RD}[\![\Delta]\!]$ and $\Delta \vdash \tau$.
Then $\mathcal{RV}[\![\tau]\!]\rho \in Rel_{\tau^{[\rho]}}$.

Proof

By the definition of $Rel_{\tau^{[\rho]}}$, it suffices to show:

$$\begin{aligned}\forall(k, v, v') \in \mathcal{RV}[\![\tau]\!]\rho.\ & \vdash v' : \tau^{[\rho]}\ \wedge \\ & \forall j \leq k.\ (j, v, v') \in \mathcal{RV}[\![\tau]\!]\rho\ \wedge \\ & (\forall v''.\ v' \prec^{ciu} v'' : \tau^{[\rho]} \implies (j, v, v'') \in \mathcal{RV}[\![\tau]\!]\rho)\end{aligned}$$

Consider arbitrary $(k, v, v') \in \mathcal{RV}[\![\tau]\!]\rho$.

- Applying Lemma C.7 to $\rho \in \mathcal{RD}[\![\Delta]\!]$, $\Delta \vdash \tau$, and $(k, v, v') \in \mathcal{RV}[\![\tau]\!]\rho$, it follows that $\vdash v' : \tau^{[\rho]}$.
- Consider arbitrary $j \leq k$.

  Applying Lemma C.9 to $\rho \in \mathcal{RD}[\![\Delta]\!]$, $\Delta \vdash \tau$, $(k, v, v') \in \mathcal{RV}[\![\tau]\!]\rho$, and $j \leq k$, it follows that $(j, v, v') \in \mathcal{RV}[\![\tau]\!]\rho$.
- Consider arbitrary v'' such that $v' \prec^{ciu} v'' : \tau^{[\rho]}$.

  Applying Lemma E.1 to $\rho \in \mathcal{RD}[\![\Delta]\!]$, $\Delta \vdash \tau$, $(k, v, v') \in \mathcal{RV}[\![\tau]\!]\rho$, and $v' \prec^{ciu} v'' : \tau^{[\rho]}$, it follows that $(k, v, v'') \in \mathcal{RV}[\![\tau]\!]\rho$.

□

E.3 $\lambda^{\forall}$ Proofs: Completeness w.r.t. Contextual Equivalence

In this section, we show that $\preceq^{ctx} \subseteq \preceq^{ciu}$ for $\lambda^{\forall\exists}$. Furthermore, for $\lambda^{\forall}$ (i.e., $\lambda^{\forall\exists}$ without existential types), we show that $\preceq^{ciu} \subseteq \leq$. Thus, we may conclude that our logical relation for $\lambda^{\forall}$ is complete with respect to contextual equivalence.

Lemma E.3 **($\lambda^{\forall\exists}$: $\preceq^{ctx}$ Congruence)**

If $\Delta; \Gamma \vdash e \preceq^{ctx} e' : \tau$ *and* $\Delta_1; \Gamma_1 \vdash C_1 : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$,
then $\Delta_1; \Gamma_1 \vdash C_1[e] \preceq^{ctx} C_1[e'] : \tau_1$.

Proof

Consider arbitrary C and τ_0 such that

- $\bullet; \bullet \vdash C : (\Delta_1; \Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0$, and
- $C[C_1[e]] \Downarrow$.

We are required to show that $C[C_1[e']] \Downarrow$.

Instantiate $\Delta; \Gamma \vdash e \preceq^{ctx} e' : \tau$ with $C[C_1[\cdot]]$ and τ_0. Note that

- $\bullet; \bullet \vdash C[C_1[\cdot]] : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0$, which follows using the (C-ctxt) rule:

$$\text{(C-ctxt)}\ \frac{\bullet; \bullet \vdash C : (\Delta_1; \Gamma_1 \triangleright \tau_1) \rightsquigarrow \tau_0 \qquad \Delta_1; \Gamma_1 \vdash C_1 : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1}{\bullet; \bullet \vdash C[C_1[\cdot]] : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_0}$$

- $C[C_1[e]] \Downarrow$.

Hence, $C[C_1[e']] \Downarrow$. □

Lemma E.4 $(\lambda^{\forall\exists}: \preceq^{ctx} \subseteq \preceq^{ciu})$

If $\Delta; \Gamma \vdash e \preceq^{ctx} e' : \tau$
then $\Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau$.

