Verifying an Open Compiler Using Multi-Language Semantics: Technical Report

James T. Perconti and Amal Ahmed

Northeastern University

This document contains:

- The paper that appears in ESOP'14.
- An appendix giving a more detailed explanation of the logical relation.
- The complete definitions and proofs for our FCA model.

Verifying an Open Compiler Using Multi-Language Semantics

James T. Perconti and Amal Ahmed

Northeastern University

Abstract. Existing verified compilers are proved correct under a closed-world assumption, i.e., that the compiler will only be used to compile *whole* programs. We present a new methodology for verifying correct compilation of program *components*, while formally allowing linking with target code of arbitrary provenance. To demonstrate our methodology, we present a two-pass type-preserving open compiler and prove that compilation preserves semantics. The central novelty of our approach is that we define a combined language that embeds the source, intermediate, and target languages and formalizes a semantics of interoperability between them, using boundaries in the style of Matthews and Findler. Compiler correctness is stated as contextual equivalence in the combined language.

Note to reader: We use blue, red, and purple to typeset terms in various languages. This paper will be difficult to follow unless read/printed in color.

1 Introduction

There has been remarkable progress on formally verified compilers over the last few years, with researchers proving the correctness of increasingly sophisticated compilers for increasingly realistic languages. The most well known instance of this is the CompCert compiler [1, 2] which uses the Coq proof assistant to both implement and verify a multi-pass optimizing compiler from C to PowerPC, ARM, and x86 assembly, proving that the compiler preserves semantics of source programs. Several other compiler-verification efforts have successfully followed CompCert's lead and basic methodology, for instance, focusing on multithreaded Java [3], just-in-time compilation [4], and C with relaxed memory concurrency [5].

Unfortunately, these projects prove compiler correctness under a *closed-world* assumption, that is, assuming that the verified compiler will always compile *whole* programs. Despite the immense effort put into verification, the compiler correctness theorem provides no guarantees about correct compilation of *components*. This whole-program assumption is completely unrealistic since most software systems today are comprised of many components written in different languages compiled to a common target, as well as runtime-library routines that may be handwritten in the target language. We need compiler correctness theorems applicable to the way we actually use these compilers.

Formally verifying that components are compiled correctly—often referred to as *compositional compiler correctness*—is a challenging problem. A key difficulty is that, in the setting of compiling components, it is not clear how to even state the compiler correctness theorem. CompCert's compiler correctness theorem is easy to state thanks to the whole program assumption: informally, it says that if a source program P_S compiles to a target program P_T, then running P_S and P_T results in the same trace of observable

events. The same sort of theorem does not make sense when we compile a component e_S to a component e_T: we cannot "run" a component since it is not a complete program.

Intuitively, we want the compiler correctness theorem to say that if a component e_S compiles to e_T, then some desired relationship $e_S \simeq e_T$ holds between e_S and e_T. The central question is: how do we *formally specify* $e_S \simeq e_T$? To answer this question, we must consider how the compiled component is actually used: it needs to be linked with some e'_T, creating a whole program that can be run. Informally, the compiler correctness theorem should guarantee that if we link e_T with e'_T, then the resulting target-level program should correspond to the source component e_S linked with e'_T. But, formally speaking, how can one link a source component with a target component and what are the rules for running the resulting source-target hybrid? These questions demand a *semantics of interoperability* between the source and target languages. We give our semantics of interoperability as a multi-language operational model. We then define $e_S \simeq e_T$ as a contextual equivalence in that model.

There are two other important issues to consider when evaluating a compositional compiler correctness theorem and its supporting formalism. The first is the degree of *horizontal compositionality* that the model allows, that is, which target components e'_T may formally be linked with a compiled component. At the lower end of the horizontal compositionality spectrum are *fully abstract* compilers. Full abstraction states that the compiler both preserves and reflects contextual equivalence. Hence, a fully abstract compiler preserves all of the source language's abstractions, and compiled components are only allowed to link with components that can be expressed in the source language.

But real systems often link together components from multiple languages with different guarantees and different expressive power. We are particularly interested in supporting interoperability between parametric typed languages like ML and low-level languages like C. Thus, full abstraction is often too restrictive. To support the whole programs that we actually run, the compiler correctness theorem should formally support linking with as large a class of programs as possible, and in particular, should not require an e'_T to have been compiled from the same source language as e_T.

Abandoning full abstraction in favor of greater horizontal compositionality does not require giving up all the guarantees of the source language. The compiler and its verification framework can be designed to preserve the source-level equivalences that are critically needed without forbidding all foreign behavior. To show that different levels of abstraction preservation are possible, we will deliberately pick a target language that is more expressive than the source and design our compiler so that it is *not* fully abstract. Our focus in this paper is on how to preserve the representation independence and information hiding guarantees provided by type abstraction in our source language.

The second important issue for a compiler correctness framework is that we want to be able to verify multi-pass compilers. For example, if we have a two-pass compiler that compiles a source component e_S to an intermediate-language component e_I to a target component e_T, we should be able verify each pass separately, showing $e_S \simeq e_I$ and $e_I \simeq e_T$, and then compose these results to get a correctness theorem for the whole compiler saying $e_S \simeq e_T$. This is typically referred to as *vertical compositionality*.

We will show that our approach of using a multi-language operational model succeeds at both horizontal and vertical compositionality. In particular, we validate our

methodology by applying it to a two-pass type-preserving compiler. The compiler deals with three languages: our source language F (System F with existential and recursive types), an intermediate language C (the target of a typed closure conversion pass), and our target language A (the target of a heap allocation pass).[1] The target language A allows tuples and closures to live only on the heap and supports both mutable and immutable references. Our closure conversion pass translates F components of type τ to C components of type $\tau^{\mathcal{C}}$, where $\tau^{\mathcal{C}}$ denotes the type translation of τ. The subsequent allocation pass translates C components of type $\boldsymbol{\tau}$ to A components of type $\boldsymbol{\tau}^{\mathcal{A}}$, where $\boldsymbol{\tau}^{\mathcal{A}}$ is the type translation of $\boldsymbol{\tau}$.

To define the semantics of interoperability between these languages, we embed them all into one language, FCA, and add syntactic boundary forms between each pair of adjacent languages, in the style of Matthews and Findler [7] and of Ahmed and Blume [8]. For instance, the term $\mathcal{CF}^{\tau}(\mathsf{e_F})$ allows an F component $\mathsf{e_F}$ of type τ to be used as a C component of type $\tau^{\mathcal{C}}$, while ${}^{\tau}\mathcal{FC}(\mathbf{e_C})$ allows a C component $\mathbf{e_C}$ of translation type $\tau^{\mathcal{C}}$ to be used as an F component of type τ. Similarly, we have boundary forms $\mathcal{AC}$ and $\mathcal{CA}$ for the next language pair. Non-adjacent languages can interact by stacking up boundaries: for example, $\mathcal{FC}(\mathcal{CA}\,\mathbf{e_A})$ (abbreviated $\mathcal{FCA}(\mathbf{e_A})$) allows an A component $\mathbf{e_A}$ to be embedded in an F term.

FCA *Design Principles* Our goal is for the FCA interoperability semantics to give us a useful specification of when a component in one of the underlying languages should be considered equivalent to a component in another language. We realize that goal by following three principles.

First, we define the operational semantics of FCA so that the original languages are *embedded* into FCA unchanged: running an FCA program that's written solely in one of the embedded languages is identical to running it in that language alone. For instance, execution of the A program $\mathbf{e_A}$ proceeds in exactly the same way whether we use the operational semantics of A or the augmented semantics for FCA.

Next, we ensure that the typing rules are similarly embedded: a component that contains syntax from only one underlying language should typecheck under that language's individual type system if and only if it typechecks under FCA's type system.

The final property we need is *boundary cancellation*, which says that wrapping two opposite language boundaries around a component yields the same behavior as the underlying component with no boundaries. For example, any $\mathsf{e_F} : \tau$ must be contextually equivalent to ${}^{\tau}\mathcal{FC}(\mathcal{CF}^{\tau}\mathsf{e_F})$, and any $\mathbf{e_C} : \tau^{\mathcal{C}}$ must be equivalent to $\mathcal{CF}^{\tau}({}^{\tau}\mathcal{FC}\mathbf{e_C})$.

Compiler Correctness We state the correctness criterion for our compiler as a contextual equivalence. For each pass of the compiler from a source S to a target T, where S and T interoperate via boundaries $\mathcal{ST}$ and $\mathcal{TS}$, define our source-target relationship by

$$e_S \simeq e_T \stackrel{\text{def}}{=} e_S \approx^{ctx}_{\mathsf{FCA}} {}^{\tau}\mathcal{ST}(e_T) : \tau.$$

We prove that if $e_S : \tau$ compiles to e_T, then $e_S \simeq e_T$. Since contextual equivalence is transitive, our framework achieves vertical compositionality immediately: it is easy to combine the two correctness proofs for the individual compiler passes, giving the overall correctness result that if $\mathsf{e_F}$ compiles to $\mathbf{e_A}$, then $\mathsf{e_F} \simeq \mathbf{e_A}$, or

$$\mathsf{e_F} \approx^{ctx}_{\mathsf{FCA}} {}^{\tau}\mathcal{FCA}(\mathbf{e_A}) : \tau.$$

[1] We have extended our F to A compiler with a code-generation pass to an assembly language, much like Morrisett *et al.*'s stack-based TAL [6]. We will report on that work in a future paper.

Reasoning About Linking Our approach enjoys a strong horizontal compositionality property: we can link with any target component e'_A that has an appropriate type, with no requirement that e'_A was produced by any particular means or from any particular source language. Specifically, if e_F expects to be linked with a component of type τ' and compiles to e_A, then e_A will expect to be linked with a component of type $((\tau')^{\mathcal{C}})^{\mathcal{A}}$. If e'_A has this type, then using our compiler correctness theorem, we can conclude that

$$(\mathsf{e}_\mathsf{F}\ {}^{\tau'}\mathcal{FCA}(\mathsf{e}'_\mathsf{A})) \approx^{ctx} \mathcal{FCA}(\mathsf{e}_\mathsf{A}\ \mathsf{e}'_\mathsf{A}),$$

or equivalently,

$$\mathcal{ACF}(\mathsf{e}_\mathsf{F}\ {}^{\tau'}\mathcal{FCA}(\mathsf{e}'_\mathsf{A})) \approx^{ctx} \mathsf{e}_\mathsf{A}\ \mathsf{e}'_\mathsf{A}.$$

The right-hand side of this equality is exactly the A program we ultimately want to run, and the left-hand side is an FCA program that models that program.

Contributions Our main contributions are our methodology and that we have proven correctness for an open multi-pass compiler. We have designed a multi-language semantics that lets us state a strong compiler-correctness theorem, and to prove the theorems, we have developed a logical relation for proving contextual equivalences between FCA components. The most significant technical challenges were related to interoperability between languages with type abstraction, specifically, in designing the multi-language semantics so it preserves type abstraction between languages (§5), and in designing the parts of the logical relation that model the handling of type abstraction in a multi-language setting (§9).

Due to space constraints, we elide various technical details and omit proofs. All definitions, lemmas, and proofs are spelled out in full detail in Appendix B.

2 Related Work: Benton-Hur Approach

Before beginning our technical development, we compare our methodology to the only prominent existing approach to compositional compiler correctness.

To eliminate the closed-world assumption, Benton and Hur [9] advocate setting up a logical relation between the source and target languages, specifying when a source term semantically approximates target code and vice versa. We will refer to a logical relation that relates terms from two *different* languages as a *cross-language* logical relation. The relation is defined by induction on source-language types. Benton and Hur verified a compiler from the simply-typed λ-calculus with recursion [9]—and later, from System F with recursion [10]—to an SECD machine, proving that if source component e_S compiles to target code e_T, then e_S and e_T are logically related. Later, Hur and Dreyer [11] used essentially the same approach to prove correctness of a compiler from an idealized ML to assembly.

However, the Benton-Hur (henceforth, BH) approach suffers from serious drawbacks in both vertical and horizontal compositionality. First, the cross-language framework does not scale to a multi-pass compiler. Both Benton-Hur and Hur-Dreyer handle only a single pass. To achieve vertical compositionality in the BH style, one would have to define separate cross-language logical relations relating the source and target of each compiler pass, and then prove that the logical relations compose transitively in order to establish that the correctness of each pass implies correctness for the entire compiler. But this kind of transitive composition of cross-language logical relations has been an open problem for some time. (We'll discuss recent work towards addressing this problem in §11.)

The second drawback to the BH approach is its limited horizontal compositionality. Consider the situation where a verified compiler from language S to language T is used to compile a source component e_S to some target code e_T. The BH compiler correctness theorem tells us that e_S and e_T are logically related. We wish to link the compiled code e_T with some other target code e'_T and verify the resulting program. To do this using the BH framework, we must now *come up with a source-level component* e'_S and show that it is logically related to e'_T. This is an onerous requirement: while it may be reasonable to come up with e'_S when the given e'_T is very simple, it seems almost impossible when e'_T consists of hundreds of lines of assembly! Further, if e'_T is compiled from some other source language R, it may not even be possible to write down an e'_S in language S that is related to e'_T.

Technically speaking, the BH approach does support linking with any target code that can be proved logically related to a source component. But it cannot support linking with any components that are not expressible in the source language. And we contend that even for the theoretically-allowed cases, in practice the approach is limited to allowing linking between only very simple components or components that were all compiled from the same source language.

Overcoming BH Limitations By reasoning about components in the FCA setting, we can overcome both limitations of the BH framework. We have already pointed out that our framework admits vertical compositionality thanks to the transitivity of contextual equivalence.

For the second limitation of the BH approach, consider a target component e'_{A}. While the BH approach would need to find a related source component to fit e'_{A} into their framework, we only need to find an FCA component that looks like a source component. Specifically, we can use e'_{A} itself in a source context by wrapping it in appropriate boundaries: $\mathcal{FCA}(\mathsf{e}'_{\mathsf{A}})$.

3 The Languages

We begin our technical development with a few notes on typesetting and notational conventions. We typeset the terms, types, and contexts of our various languages as follows:

- F (System F) in a blue sans-serif font;
- C (Closure conversion) in a **red bold font with serifs**;
- A (Allocation) in a **purple sans-serif bold font**.

For each of our languages, we will use the metavariable e for *components* and t for *terms*. In the first two languages, F and C, terms and components coincide, but the distinction will be meaningful in language A. Similarly, all languages use τ for types, v for values, E for evaluation contexts, and C for general contexts. We write $\mathrm{fv}(e)$ to denote the free term variables of e and $\mathrm{ftv}(e)$ (or $\mathrm{ftv}(\tau)$) to denote the free type variables of e (or of type τ). We use a line above a syntactic element to indicate a list of repeated instances of this element, e.g., $\overline{\alpha} = \alpha_1, \ldots, \alpha_n$ for $n \geq 0$. When the arities of different lists are required to match up in a definition or inference rule, these constraints will usually be obvious from context. Whenever two environments (e.g. Δ or Γ or Ψ) are joined by a comma, this should be interpreted as a *disjoint* union.

$\tau ::= \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \forall[\overline{\alpha}].(\overline{\tau}) \to \tau \mid \langle \overline{\tau} \rangle \mid \exists \alpha.\tau \mid \mu\alpha.\tau$

$\mathsf{e} ::= \mathsf{t}$

$\mathsf{t} ::= \mathsf{x} \mid () \mid \mathsf{n} \mid \mathsf{t}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{t}\ \mathsf{t} \mid \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \mathsf{t}\,[\overline{\tau}]\,\overline{\mathsf{t}} \mid \langle \overline{\mathsf{t}} \rangle \mid \pi_i(\mathsf{t}) \mid \mathsf{pack}\langle \tau, \mathsf{t} \rangle\ \mathsf{as}\ \exists \alpha.\tau$
$\quad \mid \mathsf{unpack}\ \langle \alpha, \mathsf{x} \rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t} \mid \mathsf{unfold}\ \mathsf{t}$

$\mathsf{p} ::= + \mid - \mid *$

$\mathsf{v} ::= () \mid \mathsf{n} \mid \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \langle \overline{\mathsf{v}} \rangle \mid \mathsf{pack}\langle \tau, \mathsf{v} \rangle\ \mathsf{as}\ \exists \alpha.\tau \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v}$

$\mathsf{E} ::= [\cdot] \mid \mathsf{E}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{v}\ \mathsf{p}\ \mathsf{E} \mid \mathsf{if0}\ \mathsf{E}\ \mathsf{t}\ \mathsf{t} \mid \mathsf{E}\,[\overline{\tau}]\,\overline{\mathsf{t}} \mid \mathsf{v}\,[\overline{\tau}]\,\overline{\mathsf{v}}\,\mathsf{E}\,\overline{\mathsf{t}} \mid \ldots$

$\boxed{\mathsf{e} \longmapsto \mathsf{e}'}$ $\quad \mathsf{E}[\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t}\,[\overline{\tau'}]\,\overline{\mathsf{v}}] \longmapsto \mathsf{E}[\mathsf{t}[\overline{\tau'/\alpha}]\,[\overline{\mathsf{v}/\mathsf{x}}]] \quad \ldots$

$\boxed{\Delta; \Gamma \vdash \mathsf{e} : \tau}$ where $\Delta ::= \cdot \mid \Delta, \alpha$ and $\Gamma ::= \cdot \mid \Gamma, \mathsf{x}:\tau$

$\tau ::= \boldsymbol{\alpha} \mid \mathbf{unit} \mid \mathbf{int} \mid \forall[\overline{\alpha}].(\overline{\tau}) \to \tau \mid \langle \overline{\tau} \rangle \mid \exists \boldsymbol{\alpha}.\tau \mid \boldsymbol{\mu\alpha}.\tau$

$\mathbf{e} ::= \mathbf{t}$

$\mathbf{t} ::= \mathbf{x} \mid () \mid \mathbf{n} \mid \mathbf{t}\ \mathbf{p}\ \mathbf{t} \mid \mathbf{if0}\ \mathbf{t}\ \mathbf{t}\ \mathbf{t} \mid \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t} \mid \mathbf{t}\,[]\,\overline{\mathbf{t}} \mid \mathbf{t}[\tau] \mid \langle \overline{\mathbf{t}} \rangle \mid \pi_i(\mathbf{t})$
$\quad \mid \mathbf{pack}\langle \tau, \mathbf{t} \rangle\ \mathbf{as}\ \exists \boldsymbol{\alpha}.\tau \mid \mathbf{unpack}\ \langle \alpha, \mathbf{x} \rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t} \mid \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{t} \mid \mathbf{unfold}\ \mathbf{t}$

$\mathbf{p} ::= + \mid - \mid *$

$\mathbf{v} ::= () \mid \mathbf{n} \mid \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t} \mid \langle \overline{\mathbf{v}} \rangle \mid \mathbf{pack}\langle \tau, \mathbf{v} \rangle\ \mathbf{as}\ \exists \boldsymbol{\alpha}.\tau \mid \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{v} \mid \mathbf{v}[\tau]$

$\mathbf{E} ::= [\cdot] \mid \ldots \mid \mathbf{E}\,[]\,\overline{\mathbf{t}} \mid \mathbf{v}\,[\overline{\tau}]\,\overline{\mathbf{v}}\,\mathbf{E}\,\overline{\mathbf{t}} \mid \mathbf{E}[\tau] \mid \ldots$

$\boxed{\mathbf{e} \longmapsto \mathbf{e}'}$ $\quad \mathbf{E}[\boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t}\,[\overline{\tau'}]\,\overline{\mathbf{v}}] \longmapsto \mathbf{E}[\mathbf{t}[\overline{\tau'/\alpha}]\,[\overline{\mathbf{v}/\mathbf{x}}]] \quad \ldots$

$\boxed{\Delta; \Gamma \vdash \mathbf{e} : \tau}$ where $\Delta ::= \cdot \mid \Delta, \alpha$ and $\Gamma ::= \cdot \mid \Gamma, \mathbf{x}:\tau$

$$\frac{\overline{\alpha}; \overline{\mathbf{x}:\tau} \vdash \mathbf{t} : \tau'}{\Delta; \Gamma \vdash \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'} \qquad \frac{\Delta; \Gamma \vdash \mathbf{t} : \forall[].(\overline{\tau}) \to \tau' \qquad \Delta; \Gamma \vdash \overline{\mathbf{t}} : \overline{\tau}}{\Delta; \Gamma \vdash \mathbf{t}\,[]\,\overline{\mathbf{t}} : \tau'}$$

$$\frac{\Delta; \Gamma \vdash \mathbf{t} : \forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau' \qquad \Delta \vdash \tau_0}{\Delta; \Gamma \vdash \mathbf{t}[\tau_0] : \forall[\overline{\alpha}].(\overline{\tau[\tau_0/\beta]}) \to \tau'[\tau_0/\beta]} \quad \ldots$$

$\tau ::= \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \exists \alpha.\tau \mid \mu\alpha.\tau \mid \mathsf{ref}\ \psi \mid \mathsf{box}\ \psi$

$\psi ::= \forall[\overline{\alpha}].(\overline{\tau}) \to \tau \mid \langle \tau, \ldots, \tau \rangle$

$\mathsf{e} ::= (\mathsf{t}, \mathsf{H})$

$\mathsf{t} ::= \mathsf{x} \mid () \mid \mathsf{n} \mid \mathsf{t}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{t}\ \mathsf{t} \mid \ell \mid \mathsf{t}\,[]\,\overline{\mathsf{t}} \mid \mathsf{t}[\tau] \mid \mathsf{pack}\langle \tau, \mathsf{t} \rangle\ \mathsf{as}\ \exists \alpha.\tau \mid \mathsf{unpack}\ \langle \alpha, \mathsf{x} \rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t}$
$\quad \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t} \mid \mathsf{unfold}\ \mathsf{t} \mid \mathsf{ralloc}\ \langle \overline{\mathsf{t}} \rangle \mid \mathsf{balloc}\ \langle \overline{\mathsf{t}} \rangle \mid \mathsf{read}[\mathsf{i}]\ \mathsf{t} \mid \mathsf{write}\ \mathsf{t}\ [\mathsf{i}] \leftarrow \mathsf{t}$

$\mathsf{p} ::= + \mid - \mid *$

$\mathsf{v} ::= () \mid \mathsf{n} \mid \mathsf{pack}\langle \tau, \mathsf{v} \rangle\ \mathsf{as}\ \exists \alpha.\tau \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v} \mid \ell \mid \mathsf{v}[\tau]$

$\mathsf{E} ::= (\mathsf{E}_t, \cdot) \qquad \mathsf{E}_t ::= [\cdot] \mid \ldots \mid \mathsf{balloc}\ \langle \overline{\mathsf{v}}, \mathsf{E}_t, \overline{\mathsf{t}} \rangle \mid \ldots$

$\mathsf{h} ::= \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \langle \mathsf{v}, \ldots, \mathsf{v} \rangle \qquad \mathsf{H} ::= \cdot \mid \mathsf{H}, \ell \mapsto \mathsf{h}$

$\boxed{\langle \mathsf{H} \mid \mathsf{e} \rangle \longmapsto \langle \mathsf{H}' \mid \mathsf{e}' \rangle}$ Reduction Relation (selected cases)

$$\langle \mathsf{H} \mid (\mathsf{t}, (\mathsf{H}', \ell \mapsto \mathsf{h})) \rangle \longmapsto \langle \mathsf{H}, \ell' \mapsto \mathsf{h} \mid (\mathsf{t}[\ell'/\ell], \mathsf{H}'[\ell'/\ell]) \rangle \quad \text{if } \ell' \notin \mathrm{dom}(\mathsf{H})$$

$$\langle \mathsf{H} \mid \mathsf{E}[\ell\,[\overline{\tau'}]\,\overline{\mathsf{v}}] \rangle \longmapsto \langle \mathsf{H} \mid \mathsf{E}[\mathsf{t}[\overline{\tau'/\alpha}][\overline{\mathsf{v}/\mathsf{x}}]] \rangle \quad \text{if } \mathsf{H}(\ell) = \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t}$$

$\boxed{\Psi \vdash \mathsf{h} : \psi}$ where $\Psi ::= \cdot \mid \Psi, \ell : {}^{\mathsf{ref}}\psi \mid \Psi, \ell : {}^{\mathsf{box}}\psi$

$\boxed{\Psi \vdash \mathsf{H} : \Psi'}$ which implies $\mathrm{dom}(\Psi) \cap \mathrm{dom}(\Psi') = \emptyset$

$\boxed{\Psi; \Delta; \Gamma \vdash \mathsf{e} : \tau}$ where $\Delta ::= \cdot \mid \Delta, \alpha$ and $\Gamma ::= \cdot \mid \Gamma, \mathsf{x}:\tau$

$$\frac{\Psi \vdash \mathsf{H} : \Psi' \qquad (\Psi, \Psi'); \Delta; \Gamma \vdash \mathsf{t} : \tau}{\Psi; \Delta; \Gamma \vdash (\mathsf{t}, \mathsf{H}) : \tau} \quad \ldots$$

$$\frac{\Psi; \Delta; \Gamma \vdash \overline{\mathsf{t}} : \overline{\tau}}{\Psi; \Delta; \Gamma \vdash \mathsf{balloc}\ \langle \overline{\mathsf{t}} \rangle : \mathsf{box}\ \langle \overline{\tau} \rangle} \qquad \frac{\Psi; \Delta; \Gamma \vdash \mathsf{t} : \mathsf{box}\ \langle \tau_0, \ldots \tau_i \ldots, \tau_n \rangle}{\Psi; \Delta; \Gamma \vdash \mathsf{read}[\mathsf{i}]\ \mathsf{t} : \tau_i}$$

Fig. 1. Definition of F (top), C (middle), and A (bottom)

Source Language Our source language F is System F with recursive types, existential types, and tuples. The syntax of types and terms in F is shown in Figure 1 (top). We combine type- and term-level abstractions of arbitrary arity into a single binding form $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$, abbreviating $\forall[].(\overline{\tau}) \to \tau'$ as $\overline{\tau} \to \tau'$. We define a small-step operational semantics for F (written $\mathsf{e} \longmapsto \mathsf{e}'$) using evaluation contexts E to lift the primitive reductions to a standard left-to-right call-by-value semantics for the language. The reduction rules are standard; we show only the application rule.

F's typing judgment has the form $\Delta; \Gamma \vdash \mathsf{e} : \tau$. The type environment Δ tracks the type variables in scope. The value environment Γ tracks the term variables in scope along with their types τ, which must be well formed under Δ (written $\Delta \vdash \tau$ and defined as $\mathrm{ftv}(\tau) \subseteq \Delta$). The typing rules are standard and hence omitted.

Intermediate Language Our intermediate language C, shown in Figure 1 (middle), is nearly identical to F, with two exceptions. First, since this language is the target of closure conversion, functions are not allowed to contain free type or term variables. Second, we allow the partial application of a function to a type. Hence, C terms include $\mathbf{t}[\boldsymbol{\tau}]$ and we consider $\mathbf{v}[\boldsymbol{\tau}]$ to be a value.

The reduction relation $\mathbf{e} \longmapsto \mathbf{e}'$ is identical to that of F, and the typing judgment $\boldsymbol{\Delta}; \boldsymbol{\Gamma} \vdash \mathbf{e} : \boldsymbol{\tau}$ differs only in the rules for abstraction and application which are shown in the figure. Note that the body of a C function must typecheck in an environment that contains only the function's formal arguments.

Target Language Our target A must serve as a target for heap allocation. Its design is similar to the language λ^A from [12]. Since we are compiling a source language without mutable references, it would suffice for A to provide only immutable references to functions and tuples that must now live on the heap. However, to provide a concrete illustration of the ability to link with target code that cannot be expressed in the source language, we augment A with mutable references to tuples.

The language A is shown in Figure 1 (bottom). Functions in A are stored only in immutable cells on the heap, while tuples are stored in heap cells that can be either mutable or immutable. We use ψ for the types of these *heap values* h. Mutable and immutable references have types $\mathsf{ref}\ \psi$ and $\mathsf{box}\ \psi$, respectively. The terms $\mathsf{ralloc}\ \langle \overline{\mathsf{t}} \rangle$ and $\mathsf{balloc}\ \langle \overline{\mathsf{t}} \rangle$—which allocate mutable and immutable cells, respectively—each allocate a new location ℓ and initialize it to the given tuple. The instructions $\mathsf{read}[\mathsf{i}]\ \ell$ and $\mathsf{write}\ \ell\ [\mathsf{i}] \leftarrow \mathsf{v}$ respectively read from and write the value v to the i-th slot in the tuple (of length n) stored at ℓ, assuming $\mathsf{0} \leq \mathsf{i} < \mathsf{n}$. The type system ensures that writes are only performed on mutable tuples.

Unlike F and C, the syntax of A distinguishes components e from terms t. A component e pairs a term t with a *heap fragment* H. H can contain functions and tuples that t may use by referring to locations in H. Intuitively, we need this notion of components because a bare term t is not as expressive as C component. In particular, A does not provide any way to dynamically allocate a location and initialize it to a function. We discuss how the compiler produces components with heap fragments in §4.

Heap fragments are assigned heap types Ψ. A heap fragment may reference locations that are to be linked in by another component, so the judgment $\Psi \vdash \mathsf{H} : \Psi'$ includes an external heap type Ψ as an environment used in assigning H the type Ψ'. Here, Ψ' must provide types for exactly the locations in H. Each h in H must typecheck

under the disjoint union of the two heap types (Ψ, Ψ'). Similarly, a component (t, H) can reference both external locations and those bound by H, that is, locations in the domain of either the external heap type Ψ or of H.

Our operational semantics for A is a relation between configurations $\langle H \mid e \rangle$. Any code or data in the internal heap fragment of component e must be loaded into memory before it can be run. We formally capture this with a reduction rule that "loads" a component by merging its internal heap fragment with the external heap. When loading a component (t, H), we must rename the locations bound in H so that they do not conflict with the external heap. After the loading step, the term component t can be evaluated using standard reduction rules.

The structure of A components also entails a small change to the structure of evaluation contexts, which are defined in two layers: contexts E expect components e, and term contexts E_t expect terms t. Terms are plugged into term contexts in the obvious way. Plugging a component-level evaluation context $E = (E_t, \cdot)$ with a component e is defined by $(E_t, \cdot)[(t, H)] = (E_t[t], H)$

4 The Compiler

Compiling F *to* C Closure conversion collects a function's free term variables in a tuple called the *closure environment* that is passed as an additional argument to the function, thus turning the function into a closed term. The closed function is paired with its environment to create a *closure*. The basic idea of typed closure conversion goes back to Minamide *et al.* [13], whom we follow in using an existential type to abstract the type of the environment. This ensures that two functions with the same type but different free variables still have the same type after closure conversion: the abstract type hides the fact that the closures' environments have different types.

We must also rewrite functions to take their free type variables as additional arguments. However, instead of collecting these types in a type environment as Minamide *et al.* do, we follow Morrisett *et al.* [12] and directly substitute the types into the function. Like the latter, we adopt a *type-erasure* interpretation, which means that since all types are erased at run time the substitution of types into functions has no run-time effect.

Our closure-conversion pass compiles F terms of type τ to C terms of type $\tau^{\mathcal{C}}$. Figure 2 (top) presents the type translation $\tau^{\mathcal{C}}$ and some of the compilation rules. Since this is closure conversion, the only interesting parts are those that involve functions. The omitted rules are defined by structural recursion on terms.

Compiling C *to* A Our second compiler pass combines hoisting of functions with explicit allocation of tuples. It takes a C component (that is, just a C term t) of type τ, and produces an A term t as well as a heap fragment H with all the hoisted functions. The component (t, H) is the overall output, and has type $\tau^{\mathcal{A}}$ under an empty external heap. The heap fragment generated by the compiler does not contain tuples: the compiler translates C tuples by generating **balloc** expressions, not by putting them in a static heap fragment. The type translation and interesting parts of the term translation are shown in Figure 2 (bottom).

5 F and C Interoperability

5.1 The Basics

We now present a formal semantics for interoperability between F and C. For now, we define a combined language FC; in §6, we will extend this to FCA. Our FC multi-

$\boxed{\tau^{\mathcal{C}}}$ Type Translation

$$\alpha^{\mathcal{C}} = \alpha \quad \mathsf{unit}^{\mathcal{C}} = \mathbf{unit} \quad \mathsf{int}^{\mathcal{C}} = \mathbf{int} \quad \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\mathcal{C}} = \exists\beta.\langle(\forall[\overline{\alpha}].(\beta, \overline{\tau^{\mathcal{C}}}) \to \tau'^{\mathcal{C}}), \beta\rangle$$

$$\exists\alpha.\tau^{\mathcal{C}} = \exists\alpha.\tau^{\mathcal{C}} \qquad \mu\alpha.\tau^{\mathcal{C}} = \mu\alpha.\tau^{\mathcal{C}} \qquad \langle\tau_1, \ldots, \tau_n\rangle^{\mathcal{C}} = \langle\tau_1{}^{\mathcal{C}}, \ldots, \tau_n{}^{\mathcal{C}}\rangle$$

$\boxed{\Delta; \Gamma \vdash \mathsf{e} : \tau \rightsquigarrow \mathbf{e}}$ Compiler (implies $\Delta^{\mathcal{C}}; \Gamma^{\mathcal{C}} \vdash \mathbf{e} : \tau^{\mathcal{C}}$)

$$\frac{\mathsf{x} : \tau \in \Gamma}{\Delta; \Gamma \vdash \mathsf{x} : \tau \rightsquigarrow \mathbf{x}} \qquad \frac{}{\Delta; \Gamma \vdash () : \mathsf{unit} \rightsquigarrow ()} \qquad \frac{}{\Delta; \Gamma \vdash \mathsf{n} : \mathsf{int} \rightsquigarrow \mathbf{n}}$$

$$\frac{\begin{array}{c}\mathsf{y}_1, \ldots, \mathsf{y}_m = \mathrm{fv}(\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t}) \qquad \beta_1, \ldots, \beta_k = \mathrm{ftv}(\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t}) \\ \Delta, \overline{\alpha}; \Gamma, \overline{\mathsf{x}:\tau} \vdash \mathsf{t} : \tau' \rightsquigarrow \mathbf{t} \qquad \tau_{\mathbf{env}} = \langle(\Gamma(\mathsf{y}_1))^{\mathcal{C}}, \ldots, (\Gamma(\mathsf{y}_m))^{\mathcal{C}}\rangle \\ \mathbf{v} = \boldsymbol{\lambda}[\overline{\beta}, \overline{\alpha}](\mathbf{z} : \tau_{\mathbf{env}}, \overline{\mathbf{x} : \tau^{\mathcal{C}}}).(\mathbf{t}[\pi_1(\mathbf{z})/\mathbf{y}_1] \cdots [\pi_m(\mathbf{z})/\mathbf{y}_m])\end{array}}{\begin{array}{l}\Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau' \rightsquigarrow \\ \qquad \mathbf{pack}\langle\tau_{\mathbf{env}}, \langle\mathbf{v}[\overline{\beta}], \langle\overline{\mathbf{y}}\rangle\rangle\rangle \ \mathbf{as}\ \exists\alpha'.\langle(\forall[\overline{\alpha}].(\alpha', \overline{\tau^{\mathcal{C}}}) \to \tau'^{\mathcal{C}}), \alpha'\rangle\end{array}}$$

$$\frac{\Delta; \Gamma \vdash \mathsf{t}_0 : \forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2 \rightsquigarrow \mathbf{t_0} \qquad \Delta \vdash \overline{\tau} \qquad \Delta; \Gamma \vdash \overline{\mathsf{t}} : \overline{\tau_1[\tau/\alpha]} \rightsquigarrow \overline{\mathbf{t}}}{\Delta; \Gamma \vdash \mathsf{t}_0\,[\overline{\tau}]\,\overline{\mathsf{t}} : \tau_2[\overline{\tau/\alpha}] \rightsquigarrow \mathbf{unpack}\,\langle\boldsymbol{\beta}, \mathbf{z}\rangle = \mathbf{t_0}\ \mathbf{in}\ \pi_1(\mathbf{z})\,[\overline{\tau^{\mathcal{C}}}]\,\pi_2(\mathbf{z}), \overline{\mathbf{t}}}$$

$\boxed{\tau^{\mathcal{A}}}$ Type Translation

$$\alpha^{\mathcal{A}} = \alpha \quad \mathbf{unit}^{\mathcal{A}} = \mathbf{unit} \quad \mathbf{int}^{\mathcal{A}} = \mathbf{int} \quad \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\mathcal{A}} = \mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau^{\mathcal{A}}}) \to \tau'^{\mathcal{A}}$$

$$\exists\alpha.\tau^{\mathcal{A}} = \exists\alpha.\tau^{\mathcal{A}} \qquad \mu\alpha.\tau^{\mathcal{A}} = \mu\alpha.\tau^{\mathcal{A}} \qquad \langle\tau_1, \ldots, \tau_n\rangle^{\mathcal{A}} = \mathbf{box}\,\langle(\tau_1{}^{\mathcal{A}}), \ldots (\tau_n{}^{\mathcal{A}})\rangle$$

$\boxed{\Delta; \Gamma \vdash \mathbf{e} : \tau \rightsquigarrow (\mathbf{t}, \mathbf{H} : \Psi)}$ Compiler (implies $\cdot \vdash \mathbf{H} : \Psi$, and $\cdot; \Delta^{\mathcal{A}}; \Gamma^{\mathcal{A}} \vdash (\mathbf{t}, \mathbf{H}) : \tau^{\mathcal{A}}$)

$$\frac{\mathbf{x} : \tau \in \Gamma}{\Delta; \Gamma \vdash \mathbf{x} : \tau \rightsquigarrow (\mathbf{x}, \cdot : \cdot)} \qquad \frac{}{\Delta; \Gamma \vdash () : \mathbf{unit} \rightsquigarrow ((), \cdot : \cdot)} \qquad \ldots$$

$$\frac{\overline{\alpha}; \overline{\mathbf{x} : \tau} \vdash \mathbf{t} : \tau' \rightsquigarrow (\mathbf{t}, \mathbf{H} : \Psi)}{\begin{array}{l}\Delta; \Gamma \vdash \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x} : \tau}).\mathbf{t} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau' \rightsquigarrow \\ \qquad (\ell, (\mathbf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x} : \tau^{\mathcal{A}}}).\mathbf{t}) : (\Psi, \ell : {}^{\mathbf{box}}\forall[\overline{\alpha}].(\overline{\tau^{\mathcal{A}}}) \to \tau'^{\mathcal{A}}))\end{array}}$$

$$\frac{\Delta; \Gamma \vdash \mathbf{t}_1 : \tau_1 \rightsquigarrow (\mathbf{t}_1, \mathbf{H}_1 : \Psi_1) \ \cdots \ \Delta; \Gamma \vdash \mathbf{t}_n : \tau_n \rightsquigarrow (\mathbf{t}_n, \mathbf{H}_n : \Psi_n)}{\begin{array}{l}\Delta; \Gamma \vdash \langle\mathbf{t}_1, \ldots, \mathbf{t}_n\rangle : \langle\tau_1, \ldots, \tau_n\rangle \rightsquigarrow \\ \qquad (\mathbf{balloc}\,\langle\mathbf{t}_1, \ldots, \mathbf{t}_n\rangle, (\mathbf{H}_1, \ldots, \mathbf{H}_n) : (\Psi_1, \ldots, \Psi_n))\end{array}}$$

Fig. 2. Compiler from F to C (top) and from C to A (bottom)

language system embeds the languages F and C so that both languages have natural access to foreign values (i.e., values from the other language). In particular, we want F components of type τ to be usable as C components of type $\tau^{\mathcal{C}}$, and vice versa. To allow cross-language communication, FC extends the original F and C with syntactic boundaries, written ${}^{\tau}\mathcal{FC}\,\mathbf{e}$ (C inside, F outside) and $\mathcal{CF}^{\tau}\,\mathsf{e}$ (F inside, C outside).

The interesting cases in the semantics of boundaries are those that handle universal and existential types. These must be defined carefully to ensure that type abstraction is not broken as values pass between languages. First, though, we explain the general principles of our boundary semantics by looking at the cases for simple types and their translations.

CF *Boundary Semantics* A term $\mathcal{CF}^{\tau}\mathsf{e}$ has type $\tau^{\mathcal{C}}$ if e has type τ. To evaluate this boundary term, CF's operational semantics require first that e be reduced to a value v (using F reduction rules). Then a type-directed meta-function is applied to v, yielding a value in C of type $\tau^{\mathcal{C}}$ (written $\mathbf{CF}^{\tau}(\mathsf{v}) = \mathbf{v}$). An important restriction on this meta-function, which we call the *value translation*, is that it is only defined for *closed* values. This is sufficient for our needs because it is used only by the FC operational semantics, and substitution-based reduction relations are defined only for closed programs. We can still write FC programs with free variables appearing under boundaries, but by the time we evaluate the boundary term, we will have supplied values for all of these free variables.

At base types, value translation is easy: for example, translating a value n of type int yields the same integer in C, $\mathbf{n}$. Most of the other types are translated simply by structural recursion.

The interesting case is the case for function types. Consider the translation of a value v of type $\tau \to \tau'$. As per the type translation, this should produce a value of type $\exists\beta.\langle((\beta, \tau^{\mathcal{C}}) \to \tau'^{\mathcal{C}}), \beta\rangle$. Since v is closed, we can simply use $\mathbf{unit}$ for the type β of the closure environment:

$$\mathbf{CF}^{\tau \to \tau'}(\mathsf{v}) = \mathbf{pack}\langle \mathbf{unit}, \langle \mathbf{v}, ()\rangle\rangle \ \mathbf{as}\ \exists\beta.\langle((\beta, \tau^{\mathcal{C}}) \to \tau'^{\mathcal{C}}), \beta\rangle$$

We must still construct the underlying function $\mathbf{v}$ for this closure, which we can do using boundary terms and the original function v:

$$\mathbf{v} = \boldsymbol{\lambda}(\mathbf{z} : \mathbf{unit}, \mathbf{x} : \tau^{\mathcal{C}}).\mathcal{CF}^{\tau'}(\mathsf{v}\ {}^{\tau}\mathcal{FC}\ \mathbf{x}).$$

The function we build simply translates its argument from C to F, applies v to the translated argument, and finally translates the result back into C.

The full translation rule for functions must also handle type arguments and requires some additional machinery, which we will discuss momentarily.

FC *Boundary Semantics* The term ${}^{\tau}\mathcal{FC}\ \mathbf{e}$ has type τ when $\mathbf{e}$ has type $\tau^{\mathcal{C}}$. As before, to evaluate a boundary term, we first evaluate the component under the boundary, this time to a value $\mathbf{v}$. Then we apply a value translation ${}^{\tau}\mathbf{FC}(\mathbf{v}) = \mathsf{v}$ that yields an F value v of type τ. Again, this translation is only defined for closed values of translation type.

Let us consider the type $\tau \to \tau'$ again. A closure $\mathbf{v}$ of type $(\tau \to \tau')^{\mathcal{C}}$ must be translated to an F function that first translates its argument from F to C, then unpacks the closure $\mathbf{v}$ and applies the code to its environment and the translated argument, and finally translates the result back from C to F:

$${}^{\tau \to \tau'}\mathbf{FC}(\mathbf{v}) = \lambda(\mathsf{x} : \tau).{}^{\tau'}\mathcal{FC}(\mathbf{unpack}\ \langle\beta, \mathbf{y}\rangle = \mathbf{v}\ \mathbf{in}\ \boldsymbol{\pi}_1(\mathbf{y})\ \boldsymbol{\pi}_2(\mathbf{y})\ \mathcal{CF}^{\tau}\mathsf{x})$$

In both function cases, notice that the direction of the conversion (and the boundary used) reverses for function arguments.

5.2 Handling Abstract Types

Now that we have established the general structure of boundary rules, we come to the interesting cases, those for abstract types.

FC *Type Abstraction* Consider the type $\forall[\alpha].(\alpha) \to \alpha$. Since $\alpha^{\mathcal{C}} = \boldsymbol{\alpha}$, the translation of this type is

$$(\forall[\alpha].(\alpha) \to \alpha)^{\mathcal{C}} = \exists\beta.\langle(\forall[\boldsymbol{\alpha}].(\beta, \boldsymbol{\alpha}) \to \boldsymbol{\alpha}), \beta\rangle.$$

If we naively try to extend the function case of the value translation given above, we get the following:

$$^{\forall[\alpha].(\alpha)\to\alpha}\mathbf{FC}(\mathbf{v}) = \lambda[\alpha](\mathsf{x}:\alpha).{}^{\alpha}\mathcal{FC}(\mathbf{unpack}\ \langle\beta,\mathbf{y}\rangle = \mathbf{v}\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{y})\ [\alpha^{\mathcal{C}}]\ \boldsymbol{\pi_2}(\mathbf{y})\ \mathcal{CF}^{\alpha}\mathsf{x})$$

Note that we have not expanded $\alpha^{\mathcal{C}}$ in the application produced by this translation. It would expand to a C type variable $\boldsymbol{\alpha}$, but we cannot allow this, because that $\boldsymbol{\alpha}$ would be unbound! What we really want is that when α is instantiated with a concrete type τ, the positions inside language C where that type is needed receive $\tau^{\mathcal{C}}$.

We resolve this by making two changes to our system: first, we add a type $\lceil\alpha\rceil$ (which may be read as "α suspended in C") that allows an F type variable to appear in a C type. The F type variable α needs to be translated, but the translation is *delayed* until α is instantiated with a concrete type. We enforce this semantics in the definition of type substitution: $\lceil\alpha\rceil[\tau/\alpha] = \tau^{\mathcal{C}}$.

Second, we adjust the type translation to turn F type variables into suspended type variables instead of C type variables. We call this modified version of the type translation the *boundary type translation*, and notate it by $\tau^{\langle\mathcal{C}\rangle}$. Formally, the rule for type variables in the compiler's type translation is replaced by the rule $\alpha^{\langle\mathcal{C}\rangle} = \lceil\alpha\rceil$ in the boundary type translation. We only want to suspend free type variables, so when we translate a type that contains bound variables, we need to restore the behavior of the compiler's type translation when we translate the binding position. We can do this using a substitution, e.g., $(\exists\alpha.\tau)^{\langle\mathcal{C}\rangle} = \exists\boldsymbol{\alpha}.(\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil])$. Thus the boundary type translation preserves the binding structure of the type to which it is applied.

With these two changes, we can correct the example above by replacing the appearance of $\alpha^{\mathcal{C}}$ with $\alpha^{\langle\mathcal{C}\rangle}$, and we get a sensible translation from C to F for values of type $(\forall[\alpha].(\alpha)\to\alpha)^{\mathcal{C}}$.

CF *Type Abstraction* Next, consider translating values of type $\forall[\alpha].(\alpha)\to\alpha$ from F into C. Once again, the existing machinery is not quite sufficient. Here is a naive attempt:

$$\mathbf{CF}^{\forall[\alpha].(\alpha)\to\alpha}(\mathsf{v}) = \mathbf{pack}\langle\mathbf{unit},\langle\mathbf{v},()\rangle\rangle\ \mathbf{as}\ (\forall[\alpha].(\alpha)\to\alpha)^{\langle\mathcal{C}\rangle}$$
$$\text{where } \mathbf{v} = \boldsymbol{\lambda}[\boldsymbol{\alpha}](\mathbf{z}:\mathbf{unit},\mathbf{x}:\boldsymbol{\alpha}).\mathcal{CF}^{\alpha}(\mathsf{v}\,[\alpha]\,{}^{\alpha}\mathcal{FC}\mathbf{x}).$$

This time, we have translated the binder for α into a C binder for $\boldsymbol{\alpha}$, but we are left with free occurrences of α in the result! This is not a suitable translation, as we must produce a closed value. Note that the boundary terms in the body of $\mathbf{v}$ expect to be annotated with a type that translates to $\boldsymbol{\alpha}$.

To fix this problem, we introduce a *lump type* $\mathsf{L}\langle\boldsymbol{\tau}\rangle$ that allows us to pass C values to F terms as opaque lumps. The introduction form for the lump type is the boundary term ${}^{\mathsf{L}\langle\tau\rangle}\mathcal{FC}\mathbf{e}$, and the elimination form is $\mathcal{CF}^{\mathsf{L}\langle\tau\rangle}\mathsf{e}$. A pair of opposite boundaries at lump type cancel, to yield the underlying C value. We extend the boundary type translation by defining $\mathsf{L}\langle\boldsymbol{\tau}\rangle^{\langle\mathcal{C}\rangle} = \boldsymbol{\tau}$.

Now the three free occurrences of α in $\mathbf{v}$ can be replaced with $\mathsf{L}\langle\boldsymbol{\alpha}\rangle$, yielding a well-typed translation.

Summary With the additional tools of lumps, suspensions, and the boundary type translation, we have now developed everything needed for the FC multi-language system. Figure 3 presents more of the details, including the complete value translations.

$\tau ::= \cdots \mid \mathsf{L}\langle\boldsymbol{\tau}\rangle$ $\quad \boldsymbol{\tau} ::= \cdots \mid \lceil\alpha\rceil$ $\quad \tau ::= \tau \mid \boldsymbol{\tau}$

$\mathsf{t} ::= \cdots \mid {}^{\tau}\mathcal{FC}\,\mathsf{e}$ $\quad \mathsf{t} ::= \cdots \mid \mathcal{CF}^{\tau}\mathsf{e}$ $\quad e ::= \mathsf{e} \mid \mathbf{e}$

$\mathsf{v} ::= \cdots \mid {}^{\mathsf{L}\langle\tau\rangle}\mathcal{FC}\mathbf{v}$ $\quad \mathbf{v} ::= \cdots$ $\quad v ::= \mathsf{v} \mid \mathbf{v}$ $\quad \Delta ::= \cdot \mid \Delta, \alpha \mid \Delta, \boldsymbol{\alpha}$

$\mathsf{E} ::= \cdots \mid {}^{\tau}\mathcal{FC}\,\mathbf{E}$ $\quad \mathbf{E} ::= \cdots \mid \mathcal{CF}^{\tau}\mathsf{E}$ $\quad E ::= \mathsf{E} \mid \mathbf{E}$ $\quad \Gamma ::= \cdot \mid \Gamma, \mathsf{x}:\tau \mid \Gamma, \mathbf{x}:\boldsymbol{\tau}$

$\boxed{\tau^{\langle\mathcal{C}\rangle}}$ Boundary Type Translation

$$\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle\mathcal{C}\rangle} = \exists\boldsymbol{\beta}.\langle\left(\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\beta}, \overline{\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]}) \to \tau'^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]\right), \boldsymbol{\beta}\rangle$$

$$\alpha^{\langle\mathcal{C}\rangle} = \lceil\alpha\rceil \qquad \mathsf{unit}^{\langle\mathcal{C}\rangle} = \mathbf{unit} \qquad \mathsf{int}^{\langle\mathcal{C}\rangle} = \mathbf{int} \qquad \exists\alpha.\tau^{\langle\mathcal{C}\rangle} = \exists\boldsymbol{\alpha}.(\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil])$$

$$\mu\alpha.\tau^{\langle\mathcal{C}\rangle} = \boldsymbol{\mu\alpha}.(\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]) \qquad \langle\overline{\tau}\rangle^{\langle\mathcal{C}\rangle} = \langle\overline{\tau^{\langle\mathcal{C}\rangle}}\rangle \qquad \mathsf{L}\langle\boldsymbol{\tau}\rangle^{\langle\mathcal{C}\rangle} = \boldsymbol{\tau}$$

Type Substitution: $\lceil\alpha\rceil[\tau/\alpha] = \tau^{\langle\mathcal{C}\rangle}$

$\boxed{\Delta;\Gamma \vdash e:\tau}$ Include F and C rules, with environments replaced by $\Delta;\Gamma$

$$\frac{\Delta;\Gamma \vdash \mathbf{e}:\tau^{\langle\mathcal{C}\rangle}}{\Delta;\Gamma \vdash {}^{\tau}\mathcal{FC}\,\mathbf{e}:\tau} \qquad \frac{\Delta;\Gamma \vdash \mathsf{e}:\tau}{\Delta;\Gamma \vdash \mathcal{CF}^{\tau}\mathsf{e}:\tau^{\langle\mathcal{C}\rangle}}$$

$\boxed{\mathbf{CF}^{\tau}(\mathsf{v}) = \mathbf{v}}$ Value Translation $\quad \mathbf{CF}^{\mathsf{unit}}(()) = () \quad \mathbf{CF}^{\mathsf{int}}(\mathsf{n}) = \mathbf{n} \quad \mathbf{CF}^{\mathsf{L}\langle\tau\rangle}({}^{\mathsf{L}\langle\tau\rangle}\mathcal{FC}\mathbf{v}) = \mathbf{v}$

$$\mathbf{CF}^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}(\mathsf{v}) = \mathbf{pack}\langle\mathbf{unit}, \langle\mathbf{v}, ()\rangle\rangle\ \mathbf{as}\ (\forall[\overline{\alpha}].(\overline{\tau}) \to \tau')^{\langle\mathcal{C}\rangle}$$

$$\text{where } \mathbf{v} = \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\mathbf{z}:\mathbf{unit}, \overline{\mathbf{x}:\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]}).\mathcal{CF}^{\tau'[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}(\mathsf{v}\,[\overline{\mathsf{L}\langle\boldsymbol{\alpha}\rangle}])\ \overline{\tau[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]\mathcal{FC}\mathbf{x}})$$

$$\mathbf{CF}^{\exists\alpha.\tau}(\mathsf{pack}\langle\tau',\mathsf{v}\rangle\ \mathsf{as}\ \exists\alpha.\tau) = \mathbf{pack}\langle\tau'^{\langle\mathcal{C}\rangle},\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\tau^{\langle\mathcal{C}\rangle} \qquad \text{where } \mathbf{CF}^{\tau[\tau'/\alpha]}(\mathsf{v}) = \mathbf{v}$$

$$\mathbf{CF}^{\mu\alpha.\tau}(\mathsf{fold}_{\mu\alpha.\tau}\mathsf{v}) = \mathbf{fold}_{\mu\alpha.\tau^{\langle\mathcal{C}\rangle}}\mathbf{v} \qquad \text{where } \mathbf{CF}^{\tau[\mu\alpha.\tau/\alpha]}(\mathsf{v}) = \mathbf{v}$$

$$\mathbf{CF}^{\langle\tau_1,\ldots,\tau_n\rangle}(\langle\mathsf{v}_1,\ldots,\mathsf{v}_n\rangle) = \langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle \qquad \text{where } \mathbf{CF}^{\tau_i}(\mathsf{v}_i) = \mathbf{v_i}$$

$\boxed{{}^{\tau}\mathbf{FC}(\mathbf{v}) = \mathsf{v}}$ Value Translation $\quad {}^{\mathsf{unit}}\mathbf{FC}(()) = () \quad {}^{\mathsf{int}}\mathbf{FC}(\mathbf{n}) = \mathsf{n} \quad {}^{\mathsf{L}\langle\tau\rangle}\mathbf{FC}(\mathbf{v}) = {}^{\mathsf{L}\langle\tau\rangle}\mathcal{FC}\mathbf{v}$

$${}^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}\mathbf{FC}(\mathbf{v}) = \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).{}^{\tau'}\mathcal{FC}(\mathbf{unpack}\ \langle\boldsymbol{\beta},\mathbf{y}\rangle = \mathbf{v}\ \mathbf{in}\ \boldsymbol{\pi}_1(\mathbf{y})\ [\overline{\lceil\alpha\rceil}]\ \boldsymbol{\pi}_2(\mathbf{y}), \overline{\mathcal{CF}^{\tau}\mathsf{x}})$$

$${}^{\exists\alpha.\tau}\mathbf{FC}(\mathbf{pack}\langle\boldsymbol{\tau}',\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\tau^{\langle\mathcal{C}\rangle}) = \mathsf{pack}\langle\mathsf{L}\langle\boldsymbol{\tau}'\rangle,\mathsf{v}\rangle\ \mathsf{as}\ \exists\alpha.\tau \qquad \text{where } {}^{\tau[\mathsf{L}\langle\tau'\rangle/\alpha]}\mathbf{FC}(\mathbf{v}) = \mathsf{v}$$

$${}^{\mu\alpha.\tau}\mathbf{FC}(\mathbf{fold}_{\mu\alpha.\tau^{\langle\mathcal{C}\rangle}}\ \mathbf{v}) = \mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{v} \qquad \text{where } {}^{\tau[\mu\alpha.\tau/\alpha]}\mathbf{FC}(\mathbf{v}) = \mathsf{v}$$

$${}^{\langle\tau_1,\ldots,\tau_n\rangle}\mathbf{FC}(\langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle) = \langle\mathsf{v}_1,\ldots,\mathsf{v}_n\rangle \qquad \text{where } {}^{\tau_i}\mathbf{FC}(\mathbf{v_i}) = \mathsf{v}_i$$

$\boxed{e \longmapsto e'}$ Include F and C rules, replacing eval. contexts E, $\mathbf{E}$ with E.

$$\frac{\mathbf{CF}^{\tau}(\mathsf{v}) = \mathbf{v}}{E[\mathcal{CF}^{\tau}\mathsf{v}] \longmapsto E[\mathbf{v}]} \qquad \frac{{}^{\tau}\mathbf{FC}(\mathbf{v}) = \mathsf{v} \qquad \tau \neq \mathsf{L}\langle\tau\rangle}{E[{}^{\tau}\mathcal{FC}\mathbf{v}] \longmapsto E[\mathsf{v}]}$$

Fig. 3. FC multi-language system (extends F and C from Figure 1)

The syntax of FC simply combines the syntax of F with that of C, and adds boundaries, lumps, and suspensions. The type judgment combines the type rules for F and C, but with the environments replaced by environments that can contain variables from both languages. We also add rules to typecheck boundary terms.

The cases of the value translations we have not yet covered mostly proceed by structural recursion, but note that the cases for existential types need to make use of lumps and suspensions (the suspensions are introduced by the boundary type translation) in ways that are dual to the function cases.

The reduction relation combines the reduction rules from F and C and adds rules for boundaries. The boundary reduction rules use the value translations to produce a value in the other language.

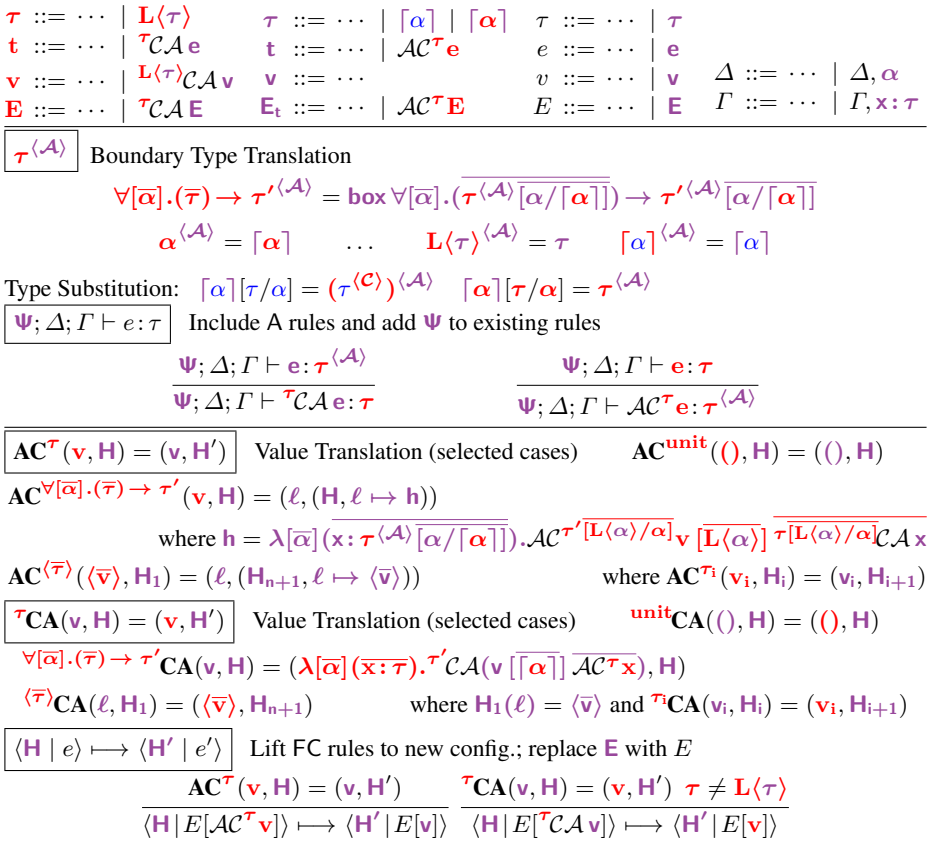

Fig. 4. FCA multi-language system (extends Figures 1 and 3)

6 C and A Interoperability

The extensions to FC for interoperability with A are given in Figure 4. The principles discussed in the development of FC still apply, but here we need to handle the presence of the heap. Specifically, since functions and tuples in A are contained in the heap, the value translations need access to the program's memory. Going from C to A, the value translation may allocate new memory for functions and tuples; going from A to C requires looking up the contents of locations and translating those contents to functions or tuples in C. Thus, we pass the current memory as an argument to the translations, and return a memory that may have had additional locations allocated. Memory cells allocated by boundaries are always immutable.

Aside from this change, the extension for the new language mostly follows what we did for FC: we augment the syntax with boundaries between C and A, a lump type $\mathbf{L}\langle\tau\rangle$ for opaquely embedding A values into C, and suspensions of type variables into A. Note that we need the boundary type translation from C to A to handle both C type variables $\boldsymbol{\alpha}$ and suspended F type variables $\lceil\alpha\rceil$. Thus A has both $\lceil\alpha\rceil$ and $\lceil\boldsymbol{\alpha}\rceil$ as suspension types. The boundary type translation $\boldsymbol{\tau}^{\langle\mathcal{A}\rangle}$ works similarly to $\tau^{\langle\mathcal{C}\rangle}$. The figure shows

$$
\begin{array}{rcl}
\mathsf{C} & ::= & [\cdot] \mid \mathsf{C}\ \mathsf{p}\ \mathsf{t} \mid \cdots \mid \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{C} \mid \cdots \mid {}^{\tau}\mathcal{FC}\ \mathbf{C} \\
\mathbf{C} & ::= & [\cdot] \mid \cdots \mid \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{C} \mid \cdots \mid \mathcal{CF}^{\tau}\mathsf{C} \mid {}^{\tau}\mathcal{CA}\ \mathbf{C} \\
\mathsf{C} & ::= & (\mathsf{C_t}, \mathsf{H}) \mid (\mathsf{t}, \mathsf{C_H}) \\
\mathsf{C_t} & ::= & [\cdot] \mid \cdots \mid \mathcal{AC}^{\tau}\mathbf{C} \qquad \mathsf{C_H} ::= \mathsf{C_H}, \ell \mapsto \mathsf{h} \mid \mathsf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathsf{C_t} \\
C & ::= & \mathsf{C} \mid \mathbf{C} \mid \mathbf{C}
\end{array}
$$

$\boxed{C[e]}$ Context Plugging (A cases shown)

$$
(\mathsf{C_t}, \mathsf{H})[e] = \begin{cases} (\mathsf{C_t}[\mathsf{t}], (\mathsf{H}, \mathsf{H}')) & e = (\mathsf{t}, \mathsf{H}') \ \wedge\ \mathsf{C_t} \text{ contains no language boundaries} \\ (\mathsf{C_t}[e], \mathsf{H}) & \text{otherwise} \end{cases}
$$

$$
(\mathsf{t}, \mathsf{C_H})[e] = \begin{cases} (\mathsf{t}, (\mathsf{C_H}[\mathsf{t}'], \mathsf{H}')) & e = (\mathsf{t}', \mathsf{H}') \ \wedge\ \mathsf{C_H} \text{ contains no language boundaries} \\ (\mathsf{t}, \mathsf{C_H}[e]) & \text{otherwise} \end{cases}
$$

$$
[\cdot][\mathsf{t}] = \mathsf{t} \qquad (\mathsf{C_t}\ \mathsf{p}\ \mathsf{t})[e] = (\mathsf{C_t}[e])\ \mathsf{p}\ \mathsf{t} \qquad \cdots
$$

$$
(\mathsf{C_H}, \ell \mapsto \mathsf{h})[e] = (\mathsf{C_H}[e]), \ell \mapsto \mathsf{h}
$$

$$
(\mathsf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathsf{C_t})[e] = \mathsf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).(\mathsf{C_t}[e])
$$

$\boxed{\vdash C : (\boldsymbol{\Psi}; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\boldsymbol{\Psi}'; \Delta'; \Gamma' \vdash \tau')}$ Context Typing (omitted)

Contextual Equivalence

$$
\begin{aligned}
\boldsymbol{\Psi}; \Delta; \Gamma \vdash e_1 \approx^{ctx} e_2 : \tau \stackrel{\text{def}}{=} \boldsymbol{\Psi}; \Delta; \Gamma \vdash e_1 : \tau \ \wedge\ \boldsymbol{\Psi}; \Delta; \Gamma \vdash e_2 : \tau \ \wedge \\
\forall C, \mathsf{H}, \boldsymbol{\Psi}', \tau'. \vdash C : (\boldsymbol{\Psi}; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\boldsymbol{\Psi}'; \cdot; \cdot \vdash \tau') \ \wedge\ \vdash \mathsf{H} : \boldsymbol{\Psi}' \\
\implies (\langle \mathsf{H} \mid C[e_1] \rangle \downarrow \iff \langle \mathsf{H} \mid C[e_2] \rangle \downarrow)
\end{aligned}
$$

Fig. 5. General Contexts & Contextual Equivalence for FCA

the function case and the cases involving lumps and suspensions. The type judgment merges the A type rules with the FC type rules, but where the latter are modified to add the extra environment $\boldsymbol{\Psi}$, and adds type rules for boundaries. Finally, the reduction relation for FCA lifts the FC reductions to use the configuration from A, with a program heap. We also add the reduction rules from A and a pair of boundary reduction rules that utilize the value translations.

7 Compiler Correctness

As mentioned in §1, we state compiler correctness in terms of FCA contextual equivalence. Below, we formally define contextual equivalence for FCA components and then present our compiler correctness theorems. We discuss how to prove these theorems in §9 and give a longer discussion and the full proofs in the appendices.

7.1 FCA Contextual Equivalence

A general context C is an FCA component with a hole. A component e can be plugged into the context only if it is from the same language as the hole. Since contexts can contain boundaries, e need not be from the same language as the outermost layer of C. The syntax of general contexts is given in Figure 5 (top). Contexts for F and C forms are standard. In A, we need contexts to be able to have their hole in either the term part of a component, or in the body of a function contained in the heap fragment. So in addition to contexts C that produce components, we have context forms $\mathsf{C_t}$ and $\mathsf{C_H}$ that produce terms and heap fragments, respectively.

When plugging an A component $(\mathbf{t}, \mathbf{H})$ into a context C, the heap fragment $\mathbf{H}$ is placed at the innermost component-level layer of C—that is, at the language boundary closest to the hole—and merged with the heap fragment already in that position. To formalize this, the A portion of the definition of plugging a component into a context is given in Figure 5 (middle). The definition of plugging for F and C contexts is standard.

Given this notion of general contexts, contextual equivalence for FCA is standard (see Figure 5, bottom). It says that two components e_1 and e_2 are contextually equivalent under environments $\mathbf{\Psi}$, Δ, Γ and at type τ if the following hold: First, both components must typecheck under $\mathbf{\Psi}$, Δ, Γ at type τ. Second, if C is a context that expects to be given a component that typechecks under $\mathbf{\Psi}$, Δ, Γ at type τ, and produces a resulting program that is closed but expects to be run with a heap of type $\mathbf{\Psi'}$, then $C[e_1]$ and $C[e_2]$ have the same termination behavior when we run them with any initial heap $\mathbf{H}$ that has type $\mathbf{\Psi'}$.

7.2 Compiler Correctness

We can now state our main result: compiler-correctness theorems for both passes of our compiler.

Theorem 1 (Closure Conversion is Semantics-Preserving). *If* $\overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e}:\tau \rightsquigarrow \mathbf{e}$, *then* $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e} \approx^{ctx} {}^{\tau}\mathcal{FC}(\mathbf{e}[\overline{\lceil\alpha\rceil/\boldsymbol{\alpha}}]\ \overline{[\mathcal{CF}^{\tau'}\mathsf{x}/\mathsf{x}]}) : \tau$.

Theorem 2 (Allocation is Semantics-Preserving). *If* $\overline{\boldsymbol{\alpha}}; \overline{\mathbf{x}:\boldsymbol{\tau'}} \vdash \mathbf{e}:\boldsymbol{\tau} \rightsquigarrow (\mathbf{t}, \mathbf{H}:\mathbf{\Psi})$, *then* $\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x}:\boldsymbol{\tau'}} \vdash \mathbf{e} \approx^{ctx} {}^{\tau}\mathcal{CA}(\mathbf{t}[\overline{\lceil\boldsymbol{\alpha}\rceil/\alpha}]\ \overline{[\mathcal{AC}^{\boldsymbol{\tau'}}\mathbf{x}/\mathsf{x}]}, \mathbf{H}) : \boldsymbol{\tau}$.

The formal theorems are essentially as we described our compiler correctness results in §1, with only one additional subtlety: we need to perform a substitution so that the free variables of the original component match those of the compiled component. Recall that the compiler turns free type and term variables α and x into type and term variables $\boldsymbol{\alpha}$ and $\mathbf{x}$ from the next language, whereas FCA needs the binding structure of components to be preserved, including free variables being in the language prescribed by the type environments Δ and Γ. To get the free variables of the two components back into sync, we substitute suspended type variables for translated type variables, and we substitute boundary terms for translated term variables. Note that we do not need to perform a substitution in the heap fragment produced by the allocation pass, since heap values must be closed anyway.

We could equivalently have stated these theorems with the substitution on the other side, and the environments correspondingly translated; e.g.

$$\cdot; \overline{\alpha}^{\mathcal{C}}; \overline{\mathsf{x}:\tau'^{\mathcal{C}}} \vdash \mathsf{e}\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}\ \overline{[\hat{\tau}'\mathcal{FC}\mathbf{x}/\mathsf{x}]} \approx^{ctx} {}^{\hat{\tau}}\mathcal{FC}\,\mathbf{e} : \hat{\tau},$$

where $\hat{\tau} = \tau\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}$ and $\hat{\tau}' = \tau'\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}$.

It also does not matter which side the boundary term is placed on: boundary cancellation lemmas allow us to prove as a corollary that, for example,

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau} \vdash \mathcal{F}^{\tau}\mathsf{e} \approx^{ctx} \mathbf{e}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\ \overline{[\mathcal{CF}^{\tau'}\mathsf{x}/\mathsf{x}]} : \tau^{\langle\mathcal{C}\rangle}.$$

Since we want to ensure that type variables in the environment remain tied to their free occurrences in the result type, this version of the theorem uses the boundary type translation $\tau^{\langle\mathcal{C}\rangle}$ for the result type (instead of the compiler's type translation $\tau^{\mathcal{C}}$).

Contextual equivalence is transitive, so we can easily chain these theorems together to prove correctness for the full compiler:

Corollary 1 (Compiler Correctness). *If* $\overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e}:\tau \rightsquigarrow \mathbf{e} \rightsquigarrow \mathbf{e}$, *then*

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e} \approx^{ctx} {}^{\tau}\mathcal{FCA}(\mathsf{e}[\overline{\lceil\alpha\rceil/\alpha}]\overline{[\mathcal{ACF}^{\tau'}\mathsf{x}/\mathsf{x}]}) : \tau.$$

8 An Example

We can use our compiler correctness theorem to make statements about linking with arbitrary A components, as long as they have translation type. In this section, we present an example showing how our framework allows linking both with A components that cannot be expressed in F, and with those that can. To keep our example concise, we use variable substitution as a simple notion of linking.

Consider the component

$$\mathsf{e} = (\lambda \mathsf{g}:\mathsf{unit}\to\mathsf{int}.\ (\mathsf{g}\ ()) * (\mathsf{g}\ ()))\ \mathsf{x},$$

where $\cdot;\cdot;(\mathsf{x}:\mathsf{unit}\to\mathsf{int}) \vdash \mathsf{e}:\mathsf{int}$. In F alone, only divergent or constant functions can have type $\mathsf{unit}\to\mathsf{int}$, but if we are compiling to A before linking, we could be given a component that makes use of A's mutable references.

Putting e through the first compiler pass, we get a C component that contains several administrative reductions. The complete result of compilation is shown in Appendix B, but for readability, we pretend that e compiles to

$$\mathbf{e} = (\boldsymbol{\lambda}\mathbf{g}:\exists\alpha.\langle(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle.(\mathbf{unpack}\ \langle\beta,\mathbf{z}\rangle = \mathbf{g}\ \mathbf{in}\ (\boldsymbol{\pi}_1(\mathbf{z})\ \boldsymbol{\pi}_2(\mathbf{z})\ ()))$$
$$* (\mathbf{unpack}\ \langle\beta,\mathbf{z}\rangle = \mathbf{g}\ \mathbf{in}\ (\boldsymbol{\pi}_1(\mathbf{z})\ \boldsymbol{\pi}_2(\mathbf{z})\ ()))\ \mathbf{x},$$

which is equivalent to the actual result of compilation, and has exactly the same function body as the closure produced by the compiler.

The second pass brings us to an A component $\mathbf{e} = (\mathbf{t}, \mathbf{H})$, where $\mathbf{t} = \ell\ \mathbf{x}$ and

$$\mathbf{H} = \ell \mapsto \boldsymbol{\lambda}\mathbf{g}:\exists\alpha.\mathbf{box}\ \langle\mathbf{box}\ (\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle.$$
$$((\mathbf{unpack}\ \langle\beta,\mathbf{z}\rangle = \mathbf{g}\ \mathbf{in}\ ((\mathbf{read}[1]\ \mathbf{z})\ (\mathbf{read}[2]\ \mathbf{z})\ ()))\ *$$
$$(\mathbf{unpack}\ \langle\beta,\mathbf{z}\rangle = \mathbf{g}\ \mathbf{in}\ ((\mathbf{read}[1]\ \mathbf{z})\ (\mathbf{read}[2]\ \mathbf{z})\ ()))).$$

By compiler correctness, we know that

$$\cdot;\cdot;(\mathsf{x}:\mathsf{unit}\to\mathsf{int}) \vdash \mathsf{e} \approx^{ctx} {}^{\mathsf{int}}\mathcal{FCA}(\mathsf{e}[\mathcal{ACF}^{\mathsf{unit}\to\mathsf{int}}\mathsf{x}/\mathsf{x}]) : \mathsf{int}.$$

Equivalently,

$$\cdot;\cdot;(\mathsf{x}:\tau) \vdash \mathcal{ACF}^{\mathsf{int}}(\mathsf{e}[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}\,\mathsf{x}/\mathsf{x}]) \approx^{ctx} \mathbf{e}:\mathbf{int},$$

where $\tau = \mathsf{unit}\to\mathsf{int}^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle} = \exists\alpha.\mathbf{box}\ \langle\mathbf{box}\ (\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle$.

Suppose we want to instantiate x with the following A component, which creates a function that uses a mutable reference to return the number of times it has been called:

$$\mathbf{e}' = (\mathbf{pack}\langle\mathbf{ref\ int},\mathbf{balloc}\ \langle\ell,\mathbf{ralloc}\ \langle\mathbf{0}\rangle\rangle\ \mathbf{as}\ \tau,$$
$$\ell \mapsto \boldsymbol{\lambda}(\mathbf{x}:\mathbf{ref\ int},\mathbf{z}:\mathbf{unit}).\ \mathbf{let\ y} = \mathbf{read}[1]\ \mathbf{x}\ \mathbf{in\ let\ z} = \mathbf{write\ x}\ [1] \leftarrow \mathbf{y}+\mathbf{1}\ \mathbf{in\ y}+\mathbf{1}).$$

We would then have

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{int}}(\mathsf{e}[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}\,\mathbf{e}'/\mathsf{x}]) \approx^{ctx} \mathbf{e}[\mathbf{e}'/\mathsf{x}]:\mathbf{int},$$

The right-hand side of this equivalence is exactly the pure-A program that we would ultimately run, and the left-hand side is an FCA program that models it. Note that on either side of the equation, the function exported by $\mathbf{e}'$ will be applied to the unit value twice, returning 1 the first time and 2 the second time. An F function could not exhibit this behavior. This demonstrates how our framework allows for linking with components that are not expressible in F.

If we want instead to link with a different A component $\hat{e}$ that was compiled from an F component $\hat{e}$, we can still make the statement

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{int}}(e[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}\,\hat{e}/x]) \approx^{ctx} e[\hat{e}/x] : \mathbf{int},$$

but we can also simplify this statement using our additional knowledge of $\hat{e}$. Our compiler correctness theorem tells us that

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{unit}\to\mathsf{int}}\,\hat{e} \approx^{ctx} \hat{e} : \tau.$$

From this, we can infer that

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{int}}(e[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}(\mathcal{ACF}^{\mathsf{unit}\to\mathsf{int}}\,\hat{e})/x]) \approx^{ctx} e[\hat{e}/x] : \mathbf{int}.$$

Applying boundary cancellation yields

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{int}}(e[\hat{e}/x]) \approx^{ctx} e[\hat{e}/x] : \mathbf{int}.$$

Now we are essentially equating the pure-A program with a pure-F program, since the only multi-language element in this statement is the integer boundary at the outermost level, which merely converts an n to $\mathbf{n}$. This demonstrates that when we do have source-language equivalents for all our target-level components, our framework allows us to model target-level linking with source-level linking.

9 Proving Compiler Correctness

To prove the compiler correctness theorem, we design a step-indexed Kripke logical relation as a sound and complete model of contextual equivalence in FCA. Our logical relation extends that of Dreyer *et al.* [14] with the ability to handle multi-language type abstraction. We give an overview of the logical relation and a more detailed discussion of its novel features in Appendix A. In this section, we briefly discuss the high-level ideas behind our model's novel elements.

A logical-relations model provides a *relational value interpretation* of each type τ. This relation, which we denote $\mathcal{V}[\![\tau]\!]$, specifies when two values of type τ should be considered related or equivalent. When τ has free type variables, an environment ρ holds *arbitrary relational interpretations* for those abstract types. The relations in ρ capture the invariants of different instantiations of polymorphic values, which allows us to prove parametricity properties.

The interpretation $\mathcal{V}[\![\alpha]\!]\rho$ is defined by just looking up $\rho(\alpha)$. To prove important properties of $\mathcal{V}[\![\tau]\!]\rho$ for all types, we must ensure those properties hold in the α case by constraining the relations we can put into ρ to require these properties to hold up-front. Interpretations that satisfy these properties are called *candidates* or *admissible relations*.

In our multi-language setting, the two key properties we need to require for admissibility are boundary cancellation and the *bridge lemma*. The bridge lemma states that, given a pair of values v_1 and v_2 related according to the interpretation $\mathcal{V}[\![\tau]\!]\rho$, the $\mathbf{CF}^{\tau}$ translations of those values must be related according to $\mathcal{V}[\![\tau^{\langle C\rangle}]\!]\rho$. Similarly, given values $\mathbf{v_1}$ and $\mathbf{v_2}$ related according to $\mathcal{V}[\![\tau^{\langle C\rangle}]\!]\rho$, their ${}^{\tau}\mathbf{FC}$ translations must be related according to $\mathcal{V}[\![\tau]\!]\rho$. (We also require the analogous properties for the second pass.)

The type translation of α is $\lceil\alpha\rceil$, so in order for the bridge lemma to hold at type α, we need a suitable definition of $\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho$, which necessarily will depend on $\rho(\alpha)$. One naïve definition we tried is the set of translations of values from $\rho(\alpha)$, roughly:

$$\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho = \{(\mathbf{v_1}, \mathbf{v_2}) \mid (v_1, v_2) \in \rho(\alpha) \ \wedge\ \mathbf{CF}(v_i) = \mathbf{v_i}\}.$$

While this definition does let us prove the bridge lemma at type α, it does not satisfy boundary cancellation: if $\mathbf{v_1}$ and $\mathbf{v_2}$ are related according to this definition of $\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho$, it is not necessarily the case that $\mathbf{CA}(\mathbf{AC}(\mathbf{v_1}))$ and $\mathbf{v_2}$ are related.

All the ways we tried to define $\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho$ by a simple formula in terms of $\rho(\alpha)$ failed for similar reasons. Instead of giving a uniform definition, we took the viewpoint that if the properties of $\rho(\alpha)$ must be given *a priori*, then the particular relations with those properties that instantiate $\mathcal{V}[\![\alpha]\!]\rho$ and $\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho$ should be given *a priori* as well. Specifically, in our model, an interpretation $\rho(\alpha)$ not just given by a relation on F values, but by a triple containing the relation on F values, a relation on C values to serve as its "translation" and instantiate $\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho$, and a relation on A values to instantiate $\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho$. Similarly, an interpretation $\rho(\boldsymbol{\alpha})$ is given by a pair containing a C-level relation and an A-level relation. For $\rho(\alpha)$, since A is the target language, only one relation is needed.

This strategy moves the burden for defining the "translations" of candidate relations to the places in our proof development where individual candidates are needed. But in all these places, there is some specific information available about the relation, so it was not difficult to construct them.

10 Discussion and Future Work

Software is composed from components written in different languages because different languages are suited to different tasks. We have provided a novel methodology for verifying *open*, *multi-pass* compilers, one that yields a stronger theorem than any existing work, allowing target-level linking with components of arbitrary provenance regardless of whether the component can be expressed in the source language compiled by the verified compiler.

Adding Compiler Passes Adding more intermediate languages to our compiler pipeline requires extending the multi-language model with new boundary forms and translation rules, and extending the logical relation with new clauses. Our aim is that the proof structure should be as modular as possible, so that the major lemmas and the correctness proof for one compiler pass can be completed independently of the rest of the pipeline. Presently, since our admissible relations design requires relations from multiple languages, we have a small number of places where a proof about one pass is affected by the other languages and passes. We hope to improve our proof engineering so that proofs for existing passes are unaffected when the compiler pipeline is changed.

Compiling to Assembly We have extended our compiler with a code-generation pass that translates A components to a stack-based typed assembly language, T. The latter is similar to Morrisett *et al.*'s stack-based TAL [6] but with a type system that tracks more information. Informally, the T type system allows us to track calls and returns of semantic "functions" that may span multiple basic blocks, and to determine the "return type" of such functions. With this information, we are able to give a formal definition of contextual equivalence for T that makes distinctions about assembly at an appropriate level of granularity. That is, we relate assembly language components comprised of any number of basic blocks, rather than relating individual basic blocks. An equivalence relation based on individual blocks would be too fine grained; for instance, it would be unable to relate two components with an unequal number of basic blocks that may

have been produced by compiling two equivalent source terms. We are working on the proofs for this pass and will report on it in a future paper.

Mutable References Consider adding mutable references to F and C. For the first compiler pass, we would extend the type translation with $(\mathsf{ref}\ \tau)^{\mathsf{C}} = \mathbf{ref}\ \tau^{\mathsf{C}}$. When defining interoperability at type $\mathsf{ref}\ \tau$, it doesn't make sense to convert an F location ℓ into a fresh C location $\boldsymbol{\ell}$ (and vice versa) since it would lead to duplication of mutable cells in the interoperating languages and these would be impossible to keep in sync. One solution is to treat a wrapped location (e.g., ${}^{\mathsf{ref}\ \tau}\mathcal{FC}\boldsymbol{\ell}$) as a value form. Operations on these wrapped locations can be performed by reduction rules such as these:

$$!({}^{\mathsf{ref}\ \tau}\mathcal{FC}\boldsymbol{\ell}) \longmapsto {}^{\tau}\mathcal{FC}(!\boldsymbol{\ell}) \quad ({}^{\mathsf{ref}\ \tau}\mathcal{FC}\boldsymbol{\ell}) := \mathsf{v} \longmapsto {}^{\mathsf{unit}}\mathcal{FC}(\boldsymbol{\ell} := \mathcal{CF}^{\tau}\mathsf{v}),$$

where $!\mathsf{v}$ is a dereference and $\mathsf{v} := \mathsf{v}'$ is an assignment. Passing references between C and A can be done analogously. While these interoperability semantics are straightforward, we expect to find nontrivial challenges in designing a logical relation to properly handle the wrapped-location value forms they introduce.

Supporting Realistic Interoperability We are particularly interested in supporting target-level interoperability between a language with parametric polymorphism such as ML and languages without type abstraction such as Scheme or C. For instance, given a generic tree library compiled from ML, we want to allow code compiled from Scheme or C to be able to use the library but ensure that such use cannot invalidate ML's parametricity guarantees by inspecting values that have abstract type on the ML side. In this paper, we have shown how to preserve ML's parametricity guarantees part-way through the compiler. Going forward we wish to develop a gradually typed assembly language that, following Matthews and Ahmed [15], uses dynamic sealing on the untyped side to enforce parametricity guarantees provided by type abstraction on the typed side.

11 Related Work

The literature on compiler verification spans over four decades but is mostly limited to whole-program compilation; we refer the reader to the bibliography by Dave [16] for compilers for first-order languages, and to Chlipala [17] for compilers for higher-order functional languages. We have already discussed the existing work [9, 11] on compositional compiler correctness in §2. Here we focus on other closely related work.

Dreyer et al. have recently been working on Relational Transition Systems (RTS's) [18] that may provide an alternative cross-language specification technique that is designed to make it possible to prove transitivity. Regardless, it is still not easy to do: see their technical report [19] where they prove transitivity for their *single-language* RTS system for an idealized ML. It is a non-trivial task to do this for multiple cross-language RTS's. Additionally, even if the RTS approach proves effective for verifying a multi-pass compiler, it still does not address the problem of linking with a component e'_T for which there is no related source-level e'_S.

The design of our multi-language system builds on that of Ahmed and Blume [8], who developed a boundary-based multi-language system embedding the source (STLC) and target (System F) of CPS translation. Ahmed and Blume did not have type abstraction in the source language, which meant that they did not have to make use of lumps or suspensions, nor design a logical relation to handle these. Our semantics preservation proof is analogous to theirs. However, since they were interested in fully abstract

CPS translation, they designed their type translation to disallow linking compiled code with target components whose behavior cannot be expressed at the source level. The additional work that they do to prove full abstraction provides a roadmap for how to extend our methodology to prove full abstraction in a setting where the type translation enforces it.

Tov and Pucella [20] design a multi-language semantics for interoperation between a language with an affine type system and a conventional language, where both languages support polymorphism. Their semantics allows only closed terms to appear under boundaries, which allows them to use slightly simpler machinery than our lumps and suspensions. But this restriction means that their model would not admit a statement like our compiler correctness theorem, since we use a boundary to relate source and target components that may have free variables.

Acknowledgements We would like to thank Nick Benton, whose views on compositional compiler correctness have been an inspiration to us. In particular, our thinking has been influenced by Benton and Hur's introduction [10], which eloquently lays out desirable features of a compiler correctness specification. We would also like to thank Aaron Turon for helpful feedback on an earlier version of this paper. This research was supported by the National Science Foundation (grant CCF-1203008).

References

1. Leroy, X.: Formal certification of a compiler back-end or: programming a compiler with a proof assistant. In: ACM Symposium on Principles of Programming Languages (POPL), Charleston, South Carolina. (January 2006)
2. Leroy, X.: A formally verified compiler back-end. Journal of Automated Reasoning **43**(4) (2009) 363–446
3. Lochbihler, A.: Verifying a compiler for Java threads. In: European Symposium on Programming (ESOP). (March 2010)
4. Myreen, M.O.: Verified just-in-time compiler on x86. In: ACM Symposium on Principles of Programming Languages (POPL), Madrid, Spain. (January 2010)
5. Sevcik, J., Vafeiadis, V., Nardelli, F.Z., Jagannathan, S., Sewell, P.: Relaxed-memory concurrency and verified compilation. In: ACM Symposium on Principles of Programming Languages (POPL), Austin, Texas. (2011)
6. Morrisett, G., Crary, K., Glew, N., Walker, D.: Stack-based typed assembly language. Journal of Functional Programming **12**(1) (2002) 43–88
7. Matthews, J., Findler, R.B.: Operational semantics for multi-language programs. In: ACM Symposium on Principles of Programming Languages (POPL), Nice, France. (January 2007) 3–10
8. Ahmed, A., Blume, M.: An equivalence-preserving CPS translation via multi-language semantics. In: International Conference on Functional Programming (ICFP), Tokyo, Japan. (September 2011) 431–444
9. Benton, N., Hur, C.K.: Biorthogonality, step-indexing and compiler correctness. In: International Conference on Functional Programming (ICFP), Edinburgh, Scotland. (September 2009)
10. Benton, N., Hur, C.K.: Realizability and compositional compiler correctness for a polymorphic language. Technical Report MSR-TR-2010-62, Microsoft Research (April 2010)
11. Hur, C.K., Dreyer, D.: A Kripke logical relation between ML and assembly. In: ACM Symposium on Principles of Programming Languages (POPL), Austin, Texas. (January 2011)

12. Morrisett, G., Walker, D., Crary, K., Glew, N.: From System F to typed assembly language. ACM Transactions on Programming Languages and Systems **21**(3) (May 1999) 527–568
13. Minamide, Y., Morrisett, G., Harper, R.: Typed closure conversion. In: ACM Symposium on Principles of Programming Languages (POPL), St. Petersburg Beach, Florida. (January 1996) 271–283
14. Dreyer, D., Neis, G., Birkedal, L.: The impact of higher-order state and control effects on local relational reasoning. Journal of Functional Programming **22**(4&5) (2012) 477–528
15. Matthews, J., Ahmed, A.: Parametric polymorphism through run-time sealing, or, theorems for low, low prices! In: European Symposium on Programming (ESOP). (March 2008) 16–31
16. Dave, M.A.: Compiler verification: A bibliography. ACM SIGSOFT Software Engineering Notes **28**(6) (2003)
17. Chlipala, A.: A verified compiler for an impure functional language. In: ACM Symposium on Principles of Programming Languages (POPL), Madrid, Spain. (January 2010)
18. Hur, C.K., Dreyer, D., Neis, G., Vafeiadis, V.: The marriage of bisimulations and Kripke logical relations. In: ACM Symposium on Principles of Programming Languages (POPL), Philadelphia, Pennsylvania. (January 2012)
19. Hur, C.K., Dreyer, D., Neis, G., Vafeiadis, V.: The marriage of bisimulations and kripke logical relations. Technical report, Max Planck Institute for Software Systems (MPI-SWS) (January 2012)
20. Tov, J.: Stateful contracts for affine types. In: European Symposium on Programming (ESOP). (March 2010)

A Multi-Language Logical Relation

Our compiler correctness theorems are stated in terms of FCA contextual equivalence, but proving contextual equivalences directly can be hard or even intractable due to the quantification over all contexts C in the definition of $\approx^{ctx}$. We prove our compiler-correctness theorems by way of a logical relations model of FCA.

Specifically, we design a step-indexed, biorthogonal, Kripke logical relation, which extends the standard Kripke logical relations design (such as that of Dreyer *et al.* [14]) with the ability to handle multi-language type abstraction. We prove that logical equivalence is sound and complete for contextual equivalence, and then we are able to prove our compiler correctness theorems in terms of logical equivalence. In this appendix, we discuss the novel aspects of our logical relation and the major steps needed to complete these proofs. We elide many non-novel details of the construction. Full definitions are given in Appendix B.

Overview of the Logical Relation The basic idea of logical relations is to define an equivalence relation on program terms by induction on the structure of their types. For instance, two functions are related at the type $\tau_1 \to \tau_2$ iff relatedness of their arguments at type τ_1 implies relatedness of their results at type τ_2; two tuples of length n are related at type $\langle \tau_1, \ldots, \tau_n \rangle$ iff their i-th components (for all $1 \leq i \leq n$) are related at type τ_i; etc.

In the presence of state, one has to make use of Kripke logical relations, which are indexed by *possible worlds* W. Kripke logical relations are needed when relatedness only holds under certain conditions; possible worlds allow us to capture these conditions and specify constraints on how the conditions may evolve over time. Our worlds W will specify constraints on heaps; we write $(\mathbf{H}_1, \mathbf{H}_2) : W$ when the heaps $\mathbf{H}_1$ and $\mathbf{H}_2$ satisfy W. For instance, two locations ℓ_1 and ℓ_2 should only be related at type $\mathbf{box}\ \psi$ if: they actually exist in any heaps that satisfy the current world W; if they contain heap values related at type ψ; and if W specifies that they are immutable cells—whose contents will remain unchanged in all future worlds W' that are accessible from W (written $W' \sqsupseteq W$, where $\sqsupseteq$ is pronounced "extends"). An important property of Kripke logical relations is monotonicity, which says that relatedness of two values in world W implies relatedness in all future possible worlds W' accessible from W.

Finally, step-indexed logical relations allow one to easily deal with features that lead to "circularities" in the construction of semantic models, e.g., recursive types and mutable references to functions. The idea is roughly to define the logical relation by induction on a natural number that, intuitively, corresponds to the number of steps of computation for which two programs behave in a related manner.

The important pieces of our logical relation are given in Figures 6 and 7. The big picture is that we define a value relation $\mathcal{V}[\![\tau]\!]$ that relates closed values at type τ, a continuation relation $\mathcal{K}[\![\tau]\!]$ that relates closed continuations (evaluation contexts) with a hole of type τ, and a term relation $\mathcal{E}[\![\tau]\!]$ that relates closed terms at type τ. Each of these relations is indexed by a world W and we build each of these relations out of well-typed values, continuations, and terms, as captured by the "Atom" definitions at the top of Figure 6. We then generalize the definition to open terms (written $\mathbf{\Psi}; \Delta; \Gamma \vdash e_1 \approx e_2 : \tau$).

Our worlds are structured as $W ::= (k, \mathbf{\Psi}_1, \mathbf{\Psi}_2, \Theta)$, where k is the number of computation steps we have left, $\mathbf{\Psi}_1$ and $\mathbf{\Psi}_2$ are the heap types that any $\mathbf{H}_1$, $\mathbf{H}_2$ must

$$
\begin{array}{lll}
\mathrm{TermAtom}[\tau_1,\tau_2] & = \{\,(W,e_1,e_2) \mid W \in \mathrm{World} \wedge \\
 & \quad W.\Psi_1;\cdot;\cdot \vdash e_1 : \tau_1 \ \wedge\ W.\Psi_2;\cdot;\cdot \vdash e_2 : \tau_2 \,\} \\
\mathrm{ValAtom}[\tau_1,\tau_2] & = \{\,(W,v_1,v_2) \in \mathrm{TermAtom}[\tau_1,\tau_2]\,\} \\
\mathrm{ContAtom}[\tau_1,\tau_2] \rightsquigarrow [\tau_1',\tau_2'] & = \{(W,E_1,E_2) \mid W \in \mathrm{World} \ \wedge \\
 & \quad \exists \Psi_1,\Psi_2.\ \vdash E_i : (W.\Psi_i;\cdot;\cdot \vdash \tau_i) \rightsquigarrow (\Psi_i;\cdot;\cdot \vdash \tau_i')\} \\
\mathrm{TermAtom}[\tau]\rho & = \mathrm{TermAtom}[\rho_1(\tau),\rho_2(\tau)] \\
\mathrm{ValAtom}[\tau]\rho & = \mathrm{ValAtom}[\rho_1(\tau),\rho_2(\tau)] \\
\mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau']\rho' & = \mathrm{ContAtom}[\rho_1(\tau),\rho_2(\tau)] \rightsquigarrow [\rho_1'(\tau'),\rho_2'(\tau')]
\end{array}
$$

$$
\begin{array}{lll}
\mathcal{V}[\![\mathsf{unit}]\!]\rho & = \{\,(W,(),()) \in \mathrm{ValAtom}[\mathsf{unit}]\rho\,\} \\
\mathcal{V}[\![\mathsf{int}]\!]\rho & = \{\,(W,\mathsf{n},\mathsf{n}) \in \mathrm{ValAtom}[\mathsf{int}]\rho\,\} \\
\mathcal{V}[\![\alpha]\!]\rho & = \rho(\alpha).\varphi^F \\
\mathcal{V}[\![\forall[\alpha].(\tau)\to\tau']\!]\rho & = \{\,(W,\mathsf{v}_1,\mathsf{v}_2) \in \mathrm{ValAtom}[\forall[\alpha].(\tau)\to\tau']\rho \mid \\
 & \quad \forall W' \sqsupseteq W.\ \forall \mathrm{VR} \in \mathrm{FValRel}.\ \forall \mathsf{v}_1',\mathsf{v}_2'.\ (W',\mathsf{v}_1',\mathsf{v}_2') \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] \\
 & \quad \implies (W',\mathsf{v}_1\,[\mathrm{VR}.\tau_1]\,\mathsf{v}_1',\mathsf{v}_2\,[\mathrm{VR}.\tau_2]\,\mathsf{v}_2') \in \mathcal{E}[\![\tau']\!]\rho[\alpha \mapsto \mathrm{VR}]\,\} \\
\mathcal{V}[\![\exists\alpha.\tau]\!]\rho & = \{(W,\mathsf{pack}\langle\tau_1,\mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\alpha.\tau),\mathsf{pack}\langle\tau_2,\mathsf{v}_2\rangle\ \mathsf{as}\ \rho_2(\exists\alpha.\tau)) \\
 & \quad \in \mathrm{ValAtom}[\exists\alpha.\tau]\rho \mid \\
 & \quad \exists \mathrm{VR} \in \mathrm{FValRel}. \\
 & \quad\quad \mathrm{VR}.\tau_1 = \tau_1 \ \wedge\ \mathrm{VR}.\tau_2 = \tau_2 \ \wedge (W,\mathsf{v}_1,\mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]\,\} \\
\mathcal{V}[\![\mu\alpha.\tau]\!]\rho & = \{\,(W,\mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\,\mathsf{v}_1,\mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\,\mathsf{v}_2) \in \mathrm{ValAtom}[\mu\alpha.\tau]\rho \mid \\
 & \quad (W,\mathsf{v}_1,\mathsf{v}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho\,\} \\
\mathcal{V}[\![\langle\tau_1,\ldots,\tau_\mathsf{n}\rangle]\!]\rho & = \{\,(W,\langle\mathsf{v}_{11},\ldots,\mathsf{v}_{1\mathsf{n}}\rangle,\langle\mathsf{v}_{21},\ldots,\mathsf{v}_{2\mathsf{n}}\rangle) \in \mathrm{ValAtom}[\langle\tau_1,\ldots,\tau_\mathsf{n}\rangle]\rho \mid \\
 & \quad \forall \mathsf{j} \in \{1,\ldots,\mathsf{n}\}.\ (W,\mathsf{v}_{1\mathsf{j}},\mathsf{v}_{2\mathsf{j}}) \in \mathcal{V}[\![\tau_\mathsf{j}]\!]\rho\,\} \\
\mathcal{V}[\![\mathsf{L}\langle\boldsymbol{\tau}\rangle]\!]\rho & = \{\,(W,{}^{\rho_1(\mathsf{L}\langle\tau\rangle)}\mathcal{FC}\mathbf{v_1},{}^{\rho_2(\mathsf{L}\langle\tau\rangle)}\mathcal{FC}\mathbf{v_2}) \in \mathrm{ValAtom}[\mathsf{L}\langle\boldsymbol{\tau}\rangle]\rho \mid \\
 & \quad (W,\mathbf{v_1},\mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho\,\} \\
\mathcal{V}[\![\boldsymbol{\alpha}]\!]\rho & = \rho(\boldsymbol{\alpha}).\varphi^C \qquad \mathcal{V}[\![\lceil\alpha\rceil]\!]\rho = \rho(\alpha).\varphi^C \\
\mathcal{V}[\![\mathbf{L}\langle\boldsymbol{\tau}\rangle]\!]\rho & = \{(W,{}^{\rho_1(\mathbf{L}\langle\tau\rangle)}\mathcal{CA}\,\mathbf{v}_1,{}^{\rho_2(\mathbf{L}\langle\tau\rangle)}\mathcal{CA}\,\mathbf{v}_2) \in \mathrm{ValAtom}[\mathbf{L}\langle\boldsymbol{\tau}\rangle]\rho \mid \\
 & \quad (W,\mathbf{v}_1,\mathbf{v}_2) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho\} \\
\mathcal{V}[\![\boldsymbol{\alpha}]\!]\rho & = \rho(\boldsymbol{\alpha}).\varphi^A \qquad \mathcal{V}[\![\lceil\alpha\rceil]\!]\rho = \rho(\alpha).\varphi^A \qquad \mathcal{V}[\![\lceil\boldsymbol{\alpha}\rceil]\!]\rho = \rho(\boldsymbol{\alpha}).\varphi^A
\end{array}
$$

Fig. 6. FCA Logical Relation

$$
\begin{aligned}
\mathcal{K}[\![\tau]\!]\rho &= \{\, (W, E_1, E_2) \in \mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau']\rho' \mid \forall W', v_1, v_2. \\
&\qquad W' \sqsupseteq_{\mathrm{pub}} W \ \wedge\ (W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho \implies (W', E_1[v_1], E_2[v_2]) \in \mathcal{O} \,\} \\
\mathcal{E}[\![\tau]\!]\rho &= \{\, (W, e_1, e_2) \in \mathrm{TermAtom}[\tau]\rho \mid \forall E_1, E_2. \\
&\qquad (W, E_1, E_2) \in \mathcal{K}[\![\tau]\!]\rho \implies (W, E_1[e_1], E_2[e_2]) \in \mathcal{O} \,\} \\
\mathcal{O} \quad &= \{\, (W, e_1, e_2) \mid \forall (\mathsf{H}_1, \mathsf{H}_2) : W.\ (\langle \mathsf{H}_1 \mid e_1 \rangle\!\downarrow \ \wedge\ \langle \mathsf{H}_2 \mid e_2 \rangle\!\downarrow) \ \vee \\
&\qquad\qquad (\mathrm{running}(W.k, \langle \mathsf{H}_1 \mid e_1 \rangle) \ \wedge\ \mathrm{running}(W.k, \langle \mathsf{H}_2 \mid e_2 \rangle)) \,\}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{D}[\![\cdot]\!] &= \{\, \emptyset \,\} \\
\mathcal{D}[\![\Delta, \alpha]\!] &= \{\, \rho[\alpha \mapsto \mathrm{VR}] \mid \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \mathrm{VR} \in \mathrm{FValRel} \,\} \\
\mathcal{D}[\![\Delta, \boldsymbol{\alpha}]\!] &= \{\, \rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] \mid \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \mathrm{VR} \in \mathrm{CValRel} \,\} \\
\mathcal{D}[\![\Delta, \alpha]\!] &= \{\, \rho[\alpha \mapsto \mathrm{VR}] \mid \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \mathrm{VR} \in \mathrm{AValRel} \,\} \\
\mathcal{H}[\![\cdot]\!] &= \mathrm{World} \\
\mathcal{H}[\![\boldsymbol{\Psi}, \ell : {}^{\mathsf{box}}\psi]\!] &= \mathcal{H}[\![\boldsymbol{\Psi}]\!] \cap \{\, W \in \mathrm{World} \mid (W, \ell, \ell) \in \mathcal{V}[\![\mathsf{box}\ \psi]\!]\emptyset \,\} \\
\mathcal{H}[\![\boldsymbol{\Psi}, \ell : {}^{\mathsf{ref}}\psi]\!] &= \mathcal{H}[\![\boldsymbol{\Psi}]\!] \cap \{\, W \in \mathrm{World} \mid (W, \ell, \ell) \in \mathcal{V}[\![\mathsf{ref}\ \psi]\!]\emptyset \,\} \\
\mathcal{G}[\![\cdot]\!]\rho &= \{\, (W, \emptyset) \mid W \in \mathrm{World} \,\} \\
\mathcal{G}[\![\Gamma, x : \tau]\!]\rho &= \{\, (W, \gamma[x \mapsto (v_1, v_2)]) \mid \gamma \in \mathcal{G}[\![\Gamma]\!]\rho \ \wedge\ (W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho \,\}
\end{aligned}
$$

$$
\begin{aligned}
\boldsymbol{\Psi}; \Delta; \Gamma \vdash e_1 \approx e_2 : \tau \stackrel{\mathrm{def}}{=} \boldsymbol{\Psi}; \Delta; \Gamma \vdash e_1 : \tau \ \wedge\ \boldsymbol{\Psi}; \Delta; \Gamma \vdash e_2 : \tau \ \wedge \\
\forall W, \rho, \gamma.\ W \in \mathcal{H}[\![\boldsymbol{\Psi}]\!] \ \wedge\ \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ (W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho \\
\implies (W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_2))) \in \mathcal{E}[\![\tau]\!]\rho
\end{aligned}
$$

Fig. 7. FCA Logical Relation (Continued)

have if they are to satisfy W, and Θ is a sequence of islands that specify invariants on disjoint parts of the heap. We will leave further details of worlds and islands to the online technical report, except to say that we reserve the first island for tracking all the immutable cells in the two heaps. We abstract the process of adding immutable cells to this island by using an operation $W \boxplus (\mathsf{H}_1, \mathsf{H}_2)$ ("box-plus" for adding **box**es to W).

The standard practice is for each of the above relations $\mathcal{V}, \mathcal{K}, \mathcal{E}$ on τ to be parametrized by a mapping ρ that provides relational interpretations for the free type variables in τ. For now, assume that ρ maps type variables α to triples $\mathrm{VR} ::= (\tau_1, \tau_2, \varphi)$, where τ_1 and τ_2 are the types used to instantiate α on the left and right sides, respectively, and φ is a relation between values of those types, that is, a subset of $\mathrm{ValAtom}[\tau_1, \tau_2]$. We will explain shortly why this structure is not quite what we need, but it suffices to explain the general principles of the logical relation. We write ρ_1 for the substitution that instantiates each $\alpha \in \mathrm{dom}(\rho)$ with the corresponding τ_1, and ρ_2 for the substitution that instantiates αs with τ_2s.

We briefly walk through the F cases of the value relation, which are shown in Figure 6. Values of base type are related if they are the same value. Values are related at type α if they are in the relational interpretation of α, $\rho(\alpha).\varphi$ (For now, ignore the superscript on φ in the figure). Functions are related if, at any point in the future, applying them to related arguments will yield related results. Packages are related at existential type if there exists some interpretation VR of the abstract type under which their bodies

are related. Values of recursive type are related if unfolding the recursion yields values that are related after expending a step (denoted by the $\triangleright$ operator). Tuples are related if all their components are related. And finally, lumps are related if the underlying values are related.

We elide most of the cases of $\mathcal{V}[\![\tau]\!]\rho$ for C and A types. The only difficult case is the case for suspended type variables, which we will return to shortly.

In the term relation $\mathcal{E}[\![\tau]\!]\rho$, two terms are related if running them in related continuations gives related observations. Two continuations are related in $\mathcal{K}[\![\tau]\!]\rho$ if whenever we are given related values in some future world (under a restricted notion of *public* future worlds; see Dreyer *et al.*), then running the continuations with those values gives us related observations. This technique of defining the term relation $\mathcal{E}$ by appealing to a continuation relation $\mathcal{K}$ is referred to as biorthogonality or $\top\top$-closure, and it yields a logical relation that is complete with respect to contextual equivalence.

Under the relation $\mathcal{O}$, two closed terms give us related observations in world W if, when we run them in two heaps that satisfy W, either they both terminate, or they are both still running after k steps, where k is the number of steps allowed by W.

Finally, our notion of logical equivalence (bottom of Figure 6) lifts $\mathcal{E}[\![\tau]\!]\rho$ to open terms. It says that e_1 and e_2 are related if, given a world (which must satisfy the heap type Ψ), a mapping ρ (which must satisfy some properties to be discussed shortly), and a pair of substitutions γ (where the values being substituted must be related), we get related components by closing off e_1 and e_2 with ρ and γ.

Admissible Relations Thus far, we have avoided discussion of what properties an interpretation VR of a type variable α must satisfy to be considered admissible. Usually, these requirements stem from any lemmas that we need about $\mathcal{V}[\![\tau]\!]\rho$: Since $\tau = \alpha$ is a base case, these properties need to hold for any interpretation of α.

In our setting, the two properties we need are boundary cancellation and the *bridge lemmas*. We have already discussed boundary cancellation, but we give an alternate statement of it in terms of $\mathcal{V}[\![\tau]\!]\rho$, which must be proved on the way to proving the version stated in §1:

Lemma 1 (FC-CF **Boundary Cancellation).**
If $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho$ *and* ${}^{\tau}\boldsymbol{FC}(\boldsymbol{CF}^{\tau}(\mathsf{v}_2)) = \mathsf{v}_2'$, *then* $(W, \mathsf{v}_1, \mathsf{v}_2') \in \mathcal{V}[\![\tau]\!]\rho$.

Statements of boundary cancellation for the other pairs of opposite boundaries are similar.

The bridge lemmas state that if two values are related at a given type, then their translations are related at translation type. Or, in the other direction, if two values are related at translation type, their backward translations are related at the corresponding source type. These lemmas are needed to prove soundness of the logical relation for contextual equivalence. One of the cases of the bridge lemma is as follows:

Lemma 2 (FC **Bridge Lemma).**
If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle C \rangle}]\!]\rho$, ${}^{\tau}\boldsymbol{FC}(\mathbf{v_1}) = \mathsf{v}_1'$, *and* ${}^{\tau}\boldsymbol{FC}(\mathbf{v_2}) = \mathsf{v}_2'$,
then $(W, \mathsf{v}_1', \mathsf{v}_2') \in \mathcal{V}[\![\tau]\!]\rho$.

We need to build in requirements that any relations we put into ρ satisfy boundary cancellation and the bridge lemmas. We will do this in layers, defining sets of relations that enforce progressively more of these properties.

$$
\begin{aligned}
\mathrm{ValRel}[\tau_1,\tau_2] \;=\; \{\, \varphi^F \subseteq \mathrm{ValAtom}[\tau_1,\tau_2] \mid \forall (W,\mathsf{v}_1,\mathsf{v}_2) \in \varphi^F.\;& \\
(\forall W' \sqsupseteq W.\; (W',\mathsf{v}_1,\mathsf{v}_2) \in \varphi^F\,) \wedge\;& \\
\forall \mathsf{v}_1',\mathsf{v}_2'.\; (\,{}^{\tau_1}\mathbf{FC}(\mathbf{CF}^{\tau_1}(\mathsf{v}_1)) = \mathsf{v}_1' \Longrightarrow (W,\mathsf{v}_1',\mathsf{v}_2) \in \varphi^F\,) \wedge\;& \\
(\,{}^{\tau_2}\mathbf{FC}(\mathbf{CF}^{\tau_2}(\mathsf{v}_2)) = \mathsf{v}_2' \Longrightarrow (W,\mathsf{v}_1,\mathsf{v}_2') \in \varphi^F)\}&
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{ValRel}[\boldsymbol{\tau_1},\boldsymbol{\tau_2}] = \{\, \varphi^C \subseteq \mathrm{ValAtom}[\boldsymbol{\tau_1},\boldsymbol{\tau_2}] \mid \forall (W,\mathbf{v_1},\mathbf{v_2}) \in \varphi^C.\;& \\
(\forall W' \sqsupseteq W.\; (W',\mathbf{v_1},\mathbf{v_2}) \in \varphi^C\,) \wedge\;& \\
\forall (\mathbf{H_1},\mathbf{H_2}) : W.\; \forall \mathbf{v_1'},\mathbf{v_2'},\mathbf{H_1'},\mathbf{H_2'}.\;& \\
(\,{}^{\tau_1}\mathbf{CA}(\mathbf{AC}^{\tau_1}(\mathbf{v_1},\mathbf{H_1})) = (\mathbf{v_1'},\mathbf{H_1} \uplus \mathbf{H_1'}) \Longrightarrow (W \boxplus (\mathbf{H_1'},\cdot),\mathbf{v_1'},\mathbf{v_2}) \in \varphi^C\,) \wedge\;& \\
(\,{}^{\tau_2}\mathbf{CA}(\mathbf{AC}^{\tau_2}(\mathbf{v_2},\mathbf{H_2})) = (\mathbf{v_2'},\mathbf{H_2} \uplus \mathbf{H_2'}) \Longrightarrow (W \boxplus (\cdot,\mathbf{H_2'}),\mathbf{v_1},\mathbf{v_2'}) \in \varphi^C)\}&
\end{aligned}
$$

$$
\mathrm{ValRel}[\tau_1,\tau_2] = \{\, \varphi^A \subseteq \mathrm{ValAtom}[\tau_1,\tau_2] \mid \forall (W,\mathsf{v}_1,\mathsf{v}_2) \in \varphi^A.\; \forall W' \sqsupseteq W.\; (W',\mathsf{v}_1,\mathsf{v}_2) \in \varphi^A\}
$$

$$
\begin{aligned}
\mathrm{TransRel}^{\mathcal{C}}[\tau_1,\tau_2] \;=\; \{\, \varphi^C \in \mathrm{ValRel}[\tau_1{}^{\langle\mathcal{C}\rangle},\tau_2{}^{\langle\mathcal{C}\rangle}] \mid \forall (W,\mathbf{v_1},\mathbf{v_2}) \in \varphi^C.\;& \\
\forall \mathbf{v_1'},\mathbf{v_2'}.\; (\,\mathbf{CF}^{\tau_1}({}^{\tau_1}\mathbf{FC}(\mathbf{v_1})) = \mathbf{v_1'} \Longrightarrow (W,\mathbf{v_1'},\mathbf{v_2}) \in \varphi^C\,) \wedge\;& \\
(\,\mathbf{CF}^{\tau_2}({}^{\tau_2}\mathbf{FC}(\mathbf{v_2})) = \mathbf{v_2'} \Longrightarrow (W,\mathbf{v_1},\mathbf{v_2'}) \in \varphi^C)\}&
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{TransRel}^{\mathcal{A}}[\boldsymbol{\tau_1},\boldsymbol{\tau_2}] = \{\, \varphi^A \in \mathrm{ValRel}[\boldsymbol{\tau_1}{}^{\langle\mathcal{A}\rangle},\boldsymbol{\tau_2}{}^{\langle\mathcal{A}\rangle}] \mid \forall (W,\mathbf{v_1},\mathbf{v_2}) \in \varphi^A.\;& \\
\forall (\mathbf{H_1},\mathbf{H_2}) : W.\; \forall \mathbf{v_1'},\mathbf{v_2'},\mathbf{H_1'},\mathbf{H_2'}.\;& \\
(\,\mathbf{AC}^{\tau_1}({}^{\tau_1}\mathbf{CA}(\mathbf{v_1},\mathbf{H_1})) = (\mathbf{v_1'},\mathbf{H_1} \uplus \mathbf{H_1'}) \Longrightarrow (W \boxplus (\mathbf{H_1'},\cdot),\mathbf{v_1'},\mathbf{v_2}) \in \varphi^A\,) \wedge\;& \\
(\,\mathbf{AC}^{\tau_2}({}^{\tau_2}\mathbf{CA}(\mathbf{v_2},\mathbf{H_2})) = (\mathbf{v_2'},\mathbf{H_2} \uplus \mathbf{H_2'}) \Longrightarrow (W \boxplus (\cdot,\mathbf{H_2'}),\mathbf{v_1},\mathbf{v_2'}) \in \varphi^A)\}&
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{CF}(\tau_1,\tau_2,\varphi^F) \;&=\; \{(W,\mathbf{v_1},\mathbf{v_2}) \mid (W,\mathsf{v}_1,\mathsf{v}_2) \in \varphi^F \;\wedge\; \mathbf{CF}^{\tau_1}(\mathsf{v}_1) = \mathbf{v_1} \;\wedge\; \mathbf{CF}^{\tau_2}(\mathsf{v}_2) = \mathbf{v_2}\} \\
&\quad \text{if } \varphi^F \in \mathrm{ValRel}[\tau_1,\tau_2] \\
\mathcal{FC}(\tau_1,\tau_2,\varphi^C) \;&=\; \{(W,\mathbf{v_1},\mathbf{v_2}) \mid (W,\mathbf{v_1},\mathbf{v_2}) \in \varphi^C \;\wedge\; {}^{\tau_1}\mathbf{FC}(\mathbf{v_1}) = \mathsf{v}_1 \;\wedge\; {}^{\tau_2}\mathbf{FC}(\mathbf{v_2}) = \mathsf{v}_2\} \\
&\quad \text{if } \varphi^C \in \mathrm{TransRel}^{\mathcal{C}}[\tau_1,\tau_2] \\
\mathcal{AC}(\boldsymbol{\tau_1},\boldsymbol{\tau_2},\varphi^C) \;&=\; \{(W \boxplus (\mathbf{H_1'},\mathbf{H_2'}),\mathbf{v_1},\mathbf{v_2}) \mid (\mathbf{H_1},\mathbf{H_2}) : W \;\wedge\; (W,\mathbf{v_1},\mathbf{v_2}) \in \varphi^C \wedge \\
&\qquad \mathbf{AC}^{\tau_1}(\mathbf{v_1},\mathbf{H_1}) = (\mathbf{v_1},\mathbf{H_1} \uplus \mathbf{H_1'}) \;\wedge\; \mathbf{AC}^{\tau_2}(\mathbf{v_2},\mathbf{H_2}) = (\mathbf{v_2},\mathbf{H_2} \uplus \mathbf{H_2'})\} \\
&\quad \text{if } \varphi^C \in \mathrm{ValRel}[\boldsymbol{\tau_1},\boldsymbol{\tau_2}] \\
\mathcal{CA}(\boldsymbol{\tau_1},\boldsymbol{\tau_2},\varphi^A) \;&=\; \{(W,\mathbf{v_1},\mathbf{v_2}) \mid (\mathbf{H_1},\mathbf{H_2}) : W \;\wedge\; (W,\mathbf{v_1},\mathbf{v_2}) \in \varphi^A \wedge \\
&\qquad {}^{\tau_1}\mathbf{CA}(\mathbf{v_1},\mathbf{H_1}) = (\mathbf{v_1},\mathbf{H_1}) \;\wedge\; {}^{\tau_2}\mathbf{CA}(\mathbf{v_2},\mathbf{H_2}) = (\mathbf{v_2},\mathbf{H_2})\} \\
&\quad \text{if } \varphi^A \in \mathrm{TransRel}^{\mathcal{A}}[\boldsymbol{\tau_1},\boldsymbol{\tau_2}]
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{FValRel} \;=\; \{\, \mathrm{VR} = (\tau_1,\tau_2,\varphi^F,\varphi^C,\varphi^A) \mid\;& \varphi^F \in \mathrm{ValRel}[\tau_1,\tau_2] \wedge \\
& \varphi^C \in \mathrm{TransRel}^{\mathcal{C}}[\tau_1,\tau_2] \;\wedge\; \varphi^A \in \mathrm{TransRel}^{\mathcal{A}}[\tau_1{}^{\langle\mathcal{C}\rangle},\tau_2{}^{\langle\mathcal{C}\rangle}] \wedge \\
& \mathcal{CF}(\tau_1,\tau_2,\varphi^F) \subseteq \varphi^C \;\wedge\; \mathcal{FC}(\tau_1,\tau_2,\varphi^C) \subseteq \varphi^F \wedge \\
& \mathcal{AC}(\tau_1{}^{\langle\mathcal{C}\rangle},\tau_2{}^{\langle\mathcal{C}\rangle},\varphi^C) \subseteq \varphi^A \;\wedge\; \mathcal{CA}(\tau_1{}^{\langle\mathcal{C}\rangle},\tau_2{}^{\langle\mathcal{C}\rangle},\varphi^A) \subseteq \varphi^C\}
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{CValRel} \;=\; \{\, \mathrm{VR} = (\boldsymbol{\tau_1},\boldsymbol{\tau_2},\varphi^C,\varphi^A) \mid\;& \varphi^C \in \mathrm{ValRel}[\boldsymbol{\tau_1},\boldsymbol{\tau_2}] \wedge \\
& \varphi^A \in \mathrm{TransRel}^{\mathcal{A}}[\boldsymbol{\tau_1},\boldsymbol{\tau_2}] \;\wedge\; \mathcal{AC}(\boldsymbol{\tau_1},\boldsymbol{\tau_2},\varphi^C) \subseteq \varphi^A \;\wedge\; \mathcal{CA}(\boldsymbol{\tau_1},\boldsymbol{\tau_2},\varphi^A) \subseteq \varphi^C\}
\end{aligned}
$$

$$
\mathrm{AValRel} \;=\; \{\, \mathrm{VR} = (\tau_1,\tau_2,\varphi^A) \mid \varphi^A \in \mathrm{ValRel}[\tau_1,\tau_2]\}
$$

Fig. 8. Admissible Relations

Boundary cancellation requirements are straightforward to state, but we must account for the fact that not every relation on C or A values relates terms of translation type. The first layer of our admissible relations definition, $\mathrm{ValRel}[\tau_1, \tau_2]$, requires monotonicity and "forward" boundary cancellation, that is, the cases of boundary cancellation where we translate a value to a language further forward along the compiler pipeline, and then back. This is given in the top part of Figure 8.

The second layer, $\mathrm{TransRel}$, also requires backward boundary cancellation when it is appropriate, that is, when we are viewing a particular relation φ as being a translation. It is given in the second part of Figure 8.

Now we need to enforce the bridge lemmas. Since $\alpha^{\langle \mathcal{C} \rangle} = \lceil \alpha \rceil$, the base cases of the bridge lemmas require us to show that the translations of elements of $\mathcal{V}[\![\alpha]\!]\rho$ are elements of $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho$. Therefore, we need to define not only our admissibility criterion but also $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho$ in such as way as to enable a proof of the bridge lemma.

Since $\lceil \alpha \rceil$ stands for the translation of whatever type instantiates α, it makes sense to think of $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho$ as the translation of the *interpretation* of α. This suggests a definition mirroring the bridge lemma itself:

$$\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho = \{(W, \mathbf{v_1}, \mathbf{v_2} \mid \mathbf{CF}^{\rho_1(\alpha)}(\mathsf{v}_1) = \mathbf{v_1'} \wedge \mathbf{CF}^{\rho_2(\alpha)}(\mathsf{v}_2) = \mathbf{v_2'} \wedge (W, \mathsf{v}_1, \mathsf{v}_2) \in \rho(\alpha).\varphi\}$$

Indeed, the bridge lemmas hold under this definition. But with this solution, forward boundary cancellation does not hold for $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho$. To see this intuitively, recall that different sequences of translations produce syntactically distinct values, even starting from the same value and ending up in the same language. Forward boundary cancellation requires $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho$ to be inhabited by values that were produced by translating *up* from A after any other translations. Though we can appeal to boundary cancellation properties of $\rho(\alpha).\varphi$ to cover many sequences of translations, the definition still only allows values that were last translated *down* from F.

One strategy we explored to overcome this was to define $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho$ as a *closure* of the set above. But directly closing this set with respect to the boundary cancellation operations we need disrupts the proof of the bridge lemma, and a more general closure with respect to equivalence, such as $\top\top$-closure, fails because we need to use this equivalence-closure before we have proven that applying opposite translations actually produces equivalent values (since this property is exactly boundary cancellation).

Ultimately, instead of trying to do all the work in the definition of $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho$, we take a different approach, and define the needed "translations" of each relation φ upfront. We do this by changing the structure of VR to include not just one relation φ on values in the language of the type variable whose interpretation is being given, but also an additional relation in each language below that. Thus, interpretations of F type variables contain relations φ^F, φ^C, and φ^A; interpretations of C type variables contain relations φ^C and φ^A; and interpretations of A type variables contain only relations φ^A. We require that these relations satisfy bridge properties between *each other*, as shown in the bottom half of Figure 8. We define $\mathcal{V}[\![\alpha]\!]\rho = \rho(\alpha).\varphi^F$, $\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho = \rho(\alpha).\varphi^C$, and the other variable and suspension cases of $\mathcal{V}$ similarly, as shown in Figure 6.

At the end of Appendix B, we give a simple example of proving a contextual equivalence that demonstrates how we can construct these multiple-relation interpretations such that all the needed properties are satisfied.