Proof

Consider arbitrary δ, γ, E, and τ_1 such that

- $\delta \models \Delta$,
- $\vdash \gamma : \delta(\Gamma)$,
- $\bullet; \bullet \vdash E : (\bullet; \bullet \triangleright \delta(\tau)) \rightsquigarrow \tau_1$, and
- $E[\gamma(e)] \Downarrow$.

If $\delta = \{\alpha_1 \mapsto \tau_1', \alpha_2 \mapsto \tau_2', \ldots \alpha_m \mapsto \tau_m'\}$ and $\gamma = \{x_1 \mapsto v_1, x_2 \mapsto v_2, \ldots, x_n \mapsto v_n\}$,
then let $C_\gamma = (\Lambda.\, \Lambda. \ldots \Lambda.\, \lambda x_1.\, \lambda x_2. \ldots \lambda x_n.\, [\cdot])\, [\,]_1\, [\,]_2 \ldots\, [\,]_m\, v_1\, v_2\, \ldots\, v_n$.
Note that if we had explicit types in terms, we would have written

$$C_\gamma = (\Lambda\alpha_1.\, \Lambda\alpha_2. \ldots \Lambda\alpha_m.\, \lambda x_1.\, \lambda x_2. \ldots \lambda x_n.\, [\cdot])\, [\tau_1']\, [\tau_2'] \ldots\, [\tau_m']\, v_1\, v_2\, \ldots\, v_n$$

Note that $\bullet; \bullet \vdash C_\gamma : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \delta(\tau)$.

Hence, note that

- $\bullet; \bullet \vdash C_\gamma[e] \preceq^{ctx} C_\gamma[e'] : \delta(\tau)$,
  which follows from Lemma E.3 applied to $\Delta; \Gamma \vdash e \preceq^{ctx} e' : \tau$ and $\bullet; \bullet \vdash C_\gamma : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \delta(\tau)$.

Instantiate this with E and τ_1. Note that

- $\bullet; \bullet \vdash E : (\bullet; \bullet \triangleright \delta(\tau)) \rightsquigarrow \tau_1$,
  which follows from above, and
- $E[C_\gamma[e]] \Downarrow$, which follows from
  - $E[C_\gamma[e]] \longmapsto^* E[\gamma(e)]$,
    which follows from the operational semantics and an examination of C_γ, and
  - $E[\gamma(e)] \Downarrow$,
    which follows from above.

Hence, $E[C_\gamma[e']] \Downarrow$.

By the operational semantics, it must be that $E[C_\gamma[e']] \longmapsto^* E[\gamma(e')]$.

Hence, it must be that $E[\gamma(e')] \Downarrow$. □

Lemma E.5 ($\lambda^{\forall}$: $\preceq^{ciu} \subseteq \leq$)

If $\Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau$
then $\Delta; \Gamma \vdash e \leq e' : \tau$.

Proof

NOTE: This lemma holds only for $\lambda^{\forall}$ (i.e., $\lambda^{\forall\exists}$ without existential types), since the proof makes use of Lemma E.1 which does not hold for existential types.

Consider arbitrary k, ρ, γ, and γ' such that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

We are required to show that $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}\,[\![\tau]\!]\,\rho$.
Consider arbitrary j and e_f such that

- $j < k$,
- $\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Note that $\Delta; \Gamma \vdash e \leq e : \tau$, which follows from Lemma C.29 applied to $\Delta; \Gamma \vdash e : \tau$.
Instantiate $\Delta; \Gamma \vdash e \leq e : \tau$ with k, ρ, γ, and γ'. Note that

- $k \geq 0$,
- $\rho \in \mathcal{RD}\,[\![\Delta]\!]$, and
- $(k, \gamma, \gamma') \in \mathcal{RG}\,[\![\Gamma]\!]\,\rho$.

Hence, $(k, \gamma(e), \gamma'(e)) \in \mathcal{RC}\,[\![\tau]\!]\,\rho$.
Instantiate this with j and e_f. Note that

- $j < k$,
- $\gamma(e) \longmapsto^{j} e_f$, and
- $\mathit{irred}(e_f)$.