Verifying An Open Compiler Using Multi-Language Semantics: Appendix B: Complete Definitions and Proofs

James T. Perconti Amal Ahmed

Contents

1 Source language: F

$$
\begin{aligned}
\tau &::= \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \forall[\overline{\alpha}].(\overline{\tau}) \to \tau \mid \exists \alpha.\tau \mid \mu\alpha.\tau \mid \langle \overline{\tau} \rangle \\
\mathsf{e} &::= \mathsf{t} \\
\mathsf{t} &::= \mathsf{x} \mid () \mid \mathsf{n} \mid \mathsf{t}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{t}\ \mathsf{t} \mid \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \mathsf{t}\,[\overline{\tau}]\,\overline{\mathsf{t}} \mid \mathsf{pack}\langle \tau, \mathsf{t} \rangle\ \mathsf{as}\ \exists\alpha.\tau \mid \mathsf{unpack}\ \langle \alpha, \mathsf{x} \rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t} \\
&\quad \mid \mathsf{unfold}\ \mathsf{t} \mid \langle \overline{\mathsf{t}} \rangle \mid \pi_{\mathsf{i}}(\mathsf{t}) \\
\mathsf{p} &::= + \mid - \mid * \\
\mathsf{v} &::= () \mid \mathsf{n} \mid \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \mathsf{pack}\langle \tau, \mathsf{v} \rangle\ \mathsf{as}\ \exists\alpha.\tau \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v} \mid \langle \overline{\mathsf{v}} \rangle \\
\mathsf{E} &::= [\cdot] \mid \mathsf{E}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{v}\ \mathsf{p}\ \mathsf{E} \mid \mathsf{if0}\ \mathsf{E}\ \mathsf{t}\ \mathsf{t} \mid \mathsf{E}\,[\overline{\tau}]\,\overline{\mathsf{t}} \mid \mathsf{v}\,[\overline{\tau}]\,\overline{\mathsf{v}}\,\mathsf{E}\,\overline{\mathsf{t}} \mid \mathsf{pack}\langle \tau, \mathsf{E} \rangle\ \mathsf{as}\ \exists\alpha.\tau \mid \mathsf{unpack}\ \langle \alpha, \mathsf{x} \rangle = \mathsf{E}\ \mathsf{in}\ \mathsf{t} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{E} \\
&\quad \mid \mathsf{unfold}\ \mathsf{E} \mid \langle \overline{\mathsf{v}}, \mathsf{E}, \overline{\mathsf{t}} \rangle \mid \pi_{\mathsf{i}}(\mathsf{E}) \\
\Delta &::= \cdot \mid \Delta, \alpha \\
\Gamma &::= \cdot \mid \Gamma, \mathsf{x}:\tau
\end{aligned}
$$

1.1 Well-Formed Type $\boxed{\Delta \vdash \tau}$

$$\frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad \frac{}{\Delta \vdash \mathsf{unit}} \qquad \frac{}{\Delta \vdash \mathsf{int}} \qquad \frac{\overline{\Delta, \overline{\alpha} \vdash \tau} \qquad \Delta, \overline{\alpha} \vdash \tau'}{\Delta \vdash \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \exists\alpha.\tau} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \mu\alpha.\tau} \qquad \frac{\Delta \vdash \tau_1 \quad \cdots \quad \Delta \vdash \tau_n}{\Delta \vdash \langle \tau_1, \ldots, \tau_n \rangle}$$

1.2 Well-Formed Type Environment $\boxed{\Delta \vdash \Gamma}$

$$\frac{}{\Delta \vdash \cdot} \qquad \frac{\Delta \vdash \Gamma \qquad \Delta \vdash \tau}{\Delta \vdash \Gamma, \mathsf{x}:\tau}$$

1.3 Well-Typed Component $\boxed{\Delta; \Gamma \vdash \mathsf{e}:\tau}$

$$\frac{\mathsf{x}:\tau \in \Gamma}{\Delta; \Gamma \vdash \mathsf{x}:\tau} \qquad \frac{}{\Delta; \Gamma \vdash ():\mathsf{unit}} \qquad \frac{}{\Delta; \Gamma \vdash \mathsf{n}:\mathsf{int}} \qquad \frac{\Delta; \Gamma \vdash \mathsf{t}_1:\mathsf{int} \qquad \Delta; \Gamma \vdash \mathsf{t}_2:\mathsf{int}}{\Delta; \Gamma \vdash \mathsf{t}_1\ \mathsf{p}\ \mathsf{t}_2:\mathsf{int}}$$

$$\frac{\Delta; \Gamma \vdash \mathsf{t}_1:\mathsf{int} \qquad \Delta; \Gamma \vdash \mathsf{t}_2:\tau \qquad \Delta; \Gamma \vdash \mathsf{t}_3:\tau}{\Delta; \Gamma \vdash \mathsf{if0}\ \mathsf{t}_1\ \mathsf{t}_2\ \mathsf{t}_3:\tau} \qquad \frac{\Delta, \overline{\alpha}; \Gamma, \overline{\mathsf{x}:\tau} \vdash \mathsf{t}:\tau'}{\Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t}:\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}$$

$$\frac{\Delta; \Gamma \vdash \mathsf{t}_0:\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2 \qquad \Delta \vdash \overline{\tau} \qquad \Delta; \Gamma \vdash \overline{\mathsf{t}}:\overline{\tau_1[\tau/\alpha]}}{\Delta; \Gamma \vdash \mathsf{t}_0\,[\overline{\tau}]\,\overline{\mathsf{t}}:\tau_2[\overline{\tau/\alpha}]} \qquad \frac{\Delta; \Gamma \vdash \mathsf{t}:\tau[\tau'/\alpha]}{\Delta; \Gamma \vdash \mathsf{pack}\langle \tau', \mathsf{t} \rangle\ \mathsf{as}\ \exists\alpha.\tau:\exists\alpha.\tau}$$

$$\frac{\Delta; \Gamma \vdash \mathsf{t}_1:\exists\alpha.\tau \qquad \Delta, \alpha; \Gamma, \mathsf{x}:\tau \vdash \mathsf{t}_2:\tau'}{\Delta; \Gamma \vdash \mathsf{unpack}\ \langle \alpha, \mathsf{x} \rangle = \mathsf{t}_1\ \mathsf{in}\ \mathsf{t}_2:\tau'} \qquad \frac{\Delta; \Gamma \vdash \mathsf{t}:\tau[\mu\alpha.\tau/\alpha]}{\Delta; \Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t}:\mu\alpha.\tau} \qquad \frac{\Delta; \Gamma \vdash \mathsf{t}:\mu\alpha.\tau}{\Delta; \Gamma \vdash \mathsf{unfold}\ \mathsf{t}:\tau[\mu\alpha.\tau/\alpha]}$$

$$\frac{\Delta; \Gamma \vdash \mathsf{t}_1:\tau_1 \qquad \cdots \qquad \Delta; \Gamma \vdash \mathsf{t}_n:\tau_n}{\Delta; \Gamma \vdash \langle \mathsf{t}_1, \ldots, \mathsf{t}_n \rangle:\langle \tau_1, \ldots, \tau_n \rangle} \qquad \frac{\Delta; \Gamma \vdash \mathsf{t}:\langle \tau_1, \ldots, \tau_n \rangle}{\Delta; \Gamma \vdash \pi_{\mathsf{i}}(\mathsf{t}):\tau_{\mathsf{i}}}$$

1.4 Reduction Relation $\boxed{\mathsf{e} \longmapsto \mathsf{e}'}$

$$
\begin{array}{lll}
\mathsf{E}[\mathsf{n}_1\ \mathsf{p}\ \mathsf{n}_2] & \longmapsto \mathsf{E}[\mathrm{prim}(\mathsf{p}, \mathsf{n}_1, \mathsf{n}_2)] & \\
\mathsf{E}[\mathsf{if0}\,0\ \mathsf{t}_1\ \mathsf{t}_2] & \longmapsto \mathsf{E}[\mathsf{t}_1] & \\
\mathsf{E}[\mathsf{if0}\,\mathsf{n}\ \mathsf{t}_1\ \mathsf{t}_2] & \longmapsto \mathsf{E}[\mathsf{t}_2] & \mathsf{n} \neq 0 \\
\mathsf{E}[\lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\tau}).\mathsf{t}\,[\overline{\tau'}]\,\overline{\mathsf{v}}] & \longmapsto \mathsf{E}[\mathsf{t}[\overline{\tau'}/\overline{\alpha}][\overline{\mathsf{v}}/\overline{\mathsf{x}}]] & \\
\mathsf{E}[\mathsf{unpack}\,\langle\alpha, \mathsf{x}\rangle = (\mathsf{pack}\langle\tau', \mathsf{v}\rangle\,\mathsf{as}\,\exists\alpha.\tau)\ \mathsf{in}\ \mathsf{t}] & \longmapsto \mathsf{E}[\mathsf{t}[\tau'/\alpha][\mathsf{v}/\mathsf{x}]] & \\
\mathsf{E}[\mathsf{unfold}\,(\mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{v})] & \longmapsto \mathsf{E}[\mathsf{v}] & \\
\mathsf{E}[\pi_\mathsf{i}(\langle \mathsf{v}_1, \ldots, \mathsf{v}_\mathsf{n}\rangle)] & \longmapsto \mathsf{E}[\mathsf{v}_\mathsf{i}] &
\end{array}
$$

2 Closure-converted language: C

$$
\begin{array}{rcl}
\tau & ::= & \alpha \mid \mathbf{unit} \mid \mathbf{int} \mid \forall[\overline{\alpha}].(\overline{\tau}) \to \tau \mid \exists \alpha.\tau \mid \mu\alpha.\tau \mid \langle \overline{\tau} \rangle \\
\mathbf{e} & ::= & \mathbf{t} \\
\mathbf{t} & ::= & \mathbf{x} \mid () \mid \mathbf{n} \mid \mathbf{t}\ \mathbf{p}\ \mathbf{t} \mid \mathbf{if0}\ \mathbf{t}\ \mathbf{t}\ \mathbf{t} \mid \lambda[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t} \mid \mathbf{t}\,[]\,\overline{\mathbf{t}} \mid \mathbf{t}[\tau] \mid \mathbf{pack}\langle\tau,\mathbf{t}\rangle\ \mathbf{as}\ \exists\alpha.\tau \\
 & & \mid \mathbf{unpack}\ \langle\alpha,\mathbf{x}\rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t} \mid \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{t} \mid \mathbf{unfold}\ \mathbf{t} \mid \langle\overline{\mathbf{t}}\rangle \mid \pi_{\mathbf{i}}(\mathbf{t}) \\
\mathbf{p} & ::= & + \mid - \mid * \\
\mathbf{v} & ::= & () \mid \mathbf{n} \mid \lambda[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t} \mid \mathbf{pack}\langle\tau,\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\tau \mid \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{v} \mid \langle\overline{\mathbf{v}}\rangle \mid \mathbf{v}[\tau] \\
\mathbf{E} & ::= & [\cdot] \mid \mathbf{E}\ \mathbf{p}\ \mathbf{t} \mid \mathbf{v}\ \mathbf{p}\ \mathbf{E} \mid \mathbf{if0}\ \mathbf{E}\ \mathbf{t}\ \mathbf{t} \mid \mathbf{E}\,[]\,\overline{\mathbf{t}} \mid \mathbf{v}\,[\overline{\tau}]\,\overline{\mathbf{v}}\,\mathbf{E}\,\overline{\mathbf{t}} \mid \mathbf{E}[\tau] \mid \mathbf{pack}\langle\tau,\mathbf{E}\rangle\ \mathbf{as}\ \exists\alpha.\tau \\
 & & \mid \mathbf{unpack}\ \langle\alpha,\mathbf{x}\rangle = \mathbf{E}\ \mathbf{in}\ \mathbf{t} \mid \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{E} \mid \mathbf{unfold}\ \mathbf{E} \mid \langle\overline{\mathbf{v}},\mathbf{E},\overline{\mathbf{t}}\rangle \mid \pi_{\mathbf{i}}(\mathbf{E}) \\
\Delta & ::= & \cdot \mid \Delta,\alpha \\
\Gamma & ::= & \cdot \mid \Gamma,\mathbf{x}:\tau
\end{array}
$$

2.1 Well-Formed Type $\boxed{\Delta \vdash \tau}$

This judgment is defined exactly as in F.

$$\frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad \frac{}{\Delta \vdash \mathbf{unit}} \qquad \frac{}{\Delta \vdash \mathbf{int}} \qquad \frac{\overline{\Delta,\overline{\alpha} \vdash \tau} \qquad \Delta,\overline{\alpha} \vdash \tau'}{\Delta \vdash \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'} \qquad \frac{\Delta,\alpha \vdash \tau}{\Delta \vdash \exists\alpha.\tau} \qquad \frac{\Delta,\alpha \vdash \tau}{\Delta \vdash \mu\alpha.\tau} \qquad \frac{\Delta \vdash \tau_1 \quad \cdots \quad \Delta \vdash \tau_n}{\Delta \vdash \langle\tau_1,\ldots,\tau_n\rangle}$$

2.2 Well-Formed Type Environment $\boxed{\Delta \vdash \Gamma}$

$$\frac{}{\Delta \vdash \cdot} \qquad \frac{\Delta \vdash \Gamma \qquad \Delta \vdash \tau}{\Delta \vdash \Gamma,\mathbf{x}:\tau}$$

2.3 Well-Typed Component $\boxed{\Delta;\Gamma \vdash \mathbf{e}:\tau}$

The type rules for abstraction and application are the only rules that differ from F:

$$\frac{\overline{\alpha};\overline{\mathbf{x}:\tau} \vdash \mathbf{t}:\tau'}{\Delta;\Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t}:\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'} \qquad \frac{\Delta;\Gamma \vdash \mathbf{t}:\forall[].(\overline{\tau}) \to \tau' \qquad \Delta;\Gamma \vdash \overline{\mathbf{t}}:\overline{\tau}}{\Delta;\Gamma \vdash \mathbf{t}\,[]\,\overline{\mathbf{t}}:\tau'}$$

$$\frac{\Delta;\Gamma \vdash \mathbf{t}:\forall[\beta,\overline{\alpha}].(\overline{\tau}) \to \tau' \qquad \Delta \vdash \tau_0}{\Delta;\Gamma \vdash \mathbf{t}[\tau_0]:\forall[\overline{\alpha}].(\overline{\tau[\tau_0/\beta]}) \to \tau'[\tau_0/\beta]}$$

For completeness, here are the rules that are identical to F rules:

$$\frac{\mathbf{x}:\tau \in \Gamma}{\Delta;\Gamma \vdash \mathbf{x}:\tau} \qquad \frac{}{\Delta;\Gamma \vdash ():\mathbf{unit}} \qquad \frac{}{\Delta;\Gamma \vdash \mathbf{n}:\mathbf{int}} \qquad \frac{\Delta;\Gamma \vdash \mathbf{t}_1:\mathbf{int} \qquad \Delta;\Gamma \vdash \mathbf{t}_2:\mathbf{int}}{\Delta;\Gamma \vdash \mathbf{t}_1\ \mathbf{p}\ \mathbf{t}_2:\mathbf{int}}$$

$$\frac{\Delta;\Gamma \vdash \mathbf{t}_1:\mathbf{int} \qquad \Delta;\Gamma \vdash \mathbf{t}_2:\tau \qquad \Delta;\Gamma \vdash \mathbf{t}_3:\tau}{\Delta;\Gamma \vdash \mathbf{if0}\ \mathbf{t}_1\ \mathbf{t}_2\ \mathbf{t}_3:\tau} \qquad \frac{\Delta;\Gamma \vdash \mathbf{t}:\tau[\tau'/\alpha]}{\Delta;\Gamma \vdash \mathbf{pack}\langle\tau',\mathbf{t}\rangle\ \mathbf{as}\ \exists\alpha.\tau:\exists\alpha.\tau}$$

$$\frac{\Delta;\Gamma \vdash \mathbf{t}_1:\exists\alpha.\tau \qquad \Delta,\alpha;\Gamma,\mathbf{x}:\tau \vdash \mathbf{t}_2:\tau'}{\Delta;\Gamma \vdash \mathbf{unpack}\ \langle\alpha,\mathbf{x}\rangle = \mathbf{t}_1\ \mathbf{in}\ \mathbf{t}_2:\tau'} \qquad \frac{\Delta;\Gamma \vdash \mathbf{t}:\tau[\mu\alpha.\tau/\alpha]}{\Delta;\Gamma \vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{t}:\mu\alpha.\tau} \qquad \frac{\Delta;\Gamma \vdash \mathbf{t}:\mu\alpha.\tau}{\Delta;\Gamma \vdash \mathbf{unfold}\ \mathbf{t}:\tau[\mu\alpha.\tau/\alpha]}$$

$$\frac{\Delta;\Gamma \vdash \mathbf{t}_1:\tau_1 \qquad \cdots \qquad \Delta;\Gamma \vdash \mathbf{t}_n:\tau_n}{\Delta;\Gamma \vdash \langle\mathbf{t}_1,\ldots,\mathbf{t}_n\rangle:\langle\tau_1,\ldots,\tau_n\rangle} \qquad \frac{\Delta;\Gamma \vdash \mathbf{t}:\langle\tau_1,\ldots,\tau_n\rangle}{\Delta;\Gamma \vdash \pi_{\mathbf{i}}(\mathbf{t}):\tau_{\mathbf{i}}}$$

2.4 Reduction Relation $\boxed{\mathbf{e} \longmapsto \mathbf{e'}}$

The reduction relation is also identical to that of F.

$$
\begin{array}{lll}
\mathbf{E}[\mathbf{n_1\ p\ n_2}] & \longmapsto \mathbf{E}[\mathbf{prim(p, n_1, n_2)}] & \\
\mathbf{E}[\mathbf{if0\ 0\ t_1\ t_2}] & \longmapsto \mathbf{E}[\mathbf{t_1}] & \\
\mathbf{E}[\mathbf{if0\ n\ t_1\ t_2}] & \longmapsto \mathbf{E}[\mathbf{t_2}] & \mathbf{n} \neq \mathbf{0} \\
\mathbf{E}[\boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{t}\ [\overline{\boldsymbol{\tau'}}]\ \overline{\mathbf{v}}] & \longmapsto \mathbf{E}[\mathbf{t}[\overline{\boldsymbol{\tau'}}/\overline{\boldsymbol{\alpha}}][\overline{\mathbf{v}}/\overline{\mathbf{x}}]] & \\
\mathbf{E}[\mathbf{unpack}\ \langle \boldsymbol{\alpha}, \mathbf{x}\rangle = (\mathbf{pack}\langle \boldsymbol{\tau'}, \mathbf{v}\rangle\ \mathbf{as}\ \exists \boldsymbol{\alpha}.\boldsymbol{\tau})\ \mathbf{in\ t}] & \longmapsto \mathbf{E}[\mathbf{t}[\boldsymbol{\tau'}/\boldsymbol{\alpha}][\mathbf{v}/\mathbf{x}]] & \\
\mathbf{E}[\mathbf{unfold}\ (\mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{v})] & \longmapsto \mathbf{E}[\mathbf{v}] & \\
\mathbf{E}[\boldsymbol{\pi}_\mathbf{i}(\langle \mathbf{v_1}, \ldots, \mathbf{v_n}\rangle)] & \longmapsto \mathbf{E}[\mathbf{v_i}] &
\end{array}
$$

2.5 Compiling F to C

2.5.1 Type Translation

$$\alpha^{\mathcal{C}} = \boldsymbol{\alpha} \qquad \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\mathcal{C}} = \exists\boldsymbol{\beta}.\langle(\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\beta}, \overline{\tau^{\mathcal{C}}}) \to \tau'^{\mathcal{C}}), \boldsymbol{\beta}\rangle$$

$$\mathsf{unit}^{\mathcal{C}} = \mathbf{unit} \qquad \exists\alpha.\tau^{\mathcal{C}} = \exists\boldsymbol{\alpha}.\tau^{\mathcal{C}}$$

$$\mathsf{int}^{\mathcal{C}} = \mathbf{int} \qquad \mu\alpha.\tau^{\mathcal{C}} = \boldsymbol{\mu\alpha}.\tau^{\mathcal{C}}$$

$$\langle\tau_1, \ldots, \tau_n\rangle^{\mathcal{C}} = \langle\tau_1{}^{\mathcal{C}}, \ldots, \tau_n{}^{\mathcal{C}}\rangle$$

2.5.2 Compiler $\boxed{\Delta; \Gamma \vdash e : \tau \rightsquigarrow \mathbf{e}}$

If the compilation judgment holds, then it follows that $\Delta; \Gamma \vdash e : \tau$ and $\Delta^{\mathcal{C}}; \Gamma^{\mathcal{C}} \vdash \mathbf{e} : \tau^{\mathcal{C}}$.

Most of the rules simply proceed by structural induction:

$$\frac{x : \tau \in \Gamma}{\Delta; \Gamma \vdash x : \tau \rightsquigarrow \mathbf{x}} \qquad \frac{}{\Delta; \Gamma \vdash () : \mathsf{unit} \rightsquigarrow ()} \qquad \frac{}{\Delta; \Gamma \vdash n : \mathsf{int} \rightsquigarrow \mathbf{n}} \qquad \frac{\Delta; \Gamma \vdash t_1 : \mathsf{int} \rightsquigarrow \mathbf{t_1} \qquad \Delta; \Gamma \vdash t_2 : \mathsf{int} \rightsquigarrow \mathbf{t_2}}{\Delta; \Gamma \vdash t_1\ \mathsf{p}\ t_2 : \mathsf{int} \rightsquigarrow \mathbf{t_1\ p\ t_2}}$$

$$\frac{\Delta; \Gamma \vdash t_1 : \mathsf{int} \rightsquigarrow \mathbf{t_1} \qquad \Delta; \Gamma \vdash t_2 : \tau \rightsquigarrow \mathbf{t_2} \qquad \Delta; \Gamma \vdash t_3 : \tau \rightsquigarrow \mathbf{t_3}}{\Delta; \Gamma \vdash \mathsf{if0}\ t_1\ t_2\ t_3 : \tau \rightsquigarrow \mathbf{if0\ t_1\ t_2\ t_3}} \qquad \frac{\Delta; \Gamma \vdash t : \tau[\tau'/\alpha] \rightsquigarrow \mathbf{t}}{\Delta; \Gamma \vdash \mathsf{pack}\langle\tau', t\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau \rightsquigarrow \mathbf{pack}\langle\tau'^{\mathcal{C}}, \mathbf{t}\rangle\ \mathbf{as}\ \exists\alpha.\tau^{\mathcal{C}}}$$

$$\frac{\Delta; \Gamma \vdash t_1 : \exists\alpha.\tau \rightsquigarrow \mathbf{t_1} \qquad \Delta, \alpha; \Gamma, x : \tau \vdash t_2 : \tau' \rightsquigarrow \mathbf{t_2}}{\Delta; \Gamma \vdash \mathsf{unpack}\ \langle\alpha, x\rangle = t_1\ \mathsf{in}\ t_2 : \tau' \rightsquigarrow \mathbf{unpack}\ \langle\boldsymbol{\alpha}, \mathbf{x}\rangle = \mathbf{t_1}\ \mathbf{in}\ \mathbf{t_2}} \qquad \frac{\Delta; \Gamma \vdash t : \tau[\mu\alpha.\tau/\alpha] \rightsquigarrow \mathbf{t}}{\Delta; \Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\ t : \mu\alpha.\tau \rightsquigarrow \mathbf{fold}_{\mu\alpha.\tau^{\mathcal{C}}}\ \mathbf{t}}$$

$$\frac{\Delta; \Gamma \vdash t : \mu\alpha.\tau \rightsquigarrow \mathbf{t}}{\Delta; \Gamma \vdash \mathsf{unfold}\ t : \tau[\mu\alpha.\tau/\alpha] \rightsquigarrow \mathbf{unfold\ t}} \qquad \frac{\Delta; \Gamma \vdash t_1 : \tau_1 \rightsquigarrow \mathbf{t_1} \qquad \ldots \qquad \Delta; \Gamma \vdash t_n : \tau_n \rightsquigarrow \mathbf{t_n}}{\Delta; \Gamma \vdash \langle t_1, \ldots, t_n\rangle : \langle\tau_1, \ldots, \tau_n\rangle \rightsquigarrow \langle\mathbf{t_1}, \ldots, \mathbf{t_2}\rangle}$$

$$\frac{\Delta; \Gamma \vdash t : \langle\tau_1, \ldots, \tau_n\rangle \rightsquigarrow \mathbf{t}}{\Delta; \Gamma \vdash \pi_i(t) : \tau_i \rightsquigarrow \boldsymbol{\pi_i(t)}}$$

The interesting rules are those for functions and application. To compile a function $\lambda[\overline{\alpha}](\overline{x:\tau}).t$, we first need to find its free type variables and term variables, and determine the type of the closure environment we will build. We next compile the body of the function, and finally, we build a closure.

$$\frac{\begin{array}{c}y_1, \ldots, y_m = \mathrm{fv}(\lambda[\overline{\alpha}](\overline{x:\tau}).t) \qquad \beta_1, \ldots, \beta_k = \mathrm{ftv}(\lambda[\overline{\alpha}](\overline{x:\tau}).t) \qquad \boldsymbol{\tau_{env}} = \langle(\Gamma(y_1))^{\mathcal{C}}, \ldots, (\Gamma(y_m))^{\mathcal{C}}\rangle \\ \Delta, \overline{\alpha}; \Gamma, \overline{x:\tau} \vdash t : \tau' \rightsquigarrow \mathbf{t} \qquad \mathbf{v} = \boldsymbol{\lambda[\overline{\beta}, \overline{\alpha}](z : \tau_{env}, \overline{x : \tau^{\mathcal{C}}}).(t[\pi_1(z)/y_1] \cdots [\pi_m(z)/y_m])}\end{array}}{\Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{x:\tau}).t : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau' \rightsquigarrow \mathbf{pack}\langle\boldsymbol{\tau_{env}}, \langle\mathbf{v}[\overline{\boldsymbol{\beta}}], \langle\overline{\mathbf{y}}\rangle\rangle\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha'}.\langle(\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\alpha'}, \overline{\tau^{\mathcal{C}}}) \to \tau'^{\mathcal{C}}), \boldsymbol{\alpha'}\rangle}$$

To compile an application, we must unpack the closure that will be produced in the function position, and apply it to its environment as well as its original arguments.

$$\frac{\Delta; \Gamma \vdash t_0 : \forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2 \rightsquigarrow \mathbf{t_0} \qquad \Delta \vdash \overline{\tau} \qquad \Delta; \Gamma \vdash \overline{t} : \overline{\tau_1[\tau/\alpha]} \rightsquigarrow \overline{\mathbf{t}}}{\Delta; \Gamma \vdash t_0\ [\overline{\tau}]\ \overline{t} : \tau_2[\overline{\tau/\alpha}] \rightsquigarrow \mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{z}\rangle = \mathbf{t_0}\ \mathbf{in}\ \boldsymbol{\pi_1(z)}\ [\overline{\tau^{\mathcal{C}}}]\ \boldsymbol{\pi_2(z)}, \overline{\mathbf{t}}}$$

3 F + C

$$
\begin{array}{ll}
\tau ::= \cdots \mid \mathsf{L}\langle \boldsymbol{\tau} \rangle & \tau ::= \tau \mid \boldsymbol{\tau} \\
\mathsf{t} ::= \cdots \mid {}^{\tau}\mathcal{FC}\,\mathbf{e} & e ::= \mathsf{e} \mid \mathbf{e} \\
\mathsf{v} ::= \cdots \mid {}^{\mathsf{L}\langle\tau\rangle}\mathcal{FC}\,\mathbf{v} & v ::= \mathsf{v} \mid \mathbf{v} \\
\mathsf{E} ::= \cdots \mid {}^{\tau}\mathcal{FC}\,\mathbf{E} & E ::= \mathsf{E} \mid \mathbf{E} \\
\boldsymbol{\tau} ::= \cdots \mid \lceil \alpha \rceil & M ::= \cdot \\
\mathbf{t} ::= \cdots \mid \mathcal{CF}^{\tau}\,\mathsf{e} & \Delta ::= \cdot \mid \Delta, \alpha \mid \Delta, \boldsymbol{\alpha} \\
\mathbf{E} ::= \cdots \mid \mathcal{CF}^{\tau}\,\mathsf{E} & \Gamma ::= \cdot \mid \Gamma, \mathsf{x}{:}\tau \mid \Gamma, \mathbf{x}{:}\boldsymbol{\tau}
\end{array}
$$

To build a language of interoperability for F and C, we add boundary terms to both languages, lumps to F types τ, and suspended F type variables to C types $\boldsymbol{\tau}$.

FC types, components, values, and evaluation contexts are just the union of F and C types, components, values, and evaluation contexts. We add memory M to the syntax of FC for convenience later, when we augment our multi-language for interoperability with languages that deal with memory. For now, M is just a piece of syntax that does nothing. Type environments Δ and Γ may contain a mixture of F and C variables.

3.1 Boundary Type Translation

$$
\begin{array}{rlrl}
\alpha^{\langle \mathcal{C} \rangle} &= \lceil \alpha \rceil & \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle \mathcal{C} \rangle} &= \exists \boldsymbol{\beta}.\langle \left(\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\beta}, \overline{\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]}) \to \tau'^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil] \right), \boldsymbol{\beta} \rangle \\
\mathsf{unit}^{\langle \mathcal{C} \rangle} &= \mathbf{unit} & \exists \alpha.\tau^{\langle \mathcal{C} \rangle} &= \exists \boldsymbol{\alpha}.(\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]) \\
\mathsf{int}^{\langle \mathcal{C} \rangle} &= \mathbf{int} & \mu \alpha.\tau^{\langle \mathcal{C} \rangle} &= \boldsymbol{\mu} \boldsymbol{\alpha}.(\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]) \\
\mathsf{L}\langle \boldsymbol{\tau} \rangle^{\langle \mathcal{C} \rangle} &= \boldsymbol{\tau} & \langle \tau_1, \ldots, \tau_n \rangle^{\langle \mathcal{C} \rangle} &= \langle \tau_1{}^{\langle \mathcal{C} \rangle}, \ldots, \tau_n{}^{\langle \mathcal{C} \rangle} \rangle
\end{array}
$$

3.2 Type Substutution

$$\lceil \alpha \rceil[\tau/\alpha] = \tau^{\langle \mathcal{C} \rangle}$$

3.3 Well-formed Type $\boxed{\Delta \vdash \tau}$

Adapt the rules for $\Delta \vdash \tau$ and $\boldsymbol{\Delta} \vdash \boldsymbol{\tau}$ by changing the environments to Δ (multilanguage environment instead of a single-language environment), and add the following rules:

$$\frac{\Delta \vdash \boldsymbol{\tau}}{\Delta \vdash \mathsf{L}\langle \boldsymbol{\tau} \rangle} \qquad \frac{\alpha \in \Delta}{\Delta \vdash \lceil \alpha \rceil}$$

3.4 Well-Typed Terms $\boxed{\Delta; \Gamma \vdash e : \tau}$

Adapt the corresponding judgments for F and C by changing all the environments to the appropriate multilanguage environment, and add the following rules:

$$\frac{\Delta; \Gamma \vdash \mathbf{e} : \tau^{\langle \mathcal{C} \rangle}}{\Delta; \Gamma \vdash {}^{\tau}\mathcal{FC}\,\mathbf{e} : \tau} \qquad \frac{\Delta; \Gamma \vdash \mathsf{e} : \tau}{\Delta; \Gamma \vdash \mathcal{CF}^{\tau}\,\mathsf{e} : \tau^{\langle \mathcal{C} \rangle}}$$

3.5 Value Translation

$$
\begin{aligned}
&\mathbf{CF}^{\mathsf{unit}}((), M) && = ((), M)\\
&\mathbf{CF}^{\mathsf{int}}(\mathsf{n}, M) && = (\mathbf{n}, M)\\
&\mathbf{CF}^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}(\mathsf{v}, M) && = (\mathbf{pack}\langle \mathbf{unit}, \langle \mathbf{v}, ()\rangle\rangle \ \mathbf{as}\ (\forall[\overline{\alpha}].(\overline{\tau})\to\tau')^{\langle\mathcal{C}\rangle}, M)\\
&\qquad\qquad \text{where } \mathbf{v} = \boldsymbol{\lambda}[\overline{\alpha}](\mathbf{z}:\mathbf{unit}, \overline{\mathbf{x}:\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]}).\mathcal{C}\mathcal{F}^{\tau'[\mathsf{L}\langle\alpha\rangle/\alpha]}\ (\mathsf{v}\ [\overline{\mathsf{L}\langle\boldsymbol{\alpha}\rangle}]\ \overline{\tau[\mathsf{L}\langle\alpha\rangle/\alpha]\mathcal{F}\mathcal{C}\ \mathbf{x}})\\
&\mathbf{CF}^{\exists\alpha.\tau}(\mathsf{pack}\langle\tau',\mathsf{v}\rangle\ \mathsf{as}\ \exists\alpha.\tau, M) && = (\mathbf{pack}\langle\tau'^{\langle\mathcal{C}\rangle}, \mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\tau^{\langle\mathcal{C}\rangle}, M') \text{ where } \mathbf{CF}^{\tau[\tau'/\alpha]}(\mathsf{v}, M) = (\mathbf{v}, M')\\
&\mathbf{CF}^{\mu\alpha.\tau}(\mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v}, M) && = (\mathbf{fold}_{\mu\alpha.\tau^{\langle\mathcal{C}\rangle}}\ \mathbf{v}, M') \qquad \text{where } \mathbf{CF}^{\tau[\mu\alpha.\tau/\alpha]}(\mathsf{v}, M) = (\mathbf{v}, M')\\
&\mathbf{CF}^{\langle\tau_1,\ldots,\tau_n\rangle}(\langle\mathsf{v}_1,\ldots,\mathsf{v}_n\rangle, M) && = (\langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle, M_{n+1})\\
&\qquad\qquad \text{where } M_1 = M \text{ and } \mathbf{CF}^{\tau_i}(\mathsf{v}_i, M_i) = (\mathbf{v_i}, M_{i+1})\\
&\mathbf{CF}^{\mathsf{L}\langle\tau\rangle}(^{\mathsf{L}\langle\tau\rangle}\mathcal{F}\mathcal{C}\ \mathbf{v}, M) && = (\mathbf{v}, M)
\end{aligned}
$$

$$
\begin{aligned}
&^{\mathsf{unit}}\mathbf{FC}((), M) && = ((), M)\\
&^{\mathsf{int}}\mathbf{FC}(\mathbf{n}, M) && = (\mathsf{n}, M)\\
&^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}\mathbf{FC}(\mathbf{v}, M) && = (\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).{}^{\tau'}\mathcal{F}\mathcal{C}\ \mathbf{e}, M)\\
&\qquad\qquad \text{where } \mathbf{e} = (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = \mathbf{v}\ \mathbf{in}\ \boldsymbol{\pi}_1(\mathbf{y})\ [\overline{\lceil\alpha\rceil}]\ \boldsymbol{\pi}_2(\mathbf{y}), \overline{\mathcal{C}\mathcal{F}^{\tau}\ \mathsf{x}})\\
&^{\exists\alpha.\tau}\mathbf{FC}(\mathbf{pack}\langle\boldsymbol{\tau}',\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\tau^{\langle\mathcal{C}\rangle}, M) && = (\mathsf{pack}\langle\mathsf{L}\langle\boldsymbol{\tau}'\rangle,\mathsf{v}\rangle\ \mathsf{as}\ \exists\alpha.\tau, M') \qquad \text{where } {}^{\tau[\mathsf{L}\langle\tau'\rangle/\alpha]}\mathbf{FC}(\mathbf{v}, M) = (\mathsf{v}, M')\\
&^{\mu\alpha.\tau}\mathbf{FC}(\mathbf{fold}_{\boldsymbol{\mu\alpha.\tau}^{\langle\mathcal{F}\rangle}}\ \mathbf{v}, M) && = (\mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v}, M') \qquad \text{where } {}^{\tau[\mu\alpha.\tau/\alpha]}\mathbf{FC}(\mathbf{v}, M) = (\mathsf{v}, M')\\
&^{\langle\tau_1,\ldots,\tau_n\rangle}\mathbf{FC}(\langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle, M) && = (\langle\mathsf{v}_1,\ldots,\mathsf{v}_n\rangle, M_{n+1})\\
&\qquad\qquad \text{where } M_1 = M \text{ and } {}^{\tau_i}\mathbf{FC}(\mathbf{v_i}, M_i) = (\mathsf{v}_i, M_{i+1})\\
&^{\mathsf{L}\langle\tau\rangle}\mathbf{FC}(\mathbf{v}, M) && = (^{\mathsf{L}\langle\tau\rangle}\mathcal{F}\mathcal{C}\ \mathbf{v}, M)
\end{aligned}
$$

3.6 Reduction Relation $\boxed{\langle M \mid e\rangle \longmapsto \langle M' \mid e'\rangle}$

Lift the F and C reduction rules to the new configuration.

$$\frac{\mathsf{e} \longmapsto \mathsf{e}'}{\langle M \mid E[\mathsf{e}]\rangle \longmapsto \langle M \mid E[\mathsf{e}']\rangle} \qquad \frac{\mathbf{e} \longmapsto \mathbf{e}'}{\langle M \mid E[\mathbf{e}]\rangle \longmapsto \langle M \mid E[\mathbf{e}']\rangle}$$

Also add the following rules for boundary forms:

$$\frac{\mathbf{CF}^{\tau}(\mathsf{v}, M) = (\mathbf{v}, M')}{\langle M \mid E[\mathcal{C}\mathcal{F}^{\tau}\ \mathsf{v}]\rangle \longmapsto \langle M' \mid E[\mathbf{v}]\rangle} \qquad \frac{{}^{\tau}\mathbf{FC}(\mathbf{v}, M) = (\mathsf{v}, M') \qquad \tau \neq \mathsf{L}\langle\boldsymbol{\tau}\rangle}{\langle M \mid E[{}^{\tau}\mathcal{F}\mathcal{C}\ \mathbf{v}]\rangle \longmapsto \langle M' \mid E[\mathsf{v}]\rangle}$$

4 Language with explicit allocation: A

$$
\begin{array}{rcl}
\tau & ::= & \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \exists\alpha.\tau \mid \mu\alpha.\tau \mid \mathsf{ref}\ \psi \mid \mathsf{box}\ \psi \\
\psi & ::= & \forall[\overline{\alpha}].(\overline{\tau}) \to \tau \mid \langle \tau, \ldots, \tau \rangle \\
\mathsf{e} & ::= & (\mathsf{t}, \mathsf{H}) \\
\mathsf{t} & ::= & \mathsf{x} \mid () \mid \mathsf{n} \mid \mathsf{t}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{t}\ \mathsf{t} \mid \ell \mid \mathsf{t}\ []\ \overline{\mathsf{t}} \mid \mathsf{t}[\tau] \mid \mathsf{pack}\langle\tau,\mathsf{t}\rangle\ \mathsf{as}\ \exists\alpha.\tau \mid \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t} \\
 & & \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t} \mid \mathsf{unfold}\ \mathsf{t} \mid \mathsf{ralloc}\ \langle\overline{\mathsf{t}}\rangle \mid \mathsf{balloc}\ \langle\overline{\mathsf{t}}\rangle \mid \mathsf{read}[\mathsf{i}]\ \mathsf{t} \mid \mathsf{write}\ \mathsf{t}\ [\mathsf{i}] \leftarrow \mathsf{t} \\
\mathsf{p} & ::= & + \mid - \mid * \\
\mathsf{v} & ::= & () \mid \mathsf{n} \mid \mathsf{pack}\langle\tau,\mathsf{v}\rangle\ \mathsf{as}\ \exists\alpha.\tau \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{v} \mid \ell \mid \mathsf{v}[\tau] \\
\mathsf{E} & ::= & (\mathsf{E_t}, \cdot) \\
\mathsf{E_t} & ::= & [\cdot] \mid \mathsf{E_t}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{v}\ \mathsf{p}\ \mathsf{E_t} \mid \mathsf{if0}\ \mathsf{E_t}\ \mathsf{t}\ \mathsf{t} \mid \mathsf{E_t}\ []\ \overline{\mathsf{t}} \mid \mathsf{v}\ []\ \overline{\mathsf{v}}\ \mathsf{E_t}\ \overline{\mathsf{t}} \mid \mathsf{E_t}[\tau] \mid \mathsf{pack}\langle\tau,\mathsf{E_t}\rangle\ \mathsf{as}\ \exists\alpha.\tau \\
 & & \mid \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{E_t}\ \mathsf{in}\ \mathsf{t} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{E_t} \mid \mathsf{unfold}\ \mathsf{E_t} \mid \mathsf{ralloc}\ \langle\overline{\mathsf{v}}, \mathsf{E_t}, \overline{\mathsf{t}}\rangle \mid \mathsf{balloc}\ \langle\overline{\mathsf{v}}, \mathsf{E_t}, \overline{\mathsf{t}}\rangle \mid \mathsf{read}[\mathsf{i}]\ \mathsf{E_t} \\
 & & \mid \mathsf{write}\ \mathsf{E_t}\ [\mathsf{i}] \leftarrow \mathsf{t} \mid \mathsf{write}\ \mathsf{v}\ [\mathsf{i}] \leftarrow \mathsf{E_t} \\
\mathsf{H} & ::= & \cdot \mid \mathsf{H}, \ell \mapsto \mathsf{h} \\
\mathsf{h} & ::= & \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\tau}).\mathsf{t} \mid \langle \mathsf{v}, \ldots, \mathsf{v} \rangle \\
\Psi & ::= & \cdot \mid \Psi, \ell : {}^{\nu}\psi \\
\nu & ::= & \mathsf{ref} \mid \mathsf{box} \\
\Delta & ::= & \cdot \mid \Delta, \alpha \\
\Gamma & ::= & \cdot \mid \Gamma, \mathsf{x}:\tau
\end{array}
$$

We will frequently abuse notation by abbreviating $(\mathsf{t}, \cdot)$ as just t.
Also note that $(\mathsf{E_t}, \cdot)[(\mathsf{t}, \mathsf{H})] \stackrel{\text{def}}{=} (\mathsf{E_t}[\mathsf{t}], \mathsf{H})$.

4.1 Well-Formed Type $\boxed{\Delta \vdash \tau}$

$$\frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad \frac{}{\Delta \vdash \mathsf{unit}} \qquad \frac{}{\Delta \vdash \mathsf{int}} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \exists\alpha.\tau} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \mu\alpha.\tau} \qquad \frac{\Delta \vdash^{\mathsf{ref}} \psi}{\Delta \vdash \mathsf{ref}\ \psi} \qquad \frac{\Delta \vdash^{\mathsf{box}} \psi}{\Delta \vdash \mathsf{box}\ \psi}$$

4.2 Well-formed Heap Value Type $\boxed{\Delta \vdash^{\nu} \psi}$

$$\frac{\overline{\Delta, \overline{\alpha} \vdash \tau} \qquad \Delta, \overline{\alpha} \vdash \tau'}{\Delta \vdash^{\mathsf{box}} \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'} \qquad\qquad \frac{\Delta \vdash \tau_1 \quad \cdots \quad \Delta \vdash \tau_n}{\Delta \vdash^{\nu} \langle \tau_1, \ldots, \tau_n \rangle}$$

4.3 Well-formed Heap Type $\boxed{\vdash \Psi}$

$$\frac{\cdot \vdash^{\nu_1} \psi_1 \qquad \cdots \qquad \cdot \vdash^{\nu_n} \psi_n}{\vdash \ell_1 : {}^{\nu_1}\psi_1, \ldots, \ell_n : {}^{\nu_n}\psi_n}$$

4.4 Well-Formed Type Environment $\boxed{\Delta \vdash \Gamma}$

$$\frac{}{\Delta \vdash \cdot} \qquad\qquad \frac{\Delta \vdash \Gamma \qquad \Delta \vdash \tau}{\Delta \vdash \Gamma, \mathsf{x}:\tau}$$

4.5 Well-Typed Heap Value $\boxed{\Psi \vdash \mathsf{h} : \psi}$

$$\frac{\Psi; \overline{\alpha}; \overline{\mathsf{x}:\tau} \vdash \mathsf{t} : \tau'}{\Psi \vdash \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\tau}).\mathsf{t} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'} \qquad\qquad \frac{\Psi; \cdot; \cdot \vdash \mathsf{v_1} : \tau_1 \qquad \cdots \qquad \Psi; \cdot; \cdot \vdash \mathsf{v_n} : \tau_n}{\Psi \vdash \langle \mathsf{v_1}, \ldots, \mathsf{v_n} \rangle : \langle \tau_1, \ldots, \tau_n \rangle}$$

4.6 Well-Typed Heap Fragment $\boxed{\Psi \vdash H : \Psi'}$

$$\frac{\mathrm{dom}(\Psi) \cap \mathrm{dom}(\Psi') = \emptyset \qquad \vdash \Psi' \qquad \Psi, \Psi' \vdash h_1 : \Psi'(\ell_1) \qquad \cdots \qquad \Psi, \Psi' \vdash h_n : \Psi'(\ell_n)}{\Psi \vdash \{\ell_1 \mapsto h_1, \ldots, \ell_n \mapsto h_n\} : \Psi'}$$

4.7 Well-Typed Component $\boxed{\Psi; \Delta; \Gamma \vdash e : \tau}$

$\mathrm{boxheap}(\Psi) \stackrel{\text{def}}{=} \forall (\ell : {}^{\nu}\psi) \in \Psi.\ \nu = \mathsf{box}$

$$\frac{\Psi \vdash H : \Psi' \qquad \mathrm{boxheap}(\Psi) \qquad (\Psi, \Psi'); \Delta; \Gamma \vdash t : \tau}{\Psi; \Delta; \Gamma \vdash (t, H) : \tau} \qquad \frac{x : \tau \in \Gamma}{\Psi; \Delta; \Gamma \vdash x : \tau} \qquad \frac{}{\Psi; \Delta; \Gamma \vdash () : \mathsf{unit}}$$

$$\frac{}{\Psi; \Delta; \Gamma \vdash n : \mathsf{int}} \qquad \frac{\Psi; \Delta; \Gamma \vdash t_1 : \mathsf{int} \qquad \Psi; \Delta; \Gamma \vdash t_2 : \mathsf{int}}{\Psi; \Delta; \Gamma \vdash t_1\ p\ t_2 : \mathsf{int}}$$

$$\frac{\Psi; \Delta; \Gamma \vdash t_1 : \mathsf{int} \qquad \Psi; \Delta; \Gamma \vdash t_2 : \tau \qquad \Psi; \Delta; \Gamma \vdash t_3 : \tau}{\Psi; \Delta; \Gamma \vdash \mathsf{if0}\ t_1\ t_2\ t_3 : \tau} \qquad \frac{\ell : {}^{\mathsf{ref}}\psi \in \Psi}{\Psi; \Delta; \Gamma \vdash \ell : \mathsf{ref}\ \psi} \qquad \frac{\ell : {}^{\mathsf{box}}\psi \in \Psi}{\Psi; \Delta; \Gamma \vdash \ell : \mathsf{box}\ \psi}$$

$$\frac{\Psi; \Delta; \Gamma \vdash t : \mathsf{box}\ \forall[].(\overline{\tau}) \to \tau' \qquad \Psi; \Delta; \Gamma \vdash \overline{t} : \overline{\tau}}{\Psi; \Delta; \Gamma \vdash t\ []\ \overline{t} : \tau'} \qquad \frac{\Psi; \Delta; \Gamma \vdash t : \mathsf{box}\ \forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau' \qquad \Delta \vdash \tau_0}{\Psi; \Delta; \Gamma \vdash t[\tau_0] : \mathsf{box}\ \forall[\overline{\alpha}].(\overline{\tau[\tau_0/\beta]}) \to \tau'[\tau_0/\beta]}$$

$$\frac{\Psi; \Delta; \Gamma \vdash t : \tau[\tau'/\alpha]}{\Psi; \Delta; \Gamma \vdash \mathsf{pack}\langle \tau', t\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau} \qquad \frac{\Psi; \Delta; \Gamma \vdash t_1 : \exists\alpha.\tau \qquad \Psi; \Delta, \alpha; \Gamma, x : \tau \vdash t_2 : \tau'}{\Psi; \Delta; \Gamma \vdash \mathsf{unpack}\ \langle \alpha, x\rangle = t_1\ \mathsf{in}\ t_2 : \tau'}$$

$$\frac{\Psi; \Delta; \Gamma \vdash t : \tau[\mu\alpha.\tau/\alpha]}{\Psi; \Delta; \Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\ t : \mu\alpha.\tau} \qquad \frac{\Psi; \Delta; \Gamma \vdash t : \mu\alpha.\tau}{\Psi; \Delta; \Gamma \vdash \mathsf{unfold}\ t : \tau[\mu\alpha.\tau/\alpha]} \qquad \frac{\Psi; \Delta; \Gamma \vdash \overline{t} : \overline{\tau}}{\Psi; \Delta; \Gamma \vdash \mathsf{ralloc}\ \langle \overline{t}\rangle : \mathsf{ref}\ \langle \overline{\tau}\rangle}$$

$$\frac{\Psi; \Delta; \Gamma \vdash \overline{t} : \overline{\tau}}{\Psi; \Delta; \Gamma \vdash \mathsf{balloc}\ \langle \overline{t}\rangle : \mathsf{box}\ \langle \overline{\tau}\rangle} \qquad \frac{\Psi; \Delta; \Gamma \vdash t : \mathsf{ref}\ \langle \tau_1, \ldots, \tau_i, \ldots, \tau_n\rangle}{\Psi; \Delta; \Gamma \vdash \mathsf{read}[i]\ t : \tau_i}$$

$$\frac{\Psi; \Delta; \Gamma \vdash t : \mathsf{box}\ \langle \tau_1, \ldots, \tau_i, \ldots, \tau_n\rangle}{\Psi; \Delta; \Gamma \vdash \mathsf{read}[i]\ t : \tau_i} \qquad \frac{\Psi; \Delta; \Gamma \vdash t_1 : \mathsf{ref}\ \langle \tau_1, \ldots, \tau_i, \ldots, \tau_n\rangle \qquad \Psi; \Delta; \Gamma \vdash t_2 : \tau_i}{\Psi; \Delta; \Gamma \vdash \mathsf{write}\ t_1\ [i] \leftarrow t_2 : \mathsf{unit}}$$

4.8 Reduction Relation $\boxed{\langle H \mid e\rangle \longmapsto \langle H' \mid e'\rangle}$

For purposes of our step-indexed logical relation, we consider the reduction rule that loads heap values from a component's heap fragment into the main program heap to take 0 reduction steps.

$$\begin{array}{lll}
\langle H \mid (t, (H', \ell \mapsto h))\rangle & \longmapsto^0 \langle (H, \ell' \mapsto h) \mid (t[\ell'/\ell], H'[\ell'/\ell])\rangle\ \ell' \notin \mathrm{dom}(H) & \\
\langle H \mid E[n_1\ p\ n_2]\rangle & \longmapsto \langle H \mid E[\mathrm{prim}(p, n_1, n_2)]\rangle & \\
\langle H \mid E[\mathsf{if0}\ 0\ t_1\ t_2]\rangle & \longmapsto \langle H \mid E[t_1]\rangle & \\
\langle H \mid E[\mathsf{if0}\ n\ t_1\ t_2]\rangle & \longmapsto \langle H \mid E[t_2]\rangle & n \neq 0 \\
\langle H \mid E[\ell\ [\overline{\tau'}]\ \overline{v}]\rangle & \longmapsto \langle H \mid E[t[\overline{\tau'}/\overline{\alpha}][\overline{v}/\overline{x}]]\rangle & H(\ell) = \lambda[\overline{\alpha}](\overline{x : \tau}).t \\
\langle H \mid E[\mathsf{unpack}\ \langle \alpha, x\rangle = \mathsf{pack}\langle \tau', v\rangle\ \mathsf{as}\ \exists\alpha.\tau\ \mathsf{in}\ t]\rangle & \longmapsto \langle H \mid E[t[\tau'/\alpha][v'/x]]\rangle & \\
\langle H \mid E[\mathsf{unfold}\ (\mathsf{fold}_{\mu\alpha.\tau}\ v)]\rangle & \longmapsto \langle H \mid E[v]\rangle & \\
\langle H \mid E[\mathsf{ralloc}\ \langle v_1, \ldots, v_n\rangle]\rangle & \longmapsto \langle H[\ell \mapsto \langle v_1, \ldots, v_n\rangle] \mid E[\ell]\rangle & \ell \notin H \\
\langle H \mid E[\mathsf{balloc}\ \langle v_1, \ldots, v_n\rangle]\rangle & \longmapsto \langle H[\ell \mapsto \langle v_1, \ldots, v_n\rangle] \mid E[\ell]\rangle & \ell \notin H \\
\langle H \mid E[\mathsf{read}[i]\ \ell]\rangle & \longmapsto \langle H \mid E[v_i]\rangle & H(\ell) = \langle v_1, \ldots, v_n\rangle \\
\langle H \mid E[\mathsf{write}\ \ell\ [i] \leftarrow v]\rangle & \longmapsto \langle H[\ell \mapsto \langle v_1, \ldots, v, \ldots, v_n\rangle] \mid E[()]\rangle & \\
 & & H(\ell) = \langle v_1, \ldots, v_i, \ldots, v_n\rangle
\end{array}$$

4.9 Compiling C to A

4.9.1 Type Translation

$$\alpha^{\mathcal{A}} = \alpha \qquad \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\mathcal{A}} = \mathsf{box}\,\forall[\overline{\alpha}].(\overline{\tau^{\mathcal{A}}}) \to \tau'^{\mathcal{A}}$$
$$\mathsf{unit}^{\mathcal{A}} = \mathsf{unit} \qquad \exists\alpha.\tau^{\mathcal{A}} = \exists\alpha.\tau^{\mathcal{A}}$$
$$\mathsf{int}^{\mathcal{A}} = \mathsf{int} \qquad \mu\alpha.\tau^{\mathcal{A}} = \mu\alpha.\tau^{\mathcal{A}}$$
$$\langle\tau_1,\ldots,\tau_n\rangle^{\mathcal{A}} = \mathsf{box}\,\langle(\tau_1{}^{\mathcal{A}}),\ldots(\tau_n{}^{\mathcal{A}})\rangle$$

4.9.2 Compiler $\boxed{\Delta;\Gamma \vdash e:\tau \rightsquigarrow (t, H:\Psi)}$

implies that $\Delta;\Gamma \vdash e:\tau$, $\cdot \vdash H:\Psi$, and $\cdot;\Delta^{\mathcal{A}};\Gamma^{\mathcal{A}} \vdash (t,H):\tau^{\mathcal{A}}$

$$\frac{x:\tau \in \Gamma}{\Delta;\Gamma \vdash x:\tau \rightsquigarrow (x,\cdot:\cdot)} \qquad \frac{}{\Delta;\Gamma \vdash ():\mathsf{unit} \rightsquigarrow ((),\cdot:\cdot)} \qquad \frac{}{\Delta;\Gamma \vdash n:\mathsf{int} \rightsquigarrow (n,\cdot:\cdot)}$$

$$\frac{\Delta;\Gamma \vdash t_1:\mathsf{int} \rightsquigarrow (t_1,H_1:\Psi_1) \qquad \Delta;\Gamma \vdash t_2:\mathsf{int} \rightsquigarrow (t_2,H_2:\Psi_2)}{\Delta;\Gamma \vdash t_1\ \mathsf{p}\ t_2:\mathsf{int} \rightsquigarrow (t_1\ \mathsf{p}\ t_2,(H_1,H_2):(\Psi_1,\Psi_2))}$$

$$\frac{\Delta;\Gamma \vdash t_1:\mathsf{int} \rightsquigarrow (t_1,H_1:\Psi_1) \qquad \Delta;\Gamma \vdash t_2:\tau \rightsquigarrow (t_2,H_2:\Psi_2) \qquad \Delta;\Gamma \vdash t_3:\tau \rightsquigarrow (t_3,H_3:\Psi_3)}{\Delta;\Gamma \vdash \mathsf{if0}\ t_1\ t_2\ t_3:\tau \rightsquigarrow (\mathsf{if0}\ t_1\ t_2\ t_3,(H_1,H_2,H_3):(\Psi_1,\Psi_2,\Psi_3))}$$

$$\frac{\overline{\alpha};\overline{x:\tau} \vdash t:\tau' \rightsquigarrow (t,H:\Psi)}{\Delta;\Gamma \vdash \lambda[\overline{\alpha}](\overline{x:\tau}).t:\forall[\overline{\alpha}].(\overline{\tau}) \to \tau' \rightsquigarrow (\ell,(H,\ell \mapsto \lambda[\overline{\alpha}](\overline{x:\tau^{\mathcal{A}}}).t):(\Psi,\ell:{}^{\mathsf{box}}\forall[\overline{\alpha}].(\overline{\tau^{\mathcal{A}}}) \to \tau'^{\mathcal{A}}))}$$

$$\frac{\Delta;\Gamma \vdash t_0:\forall[].(\overline{\tau_1}) \to \tau_2 \rightsquigarrow (t_0,H_0:\Psi_0) \qquad \Delta;\Gamma \vdash \overline{t}:\overline{\tau_1} \rightsquigarrow (\overline{t},\overline{H}:\overline{\Psi})}{\Delta;\Gamma \vdash t_0\ []\ \overline{t}:\tau_2 \rightsquigarrow (t_0\ []\ \overline{t},(H_0,\overline{H}):(\Psi_0,\overline{\Psi}))}$$

$$\frac{\Delta;\Gamma \vdash t:\forall[\beta,\overline{\alpha}].(\overline{\tau}) \to \tau' \rightsquigarrow (t,H:\Psi) \qquad \Delta \vdash \tau_0}{\Delta;\Gamma \vdash t[\tau_0]:\forall[\overline{\alpha}].(\overline{\tau[\tau_0/\beta]}) \to \tau'[\tau_0/\beta] \rightsquigarrow (t[\tau_0{}^{\mathcal{A}}],H:\Psi)}$$

$$\frac{\Delta;\Gamma \vdash t:\tau[\tau'/\alpha] \rightsquigarrow (t,H:\Psi)}{\Delta;\Gamma \vdash \mathsf{pack}\langle\tau',t\rangle\ \mathsf{as}\ \exists\alpha.\tau:\exists\alpha.\tau \rightsquigarrow (\mathsf{pack}\langle\tau'^{\mathcal{A}},t\rangle\ \mathsf{as}\ \exists\alpha.\tau^{\mathcal{A}},H:\Psi)}$$

$$\frac{\Delta;\Gamma \vdash t_1:\exists\alpha.\tau \rightsquigarrow (t_1,H_1:\Psi_1) \qquad \Delta,\alpha;\Gamma,x:\tau \vdash t_2:\tau' \rightsquigarrow (t_2,H_2:\Psi_2)}{\Delta;\Gamma \vdash \mathsf{unpack}\ \langle\alpha,x\rangle = t_1\ \mathsf{in}\ t_2:\tau' \rightsquigarrow (\mathsf{unpack}\ \langle\alpha,x\rangle = t_1\ \mathsf{in}\ t_2,(H_1,H_2):(\Psi_1,\Psi_2))}$$

$$\frac{\Delta;\Gamma \vdash t:\tau[\mu\alpha.\tau/\alpha] \rightsquigarrow (t,H:\Psi)}{\Delta;\Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\ t:\mu\alpha.\tau \rightsquigarrow (\mathsf{fold}_{\mu\alpha.\tau^{\mathcal{A}}}\ t,H:\Psi)} \qquad \frac{\Delta;\Gamma \vdash t:\mu\alpha.\tau \rightsquigarrow (t,H:\Psi)}{\Delta;\Gamma \vdash \mathsf{unfold}\ t:\tau[\mu\alpha.\tau/\alpha] \rightsquigarrow (\mathsf{unfold}\ t,H:\Psi)}$$

$$\frac{\Delta;\Gamma \vdash t:\langle\tau_1,\ldots\tau_n\rangle \rightsquigarrow (t,H:\Psi)}{\Delta;\Gamma \vdash \pi_i(t):\tau_i \rightsquigarrow (\mathsf{read}[i]\ t,H:\Psi)}$$

$$\frac{\Delta;\Gamma \vdash t_1:\tau_1 \rightsquigarrow (t_1,H_1:\Psi_1) \qquad \cdots \qquad \Delta;\Gamma \vdash t_n:\tau_n \rightsquigarrow (t_n,H_n:\Psi_n)}{\Delta;\Gamma \vdash \langle t_1,\ldots,t_n\rangle:\langle\tau_1,\ldots,\tau_n\rangle \rightsquigarrow (\mathsf{balloc}\ \langle t_1,\ldots,t_n\rangle,(H_1,\ldots,H_n):(\Psi_1,\ldots,\Psi_n))}$$

5 $(\mathbf{F}+\mathbf{C})+\mathbf{A}$

$$
\begin{array}{rcl}
\boldsymbol{\tau} & ::= & \cdots \mid \mathbf{L}\langle\tau\rangle \\
\mathbf{t} & ::= & \cdots \mid {}^{\boldsymbol{\tau}}\mathcal{C}\mathcal{A}\,\mathbf{e} \\
\mathbf{v} & ::= & \cdots \mid {}^{\mathbf{L}\langle\tau\rangle}\mathcal{C}\mathcal{A}\,\mathbf{v} \\
\mathbf{E} & ::= & \cdots \mid {}^{\boldsymbol{\tau}}\mathcal{C}\mathcal{A}\,\mathbf{E} \\
\boldsymbol{\tau} & ::= & \cdots \mid \lceil\alpha\rceil \mid \lceil\boldsymbol{\alpha}\rceil \\
\mathbf{t} & ::= & \cdots \mid \mathcal{A}\mathcal{C}^{\boldsymbol{\tau}}\,\mathbf{e} \\
\mathbf{E_t} & ::= & \cdots \mid \mathcal{A}\mathcal{C}^{\boldsymbol{\tau}}\,\mathbf{E}
\end{array}
\qquad
\begin{array}{rcl}
\tau & ::= & \cdots \mid \boldsymbol{\tau} \\
e & ::= & \cdots \mid \mathbf{e} \\
v & ::= & \cdots \mid \mathbf{v} \\
E & ::= & \cdots \mid \mathbf{E} \\
M & ::= & \mathbf{H} \\
\Psi & ::= & \boldsymbol{\Psi} \\
\Delta & ::= & \cdots \mid \Delta, \boldsymbol{\alpha} \\
\Gamma & ::= & \cdots \mid \Gamma, \mathbf{x}:\boldsymbol{\tau}
\end{array}
$$

5.1 Boundary Type Translation

$$
\begin{array}{rcl}
\boldsymbol{\alpha}^{\langle\mathcal{A}\rangle} & = & \lceil\boldsymbol{\alpha}\rceil \\
\mathbf{unit}^{\langle\mathcal{A}\rangle} & = & \mathbf{unit} \\
\mathbf{int}^{\langle\mathcal{A}\rangle} & = & \mathbf{int} \\
 & & \\
\mathbf{L}\langle\tau\rangle^{\langle\mathcal{A}\rangle} & = & \tau
\end{array}
\qquad
\begin{array}{rcl}
\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle\mathcal{A}\rangle} & = & \mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}) \to \tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil] \\
\exists\boldsymbol{\alpha}.\boldsymbol{\tau}^{\langle\mathcal{A}\rangle} & = & \exists\alpha.(\boldsymbol{\tau}^{\langle\mathcal{A}\rangle}[\alpha/\lceil\boldsymbol{\alpha}\rceil]) \\
\boldsymbol{\mu\alpha}.\boldsymbol{\tau}^{\langle\mathcal{A}\rangle} & = & \mu\alpha.(\boldsymbol{\tau}^{\langle\mathcal{A}\rangle}[\alpha/\lceil\boldsymbol{\alpha}\rceil]) \\
\langle\boldsymbol{\tau_1},\ldots,\boldsymbol{\tau_n}\rangle^{\langle\mathcal{A}\rangle} & = & \mathbf{box}\,\langle(\boldsymbol{\tau_1}^{\langle\mathcal{A}\rangle}),\ldots(\boldsymbol{\tau_n}^{\langle\mathcal{A}\rangle})\rangle \\
\lceil\alpha\rceil^{\langle\mathcal{A}\rangle} & = & \lceil\alpha\rceil
\end{array}
$$

5.2 Type Substutution

$$\lceil\alpha\rceil[\tau/\alpha] = (\tau^{\langle\mathcal{C}\rangle})^{\langle\mathcal{A}\rangle} \qquad \lceil\boldsymbol{\alpha}\rceil[\boldsymbol{\tau}/\boldsymbol{\alpha}] = \boldsymbol{\tau}^{\langle\mathcal{A}\rangle}$$

5.3 Well-formed Type $\boxed{\Delta \vdash \tau}$

$$\frac{\Delta \vdash \boldsymbol{\tau}}{\Delta \vdash \mathbf{L}\langle\tau\rangle} \qquad \frac{\boldsymbol{\alpha} \in \Delta}{\Delta \vdash \lceil\boldsymbol{\alpha}\rceil} \qquad \frac{\alpha \in \Delta}{\Delta \vdash \lceil\alpha\rceil}$$

5.4 Well-Typed Store $\boxed{\vdash M : \Psi}$

$$\frac{\cdot \vdash \mathbf{H} : \boldsymbol{\Psi}}{\vdash \mathbf{H} : \boldsymbol{\Psi}}$$

5.5 Well-Typed Component $\boxed{\Psi;\Delta;\Gamma \vdash e : \tau}$

Add a store type to each of the previous languages' typing rules, and add:

$$\frac{\Psi;\Delta;\Gamma \vdash \mathbf{e} : \boldsymbol{\tau}^{\langle\mathcal{A}\rangle}}{\Psi;\Delta;\Gamma \vdash {}^{\boldsymbol{\tau}}\mathcal{C}\mathcal{A}\,\mathbf{e} : \boldsymbol{\tau}} \qquad \frac{\Psi;\Delta;\Gamma \vdash \mathbf{e} : \boldsymbol{\tau}}{\Psi;\Delta;\Gamma \vdash \mathcal{A}\mathcal{C}^{\boldsymbol{\tau}}\,\mathbf{e} : \boldsymbol{\tau}^{\langle\mathcal{A}\rangle}}$$

5.6 Value Translation

$$
\begin{aligned}
&\mathbf{AC}^{\mathbf{unit}}((), M) && = ((), M)\\
&\mathbf{AC}^{\mathbf{int}}(\mathbf{n}, M) && = (\mathbf{n}, M)\\
&\mathbf{AC}^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}(\mathbf{v}, M) && = (\ell, (M, \ell \mapsto \mathbf{h}))\\
&\qquad\qquad && \text{where } \mathbf{h} = \boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}).\mathcal{AC}^{\boldsymbol{\tau}'[\mathbf{L}\langle\alpha\rangle/\alpha]}\,\mathbf{v}\,[\overline{\mathbf{L}\langle\alpha\rangle}]\,\overline{{}^{\boldsymbol{\tau}[\mathbf{L}\langle\alpha\rangle/\alpha]}\mathcal{CA}\,\mathbf{x}}\\
&\mathbf{AC}^{\exists\alpha.\boldsymbol{\tau}}(\mathbf{pack}\langle\boldsymbol{\tau}',\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\boldsymbol{\tau}, M) && = (\mathbf{pack}\langle\boldsymbol{\tau}'^{\langle\mathcal{A}\rangle},\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\boldsymbol{\tau}^{\langle\mathcal{A}\rangle}, M')\\
&\qquad\qquad && \text{where } \mathbf{AC}^{\boldsymbol{\tau}[\tau'/\alpha]}(\mathbf{v}, M) = (\mathbf{v}, M')\\
&\mathbf{AC}^{\mu\alpha.\boldsymbol{\tau}}(\mathbf{fold}_{\mu\alpha.\boldsymbol{\tau}}\,\mathbf{v}, M) && = (\mathbf{fold}_{\mu\alpha.\boldsymbol{\tau}\langle\mathcal{A}\rangle}\,\mathbf{v}, M') \ \text{ where } \mathbf{AC}^{\boldsymbol{\tau}[\mu\alpha.\boldsymbol{\tau}/\alpha]}(\mathbf{v}, M) = (\mathbf{v}, M')\\
&\mathbf{AC}^{\langle\tau_1,\ldots,\tau_n\rangle}(\langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle, M) && = (\ell, (M_{n+1}, \ell \mapsto \langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle))\\
&\qquad\qquad && \text{where } M_1 = M \text{ and } \mathbf{AC}^{\tau_i}(\mathbf{v_i}, M_i) = (\mathbf{v_i}, M_{i+1})\\
&\mathbf{AC}^{\mathbf{L}\langle\tau\rangle}({}^{\mathbf{L}\langle\tau\rangle}\mathcal{CA}\,\mathbf{v}, M) && = (\mathbf{v}, M)
\end{aligned}
$$

$$
\begin{aligned}
&{}^{\mathbf{unit}}\mathbf{CA}((), M) && = ((), M)\\
&{}^{\mathbf{int}}\mathbf{CA}(\mathbf{n}, M) && = (\mathbf{n}, M)\\
&{}^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}\mathbf{CA}(\mathbf{v}, M) && = (\boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).{}^{\boldsymbol{\tau}'}\mathcal{CA}\,\mathbf{v}\,[\overline{\lceil\alpha\rceil}]\,\overline{\mathcal{AC}^{\boldsymbol{\tau}}\,\mathbf{x}}, M)\\
&{}^{\exists\alpha.\boldsymbol{\tau}}\mathbf{CA}(\mathbf{pack}\langle\boldsymbol{\tau}',\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\boldsymbol{\tau}^{\langle\mathcal{A}\rangle}, M) && = (\mathbf{pack}\langle\mathbf{L}\langle\boldsymbol{\tau}'\rangle,\mathbf{v}\rangle\ \mathbf{as}\ \exists\alpha.\boldsymbol{\tau}, M')\\
&\qquad\qquad && \text{where } {}^{\boldsymbol{\tau}[\mathbf{L}\langle\tau'\rangle/\alpha]}\mathbf{CA}(\mathbf{v}, M) = (\mathbf{v}, M')\\
&{}^{\mu\alpha.\boldsymbol{\tau}}\mathbf{CA}(\mathbf{fold}_{\mu\alpha.\boldsymbol{\tau}\langle\mathcal{C}\rangle}\,\mathbf{v}, M) && = (\mathbf{fold}_{\mu\alpha.\boldsymbol{\tau}}\,\mathbf{v}, M') \qquad \text{where } {}^{\boldsymbol{\tau}[\mu\alpha.\boldsymbol{\tau}/\alpha]}\mathbf{CA}(\mathbf{v}, M) = (\mathbf{v}, M')\\
&{}^{\langle\tau_1,\ldots,\tau_n\rangle}\mathbf{CA}(\ell, M) && = (\langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle, M_{n+1}) \qquad \text{where } M(\ell) = \langle\mathbf{v_1},\ldots,\mathbf{v_n}\rangle,\\
&\qquad\qquad && M_1 = M, \text{ and } {}^{\tau_i}\mathbf{CA}(\mathbf{v_i}, M_i) = (\mathbf{v_i}, M_{i+1})\\
&{}^{\mathbf{L}\langle\tau\rangle}\mathbf{CA}(\mathbf{v}, M) && = ({}^{\mathbf{L}\langle\tau\rangle}\mathcal{CA}\,\mathbf{v}, M)
\end{aligned}
$$

5.7 Reduction Relation $\boxed{\langle M \mid e\rangle \longmapsto \langle M' \mid e'\rangle}$

$$\frac{\langle \mathbf{H} \mid \mathbf{e}\rangle \longmapsto \langle \mathbf{H}' \mid \mathbf{e}'\rangle}{\langle \mathbf{H} \mid E[\mathbf{e}]\rangle \longmapsto \langle \mathbf{H}' \mid E[\mathbf{e}']\rangle}$$

$$\frac{\mathbf{AC}^{\boldsymbol{\tau}}(\mathbf{v}, M) = (\mathbf{v}, M')}{\langle M \mid E[\mathcal{AC}^{\boldsymbol{\tau}}\,\mathbf{v}]\rangle \longmapsto \langle M' \mid E[\mathbf{v}]\rangle} \qquad \frac{{}^{\boldsymbol{\tau}}\mathbf{CA}(\mathbf{v}, M) = (\mathbf{v}, M') \qquad \boldsymbol{\tau} \neq \mathbf{L}\langle\tau\rangle}{\langle M \mid E[{}^{\boldsymbol{\tau}}\mathcal{CA}\,\mathbf{v}]\rangle \longmapsto \langle M' \mid E[\mathbf{v}]\rangle}$$

6 General Contexts and Contextual Equivalence

$$
\begin{array}{rcl}
\mathsf{C} & ::= & [\cdot] \mid \mathsf{C}\ \mathsf{p}\ \mathsf{t} \mid \mathsf{t}\ \mathsf{p}\ \mathsf{C} \mid \mathsf{if0}\ \mathsf{C}\ \mathsf{t}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{C}\ \mathsf{t} \mid \mathsf{if0}\ \mathsf{t}\ \mathsf{t}\ \mathsf{C} \mid \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{C} \mid \mathsf{C}\,[\overline{\tau}]\,\overline{\mathsf{t}} \mid \mathsf{t}\,[\overline{\tau}]\,\overline{\mathsf{t}}\ \mathsf{C}\ \overline{\mathsf{t}} \mid \mathsf{pack}\langle\tau,\mathsf{C}\rangle\ \mathsf{as}\ \exists\alpha.\tau \\
& & \mid \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{C}\ \mathsf{in}\ \mathsf{t} \mid \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{C} \mid \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{C} \mid \mathsf{unfold}\ \mathsf{C} \mid \langle\overline{\mathsf{t}},\mathsf{C},\overline{\mathsf{t}}\rangle \mid \pi_{\mathsf{i}}(\mathsf{C}) \mid {}^{\tau}\mathcal{FC}\ \mathsf{C} \\
\mathbf{C} & ::= & [\cdot] \mid \mathbf{C}\ \mathbf{p}\ \mathbf{t} \mid \mathbf{t}\ \mathbf{p}\ \mathbf{C} \mid \mathbf{if0}\ \mathbf{C}\ \mathbf{t}\ \mathbf{t} \mid \mathbf{if0}\ \mathbf{t}\ \mathbf{C}\ \mathbf{t} \mid \mathbf{if0}\ \mathbf{t}\ \mathbf{t}\ \mathbf{C} \mid \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{C} \mid \mathbf{C}\,[]\,\overline{\mathbf{t}} \mid \mathbf{t}\,[]\,\overline{\mathbf{t}}\ \mathbf{C}\ \overline{\mathbf{t}} \mid \mathbf{C}[\boldsymbol{\tau}] \\
& & \mid \mathbf{pack}\langle\boldsymbol{\tau},\mathbf{C}\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau} \mid \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{C}\ \mathbf{in}\ \mathbf{t} \mid \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{C} \mid \mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{C} \\
& & \mid \mathbf{unfold}\ \mathbf{C} \mid \langle\overline{\mathbf{t}},\mathbf{C},\overline{\mathbf{t}}\rangle \mid \boldsymbol{\pi}_{\mathbf{i}}(\mathbf{C}) \mid \mathcal{CF}^{\tau}\ \mathbf{C} \mid {}^{\tau}\mathcal{CA}\ \mathbf{C} \\
\mathbf{C} & ::= & (\mathbf{C_t},\mathbf{H}) \mid (\mathbf{t},\mathbf{C_H}) \\
\mathbf{C_t} & ::= & [\cdot] \mid \mathbf{C_t}\ \mathbf{p}\ \mathbf{t} \mid \mathbf{t}\ \mathbf{p}\ \mathbf{C_t} \mid \mathbf{if0}\ \mathbf{C_t}\ \mathbf{t}\ \mathbf{t} \mid \mathbf{if0}\ \mathbf{t}\ \mathbf{C_t}\ \mathbf{t} \mid \mathbf{if0}\ \mathbf{t}\ \mathbf{t}\ \mathbf{C_t} \mid \mathbf{C_t}\,[]\,\overline{\mathbf{t}} \mid \mathbf{t}\,[]\,\overline{\mathbf{t}},\mathbf{C_t},\overline{\mathbf{t}} \mid \mathbf{C_t}[\boldsymbol{\tau}] \\
& & \mid \mathbf{pack}\langle\boldsymbol{\tau},\mathbf{C_t}\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau} \mid \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{C_t}\ \mathbf{in}\ \mathbf{t} \mid \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{C_t} \mid \mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{C_t} \mid \mathbf{unfold}\ \mathbf{C_t} \\
& & \mid \mathbf{ralloc}\ \langle\overline{\mathbf{t}},\mathbf{C_t},\overline{\mathbf{t}}\rangle \mid \mathbf{balloc}\ \langle\overline{\mathbf{t}},\mathbf{C_t},\overline{\mathbf{t}}\rangle \mid \mathbf{read[i]}\ \mathbf{C_t} \mid \mathbf{write}\ \mathbf{C_t}\ [\mathbf{t}] \leftarrow \mathbf{t} \mid \mathbf{write}\ \mathbf{t}\ [\mathbf{i}] \leftarrow \mathbf{C_t} \mid \mathcal{AC}^{\boldsymbol{\tau}}\ \mathbf{C} \\
\mathbf{C_H} & ::= & \mathbf{C_H}, \ell \mapsto \mathbf{h} \mid \mathbf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{C_t} \\
C & ::= & \mathsf{C} \mid \mathbf{C} \mid \mathbf{C}
\end{array}
$$

6.1 Plug Function $\boxed{C[e]}$

$$
\begin{array}{rcl}
[\cdot][\mathsf{e}] & = & \mathsf{e} \\
(\mathsf{C}\ \mathsf{p}\ \mathsf{t})[e] & = & (\mathsf{C}[e])\ \mathsf{p}\ \mathsf{t} \\
(\mathsf{t}\ \mathsf{p}\ \mathsf{C})[e] & = & \mathsf{t}\ \mathsf{p}\ (\mathsf{C}[e]) \\
(\mathsf{if0}\ \mathsf{C}\ \mathsf{t}_1\ \mathsf{t}_2)[e] & = & \mathsf{if0}\ (\mathsf{C}[e])\ \mathsf{t}_1\ \mathsf{t}_2 \\
(\mathsf{if0}\ \mathsf{t}_0\ \mathsf{C}\ \mathsf{t}_2)[e] & = & \mathsf{if0}\ \mathsf{t}_0\ (\mathsf{C}[e])\ \mathsf{t}_2 \\
(\mathsf{if0}\ \mathsf{t}_0\ \mathsf{t}_1\ \mathsf{C})[e] & = & \mathsf{if0}\ \mathsf{t}_0\ \mathsf{t}_1\ (\mathsf{C}[e]) \\
(\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{C})[e] & = & \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).(\mathsf{C}[e]) \\
(\mathsf{C}\,[\overline{\tau}]\,\overline{\mathsf{t}})[e] & = & (\mathsf{C}[e])\,[\overline{\tau}]\,\overline{\mathsf{t}} \\
(\mathsf{t}'\,[\overline{\tau}]\,\overline{\mathsf{t}}\ \mathsf{C}\ \overline{\mathsf{t}})[e] & = & \mathsf{t}'\,[\overline{\tau}]\,\overline{\mathsf{t}}\ (\mathsf{C}[e])\ \overline{\mathsf{t}}
\end{array}
\qquad
\begin{array}{rcl}
(\mathsf{pack}\langle\tau,\mathsf{C}\rangle\ \mathsf{as}\ \exists\alpha.\tau)[e] & = & \mathsf{pack}\langle\tau,(\mathsf{C}[e])\rangle\ \mathsf{as}\ \exists\alpha.\tau \\
(\mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{C}\ \mathsf{in}\ \mathsf{t})[e] & = & \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = (\mathsf{C}[e])\ \mathsf{in}\ \mathsf{t} \\
(\mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{C})[e] & = & \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}\ \mathsf{in}\ (\mathsf{C}[e]) \\
(\mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{C})[e] & = & \mathsf{fold}_{\mu\alpha.\tau}\ (\mathsf{C}[e]) \\
(\mathsf{unfold}\ \mathsf{C})[e] & = & \mathsf{unfold}\ (\mathsf{C}[e]) \\
(\langle\overline{\mathsf{t}},\mathsf{C},\overline{\mathsf{t}'}\rangle)[e] & = & \langle\overline{\mathsf{t}},(\mathsf{C}[e]),\overline{\mathsf{t}'}\rangle \\
(\pi_{\mathsf{i}}(\mathsf{C}))[e] & = & \pi_{\mathsf{i}}(\mathsf{C}[e]) \\
({}^{\tau}\mathcal{FC}\ \mathbf{C})[e] & = & {}^{\tau}\mathcal{FC}\ (\mathbf{C}[e])
\end{array}
$$

$$
\begin{array}{rcl}
[\cdot][\mathbf{e}] & = & \mathbf{e} \\
(\mathbf{C}\ \mathbf{p}\ \mathbf{t})[e] & = & (\mathbf{C}[e])\ \mathbf{p}\ \mathbf{t} \\
(\mathbf{t}\ \mathbf{p}\ \mathbf{C})[e] & = & \mathbf{t}\ \mathbf{p}\ (\mathbf{C}[e]) \\
(\mathbf{if0}\ \mathbf{C}\ \mathbf{t_1}\ \mathbf{t_2})[e] & = & \mathbf{if0}\ (\mathbf{C}[e])\ \mathbf{t_1}\ \mathbf{t_2} \\
(\mathbf{if0}\ \mathbf{t_0}\ \mathbf{C}\ \mathbf{t_2})[e] & = & \mathbf{if0}\ \mathbf{t_0}\ (\mathbf{C}[e])\ \mathbf{t_2} \\
(\mathbf{if0}\ \mathbf{t_0}\ \mathbf{t_1}\ \mathbf{C})[e] & = & \mathbf{if0}\ \mathbf{t_0}\ \mathbf{t_1}\ (\mathbf{C}[e]) \\
(\boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{C})[e] & = & \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\overline{\mathbf{x}:\boldsymbol{\tau}}).(\mathbf{C}[e]) \\
(\mathbf{C}\,[]\,\overline{\mathbf{t}})[e] & = & (\mathbf{C}[e])\,[]\,\overline{\mathbf{t}} \\
(\mathbf{t}'\,[]\,\overline{\mathbf{t}}\ \mathbf{C}\ \overline{\mathbf{t}})[e] & = & \mathbf{t}'\,[]\,\overline{\mathbf{t}}\ (\mathbf{C}[e])\ \overline{\mathbf{t}} \\
(\mathbf{C}[\boldsymbol{\tau}])[e] & = & (\mathbf{C}[e])[\boldsymbol{\tau}]
\end{array}
\qquad
\begin{array}{rcl}
(\mathbf{pack}\langle\boldsymbol{\tau},\mathbf{C}\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau})[e] & = & \mathbf{pack}\langle\boldsymbol{\tau},(\mathbf{C}[e])\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau} \\
(\mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{C}\ \mathbf{in}\ \mathbf{t})[e] & = & \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = (\mathbf{C}[e])\ \mathbf{in}\ \mathbf{t} \\
(\mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{C})[e] & = & \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{t}\ \mathbf{in}\ (\mathbf{C}[e]) \\
(\mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{C})[e] & = & \mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ (\mathbf{C}[e]) \\
(\mathbf{unfold}\ \mathbf{C})[e] & = & \mathbf{unfold}\ (\mathbf{C}[e]) \\
(\langle\overline{\mathbf{t}},\mathbf{C},\overline{\mathbf{t}'}\rangle)[e] & = & \langle\overline{\mathbf{t}},(\mathbf{C}[e]),\overline{\mathbf{t}'}\rangle \\
(\boldsymbol{\pi}_{\mathbf{i}}(\mathbf{C}))[e] & = & \boldsymbol{\pi}_{\mathbf{i}}(\mathbf{C}[e]) \\
(\mathcal{CF}^{\tau}\ \mathbf{C})[e] & = & \mathcal{CF}^{\tau}\ (\mathbf{C}[e]) \\
({}^{\tau}\mathcal{CA}\ \mathbf{C})[e] & = & {}^{\tau}\mathcal{CA}\ (\mathbf{C}[e])
\end{array}
$$

$$
(\mathbf{C_t},\mathbf{H})[e] = \begin{cases} (\mathbf{C_t}[\mathbf{t}],(\mathbf{H},\mathbf{H}')) & e = (\mathbf{t},\mathbf{H}') \wedge \mathbf{C_t} \text{ contains no language boundaries} \\ (\mathbf{C_t}[e],\mathbf{H}) & \text{otherwise} \end{cases}
$$

$$
(\mathbf{t},\mathbf{C_H})[e] = \begin{cases} (\mathbf{t},(\mathbf{C_H}[\mathbf{t}],\mathbf{H}')) & e = (\mathbf{t},\mathbf{H}') \wedge \mathbf{C_H} \text{ contains no language boundaries} \\ (\mathbf{t},\mathbf{C_H}[e]) & \text{otherwise} \end{cases}
$$

$$
\begin{array}{rlrl}
[\cdot][\mathsf{t}] &= \mathsf{t} & (\mathsf{pack}\langle\tau,\mathsf{C_t}\rangle\ \mathsf{as}\ \exists\alpha.\tau)[e] &= \mathsf{pack}\langle\tau,(\mathsf{C_t}[e])\rangle\ \mathsf{as}\ \exists\alpha.\tau \\
(\mathsf{C_t\ p\ t})[e] &= (\mathsf{C_t}[e])\ \mathsf{p}\ \mathsf{t} & (\mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{C_t}\ \mathsf{in}\ \mathsf{t})[e] &= \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = (\mathsf{C_t}[e])\ \mathsf{in}\ \mathsf{t} \\
(\mathsf{t\ p\ C_t})[e] &= \mathsf{t}\ \mathsf{p}\ (\mathsf{C_t}[e]) & (\mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{C_t})[e] &= \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}\ \mathsf{in}\ (\mathsf{C_t}[e]) \\
(\mathsf{if0\ C_t\ t_1\ t_2})[e] &= \mathsf{if0}\ (\mathsf{C_t}[e])\ \mathsf{t_1}\ \mathsf{t_2} & (\mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{C_t})[e] &= \mathsf{fold}_{\mu\alpha.\tau}\ (\mathsf{C_t}[e]) \\
(\mathsf{if0\ t_0\ C_t\ t_2})[e] &= \mathsf{if0}\ \mathsf{t_0}\ (\mathsf{C_t}[e])\ \mathsf{t_2} & (\mathsf{unfold\ C_t})[e] &= \mathsf{unfold}\ (\mathsf{C_t}[e]) \\
(\mathsf{if0\ t_0\ t_1\ C_t})[e] &= \mathsf{if0}\ \mathsf{t_0}\ \mathsf{t_1}\ (\mathsf{C_t}[e]) & (\mathsf{ralloc}\ \langle\overline{\mathsf{t}},\mathsf{C_t},\overline{\mathsf{t'}}\rangle)[e] &= \mathsf{ralloc}\ \langle\overline{\mathsf{t}},(\mathsf{C_t}[e]),\overline{\mathsf{t'}}\rangle \\
(\mathsf{C_t}\ []\ \overline{\mathsf{t}})[e] &= (\mathsf{C_t}[e])\ []\ \overline{\mathsf{t}} & (\mathsf{balloc}\ \langle\overline{\mathsf{t}},\mathsf{C_t},\overline{\mathsf{t'}}\rangle)[e] &= \mathsf{balloc}\ \langle\overline{\mathsf{t}},(\mathsf{C_t}[e]),\overline{\mathsf{t'}}\rangle \\
(\mathsf{t'}\ []\ \overline{\mathsf{t}},\mathsf{C_t},\overline{\mathsf{t}})[e] &= \mathsf{t'}\ []\ \overline{\mathsf{t}},(\mathsf{C_t}[e]),\overline{\mathsf{t}} & (\mathsf{read[i]\ C_t})[e] &= \mathsf{read[i]}\ (\mathsf{C_t}[e]) \\
(\mathsf{C_t}[\tau])[e] &= (\mathsf{C_t}[e])[\tau] & (\mathsf{write\ C_t\ [i]} \leftarrow \mathsf{t})[e] &= \mathsf{write}\ \mathsf{C_t}[e]\ \mathsf{[i]} \leftarrow \mathsf{t} \\
(\mathcal{AC}^{\tau}\ \mathbf{C})[e] &= \mathcal{AC}^{\tau}\ (\mathbf{C}[e]) & (\mathsf{write\ t\ [i]} \leftarrow \mathsf{C_t})[e] &= \mathsf{write\ t\ [i]} \leftarrow \mathsf{C_t}[e]
\end{array}
$$

$$
\begin{array}{c}
(\mathsf{C_H}, \ell \mapsto \mathsf{h})[e] = \mathsf{C_H}[e], \ell \mapsto \mathsf{h} \\
(\mathsf{H}, \ell \mapsto \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{C_t})[e] = \mathsf{H}, \ell \mapsto \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).(\mathsf{C_t}[e])
\end{array}
$$

6.2 Well-Typed Context $\boxed{\vdash C : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau')}$

$$
\frac{\Psi \subseteq \Psi' \qquad \Delta \subseteq \Delta' \qquad \Gamma \subseteq \Gamma'}{\vdash [\cdot] : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau)}
\qquad
\frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathsf{int}) \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t} : \mathsf{int}}{\vdash \mathsf{C\ p\ t} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathsf{int})}
$$

$$
\frac{\Psi';\Delta';\Gamma' \vdash \mathsf{t} : \mathsf{int} \qquad \vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathsf{int})}{\vdash \mathsf{t\ p\ C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathsf{int})}
$$

$$
\frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathsf{int}) \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_1} : \tau \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_2} : \tau}{\vdash \mathsf{if0\ C\ t_1\ t_2} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau)}
$$

$$
\frac{\Psi';\Delta';\Gamma' \vdash \mathsf{t_0} : \mathsf{int} \qquad \vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau) \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_2} : \tau}{\vdash \mathsf{if0\ t_0\ C\ t_2} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau)}
$$

$$
\frac{\Psi';\Delta';\Gamma' \vdash \mathsf{t_0} : \mathsf{int} \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_1} : \tau \qquad \vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau)}{\vdash \mathsf{if0\ t_0\ t_1\ C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau)}
$$

$$
\frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';(\Delta',\overline{\alpha});(\Gamma',\overline{\mathsf{x}:\tau}) \vdash \tau')}{\vdash \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \forall[\overline{\alpha}].(\overline{\tau}) \to \tau')}
$$

$$
\frac{\begin{array}{c}\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \forall[\overline{\alpha}].(\tau_1,\ldots,\tau_n) \to \tau') \\ \Delta \vdash \overline{\tau} \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_1} : \tau_1[\overline{\tau/\alpha}] \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_n} : \tau_n[\overline{\tau/\alpha}]\end{array}}{\vdash \mathsf{C}\,[\overline{\tau}]\,\mathsf{t_1}\cdots\mathsf{t_n} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau'[\overline{\tau/\alpha}])}
$$

$$
\frac{\begin{array}{c}\Psi';\Delta';\Gamma' \vdash \mathsf{t} : \forall[\overline{\alpha}].(\tau_1,\ldots,\tau_n) \to \tau' \qquad \Delta \vdash \overline{\tau} \\ \Psi';\Delta';\Gamma' \vdash \mathsf{t_1} : \tau_1[\overline{\tau/\alpha}] \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_i} : \tau_i[\overline{\tau/\alpha}] \qquad \vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_{i+1}[\overline{\tau/\alpha}]) \\ \Psi';\Delta';\Gamma' \vdash \mathsf{t_{i+2}} : \tau_{i+2}[\overline{\tau/\alpha}] \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t_n} : \tau_n[\overline{\tau/\alpha}]\end{array}}{\vdash \mathsf{t}\,[\overline{\tau}]\,\mathsf{t_1}\cdots\mathsf{t_i}\ \mathsf{C}\ \mathsf{t_{i+2}}\cdots\mathsf{t_n} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau'[\overline{\tau/\alpha}])}
$$

$$\frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau[\tau'/\alpha])}{\vdash \mathsf{pack}\langle \tau', \mathsf{C}\rangle \ \mathsf{as}\ \exists\alpha.\tau : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \exists\alpha.\tau)}$$

$$\frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \exists\alpha.\tau) \qquad \Psi';\Delta',\alpha;\Gamma',\mathsf{x}:\tau \vdash \mathsf{t} : \tau'}{\vdash \mathsf{unpack}\ \langle \alpha, \mathsf{x}\rangle = \mathsf{C}\ \mathsf{in}\ \mathsf{t} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \exists\alpha.\tau)}$$

$$\frac{\Psi';\Delta';\Gamma' \vdash t : \exists\alpha.\tau \qquad \vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta',\alpha;\Gamma',\mathsf{x}:\tau \vdash \tau')}{\vdash \mathsf{unpack}\ \langle \alpha, \mathsf{x}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau')}$$

$$\frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau[\mu\alpha.\tau/\alpha])}{\vdash \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mu\alpha.\tau)} \qquad \frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mu\alpha.\tau)}{\vdash \mathsf{unfold}\ \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau[\mu\alpha.\tau/\alpha])}$$

$$\frac{\begin{array}{c}\Psi';\Delta';\Gamma' \vdash \mathsf{t}_1 : \tau_1 \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t}_i : \tau_i \\ \vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_{i+1}) \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t}_{i+2} : \tau_{i+2} \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathsf{t}_n : \tau_n\end{array}}{\vdash \langle \mathsf{t}_1, \ldots, \mathsf{t}_i, \mathsf{C}, \mathsf{t}_{i+2}, \ldots, \mathsf{t}_n\rangle : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \langle \tau_1, \ldots, \tau_n\rangle)}$$

$$\frac{\vdash \mathsf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \langle \tau_1, \ldots, \tau_n\rangle)}{\vdash \pi_i(\mathsf{C}) : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_i)} \qquad \frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau^{\langle \mathcal{C}\rangle})}{\vdash {}^{\tau}\mathcal{FC}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau)}$$

$$\frac{\Psi \subseteq \Psi' \qquad \Delta \subseteq \Delta' \qquad \Gamma \subseteq \Gamma'}{\vdash [\cdot] : (\Psi;\Delta;\Gamma \vdash \boldsymbol{\tau}) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau})} \qquad \frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{int}) \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t} : \mathbf{int}}{\vdash \mathbf{C}\ \mathbf{p}\ \mathbf{t} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{int})}$$

$$\frac{\Psi';\Delta';\Gamma' \vdash \mathbf{t} : \mathbf{int} \qquad \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{int})}{\vdash \mathbf{t}\ \mathbf{p}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{int})}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{int}) \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_1} : \boldsymbol{\tau} \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_2} : \boldsymbol{\tau}}{\vdash \mathbf{if0}\ \mathbf{C}\ \mathbf{t_1}\ \mathbf{t_2} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau})}$$

$$\frac{\Psi';\Delta';\Gamma' \vdash \mathbf{t_0} : \mathbf{int} \qquad \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau}) \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_2} : \boldsymbol{\tau}}{\vdash \mathbf{if0}\ \mathbf{t_0}\ \mathbf{C}\ \mathbf{t_2} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau})}$$

$$\frac{\Psi';\Delta';\Gamma' \vdash \mathbf{t_0} : \mathbf{int} \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_1} : \boldsymbol{\tau} \qquad \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau})}{\vdash \mathbf{if0}\ \mathbf{t_0}\ \mathbf{t_1}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau})}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';(\overline{\boldsymbol{\alpha}});(\overline{\mathbf{x}:\boldsymbol{\tau}}) \vdash \boldsymbol{\tau'})}{\vdash \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau'})}$$

$$\frac{\begin{array}{c}\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \forall[].(\boldsymbol{\tau_1},\ldots,\boldsymbol{\tau_n}) \to \boldsymbol{\tau'}) \\ \Psi';\Delta';\Gamma' \vdash \mathbf{t_1} : \boldsymbol{\tau_1} \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_n} : \boldsymbol{\tau_n}\end{array}}{\vdash \mathbf{C}\ []\ \mathbf{t_1} \cdots \mathbf{t_n} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau'})}$$

$$\frac{\begin{array}{c}\Psi';\Delta';\Gamma' \vdash \mathbf{t} : \forall[].(\boldsymbol{\tau_1},\ldots,\boldsymbol{\tau_n}) \to \boldsymbol{\tau'} \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_1} : \boldsymbol{\tau_1} \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_i} : \boldsymbol{\tau_i} \\ \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau_{i+1}}) \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_{i+2}} : \boldsymbol{\tau_{i+2}} \qquad \cdots \qquad \Psi';\Delta';\Gamma' \vdash \mathbf{t_n} : \boldsymbol{\tau_n}\end{array}}{\vdash \mathbf{t}\ []\ \mathbf{t_1} \cdots \mathbf{t_i}\ \mathbf{C}\ \mathbf{t_{i+2}} \cdots \mathbf{t_n} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau'})}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \forall[\boldsymbol{\beta},\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau'}) \qquad \Delta \vdash \boldsymbol{\tau_0}}{\vdash \mathbf{C}[\boldsymbol{\tau_0}] : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}[\boldsymbol{\tau_0}/\boldsymbol{\beta}]}) \to \boldsymbol{\tau'}[\boldsymbol{\tau_0}/\boldsymbol{\beta}])}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau}[\boldsymbol{\tau'}/\boldsymbol{\alpha}])}{\vdash \mathbf{pack}\langle \boldsymbol{\tau'}, \mathbf{C} \rangle \ \mathbf{as}\ \exists \boldsymbol{\alpha}.\boldsymbol{\tau} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \exists \boldsymbol{\alpha}.\boldsymbol{\tau})}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \exists \boldsymbol{\alpha}.\boldsymbol{\tau}) \qquad \Psi'; \Delta', \boldsymbol{\alpha}; \Gamma', \mathbf{x} : \boldsymbol{\tau} \vdash \mathbf{t} : \boldsymbol{\tau'}}{\vdash \mathbf{unpack}\ \langle \boldsymbol{\alpha}, \mathbf{x} \rangle = \mathbf{C}\ \mathbf{in}\ \mathbf{t} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \exists \boldsymbol{\alpha}.\boldsymbol{\tau})}$$

$$\frac{\Psi'; \Delta'; \Gamma' \vdash t : \exists \boldsymbol{\alpha}.\boldsymbol{\tau} \qquad \vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta', \boldsymbol{\alpha}; \Gamma', \mathbf{x} : \boldsymbol{\tau} \vdash \boldsymbol{\tau'})}{\vdash \mathbf{unpack}\ \langle \boldsymbol{\alpha}, \mathbf{x} \rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau'})}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau}[\boldsymbol{\mu\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}])}{\vdash \mathbf{fold}_{\boldsymbol{\mu\alpha}.\boldsymbol{\tau}}\ \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\mu\alpha}.\boldsymbol{\tau})}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\mu\alpha}.\boldsymbol{\tau})}{\vdash \mathbf{unfold}\ \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau}[\boldsymbol{\mu\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}])}$$

$$\frac{\begin{array}{c}\Psi'; \Delta'; \Gamma' \vdash \mathbf{t_1} : \boldsymbol{\tau_1} \qquad \cdots \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t_i} : \boldsymbol{\tau_i} \\ \vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau_{i+1}}) \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t_{i+2}} : \boldsymbol{\tau_{i+2}} \qquad \cdots \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t_n} : \boldsymbol{\tau_n}\end{array}}{\vdash \langle \mathbf{t_1}, \ldots, \mathbf{t_i}, \mathbf{C}, \mathbf{t_{i+2}}, \ldots, \mathbf{t_n} \rangle : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \langle \boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n} \rangle)}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \langle \boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n} \rangle)}{\vdash \boldsymbol{\pi_i}(\mathbf{C}) : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau_i})} \qquad \frac{\vdash \mathsf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \tau)}{\vdash \mathcal{CF}^{\tau}\ \mathsf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \tau^{\langle \mathcal{C} \rangle})}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau}^{\langle \mathcal{A} \rangle})}{\vdash {}^{\tau}\mathcal{CA}\ \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau})}$$

$$\frac{\Psi' \vdash \mathbf{H} : \boldsymbol{\Psi} \qquad \vdash \mathbf{C_t} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow ((\Psi', \boldsymbol{\Psi}); \Delta'; \Gamma' \vdash \boldsymbol{\tau'})}{\vdash (\mathbf{C_t}, \mathbf{H}) : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau'})}$$

$$\frac{\vdash \mathbf{C_H} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi' \vdash \boldsymbol{\Psi}) \qquad (\Psi', \boldsymbol{\Psi}); \Delta'; \Gamma' \vdash \mathbf{t} : \boldsymbol{\tau'}}{\vdash (\mathbf{t}, \mathbf{C_H}) : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau'})} \qquad \frac{\Psi \subseteq \Psi' \qquad \Delta \subseteq \Delta' \qquad \Gamma \subseteq \Gamma'}{\vdash [\cdot] : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \tau)}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \mathbf{int}) \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t} : \mathbf{int}}{\vdash \mathbf{C}\ \mathbf{p}\ \mathbf{t} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \mathbf{int})}$$

$$\frac{\Psi'; \Delta'; \Gamma' \vdash \mathbf{t} : \mathbf{int} \qquad \vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \mathbf{int})}{\vdash \mathbf{t}\ \mathbf{p}\ \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \mathbf{int})}$$

$$\frac{\vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \mathbf{int}) \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t_1} : \boldsymbol{\tau} \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t_2} : \boldsymbol{\tau}}{\vdash \mathbf{if0}\ \mathbf{C}\ \mathbf{t_1}\ \mathbf{t_2} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau})}$$

$$\frac{\Psi'; \Delta'; \Gamma' \vdash \mathbf{t_0} : \mathbf{int} \qquad \vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau}) \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t_2} : \boldsymbol{\tau}}{\vdash \mathbf{if0}\ \mathbf{t_0}\ \mathbf{C}\ \mathbf{t_2} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau})}$$

$$\frac{\Psi'; \Delta'; \Gamma' \vdash \mathbf{t_0} : \mathbf{int} \qquad \Psi'; \Delta'; \Gamma' \vdash \mathbf{t_1} : \boldsymbol{\tau} \qquad \vdash \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau})}{\vdash \mathbf{if0}\ \mathbf{t_0}\ \mathbf{t_1}\ \mathbf{C} : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \boldsymbol{\tau})}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{box}\,\forall[].(\tau_1,\ldots,\tau_n) \to \tau') \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_1 : \tau_1 \quad \cdots \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_n : \tau_n}{\vdash \mathbf{C}\ []\ \mathbf{t}_1 \cdots \mathbf{t}_n : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau')}$$

$$\frac{\begin{array}{c}\Psi';\Delta';\Gamma' \vdash \mathbf{t} : \mathbf{box}\,\forall[].(\tau_1,\ldots,\tau_n) \to \tau' \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_1 : \tau_1 \quad \cdots \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_i : \tau_i \\ \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_{i+1}) \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_{i+2} : \tau_{i+2} \quad \cdots \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_n : \tau_n\end{array}}{\vdash \mathbf{t}\ []\ \mathbf{t}_1 \cdots \mathbf{t}_i\ \mathbf{C}\ \mathbf{t}_{i+2} \cdots \mathbf{t}_n : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau')}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{box}\,\forall[\beta,\overline{\alpha}].(\overline{\tau}) \to \tau') \quad \Delta \vdash \tau_0}{\vdash \mathbf{C}[\tau_0] : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau[\tau_0/\beta]}) \to \tau'[\tau_0/\beta])}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau[\tau'/\alpha])}{\vdash \mathbf{pack}\langle\tau',\mathbf{C}\rangle\ \mathbf{as}\ \exists\alpha.\tau : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \exists\alpha.\tau)}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \exists\alpha.\tau) \quad \Psi';\Delta',\alpha;\Gamma',\mathbf{x}:\tau \vdash \mathbf{t} : \tau'}{\vdash \mathbf{unpack}\ \langle\alpha,\mathbf{x}\rangle = \mathbf{C}\ \mathbf{in}\ \mathbf{t} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \exists\alpha.\tau)}$$

$$\frac{\Psi';\Delta';\Gamma' \vdash t : \exists\alpha.\tau \quad \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta',\alpha;\Gamma',\mathbf{x}:\tau \vdash \tau')}{\vdash \mathbf{unpack}\ \langle\alpha,\mathbf{x}\rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau')}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau[\mu\alpha.\tau/\alpha])}{\vdash \mathbf{fold}_{\mu\alpha.\tau}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mu\alpha.\tau)}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mu\alpha.\tau)}{\vdash \mathbf{unfold}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau[\mu\alpha.\tau/\alpha])}$$

$$\frac{\begin{array}{c}\Psi';\Delta';\Gamma' \vdash \mathbf{t}_1 : \tau_1 \quad \cdots \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_i : \tau_i \\ \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_{i+1}) \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_{i+2} : \tau_{i+2} \quad \cdots \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_n : \tau_n\end{array}}{\vdash \mathbf{ralloc}\langle\mathbf{t}_1,\ldots,\mathbf{t}_i,\mathbf{C},\mathbf{t}_{i+2},\ldots,\mathbf{t}_n\rangle : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{ref}\,\langle\tau_1,\ldots,\tau_n\rangle)}$$

$$\frac{\begin{array}{c}\Psi';\Delta';\Gamma' \vdash \mathbf{t}_1 : \tau_1 \quad \cdots \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_i : \tau_i \\ \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_{i+1}) \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_{i+2} : \tau_{i+2} \quad \cdots \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t}_n : \tau_n\end{array}}{\vdash \mathbf{balloc}\langle\mathbf{t}_1,\ldots,\mathbf{t}_i,\mathbf{C},\mathbf{t}_{i+2},\ldots,\mathbf{t}_n\rangle : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{box}\langle\tau_1,\ldots,\tau_n\rangle)}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{ref}\,\langle\tau_1,\ldots,\tau_n\rangle)}{\vdash \mathbf{read[i]}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_i)} \qquad \frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{box}\,\langle\tau_1,\ldots,\tau_n\rangle)}{\vdash \mathbf{read[i]}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_i)}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{ref}\,\langle\tau_1,\ldots,\tau_n\rangle) \quad \Psi';\Delta';\Gamma' \vdash \mathbf{t} : \tau_i}{\vdash \mathbf{write}\ \mathbf{C}\ [\mathbf{i}] \leftarrow \mathbf{t} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{unit})}$$

$$\frac{\Psi';\Delta';\Gamma' \vdash \mathbf{t} : \mathbf{ref}\,\langle\tau_1,\ldots,\tau_n\rangle \quad \vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \tau_i)}{\vdash \mathbf{write}\ \mathbf{t}\ [\mathbf{i}] \leftarrow \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \mathbf{unit})}$$

$$\frac{\vdash \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau})}{\vdash \mathcal{AC}^{\tau}\ \mathbf{C} : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\Delta';\Gamma' \vdash \boldsymbol{\tau}^{\langle\mathcal{A}\rangle})}$$

$$\frac{\begin{array}{c}\mathbf{H} = \ell_1 \mapsto \mathbf{h}_1,\ldots,\ell_n \mapsto \mathbf{h}_n \qquad \mathbf{H}' = \ell'_1 \mapsto \mathbf{h}'_1,\ldots,\ell'_m \mapsto \mathbf{h}'_n \\ \boldsymbol{\Psi} = \{\ell_1 : \psi_1,\ldots,\ell_n : \psi_n, \ell : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau', \ell'_1 : \psi'_1,\ldots,\ell'_m : \psi'_m\} \qquad \cdot \vdash \psi_1 \ \cdots \ \cdot \vdash \psi_n \\ \Psi',\boldsymbol{\Psi} \vdash \mathbf{h}_1 : \psi_1 \ \cdots \ \Psi',\boldsymbol{\Psi} \vdash \mathbf{h}_n : \psi_n \qquad \vdash \mathbf{C}_t : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow ((\Psi',\boldsymbol{\Psi});(\overline{\alpha});(\overline{\mathbf{x}:\tau}) \vdash \tau') \\ \cdot \vdash \psi'_1 \ \cdots \ \cdot \vdash \psi'_m \qquad \Psi',\boldsymbol{\Psi} \vdash \mathbf{h}'_1 : \psi'_1 \ \cdots \ \Psi',\boldsymbol{\Psi} \vdash \mathbf{h}'_m : \psi'_m\end{array}}{\vdash \mathbf{H}, \ell \mapsto \lambda[\overline{\alpha}]\,(\overline{\mathbf{x}:\tau}).\mathbf{C}_t, \mathbf{H}' : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi' \vdash \boldsymbol{\Psi})}$$

6.3 Contextual Equivalence

$$\begin{aligned}\Psi;\Delta;\Gamma \vdash e_1 \approx^{ctx} e_2 : \tau \stackrel{\text{def}}{=}\ & \Psi;\Delta;\Gamma \vdash e_1 : \tau \ \wedge\ \Psi;\Delta;\Gamma \vdash e_2 : \tau \ \wedge \\ & \forall C, M, \Psi', \tau'.\ \vdash C : (\Psi;\Delta;\Gamma \vdash \tau) \rightsquigarrow (\Psi';\cdot;\cdot \vdash \tau') \ \wedge\ \vdash M : \Psi' \\ & \qquad \Longrightarrow\ (\langle M \mid C[e_1]\rangle \downarrow \iff \langle M \mid C[e_2]\rangle \downarrow)\end{aligned}$$

6.4 CIU Equivalence

$$\begin{aligned}\Psi;\Delta;\Gamma \vdash e_1 \approx^{ciu} e_2 : \tau \stackrel{\text{def}}{=}\ & \Psi;\Delta;\Gamma \vdash e_1 : \tau \ \wedge\ \Psi;\Delta;\Gamma \vdash e_2 : \tau \ \wedge \\ & \forall \delta, \gamma, E, M, \Psi', \tau'.\ \cdot \vdash \delta : \Delta \ \wedge\ \Psi';\cdot;\cdot \vdash \gamma : \delta(\Gamma) \ \wedge \\ & \qquad \vdash E : (\Psi;\cdot;\cdot \vdash \tau) \rightsquigarrow (\Psi';\cdot;\cdot \vdash \tau') \ \wedge\ \vdash M : \Psi' \\ & \qquad \Longrightarrow\ (\langle M \mid E[\delta(\gamma(e_1))]\rangle \downarrow \iff \langle M \mid E[\delta(\gamma(e_2))]\rangle \downarrow)\end{aligned}$$

7 Logical Relation

Worlds and Auxiliary Definitions A world W consists of a step index k, a pair of heap types Ψ_1 and Ψ_2, and a sequence Θ of islands θ. Each island expresses invariants on certain parts of memory by encoding a state transition system and a memory relation MR that establishes which pairs of memories are acceptable in each state. (See Dreyer *et al.* [14] for details.)

The first island in Θ is distinguished: it tracks the immutable contents of the heap. We assign this island the index i_{box}. Further islands can be added to a world to encode invariants about mutable data.

$$\begin{aligned}
\text{World}_n &\stackrel{\text{def}}{=} \{\, W = (k, \Psi_1, \Psi_2, \Theta) \mid k < n \ \wedge\ \exists m \geq 1.\ \Theta \in \text{Island}_k^m \ \wedge \\
&\qquad \exists s_{\text{box}}.\ \Theta(i_{\text{box}}) = \text{island}_{\text{box}}(s_{\text{box}}, k) \ \wedge\ \Psi_1^{\text{ref}} \vdash s_{\text{box}}.M_1 : \Psi_1^{\text{box}} \ \wedge\ \Psi_2^{\text{ref}} \vdash s_{\text{box}}.M_2 : \Psi_2^{\text{box}} \} \\
\text{Island}_n &\stackrel{\text{def}}{=} \{\, \theta = (s, S, \delta, \pi, \text{MR}, \text{bij}) \mid \ s \in S \ \wedge\ S \in \text{Set} \ \wedge\ \delta \subseteq S \times S \ \wedge\ \pi \subseteq \delta \ \wedge \\
&\qquad \delta, \pi \text{ reflexive} \wedge \delta, \pi \text{ transitive} \wedge \text{MR} \in S \to \text{MemRel}_n \ \wedge\ \text{bij} \in S \to \mathbb{P}(\text{Val} \times \text{Val}) \,\}
\end{aligned}$$

$$\begin{aligned}
\text{MemAtom}_n &\stackrel{\text{def}}{=} \{\, (W, M_1, M_2) \mid W \in \text{World}_n \ \wedge\ \Psi_1 \vdash M_1 : \Psi_1' \ \wedge\ \Psi_2 \vdash M_2 : \Psi_2' \ \wedge \\
&\qquad \Psi_1 \uplus \Psi_1' = W.\Psi_1 \ \wedge\ \Psi_2 \uplus \Psi_2' = W.\Psi_2 \,\} \\
\text{MemRel}_n &\stackrel{\text{def}}{=} \{\, \varphi_M \subseteq \text{MemAtom}_n \mid \ \forall (W, M_1, M_2) \in \varphi_M.\ \forall W' \sqsupseteq W.\ (W', M_1, M_2) \in \varphi_M \,\} \\
\varphi_M \otimes \varphi_M' &\stackrel{\text{def}}{=} \{\, (W, M_1 \uplus M_1', M_2 \uplus M_2') \mid (W, M_1, M_2) \in \varphi_M \ \wedge\ (W, M_1', M_2') \in \varphi_M' \}
\end{aligned}$$

The states of θ_{box} encode the contents of the immutable part of the heap on each side. This island is allowed to transition only by adding more immutable data to the heap.

$$\begin{aligned}
i_{\text{box}} &= 1 \\
S_{\text{box}} &= \{\, (M_1, M_2) \,\} \\
\delta_{\text{box}} &= \{((M_1, M_2), (M_1', M_2')) \mid M_1 \subseteq M_1' \ \wedge\ M_2 \subseteq M_2' \} \\
\text{island}_{\text{box}}(s, k) &= (s, S_{\text{box}}, \delta_{\text{box}}, \delta_{\text{box}}, \lambda s.\{(W, s.M_1, s.M_2) \mid W \in \text{World}_k\}, \lambda s.\emptyset)
\end{aligned}$$

These are standard operations for dealing with step indexing: we can approximate a world or relation to a given number of steps with $\lfloor \cdot \rfloor_k$, and we can expend a step using the $\triangleright$ operator (read "later").

$$\begin{aligned}
\lfloor (\theta_1, \ldots, \theta_m) \rfloor_k &\stackrel{\text{def}}{=} (\lfloor \theta_1 \rfloor_k, \ldots, \lfloor \theta_m \rfloor_k) \\
\lfloor (s, S, \delta, \pi, \text{MR}, \text{bij}) \rfloor_k &\stackrel{\text{def}}{=} (s, S, \delta, \pi, \lfloor \text{MR} \rfloor_k, \text{bij}) \\
\lfloor \text{MR} \rfloor_k &\stackrel{\text{def}}{=} \lambda s.\ \lfloor \text{MR}(s) \rfloor_k \\
\lfloor \varphi_M \rfloor_k &\stackrel{\text{def}}{=} \{\, (W, M_1, M_2) \in \varphi_M \mid \ W.k < k \,\}
\end{aligned}$$

$$\begin{aligned}
\triangleright(k+1, \Psi_1, \Psi_2, \Theta) &\stackrel{\text{def}}{=} (k, \Psi_1, \Psi_2, \lfloor \Theta \rfloor_k) \\
\triangleright \varphi_e &\stackrel{\text{def}}{=} \{\, (W, e_1, e_2) \mid W.k > 0 \implies (\triangleright W, e_1, e_2) \in \varphi_e \,\} \\
\triangleright \varphi_v &\stackrel{\text{def}}{=} \{\, (W, v_1, v_2) \mid W.k > 0 \implies (\triangleright W, v_1, v_2) \in \varphi_v \,\}
\end{aligned}$$

Future worlds W' of a given world W, written $W' \sqsupseteq W$, may differ from W in any or all of the following ways: they may have expended steps, added new islands, or taken transitions in existing islands. When islands are added or transitioned, additional memory can be allocated. Public future worlds $W' \sqsupseteq_{\text{pub}} W$ are

similar, but must have taken public transitions from the island states in W.

$$
\begin{aligned}
&(k', \Psi_1', \Psi_2', \Theta') \sqsupseteq (k, \Psi_1, \Psi_2, \Theta) && \stackrel{\text{def}}{=} k' \le k \ \wedge\ \Psi_1' \supseteq \Psi_1 \ \wedge\ \Psi_2' \supseteq \Psi_2 \ \wedge\ \Theta' \sqsupseteq \lfloor \Theta \rfloor_{k'} \\
&&& \quad \wedge\ (k, \Psi_1, \Psi_2, \Theta) \in \text{World} \ \wedge\ (k', \Psi_1', \Psi_2', \Theta') \in \text{World} \\
&(\theta_1', \ldots, \theta_{m'}') \sqsupseteq (\theta_1, \ldots, \theta_m) && \stackrel{\text{def}}{=} m' \ge m \ \wedge\ \forall j \in \{1, \ldots, m\}.\ \theta_j' \sqsupseteq \theta_j \\
&(s', S', \delta', \pi', \text{MR}', \text{bij}') \sqsupseteq (s, S, \delta, \pi, \text{MR}, \text{bij}) && \stackrel{\text{def}}{=} (S', \delta', \pi', \text{MR}', \text{bij}') = (S, \delta, \pi, \text{MR}, \text{bij}) \ \wedge\ (s, s') \in \delta \\
\\
&(k', \Psi_1', \Psi_2', \Theta') \sqsupseteq_{\text{pub}} (k, \Psi_1, \Psi_2, \Theta) && \stackrel{\text{def}}{=} k' \le k \ \wedge\ \Psi_1' \supseteq \Psi_1 \ \wedge\ \Psi_2' \supseteq \Psi_2 \ \wedge\ \Theta' \sqsupseteq_{\text{pub}} \lfloor \Theta \rfloor_{k'} \\
&&& \quad \wedge\ (k, \Psi_1, \Psi_2, \Theta) \in \text{World} \ \wedge\ (k', \Psi_1', \Psi_2', \Theta') \in \text{World} \\
&(\theta_1', \ldots, \theta_{m'}') \sqsupseteq_{\text{pub}} (\theta_1, \ldots, \theta_m) && \stackrel{\text{def}}{=} m' \ge m \ \wedge\ \forall j \in \{1, \ldots, m\}.\ \theta_j' \sqsupseteq_{\text{pub}} \theta_j \\
&(s', S', \delta', \pi', \text{MR}', \text{bij}') \sqsupseteq_{\text{pub}} (s, S, \delta, \pi, \text{MR}, \text{bij}) && \stackrel{\text{def}}{=} (S', \delta', \pi', \text{MR}', \text{bij}') = (S, \delta, \pi, \text{MR}, \text{bij}) \ \wedge\ (s, s') \in \pi
\end{aligned}
$$

Given a world W, we often need to talk about future worlds of W where the only change is that new immutable memory has been allocated. We use this notation to capture this:

$$
\begin{aligned}
W \boxplus (M_1, M_2) \stackrel{\text{def}}{=} (&W.k, W.\Psi_1 \uplus \Psi_1, W.\Psi_2 \uplus \Psi_2, W.\Theta[i_{\text{box}} \mapsto \text{island}_{\text{box}}(W(i_{\text{box}}).s \uplus (M_1, M_2),\ W.k)]) \\
&\text{if } W.\Psi_1 \vdash M_1 : \Psi_1 \ \wedge\ W.\Psi_2 \vdash M_2 : \Psi_2 \ \wedge\ \text{boxheap}(\Psi_1) \ \wedge\ \text{boxheap}(\Psi_2).
\end{aligned}
$$

The following is a convenient shorthand for getting the memory relation from the current state of an island:

$$\text{currentMR}(\theta) \stackrel{\text{def}}{=} \theta.\text{MR}(\theta.s)$$

Admissible Relations Atoms are well-formed worlds together with a pair of components or values that are well-typed at the indicated type under the appropriate memory type of the world.

$$
\begin{aligned}
&\text{TermAtom}_n[\tau_1, \tau_2] && \stackrel{\text{def}}{=} \{\, (W, e_1, e_2) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1; \cdot; \cdot \vdash e_1 : \tau_1 \ \wedge\ W.\Psi_2; \cdot; \cdot \vdash e_2 : \tau_2 \,\} \\
&\text{ValAtom}_n[\tau_1, \tau_2] && \stackrel{\text{def}}{=} \{\, (W, v_1, v_2) \in \text{TermAtom}_n[\tau_1, \tau_2] \,\} \\
&\text{HvalAtom}_n[\psi_1, \psi_2] && \stackrel{\text{def}}{=} \{\, (W, \mathsf{h_1}, \mathsf{h_2}) \mid W \in \text{World}_n \ \wedge\ W.\Psi_1 \vdash \mathsf{h_1} : \psi_1 \ \wedge\ W.\Psi_2 \vdash \mathsf{h_2} : \psi_2 \,\} \\
&\text{ContAtom}[\tau_1, \tau_2] \rightsquigarrow [\tau_1', \tau_2'] && \stackrel{\text{def}}{=} \{(W, E_1, E_2) \mid W \in \text{World} \ \wedge\ \exists \Psi_1, \Psi_2. \\
&&& \qquad \vdash E_1 : (W.\Psi_1; \cdot; \cdot \vdash \tau_1) \rightsquigarrow (\Psi_1; \cdot; \cdot \vdash \tau_1') \wedge \\
&&& \qquad \vdash E_2 : (W.\Psi_2; \cdot; \cdot \vdash \tau_2) \rightsquigarrow (\Psi_2; \cdot; \cdot \vdash \tau_2')\}
\end{aligned}
$$

Relations φ_v on values must respect forward boundary cancellation on each side. If they are designated as "translation relations," they must also respect backward boundary cancellation. Since boundaries can allocate (immutable) memory, boundary cancellation moves us to a future world that has added that memory to the current state of θ_{box}. The $\boxplus$ operation we defined earlier expresses this transition.

$$
\begin{aligned}
&\text{ValRel}[\tau_1, \tau_2] && \stackrel{\text{def}}{=} \{\, \varphi_v^F \subseteq \text{ValAtom}[\tau_1, \tau_2] \mid \forall (W, \mathsf{v_1}, \mathsf{v_2}) \in \varphi_v^F.\ (\forall W' \sqsupseteq W.\ (W', \mathsf{v_1}, \mathsf{v_2}) \in \varphi_v^F) \wedge \\
&&& \qquad \forall (M_1, M_2) : W.\ \forall \mathsf{v_1'}, \mathsf{v_2'}, M_1', M_2'. \\
&&& \qquad\quad (\mathsf{^{\tau_1}FC(CF^{\tau_1}}(\mathsf{v_1}, M_1)) = (\mathsf{v_1'}, M_1 \uplus M_1') \implies (W \boxplus (M_1', \{\cdot\}), \mathsf{v_1'}, \mathsf{v_2}) \in \varphi_v^F) \wedge \\
&&& \qquad\quad (\mathsf{^{\tau_2}FC(CF^{\tau_2}}(\mathsf{v_2}, M_2)) = (\mathsf{v_2'}, M_2 \uplus M_2') \implies (W \boxplus (\{\cdot\}, M_2'), \mathsf{v_1}, \mathsf{v_2'}) \in \varphi_v^F)\} \\
&\text{ValRel}[\tau_1, \tau_2] && \stackrel{\text{def}}{=} \{\, \varphi_v^C \subseteq \text{ValAtom}[\tau_1, \tau_2] \mid \forall (W, \mathsf{v_1}, \mathsf{v_2}) \in \varphi_v^C.\ (\forall W' \sqsupseteq W.\ (W', \mathsf{v_1}, \mathsf{v_2}) \in \varphi_v^C) \wedge \\
&&& \qquad \forall (M_1, M_2) : W.\ \forall \mathsf{v_1'}, \mathsf{v_2'}, M_1', M_2'. \\
&&& \qquad\quad (\mathsf{^{\tau_1}CA(AC^{\tau_1}}(\mathsf{v_1}, M_1)) = (\mathsf{v_1'}, M_1 \uplus M_1') \implies (W \boxplus (M_1', \{\cdot\}), \mathsf{v_1'}, \mathsf{v_2}) \in \varphi_v^C) \wedge \\
&&& \qquad\quad (\mathsf{^{\tau_2}CA(AC^{\tau_2}}(\mathsf{v_2}, M_2)) = (\mathsf{v_2'}, M_2 \uplus M_2') \implies (W \boxplus (\{\cdot\}, M_2'), \mathsf{v_1}, \mathsf{v_2'}) \in \varphi_v^C)\} \\
&\text{ValRel}[\tau_1, \tau_2] && \stackrel{\text{def}}{=} \{\, \varphi_v^A \subseteq \text{ValAtom}[\tau_1, \tau_2] \mid \forall (W, \mathsf{v_1}, \mathsf{v_2}) \in \varphi_v^A.\ \forall W' \sqsupseteq W.\ (W', \mathsf{v_1}, \mathsf{v_2}) \in \varphi_v^A\}
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{TransRel}^{\mathcal{C}}[\tau_1,\tau_2] \stackrel{\text{def}}{=} \{\, \varphi_v^C \in \mathrm{ValRel}[\tau_1{}^{\langle \mathcal{C}\rangle}, \tau_2{}^{\langle \mathcal{C}\rangle}] \mid \forall (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C.\ \forall (M_1, M_2) : W.\ \forall \mathbf{v_1'}, \mathbf{v_2'}, M_1', M_2'.\\
(\,\mathbf{CF}^{\tau_1}({}^{\tau_1}\mathbf{FC}(\mathbf{v_1}, M_1)) = (\mathbf{v_1'}, M_1 \uplus M_1') \implies (W \uplus (M_1', \{\cdot\}), \mathbf{v_1'}, \mathbf{v_2}) \in \varphi_v^C\,) \wedge\\
(\,\mathbf{CF}^{\tau_2}({}^{\tau_2}\mathbf{FC}(\mathbf{v_2}, M_2)) = (\mathbf{v_2'}, M_2 \uplus M_2') \implies (W \uplus (\{\cdot\}, M_2'), \mathbf{v_1}, \mathbf{v_2'}) \in \varphi_v^C)\}\\
\mathrm{TransRel}^{\mathcal{A}}[\tau_1,\tau_2] \stackrel{\text{def}}{=} \{\, \varphi_v^A \in \mathrm{ValRel}[\tau_1{}^{\langle \mathcal{A}\rangle}, \tau_2{}^{\langle \mathcal{A}\rangle}] \mid \forall (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^A.\ \forall (M_1, M_2) : W.\ \forall \mathbf{v_1'}, \mathbf{v_2'}, M_1', M_2'.\\
(\,\mathbf{AC}^{\tau_1}({}^{\tau_1}\mathbf{CA}(\mathbf{v_1}, M_1)) = (\mathbf{v_1'}, M_1 \uplus M_1') \implies (W \uplus (M_1', \{\cdot\}), \mathbf{v_1'}, \mathbf{v_2}) \in \varphi_v^A\,) \wedge\\
(\,\mathbf{AC}^{\tau_2}({}^{\tau_2}\mathbf{CA}(\mathbf{v_2}, M_2)) = (\mathbf{v_2'}, M_2 \uplus M_2') \implies (W \uplus (\{\cdot\}, M_2'), \mathbf{v_1}, \mathbf{v_2'}) \in \varphi_v^A)\}
\end{aligned}
$$

We need a basic notion of the translation of a relation φ_v. Given a relation interpretating a type variable, the definitions below express the bare minimum requirement for what should be related under the relation that interprets its translation.

$$
\begin{aligned}
\mathcal{CF}(\tau_1,\tau_2,\varphi_v^F) &= \{(W \uplus (M_1', M_2'), \mathbf{v_1}, \mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^F \ \wedge\\
&\qquad \mathbf{CF}^{\tau_1}(\mathbf{v_1}, M_1) = (\mathbf{v_1}, M_1 \uplus M_1') \ \wedge\ \mathbf{CF}^{\tau_2}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2')\}\\
&\quad \text{if } \varphi_v^F \in \mathrm{ValRel}[\tau_1,\tau_2]\\
\mathcal{FC}(\tau_1,\tau_2,\varphi_v^C) &= \{(W \uplus (M_1', M_2'), \mathbf{v_1}, \mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C \ \wedge\\
&\qquad {}^{\tau_1}\mathbf{FC}(\mathbf{v_1}, M_1) = (\mathbf{v_1}, M_1 \uplus M_1') \ \wedge\ {}^{\tau_2}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2')\}\\
&\quad \text{if } \varphi_v^C \in \mathrm{TransRel}^{\mathcal{C}}[\tau_1,\tau_2]\\
\mathcal{AC}(\tau_1,\tau_2,\varphi_v^C) &= \{(W \uplus (M_1', M_2'), \mathbf{v_1}, \mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C \ \wedge\\
&\qquad \mathbf{AC}^{\tau_1}(\mathbf{v_1}, M_1) = (\mathbf{v_1}, M_1 \uplus M_1') \ \wedge\ \mathbf{AC}^{\tau_2}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2')\}\\
&\quad \text{if } \varphi_v^C \in \mathrm{ValRel}[\tau_1,\tau_2]\\
\mathcal{CA}(\tau_1,\tau_2,\varphi_v^A) &= \{(W \uplus (M_1', M_2'), \mathbf{v_1}, \mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^A \ \wedge\\
&\qquad {}^{\tau_1}\mathbf{CA}(\mathbf{v_1}, M_1) = (\mathbf{v_1}, M_1 \uplus M_1') \ \wedge\ {}^{\tau_2}\mathbf{CA}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2')\}\\
&\quad \text{if } \varphi_v^A \in \mathrm{TransRel}^{\mathcal{A}}[\tau_1,\tau_2]
\end{aligned}
$$

We now define the full requirements for interpretations of type variables, which much include relations specifying how the translation should be interpreted:

$$
\begin{aligned}
\mathrm{FValRel} &\stackrel{\text{def}}{=} \{\, \mathrm{VR} = (\tau_1,\tau_2,\varphi_v^F,\varphi_v^C,\varphi_v^A) \mid\\
&\qquad \varphi_v^F \in \mathrm{ValRel}[\tau_1,\tau_2] \ \wedge\ \varphi_v^C \in \mathrm{TransRel}^{\mathcal{C}}[\tau_1,\tau_2] \ \wedge\ \varphi_v^A \in \mathrm{TransRel}^{\mathcal{A}}[\tau_1{}^{\langle \mathcal{C}\rangle}, \tau_2{}^{\langle \mathcal{C}\rangle}] \wedge\\
&\qquad \mathcal{CF}(\tau_1,\tau_2,\varphi_v^F) \subseteq \varphi_v^C \ \wedge\ \mathcal{FC}(\tau_1,\tau_2,\varphi_v^C) \subseteq \varphi_v^F \ \wedge\\
&\qquad \mathcal{AC}(\tau_1{}^{\langle \mathcal{C}\rangle}, \tau_2{}^{\langle \mathcal{C}\rangle}, \varphi_v^C) \subseteq \varphi_v^A \ \wedge\ \mathcal{CA}(\tau_1{}^{\langle \mathcal{C}\rangle}, \tau_2{}^{\langle \mathcal{C}\rangle}, \varphi_v^A) \subseteq \varphi_v^C\}\\
\mathrm{CValRel} &\stackrel{\text{def}}{=} \{\, \mathrm{VR} = (\tau_1,\tau_2,\varphi_v^C,\varphi_v^A) \mid \varphi_v^C \in \mathrm{ValRel}[\tau_1,\tau_2] \ \wedge\ \varphi_v^A \in \mathrm{TransRel}^{\mathcal{A}}[\tau_1,\tau_2] \wedge\\
&\qquad \mathcal{AC}(\tau_1,\tau_2,\varphi_v^C) \subseteq \varphi_v^A \ \wedge\ \mathcal{CA}(\tau_1,\tau_2,\varphi_v^A) \subseteq \varphi_v^C\}\\
\mathrm{AValRel} &\stackrel{\text{def}}{=} \{\, \mathrm{VR} = (\tau_1,\tau_2,\varphi_v^A) \mid \varphi_v^A \in \mathrm{ValRel}[\tau_1,\tau_2]\}
\end{aligned}
$$

The set $\mathcal{D}[\![\Delta]\!]$ ensures that an environment ρ mapping type variables to value relations is well-formed.

$$
\begin{aligned}
\mathcal{D}[\![\cdot]\!] &\stackrel{\text{def}}{=} \{\, \emptyset \,\}\\
\mathcal{D}[\![\Delta, \alpha]\!] &\stackrel{\text{def}}{=} \{\, \rho[\alpha \mapsto \mathrm{VR}] \mid\ \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \mathrm{VR} \in \mathrm{FValRel}\,\}\\
\mathcal{D}[\![\Delta, \boldsymbol{\alpha}]\!] &\stackrel{\text{def}}{=} \{\, \rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] \mid\ \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \mathrm{VR} \in \mathrm{CValRel}\,\}\\
\mathcal{D}[\![\Delta, \boldsymbol{\alpha}]\!] &\stackrel{\text{def}}{=} \{\, \rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] \mid\ \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge\ \mathrm{VR} \in \mathrm{AValRel}\,\}
\end{aligned}
$$

We use ρ_1 and ρ_2 to denote the substitutions formed by mapping variables in $\mathrm{dom}\,\rho$ to the first and second components, respectively, of the tuples they map to.