Hence, there exists e'_f such that

- $\gamma'(e) \longmapsto^{*} e'_f$, and
- $(k - j, e_f, e'_f) \in \mathcal{RV}\,[\![\tau]\!]\,\rho$.

Note that $e_f \equiv v_f$ and $e'_f \equiv v'_f$.
Hence, $\gamma'(e) \Downarrow v'_f$.
Let $\delta_\rho = \{\alpha \mapsto \tau \mid \ \rho(\alpha) = (\chi, \tau)\}$.
Instantiate $\Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau$ with δ_ρ, γ', $[\cdot]$, and τ. Note that

- $\delta_\rho \models \Delta$,
  which follows from $dom(\delta_\rho) = dom(\rho) = \Delta$,
- $\vdash \gamma' : \delta_\rho(\Gamma)$
  $\equiv \vdash \gamma' : \Gamma^{[\rho]}$,
  which follows from Lemma C.8 applied to $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$,
- $\bullet;\bullet \vdash [\cdot] : (\bullet;\bullet \triangleright \delta_\rho(\tau)) \rightsquigarrow \delta_\rho(\tau)$, and
- $\gamma'(e) \Downarrow$.

Hence, there exists v_f'' such that $\gamma'(e') \Downarrow v_f''$.
Let $e_f'' = v_f''$.
We are required to show that

- $\gamma'(e') \longmapsto^* v_f''$,
  which follows from above, and
- $(k - j, v_f, v_f'') \in \mathcal{RV}[\![\tau]\!]\,\rho$,
  which follows from Lemma E.1 applied to
  - $\rho \in \mathcal{RD}[\![\Delta]\!]$,
  - $\Delta \vdash \tau$,
  - $(k - j, v_f, v_f') \in \mathcal{RV}[\![\tau]\!]\,\rho$, and
  - $v_f' \prec^{ciu} v_f'' : \tau^{[\rho]}$,
    which follows from
    - Consider arbitrary E_1 and τ_1 such that
      - $\bullet;\bullet \vdash E_1 : (\bullet;\bullet \triangleright \tau^{[\rho]}) \rightsquigarrow \tau_1$, and
      - $E_1[v_f'] \Downarrow$.

      We are required to show that $E_1[v_f''] \Downarrow$.
      Let $\delta_\rho = \{\alpha \mapsto \tau \mid \ \rho(\alpha) = (\chi, \tau)\}$.
      Instantiate $\Delta; \Gamma \vdash e \preceq^{ciu} e' : \tau$ with δ_ρ, γ', E_1, and τ_1. Note that
      - $\delta_\rho \models \Delta$,
        which follows from $dom(\delta_\rho) = dom(\rho) = \Delta$,
      - $\vdash \gamma' : \delta_\rho(\Gamma)$
        $\equiv \vdash \gamma' : \Gamma^{[\rho]}$,
        which follows from Lemma C.8 applied to $(k, \gamma, \gamma') \in \mathcal{RG}[\![\Gamma]\!]\,\rho$,
      - $\bullet;\bullet \vdash E_1 : (\bullet;\bullet \triangleright \delta_\rho(\tau)) \rightsquigarrow \tau_1$, and
      - $E_1[\gamma'(e)] \Downarrow$,
        which follows from
        - $E_1[\gamma'(e)] \longmapsto^* E_1[v_f]$,
          which follows from $\gamma'(e) \longmapsto^* v_f$, and

- $E_1[v_f] \Downarrow$,
  which follows from above.

Hence, $E_1[\gamma'(e')] \Downarrow$.

By the operational semantics, it must be that $E_1[\gamma'(e')] \longmapsto^* E_1[v''_f]$, which follows from $\gamma'(e') \longmapsto^* v''_f$ above.

Hence, it must be that $E_1[v''_f] \Downarrow$.

□

E.4 $\lambda^{\forall}$ Example

In this section, we return to the higher-order function example in Section D.3. This is the only example we considered in Appendix D that did not involve existential types. In this section, we work out the same example using our new logical relation, which uses the modified definition of Rel_τ.