We also use some shorthands for referring to atoms of a particular type in terms of an environment ρ:

$$
\begin{array}{ll}
\mathrm{TermAtom}[\tau]\rho & \stackrel{\mathrm{def}}{=} \mathrm{TermAtom}[\rho_1(\tau), \rho_2(\tau)] \\
\mathrm{ValAtom}[\tau]\rho & \stackrel{\mathrm{def}}{=} \mathrm{ValAtom}[\rho_1(\tau), \rho_2(\tau)] \\
\mathrm{HvalAtom}[\psi]\rho & \stackrel{\mathrm{def}}{=} \mathrm{HvalAtom}[\rho_1(\psi), \rho_2(\psi)] \\
\mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau']\rho' & \stackrel{\mathrm{def}}{=} \mathrm{ContAtom}[\rho_1(\tau), \rho_2(\tau)] \rightsquigarrow [\rho_1'(\tau_1'), \rho_2'(\tau_2')]
\end{array}
$$

Core Relations The relation $\mathcal{V}[\![\tau]\!]\rho$ expresses when two values are related under a given world. For values from language F, it is almost completely standard.

$$
\begin{array}{ll}
\mathcal{V}[\![\alpha]\!]\rho & = \rho(\alpha).\varphi_v^F \\
\mathcal{V}[\![\mathsf{unit}]\!]\rho & = \{\, (W, (), ()) \in \mathrm{ValAtom}[\mathsf{unit}]\rho \,\} \\
\mathcal{V}[\![\mathsf{int}]\!]\rho & = \{\, (W, \mathsf{n}, \mathsf{n}) \in \mathrm{ValAtom}[\mathsf{int}]\rho \,\} \\
\mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho & = \{\, (W, \mathsf{v}_1, \mathsf{v}_2) \in \mathrm{ValAtom}[\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\rho \mid \\
& \quad \forall W' \sqsupseteq W.\ \forall \overline{\mathrm{VR} \in \mathrm{FValRel}}.\ \forall \overline{\mathsf{v}_1'}, \overline{\mathsf{v}_2'}.\ \overline{(W', \mathsf{v}_1', \mathsf{v}_2') \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]} \\
& \quad \implies (W', \mathsf{v}_1\ \overline{[\mathrm{VR}.\tau_1]}\ \overline{\mathsf{v}_1'}, \mathsf{v}_2\ \overline{[\mathrm{VR}.\tau_2]}\ \overline{\mathsf{v}_2'}) \in \mathcal{E}[\![\tau']\!]\rho\overline{[\alpha \mapsto \mathrm{VR}]}\,\} \\
\mathcal{V}[\![\exists\alpha.\tau]\!]\rho & = \{(W, \mathsf{pack}\langle\tau_1,\mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\alpha.\tau), \mathsf{pack}\langle\tau_2,\mathsf{v}_2\rangle\ \mathsf{as}\ \rho_2(\exists\alpha.\tau)) \in \mathrm{ValAtom}[\exists\alpha.\tau]\rho \mid \\
& \quad \exists \mathrm{VR} \in \mathrm{FValRel}.\ \mathrm{VR}.\tau_1 = \tau_1\ \wedge\ \mathrm{VR}.\tau_2 = \tau_2\ \wedge\ (W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]\,\} \\
\mathcal{V}[\![\mu\alpha.\tau]\!]\rho & = \{\, (W, \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\ \mathsf{v}_1, \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\ \mathsf{v}_2) \in \mathrm{ValAtom}[\mu\alpha.\tau]\rho \mid \\
& \quad (W, \mathsf{v}_1, \mathsf{v}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho\,\} \\
\mathcal{V}[\![\langle\tau_1, \ldots, \tau_\mathsf{n}\rangle]\!]\rho & = \{\, (W, \langle\mathsf{v}_{11}, \ldots, \mathsf{v}_{1\mathsf{n}}\rangle, \langle\mathsf{v}_{21}, \ldots, \mathsf{v}_{2\mathsf{n}}\rangle) \in \mathrm{ValAtom}[\langle\tau_1, \ldots, \tau_\mathsf{n}\rangle]\rho \mid \\
& \quad \forall \mathsf{j} \in \{1, \ldots, \mathsf{n}\}.\ (W, \mathsf{v}_{1\mathsf{j}}, \mathsf{v}_{2\mathsf{j}}) \in \mathcal{V}[\![\tau_\mathsf{j}]\!]\rho\,\} \\
\mathcal{V}[\![\mathsf{L}\langle\tau\rangle]\!]\rho & = \{\, (W, {}^{\rho_1(\mathsf{L}\langle\tau\rangle)}\mathcal{FC}\ \mathsf{v}_1, {}^{\rho_2(\mathsf{L}\langle\tau\rangle)}\mathcal{FC}\ \mathsf{v}_2) \in \mathrm{ValAtom}[\mathsf{L}\langle\tau\rangle]\rho \mid (W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho\,\}
\end{array}
$$

The cases for language C types are almost identical to those for language F. The only addition is the case for a suspended type variable.

$$
\begin{array}{ll}
\mathcal{V}[\![\boldsymbol{\alpha}]\!]\rho & = \rho(\boldsymbol{\alpha}).\varphi_v^C \\
\mathcal{V}[\![\mathbf{unit}]\!]\rho & = \{\, (W, (), ()) \in \mathrm{ValAtom}[\mathbf{unit}]\rho \,\} \\
\mathcal{V}[\![\mathbf{int}]\!]\rho & = \{\, (W, \mathbf{n}, \mathbf{n}) \in \mathrm{ValAtom}[\mathbf{int}]\rho \,\} \\
\mathcal{V}[\![\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau'}]\!]\rho & = \{\, (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau'}]\rho \mid \\
& \quad \forall W' \sqsupseteq W.\ \forall \overline{\mathrm{VR} \in \mathrm{CValRel}}.\ \forall \overline{\mathbf{v_1'}}, \overline{\mathbf{v_2'}}.\ \overline{(W', \mathbf{v_1'}, \mathbf{v_2'}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]} \\
& \quad \implies (W', \mathbf{v_1}\ \overline{[\mathrm{VR}.\boldsymbol{\tau_1}]}\ \overline{\mathbf{v_1'}}, \mathbf{v_2}\ \overline{[\mathrm{VR}.\boldsymbol{\tau_2}]}\ \overline{\mathbf{v_2'}}) \in \mathcal{E}[\![\boldsymbol{\tau'}]\!]\rho\overline{[\boldsymbol{\alpha} \mapsto \mathrm{VR}]}\} \\
\mathcal{V}[\![\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\!]\rho & = \{\, (W, \mathbf{pack}\langle\boldsymbol{\tau_1},\mathbf{v_1}\rangle\ \mathbf{as}\ \rho_1(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}), \mathbf{pack}\langle\boldsymbol{\tau_2},\mathbf{v_2}\rangle\ \mathbf{as}\ \rho_2(\exists\boldsymbol{\alpha}.\boldsymbol{\tau})) \in \mathrm{ValAtom}[\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\rho \mid \\
& \quad \exists \mathrm{VR} \in \mathrm{CValRel}.\ \mathrm{VR}.\boldsymbol{\tau_1} = \boldsymbol{\tau_1}\ \wedge\ \mathrm{VR}.\boldsymbol{\tau_2} = \boldsymbol{\tau_2}\ \wedge\ (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]\,\} \\
\mathcal{V}[\![\mu\boldsymbol{\alpha}.\boldsymbol{\tau}]\!]\rho & = \{\, (W, \mathbf{fold}_{\rho_1(\mu\boldsymbol{\alpha}.\boldsymbol{\tau})}\ \mathbf{v_1}, \mathbf{fold}_{\rho_2(\mu\boldsymbol{\alpha}.\boldsymbol{\tau})}\ \mathbf{v_2}) \in \mathrm{ValAtom}[\mu\boldsymbol{\alpha}.\boldsymbol{\tau}]\rho \mid \\
& \quad (W, \mathbf{v_1}, \mathbf{v_2}) \in \triangleright\mathcal{V}[\![\boldsymbol{\tau}[\mu\boldsymbol{\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}]]\!]\rho\,\} \\
\mathcal{V}[\![\langle\boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n}\rangle]\!]\rho & = \{\, (W, \langle\mathbf{v_{11}}, \ldots, \mathbf{v_{1n}}\rangle, \langle\mathbf{v_{21}}, \ldots, \mathbf{v_{2n}}\rangle) \in \mathrm{ValAtom}[\langle\boldsymbol{\tau_1}, \ldots, \boldsymbol{\tau_n}\rangle]\rho \mid \\
& \quad \forall \mathbf{j} \in \{\mathbf{1}, \ldots, \mathbf{n}\}.\ (W, \mathbf{v_{1j}}, \mathbf{v_{2j}}) \in \mathcal{V}[\![\boldsymbol{\tau_j}]\!]\rho\,\} \\
\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho & = \rho(\alpha).\varphi_v^C \\
\mathcal{V}[\![\mathbf{L}\langle\tau\rangle]\!]\rho & = \{\, (W, {}^{\rho_1(\mathbf{L}\langle\tau\rangle)}\mathcal{CA}\ \mathbf{v_1}, {}^{\rho_2(\mathbf{L}\langle\tau\rangle)}\mathcal{CA}\ \mathbf{v_2}) \in \mathrm{ValAtom}[\mathbf{L}\langle\tau\rangle]\rho \mid (W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho\,\}
\end{array}
$$

For language A, we add cases for mutable and immutable references, and a second relation $\mathcal{HV}[\![\psi]\!]\rho$ to describe when heap values are related, but otherwise we continue the patterns of previous languages.

$$
\begin{aligned}
\mathcal{V}[\![\alpha]\!]\rho &= \rho(\alpha).\varphi_v^A \\
\mathcal{V}[\![\mathsf{unit}]\!]\rho &= \{\,(W, (), ()) \in \mathrm{ValAtom}[\mathsf{unit}]\rho\,\} \\
\mathcal{V}[\![\mathsf{int}]\!]\rho &= \{\,(W, \mathsf{n}, \mathsf{n}) \in \mathrm{ValAtom}[\mathsf{int}]\rho\,\} \\
\mathcal{V}[\![\exists\alpha.\tau]\!]\rho &= \{\,(W, \mathsf{pack}\langle\tau_1,\mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\alpha.\tau), \mathsf{pack}\langle\tau_2,\mathsf{v}_2\rangle\ \mathsf{as}\ \rho_2(\exists\alpha.\tau)) \in \mathrm{ValAtom}[\exists\alpha.\tau]\rho \mid \\
&\qquad \exists \mathrm{VR} \in \mathrm{AValRel}.\, \mathrm{VR}.\tau_1 = \tau_1 \wedge \mathrm{VR}.\tau_2 = \tau_2 \wedge (W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]\,\} \\
\mathcal{V}[\![\mu\alpha.\tau]\!]\rho &= \{\,(W, \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\ \mathsf{v}_1, \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\ \mathsf{v}_2) \in \mathrm{ValAtom}[\mu\alpha.\tau]\rho \mid \\
&\qquad (W, \mathsf{v}_1, \mathsf{v}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho\,\} \\
\mathcal{V}[\![\mathsf{ref}\ \psi]\!]\rho &= \{(W, \ell_1, \ell_2) \in \mathrm{ValAtom}[\mathsf{ref}\ \psi]\rho \mid \exists i.\ \forall W' \sqsupseteq W.\ (\ell_1, \ell_2) \in W'(i).\mathrm{bij}(W'(i).s) \wedge \\
&\qquad \exists\varphi_M.\ \mathrm{currentMR}(W'(i)) = \varphi_M \otimes \\
&\qquad\qquad \{(\widetilde{W}, \{\ell_1 \mapsto \mathsf{h}_1\}, \{\ell_2 \mapsto \mathsf{h}_2\}) \in \mathrm{MemAtom} \mid (\widetilde{W}, \mathsf{h}_1, \mathsf{h}_2) \in \mathcal{HV}[\![\psi]\!]\rho\} \\
\mathcal{V}[\![\mathsf{box}\,\langle\tau_1, \ldots, \tau_\mathsf{n}\rangle]\!]\rho &= \{\,(W, \ell_1, \ell_2) \in \mathrm{ValAtom}[\mathsf{box}\,\langle\tau_1, \ldots, \tau_\mathsf{n}\rangle]\rho \mid \\
&\qquad \forall (W', M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}})). \\
&\qquad\quad (W', M_1(\ell_1), M_2(\ell_2)) \in \mathcal{HV}[\![\langle\tau_1, \ldots, \tau_\mathsf{n}\rangle]\!]\rho\,\} \\
\mathcal{V}[\![\mathsf{box}\,\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho &= \{\,(W, \ell_1[\tau'_{11}, \ldots, \tau'_{1\mathsf{m}}], \ell_2[\tau'_{21}, \ldots, \tau'_{2\mathsf{n}}]) \in \mathrm{ValAtom}[\mathsf{box}\,\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\rho \mid \\
&\qquad \forall (W', M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}})). \\
&\qquad\quad M_1(\ell_1) = \lambda[\beta_{11}, \ldots, \beta_{1\mathsf{m}}, \overline{\alpha}]\,(\overline{\mathsf{x}:\tau_1}).\mathsf{t}_1 \ \wedge\ \overline{\tau_1[\overline{\tau'_1/\beta_1}] = \rho_1(\tau)} \wedge \\
&\qquad\quad M_2(\ell_2) = \lambda[\beta_{21}, \ldots, \beta_{2\mathsf{n}}, \overline{\alpha}]\,(\overline{\mathsf{x}:\tau_2}).\mathsf{t}_2 \ \wedge\ \overline{\tau_2[\overline{\tau'_2/\beta_2}] = \rho_2(\tau)} \wedge \\
&\qquad\quad (W', \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\rho_1(\tau)}).\mathsf{t}_1[\overline{\tau'_1/\beta_1}], \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\rho_2(\tau)}).\mathsf{t}_2[\overline{\tau'_2/\beta_2}]) \\
&\qquad\qquad \in \mathcal{HV}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho\,\} \\
\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho &= \rho(\alpha).\varphi_v^A \\
\mathcal{V}[\![\lceil\boldsymbol{\alpha}\rceil]\!]\rho &= \rho(\boldsymbol{\alpha}).\varphi_v^A
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{HV}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho &= \{\,(W, \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\rho_1(\tau)}).\mathsf{t}_1, \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\rho_2(\tau)}).\mathsf{t}_2) \in \mathrm{HvalAtom}[\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\rho \mid \\
&\qquad \forall W' \sqsupseteq W.\ \forall\overline{\mathrm{VR} \in \mathrm{AValRel}}.\ \forall\overline{\mathsf{v}_1, \mathsf{v}_2}.\ \overline{(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]} \\
&\qquad\quad \Longrightarrow\ (W', \mathsf{t}_1[\overline{\mathrm{VR}.\tau_1/\alpha}][\overline{\mathsf{v}_1/\mathsf{x}}], \mathsf{t}_2[\overline{\mathrm{VR}.\tau_2/\alpha}][\overline{\mathsf{v}_2/\mathsf{x}}]) \in \mathcal{E}[\![\tau']\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}]\} \\
\mathcal{HV}[\![\langle\tau_1, \ldots, \tau_\mathsf{n}\rangle]\!]\rho &= \{\,(W, \langle\mathsf{v}_{11}, \ldots, \mathsf{v}_{1\mathsf{n}}\rangle, \langle\mathsf{v}_{21}, \ldots, \mathsf{v}_{2\mathsf{n}}\rangle) \in \mathrm{HvalAtom}[\langle\tau_1, \ldots, \tau_\mathsf{n}\rangle]\rho \mid \\
&\qquad \forall \mathsf{j} \in \{1, \ldots, \mathsf{n}\}.\ (W, \mathsf{v}_{1\mathsf{j}}, \mathsf{v}_{2\mathsf{j}}) \in \mathcal{V}[\![\tau_\mathsf{j}]\!]\rho\,\}
\end{aligned}
$$

The relations $\mathcal{K}[\![\tau]\!]\rho$ and $\mathcal{E}[\![\tau]\!]\rho$ interpret types as sets of continuations or terms, respectively. They depend on a notion of related observations, $\mathcal{O}$.

$$\begin{aligned}
\mathcal{K}[\![\tau]\!]\rho &= \{\, (W, E_1, E_2) \in \mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau']\rho' \mid \\
&\qquad \forall W', v_1, v_2.\ W' \sqsupseteq_{\mathrm{pub}} W \ \wedge\ (W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho \implies (W', E_1[v_1], E_2[v_2]) \in \mathcal{O} \,\} \\
\mathcal{E}[\![\tau]\!]\rho &= \{\, (W, e_1, e_2) \in \mathrm{TermAtom}[\tau]\rho \mid \\
&\qquad \forall E_1, E_2.\ (W, E_1, E_2) \in \mathcal{K}[\![\tau]\!]\rho \implies (W, E_1[e_1], E_2[e_2]) \in \mathcal{O} \,\}
\end{aligned}$$

$$\begin{aligned}
(M_1, M_2) : W &= (W.k > 0 \implies (\triangleright W, M_1, M_2) \in \bigotimes\{\, \mathrm{currentMR}(\theta) \mid \theta \in W.\Theta \,\}) \\
\mathrm{running}(k, \langle M \mid e \rangle) &= \exists M', e'.\ \langle M \mid e \rangle \longmapsto^{k+1} \langle M' \mid e' \rangle \\
\mathcal{O} &= \{\, (W, e_1, e_2) \mid\ \forall (M_1, M_2) : W.\ (\langle M_1 \mid e_1 \rangle \downarrow\ \wedge\ \langle M_2 \mid e_2 \rangle \downarrow) \vee \\
&\qquad\qquad (\mathrm{running}(W.k, \langle M_1 \mid e_1 \rangle)\ \wedge\ \mathrm{running}(W.k, \langle M_2 \mid e_2 \rangle)) \,\}
\end{aligned}$$

Finally, we have interpretations for environments. $\mathcal{D}[\![\Delta]\!]$ was given earlier; we here define $\mathcal{H}[\![\Psi]\!]$ and $\mathcal{G}[\![\Gamma]\!]\rho$.

$$\begin{aligned}
\mathcal{H}[\![\{\cdot\}]\!] &= \mathrm{World} \\
\mathcal{H}[\![\Psi, \ell : {}^{\mathsf{box}}\psi]\!] &= \mathcal{H}[\![\Psi]\!] \cap \{\, W \in \mathrm{World} \mid (W, \ell, \ell) \in \mathcal{V}[\![\mathbf{box}\ \psi]\!]\emptyset \,\} \\
\mathcal{H}[\![\Psi, \ell : {}^{\mathsf{ref}}\psi]\!] &= \mathcal{H}[\![\Psi]\!] \cap \{\, W \in \mathrm{World} \mid (W, \ell, \ell) \in \mathcal{V}[\![\mathbf{ref}\ \psi]\!]\emptyset \,\} \\
\mathcal{G}[\![\cdot]\!]\rho &= \{\, (W, \emptyset) \mid\ W \in \mathrm{World} \,\} \\
\mathcal{G}[\![\Gamma, x : \tau]\!]\rho &= \{\, (W, \gamma[x \mapsto (v_1, v_2)]) \mid \gamma \in \mathcal{G}[\![\Gamma]\!]\rho\ \wedge\ (W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho \,\}
\end{aligned}$$

Our definition of logical equivalence is this:

$$\begin{aligned}
\Psi; \Delta; \Gamma \vdash e_1 \approx e_2 : \tau \stackrel{\mathrm{def}}{=}\ & \Psi; \Delta; \Gamma \vdash e_1 : \tau\ \wedge\ \Psi; \Delta; \Gamma \vdash e_2 : \tau\ \wedge \\
& \forall W, \rho, \gamma.\ W \in \mathcal{H}[\![\Psi]\!]\ \wedge\ \rho \in \mathcal{D}[\![\Delta]\!]\ \wedge\ (W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho \\
& \qquad \implies (W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_2))) \in \mathcal{E}[\![\tau]\!]\rho
\end{aligned}$$

8 Proofs: Basic Properties

8.1 Embedding Theorems

Theorem 8.1 (Multi-Language Type Judgment Embeds Single-Language Type Judgments)

1. If $\Delta; \Gamma \vdash \mathsf{e} : \tau$ under the type judgment for language F, then $\cdot; \Delta; \Gamma \vdash \mathsf{e} : \tau$ under the judgment for FCA.
2. If $\boldsymbol{\Delta}; \boldsymbol{\Gamma} \vdash \mathbf{e} : \boldsymbol{\tau}$ in language C, then $\cdot; \boldsymbol{\Delta}; \boldsymbol{\Gamma} \vdash \mathbf{e} : \boldsymbol{\tau}$ in FCA.
3. If $\Psi; \Delta; \Gamma \vdash \mathsf{e} : \tau$ in language A, then $\Psi; \Delta; \Gamma \vdash \mathsf{e} : \tau$ in FCA.

Proof

By induction on the single-language type derivations. □

Theorem 8.2 (Multi-Language Reduction Embeds Single-Language Reduction)

1. If $\mathsf{e} \longmapsto \mathsf{e}'$ under the reduction relation for language F, then for any M, $\langle M \mid \mathsf{e} \rangle \longmapsto \langle M \mid \mathsf{e}' \rangle$ in FCA.
2. If $\mathbf{e} \longmapsto \mathbf{e}'$ in C, then for any M, $\langle M \mid \mathbf{e} \rangle \longmapsto \langle M \mid \mathbf{e}' \rangle$ in FCA.
3. If $\langle \mathsf{H} \mid \mathsf{e} \rangle \longmapsto \langle \mathsf{H} \mid \mathsf{e}' \rangle$ in A, then $\langle \mathsf{H} \mid \mathsf{e} \rangle \longmapsto \langle \mathsf{H} \mid \mathsf{e}' \rangle$ in FCA.

Proof

By inspection of the reduction relations. □

8.2 Properties of the Value Translations

Lemma 8.3 (Value Translation Only Adds Memory)
For any v, $\mathbf{v}$, $\mathbf{v}$, M where $\vdash M : \Psi$ and

$$\Psi; \cdot; \cdot \vdash \mathsf{v} : \tau, \quad \Psi; \cdot; \cdot \vdash \mathbf{v} : \boldsymbol{\tau}, \quad \text{and } \Psi; \cdot; \cdot \vdash \mathbf{v} : \tau,$$

the following hold:

- $\exists! \mathbf{v}'.\ \mathbf{CF}^{\tau}(\mathsf{v}, M) = (\mathbf{v}', M)$.
- $\exists! \mathsf{v}'.\ {}^{\tau}\mathbf{FC}(\mathbf{v}, M) = (\mathsf{v}', M)$.
- $\exists \mathbf{v}', \mathsf{H}, \Psi.\ \mathbf{AC}^{\tau}(\mathbf{v}, M) = (\mathbf{v}', (M \uplus \mathsf{H})) \ \wedge \ \Psi \vdash \mathsf{H} : \Psi$.
- $\exists! \mathbf{v}'.\ {}^{\tau}\mathbf{CA}(\mathbf{v}, M) = (\mathbf{v}', M)$.

Proof

By inspection of the translations. □

Lemma 8.4 (Weakening for Value Translation)
If $\mathbf{AC}^{\tau}(\mathbf{v}, M) = (\mathbf{v}, M')$ and $\mathrm{dom}(M') \cap \mathrm{dom}(M'') = \emptyset$, then $\mathbf{AC}^{\tau}(\mathbf{v}, M \uplus M'') = (\mathbf{v}, M' \uplus M'')$.

Proof

By inspection of the translations. □

Lemma 8.5 (Value Translation Preserves Types)
Let $\vdash M : \Psi$ and $\vdash M' : \Psi'$. Then

1. If $\Psi; \cdot; \cdot \vdash \mathsf{v} : \tau$ and $\mathbf{CF}^{\tau}(\mathsf{v}, M) = (\mathbf{v}, M')$, then $\Psi'; \cdot; \cdot \vdash \mathbf{v} : \tau^{\langle \mathcal{C} \rangle}$.
2. If $\Psi; \cdot; \cdot \vdash \mathbf{v} : \tau^{\langle \mathcal{C} \rangle}$ and ${}^{\tau}\mathbf{FC}(\mathbf{v}, M) = (\mathsf{v}, M')$, then $\Psi'; \cdot; \cdot \vdash \mathsf{v} : \tau$.
3. If $\Psi; \cdot; \cdot \vdash \mathbf{v} : \boldsymbol{\tau}$ and $\mathbf{AC}^{\tau}(\mathbf{v}, M) = (\mathbf{v}, M')$, then $\Psi'; \cdot; \cdot \vdash \mathbf{v} : \boldsymbol{\tau}^{\langle \mathcal{A} \rangle}$.
4. If $\Psi; \cdot; \cdot \vdash \mathbf{v} : \boldsymbol{\tau}^{\langle \mathcal{A} \rangle}$ and ${}^{\tau}\mathbf{CA}(\mathbf{v}, M) = (\mathbf{v}, M')$, then $\Psi'; \cdot; \cdot \vdash \mathbf{v} : \boldsymbol{\tau}$.

Proof

By induction on the type derivations and inspection of the translations. □

8.3 Operations on Worlds

Lemma 8.6 (World Extension is Reflexive and Transitive)
For any $W, W', W'' \in \text{World}$, we have

1. $W \sqsupseteq W$
2. $W \sqsupseteq_{\text{pub}} W$
3. if $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$, then $W'' \sqsupseteq W$
4. if $W'' \sqsupseteq_{\text{pub}} W'$ and $W' \sqsupseteq_{\text{pub}} W$, then $W'' \sqsupseteq_{\text{pub}} W$.

Proof

By definition of $\sqsupseteq$ and $\sqsupseteq_{\text{pub}}$ for worlds and islands, and by the reflexivity and transitivity of the transition relations in the definition of well-formed islands. □

Lemma 8.7 (Properties of $\boxplus$)
Let $W \in \text{World}$.

1. If $(M_1, M_2) : W$ and $W \boxplus (M_1', M_2')$ is defined, then $(M_1 \uplus M_1', M_2 \uplus M_2') : W \boxplus (M_1', M_2')$.
2. $(W \boxplus (M_1, M_2)) \boxplus (M_1', M_2') = W \boxplus (M_1 \uplus M_1', M_2 \uplus M_2')$.
3. If $W' \sqsupseteq W \boxplus (M_1, M_2)$, then there is some $\widetilde{W}$ such that $W' = \widetilde{W} \boxplus (M_1, M_2)$.

Proof

By definition of $W(i_{\text{box}})$. □

Lemma 8.8 (Properties of $\triangleright$)
For any $W \in \text{World}$, we have

1. $\triangleright W \sqsupseteq W$
2. $\triangleright W \sqsupseteq_{\text{pub}} W$
3. If $(M_1, M_2) : W$, then $(M_1, M_2) : \triangleright W$.

Proof

1. By definition of $\triangleright$ and $\sqsupseteq$, it suffices to show that $\lfloor \theta \rfloor_{W.k-1} \sqsupseteq \lfloor \theta \rfloor_{W.k-1}$ for each island $\theta \in W.\Theta$. But this relation is reflexive, so we are done.
2. Similar.
3. Note that if $W.k = 0$, there is nothing to show. Otherwise, the claim follows from the definitions of MemRel and $\lfloor \varphi_M \rfloor_k$.

□

8.4 Basic Properties of Value and Component Relations

Lemma 8.9 (Related Values are Related Components)
If $(W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$, then $(W, v_1, v_2) \in \mathcal{E}[\![\tau]\!]\rho$.

Proof

Let $(W, E_1, E_2) \in \mathcal{K}[\![\tau]\!]\rho$. We need to show that $(W, E_1[v_1], E_2[v_2]) \in \mathcal{O}$. But instantiating $\mathcal{K}[\![\tau]\!]\rho$ with our hypotheses gives the result immediately. □

Lemma 8.10 (Monotonicity)
Let $\rho \in \mathcal{D}[\![\Delta]\!]$, where $\Delta \vdash \boldsymbol{\tau}$, $\Delta \vdash \psi$, $\Delta \vdash \boldsymbol{\tau}$, and $\Delta \vdash \tau$. If $W' \sqsupseteq W$, then

1. $(W, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho \implies (W', \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$
2. $(W, \mathsf{h_1}, \mathsf{h_2}) \in \mathcal{HV}[\![\psi]\!]\rho \implies (W', \mathsf{h_1}, \mathsf{h_2}) \in \mathcal{HV}[\![\tau]\!]\rho$
3. $(W, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho \implies (W', \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho$
4. $(W, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho \implies (W', \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$

Proof

The proofs, like the claims, are presented working up from the target language. This is because the case for lump types in each language depends on the property holding in the next language down. However, it may be easiest to read the proof starting from the source language. Many other proofs will also be structured in this way.

1. Proved by induction on $W'.k$ and on the structure of τ, simultaneously with Claim 2.
   In each case, we will need to show $(W', \mathsf{v_1}, \mathsf{v_2}) \in \mathrm{ValAtom}[\tau]\rho$. This amounts to showing that $W'.\Psi_i; \cdot; \cdot \vdash \mathsf{v_i} : \tau$ for $i \in \{1, 2\}$. We have by assumption that $W.\Psi_i; \cdot; \cdot \vdash \mathsf{v_i} : \tau$. By definition of world extension, $W'.\Psi_i \supseteq W.\Psi_i$, so this property holds.
   To complete the proof, consider the possible cases of τ:
   Case α By definition of ValRel.
   Case unit Immediate.
   Case int Immediate.
   Case $\exists\alpha.\tau'$ Follows from the induction hypothesis for the type.
   Case $\mu\alpha.\tau'$ Follows from the induction hypothesis for the step index.
   Case $\mathsf{ref}\ \psi'$ By transitivity of world extension.
   Case $\mathsf{box}\ \langle\tau_1, \ldots, \tau_n\rangle$ We need to show that $(W', \ell_1, \ell_2) \in \mathcal{V}[\![\mathsf{box}\ \langle\tau_1, \ldots, \tau_n\rangle]\!]\rho$.
   Let $(\widetilde{W}, M_1', M_2') \in \mathrm{currentMR}(W'(i_{\mathrm{box}}))$. By definition of $\mathrm{island}_{\mathrm{box}}$, $M_1' = W'(i_{\mathrm{box}}).s.M_1$ and $M_2' = W'(i_{\mathrm{box}}).s.M_2$. We need to show that
   $$(\widetilde{W}, M_1'(\ell_1), M_2'(\ell_2)) \in \mathcal{HV}[\![\langle\tau_1, \ldots, \tau_n\rangle]\!]\rho.$$
   By assumption, it suffices to find M_1 and M_2 such that $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W'(i_{\mathrm{box}}))$, $M_1(\ell_1) = M_1'(\ell_1)$, and $M_2(\ell_2) = M_2'(\ell_2)$.
   We choose $M_1 = W(i_{\mathrm{box}}).s.M_1$ and $M_2 = W(i_{\mathrm{box}}).s.M_2$. The first condition holds immediately by definition of $\mathrm{island}_{\mathrm{box}}$. Since $W' \sqsupseteq W$, we know that $M_1 \subseteq M_1'$ and $M_2 \subseteq M_2'$. Since $(W, \ell_1, \ell_2) \in \mathrm{TermAtom}[\mathsf{box}\ \langle\tau_1, \ldots, \tau_n\rangle]\rho$, ℓ_1 and ℓ_2 must be in the domain of H_1 and H_2, so we have the desired property.
   Case $\mathsf{box}\,\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ Let $(\widetilde{W}, M_1', M_2') \in \mathrm{currentMR}(W'(i_{\mathrm{box}}))$. It suffices to find some M_1 and M_2 such that $(\widetilde{W}, M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$, $M_1(\ell_1) = M_1'(\ell_1)$, and $M_2(\ell_2) = M_2'(\ell_2)$. This can be done exactly as in the previous case.
   Case $\lceil\alpha\rceil$ By definition of ValRel.
   Case $\lceil\boldsymbol{\alpha}\rceil$ By definition of ValRel.
2. Proved simultaneously with Claim 1.
   In both cases, we need to show that $(W', \mathsf{h_1}, \mathsf{h_2}) \in \mathrm{HvalAtom}[\psi]\rho$. This amounts to showing that $W'.\Psi_i \vdash \mathsf{h_i} : \psi$ for $i \in \{1, 2\}$. We have by assumption that $W.\Psi_i \vdash \mathsf{h_i} : \psi$. By definition of world extension, $W'.\Psi_i \supseteq W.\Psi_i$, so this property holds.
   Consider the possible cases of ψ:
   Case $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ By transitivity of world extension.
   Case $\langle\tau_1, \ldots, \tau_n\rangle$ Follows from Claim 1 using the induction hypothesis for the type.
3. By induction on $W'.k$ and on the structure of $\boldsymbol{\tau}$.
   In each case, we will need to show $(W', \mathsf{v_1}, \mathsf{v_2}) \in \mathrm{ValAtom}[\boldsymbol{\tau}]\rho$. This holds by an analogous argument to Claim 1. To complete the proof, we consider the possible cases of $\boldsymbol{\tau}$:

Case $\boldsymbol{\alpha}$ By definition of ValRel.

Case $\mathbf{unit}$ Immediate.

Case $\mathbf{int}$ Immediate.

Case $\boldsymbol{\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}$ Follows by transitivity of world extension.

Case $\boldsymbol{\exists \alpha.\tau'}$ Follows from the induction hypothesis for the type.

Case $\boldsymbol{\mu \alpha.\tau'}$ Follows from the induction hypothesis for the step index.

Case $\boldsymbol{\langle \tau_1, \ldots, \tau_n \rangle}$ Follows from the induction hypotheses for the type.

Case $\lceil \alpha \rceil$ By definition of ValRel.

Case $\mathbf{L}\langle \tau \rangle$ Follows from Claim 1.

4. By induction on $W'.k$ and on the structure of τ. We will need to show $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathrm{ValAtom}[\tau]\rho$. This holds by analogously to Claim 1. To complete the proof, we consider the possible cases of τ:

   Case α By definition of ValRel.

   Case unit Immediate.

   Case int Immediate.

   Case $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ By transitivity of world extension.

   Case $\exists \alpha.\tau'$ Follows from the induction hypothsis for the type.

   Case $\mu \alpha.\tau'$ Follows from the induction hypothesis for the step index.

   Case $\langle \tau_1, \ldots, \tau_n \rangle$ Follows from the induction hypotheses for the type.

   Case $\mathsf{L}\langle \tau \rangle$ Follows from Claim 3.

□

8.5 Reduction Lemmas

Lemma 8.11 ($\mathcal{O}$ Closed under Anti-Reduction)
Given $W' \sqsupseteq W$, if $W.k \leq W'.k + k_1$, $W.k \leq W'.k + k_2$, and

$$\forall (M_1, M_2) : W.\ \exists (M_1', M_2') : W'.\ \langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle \ \wedge\ \langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle,$$

then

$$(W', e_1', e_2') \in \mathcal{O} \implies (W, e_1, e_2) \in \mathcal{O}.$$

Proof

Let $(M_1, M_2) : W$. Then, by our assumption, $\langle M_1 \mid e_1 \rangle \longmapsto^{k_1} \langle M_1' \mid e_1' \rangle$ and $\langle M_2 \mid e_2 \rangle \longmapsto^{k_2} \langle M_2' \mid e_2' \rangle$ for some $(M_1', M_2') : W'$. Since $(W', e_1', e_2') \in \mathcal{O}$, we have either that $\langle M_1' \mid e_1' \rangle \downarrow$ and $\langle M_2' \mid e_2' \rangle \downarrow$ or that running$(W'.k, \langle M_1' \mid e_1' \rangle)$ and running$(W'.k, \langle M_2' \mid e_2' \rangle)$.

In the former case, we have $\langle M_1 \mid e_1 \rangle \downarrow$ and $\langle M_2 \mid e_2 \rangle \downarrow$ by assumption. In the latter case, we have running$(W'.k + k_1, \langle M_1 \mid e_1 \rangle)$ and running$(W'.k + k_2, \langle M_2 \mid e_2 \rangle)$. Since we have as assumptions that both of these are more steps than needed, we have the result. □

Lemma 8.12 ($\mathcal{O}$ Closed under Generalized Anti-Reduction)
If $(M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$ and $\langle M_2 \mid e \rangle \longmapsto \langle M_2 \mid e' \rangle$, then

$$(W, e_1, e_2[e'/x]) \in \mathcal{O} \implies (W, e_1, e_2[e/x]) \in \mathcal{O}.$$

Proof

Let $(W, e_1, e_2[e'/x]) \in \mathcal{O}$ and let $(M_1', M_2') : W$. We have either that $\langle M_1' \mid e_1 \rangle \downarrow$ and $\langle M_2' \mid e_2[e'/x] \rangle \downarrow$, or that running$(W.k, \langle M_1' \mid e_1 \rangle)$ and running$(W.k, \langle M_1' \mid e_2[e'/x] \rangle)$. In the first case, it suffices to show that $\langle M_2' \mid e_2[e/x] \rangle \downarrow$. In the second case, it suffices to show that running$(W.k, \langle M_1' \mid e_2[e/x] \rangle)$. These can both be proven by induction on the structure of e_2. □

Lemma 8.13 ($\mathcal{O}$ Closed under Loading Heap Values)
If $(W, e_1, E[(\mathbf{t}, \mathbf{H})]) \in \mathcal{O}$, then $(W \boxplus (\{\cdot\}, \mathbf{H}), e_1, E[\mathbf{t}]) \in \mathcal{O}$.

Proof

Similar to the proof of Lemma 8.11. Note that if $(M_1, M_2) : W$, $\langle M_2 \mid E[(\mathbf{t}, \mathbf{H})]\rangle \longmapsto^0 \langle M_2, \mathbf{H} \mid E[\mathbf{t}]\rangle$. □

Lemma 8.14 ($\mathcal{E}[\![\tau]\!]\rho$ Closed under Type-Preserving Anti-Reduction)
Let $(W, e_1, e_2) \in \mathrm{TermAtom}[\tau]\rho$. Given $W' \sqsupseteq W$, if $W.k \leq W'.k + k_1$, $W.k \leq W'.k + k_2$, and

$$\forall (M_1, M_2) : W.\ \exists (M_1', M_2') : W'.\ \langle M_1 \mid e_1\rangle \longmapsto^* \langle M_1' \mid e_1'\rangle \ \wedge\ \langle M_2 \mid e_2\rangle \longmapsto^* \langle M_2' \mid e_2'\rangle,$$

then

$$(W', e_1', e_2') \in \mathcal{E}[\![\tau]\!]\rho \implies (W, e_1, e_1) \in \mathcal{E}[\![\tau]\!]\rho.$$

Proof

Let $(W, E_1, E_2) \in \mathcal{K}[\![\tau]\!]\rho$. We need to show that $(W, E_1[e_1], E_2[e_2]) \in \mathcal{O}$. By our assumption, $(W', E_1[e_1'], E_2[e_2']) \in \mathcal{O}$. By inspection of the operational semantics and by assumption, for any $(M_1, M_2) : W$, there is an $(M_1', M_2') : W'$ such that

$$\langle M_1 \mid E_1[e_1]\rangle \longmapsto^* \langle M_1' \mid E_1[e_1']\rangle \quad \text{and} \quad \langle M_2 \mid E_2[e_2]\rangle \longmapsto^* \langle M_2' \mid E_2[e_2']\rangle.$$

The result follows by Lemma 8.11. □

Lemma 8.15 ($\mathcal{E}[\![\tau]\!]\rho$ Closed under Memory-Invariant Anti-Reduction)
Let $(W, e_1, e_2) \in \mathcal{E}[\![\tau]\!]\rho$. If

$$\forall (M_1, M_2) : W.\ \langle M_1 \mid e_1\rangle \longmapsto^* \langle M_1 \mid e_1'\rangle \ \wedge\ \langle M_2 \mid e_2\rangle \longmapsto^* \langle M_2 \mid e_2'\rangle,$$

then

$$(W, e_1', e_2') \in \mathcal{E}[\![\tau]\!]\rho \implies (W, e_1, e_2) \in \mathcal{E}[\![\tau]\!]\rho.$$

Proof

Follows from Lemma 8.14 using $W' = W$, $M_1' = M_1$, and $M_2' = M_2$. □

Lemma 8.16 ($\mathcal{E}[\![\tau]\!]\rho$ Closed under Boundary Anti-Reduction)
If $(M_1, M_2) : W$ and $\langle M_2 \mid \mathcal{AC}^{\tau}\ \mathbf{v_2}\rangle \longmapsto \langle M_2 \uplus M' \mid \mathbf{v_2}\rangle$, then

$$(W \boxplus (\{\cdot\}, M'), \mathbf{e_1}, \mathbf{v_2}) \in \mathcal{E}[\![\boldsymbol{\tau}^{\langle \mathcal{A}\rangle}]\!]\rho \implies (W, \mathbf{e_1}, \mathcal{AC}^{\tau}\ \mathbf{v_2}) \in \mathcal{E}[\![\boldsymbol{\tau}^{\langle \mathcal{A}\rangle}]\!]\rho.$$

Proof

Follows from Lemma 8.14 using $W' = W \boxplus (\{\cdot\}, M')$, $M_1' = M_1$, and $M_2' = M_2 \uplus M'$. □

Lemma 8.17 ($\mathcal{E}[\![\tau]\!]\rho$ Closed under Generalized Anti-Reduction)
If $(M_1, M_2) \in \mathrm{currentMR}(W(i_{\mathrm{box}}))$, $\langle M_2 \mid e\rangle \longmapsto \langle M_2 \mid e'\rangle$, and $(W, e_1, e_2[e/x]) \in \mathrm{TermAtom}[\tau]\rho$, then

$$(W, e_1, e_2[e'/x]) \in \mathcal{E}[\![\tau]\!]\rho \implies (W, e_1, e_2[e/x]) \in \mathcal{E}[\![\tau]\!]\rho.$$

Proof

By Lemma 8.12. □

Lemma 8.18 ($\mathcal{E}[\![\tau]\!]\rho$ Closed under Loading Heap Values)
If $(W, e_1, E[(\mathbf{t}, \mathbf{H})]) \in \mathcal{E}[\![\tau]\!]\rho$, then $(W \boxplus (\{\cdot\}, \mathbf{H}), e_1, E[\mathbf{t}]) \in \mathcal{E}[\![\tau]\!]\rho$.

Proof

By Lemma 8.13. □

Lemma 8.19 (Plugging Continuations Preserves Atoms)
Let $(W, E_1, E_2) \in \mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau']\rho'$.

- If $(W, e_1, e_2) \in \mathrm{TermAtom}[\tau]\rho$, then $(W, E_1[e_1], E_2[e_2]) \in \mathrm{TermAtom}[\tau']\rho'$.
- If $(W, E_1', E_2') \in \mathrm{ContAtom}[\tau']\rho' \rightsquigarrow [\tau'']\rho''$, then $(W, E_1'[E_1], E_2'[E_2]) \in \mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau'']\rho''$.

Proof

By induction on the type derivations. □

Lemma 8.20 (Monadic Bind)
If $(W, e_1, e_2) \in \mathcal{E}[\![\tau]\!]\rho$, $(W, E_1, E_2) \in \mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau']\rho'$ and

$$\forall W' \sqsupseteq_{\mathrm{pub}} W.\ \forall v_1, v_2.\ (W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho \implies (W', E_1[v_1], E_2[v_2]) \in \mathcal{E}[\![\tau']\!]\rho',$$

then $(W, E_1[e_1], E_2[e_2]) \in \mathcal{E}[\![\tau']\!]\rho'$.

Proof

We first need to show that $(W, E_1[e_1], E_2[e_2]) \in \mathrm{TermAtom}[\tau']\rho'$. But this follows from Lemma 8.19, since $(W, e_1, e_2) \in \mathrm{TermAtom}[\tau]\rho$.

Let $(W, E_1', E_2') \in \mathcal{K}[\![\tau']\!]\rho'$. We need to show that $(W, E_1'[E_1[e_1]], E_2'[E_2[e_1]]) \in \mathcal{O}$. It suffices to show that

$$(W, E_1'[E_1], E_2'[E_2]) \in \mathcal{K}[\![\tau]\!]\rho.$$

To get this, we first need $(W, E_1'[E_1], E_2'[E_2]) \in \mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau'']\rho''$ for some τ'' and ρ'', but this follows immediately from our assumption and Lemma 8.19.

Next, let $W' \sqsupseteq_{\mathrm{pub}} W$ such that $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$. We must show that

$$(W', E_1'[E_1[v_1]], E_2'[E_2[v_2]]) \in \mathcal{O}.$$

Applying our premise, we find that $(W', E_1[v_1], E_2[v_2]) \in \mathcal{E}[\![\tau']\!]\rho'$. Instantiating this with the fact that $(W, E_1', E_2') \in \mathcal{K}[\![\tau']\!]\rho'$ gives the result. □

8.6 Identities on Abstract Type Interpretations

The weakening property established in the following few lemmas is trivial, but its proof shows the induction structure necessary to prove other identities about the value interpretation relation $\mathcal{V}[\![\tau]\!]\rho$ and the other parts of the logical relation it (mutually) depends on.

Lemma 8.21
If $\rho[\alpha \mapsto \mathrm{VR}] \in \mathcal{D}[\![\Delta, \alpha]\!]$ and $\alpha \notin \mathrm{ftv}(\tau)$, $\alpha \notin \mathrm{ftv}(\psi)$, then

1. $\mathcal{V}[\![\tau]\!]\rho = \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]$
2. $\mathcal{HV}[\![\psi]\!]\rho = \mathcal{HV}[\![\psi]\!]\rho[\alpha \mapsto \mathrm{VR}]$
3. $\mathcal{E}[\![\tau]\!]\rho = \mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]$
4. $\mathcal{K}[\![\tau]\!]\rho = \mathcal{K}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]$.

Proof

We prove all claims simultaneously, by induction on the step index and τ.

1. Consider the possible cases of τ:
   Case α Immediate, since $\alpha \neq \alpha$.
   Case unit Immediate.
   Case int Immediate.

Case $\exists\boldsymbol{\alpha}.\boldsymbol{\tau}$ Follows from the induction hypothesis for $\boldsymbol{\tau}$.

Case $\mu\boldsymbol{\alpha}.\boldsymbol{\tau}$ Follows from the induction hypothesis for the step index.

Case $\mathbf{ref}\ \psi$ Follows from claim 2.

Case $\mathbf{box}\,\langle\boldsymbol{\tau_1},\ldots,\boldsymbol{\tau_n}\rangle$ Follows from claim 2.

Case $\mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau})\to\boldsymbol{\tau'}$ Follows from claim 2.

Case $\lceil\alpha\rceil$ Immediate, since $\alpha\neq\alpha$.

Case $\lceil\boldsymbol{\alpha}\rceil$ Immediate, since $\alpha\neq\boldsymbol{\alpha}$.

2. Consider the possible cases of ψ:

   Case $\forall[\overline{\alpha}].(\overline{\tau})\to\boldsymbol{\tau'}$ Follows from the induction hypothesis for $\boldsymbol{\tau}$ and from claim 3 (also using the induction hypothesis for $\boldsymbol{\tau}$).

   Case $\langle\boldsymbol{\tau_1},\ldots,\boldsymbol{\tau_n}\rangle$ Follows from the induction hypothesis for $\boldsymbol{\tau}$.

3. Follows from claim 4.
4. Follows from claim 1.

□

Lemma 8.22
If $\rho[\alpha\mapsto \mathrm{VR}]\in\mathcal{D}[\![\Delta,\alpha]\!]$ and $\alpha\notin\mathrm{ftv}(\boldsymbol{\tau})$, then

1. $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho=\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\alpha\mapsto\mathrm{VR}]$
2. $\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho=\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\alpha\mapsto\mathrm{VR}]$
3. $\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho=\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\alpha\mapsto\mathrm{VR}]$.

Proof

We prove all claims simultaneously, by induction on the step index and $\boldsymbol{\tau}$.

1. Consider the possible cases of $\boldsymbol{\tau}$:

   Case $\boldsymbol{\alpha}$ Immediate, since $\alpha\neq\boldsymbol{\alpha}$.

   Case $\mathbf{unit}$ Immediate.

   Case $\mathbf{int}$ Immediate.

   Case $\forall[\overline{\alpha}].(\overline{\tau})\to\boldsymbol{\tau'}$ Follows from the induction hypothesis for $\boldsymbol{\tau}$ and from claim 2 (also using the induction hypothesis for $\boldsymbol{\tau}$).

   Case $\exists\boldsymbol{\alpha}.\boldsymbol{\tau}$ Follows from the induction hypothesis for $\boldsymbol{\tau}$.

   Case $\mu\boldsymbol{\alpha}.\boldsymbol{\tau}$ Follows from the induction hypothesis for the step index.

   Case $\langle\boldsymbol{\tau_1},\ldots,\boldsymbol{\tau_n}\rangle$ Follows from the induction hypothesis for $\boldsymbol{\tau}$.

   Case $\lceil\alpha\rceil$ Immediate, since $\alpha\neq\alpha$.

   Case $\mathbf{L}\langle\tau\rangle$ Follows from Lemma 8.21.

2. Follows from claim 3.
3. Follows from claim 1.

□

Lemma 8.23
If $\rho[\alpha\mapsto \mathrm{VR}]\in\mathcal{D}[\![\Delta,\alpha]\!]$ and $\alpha\notin\mathrm{ftv}(\tau)$, then

1. $\mathcal{V}[\![\tau]\!]\rho=\mathcal{V}[\![\tau]\!]\rho[\alpha\mapsto\mathrm{VR}]$
2. $\mathcal{E}[\![\tau]\!]\rho=\mathcal{E}[\![\tau]\!]\rho[\alpha\mapsto\mathrm{VR}]$
3. $\mathcal{K}[\![\tau]\!]\rho=\mathcal{K}[\![\tau]\!]\rho[\alpha\mapsto\mathrm{VR}]$.

Proof

We prove all claims simultaneously, by induction on the step index and τ.

1. Consider the possible cases of τ:
   - **Case** α Immediate, since $\alpha \neq \alpha$.
   - **Case** unit Immediate.
   - **Case** int Immediate.
   - **Case** $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ Follows from the induction hypothesis for τ and from claim 2 (also using the induction hypothesis for τ).
   - **Case** $\exists\alpha.\tau$ Follows from the induction hypothesis for τ.
   - **Case** $\mu\alpha.\tau$ Follows from the induction hypothesis for the step index.
   - **Case** $\langle\tau_1, \ldots, \tau_n\rangle$ Follows from the induction hypothesis for τ.
   - **Case** $\mathsf{L}\langle\boldsymbol{\tau}\rangle$ Follows from Lemma 8.22.
2. Follows from claim 3.
3. Follows from claim 1.

□

We establish several identities that arise from the way our multi-language semantics handles abstract types. As we have seen, types from different languages can be embedded in each other, but only in particular ways: a lower-level type can only appear inside a lump type in the next higher language, and a higher-level type cannot appear in a lower-level type except for suspended type variables.

Together with the fact that $\mathsf{L}\langle\boldsymbol{\tau}\rangle^{\langle\mathcal{C}\rangle} = \boldsymbol{\tau}$ (and $\mathbf{L}\langle\tau\rangle^{\langle\mathcal{A}\rangle} = \tau$), this means that we can rewrite our interpretation of an abstract type in several interesting ways, captured by the operations defined throughout the rest of this section.

The first set of translation identities shows that, as long as we are observing at a lower-level language type, we can replace a higher-level type variable (which can appear only in a suspension) with a lower-level variable by "translating" its interpretation.

Definition 8.24

$$\mathcal{CF}(\tau_1, \tau_2, \varphi_v^F, \varphi_v^C, \varphi_v^A) \stackrel{\text{def}}{=} (\tau_1{}^{\langle\mathcal{C}\rangle}, \tau_2{}^{\langle\mathcal{C}\rangle}, \varphi_v^C, \varphi_v^A)$$
$$\mathcal{AC}(\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_v^C, \varphi_v^A) \stackrel{\text{def}}{=} (\boldsymbol{\tau_1}{}^{\langle\mathcal{A}\rangle}, \boldsymbol{\tau_2}{}^{\langle\mathcal{A}\rangle}, \varphi_v^A)$$

Lemma 8.25

1. If $\mathrm{VR} \in \mathrm{FValRel}$, then $\mathcal{CF}\mathrm{VR} \in \mathrm{CValRel}$.
2. If $\mathrm{VR} \in \mathrm{CValRel}$, then $\mathcal{AC}\mathrm{VR} \in \mathrm{AValRel}$.

Proof

Immediate, by the definitions of FValRel, CValRel, and AValRel. □

Lemma 8.26

If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\boldsymbol{\alpha} \notin \mathrm{ftv}(\boldsymbol{\tau})$, $\boldsymbol{\alpha} \notin \mathrm{ftv}(\psi)$, then

1. $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathcal{AC}\mathrm{VR}]$
2. $\mathcal{HV}[\![\psi]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{HV}[\![\psi[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathcal{AC}\mathrm{VR}]$
3. $\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{E}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathcal{AC}\mathrm{VR}]$
4. $\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{K}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathcal{AC}\mathrm{VR}]$.

Proof

The proof follows the same structure as Lemma 8.21. The only interesting case is in claim 1, when $\tau = \lceil \alpha \rceil$. In this case we have

$$\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathrm{VR}.\varphi_v^A = \mathcal{AC}\mathrm{VR}.\varphi_v^A = \mathcal{V}[\![\alpha]\!]\rho[\alpha \mapsto \mathcal{AC}\mathrm{VR}] = \mathcal{V}[\![\lceil \alpha \rceil[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{AC}\mathrm{VR}].$$

□

Lemma 8.27
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\alpha \notin \mathrm{ftv}(\tau)$, $\alpha \notin \mathrm{ftv}(\psi)$, then

1. $\mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{ACCF}\mathrm{VR}]$
2. $\mathcal{HV}[\![\psi]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{HV}[\![\psi[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{ACCF}\mathrm{VR}]$
3. $\mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{E}[\![\tau[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{ACCF}\mathrm{VR}]$
4. $\mathcal{K}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{K}[\![\tau[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{ACCF}\mathrm{VR}]$.

Proof

The proof follows the same structure as Lemma 8.21. The only interesting case is in claim 1, when $\tau = \lceil \alpha \rceil$. In this case we have

$$\begin{aligned}\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho[\alpha \mapsto \mathrm{VR}] &= \mathrm{VR}.\varphi_v^A \\ &= \mathcal{AC}\mathrm{VR}.\varphi_v^A = \mathcal{V}[\![\alpha]\!]\rho[\alpha \mapsto \mathcal{ACCF}\mathrm{VR}] = \mathcal{V}[\![\lceil \alpha \rceil[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{ACCF}\mathrm{VR}].\end{aligned}$$

□

Lemma 8.28
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\alpha \notin \mathrm{ftv}(\tau)$, then

1. $\mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{CF}\mathrm{VR}]$
2. $\mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{E}[\![\tau[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{CF}\mathrm{VR}]$
3. $\mathcal{K}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{K}[\![\tau[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{CF}\mathrm{VR}]$.

Proof

The proof follows the same structure as Lemma 8.22. The only interesting case is in claim 1, when $\tau = \lceil \alpha \rceil$. In this case we have

$$\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathrm{VR}.\varphi_v^C = \mathcal{CF}\mathrm{VR}.\varphi_v^C = \mathcal{V}[\![\alpha]\!]\rho[\alpha \mapsto \mathcal{CF}\mathrm{VR}] = \mathcal{V}[\![\lceil \alpha \rceil[\alpha/\lceil \alpha \rceil]]\!]\rho[\alpha \mapsto \mathcal{CF}\mathrm{VR}].$$

□

The second set of identities is intuitively the inverse of the first set. We can "lump" an interpretation of a lower-language type variable to replace it with a (properly suspended) higher-language type variable.

Definition 8.29

$$\begin{aligned}\mathsf{L}\langle(\tau_1, \tau_2, \varphi_v^C, \varphi_v^A)\rangle &\stackrel{\text{def}}{=} (\mathsf{L}\langle\tau_1\rangle, \mathsf{L}\langle\tau_2\rangle, \{(W, {}^{\mathsf{L}\langle\tau_1\rangle}\mathcal{FC}\,\mathbf{v_1}, {}^{\mathsf{L}\langle\tau_2\rangle}\mathcal{FC}\,\mathbf{v_2}) \mid (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C\}, \varphi_v^C, \varphi_v^A) \\ \mathbf{L}\langle(\tau_1, \tau_2, \varphi_v^A)\rangle &\stackrel{\text{def}}{=} (\mathbf{L}\langle\tau_1\rangle, \mathbf{L}\langle\tau_2\rangle, \{(W, {}^{\mathbf{L}\langle\tau_1\rangle}\mathcal{CA}\,\mathbf{v_1}, {}^{\mathbf{L}\langle\tau_2\rangle}\mathcal{CA}\,\mathbf{v_2}) \mid (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^A\}, \varphi_v^A)\end{aligned}$$

Lemma 8.30

1. If $\mathrm{VR} \in \mathrm{CValRel}$, then $\mathsf{L}\langle\mathrm{VR}\rangle \in \mathrm{FValRel}$.
2. If $\mathrm{VR} \in \mathrm{AValRel}$, then $\mathbf{L}\langle\mathrm{VR}\rangle \in \mathrm{CValRel}$.

Proof

1. Let $\mathrm{VR} = (\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_v^C, \varphi_v^A)$. After applying the hypothesis, we need to show:
   - $\varphi_v^F = \{(W, {}^{\mathsf{L}\langle\boldsymbol{\tau_1}\rangle}\mathcal{FC}\ \mathbf{v_1}, {}^{\mathsf{L}\langle\boldsymbol{\tau_2}\rangle}\mathcal{FC}\ \mathbf{v_2}) \mid (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C\} \in \mathrm{ValRel}[\mathsf{L}\langle\boldsymbol{\tau_1}\rangle, \mathsf{L}\langle\boldsymbol{\tau_2}\rangle]$,
   - $\varphi_v^C \in \mathrm{TransRel}^{\mathcal{C}}[\mathsf{L}\langle\boldsymbol{\tau_1}\rangle, \mathsf{L}\langle\boldsymbol{\tau_2}\rangle]$,
   - $\mathcal{CF}(\mathsf{L}\langle\boldsymbol{\tau_1}\rangle, \mathsf{L}\langle\boldsymbol{\tau_2}\rangle, \varphi_v^F) \subseteq \varphi_v^C$,
   - $\mathcal{FC}(\mathsf{L}\langle\boldsymbol{\tau_1}\rangle, \mathsf{L}\langle\boldsymbol{\tau_2}\rangle, \varphi_v^C) \subseteq \varphi_v^F$.

   All of these follow easily from the definition of $\mathsf{L}\langle\mathrm{VR}\rangle$.
2. Analagous to claim (1).

□

Lemma 8.31
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\boldsymbol{\alpha} \notin \mathrm{ftv}(\boldsymbol{\tau})$, $\boldsymbol{\alpha} \notin \mathrm{ftv}(\boldsymbol{\psi})$, then

1. $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle] = \mathcal{V}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]$
2. $\mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle] = \mathcal{HV}[\![\boldsymbol{\psi}[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]$
3. $\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle] = \mathcal{E}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]$
4. $\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle] = \mathcal{K}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]$.

Proof

The proof follows the same structure as the proof of Lemma 8.21. The only interesting case is in claim 1, when $\boldsymbol{\tau} = \lceil\boldsymbol{\alpha}\rceil$. In this case we have

$$\mathcal{V}[\![\lceil\boldsymbol{\alpha}\rceil]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle] = \mathbf{L}\langle\mathrm{VR}\rangle.\varphi_v^A = \mathrm{VR}.\varphi_v^A = \mathcal{V}[\![\boldsymbol{\alpha}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\lceil\boldsymbol{\alpha}\rceil[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}].$$

□

Lemma 8.32
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\boldsymbol{\alpha} \notin \mathrm{ftv}(\boldsymbol{\tau})$, $\boldsymbol{\alpha} \notin \mathrm{ftv}(\boldsymbol{\psi})$, then

1. $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathbf{L}\langle\mathrm{VR}\rangle\rangle] = \mathcal{V}[\![\boldsymbol{\tau}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}]$
2. $\mathcal{HV}[\![\boldsymbol{\psi}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathbf{L}\langle\mathrm{VR}\rangle\rangle] = \mathcal{HV}[\![\boldsymbol{\psi}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}]$
3. $\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathbf{L}\langle\mathrm{VR}\rangle\rangle] = \mathcal{E}[\![\boldsymbol{\tau}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}]$
4. $\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathbf{L}\langle\mathrm{VR}\rangle\rangle] = \mathcal{K}[\![\boldsymbol{\tau}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}]$.

Proof

The proof follows the same structure as the proof of Lemma 8.21. The only interesting case is in claim 1, when $\boldsymbol{\tau} = \lceil\alpha\rceil$. In this case we have

$$\begin{aligned}\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathbf{L}\langle\mathrm{VR}\rangle\rangle] &= \mathsf{L}\langle\mathbf{L}\langle\mathrm{VR}\rangle\rangle.\varphi_v^A \\ &= \mathrm{VR}.\varphi_v^A = \mathcal{V}[\![\boldsymbol{\alpha}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\lceil\boldsymbol{\alpha}\rceil[\boldsymbol{\alpha}/\lceil\boldsymbol{\alpha}\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}].\end{aligned}$$

□

Lemma 8.33
If $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\boldsymbol{\alpha} \notin \mathrm{ftv}(\boldsymbol{\tau})$, then

1. $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}\rangle] = \mathcal{V}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\alpha\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]$
2. $\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}\rangle] = \mathcal{E}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\alpha\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]$
3. $\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}\rangle] = \mathcal{K}[\![\boldsymbol{\tau}[\boldsymbol{\alpha}/\lceil\alpha\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}]$.

Proof

The proof follows the same structure as the proof of Lemma 8.22. The only interesting case is in claim 1, when $\boldsymbol{\tau} = \lceil \alpha \rceil$. In this case we have

$$\mathcal{V}[\![\lceil \alpha \rceil]\!]\rho[\alpha \mapsto \mathsf{L}\langle \mathrm{VR} \rangle] = \mathsf{L}\langle \mathrm{VR} \rangle.\varphi_v^C = \mathrm{VR}.\varphi_v^C = \mathcal{V}[\![\boldsymbol{\alpha}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\lceil \alpha \rceil[\boldsymbol{\alpha}/\lceil \alpha \rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}].$$

□

Finally, this set of identities deals with a property of the lump type exploited by the value translations in our multi-language framework, which we need to reason about in order to prove boundary cancellation.

Since the translation of e.g. $\mathsf{L}\langle \tau^{\langle \mathcal{C} \rangle} \rangle$ is the same as the translation of τ, we can transform the interpretation of an abstract type between these two instantiations. Intuitively, thanks to parametricity, nothing can be done with an abstract value except to return it from the term that was required to keep it abstract, and similarly, there are no operations on a lump except to send it over the boundary. If the return from an abstract view requires passing through a boundary, a lump of the translation of a value is indistinguishable from the original value. Thus, an interpretation VR of a type variable is equivalent to this transformation of it (opaqueR(VR)), as long as we are viewing it from a lower-level language, where we have to perform a translation to get to the underlying values.

Definition 8.34

$$\begin{aligned}
\mathrm{opaqueR}(\tau_1, \tau_2, \varphi_v^F, \varphi_v^C, \varphi_v^A) &\stackrel{\mathrm{def}}{=} (\tau_1, \mathsf{L}\langle (\tau_2^{\langle \mathcal{C} \rangle}) \rangle, \hat{\varphi}_v^F, \varphi_v^C, \varphi_v^A) \\
&\quad \text{where } \hat{\varphi}_v^F = \{(W, \mathsf{v}_1, {}^{\mathsf{L}\langle (\tau_2^{\langle \mathcal{C} \rangle}) \rangle}\mathcal{FC}\,\mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathsf{v}_1, \mathsf{v}_2) \in \varphi_v^F \ \wedge \\
&\qquad\qquad \mathbf{CF}^{\tau_2}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2)\} \\
&\qquad \cup \{(W, \mathsf{v}_1, {}^{\mathsf{L}\langle (\tau_2^{\langle \mathcal{C} \rangle}) \rangle}\mathcal{FC}\,\mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C \ \wedge \\
&\qquad\qquad {}^{\tau_1}\mathbf{FC}(\mathbf{v_1}, M_1) = (\mathsf{v}_1, M_1)\} \\
\mathrm{opaqueR}(\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_v^C, \varphi_v^A) &\stackrel{\mathrm{def}}{=} (\boldsymbol{\tau_1}, \mathbf{L}\langle (\boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle}) \rangle, \hat{\varphi}_v^C, \varphi_v^A) \\
&\quad \text{where } \hat{\varphi}_v^C = \{(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, {}^{\mathbf{L}\langle (\tau_2^{\langle \mathcal{A} \rangle}) \rangle}\mathcal{CA}\,\mathsf{v}_2) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathsf{v}_2) \in \varphi_v^A \ \wedge \\
&\qquad\qquad \mathbf{AC}^{\tau_2}(\mathsf{v}_2, M_2) = (\mathsf{v}_2, M_2 \uplus M')\} \\
&\qquad \cup \{(W, \mathbf{v_1}, {}^{\mathbf{L}\langle (\tau_2^{\langle \mathcal{A} \rangle}) \rangle}\mathcal{CA}\,\mathsf{v}_2) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathsf{v}_2) \in \varphi_v^A \ \wedge \\
&\qquad\qquad {}^{\tau_1}\mathbf{CA}(\mathbf{v_1}, M_1) = (\mathbf{v_1}, M_1)\}
\end{aligned}$$

Lemma 8.35

1. If VR ∈ FValRel, then opaqueR(VR) ∈ FValRel.
2. If VR ∈ CValRel, then opaqueR(VR) ∈ CValRel.

Proof

1. Let $\mathrm{VR} = (\tau_1, \tau_2, \varphi_v^F, \varphi_v^C, \varphi_v^A)$,

   $$\hat{\varphi}_v^F{}_1 = \{(W, \mathsf{v}_1, {}^{\mathsf{L}\langle (\tau_2^{\langle \mathcal{C} \rangle}) \rangle}\mathcal{FC}\,\mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathsf{v}_1, \mathsf{v}_2) \in \varphi_v^F \ \wedge\ \mathbf{CF}^{\tau_2}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2)\},$$

   and

   $$\hat{\varphi}_v^F{}_2 = \{(W, \mathsf{v}_1, {}^{\mathsf{L}\langle (\tau_2^{\langle \mathcal{C} \rangle}) \rangle}\mathcal{FC}\,\mathbf{v_2}) \mid (M_1, M_2) : W \ \wedge\ (W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C \ \wedge\ {}^{\tau_1}\mathbf{FC}(\mathbf{v_1}, M_1) = (\mathsf{v}_1, M_1)\}.$$

   After applying the hypothesis, we need to show:
   - $(\hat{\varphi}_v^F{}_1 \cup \hat{\varphi}_v^F{}_2) \in \mathrm{ValRel}[\tau_1, \mathsf{L}\langle \tau_2^{\langle \mathcal{C} \rangle} \rangle]$,
   - $\varphi_v^C \in \mathrm{TransRel}^{\mathcal{C}}[\tau_1, \mathsf{L}\langle \tau_2^{\langle \mathcal{C} \rangle} \rangle]$,
   - $\mathcal{CF}(\tau_1, \mathsf{L}\langle \tau_2^{\langle \mathcal{C} \rangle} \rangle, (\hat{\varphi}_v^F{}_1 \cup \hat{\varphi}_v^F{}_2)) \subseteq \varphi_v^C$, and
   - $\mathcal{FC}(\tau_1, \mathsf{L}\langle \tau_2^{\langle \mathcal{C} \rangle} \rangle, \varphi_v^C) \subseteq (\hat{\varphi}_v^F{}_1 \cup \hat{\varphi}_v^F{}_2)$.

The first two requirements are boundary cancellation properties. On the left, they follow from the boundary cancellation properties given by $\varphi_v^F \in \mathrm{ValRel}[\tau_1, \tau_2]$ and $\varphi_v^C \in \mathrm{TransRel}^{\mathcal{C}}[\tau_1, \tau_2]$. On the right, they follow directly from the translation rules for lump types.

The latter two requirements are bridge properties. We can break them down to the following:

- $\mathcal{CF}(\tau_1, \mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle, \hat{\varphi}_v^F{}_1) \subseteq \varphi_v^C$,
- $\mathcal{CF}(\tau_1, \mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle, \hat{\varphi}_v^F{}_2) \subseteq \varphi_v^C$, and
- $\mathcal{FC}(\tau_1, \mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle, \varphi_v^C) \subseteq \hat{\varphi}_v^F{}_2$.

These follow easily from the definitions of $\hat{\varphi}_v^F{}_1$ and $\hat{\varphi}_v^F{}_2$ and from the boundary cancellation property given in $\varphi_v^C \in \mathrm{TransRel}^{\mathcal{C}}[\tau_1, \tau_2]$.

2. Analogous to claim (1).

□

Lemma 8.36
Let $\mathrm{VR} \in \mathrm{ValRel}[\tau_1, \tau_2]$ and $\mathrm{VR}' = \mathrm{opaqueR}(\mathrm{VR})$. Let $\varphi_v^F = \mathrm{VR}.\varphi_v^F$ and $\hat{\varphi}_v^F = \mathrm{VR}'.\varphi_v^F$.

1. If $(W, \mathsf{v}_1, \mathsf{v}_2) \in \varphi_v^F$, $(M_1, M_2) : W$, and $\mathbf{CF}^{\tau_2}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2)$, then $(W, \mathsf{v}_1, {}^{\mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle}\mathcal{FC}\,\mathbf{v_2}) \in \hat{\varphi}_v^F$.
2. If $(W, \mathsf{v}_1, {}^{\mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle}\mathcal{FC}\,\mathbf{v_2}) \in \hat{\varphi}_v^F$, $(M_1, M_2) : W$, and ${}^{\tau_2}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathsf{v}_2, M_2)$, then $(W, \mathsf{v}_1, \mathsf{v}_2) \in \varphi_v^F$.

Proof

1. Immediate from the first part of the definition of $\hat{\varphi}_v^F$.
2. By boundary cancellation on φ_v^F and the bridge property from $\mathrm{VR}.\varphi_v^C$ to φ_v^F.

□

Lemma 8.37
Let $\mathrm{VR} \in \mathrm{ValRel}[\boldsymbol{\tau_1}, \boldsymbol{\tau_2}]$ and $\mathrm{VR}' = \mathrm{opaqueR}(\mathrm{VR})$. Let $\varphi_v^C = \mathrm{VR}.\varphi_v^C$ and $\hat{\varphi}_v^C = \mathrm{VR}'.\varphi_v^C$.

1. If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C$, $(M_1, M_2) : W$, and $\mathbf{AC}^{\tau_2}(\mathbf{v_2}, M_2) = (\mathsf{v}_2, M_2 \uplus M')$, then
$$(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, {}^{\mathbf{L}\langle\tau_2{}^{\langle\mathcal{A}\rangle}\rangle}\mathcal{CA}\,\mathsf{v}_2) \in \hat{\varphi}_v^C.$$
2. If $(W, \mathbf{v_1}, {}^{\mathbf{L}\langle\tau_2{}^{\langle\mathcal{A}\rangle}\rangle}\mathcal{CA}\,\mathsf{v}_2) \in \hat{\varphi}_v^C$, $(M_1, M_2) : W$, and ${}^{\tau_2}\mathbf{CA}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2)$, then $(W, \mathbf{v_1}, \mathbf{v_2}) \in \varphi_v^C$.

Proof

1. Immediate from the first part of the definition of $\hat{\varphi}_v^C$.
2. By boundary cancellation on φ_v^C and the bridge property from $\mathrm{VR}.\varphi_v^A$ to φ_v^C.

□

Lemma 8.38

1. $\mathcal{V}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{opaqueR}(\mathrm{VR})]$
2. $\mathcal{HV}[\![\psi]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{HV}[\![\psi]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{opaqueR}(\mathrm{VR})]$
3. $\mathcal{E}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{E}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{opaqueR}(\mathrm{VR})]$
4. $\mathcal{K}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{K}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{opaqueR}(\mathrm{VR})]$.

Proof

Follows the structure of Lemma 8.21. The only interesting case is in claim (1) with $\tau = \lceil\boldsymbol{\alpha}\rceil$, where
$$\mathcal{V}[\![\lceil\boldsymbol{\alpha}\rceil]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathrm{VR}.\varphi_v^A = \mathrm{opaqueR}(\mathrm{VR}).\varphi_v^A = \mathcal{V}[\![\lceil\boldsymbol{\alpha}\rceil]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{opaqueR}(\mathrm{VR})]$$
by definition. □

Lemma 8.39

1. $\mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$
2. $\mathcal{HV}[\![\psi]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{HV}[\![\psi]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$
3. $\mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$
4. $\mathcal{K}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{K}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$.

Proof

Follows the structure of Lemma 8.21. The only interesting case is in claim (1) with $\tau = \lceil\alpha\rceil$, where

$$\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathrm{VR}.\varphi_v^A = \mathrm{opaqueR(VR)}.\varphi_v^A = \mathcal{V}[\![\lceil\alpha\rceil]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$$

by definition. □

Lemma 8.40

1. $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$
2. $\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$
3. $\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$.

Proof

Follows the structure of Lemma 8.22. The only interesting case is in claim (1) with $\boldsymbol{\tau} = \lceil\alpha\rceil$, where

$$\mathcal{V}[\![\lceil\alpha\rceil]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathrm{VR}.\varphi_v^C = \mathrm{opaqueR(VR)}.\varphi_v^C = \mathcal{V}[\![\lceil\alpha\rceil]\!]\rho[\alpha \mapsto \mathrm{opaqueR(VR)}]$$

by definition. □

9 Proofs: Boundary Cancellation

Lemma 9.1
Given W, τ, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\beta}]\!]$ such that $\rho = \rho_0[\overline{\beta \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\beta \mapsto \mathrm{VR}'}]$, where for each VR_i, VR'_i, either $\mathrm{VR}_i = \mathrm{opaqueR}(\mathrm{VR}'_i)$ or $\mathrm{opaqueR}(\mathrm{VR}_i) = \mathrm{VR}'_i$. Also let $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathrm{ValAtom}[\tau]\rho$, $(M_1, M_2) : W$, and ${}^{\rho'_2(\tau)}\mathbf{FC}(\mathbf{CF}^{\rho_2(\tau)}(\mathsf{v}_2, M_2)) = (\mathsf{v}'_2, M_2)$. Then $(W, \mathsf{v}_1, \mathsf{v}'_2) \in \mathrm{ValAtom}[\tau]\rho'$.

Proof

We need to show that $(W, \mathsf{v}_1, \mathsf{v}'_2) \in \mathrm{TermAtom}[\tau]\rho'$. From $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathrm{ValAtom}[\tau]\rho$, we know that $W \in \mathrm{World}$, $W.\Psi_1; \cdot; \cdot \vdash \mathsf{v}_1 : \rho_1(\tau)$, and $W.\Psi_2; \cdot; \cdot \vdash \mathsf{v}_2 : \rho_2(\tau)$. By definition of opaqueR, $\rho'_1 = \rho_1$, so it suffices to show that $W.\Psi_2; \cdot; \cdot \vdash \mathsf{v}'_2 : \rho'_2(\tau)$. But now we need only use our hypothesis that ${}^{\rho'_2(\tau)}\mathbf{FC}(\mathbf{CF}^{\rho_2(\tau)}(\mathsf{v}_2, M_2)) = (\mathsf{v}'_2, M_2)$ to apply Lemma 8.5 twice. □

Lemma 9.2 (FC/CF Boundary Cancellation)
Given W, τ, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\beta}]\!]$ such that $\rho = \rho_0[\overline{\beta \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\beta \mapsto \mathrm{VR}'}]$, where for each VR_i, VR'_i, either $\mathrm{VR}_i = \mathrm{opaqueR}(\mathrm{VR}'_i)$ or $\mathrm{opaqueR}(\mathrm{VR}_i) = \mathrm{VR}'_i$. Then

1. If $(W, \mathsf{e}_1, \mathsf{e}_2) \in \mathcal{E}[\![\tau]\!]\rho$, then $(W, \mathsf{e}_1, {}^{\rho'_2(\tau)}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau)}\,\mathsf{e}_2) \in \mathcal{E}[\![\tau]\!]\rho'$.
2. If $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho$, $(M_1, M_2) : W$, and ${}^{\rho'_2(\tau)}\mathbf{FC}(\mathbf{CF}^{\rho_2(\tau)}(\mathsf{v}_2, M_2)) = (\mathsf{v}'_2, M_2)$, then
$$(W, \mathsf{v}_1, \mathsf{v}'_2) \in \mathcal{V}[\![\tau]\!]\rho'.$$

Proof

We prove both claims simultaneously by induction on $W.k$ and then on the structure of τ.

For claim (1), let $W' \sqsupseteq_{\mathrm{pub}} W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho$. Note that $(W, [\cdot], {}^{\rho'_2(\tau)}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau)}\,[\cdot]) \in \mathrm{ContAtom}[\tau]\rho \rightsquigarrow [\tau]\rho'$. By Lemma 8.20, it suffices to show

$$(W', \mathsf{v}_1, {}^{\rho'_2(\tau)}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau)}\,\mathsf{v}_2) \in \mathcal{E}[\![\tau]\!]\rho'.$$

Note that $(W', \mathsf{v}_1, {}^{\rho'_2(\tau)}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau)}\,\mathsf{v}_2) \in \mathrm{TermAtom}[\tau]\rho'$.

By Lemma 8.3, for any M, there is a v'_2 such that $\langle M \mid {}^{\rho'_2(\tau)}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau)}\,\mathsf{v}_2\rangle \longmapsto^2 \langle M \mid \mathsf{v}'_2\rangle$. Thus, by Lemma 8.15, it suffices to show $(W', \mathsf{v}_1, \mathsf{v}'_2) \in \mathcal{E}[\![\tau]\!]\rho'$, and finally, by Lemma 8.9, we need only show $(W', \mathsf{v}_1, \mathsf{v}'_2) \in \mathcal{V}[\![\tau]\!]\rho'$, which we have by claim (2).

We prove claim (2) by considering the possible cases of τ:

Case α

Since $\rho \in \mathcal{D}[\![\Delta, \overline{\alpha}]\!]$, we know that $\rho(\alpha) \in \mathrm{FValRel}$. By Lemma 8.35, $\rho'(\alpha) \in \mathrm{FValRel}$ as well. Consider the three possible cases of $\rho(\alpha)$ and $\rho'(\alpha)$:

- If $\rho(\alpha) = \rho'(\alpha) = (\tau_1, \tau_2, \varphi_v^F, \varphi_v^C, \varphi_v^A)$, then the result is immediate, since $\rho(\alpha) \in \mathrm{ValRel}[\tau_1, \tau_2]$.
- If $\rho(\alpha) = (\tau_1, \tau_2, \varphi_v^F, \varphi_v^C, \varphi_v^A)$ and $\rho'(\alpha) = \mathrm{opaqueR}(\rho(\alpha)) = (\tau_1, \mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle, \hat{\varphi}_v^F, \varphi_v^C, \varphi_v^A)$, then by Lemma 8.5, $\mathsf{v}'_2 = {}^{\mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle}\mathcal{FC}\,\mathbf{v_2}$ for some $\mathbf{v_2}$ such that $\mathbf{CF}^{\tau_2}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2)$. The result follows from Lemma 8.36.
- Finally, if $\rho'(\alpha) = (\tau_1, \tau_2, \varphi_v^F, \varphi_v^C, \varphi_v^A)$ and
$$\rho(\alpha) = \mathrm{opaqueR}(\rho'(\alpha)) = (\tau_1, \mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle, \hat{\varphi}_v^F, \varphi_v^C, \varphi_v^A),$$
then there exists some $\mathbf{v_2}$ such that $\mathsf{v}_2 = {}^{\mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle}\mathcal{FC}\,\mathbf{v_2}$, and ${}^{\tau_2}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathsf{v}'_2, M_2)$. The result follows from Lemma 8.36.

Case unit

By inspection of the translation, $\mathsf{v}'_2 = \mathsf{v}_2 = ()$, so we are done.

Case int

By inspection of the translation, $\mathsf{v}'_2 = \mathsf{v}_2 = \mathsf{n}$, so we are done.

Case $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$

By Lemma 9.1, we know that $(W, \mathsf{v}_1, \mathsf{v}_2') \in \mathrm{ValAtom}[\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\rho'$.

Let $W' \sqsupseteq W$, $\overline{\mathrm{VR} \in \mathrm{FValRel}}$ and $\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho'[\alpha \mapsto \mathrm{VR}]}$. We need to show that

$$(W', \mathsf{v}_1\ [\overline{\mathrm{VR}.\tau_1}]\ \overline{\hat{\mathsf{v}}_1}, \mathsf{v}_2'\ [\overline{\mathrm{VR}.\tau_2}]\ \overline{\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho'[\overline{\alpha \mapsto \mathrm{VR}}].$$

For convenience, let $\overline{\tau_1 = \mathrm{VR}.\tau_1}$, $\overline{\tau_2 = \mathrm{VR}.\tau_2}$, $\hat{\rho} = \rho\overline{[\alpha \mapsto \mathrm{opaqueR}(\mathrm{VR})]}$, and $\hat{\rho}' = \rho'\overline{[\alpha \mapsto \mathrm{VR}]}$. Thus we can restate our assumptions as $\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\hat{\rho}'}$, and we can restate our proof obligation as $(W', \mathsf{v}_1\ [\overline{\tau_1}]\ \overline{\hat{\mathsf{v}}_1}, \mathsf{v}_2'\ [\overline{\tau_2}]\ \overline{\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\hat{\rho}'$.

By Lemma 8.3, there are some $\hat{\mathbf{v}}$ and $\overline{\hat{\mathsf{v}}_2'}$ such that

$$\overline{\mathbf{CF}^{\hat{\rho}_2(\tau)}(\hat{\mathsf{v}}_2, M) = (\hat{\mathbf{v}}, M)} \qquad \text{and} \qquad \overline{{}^{\hat{\rho}_2'(\tau)}\mathbf{FC}(\hat{\mathbf{v}}, M) = (\hat{\mathsf{v}}_2', M)}.$$

By the induction hypothesis,

$$\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2') \in \mathcal{V}[\![\tau]\!]\hat{\rho}}.$$

Hence, by our assumption that $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho$, we have

$$(W', \mathsf{v}_1\ [\overline{\tau_1}]\ \overline{\hat{\mathsf{v}}_1}, \mathsf{v}_2\ \overline{[\mathsf{L}\langle\tau_2\langle\mathcal{C}\rangle\rangle]}\ \overline{\hat{\mathsf{v}}_2'}) \in \mathcal{E}[\![\tau']\!]\hat{\rho}.$$

By the induction hypothesis and by claim (1),

$$(W', \mathsf{v}_1\ [\overline{\tau_1}]\ \overline{\hat{\mathsf{v}}_1}, {}^{\hat{\rho}_2'(\tau')}\mathcal{FC}\,\mathcal{C}\mathcal{F}^{\hat{\rho}_2(\tau')}\ \mathsf{v}_2\ \overline{[\mathsf{L}\langle\tau_2\langle\mathcal{C}\rangle\rangle]}\ \overline{\hat{\mathsf{v}}_2'}) \in \mathcal{E}[\![\tau']\!]\hat{\rho}'.$$

By Lemma 8.15, it suffices to show that

$$\langle M \mid \mathsf{v}_2'\ [\overline{\tau_2}]\ \overline{\hat{\mathsf{v}}_2}\rangle \longmapsto^* \langle M \mid {}^{\hat{\rho}_2'(\tau')}\mathcal{FC}\,\mathcal{C}\mathcal{F}^{\hat{\rho}_2(\tau')}\ \mathsf{v}_2\ \overline{[\mathsf{L}\langle\tau_2\langle\mathcal{C}\rangle\rangle]}\ \overline{\hat{\mathsf{v}}_2'}\rangle.$$

To show this, we derive the shape of v_2'. By definition,

$$\mathbf{CF}^{\rho_2(\forall[\overline{\alpha}].(\overline{\tau}) \to \tau')}(\mathsf{v}_2, M) = (\mathbf{pack}\langle\mathbf{unit}, \langle \mathbf{v}, ()\rangle\rangle\ \mathbf{as}\ (\rho_2(\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'))^{\langle\mathcal{C}\rangle}, M),$$

where

$$\mathbf{v} = \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\mathbf{z} : \mathbf{unit}, \overline{\mathbf{x} : \rho_2(\tau)^{\langle\mathcal{C}\rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}}).\mathcal{C}\mathcal{F}^{\rho_2(\tau')\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}}\ \mathsf{v}_2\ \overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle]}\ \overline{{}^{\rho_2(\tau)\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}}\mathcal{FC}\,\mathbf{x}}.$$

Also by definition,

$${}^{\rho_2'(\forall[\overline{\alpha}].(\overline{\tau}) \to \tau')}\mathbf{FC}(\mathbf{pack}\langle\mathbf{unit}, \langle \mathbf{v}, ()\rangle\rangle, M) = (\lambda[\overline{\alpha}]\,(\overline{\mathsf{x} : \tau}).{}^{\rho_2'(\tau')}\mathcal{FC}\,\mathbf{e}, M),$$

where

$$\mathbf{e} = \mathbf{unpack}\,\langle\boldsymbol{\beta}, \mathbf{y}\rangle = \mathbf{pack}\langle\mathbf{unit}, \langle \mathbf{v}, ()\rangle\rangle\ \mathbf{in}\ (\boldsymbol{\pi}_1(\mathbf{y}))\ \overline{[\lceil\alpha\rceil]}\ \boldsymbol{\pi}_2(\mathbf{y}), \overline{\mathcal{C}\mathcal{F}^{\rho_2'(\tau)}\,\mathsf{x}}.$$

Thus $\mathsf{v}_2' = \lambda[\overline{\alpha}]\,(\overline{\mathsf{x} : \tau}).{}^{\rho_2'(\tau')}\mathcal{FC}\,\mathbf{e}$.

By the operational semantics, we have

$$\begin{array}{lll}
\langle M \mid \mathsf{v}_2'\ [\overline{\tau_2}]\ \overline{\hat{\mathsf{v}}_2}\rangle & \longmapsto & \langle M \mid ({}^{\rho_2'(\tau')}\mathcal{FC}\,\mathbf{e})\overline{[\tau_2/\alpha][\hat{\mathsf{v}}_2/\mathsf{x}]}\rangle \\
& \longmapsto^* & \langle M \mid {}^{\hat{\rho}_2'(\tau')}\mathcal{FC}\ (\mathbf{v}\ \overline{[\tau_2\langle\mathcal{C}\rangle]}\ (), \overline{\mathcal{C}\mathcal{F}^{\hat{\rho}_2'(\tau)}\ \hat{\mathsf{v}}_2})\rangle \\
& \longmapsto^* & \langle M \mid {}^{\hat{\rho}_2'(\tau')}\mathcal{FC}\ (\mathbf{v}\ \overline{[\tau_2\langle\mathcal{C}\rangle]}\ (), \overline{\hat{\mathbf{v}}})\rangle \\
& \longmapsto & \langle M \mid {}^{\hat{\rho}_2'(\tau')}\mathcal{FC}\,\mathcal{C}\mathcal{F}^{\hat{\rho}_2(\tau')}\ \mathsf{v}_2\ \overline{[\mathsf{L}\langle\tau_2\langle\mathcal{C}\rangle\rangle]}\ \overline{{}^{\hat{\rho}_2(\tau)}\mathcal{FC}\ \hat{\mathbf{v}}}\rangle \\
& \longmapsto^* & \langle M \mid {}^{\hat{\rho}_2'(\tau')}\mathcal{FC}\,\mathcal{C}\mathcal{F}^{\hat{\rho}_2(\tau')}\ \mathsf{v}_2\ \overline{[\mathsf{L}\langle\tau_2\langle\mathcal{C}\rangle\rangle]}\ \overline{\hat{\mathsf{v}}_2'}\rangle,
\end{array}$$

as desired.

Case $\exists\alpha.\tau$

By Lemma 9.1, we know that $(W, \mathsf{v}_1, \mathsf{v}_2') \in \mathrm{ValAtom}[\exists\alpha.\tau]\rho'$.
By our hypothesis that $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\exists\alpha.\tau]\!]\rho$, we know that

$$\mathsf{v}_1 = \mathsf{pack}\langle\tau_1,\hat{\mathsf{v}}_1\rangle \,\mathsf{as}\, \rho_1(\exists\alpha.\tau), \qquad \mathsf{v}_2 = \mathsf{pack}\langle\tau_2,\hat{\mathsf{v}}_2\rangle \,\mathsf{as}\, \rho_2(\exists\alpha.\tau),$$

and that there is some $\mathrm{VR} \in \mathrm{FValRel}$ such that $\mathrm{VR}.\tau_1 = \tau_1$, $\mathrm{VR}.\tau_2 = \tau_2$, and

$$(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}].$$

By Lemma 8.3, there are some $\hat{\mathbf{v}}_2$ and $\hat{\mathsf{v}}_2'$ such that

$$\mathbf{CF}^{\rho_2(\tau)[\tau_2/\alpha]}(\hat{\mathsf{v}}_2, M) = (\hat{\mathbf{v}}, M) \qquad \text{and} \qquad {}^{\rho_2'(\tau)[\mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle/\alpha]}\mathbf{FC}(\hat{\mathbf{v}}, M) = (\hat{\mathsf{v}}_2', M).$$

By definition of the value translations, we have $\mathsf{v}_2' = \mathsf{pack}\langle\mathsf{L}\langle\tau_2^{\langle\mathcal{C}\rangle}\rangle,\hat{\mathsf{v}}_2'\rangle \,\mathsf{as}\, \rho_2'(\exists\alpha.\tau)$. To show that $(W, \mathsf{v}_1, \mathsf{v}_2') \in \mathcal{V}[\![\exists\alpha.\tau]\!]\rho'$, we need to find $\mathrm{VR}' \in \mathrm{FValRel}$ such that $\mathrm{VR}'.\tau_1 = \tau_1$, $\mathrm{VR}'.\tau_2 = \mathsf{L}\langle\tau_2{}^{\langle\mathcal{C}\rangle}\rangle$, and

$$(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2') \in \mathcal{V}[\![\tau]\!]\rho'[\alpha \mapsto \mathrm{VR}'].$$

By the induction hypothesis, $\mathrm{VR}' = \mathrm{opaqueR}(\mathrm{VR})$ does exactly this, so we are done.

Case $\mu\alpha.\tau$

By Lemma 9.1, we know that $(W, \mathsf{v}_1, \mathsf{v}_2') \in \mathrm{ValAtom}[\mu\alpha.\tau]\rho'$.
By our hypothesis that $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mu\alpha.\tau]\!]\rho$, we know that

$$\mathsf{v}_1 = \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\, \hat{\mathsf{v}}_1, \qquad \mathsf{v}_2 = \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\, \hat{\mathsf{v}}_2,$$

and that $(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$.
By Lemma 8.3, there are some $\hat{\mathbf{v}}_2$ and $\hat{\mathsf{v}}_2'$ such that

$$\mathbf{CF}^{\rho(\tau)}(\hat{\mathsf{v}}_2, M) = (\hat{\mathbf{v}}_2, M) \qquad \text{and} \qquad {}^{\rho(\tau)}\mathbf{FC}(\hat{\mathbf{v}}_2, M) = (\hat{\mathsf{v}}_2', M).$$

By the induction hypothesis,

$$(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2') \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho'.$$

It remains only to show that $\mathsf{v}_2' = \mathsf{fold}_{\rho_2'(\mu\alpha.\tau)}\, \hat{\mathsf{v}}_2'$, but this follows easily from the definition of the value translations.

Case $\langle\overline{\tau}\rangle$

By the definition of the value translations and the induction hypothesis.

Case $\mathsf{L}\langle\boldsymbol{\tau}\rangle$

By Lemma 9.1, we know that $(W, \mathsf{v}_1, \mathsf{v}_2') \in \mathrm{ValAtom}[\mathsf{L}\langle\boldsymbol{\tau}\rangle]\rho'$.
By assumption, we know that

$$\mathsf{v}_1 = {}^{\rho_1(\mathsf{L}\langle\boldsymbol{\tau}\rangle)}\mathcal{FC}\, \hat{\mathbf{v}}_1, \qquad \mathsf{v}_2 = {}^{\rho_2(\mathsf{L}\langle\boldsymbol{\tau}\rangle)}\mathcal{FC}\, \hat{\mathbf{v}}_2,$$

and $(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho$. By inspection of the value translations, we know that $\mathsf{v}_2' = {}^{\rho_2'(\mathsf{L}\langle\boldsymbol{\tau}\rangle)}\mathcal{FC}\, \hat{\mathbf{v}}_2$, so we need to show only that $(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho'$. But this follows by Lemma 8.40.

□

Lemma 9.3
Given W, τ, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\beta}]\!]$ such that $\rho = \rho_0[\overline{\beta \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\beta \mapsto \mathrm{opaqueR}(\mathrm{VR})}]$. Also let $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[\tau^{\langle\mathcal{C}\rangle}]\rho$, $(M_1, M_2) : W$, and $\mathbf{CF}^{\rho_2'(\tau)}({}^{\rho_2'(\tau)}\mathbf{FC}(\mathbf{v_2}, M_2)) = (\mathbf{v_2'}, M_2)$. Then

$$(W, \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{ValAtom}[\tau^{\langle\mathcal{C}\rangle}]\rho.$$

Proof

We need to show that $(W, \mathbf{v_1}, \mathbf{v'_2}) \in \mathrm{TermAtom}[\rho_1(\tau^{\langle \mathcal{C} \rangle}), \rho_2(\tau^{\langle \mathcal{C} \rangle})]$. By $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[\tau^{\langle \mathcal{C} \rangle}]\rho$, we know that $W \in \mathrm{World}$, $W.\Psi; \cdot; \cdot \vdash \mathbf{v_1} : \rho_1(\tau^{\langle \mathcal{C} \rangle})$, and $W.\Psi; \cdot; \cdot \vdash \mathbf{v_2} : \rho_2(\tau^{\langle \mathcal{C} \rangle})$. It suffices to show that $W.\Psi; \cdot; \cdot \vdash \mathbf{v'_2} : \rho_2(\tau^{\langle \mathcal{C} \rangle})$. But we can simply use $\mathbf{CF}^{\rho'_2(\tau)}(^{\rho'_2(\tau)}\mathbf{FC}(\mathbf{v_2}, M_2)) = (\mathbf{v'_2}, M_2)$ to apply Lemma 8.5 twice. □

Lemma 9.4 (CF/FC Boundary Cancellation)
Given W, τ, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\beta}]\!]$ such that $\rho = \rho_0[\overline{\beta \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\beta \mapsto \mathrm{opaqueR}(\mathrm{VR})}]$. Then

1. If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$, then $(W, \mathbf{e_1}, \mathcal{CF}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{FC}\ \mathbf{e_2}) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$.
2. If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$, $(M_1, M_2) : W$, and $\mathbf{CF}^{\rho'_2(\tau)}(^{\rho'_2(\tau)}\mathbf{FC}(\mathbf{v_2}, M_2)) = (\mathbf{v'_2}, M_2)$, then
$$(W, \mathbf{v_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho.$$

Proof

We prove both claims simultaneously by induction on $W.k$ and then on the structure of τ.

For claim (1), let $W' \sqsupseteq_{\mathrm{pub}} W$ and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$. Note that $(W, [\cdot], \mathcal{CF}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{FC}\ [\cdot]) \in \mathrm{ContAtom}[\tau^{\langle \mathcal{C} \rangle}]\rho \rightsquigarrow [\tau^{\langle \mathcal{C} \rangle}]\rho$. By Lemma 8.20, it suffices to show

$$(W', \mathbf{v_1}, \mathcal{CF}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{FC}\ \mathbf{v_2}) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho.$$

By Lemma 8.3, for any M, there is a $\mathbf{v'_2}$ such that $\langle M \mid \mathcal{CF}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{FC}\ \mathbf{v_2} \rangle \longmapsto^* \langle M \mid \mathbf{v'_2} \rangle$. Thus, by Lemma 8.15, it suffices to show $(W', \mathbf{v_1}, \mathbf{v'_2}) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$, and finally, by Lemma 8.9, we need only show $(W', \mathbf{v_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$. We have this by claim (2).

We prove claim (2) by cases of τ:

Case α

Since $\rho'(\alpha) \in \mathrm{FValRel}$, we have $\rho(\alpha).\varphi_v^C = \rho'(\alpha).\varphi_v^C \in \mathrm{TransRel}^{\mathcal{C}}[\rho'_1(\alpha), \rho'_2(\alpha)]$. This gives the result immediately.

Case unit

By inspection of the translation, $\mathbf{v'_2} = \mathbf{v_2} = ()$, so we are done.

Case int

By inspection of the translation, $\mathbf{v'_2} = \mathbf{v_2} = \mathbf{n}$, so we are done.

Case $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$

By Lemma 9.3, we know that $(W, \mathbf{v_1}, \mathbf{v'_2}) \in \mathrm{ValAtom}[\lambda[\overline{\alpha}](\overline{\tau}).\tau'^{\langle \mathcal{C} \rangle}]\rho$.

Recall that

$$\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle \mathcal{C} \rangle} = \exists \boldsymbol{\beta}.\langle \left(\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\beta}, \overline{\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]}) \to \tau'^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil] \right), \boldsymbol{\beta} \rangle.$$

Let $\boldsymbol{\tau_f} = \forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\beta}, \overline{\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]}) \to \tau'^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]$. Since $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\exists \boldsymbol{\beta}.\langle \boldsymbol{\tau_f}, \boldsymbol{\beta} \rangle]\!]\rho$, we know that

$$\mathbf{v_1} = \mathbf{pack}\langle \boldsymbol{\tau_1}, \langle \mathbf{v_{f1}}, \mathbf{v_{env1}} \rangle \rangle\ \mathbf{as}\ \exists \boldsymbol{\beta}.\langle \rho_1(\boldsymbol{\tau_f}), \boldsymbol{\beta} \rangle, \quad \mathbf{v_2} = \mathbf{pack}\langle \boldsymbol{\tau_2}, \langle \mathbf{v_{f2}}, \mathbf{v_{env2}} \rangle \rangle\ \mathbf{as}\ \exists \boldsymbol{\beta}.\langle \rho_2(\boldsymbol{\tau_f}), \boldsymbol{\beta} \rangle,$$

and there is some $\mathrm{VR} \in \mathrm{CValRel}$ such that $\mathrm{VR}.\boldsymbol{\tau_1} = \boldsymbol{\tau_1}$, $\mathrm{VR}.\boldsymbol{\tau_2} = \boldsymbol{\tau_2}$,

$$(W, \mathbf{v_{f1}}, \mathbf{v_{f2}}) \in \mathcal{V}[\![\boldsymbol{\tau_f}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}], \quad \text{and} \quad (W, \mathbf{v_{env1}}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C.$$

By inpection of the translations, $\mathbf{v'_2} = \mathbf{pack}\langle \mathbf{unit}, \langle \mathbf{v'_{f2}}, () \rangle \rangle\ \mathbf{as}\ \exists \boldsymbol{\beta}.\langle \rho_2(\boldsymbol{\tau_f}), \boldsymbol{\beta} \rangle$. We need to find some $\mathrm{VR}' \in \mathrm{CValRel}$ such that $\mathrm{VR}'.\boldsymbol{\tau_1} = \boldsymbol{\tau_1}$, $\mathrm{VR}'.\boldsymbol{\tau_2} = \mathbf{unit}$,

$$(W, \mathbf{v_{env1}}, ()) \in \mathrm{VR}'.\varphi_v^C, \quad \text{and} \quad (W, \mathbf{v_{f1}}, \mathbf{v'_{f2}}) \in \mathcal{V}[\![\boldsymbol{\tau_f}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}'].$$

We will construct such a VR' shortly. First, we will show that the last condition can be derived from the first three and the property that if $(W', \mathbf{v_1}, ()) \in \mathrm{VR}'.\varphi_v^C$, then $(W', \mathbf{v_1}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C$. We are proving that $(W, \mathbf{v_{f1}}, \mathbf{v'_{f2}}) \in \mathcal{V}[\![\boldsymbol{\tau_f}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}']$. Let $W' \sqsupseteq W$, $\overline{\mathrm{VR}^* \in \mathrm{CValRel}}$,

$$\rho^* = \rho[\boldsymbol{\beta} \mapsto \mathrm{VR}'][\boldsymbol{\alpha} \mapsto \overline{\mathrm{VR}^*}],$$

$(W', \mathbf{v^*_{env1}}, \mathbf{v^*_{env2}}) \in \mathrm{VR}'.\varphi_v^C$, and $\overline{(W', \mathbf{v_1^*}, \mathbf{v_2^*}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho^*}$. For convenience, also let $\boldsymbol{\tau_1^*} = \mathrm{VR}^*.\boldsymbol{\tau_1}$ and $\boldsymbol{\tau_2^*} = \mathrm{VR}^*.\boldsymbol{\tau_2}$. We need to show that

$$(W', \mathbf{v_{f1}}\ \overline{[\boldsymbol{\tau_1^*}]}\ \mathbf{v^*_{env1}}, \overline{\mathbf{v_1^*}}, \mathbf{v'_{f2}}\ \overline{[\boldsymbol{\tau_2^*}]}\ \mathbf{v^*_{env2}}, \overline{\mathbf{v_2^*}}) \in \mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho^*.$$

Let $\hat{\rho} = \rho[\boldsymbol{\beta} \mapsto \mathrm{VR}]\overline{[\boldsymbol{\alpha} \mapsto \mathrm{VR}^*]}$. By Lemma 8.3, there exist $\overline{\mathsf{v}_2^*}$ and $\overline{\mathbf{v_2^{*\prime}}}$ such that

$$\overline{\rho_2'(\tau)[\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle/\alpha]}\mathbf{FC}(\mathbf{v_2^*}, M) = (\mathsf{v}_2^*, M) \quad \text{and} \quad \overline{\mathbf{CF}^{\rho_2'(\tau)[\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle/\alpha]}(\mathsf{v}_2^*, M) = (\mathbf{v_2^{*\prime}}, M)}.$$

By Lemma 8.33, $\overline{\mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho^* = \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}'][\alpha \mapsto \mathsf{L}\langle\mathrm{VR}^*\rangle]}$, so we can apply the induction hypothesis and get $\overline{(W', \mathbf{v_1^*}, \mathbf{v_2^{*\prime}}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho^*}$. Note that ρ^* and $\hat{\rho}$ only differ at $\boldsymbol{\beta}$, and that $\overline{\boldsymbol{\beta} \notin \mathrm{ftv}(\tau^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]})}$. Therefore, by Lemma 8.22,

$$\overline{(W', \mathbf{v_1^*}, \mathbf{v_2^{*\prime}}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\hat{\rho}}.$$

Since $\mathrm{VR}'.\boldsymbol{\tau_2} = \mathbf{unit}$, we must have $\mathbf{v^*_{env2}} = ()$. By our assumption about VR', we have that $(W', \mathbf{v^*_{env1}}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C$. Therefore, by our hypothesis that $(W, \mathbf{v_{f1}}, \mathbf{v_{f2}}) \in \mathcal{V}[\![\boldsymbol{\tau_f}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}]$, we have

$$(W', \mathbf{v_{f1}}\ \overline{[\boldsymbol{\tau_1^*}]}\ \mathbf{v^*_{env1}}, \overline{\mathbf{v_1^*}}, \mathbf{v_{f2}}\ \overline{[\boldsymbol{\tau_2^*}]}\ \mathbf{v_{env2}}, \overline{\mathbf{v_2^{*\prime}}}) \in \mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\hat{\rho}.$$

Once again, $\boldsymbol{\beta} \notin \mathrm{ftv}(\tau'^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]})$, so

$$(W', \mathbf{v_{f1}}\ \overline{[\boldsymbol{\tau_1^*}]}\ \mathbf{v^*_{env1}}, \overline{\mathbf{v_1^*}}, \mathbf{v_{f2}}\ \overline{[\boldsymbol{\tau_2^*}]}\ \mathbf{v_{env2}}, \overline{\mathbf{v_2^{*\prime}}}) \in \mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho^*.$$

By Lemma 8.33,

$$\mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho^* = \mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}']\overline{[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}^*\rangle]},$$

so we can apply the induction hypothesis to get

$$(W', \mathbf{v_{f1}}\ \overline{[\boldsymbol{\tau_1^*}]}\ \mathbf{v^*_{env1}}, \overline{\mathbf{v_1^*}}, \mathcal{CF}^{\rho'(\tau')\overline{[\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle/\alpha]}}\ (^{\rho'(\tau')\overline{[\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle/\alpha]}}\mathcal{FC}\ \mathbf{v_{f2}}\ \overline{[\boldsymbol{\tau_2^*}]}\ \mathbf{v_{env2}}, \overline{\mathbf{v_2^{*\prime}}})) \\ \in \mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho^*,$$

By Lemma 8.15, it suffices to show that

$$\mathbf{v'_{f2}}\ \overline{[\boldsymbol{\tau_2^*}]}\ (), \overline{\mathbf{v_2^*}} \longmapsto^* \mathcal{CF}^{\rho'(\tau')\overline{[\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle/\alpha]}}\ (^{\rho'(\tau')\overline{[\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle/\alpha]}}\mathcal{FC}\ \mathbf{v_{f2}}\ \overline{[\boldsymbol{\tau_2^*}]}\ \mathbf{v_{env2}}, \overline{\mathbf{v_2^{*\prime}}}).$$

To show this, we examine the value translations to determine the structure of $\mathbf{v'_{f2}}$. We have that

$$\mathbf{v'_{f2}} = \boldsymbol{\lambda}\overline{[\boldsymbol{\alpha}]}(\mathbf{z} : \mathbf{unit}, \overline{\mathbf{x} : \rho_2(\tau^{\langle \mathcal{C} \rangle})\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}}).\mathcal{CF}^{\rho_2'(\tau')\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}}\ \mathsf{v}\ \overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle]}\ \overline{^{\rho_2'(\tau)\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}}\mathcal{FC}\ \mathbf{x}},$$

where

$$^{\rho_2(\forall\overline{[\alpha]}.(\overline{\tau}) \to \tau'^{\langle \mathcal{C} \rangle})}\mathbf{FC}(\mathbf{v_2}, M) = (\mathsf{v}, M).$$

In particular,

$$\mathsf{v} = \lambda[\alpha](\overline{\mathsf{x} : \tau}).^{\rho_2'(\tau')}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = \mathbf{v_2}\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{y})\ \overline{[\lceil\alpha\rceil]}\ \boldsymbol{\pi_2}(\mathbf{y}), \overline{\mathcal{CF}^{\rho_2'(\tau)}\ \mathsf{x}}).$$

Therefore,

$$\begin{aligned}
& \langle M \mid \mathbf{v'_{f2}}\ [\overline{\boldsymbol{\tau_2^*}}]\ (), \overline{\mathbf{v_2^*}} \rangle \\
\longmapsto\ & \langle M \mid \mathcal{CF}^{\rho'_2(\tau')[\overline{\mathsf{L}\langle\tau_2^*\rangle/\alpha}]}\ \mathsf{v}\ [\overline{\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle}]\ \overline{\rho'_2(\tau)[\overline{\mathsf{L}\langle\tau_2^*\rangle/\alpha}]\mathcal{FC}\ \mathbf{v_2^*}} \rangle \\
\longmapsto^*\ & \langle M \mid \mathcal{CF}^{\rho'_2(\tau')[\overline{\mathsf{L}\langle\tau_2^*\rangle/\alpha}]}\ \mathsf{v}\ [\overline{\mathsf{L}\langle\boldsymbol{\tau_2^*}\rangle}]\ \overline{\mathsf{v}_2^*} \rangle \\
\longmapsto^4\ & \langle M \mid \mathcal{CF}^{\rho'_2(\tau')[\overline{\mathsf{L}\langle\tau_2^*\rangle/\alpha}]}\ \mathcal{FC}\ \mathbf{v_{f2}}\ [\overline{\boldsymbol{\tau_2^*}}]\ \mathbf{v_{env2}}, \overline{\mathcal{CF}^{\rho'_2(\tau)[\overline{\mathsf{L}\langle\tau_2^*\rangle/\alpha}]}\ \mathsf{v}_2^*} \rangle \\
\longmapsto^*\ & \langle M \mid \mathcal{CF}^{\rho'_2(\tau')[\overline{\mathsf{L}\langle\tau_2^*\rangle/\alpha}]}\ \rho'_2(\tau')[\overline{\mathsf{L}\langle\tau_2^*\rangle/\alpha}]\mathcal{FC}\ \mathbf{v_{f2}}\ [\overline{\boldsymbol{\tau_2^*}}]\ \mathbf{v_{env2}}, \overline{\mathbf{v_2^{*\prime}}} \rangle,
\end{aligned}$$

as desired.

It remains to construct VR'. Recall that the properties VR' must satisfy are these:

- $\mathrm{VR}' \in \mathrm{CValRel}$
- $\mathrm{VR}'.\boldsymbol{\tau_1} = \boldsymbol{\tau_1}$
- $\mathrm{VR}'.\boldsymbol{\tau_2} = \mathbf{unit}$
- $(W, \mathbf{v_{env1}}, ()) \in \mathrm{VR}'.\varphi_v^C$
- If $(W', \mathbf{v}, ()) \in \mathrm{VR}'.\varphi_v^C$, then $(W', \mathbf{v}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C$.

Define VR' as follows:

$$\begin{aligned}
\varphi_v^C{}_0 &= \{(W', \mathbf{v_{env1}}, ()) \mid W' \sqsupseteq W\} & \varphi_v^A{}_0 &= \{\} \\
\varphi_v^C{}_{n+1} &= \varphi_v^C{}_n \cup \mathcal{CA}(\boldsymbol{\tau_1}, \mathbf{unit}, \varphi_v^A{}_n) & \varphi_v^A{}_{n+1} &= \varphi_v^A{}_n \cup \mathcal{AC}(\boldsymbol{\tau_1}, \mathbf{unit}, \varphi_v^C{}_n) \\
\hat{\varphi}_v^C &= \textstyle\bigcup_{i=0}^{\infty} \varphi_v^C{}_i & \hat{\varphi}_v^A &= \textstyle\bigcup_{i=0}^{\infty} \varphi_v^A{}_i
\end{aligned}$$

$$\mathrm{VR}' = (\boldsymbol{\tau_1}, \mathbf{unit}, \hat{\varphi}_v^C, \hat{\varphi}_v^A).$$

We need to show the first and last of the required properties; the others hold obviously.

To show that $\mathrm{VR}' \in \mathrm{CValRel}$, we need to show the following:

1. $\hat{\varphi}_v^C \in \mathrm{ValRel}[\boldsymbol{\tau_1}, \mathbf{unit}]$
2. $\hat{\varphi}_v^A \in \mathrm{TransRel}^{\mathcal{A}}[\boldsymbol{\tau_1}, \mathbf{unit}]$
3. $\mathcal{AC}(\boldsymbol{\tau_1}, \mathbf{unit}, \hat{\varphi}_v^C) \subseteq \hat{\varphi}_v^A$
4. $\mathcal{CA}(\boldsymbol{\tau_1}, \mathbf{unit}, \hat{\varphi}_v^A) \subseteq \hat{\varphi}_v^C$.

Part (1) requires monotonicity and forward boundary cancellation. Monotonicity holds by induction on i, noting that the translation operators preserve monotonicity. Boundary cancellation holds on the left by definition: for any element of $\varphi_v^C{}_i$, the required translation is in $\varphi_v^C{}_{i+2}$. On the right, boundary cancellation holds by the translation rules for the unit value.

Part (2) requires monotonicity and backward boundary cancellation. These properties hold by similar arguments to those for part (1).

Parts (3) and (4) hold by definition.

Finally, we must show that $(W', \mathbf{v}, ()) \in \hat{\varphi}_v^C$, implies $(W', \mathbf{v}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C$. We prove this simultaneously with the property that for any $(W', \mathbf{v}, ()) \in \hat{\varphi}_v^A$, if $(M_1, M_2) : W'$ and ${}^{\boldsymbol{\tau_1}}\mathbf{CA}(\mathbf{v}, M_1) = (\mathbf{v}, M_1)$, then $(W', \mathbf{v}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C$, using induction on i.

For the first proposition, we have $(W', \mathbf{v}, ()) \in \varphi_v^C{}_i$ for some i. If $i = 0$, we have the result since we know that $(W, \mathbf{v_{env1}}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C$. If $i > 0$, then either $(W', \mathbf{v}, ()) \in \varphi_v^C{}_{i-1}$, in which case the induction hypothesis gives the result immediately, or there is some $\mathbf{v}$ such that ${}^{\boldsymbol{\tau_1}}\mathbf{CA}(\mathbf{v}, M_1) = (\mathbf{v}, M_1)$ and $(W', \mathbf{v}, ()) \in \varphi_v^A{}_{i-1}$, in which case the induction hypothesis for the second proposition gives the result immediately.

For the second proposition, we have $(W', \mathbf{v}, ()) \in \varphi_v^A{}_i$ for some i. If $i = 0$, we have a contradiction since $\varphi_v^A{}_0$ is empty, so we are done. If $i > 0$, then either $(W', \mathbf{v}, ()) \in \varphi_v^A{}_{i-1}$, in which case the induction hypothesis gives the result immediately, or there are some $\mathbf{v}$, $\widetilde{W}$, and M' such that $W' = \widetilde{W} \boxplus (M', \{\cdot\})$, $\mathbf{AC}^{\boldsymbol{\tau_1}}(\mathbf{v}, M_1) = (\mathbf{v}, M_1 \uplus M')$, and $(\widetilde{W}, \mathbf{v}, ()) \in \hat{\varphi}_v^C{}_{i-1}$. By the induction hypothesis for the first proposition, $(\widetilde{W}, \mathbf{v}, \mathbf{v_{env2}}) \in \mathrm{VR}.\varphi_v^C$. The result follows from boundary cancellation on $\mathrm{VR}.\varphi_v^C$.

This completes the proof of the most difficult case of boundary cancellation!

Case $\exists\alpha.\tau$

By Lemma 9.3, we know that $(W, \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{ValAtom}[\exists\alpha.\tau^{\langle \mathcal{C} \rangle}]\rho$.

We know that $\mathbf{v_1} = \mathbf{pack}\langle \boldsymbol{\tau_1}, \hat{\mathbf{v}}_1 \rangle \ \mathbf{as}\ \rho_1(\exists\alpha.\tau^{\langle \mathcal{C} \rangle})$ and $\mathbf{v_2} = \mathbf{pack}\langle \boldsymbol{\tau_2}, \hat{\mathbf{v}}_2 \rangle \ \mathbf{as}\ \rho_2(\exists\alpha.\tau^{\langle \mathcal{C} \rangle})$, and that there is some VR $\in$ CValRel such that $\mathrm{VR}.\boldsymbol{\tau_1} = \boldsymbol{\tau_1}$, $\mathrm{VR}.\boldsymbol{\tau_2} = \boldsymbol{\tau_2}$, and (applying Lemma 8.33)

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho[\alpha \mapsto \mathsf{L}\langle \mathrm{VR} \rangle].$$

By Lemma 8.3, there exist $\hat{\mathbf{v}}$ and $\hat{\mathbf{v}}_2'$ such that

$$^{\rho_2'(\tau)[\mathsf{L}\langle\boldsymbol{\tau_1}\rangle/\alpha]}\mathbf{FC}(\hat{\mathbf{v}}_2, M) = (\hat{\mathbf{v}}, M) \quad \text{and} \quad \mathbf{CF}^{\rho_2'(\tau)[\mathsf{L}\langle\boldsymbol{\tau_1}\rangle/\alpha]}(\hat{\mathbf{v}}, M) = (\hat{\mathbf{v}}_2', M).$$

Thus we can apply the induction hypothesis and Lemma 8.33 to get

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho[\alpha \mapsto \mathsf{L}\langle \mathrm{VR} \rangle] = \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}].$$

By inspection of the translations, $\mathbf{v_2'} = \mathbf{pack}\langle \boldsymbol{\tau_2}, \hat{\mathbf{v}}_2' \rangle \ \mathbf{as}\ (\rho_2(\exists\alpha.\tau)^{\langle \mathcal{C} \rangle})$, so we have the desired result of

$$(W, \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{V}[\![\exists\alpha.\tau^{\langle \mathcal{C} \rangle}]\!]\rho$$

by using VR to instantiate the existential.

Case $\mu\alpha.\tau$

By Lemma 9.3, we know that $(W, \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{ValAtom}[\mu\alpha.\tau^{\langle \mathcal{C} \rangle}]\rho$.

We know that $\mathbf{v_1} = \mathbf{fold}_{\rho_1(\mu\alpha.\tau^{\langle \mathcal{C} \rangle})}\ \hat{\mathbf{v}}_1$, $\mathbf{v_2} = \mathbf{fold}_{\rho_2(\mu\alpha.\tau^{\langle \mathcal{C} \rangle})}\ \hat{\mathbf{v}}_2$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright\mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil][\mu\alpha.\tau^{\langle \mathcal{C} \rangle}/\boldsymbol{\alpha}]]\!]\rho = \triangleright\mathcal{V}[\![(\tau[\mu\alpha.\tau/\alpha])^{\langle \mathcal{C} \rangle}]\!]\rho.$$

By Lemma 8.3, there exist $\hat{\mathbf{v}}$ and $\hat{\mathbf{v}}_2'$ such that

$$^{\rho_2'(\tau[\mu\alpha.\tau/\alpha])}\mathbf{FC}(\hat{\mathbf{v}}_2, M) = (\hat{\mathbf{v}}, M) \quad \text{and} \quad \mathbf{CF}^{\rho_2'(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathbf{v}}, M) = (\hat{\mathbf{v}}_2', M).$$

Thus we can apply the induction hypothesis to get

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \triangleright\mathcal{V}[\![(\tau[\mu\alpha.\tau/\alpha])^{\langle \mathcal{C} \rangle}]\!]\rho = \triangleright\mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil][\mu\alpha.\tau^{\langle \mathcal{C} \rangle}/\boldsymbol{\alpha}]]\!]\rho.$$

By inspection of the translations, $\mathbf{v_2'} = \mathbf{fold}_{\rho_2(\mu\alpha.\tau^{\langle \mathcal{C} \rangle})}\ \hat{\mathbf{v}}_2'$, so we have the result.

Case $\langle\overline{\tau}\rangle$

By definition of the value translations and the induction hypothesis.

Case $\mathsf{L}\langle\boldsymbol{\tau}\rangle$

By inspection of the translations at type $\mathsf{L}\langle\boldsymbol{\tau}\rangle$, $\mathbf{v_2'} = \mathbf{v_2}$, so we are done.

□

Lemma 9.5

Given W, $\boldsymbol{\tau}$, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\boldsymbol{\beta}}]\!]$ such that $\rho = \rho_0[\overline{\boldsymbol{\beta} \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\boldsymbol{\beta} \mapsto \mathrm{VR}'}]$, where for each VR_i, VR_i', either $\mathrm{VR}_i = \mathrm{opaqueR}(\mathrm{VR}_i')$ or $\mathrm{opaqueR}(\mathrm{VR}_i) = \mathrm{VR}_i'$. Also let $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[\boldsymbol{\tau}]\rho$, $(M_1, M_2) : W$, and $^{\rho_2'(\boldsymbol{\tau})}\mathbf{CA}(\mathbf{AC}^{\rho_2(\boldsymbol{\tau})}(\mathbf{v_2}, M_2)) = (\mathbf{v_2'}, M_2 \uplus M_2')$. Then $(W \boxplus (\{\cdot\}, M_2'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{ValAtom}[\boldsymbol{\tau}]\rho'$.

Proof

We need to show that $(W \boxplus (\{\cdot\}, M_2'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{TermAtom}[\boldsymbol{\tau}]\rho'$. From $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[\boldsymbol{\tau}]\rho$ we know that $W \in \mathrm{World}$, $W.\Psi_1; \cdot; \cdot \vdash \mathbf{v_1} : \rho_1(\boldsymbol{\tau})$, and $W.\Psi_2; \cdot; \cdot \vdash \mathbf{v_2} : \rho_2(\boldsymbol{\tau})$. By definition of opaqueR, $\rho_1' = \rho_1$, so it suffices to show $(W \boxplus (\{\cdot\}, M_2')).\Psi_2; \cdot; \cdot \vdash \mathbf{v_2'} : \rho_2'(\boldsymbol{\tau})$. But now we need only use our hypothesis that $^{\rho_2'(\boldsymbol{\tau})}\mathbf{CA}(\mathbf{AC}^{\rho_2(\boldsymbol{\tau})}(\mathbf{v_2}, M_2)) = (\mathbf{v_2'}, M_2 \uplus M_2')$ to apply Lemma 8.5 twice. □

Lemma 9.6 (CA/AC Boundary Cancellation)

Given W, $\boldsymbol{\tau}$, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\boldsymbol{\beta}}]\!]$ such that $\rho = \rho_0[\overline{\boldsymbol{\beta} \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\boldsymbol{\beta} \mapsto \mathrm{VR}'}]$, where for each VR_i, VR_i', either $\mathrm{VR}_i = \mathrm{opaqueR}(\mathrm{VR}_i')$ or $\mathrm{opaqueR}(\mathrm{VR}_i) = \mathrm{VR}_i'$. Then

1. If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\boldsymbol{\tau}]\!]\rho$, then $(W, \mathbf{e_1}, {}^{\rho_2'(\boldsymbol{\tau})}\mathcal{CA}\,\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\,\mathbf{e_2}) \in \mathcal{E}[\![\boldsymbol{\tau}]\!]\rho'$.
2. If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho$, $(M_1, M_2) : W$, and ${}^{\rho_2'(\boldsymbol{\tau})}\mathbf{CA}(\mathbf{AC}^{\rho_2(\boldsymbol{\tau})}(\mathbf{v_2}, M_2)) = (\mathbf{v_2'}, M_2 \uplus M')$, then
$$(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho'.$$

Proof

We prove both claims simultaneously by induction on $W.k$ and then on the structure of $\boldsymbol{\tau}$.

For claim (1), let $W' \sqsupseteq_{\text{pub}} W$ and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho$. Note that $(W, [\cdot], {}^{\rho_2'(\boldsymbol{\tau})}\mathcal{CA}\,\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\,[\cdot]) \in \text{ContAtom}[\boldsymbol{\tau}]\rho \rightsquigarrow [\boldsymbol{\tau}]\rho'$. By Lemma 8.20, it suffices to show

$$(W', \mathbf{v_1}, {}^{\rho_2'(\boldsymbol{\tau})}\mathcal{CA}\,\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\,\mathbf{v_2}) \in \mathcal{E}[\![\boldsymbol{\tau}]\!]\rho'.$$

Note that $(W', \mathbf{v_1}, {}^{\rho_2'(\boldsymbol{\tau})}\mathcal{CA}\,\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\,\mathbf{v_2}) \in \text{TermAtom}[\boldsymbol{\tau}]\rho'$.

By Lemma 8.3, for any $(M_1, M_2) : W$, there is a $\mathbf{v_2'}$ such that

$$\langle M_2 \mid {}^{\rho_2'(\boldsymbol{\tau})}\mathcal{CA}\,\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\,\mathbf{v_2}\rangle \longmapsto^* \langle M_2 \uplus M' \mid \mathbf{v_2'}\rangle.$$

Thus, by Lemma 8.16, it suffices to show $(W' \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{E}[\![\boldsymbol{\tau}]\!]\rho'$, and finally, by Lemma 8.9, we need only show $(W' \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho'$, which we have by claim (2).

We prove claim (2) by considering the possible cases of $\boldsymbol{\tau}$:

Case $\boldsymbol{\alpha}$

Since $\rho \in \mathcal{D}[\![\Delta, \overline{\boldsymbol{\alpha}}]\!]$, we know that $\rho(\boldsymbol{\alpha}) \in \text{CValRel}$. By Lemma 8.35, $\rho'(\boldsymbol{\alpha}) \in \text{CValRel}$ as well. Consider the three possible cases of $\rho(\boldsymbol{\alpha})$ and $\rho'(\boldsymbol{\alpha})$:

- If $\rho(\boldsymbol{\alpha}) = \rho'(\boldsymbol{\alpha}) = (\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_v^C, \varphi_v^A)$, then the result is immediate, since $\rho(\boldsymbol{\alpha}) \in \text{ValRel}[\boldsymbol{\tau_1}, \boldsymbol{\tau_2}]$.
- If $\rho(\boldsymbol{\alpha}) = (\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_v^C, \varphi_v^A)$ and $\rho'(\boldsymbol{\alpha}) = \text{opaqueR}(\rho(\boldsymbol{\alpha})) = (\boldsymbol{\tau_1}, \mathbf{L}\langle \boldsymbol{\tau_2}{}^{\langle \mathcal{A} \rangle}\rangle, \hat{\varphi}_v^C, \varphi_v^A)$, then by Lemma 8.5, $\mathbf{v_2'} = {}^{\mathbf{L}\langle \boldsymbol{\tau_2}{}^{\langle \mathcal{A} \rangle}\rangle}\mathcal{CA}\,\mathbf{v_2}$ for some $\mathbf{v_2}$ such that $\mathbf{AC}^{\boldsymbol{\tau_2}}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M')$. The result follows from Lemma 8.37.
- Finally, if $\rho'(\boldsymbol{\alpha}) = (\boldsymbol{\tau_1}, \boldsymbol{\tau_2}, \varphi_v^C, \varphi_v^A)$ and $\rho(\boldsymbol{\alpha}) = \text{opaqueR}(\rho'(\boldsymbol{\alpha})) = (\boldsymbol{\tau_1}, \mathbf{L}\langle \boldsymbol{\tau_2}{}^{\langle \mathcal{A} \rangle}\rangle, \hat{\varphi}_v^C, \varphi_v^A)$, then there exists some $\mathbf{v_2}$ such that $\mathbf{v_2} = {}^{\mathbf{L}\langle \boldsymbol{\tau_2}{}^{\langle \mathcal{A} \rangle}\rangle}\mathcal{CA}\,\mathbf{v_2}$ and ${}^{\boldsymbol{\tau_2}}\mathbf{CA}(\mathbf{v_2}, M_2) = (\mathbf{v_2'}, M_2)$. The result follows from Lemma 8.37.

Case unit

By inspection of the translation, $\mathbf{v_2'} = \mathbf{v_2} = ()$, so we are done.

Case int

By inspection of the translation, $\mathbf{v_2'} = \mathbf{v_2} = \mathbf{n}$, so we are done.

Case $\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau'}$

By Lemma 9.5, we know that $(W, \mathbf{v_1}, \mathbf{v_2'}) \in \text{ValAtom}[\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau'}]\rho'$.

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, M')$, $\overline{\text{VR} \in \text{CValRel}}$, SR $\in$ TStackRel, and $\overline{(W', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho'[\boldsymbol{\alpha} \mapsto \text{VR}]}$. We need to show that

$$(W', \mathbf{v_1}\ \overline{[\text{VR}.\boldsymbol{\tau_1}]\ \hat{\mathbf{v}}_1}, \mathbf{v_2'}\ \overline{[\text{VR}.\boldsymbol{\tau_2}]\ \hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\boldsymbol{\tau'}]\!]\rho'[\boldsymbol{\alpha} \mapsto \text{VR}].$$

For convenience, let $\overline{\boldsymbol{\tau_1}} = \overline{\text{VR}.\boldsymbol{\tau_1}}$, $\overline{\boldsymbol{\tau_2}} = \overline{\text{VR}.\boldsymbol{\tau_2}}$, $\hat{\rho} = \rho[\boldsymbol{\alpha} \mapsto \text{opaqueR}(\text{VR})]$, and $\hat{\rho}' = \rho'[\boldsymbol{\alpha} \mapsto \text{VR}]$. Thus we can restate our assumptions as $\overline{(W', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\hat{\rho}'}$, and we can restate our proof obligation as $(W', \mathbf{v_1}\ \overline{[\boldsymbol{\tau_1}]\ \hat{\mathbf{v}}_1}, \mathbf{v_2'}\ \overline{[\boldsymbol{\tau_2}]\ \hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\boldsymbol{\tau'}]\!]\hat{\rho}'$.