As in Section D, we wish to show that the closed terms e and e' of type τ are contextually equivalent — that is, $\bullet;\bullet \vdash e \simeq^{ctx} e' : \tau$. It suffices to show $\bullet;\bullet \vdash e \sim e' : \tau$.

Notation Let χ be a set of tuples of the form (k, v, v') such that $\vdash v' : \tau$. We define the transitive closure of χ under ciu approximation at type τ as follows:

$$\chi^*_\tau \quad = \quad \{(k, v_1, v_2) \mid \ (k, v_1, v_2) \in \chi \ \vee \ ((k, v_1, v) \in \chi \ \wedge \ v \preceq^{ciu} v_2 : \tau)\}$$

Example: Higher Order Functions I (see Section D.3)

Consider the following higher-order functions e and e' of type τ (see Sumii and Pierce [19], Section 4.5). Note that this example is essentially the "dual" of the example in Section D.1.

$$\begin{array}{lcl} e & = & \lambda f.\, f\,[\,]\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle \\ e' & = & \lambda f.\, f\,[\,]\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle \\ \sigma & = & \forall\alpha.\, (\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1} \\ \tau & = & \sigma \to \mathbf{1} \end{array}$$

We are required to show that $\bullet;\bullet \vdash e \sim e' : \tau$. The proof is in two parts.

I. Show $\bullet;\bullet \vdash e \leq e' : \tau$.

Consider an arbitrary $k \geq 0$.

Unwinding definitions, we see that since e and e' are closed values of closed type, it suffices to show that $(k, e, e') \in \mathcal{RV}\,[\![\tau]\!]\,\emptyset \equiv (k, \lambda f.\, f\,[\,]\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle, \lambda f.\, f\,[\,]\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\sigma \to \mathbf{1}]\!]\,\emptyset$.

Note that we already have $\vdash e' : \sigma \to \mathbf{1}$.

Consider arbitrary j, v, and v' such that

- $j < k$, and
- $(j, v, v') \in \mathcal{RV}\,[\![\sigma]\!]\,\emptyset$
  $\equiv (j, v, v') \in \mathcal{RV}\,[\![\forall\alpha.\, (\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset$.

Note that $\vdash v' : \sigma$, which follows from Lemma C.7 applied to $(j, v, v') \in \mathcal{RV}\,[\![\sigma]\!]\,\emptyset$.

Also, note that $v = \Lambda.\, e_1$ and $v' = \Lambda.\, e_1'$, which follows from $(j, v, v') \in \mathcal{RV}\,[\![\forall\alpha.\ \ldots]\!]\,\emptyset$.

We are required to show that
$(j,\ \ (f\,[\,]\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle)[v/f],\ \ (f\,[\,]\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle)[v'/f]) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset$
$\equiv (j,\ \ (v\,[\,])\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle,\ \ (v'\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset$
$\equiv (j,\ \ (\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle,\ \ (\Lambda.\, e_1'\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset$.

Consider arbitrary j_1 and e_{f_1} such that

- $j_1 < j$,
- $((\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) \longmapsto^{j_1} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

By the operational semantics, it follows that

$$((\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle) \underset{\longmapsto^{j_1-1}}{\longmapsto^{1}} (e_1\,\langle 1, \lambda x.\, x \overset{\text{int}}{=} 0\rangle)\ e_{f_1}$$

Hence, by the operational semantics, it follows that there must exist j_{11} and $e_{f_{11}}$ such that

- $e_1 \longmapsto^{j_{11}} e_{f_{11}}$,
- $\mathit{irred}(e_{f_{11}})$, and
- $j_{11} \leq j_1 - 1$.

Let $\chi_0 = \{(k', 1, \mathtt{tt}) \mid \ k' \geq 0\}$.
Take $\tau_2 = \mathsf{bool}$ and $\chi = (\chi_0)^*_{\mathsf{bool}}$.
Instantiate the second conjunct of $(j, \Lambda.\, e_1, \Lambda.\, e_1') \in \mathcal{RV}\,[\![\forall\alpha.\, (\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset$ with χ and τ_2.
Note that $\chi \in \mathit{Rel}_{\mathsf{bool}}$, which follows from the definition of χ_0 and $(\chi_0)^*_{\mathsf{bool}}$.
Hence, we have $\forall i < j.\ (i, e_1, e_1') \in \mathcal{RC}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
Instantiate this with j_1 noting that $j_1 < j$.
Hence, we have $(j_1, e_1, e_1') \in \mathcal{RC}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
Instantiate this with j_{11} and $e_{f_{11}}$. Note that

- $j_{11} < j_1$, which follows from $j_{11} \leq j_1 - 1$,
- $e_1 \longmapsto^{j_{11}} e_{f_{11}}$, and
- $\mathit{irred}(e_{f_{11}})$.