Suppose $(\hat{M}_1, \hat{M}_2) : W'$. By Lemma 8.3, there are some $\overline{\hat{\mathbf{v}}}$ and $\overline{\hat{\mathbf{v}}_2'}$ such that

$$\overline{\mathbf{AC}^{\hat{\rho}_2(\boldsymbol{\tau})}(\hat{\mathbf{v}}_2, \hat{M}_2) = (\hat{\mathbf{v}}, \hat{M}_2 \uplus \hat{M}_i')} \quad \text{and} \quad \overline{{}^{\hat{\rho}_2'(\boldsymbol{\tau})}\mathbf{CA}(\hat{\mathbf{v}}, \hat{M}_2 \uplus \hat{M}_i') = (\hat{\mathbf{v}}_2', \hat{M}_2 \uplus \hat{M}_i')}.$$

Let $\hat{M}' = \bigcup M_i'$. By the induction hypothesis and monotonicity,

$$\overline{(W' \boxplus (\{\cdot\}, \hat{M}'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\hat{\rho}}.$$

Hence, by our assumption that $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau}']\!]\rho$, we have

$$(W' \boxplus (\{\cdot\}, \hat{M}'), \mathbf{v_1}\ [\overline{\boldsymbol{\tau_1}}]\ \overline{\hat{\mathbf{v}}_1}, \mathbf{v_2}\ [\overline{\mathbf{L}\langle \boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle} \rangle}]\ \overline{\hat{\mathbf{v}}_2'}) \in \mathcal{E}[\![\boldsymbol{\tau}']\!]\hat{\rho}.$$

By the induction hypothesis and by claim (1),

$$(W' \boxplus (\{\cdot\}, \hat{M}'), \mathbf{v_1}\ [\overline{\boldsymbol{\tau_1}}]\ \overline{\hat{\mathbf{v}}_1}, {}^{\hat{\rho}_2'(\boldsymbol{\tau}')}\mathcal{CA}\,\mathcal{AC}^{\hat{\rho}_2(\boldsymbol{\tau}')}\ \mathbf{v_2}\ [\overline{\mathbf{L}\langle \boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle} \rangle}]\ \overline{\hat{\mathbf{v}}_2'}) \in \mathcal{E}[\![\boldsymbol{\tau}']\!]\hat{\rho}'.$$

We claim that

$$\langle \hat{M}_2 \mid \mathbf{v_2'}\ [\overline{\boldsymbol{\tau_2}}]\ \overline{\hat{\mathbf{v}}_2} \rangle \longmapsto^* \langle \hat{M}_2 \cup \hat{M}' \mid {}^{\hat{\rho}_2'(\boldsymbol{\tau}')}\mathcal{CA}\,\mathcal{AC}^{\hat{\rho}_2(\boldsymbol{\tau}')}\ \mathbf{v_2}\ [\overline{\mathbf{L}\langle \boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle} \rangle}]\ \overline{\hat{\mathbf{v}}_2'} \rangle$$

using only memory-invariant reduction steps and translation reduction steps that only affect memory by allocating the $\hat{M}_i'$. By Lemmas 8.15 and 8.16, this is sufficient to complete the proof.
To show this reduction sequence, we derive the shape of $\mathbf{v_2'}$. By definition,

$$\mathbf{AC}^{\rho_2(\forall[\overline{\alpha}].(\overline{\tau}) \to \tau')}(\mathbf{v_2}, M_2) = (\ell, M_2 \uplus M'),$$

where

$$M' = \ell \mapsto \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x} : \rho_2(\boldsymbol{\tau})^{\langle \mathcal{A} \rangle}[\boldsymbol{\alpha}/\lceil \boldsymbol{\alpha} \rceil]}).\mathcal{AC}^{\rho_2(\boldsymbol{\tau}')[\overline{\mathbf{L}\langle \alpha \rangle/\alpha}]}\ \mathbf{v_2}\ [\overline{\mathbf{L}\langle \boldsymbol{\alpha} \rangle}]\ \overline{{}^{\rho_2(\boldsymbol{\tau})[\overline{\mathbf{L}\langle \alpha \rangle/\alpha}]}\mathcal{CA}\,\mathbf{x}}.$$

Also by definition,

$${}^{\rho_2'(\forall[\overline{\alpha}].(\overline{\tau}) \to \tau')}\mathbf{CA}(\ell, M_2 \uplus M') = (\boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x} : \boldsymbol{\tau}}).{}^{\rho_2'(\boldsymbol{\tau}')}\mathcal{CA}\ (\ell\ [\overline{\lceil \boldsymbol{\alpha} \rceil}]\ \overline{\mathcal{AC}^{\rho_2'(\boldsymbol{\tau})}\ \mathbf{x}}), M_2 \uplus M').$$

Thus $\mathbf{v_2'} = \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x} : \boldsymbol{\tau}}).{}^{\rho_2'(\boldsymbol{\tau}')}\mathcal{CA}\ (\ell\ [\overline{\lceil \boldsymbol{\alpha} \rceil}]\ \overline{\mathcal{AC}^{\rho_2'(\boldsymbol{\tau})}\ \mathbf{x}})$.
By the operational semantics and by the property that $\hat{M}_2(\ell) = M'(\ell)$ (which follows from the definitions of $\boxplus$ and world extension), we have

$$\begin{array}{lll}
\langle \hat{M}_2 \mid \mathbf{v_2'}\ [\overline{\boldsymbol{\tau_2}}]\ \overline{\hat{\mathbf{v}}_2} \rangle & \longmapsto & \langle \hat{M}_2 \mid {}^{\hat{\rho}_2'(\boldsymbol{\tau}')}\mathcal{CA}\ (\ell\ [\overline{\boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle}}]\ \overline{\mathcal{AC}^{\hat{\rho}_2'(\boldsymbol{\tau})}\ \hat{\mathbf{v}}_2}) \rangle \\
& \longmapsto^* & \langle \hat{M}_2 \uplus \hat{M}' \mid {}^{\hat{\rho}_2'(\boldsymbol{\tau}')}\mathcal{CA}\ (\ell\ [\overline{\boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle}}]\ \overline{\hat{\mathbf{v}}}) \rangle \\
& \longmapsto & \langle \hat{M}_2 \uplus \hat{M}' \mid {}^{\hat{\rho}_2'(\boldsymbol{\tau}')}\mathcal{CA}\,\mathcal{AC}^{\hat{\rho}_2(\boldsymbol{\tau}')}\ \mathbf{v_2}\ [\overline{\mathbf{L}\langle \boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle} \rangle}]\ \overline{{}^{\hat{\rho}_2(\boldsymbol{\tau})}\mathcal{CA}\ \hat{\mathbf{v}}} \rangle \\
& \longmapsto^* & \langle \hat{M}_2 \uplus \hat{M}' \mid {}^{\hat{\rho}_2'(\boldsymbol{\tau}')}\mathcal{CA}\,\mathcal{AC}^{\hat{\rho}_2(\boldsymbol{\tau}')}\ \mathbf{v_2}\ [\overline{\mathbf{L}\langle \boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle} \rangle}]\ \overline{\hat{\mathbf{v}}_2'} \rangle,
\end{array}$$

as desired.

Case $\exists\boldsymbol{\alpha}.\boldsymbol{\tau}$

By Lemma 9.5, we know that $(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{ValAtom}[\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\rho'$.
By our hypothesis that $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\exists\boldsymbol{\alpha}.\boldsymbol{\tau}]\!]\rho$, we know that

$$\mathbf{v_1} = \mathbf{pack}\langle \boldsymbol{\tau_1}, \hat{\mathbf{v}}_1 \rangle\ \mathbf{as}\ \rho_1(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}), \qquad \mathbf{v_2} = \mathbf{pack}\langle \boldsymbol{\tau_2}, \hat{\mathbf{v}}_2 \rangle\ \mathbf{as}\ \rho_2(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}),$$

and that there is some $\mathrm{VR} \in \mathrm{CValRel}$ such that $\mathrm{VR}.\boldsymbol{\tau_1} = \boldsymbol{\tau_1}$, $\mathrm{VR}.\boldsymbol{\tau_2} = \boldsymbol{\tau_2}$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}].$$

Note that by Lemma 8.3, there are some $\hat{\mathbf{v}}$ and $\hat{\mathbf{v}}_2'$ such that

$$\mathbf{AC}^{\rho(\boldsymbol{\tau})[\boldsymbol{\tau_2}/\boldsymbol{\alpha}]}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}, M_2 \uplus M') \quad \text{and} \quad {}^{\rho(\boldsymbol{\tau})[\mathbf{L}\langle \boldsymbol{\tau_2}^{\langle \mathcal{A} \rangle} \rangle/\boldsymbol{\alpha}]}\mathbf{CA}(\hat{\mathbf{v}}, M_2 \uplus M') = (\hat{\mathbf{v}}_2', M_2 \uplus M').$$

Consider the form of $\mathbf{v_2'}$. By definition,

$$\mathbf{AC}^{\rho_2(\exists\alpha.\tau)}(\mathbf{v_2}, M_2) = (\mathbf{pack}\langle\tau_2{}^{\langle\mathcal{A}\rangle}, \hat{\mathbf{v}}\rangle \mathbf{\ as\ } (\rho_2(\exists\alpha.\tau))^{\langle\mathcal{A}\rangle}, M_2 \uplus M')$$

and

$${}^{\rho_2'(\exists\alpha.\tau)}\mathbf{CA}(\mathbf{pack}\langle\tau_2{}^{\langle\mathcal{A}\rangle}, \hat{\mathbf{v}}\rangle \mathbf{\ as\ } (\rho_2(\exists\alpha.\tau))^{\langle\mathcal{A}\rangle}, M_2 \uplus M') = (\mathbf{pack}\langle\mathbf{L}\langle\tau_2{}^{\langle\mathcal{A}\rangle}\rangle, \hat{\mathbf{v}}_2'\rangle, M_2 \uplus M').$$

So to show that $(W, \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{V}[\![\exists\alpha.\tau]\!]\rho'$, we need to show that there is some $\mathrm{VR}' \in \mathrm{CValRel}$ such that $\mathrm{VR}'.\tau_1 = \tau_1$, $\mathrm{VR}'.\tau_2 = \mathbf{L}\langle\tau_2{}^{\langle\mathcal{A}\rangle}\rangle$, and

$$(W \boxplus (\{\cdot\}, M'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \mathcal{V}[\![\tau]\!]\rho'[\alpha \mapsto \mathrm{VR}'].$$

By the induction hypothesis, $\mathrm{VR}' = \mathrm{opaqueR}(\mathrm{VR})$ does exactly this, so we are done.

Case $\mu\alpha.\tau$

By Lemma 9.5, we know that $(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{ValAtom}[\mu\alpha.\tau]\rho'$.
By our hypothesis that $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\mu\alpha.\tau]\!]\rho$, we know that

$$\mathbf{v_1} = \mathbf{fold}_{\rho_1(\mu\alpha.\tau)}\ \hat{\mathbf{v}}_1, \qquad \mathbf{v_2} = \mathbf{fold}_{\rho_2(\mu\alpha.\tau)}\ \hat{\mathbf{v}}_2,$$

and that $(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$.
By Lemma 8.3, there are some $\hat{\mathbf{v}}$ and $\hat{\mathbf{v}}_2'$ such that

$$\mathbf{AC}^{\rho_2(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}, M_2 \uplus M') \quad \text{and} \quad {}^{\rho_2(\tau[\mu\alpha.\tau/\alpha])}\mathbf{CA}(\hat{\mathbf{v}}, M_2 \uplus M') = (\hat{\mathbf{v}}_2', M_2 \uplus M').$$

By the induction hypothesis,

$$(W \boxplus (\{\cdot\}, M'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho'.$$

It remains only to show that $\mathbf{v_2'} = \mathbf{fold}_{\rho_2'(\mu\alpha.\tau)}\ \hat{\mathbf{v}}_2'$, but this follows easily from the definition of the value translations.

Case $\langle\tau_1, \ldots, \tau_n\rangle$

By Lemma 9.5, we know that $(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathrm{ValAtom}[\langle\tau_1, \ldots, \tau_n\rangle]\rho'$. By our hypothesis that $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\langle\tau_1, \ldots, \tau_n\rangle]\!]\rho$, we know that

$$\mathbf{v_1} = \langle\mathbf{v_{11}}, \ldots, \mathbf{v_{1n}}\rangle, \qquad \mathbf{v_2} = \langle\mathbf{v_{21}}, \ldots, \mathbf{v_{2n}}\rangle,$$

and that for each $\mathbf{i}$, $(W, \mathbf{v_{1i}}, \mathbf{v_{2i}}) \in \mathcal{V}[\![\tau_i]\!]\rho$.
By inspection of the translations,

$$M' = M_1' \uplus \cdots \uplus M_n' \uplus (\ell \mapsto \langle\hat{\mathbf{v}}_1, \ldots, \hat{\mathbf{v}}_n\rangle) \quad \text{and} \quad \mathbf{v_2'} = \langle\hat{\mathbf{v}}_1, \ldots, \hat{\mathbf{v}}_n\rangle$$

for some $\hat{\mathbf{v}}_1, \ldots, \hat{\mathbf{v}}_n$ and $\hat{\mathbf{v}}_1, \ldots, \hat{\mathbf{v}}_n$ such that

$$\mathbf{AC}^{\rho_2(\tau_i)}(\mathbf{v_{2i}}, M_2 \uplus M_1' \uplus \cdots \uplus M_{i-1}') = (\hat{\mathbf{v}}_i, M_2 \uplus M_1' \uplus \cdots \uplus M_i')$$

and

$${}^{\rho_2'(\tau_i)}\mathbf{CA}(\hat{\mathbf{v}}_i, M_2 \uplus M') = (\hat{\mathbf{v}}_i, M_2 \uplus M').$$

By the induction hypothesis and monotonicity, each $(W \boxplus (\{\cdot\}, M'), \mathbf{v_{1i}}, \hat{\mathbf{v}}_i) \in \mathcal{V}[\![\tau_i]\!]\rho'$. Thus $(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{V}[\![\langle\tau_1, \ldots, \tau_n\rangle]\!]\rho'$ as desired.

Case $\lceil\alpha\rceil$

Since $\rho'(\alpha) = \rho(\alpha)$,this follows from $\rho(\alpha).\varphi_v^C \in \mathrm{ValRel}[\rho_1(\alpha)^{\langle\mathcal{C}\rangle}, \rho_2(\alpha)^{\langle\mathcal{C}\rangle}]$.

Case $\mathbf{L}\langle\tau\rangle$

By Lemma 9.5, we know that $(W \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v'_2}) \in \mathrm{ValAtom}[\mathbf{L}\langle\tau\rangle]\rho'$.

By assumption, we know that

$$\mathbf{v_1} = {}^{\rho_1(\mathbf{L}\langle\tau\rangle)}\mathcal{CA}\,\hat{\mathbf{v}}_1, \qquad \mathbf{v_2} = {}^{\rho_2(\mathbf{L}\langle\tau\rangle)}\mathcal{CA}\,\hat{\mathbf{v}}_2,$$

and $(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho$. By inspection of the value translations, we know that

$$\mathbf{v'_2} = {}^{\rho'_2(\mathbf{L}\langle\tau\rangle)}\mathcal{CA}\,\hat{\mathbf{v}}_2 \qquad \text{and} \qquad M' = \{\cdot\},$$

so we need to show only that $(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho'$. But this follows by Lemma 8.38.

□

Lemma 9.7
Given W, τ, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\beta}]\!]$ such that $\rho = \rho_0[\overline{\beta \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\beta \mapsto \mathrm{opaqueR}(\mathrm{VR})}]$. Also let $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[\tau^{\langle\mathcal{A}\rangle}]\rho$, $(M_1, M_2) : W$, and $\mathbf{AC}^{\rho'_2(\tau)}({}^{\rho'_2(\tau)}\mathbf{CA}(\mathbf{v_2}, M_2)) = (\mathbf{v'_2}, M_2 \uplus M'_2)$. Then

$$(W \boxplus (\{\cdot\}, M'_2), \mathbf{v_1}, \mathbf{v'_2}) \in \mathrm{ValAtom}[\tau^{\langle\mathcal{A}\rangle}]\rho.$$

Proof

We need to show that $(W, \mathbf{v_1}, \mathbf{v'_2}) \in \mathrm{TermAtom}[\tau^{\langle\mathcal{A}\rangle}]\rho$. From $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathrm{ValAtom}[\tau^{\langle\mathcal{A}\rangle}]\rho$, we know that $W \in \mathrm{World}$, $W.\Psi; \cdot; \cdot \vdash \mathbf{v_1} : \rho_1(\tau^{\langle\mathcal{A}\rangle})$, and $W.\Psi; \cdot; \cdot \vdash \mathbf{v_2} : \rho_2(\tau^{\langle\mathcal{A}\rangle})$. It suffices to show that $W.\Psi; \cdot; \cdot \vdash \mathbf{v'_2} : \rho_2(\tau^{\langle\mathcal{A}\rangle})$. But we can simply use $\mathbf{AC}^{\rho'_2(\tau)}({}^{\rho'_2(\tau)}\mathbf{CA}(\mathbf{v_2}, M_2)) = (\mathbf{v'_2}, M_2)$ to apply Lemma 8.5 twice. □

Lemma 9.8 (AC/CA Boundary Cancellation)
Given W, τ, and Δ, let $\rho \in \mathcal{D}[\![\Delta, \overline{\beta}]\!]$ such that $\rho = \rho_0[\overline{\beta \mapsto \mathrm{VR}}]$ and $\rho' = \rho_0[\overline{\beta \mapsto \mathrm{opaqueR}(\mathrm{VR})}]$. Then

1. If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$, then $(W, \mathbf{e_1}, \mathcal{AC}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{CA}\,\mathbf{e_2}) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$.
2. If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$, $(M_1, M_2) : W$, and $\mathbf{AC}^{\rho'_2(\tau)}({}^{\rho'_2(\tau)}\mathbf{CA}(\mathbf{v_2}, M_2)) = (\mathbf{v'_2}, M_2 \uplus M'_2)$, then

$$(W \boxplus (\{\cdot\}, M'_2), \mathbf{v_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho.$$

Proof

We prove both claims simultaneously by induction on $W.k$ and then on the structure of τ.

For claim (1), let $W' \sqsupseteq_{\mathrm{pub}} W$ and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$. Note that $(W, [\cdot], \mathcal{AC}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{CA}\,[\cdot]) \in \mathrm{ContAtom}[\tau^{\langle\mathcal{A}\rangle}]\rho \rightsquigarrow [\tau^{\langle\mathcal{A}\rangle}]\rho$. By Lemma 8.20, it suffices to show

$$(W', \mathbf{v_1}, \mathcal{AC}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{CA}\,\mathbf{v_2}) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho.$$

Note that $(W', \mathbf{v_1}, \mathcal{AC}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{CA}\,\mathbf{v_2}) \in \mathrm{TermAtom}[\tau]\rho'$.

By Lemma 8.3, for any $(M_1, M_2) : W$, there is a $\mathbf{v'_2}$ such that

$$\langle M_2 \mid \mathcal{AC}^{\rho'_2(\tau)\ \rho'_2(\tau)}\mathcal{CA}\,\mathbf{v_2}\rangle \longmapsto^* \langle M_2 \uplus M' \mid \mathbf{v'_2}\rangle.$$

Thus, by Lemma 8.16, it suffices to show $(W' \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v'_2}) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$, and finally, by Lemma 8.9, we need only show $(W' \boxplus (\{\cdot\}, M'), \mathbf{v_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$. We have this by claim (2).

We prove claim (2) by cases of τ:

Case α

Since $\rho(\alpha) \in \mathrm{CValRel}$, we have $\rho(\alpha).\varphi^A_v = \rho'(\alpha).\varphi^A_v \in \mathrm{TransRel}^{\mathcal{A}}[\rho'_1(\alpha), \rho'_2(\alpha)]$. This gives the result immediately.

Case unit

By inspection of the translation, $\mathsf{v}_2' = \mathsf{v}_2 = ()$, so we are done.

Case int

By inspection of the translation, $\mathsf{v}_2' = \mathsf{v}_2 = \mathsf{n}$, so we are done.

Case $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$

By Lemma 9.7, we know that $(W, \mathsf{v}_1, \mathsf{v}_2') \in \mathrm{ValAtom}[\boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\tau}).\tau'^{\langle\mathcal{A}\rangle}]\rho$.

Recall that

$$\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle\mathcal{A}\rangle} = \mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}) \to \tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil].$$

Let $\psi_\mathsf{f} = \forall[\overline{\alpha}].(\overline{\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}) \to \tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]$. Since $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mathbf{box}\,\psi_\mathsf{f}]\!]\rho$, we know that

$$\mathsf{v}_1 = \ell_1[\hat{\tau}_{11}, \ldots, \hat{\tau}_{1\mathsf{m}}], \qquad \mathsf{v}_2 = \ell_2[\hat{\tau}_{21}, \ldots, \hat{\tau}_{2\mathsf{n}}],$$
$$M_1(\ell_1) = \boldsymbol{\lambda}[\beta_{11}, \ldots, \beta_{1\mathsf{m}}, \overline{\alpha}]\,(\overline{\mathsf{x}\colon \rho_1(\tau_1)}).\mathsf{t}_1, \qquad \overline{\tau} = \overline{\tau_1[\hat{\tau}_1/\beta_1]},$$
$$M_2(\ell_2) = \boldsymbol{\lambda}[\beta_{21}, \ldots, \beta_{2\mathsf{n}}, \overline{\alpha}]\,(\overline{\mathsf{x}\colon \rho_2(\tau_2)}).\mathsf{t}_2, \qquad \overline{\tau} = \overline{\tau_2[\hat{\tau}_2/\beta_2]},$$

and

$$(W, \boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\mathsf{x}\colon \rho_1(\tau_1)}).\mathsf{t}_1[\hat{\tau}_1/\beta_1], \boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\mathsf{x}\colon \rho_2(\tau_2)}).\mathsf{t}_2[\hat{\tau}_2/\beta_2]) \in \mathcal{HV}[\![\psi_\mathsf{f}]\!]\rho.$$

By inpection of the translations, $\mathsf{v}_2' = \ell$ and $M' = \ell \mapsto \mathsf{h}$, where

$$\mathsf{h} = \boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\mathsf{x}\colon \rho_2'(\tau)^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}).\mathsf{e}, \qquad \mathsf{e} = \mathcal{AC}^{\rho_2'(\tau')[\mathbf{L}\langle\alpha\rangle/\alpha]}\,\mathsf{v}\,[\overline{\mathbf{L}\langle\alpha\rangle}]\,\overline{\mathcal{AC}^{\rho_2'(\tau)[\mathbf{L}\langle\alpha\rangle/\alpha]}\mathsf{x}},$$

and

$$\mathsf{v} = \boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\mathsf{x}\colon \rho_2'(\tau)}).^{\rho_2'(\tau')}\mathcal{CA}\,\ell_2\,[\overline{\hat{\tau}_2}, \overline{\lceil\alpha\rceil}]\,\overline{\mathcal{AC}^{\rho_2'(\tau)}\mathsf{x}}.$$

We need to show that

$$(W \uplus (\{\cdot\}, M'), \boldsymbol{\lambda}[\overline{\alpha}]\,(\overline{\mathsf{x}\colon \rho_1(\tau_1)}).\mathsf{t}_1[\hat{\tau}_1/\beta_1], \mathsf{h}) \in \mathcal{HV}[\![\psi_\mathsf{f}]\!]\rho.$$

Let $W' \sqsupseteq W$, $\overline{\mathrm{VR} \in \mathrm{AValRel}}$, $\overline{(W', \mathsf{v}_1^*, \mathsf{v}_2^*) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}]}$. For convenience, also let $\overline{\tau_1^* = \mathrm{VR}.\tau_1}$ and $\overline{\tau_2^* = \mathrm{VR}.\tau_2}$. We need to show that

$$(W', \mathsf{t}_1[\hat{\tau}_1/\beta_1][\tau_1^*/\alpha][\mathsf{v}_1^*/\mathsf{x}], \mathsf{e}[\tau_2^*/\alpha][\mathsf{v}_2^*/\mathsf{x}]) \in \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}].$$

By Lemma 8.3, for any $(M_1', M_2') : W'$, there exist $\overline{\mathsf{v}_2^*}$, $\overline{\mathsf{v}_2^{*\prime}}$, and $M^* = M_1^* \uplus \cdots \uplus M_k^*$ such that

$$\overline{\rho_2(\tau)[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}\mathbf{CA}(\mathsf{v}_2^*, M_2') = (\mathsf{v}_2^*, M_2')$$

and

$$\overline{\mathbf{AC}^{\rho_2(\tau)[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}(\mathsf{v}_2^*, M_2') = (\mathsf{v}_2^{*\prime}, M_2' \uplus M_i^*)}.$$

By Lemma 8.31, $\overline{\mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho[\alpha \mapsto \mathbf{L}\langle\mathrm{VR}\rangle]}$, so we can apply the induction hypothesis and monotonicity to get

$$\overline{(W' \uplus (\{\cdot\}, M^*), \mathsf{v}_1^*, \mathsf{v}_2^{*\prime}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}]}.$$

By instantiating our hypothesis, we know that

$$(W' \uplus (\{\cdot\}, M^*), \mathsf{t}_1[\hat{\tau}_1/\beta_1][\tau_1^*/\alpha][\mathsf{v}_1^*/\mathsf{x}], \mathsf{t}_2[\hat{\tau}_2/\beta_2][\tau_2^*/\alpha][\mathsf{v}_2^*/\mathsf{x}]) \in \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}].$$

By Lemma 8.31, $\mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}]\!]\rho[\alpha \mapsto \mathbf{L}\langle\mathrm{VR}\rangle]$, so we can apply the induction hypothesis to get

$$(W' \uplus (\{\cdot\}, M^*), \mathsf{t}_1[\hat{\tau}_1/\beta_1][\tau_1^*/\alpha][\mathsf{v}_1^*/\mathsf{x}], \mathcal{AC}^{\rho'(\tau')[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}\mathcal{CA}\,\mathsf{t}_2[\hat{\tau}_2/\beta_2][\tau_2^*/\alpha][\mathsf{v}_2^*/\mathsf{x}])$$
$$\in \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}],$$

We claim that

$$\langle M_2' \mid \mathbf{e}\overline{[\tau_2^*/\alpha][\mathbf{v}_2^*/\mathbf{x}]}\rangle \longmapsto^* \langle M_2' \uplus M^* \mid \mathcal{AC}^{\rho'(\tau')\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\mathcal{CA}\,\mathbf{t}_2\overline{[\hat{\tau}_2/\beta_2][\tau_2^*/\alpha][\mathbf{v}_2^*/\mathbf{x}]}\rangle$$

using only memory-invariant reduction steps and translation reduction steps that only affect memory by allocating the M_i^*. By Lemmas 8.15 and 8.16, this is sufficient to complete the proof.

By the operational semantics and by the property that $M_2'(\ell) = \mathbf{h}$ (which follows from the definitions of $\boxplus$ and world extension), we have

$$\begin{aligned}
\langle M_2' \mid \mathbf{e}\overline{[\tau_2^*/\alpha][\mathbf{v}_2^*/\mathbf{x}]}\rangle = \quad & \langle M_2' \mid \mathcal{AC}^{\rho_2(\tau')\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\ \mathbf{v}\ \overline{[\mathbf{L}\langle\tau_2^*\rangle]}\ \overline{{}^{\rho_2(\tau)\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\mathcal{CA}\,\mathbf{v}_2^*}\rangle \\
\longmapsto^* & \langle M_2' \mid \mathcal{AC}^{\rho_2(\tau')\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\ \mathbf{v}\ \overline{[\mathbf{L}\langle\tau_2^*\rangle]}\ \overline{\mathbf{v}_2^*}\rangle \\
\longmapsto & \langle M_2' \mid \mathcal{AC}^{\rho_2(\tau')\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\mathcal{CA}\,\ell_2\ \overline{[\hat{\tau}_2, \tau_2^*]}\ \overline{\mathcal{AC}^{\rho_2(\tau)\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\ \mathbf{v}_2^*}\rangle \\
\longmapsto^* & \langle M_2' \uplus M^* \mid \mathcal{AC}^{\rho_2(\tau')\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\mathcal{CA}\,\ell_2\ \overline{[\hat{\tau}_2, \tau_2^*]}\ \overline{\mathbf{v}_2^{*\prime}}\rangle \\
\longmapsto & \langle M_2' \uplus M^* \mid \mathcal{AC}^{\rho'(\tau')\overline{[\mathbf{L}\langle\tau_2^*\rangle/\alpha]}}\mathcal{CA}\,\mathbf{t}_2\overline{[\hat{\tau}_2/\beta_2][\tau_2^*/\alpha][\mathbf{v}_2^*/\mathbf{x}]}\rangle,
\end{aligned}$$

as desired.

Case $\exists\alpha.\tau$

By Lemma 9.7, we know that $(W, \mathbf{v}_1, \mathbf{v}_2') \in \mathrm{ValAtom}[\exists\alpha.\tau^{\langle\mathcal{A}\rangle}]\rho$.

We know that $\mathbf{v}_1 = \mathbf{pack}\langle\tau_1,\hat{\mathbf{v}}_1\rangle\ \mathbf{as}\ \rho_1(\exists\alpha.\tau^{\langle\mathcal{A}\rangle})$ and $\mathbf{v}_2 = \mathbf{pack}\langle\tau_2,\hat{\mathbf{v}}_2\rangle\ \mathbf{as}\ \rho_2(\exists\alpha.\tau^{\langle\mathcal{A}\rangle})$, and that there is some $\mathrm{VR} \in \mathrm{AValRel}$ such that $\mathrm{VR}.\tau_1 = \tau_1$, $\mathrm{VR}.\tau_2 = \tau_2$, and (applying Lemma 8.31)

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho[\alpha \mapsto \mathbf{L}\langle\mathrm{VR}\rangle].$$

By Lemma 8.3, there exist $\hat{\mathbf{v}}$ and $\hat{\mathbf{v}}_2'$ such that

$$\mathbf{CA}^{\rho_2'(\tau)[\mathbf{L}\langle\tau_1\rangle/\alpha]}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}, M_2) \quad \text{and} \quad \mathbf{AC}^{\rho_2'(\tau)[\mathbf{L}\langle\tau_1\rangle/\alpha]}(\hat{\mathbf{v}}, M_2) = (\hat{\mathbf{v}}_2', M_2 \uplus M').$$

Thus we can apply the induction hypothesis and Lemma 8.31 to get

$$(W \boxplus (\{\cdot\}, M'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho[\alpha \mapsto \mathbf{L}\langle\mathrm{VR}\rangle] = \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}].$$

By inspection of the translations, $\mathbf{v}_2' = \mathbf{pack}\langle\tau_2,\hat{\mathbf{v}}_2'\rangle\ \mathbf{as}\ (\rho_2(\exists\alpha.\tau)^{\langle\mathcal{A}\rangle})$, so we have the desired result of

$$(W \boxplus (\{\cdot\}, M'), \mathbf{v}_1, \mathbf{v}_2') \in \mathcal{V}[\![\exists\alpha.\tau^{\langle\mathcal{A}\rangle}]\!]\rho$$

by using VR to instantiate the existential.

Case $\mu\alpha.\tau$

By Lemma 9.7, we know that $(W, \mathbf{v}_1, \mathbf{v}_2') \in \mathrm{ValAtom}[\mu\alpha.\tau^{\langle\mathcal{A}\rangle}]\rho$.

We know that $\mathbf{v}_1 = \mathbf{fold}_{\rho_1(\mu\alpha.\tau^{\langle\mathcal{A}\rangle})}\ \hat{\mathbf{v}}_1$, $\mathbf{v}_2 = \mathbf{fold}_{\rho_2(\mu\alpha.\tau^{\langle\mathcal{A}\rangle})}\ \hat{\mathbf{v}}_2$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright\mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil][\mu\alpha.\tau^{\langle\mathcal{A}\rangle}/\alpha]]\!]\rho = \triangleright\mathcal{V}[\![(\tau[\mu\alpha.\tau/\alpha])^{\langle\mathcal{A}\rangle}]\!]\rho.$$

By Lemma 8.3, there exist $\hat{\mathbf{v}}$ and $\hat{\mathbf{v}}_2'$ such that

$$\mathbf{CA}^{\rho_2'(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}, M_2) \quad \text{and} \quad \mathbf{AC}^{\rho_2'(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathbf{v}}, M_2) = (\hat{\mathbf{v}}_2', M_2 \uplus M').$$

Thus we can apply the induction hypothesis to get

$$(W \boxplus (\{\cdot\}, M'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \triangleright\mathcal{V}[\![(\tau[\mu\alpha.\tau/\alpha])^{\langle\mathcal{A}\rangle}]\!]\rho = \triangleright\mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil][\mu\alpha.\tau^{\langle\mathcal{A}\rangle}/\alpha]]\!]\rho.$$

By inspection of the translations, $\mathbf{v}_2' = \mathbf{fold}_{\rho_2(\mu\alpha.\tau^{\langle\mathcal{A}\rangle})}\ \hat{\mathbf{v}}_2'$, so we have the result.

Case $\langle \tau_1, \ldots, \tau_n \rangle$

By Lemma 9.7, we know that $(W \uplus (\{\cdot\}, M'), \mathsf{v}_1, \mathsf{v}_2') \in \mathrm{ValAtom}[\langle \tau_1, \ldots, \tau_n \rangle^{\langle \mathcal{A} \rangle}]\rho'$. By our hypothesis that $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\langle \tau_1, \ldots, \tau_n \rangle^{\langle \mathcal{A} \rangle}]\!]\rho = \mathcal{V}[\![\mathsf{box}\, \langle \tau_1{}^{\langle \mathcal{A} \rangle}, \ldots, \tau_n{}^{\langle \mathcal{A} \rangle} \rangle]\!]\rho$, we know that $\mathsf{v}_1 = \ell_1$ and $\mathsf{v}_2 = \ell_2$, where

$$M_1(\ell_1) = \langle \mathsf{v}_{11}, \ldots, \mathsf{v}_{1n} \rangle, \qquad M_2(\ell_2) = \langle \mathsf{v}_{21}, \ldots, \mathsf{v}_{2n} \rangle,$$

and that for each i, $(W, \mathsf{v}_{1i}, \mathsf{v}_{2i}) \in \mathcal{V}[\![\tau_i]\!]\rho$.

By inspection of the translations,

$$M' = M_1' \uplus \cdots \uplus M_n' \uplus (\ell \mapsto \langle \hat{\mathsf{v}}_1, \ldots, \hat{\mathsf{v}}_n \rangle)\restriction \quad \text{and} \quad \mathsf{v}_2' = \ell$$

for some $\hat{\mathsf{v}}_1, \ldots, \hat{\mathsf{v}}_n$ and $\hat{\mathsf{v}}_1, \ldots, \hat{\mathsf{v}}_n$ such that

$$^{\rho_2'(\tau_i)}\mathbf{CA}(\mathsf{v}_{2i}, M_2) = (\hat{\mathsf{v}}_i, M_2)$$

and

$$\mathbf{AC}^{\rho_2'(\tau_i)}(\hat{\mathsf{v}}_i, M_2 \uplus M_1' \uplus \cdots \uplus M_{i-1}') = (\hat{\mathsf{v}}_i, M_2 \uplus M_1' \uplus \cdots \uplus M_i').$$

By the induction hypothesis and monotonicity, each $(W \uplus (\{\cdot\}, M'), \mathsf{v}_{1i}, \hat{\mathsf{v}}_i) \in \mathcal{V}[\![\tau_i]\!]\rho'$. Thus $(W \uplus (\{\cdot\}, M'), \mathsf{v}_1, \mathsf{v}_2') \in \mathcal{V}[\![\langle \tau_1, \ldots, \tau_n \rangle^{\langle \mathcal{A} \rangle}]\!]\rho'$ as desired.

Case $\lceil \alpha \rceil$

Since $\rho'(\alpha) = \rho(\alpha)$, this follows from $\rho(\alpha).\varphi_v^A \in \mathrm{TransRel}^{\mathcal{A}}[\rho_1(\alpha)^{\langle \mathcal{C} \rangle}, \rho_2(\alpha)^{\langle \mathcal{C} \rangle}]$.

Case $\mathbf{L}\langle \tau \rangle$

By inspection of the translations at type $\mathbf{L}\langle \tau \rangle$, $\mathsf{v}_2' = \mathsf{v}_2$, so we are done.

□

10 Proofs: Soundness and Completeness

10.1 Bridge Lemmas

Lemma 10.1
Let $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \tau$.

1. (a) If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$, then $(W, {}^{\rho_1(\tau)}\mathcal{FC}\ \mathbf{e_1}, {}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{e_2}) \in \mathcal{E}[\![\tau]\!]\rho$.
   (b) If $(W, \mathsf{e}_1, \mathsf{e}_2) \in \mathcal{E}[\![\tau]\!]\rho$, then $(W, \mathcal{CF}^{\rho_1(\tau)}\ \mathsf{e}_1, \mathcal{CF}^{\rho_2(\tau)}\ \mathsf{e}_2) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$.
2. (a) $\mathcal{FC}(\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho) \subseteq \mathcal{V}[\![\tau]\!]\rho$.
   (b) $\mathcal{CF}(\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho) \subseteq \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$

Proof

We can restate claim (2) as follows:

(a) If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$, $(M_1, M_2) : W$, ${}^{\rho_1(\tau_1)}\mathbf{FC}(\mathbf{v_1}, M_1) = (\mathsf{v}_1, M_1)$, ${}^{\rho_2(\tau_2)}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathsf{v}_2, M_2)$, then $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho$.

(b) If $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho$, $(M_1, M_2) : W$, $\mathbf{CF}^{\rho_1(\tau_1)}(\mathsf{v}_1, M_1) = (\mathbf{v_1}, M_1)$, $\mathbf{CF}^{\rho_1(\tau_2)}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2)$, then $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$.

We prove all the claims simultaneously by induction on $W.k$ and the structure of τ.

For claim (1), let $W' \sqsupseteq_{\text{pub}} W$, $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho$, and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho$. Note that

$$(W, {}^{\rho_1(\tau)}\mathcal{FC}\ [\cdot], {}^{\rho_2(\tau)}\mathcal{FC}\ [\cdot]) \in \text{ContAtom}[\tau^{\langle \mathcal{C} \rangle}]\rho \rightsquigarrow [\tau]\rho$$

and

$$(W, \mathcal{CF}^{\rho_1(\tau)}\ [\cdot], \mathcal{CF}^{\rho_2(\tau)}\ [\cdot]) \in \text{ContAtom}[\tau]\rho \rightsquigarrow [\tau^{\langle \mathcal{C} \rangle}]\rho.$$

By Lemma 8.20, for part (a) it suffices to show that

$$(W', {}^{\rho_1(\tau)}\mathcal{FC}\ \mathbf{v_1}, {}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{v_2}) \in \mathcal{E}[\![\tau]\!]\rho,$$

and for part (b) it suffices to show that

$$(W', \mathcal{CF}^{\rho_1(\tau)}\ \mathsf{v}_1, \mathcal{CF}^{\rho_2(\tau)}\ \mathsf{v}_2) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho.$$

But by Lemma 8.3, for any $(M_1, M_2) : W$, there exist $\mathbf{v_1'}$, $\mathbf{v_2'}$, v_1', and v_2' such that

$$\langle M_1 \mid {}^{\rho_1(\tau)}\mathcal{FC}\ \mathbf{v_1} \rangle \longmapsto \langle M_1 \mid \mathsf{v}_1' \rangle \qquad \langle M_2 \mid {}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{v_2} \rangle \longmapsto \langle M_2 \mid \mathsf{v}_2' \rangle$$
$$\langle M_1 \mid \mathcal{CF}^{\rho_1(\tau)}\ \mathsf{v}_1 \rangle \longmapsto \langle M_1 \mid \mathbf{v_1'} \rangle \qquad \langle M_2 \mid \mathcal{CF}^{\rho_2(\tau)}\ \mathsf{v}_2 \rangle \longmapsto \langle M_2 \mid \mathbf{v_2'} \rangle.$$

So by Lemma 8.15, Lemma 8.9, and claim (2), we have the result.

For claim (2), we consider the possible cases of τ:

Case α

Since $\rho(\alpha) \in \text{FValRel}$, we have this immediately.

Case unit

Immediate.

Case int

Immediate.

Case $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$

For part (a), let $W' \sqsupseteq W$, $\overline{\mathrm{VR} \in \mathrm{FValRel}}$, and $\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]}$. For convenience, also let $\overline{\hat{\tau}_1 = \mathrm{VR}.\tau_1}$, $\overline{\hat{\tau}_2 = \mathrm{VR}.\tau_2}$, and $\rho' = \rho[\overline{\alpha \mapsto \mathrm{VR}}]$. We need to show that

$$(W', \mathsf{v}_1\ \overline{[\hat{\tau}_1]}\ \overline{\hat{\mathsf{v}}_1}, \mathsf{v}_2\ \overline{[\hat{\tau}_2]}\ \overline{\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho'.$$

By our assumption, there is some VR^* such that

$$\mathbf{v_1} = \mathbf{pack}\langle \boldsymbol{\tau}_{\mathbf{1env}}, \langle \mathbf{v_{1f}}, \mathbf{v_{1env}} \rangle \rangle\ \mathbf{as}\ \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle \mathcal{C} \rangle},$$
$$\mathbf{v_2} = \mathbf{pack}\langle \boldsymbol{\tau}_{\mathbf{2env}}, \langle \mathbf{v_{2f}}, \mathbf{v_{2env}} \rangle \rangle\ \mathbf{as}\ \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle \mathcal{C} \rangle},$$

$\mathrm{VR}^*.\boldsymbol{\tau_1} = \boldsymbol{\tau}_{\mathbf{1env}}$, $\mathrm{VR}^*.\boldsymbol{\tau_2} = \boldsymbol{\tau}_{\mathbf{2env}}$, $(W, \mathbf{v_{1env}}, \mathbf{v_{2env}}) \in \mathrm{VR}^*.\varphi_v^C$, and

$$(W, \mathbf{v_{1f}}, \mathbf{v_{2f}}) \in \mathcal{V}[\![\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\beta}, \overline{\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]}) \to \tau'^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}^*].$$

Let $(M_1', M_2') : W'$. By Lemma 8.3 and the induction hypothesis, there are some $\overline{\hat{\mathbf{v}}_1}$ and $\overline{\hat{\mathbf{v}}_2}$ such that $\mathbf{CF}^{\hat{\tau}_1}(\hat{\mathsf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1)$, $\mathbf{CF}^{\hat{\tau}_2}(\hat{\mathsf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2)$, and

$$\overline{(W', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho' = \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}^*][\overline{\boldsymbol{\alpha} \mapsto \mathcal{CF}\mathrm{VR}}]}.$$

Instantiating the previous fact with this, we get

$$(W', \mathbf{v_{1f}}\ \overline{[\hat{\tau}_1^{\langle \mathcal{C} \rangle}]}\ \mathbf{v_{1env}}, \overline{\hat{\mathbf{v}}_1}, \mathbf{v_{2f}}\ \overline{[\hat{\tau}_2^{\langle \mathcal{C} \rangle}]}\ \mathbf{v_{2env}}, \overline{\hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}^*][\overline{\boldsymbol{\alpha} \mapsto \mathcal{CF}\mathrm{VR}}] = \mathcal{E}[\![\tau'^{\langle \mathcal{C} \rangle}]\!]\rho'.$$

By the induction hypothesis,

$$(W', {}^{\rho_1'(\tau')}\mathcal{FC}\ \mathbf{v_{1f}}\ \overline{[\hat{\tau}_1^{\langle \mathcal{C} \rangle}]}\ \mathbf{v_{1env}}, \overline{\hat{\mathbf{v}}_1}, {}^{\rho_2'(\tau')}\mathcal{FC}\ \mathbf{v_{2f}}\ \overline{[\hat{\tau}_2^{\langle \mathcal{C} \rangle}]}\ \mathbf{v_{2env}}, \overline{\hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho'.$$

By Lemma 8.15, it suffices to show for $i = 1, 2$ that

$$\langle M_i \mid \mathsf{v}_i\ \overline{[\hat{\tau}_i]}\ \overline{\hat{\mathsf{v}}_i} \rangle \longmapsto^* \langle M_i \mid {}^{\rho_i'(\tau')}\mathcal{FC}\ \mathbf{v_{if}}\ \overline{[\hat{\tau}_i^{\langle \mathcal{C} \rangle}]}\ \mathbf{v_{ienv}}, \overline{\hat{\mathbf{v}}_i} \rangle.$$

To show this, note by the translation definitions that

$$\mathsf{v}_i = \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).{}^{\rho_i(\tau')}\mathcal{FC}\ (\mathbf{unpack}\ \langle \boldsymbol{\beta}, \mathbf{y} \rangle = \mathbf{v_i}\ \mathbf{in}\ \boldsymbol{\pi}_\mathbf{1}(\mathbf{y})\ \overline{[\lceil \alpha \rceil]}\ \boldsymbol{\pi}_\mathbf{2}(\mathbf{y}), \overline{\mathcal{CF}^{\rho_i(\tau)}\,\mathsf{x}}).$$

Thus we have

$$\begin{aligned}
& \langle M_i \mid \mathsf{v}_i\ \overline{[\hat{\tau}_i]}\ \overline{\hat{\mathsf{v}}_i} \rangle \\
\longmapsto\ & \langle M_i \mid {}^{\rho_i'(\tau')}\mathcal{FC}\ (\mathbf{unpack}\ \langle \boldsymbol{\beta}, \mathbf{y} \rangle = \mathbf{v_i}\ \mathbf{in}\ \boldsymbol{\pi}_\mathbf{1}(\mathbf{y})\ \overline{[\hat{\tau}_i^{\langle \mathcal{C} \rangle}]}\ \boldsymbol{\pi}_\mathbf{2}(\mathbf{y}), \overline{\mathcal{CF}^{\rho_i'(\tau)}\,\hat{\mathsf{v}}_i}) \rangle \\
\longmapsto^*\ & \langle M_i \mid {}^{\rho_i'(\tau')}\mathcal{FC}\ (\mathbf{v_{if}}\ \overline{[\hat{\tau}_i^{\langle \mathcal{C} \rangle}]}\ \mathbf{v_{ienv}}, \overline{\mathcal{CF}^{\rho_i'(\tau)}\,\hat{\mathsf{v}}_i}) \rangle \\
\longmapsto^*\ & \langle M_i \mid {}^{\rho_i'(\tau')}\mathcal{FC}\ (\mathbf{v_{if}}\ \overline{[\hat{\tau}_i^{\langle \mathcal{C} \rangle}]}\ \mathbf{v_{ienv}}, \overline{\hat{\mathbf{v}}_i}) \rangle,
\end{aligned}$$

as desired.

For part (b), recall that

$$\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle \mathcal{C} \rangle} = \exists\boldsymbol{\beta}.\langle \boldsymbol{\tau}_\mathbf{f}, \boldsymbol{\beta} \rangle, \quad \text{where} \quad \boldsymbol{\tau}_\mathbf{f} = \forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\beta}, \overline{\tau^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]}) \to \tau'^{\langle \mathcal{C} \rangle}\overline{[\boldsymbol{\alpha}/\lceil \alpha \rceil]}.$$

By inspection of the translations,

$$\mathbf{v_1} = \mathbf{pack}\langle \mathbf{unit}, \langle \mathbf{v_1'}, () \rangle \rangle\ \mathbf{as}\ \exists\boldsymbol{\beta}.\langle \rho_1(\boldsymbol{\tau}_\mathbf{f}), \boldsymbol{\beta} \rangle \quad \text{and} \quad \mathbf{v_2} = \mathbf{pack}\langle \mathbf{unit}, \langle \mathbf{v_2'}, () \rangle \rangle\ \mathbf{as}\ \exists\boldsymbol{\beta}.\langle \rho_2(\boldsymbol{\tau}_\mathbf{f}), \boldsymbol{\beta} \rangle,$$

where

$$\mathbf{v_1'} = \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\mathbf{z} : \mathbf{unit}, \overline{\mathbf{x} : \rho_1(\tau)^{\langle \mathcal{C} \rangle}[\boldsymbol{\alpha}/\lceil \alpha \rceil]}).\mathcal{CF}^{\rho_1(\tau')\overline{[\mathsf{L}\langle \alpha \rangle/\alpha]}}\ \mathsf{v}_1\ \overline{[\mathsf{L}\langle \alpha \rangle]}\ {}^{\overline{\rho_1(\tau)[\mathsf{L}\langle \alpha \rangle/\alpha]}}\mathcal{FC}\ \mathbf{x}$$

and

$$\mathbf{v_2'} = \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\mathbf{z}:\mathbf{unit}, \overline{\mathbf{x}:\rho_2(\tau)^{\langle \mathcal{C}\rangle}\,\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}}).\mathcal{CF}^{\rho_2(\tau')\overline{[\mathsf{L}\langle\alpha\rangle/\alpha]}}\,\mathsf{v}_2\,\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle]}\,\overline{\rho_2(\tau)\overline{[\mathsf{L}\langle\alpha\rangle/\alpha]}\mathcal{FC}\,\mathbf{x}}.$$

Let

$$\mathrm{VR} = (\mathbf{unit}, \mathbf{unit}, \{(W, (), ()) \mid W \in \mathrm{World}\}, \{(W, (), ()) \mid W \in \mathrm{World}\}).$$

Clearly, $\mathrm{VR} \in \mathrm{CValRel}$. It suffices to prove that

$$(W, \mathbf{v_1'}, \mathbf{v_2'}) \in \mathcal{V}[\![\boldsymbol{\tau_f}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}].$$

To do this, let $W' \sqsupseteq W$, $\overline{\mathrm{VR}' \in \mathrm{CValRel}}$, $\rho' = \rho[\boldsymbol{\beta} \mapsto \mathrm{VR}]\overline{[\boldsymbol{\alpha} \mapsto \mathrm{VR}']}$, and

$$\overline{(W', \hat{\mathbf{v}}_\mathbf{1}, \hat{\mathbf{v}}_\mathbf{2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho' = \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}]\overline{[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}'\rangle]}}.$$

For convenience, also let $\overline{\hat{\boldsymbol{\tau}}_\mathbf{1} = \mathrm{VR}'.\boldsymbol{\tau_1}}$ and $\overline{\hat{\boldsymbol{\tau}}_\mathbf{2} = \mathrm{VR}'.\boldsymbol{\tau_2}}$. We need to show that

$$(W', \mathbf{v_1'}\,\overline{[\hat{\boldsymbol{\tau}}_\mathbf{1}]}\,\overline{\hat{\mathbf{v}}_\mathbf{1}}, \mathbf{v_2'}\,\overline{[\hat{\boldsymbol{\tau}}_\mathbf{2}]}\,\overline{\hat{\mathbf{v}}_\mathbf{2}}) \in \mathcal{E}[\![\tau'^{\langle\mathcal{C}\rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho'.$$

Recall that $\mathcal{E}[\![\tau'^{\langle\mathcal{C}\rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho' = \mathcal{E}[\![\tau'^{\langle\mathcal{C}\rangle}]\!]\rho[\boldsymbol{\beta} \mapsto \mathrm{VR}]\overline{[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}'\rangle]}$. By Lemma 8.3, there are some $\overline{\hat{\mathsf{v}}_1}$ and $\overline{\hat{\mathsf{v}}_2}$ such that

$$\overline{\rho_1'(\tau)\mathbf{FC}(\hat{\mathbf{v}}_\mathbf{1}, M_\mathbf{1}) = (\hat{\mathsf{v}}_1, M_1)} \quad \text{and} \quad \overline{\rho_2'(\tau)\mathbf{FC}(\hat{\mathbf{v}}_\mathbf{2}, M_\mathbf{2}) = (\hat{\mathsf{v}}_2, M_2)}.$$

By the induction hypothesis, $\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho'}$. Instantiating $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\forall\overline{[\alpha]}.(\overline{\tau}) \to \tau']\!]\rho$, we have that

$$(W', \mathsf{v}_1\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{1}\rangle]}\,\overline{\hat{\mathsf{v}}_1}, \mathsf{v}_2\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{2}\rangle]}\,\overline{\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho\overline{[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}'\rangle]}.$$

By the induction hypothesis,

$$(W', \mathcal{CF}^{\rho_1'(\tau')}\,\mathsf{v}_1\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{1}\rangle]}\,\overline{\hat{\mathsf{v}}_1}, \mathcal{CF}^{\rho_2'(\tau')}\,\mathsf{v}_2\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{2}\rangle]}\,\overline{\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau'^{\langle\mathcal{C}\rangle}]\!]\rho\overline{[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}'\rangle]}.$$

By Lemmas 8.22 and 8.33,

$$(W', \mathcal{CF}^{\rho_1'(\tau')}\,\mathsf{v}_1\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{1}\rangle]}\,\overline{\hat{\mathsf{v}}_1}, \mathcal{CF}^{\rho_2'(\tau')}\,\mathsf{v}_2\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{2}\rangle]}\,\overline{\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau'^{\langle\mathcal{C}\rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho'.$$

By Lemma 8.15, it suffices to show for $i = 1, 2$ that

$$\langle M_i \mid \mathbf{v_i'}\,\overline{[\hat{\boldsymbol{\tau}}_\mathbf{i}]}\,\overline{\hat{\mathbf{v}}_\mathbf{i}}\rangle \longmapsto^* \langle M_i \mid \mathcal{CF}^{\rho_1'(\tau')}\,\mathsf{v}_1\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{1}\rangle]}\,\overline{\hat{\mathsf{v}}_1}\rangle.$$

By inspection of the operational semantics, we have

$$\begin{aligned} & \langle M_i \mid \mathbf{v_i'}\,\overline{[\hat{\boldsymbol{\tau}}_\mathbf{i}]}\,\overline{\hat{\mathbf{v}}_\mathbf{i}}\rangle \\ \longmapsto\ & \langle M_i \mid \mathcal{CF}^{\rho_i'(\tau')}\,\mathsf{v}_i\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{i}\rangle]}\,\overline{\rho_i'(\tau)\mathcal{FC}\,\hat{\mathbf{v}}_\mathbf{i}}\rangle \\ \longmapsto^*\ & \langle M_i \mid \mathcal{CF}^{\rho_i'(\tau')}\,\mathsf{v}_i\,\overline{[\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{i}\rangle]}\,\overline{\hat{\mathsf{v}}_\mathbf{i}}\rangle, \end{aligned}$$

as desired.

Case $\exists\alpha.\tau$

For part (a), we have $\mathbf{v_1} = \mathbf{pack}\langle\hat{\boldsymbol{\tau}}_\mathbf{1}, \hat{\mathbf{v}}_\mathbf{1}\rangle\,\mathbf{as}\,\rho_1(\exists\alpha.\tau^{\langle\mathcal{C}\rangle})$, $\mathbf{v_2} = \mathbf{pack}\langle\hat{\boldsymbol{\tau}}_\mathbf{2}, \hat{\mathbf{v}}_\mathbf{2}\rangle\,\mathbf{as}\,\rho_2(\exists\alpha.\tau^{\langle\mathcal{C}\rangle})$, and that there is some $\mathrm{VR} \in \mathrm{CValRel}$ such that $\mathrm{VR}.\boldsymbol{\tau_1} = \hat{\boldsymbol{\tau}}_\mathbf{1}$, $\mathrm{VR}.\boldsymbol{\tau_2} = \hat{\boldsymbol{\tau}}_\mathbf{2}$, and

$$(W, \hat{\mathbf{v}}_\mathbf{1}, \hat{\mathbf{v}}_\mathbf{2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}\overline{[\boldsymbol{\alpha}/\lceil\alpha\rceil]}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}]\!]\rho[\alpha \mapsto \mathsf{L}\langle\mathrm{VR}\rangle].$$

By inspection of the translations,

$$\mathsf{v}_1 = \mathsf{pack}\langle\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{1}\rangle, \hat{\mathsf{v}}_1\rangle\,\mathsf{as}\,\rho_1(\exists\alpha.\tau) \quad \text{and} \quad \mathsf{v}_2 = \mathsf{pack}\langle\mathsf{L}\langle\hat{\boldsymbol{\tau}}_\mathbf{2}\rangle, \hat{\mathsf{v}}_2\rangle\,\mathsf{as}\,\rho_2(\exists\alpha.\tau),$$

where

$$\mathbf{FC}^{\rho_1(\tau)[\mathsf{L}\langle\hat{\tau}_1\rangle/\alpha]}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1) \quad \text{and} \quad \mathbf{FC}^{\rho_1(\tau)[\mathsf{L}\langle\hat{\tau}_2\rangle/\alpha]}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2).$$

By the induction hypothesis,

$$(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathsf{L}\langle \mathrm{VR}\rangle].$$

We can use $\mathsf{L}\langle \mathrm{VR}\rangle$ to instantiate the definition of $\mathcal{V}[\![\exists\alpha.\tau]\!]\rho$ and reach the result.
Part (b) is similar: we have $\mathsf{v}_1 = \mathsf{pack}\langle\hat{\tau}_1,\hat{\mathsf{v}}_1\rangle \,\mathsf{as}\, \rho_1(\exists\alpha.\tau)$, $\mathsf{v}_2 = \mathsf{pack}\langle\hat{\tau}_2,\hat{\mathsf{v}}_2\rangle \,\mathsf{as}\, \rho_2(\exists\alpha.\tau)$, and that there is some $\mathrm{VR} \in \mathrm{FValRel}$ such that $\mathrm{VR}.\tau_1 = \hat{\tau}_1$, $\mathrm{VR}.\tau_2 = \hat{\tau}_2$, and

$$(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}].$$

By inspection of the translations,

$$\mathbf{v_1} = \mathbf{pack}\langle\hat{\tau}_1{}^{\langle\mathcal{C}\rangle},\hat{\mathbf{v}}_1\rangle \,\mathbf{as}\, \rho_1(\exists\alpha.\tau^{\langle\mathcal{C}\rangle}) \quad \text{and} \quad \mathbf{v_2} = \mathbf{pack}\langle\hat{\tau}_2{}^{\langle\mathcal{C}\rangle},\hat{\mathbf{v}}_2\rangle \,\mathbf{as}\, \rho_2(\exists\alpha.\tau^{\langle\mathcal{C}\rangle}),$$

where

$$\mathbf{CF}^{\tau[\hat{\tau}_1/\alpha]}(\hat{\mathsf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1) \quad \text{and} \quad \mathbf{CF}^{\tau[\hat{\tau}_2/\alpha]}(\hat{\mathsf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2).$$

By the induction hypothesis and Lemma 8.28,

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathcal{FC}\mathrm{VR}].$$

We now instantiate $\mathcal{V}[\![\exists\alpha.\tau^{\langle\mathcal{C}\rangle}]\!]\rho$ with $\mathcal{FC}\mathrm{VR}$ to complete the proof.

Case $\mu\alpha.\tau$

For part (a), we have $\mathbf{v_1} = \mathbf{fold}_{\rho_1(\mu\alpha.\tau^{\langle\mathcal{C}\rangle})}\,\hat{\mathbf{v}}_1$, $\mathbf{v_2} = \mathbf{fold}_{\rho_2(\mu\alpha.\tau^{\langle\mathcal{C}\rangle})}\,\hat{\mathbf{v}}_2$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright\mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil][\boldsymbol{\mu\alpha.\tau/\alpha}]]\!]\rho. = \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]^{\langle\mathcal{C}\rangle}]\!]\rho$$

By inspection of the translations,

$$\mathsf{v}_1 = \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\,\hat{\mathsf{v}}_1 \quad \text{and} \quad \mathsf{v}_2 = \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\,\hat{\mathsf{v}}_2,$$

where

$$\mathbf{FC}^{\rho_1(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1) \quad \text{and} \quad \mathbf{FC}^{\rho_2(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathsf{v}}_2, M_2).$$

By the induction hypothesis,

$$(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho,$$

which is sufficient to prove $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mu\alpha.\tau]\!]\rho$.
Part (b) is similar: we have $\mathsf{v}_1 = \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\,\hat{\mathsf{v}}_1$, $\mathsf{v}_2' = \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\,\hat{\mathsf{v}}_2$, and

$$(W, \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

By inspection of the translations,

$$\mathbf{v_1} = \mathbf{fold}_{\rho_1(\mu\alpha.\tau^{\langle\mathcal{C}\rangle})}\,\hat{\mathbf{v}}_1 \quad \text{and} \quad \mathbf{v_2} = \mathbf{fold}_{\rho_2(\mu\alpha.\tau^{\langle\mathcal{C}\rangle})}\,\hat{\mathbf{v}}_2,$$

where

$$\mathbf{CF}^{\rho_1(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathsf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1) \quad \text{and} \quad \mathbf{CF}^{\rho_2(\tau[\mu\alpha.\tau/\alpha])}(\hat{\mathsf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2).$$

By the induction hypothesis,

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]^{\langle\mathcal{C}\rangle}]\!]\rho = \triangleright\mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}[\boldsymbol{\alpha}/\lceil\alpha\rceil][\boldsymbol{\mu\alpha.\tau/\alpha}]]\!]\rho.$$

This completes the proof.

Case $\langle\overline{\tau}\rangle$

By definition of the value translations and the induction hypothesis.

Case $\mathsf{L}\langle\tau\rangle$

Follows immediately from the definitions of $\mathcal{V}[\![\mathsf{L}\langle\tau\rangle]\!]\rho$ and the translation rules for lumps.

□

Lemma 10.2
Let $\rho \in \mathcal{D}[\![\Delta]\!]$ and $\Delta \vdash \tau$.

1. (a) If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$, then $(W, {}^{\rho_1(\tau)}\mathcal{CA}\,\mathbf{e_1}, {}^{\rho_2(\tau)}\mathcal{CA}\,\mathbf{e_2}) \in \mathcal{E}[\![\tau]\!]\rho$.
   (b) If $(W, \mathbf{e_1}, \mathbf{e_2}) \in \mathcal{E}[\![\tau]\!]\rho$, then $(W, \mathcal{AC}^{\rho_1(\tau)}\,\mathbf{e_1}, \mathcal{AC}^{\rho_2(\tau)}\,\mathbf{e_2}) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$.
2. (a) $\mathcal{CA}(\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho) \subseteq \mathcal{V}[\![\tau]\!]\rho$.
   (b) $\mathcal{AC}(\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho) \subseteq \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$.

Proof

We can restate claim (2) as follows:

(a) If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$, $(M_1, M_2) : W$,

$$ {}^{\rho_1(\tau)}\mathbf{CA}(\mathbf{v_1}, M_1) = (\mathbf{v_1}, M_1), \quad \text{and} \quad {}^{\rho_2(\tau)}\mathbf{CA}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2), $$

then $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$.

(b) If $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$, $(M_1, M_2) : W$,

$$ \mathbf{AC}^{\rho_1(\tau)}(\mathbf{v_1}, M_1) = (\mathbf{v_1}, M_1 \uplus M_1'), \quad \text{and} \quad \mathbf{AC}^{\rho_2(\tau)}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2'), $$

then $(W \boxplus (M_1', M_2'), \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$.

We prove all the claims simultaneously by induction on $W.k$ and the structure of τ.
For claim (1), let $W' \sqsupseteq_{\text{pub}} W$, $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho$, and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho$. Note that

$$ (W, {}^{\rho_1(\tau)}\mathcal{CA}\,[\cdot], {}^{\rho_2(\tau)}\mathcal{CA}\,[\cdot]) \in \text{ContAtom}[\tau^{\langle\mathcal{A}\rangle}]\rho \rightsquigarrow [\tau]\rho $$

and

$$ (W, \mathcal{AC}^{\rho_1(\tau)}\,[\cdot], \mathcal{AC}^{\rho_2(\tau)}\,[\cdot]) \in \text{ContAtom}[\tau]\rho \rightsquigarrow [\tau^{\langle\mathcal{A}\rangle}]\rho. $$

By Lemma 8.20, for part (a) it suffices to show that

$$ (W', {}^{\rho_1(\tau)}\mathcal{CA}\,\mathbf{v_1}, {}^{\rho_2(\tau)}\mathcal{CA}\,\mathbf{v_2}) \in \mathcal{E}[\![\tau]\!]\rho, $$

and for part (b) it suffices to show that

$$ (W', \mathcal{AC}^{\rho_1(\tau)}\,\mathbf{v_1}, \mathcal{AC}^{\rho_2(\tau)}\,\mathbf{v_2}) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho. $$

But by Lemma 8.3, for any $(M_1, M_2) : W$, there exist $\mathbf{v_1'}$, $\mathbf{v_2'}$, $\mathbf{v_1'}$, and $\mathbf{v_2'}$ such that

$$ \langle M_1 \mid {}^{\rho_1(\tau)}\mathcal{CA}\,\mathbf{v_1}\rangle \longmapsto \langle M_1 \mid \mathbf{v_1'}\rangle \qquad \langle M_2 \mid {}^{\rho_2(\tau)}\mathcal{CA}\,\mathbf{v_2}\rangle \longmapsto \langle M_2 \mid \mathbf{v_2'}\rangle $$
$$ \langle M_1 \mid \mathcal{AC}^{\rho_1(\tau)}\,\mathbf{v_1}\rangle \longmapsto \langle M_1 \uplus M_1' \mid \mathbf{v_1'}\rangle \qquad \langle M_2 \mid \mathcal{AC}^{\rho_2(\tau)}\,\mathbf{v_2}\rangle \longmapsto \langle M_2 \uplus M_2' \mid \mathbf{v_2'}\rangle. $$

So by Lemma 8.15, Lemma 8.9, and claim (2), we have the result.
For claim (2), we consider the possible cases of τ:

Case α

Since $\rho(\alpha) \in \text{CValRel}$, we have this immediately.

Case $\mathbf{unit}$

Immediate.

Case $\mathbf{int}$

Immediate.