Hence, there exists $e'_{f_{11}}$ such that

- $e_1' \longmapsto^* e'_{f_{11}}$ and
- $(j_1 - j_{11}, e_{f_{11}}, e'_{f_{11}}) \in \mathcal{RV}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.

Hence, $e_{f_{11}} = \lambda z.\, e_2$ and $e'_{f_{11}} = \lambda z.\, e_2'$.
Then, by the operational semantics it follows that

$$\begin{aligned}
((\Lambda.\, e_1\,[\,])\,\langle 1, \lambda x.\, x \overset{\mathrm{int}}{=} 0\rangle) &\longmapsto^1 \ (e_1\,\langle 1, \lambda x.\, x \overset{\mathrm{int}}{=} 0\rangle) \\
&\longmapsto^{j_{11}} \ (e_{f_{11}}\,\langle 1, \lambda x.\, x \overset{\mathrm{int}}{=} 0\rangle) \\
&\equiv \ (\lambda z.\, e_2\,\langle 1, \lambda x.\, x \overset{\mathrm{int}}{=} 0\rangle) \\
&\longmapsto^1 \ (e_2[\langle 1, \lambda x.\, x \overset{\mathrm{int}}{=} 0\rangle / z]) \\
&\longmapsto^{j_{12}} \ e_{f_1}
\end{aligned}$$

Note that $j_1 = 1 + j_{11} + 1 + j_{12}$.
Let $v_z = \langle 1, \lambda x.\, x \overset{\mathrm{int}}{=} 0\rangle$.
Let $v_z' = \langle \mathtt{tt}, \lambda x.\, \neg x\rangle$.
Instantiate $(j_1 - j_{11}, \lambda z.\, e_2, \lambda z.\, e_2') \in \mathcal{RV}\,[\![(\alpha \times (\alpha \to \mathsf{bool})) \to \mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$ with $j_{12} + 1$, v_z, and v_z'. Note that

- $j_{12} + 1 < j_1 - j_{11}$, which follows from $j_{12} = j_1 - 1 - j_{11} - 1$, and
- $(j_{12} + 1, v_z, v_z') \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv \ (j_{12} + 1,\ \langle 1, \lambda x.\, x \overset{\mathrm{int}}{=} 0\rangle,\ \langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \in \mathcal{RV}\,[\![\alpha \times (\alpha \to \mathsf{bool})]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$,
  which follows from
  - $\vdash \langle \mathtt{tt}, \lambda x.\, \neg x\rangle : (\alpha \times (\alpha \to \mathsf{bool}))[\mathsf{bool}/\alpha]$
    $\equiv \ \vdash \langle \mathtt{tt}, \lambda x.\, \neg x\rangle : \mathsf{bool} \times (\mathsf{bool} \to \mathsf{bool})$, which follows from the static semantics.
  - $(j_{12} + 1, 1, \mathtt{tt}) \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
    $\equiv (j_{12} + 1, 1, \mathtt{tt}) \in \chi$ (by the definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$)
    which follows from $(j_{12} + 1, 1, \mathtt{tt}) \in \chi_0$ and $\chi_0 \subseteq \chi$, which follows from our choice of χ.

- $(j_{12}+1, \lambda x.\, x \stackrel{\text{int}}{=} 0, \lambda x.\, \neg x) \in \mathcal{RV}\,[\![\alpha \to \mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which we conclude as follows:

  First, note that $\vdash \lambda x.\, \neg x : (\alpha \to \mathsf{bool})[\mathsf{bool}/\alpha] \;\equiv\; \vdash \lambda x.\, \neg x : \mathsf{bool} \to \mathsf{bool}$, which follows easily from the static semantics.

  Next, consider arbitrary i, v_1, and v_1' such that

  - $i < j_{12} + 1$, and
  - $(i, v_1, v_1') \in \mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.

  Note that $\mathcal{RV}\,[\![\alpha]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \equiv \chi$ by definition of $\mathcal{RV}\,[\![\alpha]\!]\,\rho$.

  Hence, $(i, v_1, v_1') \in \chi$.

  Then, it must be that $v_1 = 1$, which follows from the definition of χ.

  Furthermore, it must be that $v_1' = \mathtt{tt}$, which we conclude from the definition of χ as follows: By the definition of χ, note that either

  - $v_1' = \mathtt{tt}$, or
  - $v_1' = v$ for some v such that $\mathtt{tt} \prec^{ciu} v : \mathsf{bool}$. Since $\prec^{ciu} \equiv \leq$ (by Lemmas C.46, E.4, and E.5), it follows that $\mathtt{tt} \leq v : \mathsf{bool}$. Hence, from the definiton of $\leq$ and $\mathcal{RV}\,[\![\mathsf{bool}]\!]$, it follows that $v = \mathtt{tt}$.

  We are required to show that

  $$\begin{array}{rcl} (i, (x \stackrel{\text{int}}{=} 0)[v_1/x], (\neg x)[v_1'/x]) & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \\ \equiv (i, v_1 \stackrel{\text{int}}{=} 0, \neg v_1') & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \\ \equiv (i, 1 \stackrel{\text{int}}{=} 0, \neg \mathtt{tt}) & \in & \mathcal{RC}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})] \end{array}$$

  Note that $(1 \stackrel{\text{int}}{=} 0) \longmapsto^1 \mathtt{ff}$ and $(\neg \mathtt{tt}) \longmapsto^* \mathtt{ff}$.

  Hence, it remains for us to show that $(i - 1, \mathtt{ff}, \mathtt{ff}) \in \mathcal{RV}\,[\![\mathsf{bool}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$, which is immediate.

Hence, $(j_{12} + 1, e_2[v_z/z], e_2'[v_z'/z]) \in \mathcal{RC}\,[\![\mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.
Instantiate this with j_{12} and e_{f_1}. Note that

- $j_{12} < j_{12} + 1$,
- $e_2[v_z/z] \longmapsto^{j_{12}} e_{f_1}$, and
- $\mathit{irred}(e_{f_1})$.

Hence, there exists e_{f_1}' such that

- $e_2'[v_z'/z] \longmapsto^* e_{f_1}'$, and
- $(j_{12} + 1 - j_{12}, e_{f_1}, e_{f_1}') \in \mathcal{RV}\,[\![\mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$
  $\equiv (1, e_{f_1}, e_{f_1}') \in \mathcal{RV}\,[\![\mathbf{1}]\!]\,\emptyset[\alpha \mapsto (\chi, \mathsf{bool})]$.

Hence, $e_{f_1} = \langle\,\rangle$ and $e'_{f_1} = \langle\,\rangle$.

Hence, by the operational semantics we have

$$\begin{array}{rl} ((\Lambda.\, e'_1\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) & \longmapsto^1 \;\; (e'_1\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \\ & \longmapsto^* \;\; (e'_{f_{11}}\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \\ & \equiv \;\; (\lambda z.\, e'_2\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle) \\ & \longmapsto^1 \;\; (e'_2[\langle \mathtt{tt}, \lambda x.\, \neg x\rangle / z]) \\ & \longmapsto^* \;\; e'_{f_1} \end{array}$$

Take $e'_{f_1} = e'_{f_1} \equiv \langle\,\rangle$. We are required to show

- $(\Lambda.\, e'_1\,[\,])\,\langle \mathtt{tt}, \lambda x.\, \neg x\rangle \longmapsto^* e'_{f_1}$,
  which follows from above, and
- $(j - j_1, e_{f_1}, e'_{f_1}) \in \mathcal{RV}\,[\![\mathbf{1}]\!]\,\emptyset$,
  which follows from $e_{f_1} = e'_{f_1} = \langle\,\rangle$.

II. Show $\bullet; \bullet \vdash e' \leq e : \tau$.

The proof is analogous to that of **(I)**.