Case $\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$

For part (a), let $W' \sqsupseteq W$, $\overline{\mathrm{VR} \in \mathrm{CValRel}}$, and $\overline{(W', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]}$. For convenience, also let $\overline{\hat{\tau}_1 = \mathrm{VR}.\tau_1}$, $\overline{\hat{\tau}_2 = \mathrm{VR}.\tau_2}$, and $\rho' = \rho[\overline{\alpha \mapsto \mathrm{VR}}]$. We need to show that

$$(W', \mathbf{v}_1\ [\overline{\hat{\tau}_1}]\ \overline{\hat{\mathbf{v}}_1}, \mathbf{v}_2\ [\overline{\hat{\tau}_2}]\ \overline{\hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho'.$$

By our assumption,

$$\mathbf{v}_1 = \ell_1[\overline{\tau_1^*}], \qquad M_1(\ell_1) = \lambda[\overline{\beta_1}, \overline{\alpha}](\overline{\mathbf{x} : \tau_1}).\mathbf{t}_1, \qquad \overline{\overline{\tau_1[\tau_1^*/\beta_1]} = \rho_1(\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil])},$$
$$\mathbf{v}_2 = \ell_2[\overline{\tau_2^*}], \qquad M_2(\ell_2) = \lambda[\overline{\beta_1}, \overline{\alpha}](\overline{\mathbf{x} : \tau_2}).\mathbf{t}_2, \qquad \overline{\overline{\tau_2[\tau_2^*/\beta_2]} = \rho_2(\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil])},$$

and

$$(W, \lambda[\overline{\alpha}](\overline{\mathbf{x} : \rho_1(\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil])}).\mathbf{t}_1[\overline{\tau_1^*/\beta_1}], \lambda[\overline{\alpha}](\overline{\mathbf{x} : \rho_2(\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil])}).\mathbf{t}_2[\overline{\tau_2^*/\beta_2}])$$
$$\in \mathcal{HV}[\![\forall[\overline{\alpha}].(\overline{\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}) \to \tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho.$$

Let $(M_1', M_2') : W'$. By Lemma 8.3 and the induction hypothesis, there are some $\overline{\hat{\mathbf{v}}_1}$ and $\overline{\hat{\mathbf{v}}_2}$ such that $\overline{\mathbf{AC}^{\hat{\tau}_1}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1 \uplus M_{1i}')}$, $\overline{\mathbf{AC}^{\hat{\tau}_2}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2 \uplus M_{2i}')}$, and

$$\overline{(W' \boxplus (M_1', M_2'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho' = \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathcal{AC}\mathrm{VR}]},$$

where $M_1' = \biguplus M_{1i}'$ and $M_2' = \biguplus M_{2i}'$. Instantiating the previous fact with this, we get

$$(W' \boxplus (M_1', M_2'), \mathbf{t}_1[\overline{\tau_1^*/\beta_1}][\overline{\hat{\tau}_1{}^{\langle\mathcal{A}\rangle}/\alpha}][\overline{\hat{\mathbf{v}}_1/\mathbf{x}}], \mathbf{t}_2[\overline{\tau_2^*/\beta_2}][\overline{\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}/\alpha}][\overline{\hat{\mathbf{v}}_2/\mathbf{x}}])$$
$$\in \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathcal{CAVR}] = \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}]\!]\rho'.$$

By the induction hypothesis,

$$(W' \boxplus (M_1', M_2'), {}^{\rho_1'(\tau')}\mathcal{CA}\,\mathbf{t}_1[\overline{\tau_1^*/\beta_1}][\overline{\hat{\tau}_1{}^{\langle\mathcal{A}\rangle}/\alpha}][\overline{\hat{\mathbf{v}}_1/\mathbf{x}}], {}^{\rho_2'(\tau')}\mathcal{CA}\,\mathbf{t}_2[\overline{\tau_2^*/\beta_2}][\overline{\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}/\alpha}][\overline{\hat{\mathbf{v}}_2/\mathbf{x}}])$$
$$\in \mathcal{E}[\![\tau']\!]\rho'.$$

By Lemma 8.15, it suffices to show for $i = 1, 2$ that

$$\langle M_i \mid \mathbf{v_i}\ [\overline{\hat{\tau}_i}]\ \overline{\hat{\mathbf{v}}_i}\rangle \longmapsto^* \langle M_i \uplus M_i' \mid {}^{\rho_i'(\tau')}\mathcal{CA}\,\mathbf{t_i}[\overline{\tau_i^*/\beta_i}][\overline{\hat{\tau}_i{}^{\langle\mathcal{A}\rangle}/\alpha}][\overline{\hat{\mathbf{v}}_i/\mathbf{x}}]\rangle.$$

To show this, note by the translation definitions that

$$\mathbf{v_i} = \lambda[\overline{\alpha}](\overline{\mathbf{x} : \tau}).{}^{\rho_i(\tau')}\mathcal{CA}\,\mathbf{v_i}\ [\overline{\lceil\alpha\rceil}]\ \overline{\mathcal{AC}^{\rho_i(\tau)}\,\mathbf{x}}.$$

Thus we have

$$\begin{aligned}
&\langle M_i \mid \mathbf{v_i}\ [\overline{\hat{\tau}_i}]\ \overline{\hat{\mathbf{v}}_i}\rangle \\
\longmapsto\ &\langle M_i \mid {}^{\rho_i'(\tau')}\mathcal{CA}\,\mathbf{v_i}\ [\overline{\hat{\tau}_i{}^{\langle\mathcal{A}\rangle}}]\ \overline{\mathcal{AC}^{\rho_i'(\tau)}\,\hat{\mathbf{v}}_i}\rangle \\
\longmapsto^*\ &\langle M_i \mid {}^{\rho_i'(\tau')}\mathcal{CA}\,(\mathbf{v_i}\ [\overline{\hat{\tau}_i{}^{\langle\mathcal{A}\rangle}}]\ \overline{\hat{\mathbf{v}}_i})\rangle \\
\longmapsto^*\ &\langle M_i \mid {}^{\rho_i'(\tau')}\mathcal{CA}\,\mathbf{t_i}[\overline{\tau_i^*/\beta_i}][\overline{\hat{\tau}_i{}^{\langle\mathcal{A}\rangle}/\alpha}][\overline{\hat{\mathbf{v}}_i/\mathbf{x}}]\rangle,
\end{aligned}$$

as desired.

For part (b), recall that

$$\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'^{\langle\mathcal{A}\rangle} = \mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}) \to \tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil].$$

By inspection of the translations, $\mathbf{v_1} = \ell_1$ and $\mathbf{v_2} = \ell_2$, where

$$M_1'(\ell_1) = \mathbf{h_1} = \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}\colon \rho_1(\tau)^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}).\mathcal{AC}^{\rho_1(\tau')[\mathbf{L}\langle\alpha\rangle/\alpha]}\,\mathbf{v_1}\,[\overline{\mathbf{L}\langle\alpha\rangle}]\;\overline{{}^{\rho_1(\tau)[\mathbf{L}\langle\alpha\rangle/\alpha]}\mathcal{CA}\,\mathbf{x}}$$

and

$$M_2'(\ell_2) = \mathbf{h_2} = \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}\colon \rho_2(\tau)^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}).\mathcal{AC}^{\rho_2(\tau')[\mathbf{L}\langle\alpha\rangle/\alpha]}\,\mathbf{v_2}\,[\overline{\mathbf{L}\langle\alpha\rangle}]\;\overline{{}^{\rho_2(\tau)[\mathbf{L}\langle\alpha\rangle/\alpha]}\mathcal{CA}\,\mathbf{x}}.$$

It suffices to prove that

$$(W \boxplus (M_1', M_2'), \mathbf{h_1}, \mathbf{h_2}) \in \mathcal{HV}[\![\forall[\overline{\alpha}].(\overline{\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]}) \to \tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho.$$

To do this, let $W' \sqsupseteq W \boxplus (M_1', M_2')$, $\overline{\mathrm{VR}' \in \mathrm{AValRel}}$, and

$$\overline{(W', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}']} = \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}'\rangle].$$

For convenience, also let $\overline{\hat{\tau}_1 = \mathrm{VR}'.\tau_1}$ and $\overline{\hat{\tau}_2 = \mathrm{VR}'.\tau_2}$. We need to show that

$$\begin{aligned}(W', &\mathcal{AC}^{\rho_1(\tau')[\mathbf{L}\langle\alpha\rangle/\alpha]}\,\mathbf{v_1}\,[\overline{\mathbf{L}\langle\hat{\tau}_1\rangle}]\;\overline{{}^{\rho_1(\tau)[\mathbf{L}\langle\hat{\tau}_1\rangle/\alpha]}\mathcal{CA}\,\hat{\mathbf{v}}_1},\\ &\mathcal{AC}^{\rho_2(\tau')[\mathbf{L}\langle\alpha\rangle/\alpha]}\,\mathbf{v_2}\,[\overline{\mathbf{L}\langle\hat{\tau}_2\rangle}]\;\overline{{}^{\rho_2(\tau)[\mathbf{L}\langle\hat{\tau}_2\rangle/\alpha]}\mathcal{CA}\,\hat{\mathbf{v}}_2})\\ &\qquad\qquad\in \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho\overline{[\alpha \mapsto \mathrm{VR}']} = \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}]\!]\rho\overline{[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}'\rangle]}.\end{aligned}$$

By Lemma 8.3, there are some $\overline{\hat{\mathbf{v}}_1}$ and $\overline{\hat{\mathbf{v}}_2}$ such that

$$\overline{{}^{\rho_1'(\tau)}\mathbf{CA}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1)} \quad\text{and}\quad \overline{{}^{\rho_2'(\tau)}\mathbf{CA}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2)}.$$

By the induction hypothesis, $\overline{(W', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle']}$. Instantiating

$$(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho,$$

we have that

$$(W', \mathbf{v_1}\,[\overline{\mathbf{L}\langle\hat{\tau}_1\rangle}]\;\overline{\hat{\mathbf{v}}_1}, \mathbf{v_2}\,[\overline{\mathbf{L}\langle\hat{\tau}_2\rangle}]\;\overline{\hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho\overline{[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}'\rangle]}.$$

By the induction hypothesis,

$$(W', \mathcal{AC}^{\rho_1'(\tau')}\,\mathbf{v_1}\,[\overline{\mathbf{L}\langle\hat{\tau}_1\rangle}]\;\overline{\hat{\mathbf{v}}_1}, \mathcal{AC}^{\rho_2'(\tau')}\,\mathbf{v_2}\,[\overline{\mathbf{L}\langle\hat{\tau}_2\rangle}]\;\overline{\hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\tau'^{\langle\mathcal{A}\rangle}]\!]\rho\overline{[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}'\rangle]}.$$

The result follows by Lemma 8.15.

Case $\exists\boldsymbol{\alpha}.\boldsymbol{\tau}$

For part (a), we have $\mathbf{v_1} = \mathbf{pack}\langle\hat{\tau}_1,\hat{\mathbf{v}}_1\rangle\,\mathbf{as}\,\rho_1(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}^{\langle\mathcal{A}\rangle})$, $\mathbf{v_2} = \mathbf{pack}\langle\hat{\tau}_2,\hat{\mathbf{v}}_2\rangle\,\mathbf{as}\,\rho_2(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}^{\langle\mathcal{A}\rangle})$, and that there is some $\mathrm{VR} \in \mathrm{AValRel}$ such that $\mathrm{VR}.\tau_1 = \hat{\tau}_1$, $\mathrm{VR}.\tau_2 = \hat{\tau}_2$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}[\alpha/\lceil\alpha\rceil]]\!]\rho[\alpha \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle].$$

By inspection of the translations,

$$\mathbf{v_1} = \mathbf{pack}\langle\mathbf{L}\langle\hat{\tau}_1\rangle,\hat{\mathbf{v}}_1\rangle\,\mathbf{as}\,\rho_1(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}) \quad\text{and}\quad \mathbf{v_2} = \mathbf{pack}\langle\mathbf{L}\langle\hat{\tau}_2\rangle,\hat{\mathbf{v}}_2\rangle\,\mathbf{as}\,\rho_2(\exists\boldsymbol{\alpha}.\boldsymbol{\tau}),$$

where

$${}^{\rho_1(\tau)[\mathbf{L}\langle\hat{\tau}_1\rangle/\alpha]}\mathbf{CA}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1) \quad\text{and}\quad {}^{\rho_1(\tau)[\mathbf{L}\langle\hat{\tau}_2\rangle/\alpha]}\mathbf{CA}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2).$$

By the induction hypothesis,

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\boldsymbol{\alpha} \mapsto \mathbf{L}\langle\mathrm{VR}\rangle].$$

We can use $\mathbf{L}\langle \mathrm{VR} \rangle$ to instantiate the definition of $\mathcal{V}[\![\exists \boldsymbol{\alpha}.\boldsymbol{\tau}]\!]\rho$ and reach the result.
Part (b) is similar: we have $\mathbf{v_1} = \mathbf{pack}\langle \hat{\tau}_1, \hat{\mathbf{v}}_1 \rangle \mathbf{\ as\ } \rho_1(\exists \boldsymbol{\alpha}.\boldsymbol{\tau})$, $\mathbf{v_2} = \mathbf{pack}\langle \hat{\tau}_2, \hat{\mathbf{v}}_2 \rangle \mathbf{\ as\ } \rho_2(\exists \boldsymbol{\alpha}.\boldsymbol{\tau})$, and that there is some $\mathrm{VR} \in \mathrm{CValRel}$ such that $\mathrm{VR}.\boldsymbol{\tau_1} = \hat{\tau}_1$, $\mathrm{VR}.\boldsymbol{\tau_2} = \hat{\tau}_2$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}].$$

By inspection of the translations,

$$\mathbf{v_1} = \mathbf{pack}\langle \hat{\tau}_1{}^{\langle \mathcal{A} \rangle}, \hat{\mathbf{v}}_1 \rangle \mathbf{\ as\ } \rho_1(\exists \boldsymbol{\alpha}.\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}) \quad \text{and} \quad \mathbf{v_2} = \mathbf{pack}\langle \hat{\tau}_2{}^{\langle \mathcal{A} \rangle}, \hat{\mathbf{v}}_2 \rangle \mathbf{\ as\ } \rho_2(\exists \boldsymbol{\alpha}.\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}),$$

where

$$\mathbf{AC}^{\boldsymbol{\tau}[\hat{\tau}_1/\boldsymbol{\alpha}]}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1 \uplus M_1') \quad \text{and} \quad \mathbf{AC}^{\boldsymbol{\tau}[\hat{\tau}_2/\boldsymbol{\alpha}]}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2 \uplus M_2').$$

By the induction hypothesis and Lemma 8.26,

$$(W \boxplus (M_1', M_2'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}]\!]\rho[\boldsymbol{\alpha} \mapsto \mathrm{VR}] = \mathcal{V}[\![\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}[\boldsymbol{\alpha}/\lceil \boldsymbol{\alpha} \rceil]]\!]\rho[\boldsymbol{\alpha} \mapsto \mathcal{CA}\mathrm{VR}].$$

We now instantiate $\mathcal{V}[\![\exists \boldsymbol{\alpha}.\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}]\!]\rho$ with $\mathcal{CA}\mathrm{VR}$ to complete the proof.

Case $\boldsymbol{\mu\alpha.\tau}$

For part (a), we have $\mathbf{v_1} = \mathbf{fold}_{\rho_1(\boldsymbol{\mu\alpha.\tau}^{\langle \mathcal{A} \rangle})}\ \hat{\mathbf{v}}_1$, $\mathbf{v_2} = \mathbf{fold}_{\rho_2(\boldsymbol{\mu\alpha.\tau}^{\langle \mathcal{A} \rangle})}\ \hat{\mathbf{v}}_2$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright \mathcal{V}[\![\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}[\boldsymbol{\alpha}/\lceil \boldsymbol{\alpha} \rceil][\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}]]\!]\rho. = \triangleright \mathcal{V}[\![\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}]^{\langle \mathcal{A} \rangle}]\!]\rho$$

By inspection of the translations,

$$\mathbf{v_1} = \mathbf{fold}_{\rho_1(\boldsymbol{\mu\alpha.\tau})}\ \hat{\mathbf{v}}_1 \quad \text{and} \quad \mathbf{v_2} = \mathbf{fold}_{\rho_2(\boldsymbol{\mu\alpha.\tau})}\ \hat{\mathbf{v}}_2,$$

where

$${}^{\rho_1(\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}])}\mathbf{CA}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1) \quad \text{and} \quad {}^{\rho_2(\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}])}\mathbf{CA}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2).$$

By the induction hypothesis,

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright \mathcal{V}[\![\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}]]\!]\rho,$$

which is sufficient to prove $(W, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\mu\alpha.\tau}]\!]\rho$.
Part (b) is similar: we have $\mathbf{v_1} = \mathbf{fold}_{\rho_1(\boldsymbol{\mu\alpha.\tau})}\ \hat{\mathbf{v}}_1$, $\mathbf{v_2'} = \mathbf{fold}_{\rho_2(\boldsymbol{\mu\alpha.\tau})}\ \hat{\mathbf{v}}_2$, and

$$(W, \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright \mathcal{V}[\![\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}]]\!]\rho.$$

By inspection of the translations,

$$\mathbf{v_1} = \mathbf{fold}_{\rho_1(\boldsymbol{\mu\alpha.\tau}^{\langle \mathcal{A} \rangle})}\ \hat{\mathbf{v}}_1 \quad \text{and} \quad \mathbf{v_2} = \mathbf{fold}_{\rho_2(\boldsymbol{\mu\alpha.\tau}^{\langle \mathcal{A} \rangle})}\ \hat{\mathbf{v}}_2,$$

where

$$\mathbf{AC}^{\rho_1(\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}])}(\hat{\mathbf{v}}_1, M_1) = (\hat{\mathbf{v}}_1, M_1 \uplus M_1') \quad \text{and} \quad \mathbf{AC}^{\rho_2(\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}])}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2 \uplus M_2').$$

By the induction hypothesis,

$$(W \boxplus (M_1', M_2'), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \triangleright \mathcal{V}[\![\boldsymbol{\tau}[\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}]^{\langle \mathcal{A} \rangle}]\!]\rho = \triangleright \mathcal{V}[\![\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}[\boldsymbol{\alpha}/\lceil \boldsymbol{\alpha} \rceil][\boldsymbol{\mu\alpha.\tau}/\boldsymbol{\alpha}]]\!]\rho.$$

This completes the proof.

Case $\langle \overline{\boldsymbol{\tau}} \rangle$

By definition of the value translations and the induction hypothesis.

Case $\lceil \alpha \rceil$

Since $\rho(\alpha) \in \mathrm{FValRel}$, we have this immediately.

Case $\mathbf{L}\langle \boldsymbol{\tau} \rangle$

Follows immediately from the definitions of $\mathcal{V}[\![\mathbf{L}\langle \boldsymbol{\tau} \rangle]\!]\rho$ and the translation rules for lumps.

□

10.2 Substitution

Lemma 10.3
Let $\rho \in \mathcal{D}[\![\Delta]\!]$.

1. If $\Delta \vdash \tau$, then $\mathcal{V}[\![\tau]\!]\rho \in \mathrm{ValRel}[\rho_1(\tau), \rho_2(\tau)]$ and $\mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho \in \mathrm{TransRel}^{\mathcal{C}}[\rho_1(\tau), \rho_2(\tau)]$.
2. If $\Delta \vdash \boldsymbol{\tau}$, then $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho \in \mathrm{ValRel}[\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau})]$ and $\mathcal{V}[\![\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}]\!]\rho \in \mathrm{TransRel}^{\mathcal{A}}[\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau})]$.
3. If $\Delta \vdash \tau$, then $\mathcal{V}[\![\tau]\!]\rho \in \mathrm{ValRel}[\rho_1(\tau), \rho_2(\tau)]$.

Proof

Follows from monotonicity and boundary cancellation. □

Lemma 10.4
Let $\rho \in \mathcal{D}[\![\Delta]\!]$.

1. If $\Delta \vdash \tau$, then $(\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho, \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho, \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle\langle \mathcal{A} \rangle}]\!]\rho) \in \mathrm{FValRel}$.
2. If $\Delta \vdash \boldsymbol{\tau}$, then $(\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau}), \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho, \mathcal{V}[\![\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}]\!]\rho) \in \mathrm{CValRel}$.
3. If $\Delta \vdash \tau$, then $(\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho) \in \mathrm{AValRel}$.

Proof

Follows from Lemma 10.3 and the bridge lemmas. □

To avoid repetition, for the next three lemmas, let $\rho \in \mathcal{D}[\![\Delta]\!]$, and define the function V as follows:

$$\begin{aligned}
\mathrm{V}(\tau) &= (\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho, \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho, \mathcal{V}[\![\tau^{\langle \mathcal{C} \rangle\langle \mathcal{A} \rangle}]\!]\rho) \\
\mathrm{V}(\boldsymbol{\tau}) &= (\rho_1(\boldsymbol{\tau}), \rho_2(\boldsymbol{\tau}), \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho, \mathcal{V}[\![\boldsymbol{\tau}^{\langle \mathcal{A} \rangle}]\!]\rho) \\
\mathrm{V}(\tau) &= (\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho)
\end{aligned}$$

Note that by Lemma 10.4, $\rho[\alpha \mapsto \mathrm{V}(\tau)] \in \mathcal{D}[\![\Delta, \alpha]\!]$ as long as τ and α are in the same language and $\alpha \notin \Delta$. We assume this is the case for the next three lemmas.

We now state a key set of substitution lemmas:

Lemma 10.5

1. $\mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{V}[\![\tau[\tau/\alpha]]\!]\rho$.
2. $\mathcal{HV}[\![\psi]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{HV}[\![\psi[\tau/\alpha]]\!]\rho$.
3. $\mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{E}[\![\tau[\tau/\alpha]]\!]\rho$
4. $\mathcal{K}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{K}[\![\tau[\tau/\alpha]]\!]\rho$.

Proof

Follows the induction structure of Lemma 8.21. The base cases (for type variables and suspensions) follow from the definition of $\mathrm{V}(\tau)$. □

Lemma 10.6

1. $\mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{V}[\![\boldsymbol{\tau}[\tau/\alpha]]\!]\rho$.
2. $\mathcal{E}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{E}[\![\boldsymbol{\tau}[\tau/\alpha]]\!]\rho$
3. $\mathcal{K}[\![\boldsymbol{\tau}]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{K}[\![\boldsymbol{\tau}[\tau/\alpha]]\!]\rho$.

Proof

Follows the induction structure of Lemma 8.22. The base cases (for type variables and suspensions) follow from the definition of $\mathrm{V}(\tau)$. □

Lemma 10.7

1. $\mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{V}[\![\tau[\tau/\alpha]]\!]\rho$.
2. $\mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{E}[\![\tau[\tau/\alpha]]\!]\rho$
3. $\mathcal{K}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{V}(\tau)] = \mathcal{K}[\![\tau[\tau/\alpha]]\!]\rho$.

Proof

Follows the induction structure of Lemma 8.23. The base case (for type variables) follows from the definition of $\mathrm{V}(\tau)$. □

10.3 Compatability Lemmas

Because of the recursive dependence between the relations $\mathcal{E}[\![\tau]\!]\rho$, $\mathcal{V}[\![\tau]\!]\rho$, and $\mathcal{HV}[\![\psi]\!]\rho$, to prove the fundamental property we will need to define relations for open values and heap values:

Definition 10.8 (Logical Relation for Values)

$$\Psi;\Delta;\Gamma \vdash v_1 \approx_{\mathrm{v}} v_2 : \tau \stackrel{\text{def}}{=} \Psi;\Delta;\Gamma \vdash v_1 : \tau \ \wedge \ \Psi;\Delta;\Gamma \vdash v_2 : \tau \ \wedge$$
$$\forall W, \rho, \gamma.\ W \in \mathcal{H}[\![\Psi]\!] \ \wedge \ \rho \in \mathcal{D}[\![\Delta]\!] \ \wedge \ (W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$$
$$\implies (W, \rho_1(\gamma_1(v_1)), \rho_2(\gamma_2(v_2))) \in \mathcal{V}[\![\tau]\!]\rho$$
$$\Psi \vdash \mathsf{h_1} \approx_{\mathrm{hv}} \mathsf{h_2} : \psi \stackrel{\text{def}}{=} \Psi \vdash \mathsf{h_1} : \psi \ \wedge \ \Psi \vdash \mathsf{h_2} : \psi \ \wedge \forall W \in \mathcal{H}[\![\Psi]\!].\ (W, \mathsf{h_1}, \mathsf{h_2}) \in \mathcal{HV}[\![\psi]\!]\emptyset$$

The compatibility lemmas for value forms will have two similar statements: one for the logical relation for terms, and one for the logical relation for values. We will only address the former in the proofs, because the latter can always be shown with a very similar proof.

Lemma 10.9 (F Variable)
If $\mathsf{x} : \tau \in \Gamma$, then $\Psi;\Delta;\Gamma \vdash \mathsf{x} \approx \mathsf{x} : \tau$.

Proof

First note that $\Psi;\Delta;\Gamma \vdash \mathsf{x} : \tau$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By definition of $\mathcal{G}[\![\Gamma]\!]\rho$,

$$(W, \rho_1(\gamma_1(\mathsf{x})), \rho_2(\gamma_2(\mathsf{x}))) = (W, \gamma_1(\mathsf{x}), \gamma_2(\mathsf{x})) \in \mathcal{V}[\![\tau]\!]\rho.$$

Then by Lemma 8.9, $(W, \rho_1(\gamma_1(\mathsf{x})), \rho_2(\gamma_2(\mathsf{x}))) \in \mathcal{E}[\![\tau]\!]\rho$, as desired. □

Lemma 10.10 (F Unit)

- $\Psi;\Delta;\Gamma \vdash () \approx () : \mathsf{unit}$
- $\Psi;\Delta;\Gamma \vdash () \approx_{\mathrm{v}} () : \mathsf{unit}$.

Proof

First note that $\Psi;\Delta;\Gamma \vdash () : \mathsf{unit}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By definition,

$$(W, \rho_1(\gamma_1(()))), \rho_2(\gamma_2(()))) = (W, (), ()) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho.$$

By Lemma 8.9, $(W, \rho_1(\gamma_1(()))), \rho_2(\gamma_2(()))) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho$, as desired. □

Lemma 10.11 (F Int)

- $\Psi; \Delta; \Gamma \vdash \mathsf{n} \approx \mathsf{n} : \mathsf{int}$
- $\Psi; \Delta; \Gamma \vdash \mathsf{n} \approx_{\mathrm{v}} \mathsf{n} : \mathsf{int}$.

Proof

First note that $\Psi; \Delta; \Gamma \vdash \mathsf{n} : \mathsf{int}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By definition,

$$(W, \rho_1(\gamma_1(\mathsf{n})), \rho_2(\gamma_2(\mathsf{n}))) = (W, \mathsf{n}, \mathsf{n}) \in \mathcal{V}[\![\mathsf{int}]\!]\rho.$$

By Lemma 8.9, $(W, \rho_1(\gamma_1(\mathsf{n})), \rho_2(\gamma_2(\mathsf{n}))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho$, as desired. □

Lemma 10.12 (F Primitive)
If $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \mathsf{int}$ and $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1' \approx \mathsf{t}_2' : \mathsf{int}$, then $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1 \ \mathsf{p} \ \mathsf{t}_1' \approx \mathsf{t}_2 \ \mathsf{p} \ \mathsf{t}_2' : \mathsf{int}$.

Proof

First note that $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1 \ \mathsf{p} \ \mathsf{t}_1' : \mathsf{int}$ and $\Psi; \Delta; \Gamma \vdash \mathsf{t}_2 \ \mathsf{p} \ \mathsf{t}_2' : \mathsf{int}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.

We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{t}_1 \ \mathsf{p} \ \mathsf{t}_1')), \rho_2(\gamma_2(\mathsf{t}_2 \ \mathsf{p} \ \mathsf{t}_2'))) = (W, \rho_1(\gamma_1(\mathsf{t}_1)) \ \mathsf{p} \ \rho_1(\gamma_1(\mathsf{t}_1')), \rho_2(\gamma_2(\mathsf{t}_2)) \ \mathsf{p} \ \rho_2(\gamma_2(\mathsf{t}_2'))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho.$$

By assumption, $(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho$ and $(W, \rho_1(\gamma_1(\mathsf{t}_1')), \rho_2(\gamma_2(\mathsf{t}_2'))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho$.

Let $W' \sqsupseteq_{\mathrm{pub}} W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mathsf{int}]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{v}_1 \ \mathsf{p} \ \rho_1(\gamma_1(\mathsf{t}_1')), \mathsf{v}_2 \ \mathsf{p} \ \rho_2(\gamma_2(\mathsf{t}_2'))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho.$$

Let $W'' \sqsupseteq_{\mathrm{pub}} W'$ and $(W', \mathsf{v}_1', \mathsf{v}_2') \in \mathcal{V}[\![\mathsf{int}]\!]\rho$. By another application of Lemma 8.20, it suffices to show that

$$(W'', \mathsf{v}_1 \ \mathsf{p} \ \mathsf{v}_1', \mathsf{v}_2 \ \mathsf{p} \ \mathsf{v}_2') \in \mathcal{E}[\![\mathsf{int}]\!]\rho.$$

But by definition of $\mathcal{V}[\![\mathsf{int}]\!]\rho$, $\mathsf{v}_1 = \mathsf{v}_2 = \mathsf{m}$ and $\mathsf{v}_1' = \mathsf{v}_2' = \mathsf{n}$. For any $(M_1, M_2) : W''$,

$$\langle M_i \mid \mathsf{m} \ \mathsf{p} \ \mathsf{n} \rangle \longmapsto \langle M_i \mid \mathsf{n}' \rangle.$$

By definition, $(W'', \mathsf{n}', \mathsf{n}') \in \mathcal{V}[\![\mathsf{int}]\!]\rho$. So by Lemma 8.9 and Lemma 8.15, we have the result. □

Lemma 10.13 (F If0)
If $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \mathsf{int}$, $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1' \approx \mathsf{t}_2' : \tau$, and $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1'' \approx \mathsf{t}_2'' : \tau$, then

$$\Psi; \Delta; \Gamma \vdash \mathsf{if0} \ \mathsf{t}_1 \ \mathsf{t}_1' \ \mathsf{t}_1'' \approx \mathsf{if0} \ \mathsf{t}_2 \ \mathsf{t}_2' \ \mathsf{t}_2'' : \tau.$$

Proof

First note that $\Psi; \Delta; \Gamma \vdash \mathsf{if0} \ \mathsf{t}_1 \ \mathsf{t}_1' \ \mathsf{t}_1'' : \tau$ and $\Psi; \Delta; \Gamma \vdash \mathsf{if0} \ \mathsf{t}_2 \ \mathsf{t}_2' \ \mathsf{t}_2'' : \tau$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.

We need to show that

$$\begin{aligned}(W, \rho_1(\gamma_1(\mathsf{if0} \ \mathsf{t}_1 \ \mathsf{t}_1' \ \mathsf{t}_1'')), \rho_2(\gamma_2(\mathsf{if0} \ \mathsf{t}_2 \ \mathsf{t}_2' \ \mathsf{t}_2'')))& \\ = (W, \mathsf{if0} \ \rho_1(\gamma_1(\mathsf{t}_1)) \ \rho_1(\gamma_1(\mathsf{t}_1')) \ \rho_1(\gamma_1(\mathsf{t}_1'')), \mathsf{if0} \ \rho_2(\gamma_2(\mathsf{t}_2)) \ \rho_2(\gamma_2(\mathsf{t}_2')) \ \rho_2(\gamma_2(\mathsf{t}_2'')))& \in \mathcal{E}[\![\tau]\!]\rho.\end{aligned}$$

By assumption, $(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho$,

$$(W, \rho_1(\gamma_1(\mathsf{t}_1')), \rho_2(\gamma_2(\mathsf{t}_2'))) \in \mathcal{E}[\![\tau]\!]\rho, \quad \text{and} \quad (W, \rho_1(\gamma_1(\mathsf{t}_1'')), \rho_2(\gamma_2(\mathsf{t}_2''))) \in \mathcal{E}[\![\tau]\!]\rho.$$

Let $W' \sqsupseteq_{\text{pub}} W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mathsf{int}]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{if0}\,\mathsf{v}_1\ \rho_1(\gamma_1(\mathsf{t}_1'))\ \rho_1(\gamma_1(\mathsf{t}_1'')), \mathsf{if0}\,\mathsf{v}_2\ \rho_2(\gamma_2(\mathsf{t}_2'))\ \rho_2(\gamma_2(\mathsf{t}_2''))) \in \mathcal{E}[\![\tau]\!]\rho.$$

By definition of $\mathcal{V}[\![\mathsf{int}]\!]\rho$, $\mathsf{v}_1 = \mathsf{v}_2 = \mathsf{n}$. Depending on whether $\mathsf{n} = \mathsf{0}$, for any $(M_1, M_2) : W'$, either

$$\langle M_i \mid \mathsf{if0}\,\mathsf{v}_i\ \rho_i(\gamma_i(\mathsf{t}_i'))\ \rho_i(\gamma_i(\mathsf{t}_i''))\rangle \longmapsto \langle M_i \mid \rho_i(\gamma_i(\mathsf{t}_i'))\rangle$$

or

$$\langle M_i \mid \mathsf{if0}\,\mathsf{v}_i\ \rho_i(\gamma_i(\mathsf{t}_i'))\ \rho_i(\gamma_i(\mathsf{t}_i''))\rangle \longmapsto \langle M_i \mid \rho_i(\gamma_i(\mathsf{t}_i''))\rangle.$$

Thus, by Lemma 8.15, it suffices to show that

$$(W, \rho_1(\gamma_1(\mathsf{t}_1')), \rho_2(\gamma_2(\mathsf{t}_2'))) \in \mathcal{E}[\![\tau]\!]\rho \quad \text{and} \quad (W, \rho_1(\gamma_1(\mathsf{t}_1'')), \rho_2(\gamma_2(\mathsf{t}_2''))) \in \mathcal{E}[\![\tau]\!]\rho.$$

But we already have these facts, so we are done. □

Lemma 10.14 (F Function)
If $\Psi; (\Delta, \overline{\alpha}); (\Gamma, \overline{\mathsf{x} : \tau}) \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \tau'$, then

- $\Psi; \Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_1 \approx \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_2 : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$
- $\Psi; \Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_1 \approx_{\text{v}} \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_2 : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$.

Proof

First note that $\Psi; \Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_1 : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ and $\Psi; \Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_2 : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$.
Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
We need to show that

$$(W, \rho_1(\gamma_1(\lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_1)), \rho_2(\gamma_2(\lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\mathsf{t}_2))) = (W, \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\rho_1(\gamma_1(\mathsf{t}_1)), \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho.$$

By Lemma 8.9, it suffices to show that

$$(W, \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\rho_1(\gamma_1(\mathsf{t}_1)), \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho.$$

Let $W' \sqsupseteq W$, $\overline{\text{VR} \in \text{FValRel}}$, and $\overline{(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \text{VR}]}$. For convenience, also let $\overline{\tau_1 = \text{VR}.\tau_1}$ and $\overline{\tau_2 = \text{VR}.\tau_2}$ We need to show that

$$(W, \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\rho_1(\gamma_1(\mathsf{t}_1))\ [\overline{\tau_1}]\ \overline{\mathsf{v}_1}, \lambda[\overline{\alpha}](\overline{\mathsf{x} : \tau}).\rho_2(\gamma_2(\mathsf{t}_2))\ [\overline{\tau_2}]\ \overline{\mathsf{v}_2}) \in \mathcal{E}[\![\tau']\!]\rho[\overline{\alpha \mapsto \text{VR}}].$$

By Lemma 8.15, it suffices to show that

$$(W, \rho_1(\gamma_1(\mathsf{t}_1))\overline{[\tau_1/\alpha][\mathsf{v}_1/\mathsf{x}]}, \rho_2(\gamma_2(\mathsf{t}_2))\overline{[\tau_2/\alpha][\mathsf{v}_2/\mathsf{x}]}) \in \mathcal{E}[\![\tau'\rho[\overline{\alpha \mapsto \text{VR}}]]\!].$$

By definition, $W' \in \mathcal{H}[\![\Psi]\!]$ and $\rho[\overline{\alpha \mapsto \text{VR}}] \in \mathcal{D}[\![\Delta, \overline{\alpha}]\!]$. By definition and by monotonicity,

$$(W', \gamma[\overline{\mathsf{x} \mapsto (\mathsf{v}_1, \mathsf{v}_2)}]) \in \mathcal{G}[\![\Gamma, \overline{\mathsf{x} : \tau}]\!]\rho[\overline{\alpha \mapsto \text{VR}}].$$

Applying our assumption gives the result. □

Lemma 10.15 (F Application)
If $\Psi; \Delta; \Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$, $\overline{\Delta \vdash \hat{\tau}}$, and $\overline{\Psi; \Delta; \Gamma \vdash \mathsf{t}_1' \approx \mathsf{t}_2' : \tau[\hat{\tau}/\alpha]}$, then

$$\Psi; \Delta; \Gamma \vdash \mathsf{t}_1\ [\overline{\hat{\tau}}]\ \overline{\mathsf{t}_1'} \approx \mathsf{t}_2\ [\overline{\hat{\tau}}]\ \overline{\mathsf{t}_2'} : \tau'\overline{[\hat{\tau}/\alpha]}.$$

Proof

First note that $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1\ [\overline{\hat{\tau}}]\ \overline{\mathsf{t}'_1} : \tau'[\overline{\hat{\tau}/\alpha}]$ and $\Psi;\Delta;\Gamma \vdash \mathsf{t}_2\ [\overline{\hat{\tau}}]\ \overline{\mathsf{t}'_2} : \tau'[\overline{\hat{\tau}/\alpha}]$.
Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{t}_1\ [\overline{\hat{\tau}}]\ \overline{\mathsf{t}'_1})), \rho_2(\gamma_2(\mathsf{t}_2\ [\overline{\hat{\tau}}]\ \overline{\mathsf{t}'_2}))) \\ = (W, \rho_1(\gamma_1(\mathsf{t}_1))\ \overline{[\rho_1(\hat{\tau})]}\ \overline{\rho_1(\gamma_1(\mathsf{t}'_1))}, \rho_2(\gamma_2(\mathsf{t}_2))\ \overline{[\rho_2(\hat{\tau})]}\ \overline{\rho_2(\gamma_2(\mathsf{t}'_2))}) \in \mathcal{E}[\![\tau'[\overline{\hat{\tau}/\alpha}]]\!]\rho.$$

Let $\overline{\mathrm{VR} = (\rho_1(\hat{\tau}), \rho_2(\hat{\tau}), \mathcal{V}[\![\hat{\tau}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{C}\rangle}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle}]\!]\rho)}$. By Lemma 10.7,

$$\mathcal{E}[\![\tau'[\overline{\hat{\tau}/\alpha}]]\!]\rho = \mathcal{E}[\![\tau']\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}] \quad \text{and} \quad \overline{\mathcal{V}[\![\tau[\overline{\hat{\tau}/\alpha}]]\!]\rho = \mathcal{V}[\![\tau]\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}]}.$$

We will use these equalities throughout the proof.
Let $W_0 \sqsupseteq_{\mathrm{pub}} W$ and $(W_0, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W_0, \mathsf{v}_1\ \overline{[\rho_1(\hat{\tau})]}\ \overline{\rho_1(\gamma_1(\mathsf{t}'_1))}, \mathsf{v}_2\ \overline{[\rho_2(\hat{\tau})]}\ \overline{\rho_2(\gamma_2(\mathsf{t}'_2))}) \in \mathcal{E}[\![\tau'[\overline{\hat{\tau}/\alpha}]]\!]\rho.$$

Let $W_i \sqsupseteq_{\mathrm{pub}} W_{i-1}$ and $\overline{(W_i, \mathsf{v}'_{1i}, \mathsf{v}'_{2i}) \in \mathcal{V}[\![\tau[\overline{\hat{\tau}/\alpha}]]\!]\rho}$. By further applications of 8.20, it suffices to show that

$$(W_n, \mathsf{v}_1\ \overline{[\rho_1(\hat{\tau})]}\ \overline{\mathsf{v}'_1}, \mathsf{v}_2\ \overline{[\rho_2(\hat{\tau})]}\ \overline{\mathsf{v}'_2}) \in \mathcal{E}[\![\tau'[\overline{\hat{\tau}/\alpha}]]\!]\rho.$$

Since $W_n \sqsupseteq W_0$, $\overline{\mathrm{VR} \in \mathrm{FValRel}}$, and $\overline{(W_n, \mathsf{v}'_1, \mathsf{v}'_2) \in \mathcal{V}[\![\tau]\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}]}$, we can instantiate our assumption that

$$(W_0, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho$$

to get exactly the needed result. □

Lemma 10.16 (F Pack)

- If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \tau[\tau'/\alpha]$, then $\Psi;\Delta;\Gamma \vdash \mathsf{pack}\langle\tau',\mathsf{t}_1\rangle\ \mathsf{as}\ \exists\alpha.\tau \approx \mathsf{pack}\langle\tau',\mathsf{t}_2\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau$
- If $\Psi;\Delta;\Gamma \vdash \mathsf{v}_1 \approx_{\mathrm{v}} \mathsf{v}_2 : \tau[\tau'/\alpha]$, then $\Psi;\Delta;\Gamma \vdash \mathsf{pack}\langle\tau',\mathsf{v}_1\rangle\ \mathsf{as}\ \exists\alpha.\tau \approx_{\mathrm{v}} \mathsf{pack}\langle\tau',\mathsf{v}_2\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathsf{pack}\langle\tau',\mathsf{t}_1\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau$ and $\Psi;\Delta;\Gamma \vdash \mathsf{pack}\langle\tau',\mathsf{t}_2\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau$.
Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{pack}\langle\tau',\mathsf{t}_1\rangle\ \mathsf{as}\ \exists\alpha.\tau)), \rho_2(\gamma_2(\mathsf{pack}\langle\tau',\mathsf{t}_2\rangle\ \mathsf{as}\ \exists\alpha.\tau))) \\ = (W, \mathsf{pack}\langle\rho_1(\tau'),\rho_1(\gamma_1(\mathsf{t}_1))\rangle\ \mathsf{as}\ \exists\alpha.\tau, \mathsf{pack}\langle\rho_2(\tau'),\rho_2(\gamma_2(\mathsf{t}_2))\rangle\ \mathsf{as}\ \exists\alpha.\tau) \in \mathcal{E}[\![\exists\alpha.\tau]\!]\rho.$$

Let $\mathrm{VR} = (\rho_1(\tau'), \rho_2(\tau'), \mathcal{V}[\![\tau']\!]\rho, \mathcal{V}[\![\tau'^{\langle\mathcal{C}\rangle}]\!]\rho, \mathcal{V}[\![\tau'^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle}]\!]\rho)$. By our assumption and Lemma 10.7,

$$(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho = \mathcal{E}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}].$$

Let $W' \sqsupseteq_{\mathrm{pub}} W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]$. By Lemma 8.20, it suffices to show that

$$(W, \mathsf{pack}\langle\rho_1(\tau'),\mathsf{v}_1\rangle\ \mathsf{as}\ \exists\alpha.\tau, \mathsf{pack}\langle\rho_2(\tau'),\mathsf{v}_2\rangle\ \mathsf{as}\ \exists\alpha.\tau) \in \mathcal{E}[\![\exists\alpha.\tau]\!]\rho.$$

By Lemma 8.9, it suffices to show that

$$(W, \mathsf{pack}\langle\mathsf{v}_1,\rho_1(\gamma_1(\mathsf{t}_1))\rangle\ \mathsf{as}\ \exists\alpha.\tau, \mathsf{pack}\langle\mathsf{v}_2,\rho_2(\gamma_2(\mathsf{t}_2))\rangle\ \mathsf{as}\ \exists\alpha.\tau) \in \mathcal{V}[\![\exists\alpha.\tau]\!]\rho.$$

But $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]$ is sufficient to give this. □

Lemma 10.17 (F Unpack)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \exists\alpha.\tau$ and $\Psi;(\Delta,\alpha);(\Gamma,\mathsf{x}:\tau) \vdash \mathsf{t}'_1 \approx \mathsf{t}'_2 : \tau'$, then

$$\Psi;\Delta;\Gamma \vdash \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}_1\ \mathsf{in}\ \mathsf{t}'_1 \approx \mathsf{unpack}\ \langle\alpha,\mathsf{x}\rangle = \mathsf{t}_2\ \mathsf{in}\ \mathsf{t}'_2 : \tau'.$$

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \mathsf{t}_1\ \mathsf{in}\ \mathsf{t}_1' : \tau'$ and $\Psi;\Delta;\Gamma \vdash \mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \mathsf{t}_2\ \mathsf{in}\ \mathsf{t}_2' : \tau'$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \mathsf{t}_1\ \mathsf{in}\ \mathsf{t}_1')), \rho_2(\gamma_2(\mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \mathsf{t}_2\ \mathsf{in}\ \mathsf{t}_2')))\\ &\quad = (W, \mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \rho_1(\gamma_1(\mathsf{t}_1))\ \mathsf{in}\ \rho_1(\gamma_1(\mathsf{t}_1')), \mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \rho_2(\gamma_2(\mathsf{t}_2))\ \mathsf{in}\ \rho_2(\gamma_2(\mathsf{t}_2'))) \in \mathcal{E}[\![\tau']\!]\rho.\end{aligned}$$

By our assumption, $(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\exists\alpha.\tau]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\exists\alpha.\tau]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \mathsf{v}_1\ \mathsf{in}\ \rho_1(\gamma_1(\mathsf{t}_1')), \mathsf{unpack}\,\langle\alpha,\mathsf{x}\rangle = \mathsf{v}_2\ \mathsf{in}\ \rho_2(\gamma_2(\mathsf{t}_2'))) \in \mathcal{E}[\![\tau']\!]\rho.$$

By definition of $\mathcal{V}[\![\exists\alpha.\tau]\!]\rho$, $\mathsf{v}_1 = \mathsf{pack}\langle\tau_1,\hat{\mathsf{v}}_1\rangle\,\mathsf{as}\,\rho_1(\exists\alpha.\tau)$ and $\mathsf{v}_2 = \mathsf{pack}\langle\tau_2,\hat{\mathsf{v}}_2\rangle\,\mathsf{as}\,\rho_2(\exists\alpha.\tau)$, where there is some VR $\in$ FValRel such that $\mathrm{VR}.\tau_1 = \tau_1$, $\mathrm{VR}.\tau_2 = \tau_2$, and $(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]$. By the operational semantics and by Lemma 8.15, it suffices to show that

$$(W', \rho_1(\gamma_1(\mathsf{t}_1'))[\tau_1/\alpha][\hat{\mathsf{v}}_1/\mathsf{x}], \rho_2(\gamma_2(\mathsf{t}_2'))[\tau_2/\alpha][\hat{\mathsf{v}}_2/\mathsf{x}]) \in \mathcal{E}[\![\tau']\!]\rho.$$

By our hypothesis, this follows from $W' \in \mathcal{H}[\![\Psi]\!]$, $\rho[\alpha \mapsto \mathrm{VR}] \in \mathcal{D}[\![\Delta,\alpha]\!]$, and

$$(W', \gamma[\mathsf{x} \mapsto (\mathsf{v}_1, \mathsf{v}_2)]) \in \mathcal{G}[\![\Gamma, \mathsf{x}:\tau]\!]\rho[\alpha \mapsto \mathrm{VR}].$$

The first two of these conditions hold immediately, and the last holds by monotonicity and since $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]$. □

Lemma 10.18 (F Fold)

- If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \tau[\mu\alpha.\tau/\alpha]$, then $\Psi;\Delta;\Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{t}_1 \approx \mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{t}_2 : \mu\alpha.\tau$
- If $\Psi;\Delta;\Gamma \vdash \mathsf{v}_1 \approx_{\mathrm{v}} \mathsf{v}_2 : \tau[\mu\alpha.\tau/\alpha]$, then $\Psi;\Delta;\Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{v}_1 \approx_{\mathrm{v}} \mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{v}_2 : \mu\alpha.\tau$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{t}_1 : \mu\alpha.\tau$ and $\Psi;\Delta;\Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{t}_2 : \mu\alpha.\tau$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{fold}_{\mu\alpha.\tau}\,\mathsf{t}_2)))\\ &\qquad = (W, \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\,\rho_1(\gamma_1(\mathsf{t}_1)), \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\,\rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\mu\alpha.\tau]\!]\rho.\end{aligned}$$

By our assumption and monotonicity,

$$(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \triangleright\mathcal{E}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

Let $W' \sqsupseteq_{\mathrm{pub}} W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\,\mathsf{v}_1, \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\,\mathsf{v}_2) \in \mathcal{E}[\![\mu\alpha.\tau]\!]\rho.$$

By Lemma 8.9, it suffices to show that

$$(W', \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\,\mathsf{v}_1, \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\,\mathsf{v}_2) \in \mathcal{V}[\![\mu\alpha.\tau]\!]\rho.$$

But $(W', \mathsf{v}_1, \mathsf{v}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$ is sufficient to give this. □

Lemma 10.19 (F Unfold)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \mu\alpha.\tau$, then $\Psi;\Delta;\Gamma \vdash \mathsf{unfold}\,\mathsf{t}_1 \approx \mathsf{unfold}\,\mathsf{t}_2 : \tau[\mu\alpha.\tau/\alpha]$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathsf{unfold}\,\mathsf{t}_1 : \tau[\mu\alpha.\tau/\alpha]$ and $\Psi;\Delta;\Gamma \vdash \mathsf{unfold}\,\mathsf{t}_2 : \tau[\mu\alpha.\tau/\alpha]$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{unfold}\,\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{unfold}\,\mathsf{t}_2))) = (W, \mathsf{unfold}\,\rho_1(\gamma_1(\mathsf{t}_1)), \mathsf{unfold}\,\rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

By our assumption, $(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\mu\alpha.\tau]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mu\alpha.\tau]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{unfold}\,\mathsf{v}_1, \mathsf{unfold}\,\mathsf{v}_2) \in \mathcal{E}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

By definition of $\mathcal{V}[\![\mu\alpha.\tau]\!]\rho$, $\mathsf{v}_1 = \mathsf{fold}_{\rho_1(\mu\alpha.\tau)}\,\hat{\mathsf{v}}_1$ and $\mathsf{v}_2 = \mathsf{fold}_{\rho_2(\mu\alpha.\tau)}\,\hat{\mathsf{v}}_2$, where

$$(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

By the operational semantics and by Lemma 8.15, it suffices to show that

$$(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{E}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho.$$

But this follows from Lemma 8.9. □

Lemma 10.20 (F Tuple)

- If $\overline{\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \tau}$, then $\Psi;\Delta;\Gamma \vdash \langle\overline{\mathsf{t}_1}\rangle \approx \langle\overline{\mathsf{t}_2}\rangle : \langle\overline{\tau}\rangle$
- If $\overline{\Psi;\Delta;\Gamma \vdash \mathsf{v}_1 \approx_{\mathrm{v}} \mathsf{v}_2 : \tau}$, then $\Psi;\Delta;\Gamma \vdash \langle\overline{\mathsf{v}_1}\rangle \approx_{\mathrm{v}} \langle\overline{\mathsf{v}_2}\rangle : \langle\overline{\tau}\rangle$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \langle\overline{\mathsf{t}_1}\rangle : \langle\overline{\tau}\rangle$ and $\Psi;\Delta;\Gamma \vdash \langle\overline{\mathsf{t}_2}\rangle : \langle\overline{\tau}\rangle$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\langle\overline{\mathsf{t}_1}\rangle)), \rho_2(\gamma_2(\langle\overline{\mathsf{t}_2}\rangle))) = (W, \langle\overline{\rho_1(\gamma_1(\mathsf{t}_1))}\rangle, \langle\overline{\rho_2(\gamma_2(\mathsf{t}_2))}\rangle) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

By our assumption,

$$\overline{(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\tau]\!]\rho}.$$

Let $W_0 = W$, $W_i \sqsupseteq_{\mathrm{pub}} W_{i-1}$, and $\overline{(W_i, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho}$. By repeated use of Lemma 8.20, it suffices to show that

$$(W_n, \langle\overline{\mathsf{v}_1}\rangle, \langle\overline{\mathsf{v}_2}\rangle) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

By Lemma 8.9, it suffices to show that

$$(W_n, \langle\overline{\mathsf{v}_1}\rangle, \langle\overline{\mathsf{v}_2}\rangle) \in \mathcal{V}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

But we have this by its definition and by monotonicity. □

Lemma 10.21 (F Projection)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \langle\overline{\tau}\rangle$, then $\Psi;\Delta;\Gamma \vdash \pi_{\mathsf{i}}(\mathsf{t}_1) \approx \pi_{\mathsf{i}}(\mathsf{t}_2) : \tau_{\mathsf{i}}$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \pi_{\mathsf{i}}(\mathsf{t}_1) : \tau_{\mathsf{i}}$ and $\Psi;\Delta;\Gamma \vdash \pi_{\mathsf{i}}(\mathsf{t}_2) : \tau_{\mathsf{i}}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\pi_{\mathsf{i}}(\mathsf{t}_1))), \rho_2(\gamma_2(\pi_{\mathsf{i}}(\mathsf{t}_2)))) = (W, \pi_{\mathsf{i}}(\rho_1(\gamma_1(\mathsf{t}_1))), \pi_{\mathsf{i}}(\rho_2(\gamma_2(\mathsf{t}_2)))) \in \mathcal{E}[\![\tau_{\mathsf{i}}]\!]\rho.$$

By our assumption, $(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\langle\overline{\tau}\rangle]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \pi_{\mathsf{i}}(\mathsf{v}_1), \pi_{\mathsf{i}}(\mathsf{v}_2)) \in \mathcal{E}[\![\tau_{\mathsf{i}}]\!]\rho.$$

By definition of $\mathcal{V}[\![\langle\overline{\tau}\rangle]\!]\rho$, $\mathsf{v}_1 = \langle\overline{\hat{\mathsf{v}}_1}\rangle$ and $\mathsf{v}_2 = \langle\overline{\hat{\mathsf{v}}_2}\rangle$, where $\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho}$. By the operational semantics and by Lemma 8.15, it suffices to show that

$$(W', \hat{\mathsf{v}}_{1\mathsf{i}}, \hat{\mathsf{v}}_{2\mathsf{i}}) \in \mathcal{E}[\![\tau_{\mathsf{i}}]\!]\rho.$$

But this follows from Lemma 8.9. □

Lemma 10.22 (FC Boundary)
If $\Psi;\Delta;\Gamma \vdash \mathbf{e_1} \approx \mathbf{e_2} : \tau^{\langle \mathcal{C} \rangle}$, then $\Psi;\Delta;\Gamma \vdash {}^{\tau}\mathcal{FC}\,\mathbf{e_1} \approx {}^{\tau}\mathcal{FC}\,\mathbf{e_2} : \tau$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash {}^{\tau}\mathcal{FC}\,\mathbf{e_2} : \tau$ and $\Psi;\Delta;\Gamma \vdash {}^{\tau}\mathcal{FC}\,\mathbf{e_2} : \tau$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By our assumption,

$$(W, \rho_1(\gamma_1(\mathbf{e_1})), \rho_2(\gamma_2(\mathbf{e_2}))) \in \mathcal{E}[\![\tau^{\langle \mathcal{C} \rangle}]\!]\rho.$$

By the bridge lemma,

$$(W, {}^{\rho_1(\tau)}\mathcal{FC}\,\rho_1(\gamma_1(\mathbf{e_1})), {}^{\rho_2(\tau)}\mathcal{FC}\,\rho_2(\gamma_2(\mathbf{e_2}))) = (W, \rho_1(\gamma_1({}^{\tau}\mathcal{FC}\,\mathbf{e_1})), \rho_2(\gamma_2({}^{\tau}\mathcal{FC}\,\mathbf{e_2}))) \in \mathcal{E}[\![\tau]\!]\rho,$$

as desired. □

Lemma 10.23 (C Function)
If $\Psi;(\overline{\alpha});(\overline{\mathbf{x}:\tau}) \vdash \mathbf{t_1} \approx \mathbf{t_2} : \tau'$, then

- $\Psi;\Delta;\Gamma \vdash \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_1} \approx \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_2} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$
- $\Psi;\Delta;\Gamma \vdash \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_1} \approx_{\mathrm{v}} \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_2} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$.

Proof

First note that $\Psi;\Delta;\Gamma \vdash \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_1} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ and $\Psi;\Delta;\Gamma \vdash \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_2} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.

We need to show that

$$(W, \rho_1(\gamma_1(\boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_1})), \rho_2(\gamma_2(\boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_2}))) = (W, \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_1}, \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_2}) \in \mathcal{E}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho.$$

By Lemma 8.9, it suffices to show that

$$(W, \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_1}, \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_2}) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho.$$

Let $W' \sqsupseteq W$, $\overline{\mathrm{VR} \in \mathrm{CValRel}}$, and $\overline{(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}]}$. For convenience, let $\overline{\tau_1 = \mathrm{VR}.\tau_1}$ and $\overline{\tau_2 = \mathrm{VR}.\tau_2}$ We need to show that

$$(W, \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_1}\ \overline{[\tau_1]}\ \overline{\mathbf{v_1}}, \boldsymbol{\lambda}[\overline{\alpha}](\overline{\mathbf{x}:\tau}).\mathbf{t_2}\ \overline{[\tau_2]}\ \overline{\mathbf{v_2}}) \in \mathcal{E}[\![\tau']\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}].$$

By Lemma 8.15, it suffices to show that

$$(W, \mathbf{t_1}\overline{[\tau_1/\alpha][\mathbf{v_1}/\mathbf{x}]}, \mathbf{t_2}\overline{[\tau_2/\alpha][\mathbf{v_2}/\mathbf{x}]}) \in \mathcal{E}[\![\tau']\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}].$$

By definition, $W' \in \mathcal{H}[\![\Psi]\!]$, $\cdot[\overline{\alpha \mapsto \mathrm{VR}}] \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W', \cdot[\overline{\mathbf{x} \mapsto (\mathbf{v_1}, \mathbf{v_2})}]) \in \mathcal{G}[\![\overline{\mathbf{x}:\tau}]\!]\rho[\overline{\alpha \mapsto \mathrm{VR}}]$. Applying our assumption gives the result. □

Lemma 10.24 (C Application)
If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \forall[].(\overline{\tau}) \to \tau'$ and $\overline{\Psi;\Delta;\Gamma \vdash \mathbf{t_1'} \approx \mathbf{t_2'} : \tau}$, then $\Psi;\Delta;\Gamma \vdash \mathbf{t_1}\ []\ \overline{\mathbf{t_1'}} \approx \mathbf{t_2}\ []\ \overline{\mathbf{t_2'}} : \tau'$.

Proof

First note that $\Psi;\Delta;\Gamma \vdash \mathbf{t_1}\ []\ \overline{\mathbf{t_1'}} : \tau'$ and $\Psi;\Delta;\Gamma \vdash \mathbf{t_2}\ []\ \overline{\mathbf{t_2'}} : \tau'$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathbf{t_1}\ []\ \overline{\mathbf{t_1'}})), \rho_2(\gamma_2(\mathbf{t_2}\ []\ \overline{\mathbf{t_2'}}))) = (W, \rho_1(\gamma_1(\mathbf{t_1}))\ []\ \overline{\rho_1(\gamma_1(\mathbf{t_1'}))}, \rho_2(\gamma_2(\mathbf{t_2}))\ []\ \overline{\rho_2(\gamma_2(\mathbf{t_2'}))}) \in \mathcal{E}[\![\tau']\!]\rho.$$

Let $W_0 \sqsupseteq_{\text{pub}} W$ and $(W_0, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[].(\overline{\tau}) \to \tau']\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W_0, \mathbf{v_1}\ [] \overline{\rho_1(\gamma_1(\mathbf{t'_1}))}, \mathbf{v_2}\ [] \overline{\rho_2(\gamma_2(\mathbf{t'_2}))}) \in \mathcal{E}[\![\tau']\!]\rho.$$

Let $W_i \sqsupseteq_{\text{pub}} W_{i-1}$ and $\overline{(W_i, \mathbf{v'_{1i}}, \mathbf{v'_{2i}}) \in \mathcal{V}[\![\tau]\!]\rho}$. By further applications of 8.20, it suffices to show that

$$(W_n, \mathbf{v_1}\ [] \overline{\mathbf{v'_1}}, \mathbf{v_2}\ [] \overline{\mathbf{v'_2}}) \in \mathcal{E}[\![\tau']\!]\rho.$$

Since $W_n \sqsupseteq W_0$ and $\overline{(W_n, \mathbf{v'_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau]\!]\rho}$, we can instantiate our assumption that

$$(W_0, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[].(\overline{\tau}) \to \tau']\!]\rho$$

to get exactly the needed result. □

Lemma 10.25 (C Type Application)
If $\Psi; \Delta; \Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau'$ and $\Delta \vdash \hat{\tau}$, then

$$\Psi; \Delta; \Gamma \vdash \mathbf{t_1}[\hat{\tau}] \approx \mathbf{t_2}[\hat{\tau}] : \forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta].$$

Proof

First note that $\Psi; \Delta; \Gamma \vdash \mathbf{t_i}[\hat{\tau}] : \forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]$ for $i \in \{1, 2\}$.
Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathbf{t_1}[\hat{\tau}])), \rho_2(\gamma_2(\mathbf{t_2}[\hat{\tau}])))$$
$$= (W, \rho_1(\gamma_1(\mathbf{t_1}))[\rho_1(\hat{\tau})], \rho_2(\gamma_2(\mathbf{t_2}))[\rho_2(\hat{\tau})]) \in \mathcal{E}[\![\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]]\!]\rho.$$

By our assumption, $(W, \rho_1(\gamma_1(\mathbf{t_1})), \rho_2(\gamma_2(\mathbf{t_2}))) \in \mathcal{E}[\![\forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho$. Let $W' \sqsupseteq W$ and

$$(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho.$$

By Lemma 8.20, it suffices to show that

$$(W', \mathbf{v_1}[\rho_1(\hat{\tau})], \mathbf{v_2}[\rho_2(\hat{\tau})]) \in \mathcal{E}[\![\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]]\!]\rho.$$

Let $\text{VR} = (\rho_1(\hat{\tau}), \rho_2(\hat{\tau}), \mathcal{V}[\![\hat{\tau}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{A}\rangle}]\!]\rho)$. By Lemma 8.9 and Lemma 10.5, it suffices to show that

$$(W', \mathbf{v_1}[\rho_1(\hat{\tau})], \mathbf{v_2}[\rho_2(\hat{\tau})]) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]]\!]\rho = \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho[\beta \mapsto \text{VR}].$$

We can reach this easily from our hypothesis that $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho$. □

Lemma 10.26 (CF Boundary)
If $\Psi; \Delta; \Gamma \vdash \mathsf{e_1} \approx \mathsf{e_2} : \tau$, then $\Psi; \Delta; \Gamma \vdash \mathcal{CF}^{\tau}\ \mathsf{e_1} \approx \mathcal{CF}^{\tau}\ \mathsf{e_2} : \tau^{\langle\mathcal{C}\rangle}$.

Proof

Note that $\Psi; \Delta; \Gamma \vdash \mathcal{CF}^{\tau}\ \mathsf{e_1} : \tau^{\langle\mathcal{C}\rangle}$ and $\Psi; \Delta; \Gamma \vdash \mathcal{CF}^{\tau}\ \mathsf{e_2} : \tau^{\langle\mathcal{C}\rangle}$.
Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By our assumption,

$$(W, \rho_1(\gamma_1(\mathsf{e_1})), \rho_2(\gamma_2(\mathsf{e_2}))) \in \mathcal{E}[\![\tau]\!]\rho.$$

By the bridge lemma,

$$(W, \mathcal{CF}^{\rho_1(\tau)}\ \rho_1(\gamma_1(\mathsf{e_1})), \mathcal{CF}^{\rho_2(\tau)}\ \rho_2(\gamma_2(\mathsf{e_2}))) = (W, \rho_1(\gamma_1(\mathcal{CF}^{\tau}\ \mathsf{e_1})), \rho_2(\gamma_2(\mathcal{CF}^{\tau}\ \mathsf{e_2}))) \in \mathcal{E}[\![\tau^{\langle\mathcal{C}\rangle}]\!]\rho,$$

as desired. □

Lemma 10.27 (CA Boundary)
If $\Psi; \Delta; \Gamma \vdash \mathsf{e_1} \approx \mathsf{e_2} : \tau^{\langle\mathcal{A}\rangle}$, then $\Psi; \Delta; \Gamma \vdash {}^{\tau}\mathcal{CA}\,\mathsf{e_1} \approx {}^{\tau}\mathcal{CA}\,\mathsf{e_2} : \tau$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash {}^{\tau}\mathcal{CA}\,\mathbf{e_2} : \boldsymbol{\tau}$ and $\Psi;\Delta;\Gamma \vdash {}^{\tau}\mathcal{CA}\,\mathbf{e_2} : \boldsymbol{\tau}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By our assumption,

$$(W, \rho_1(\gamma_1(\mathbf{e_1})), \rho_2(\gamma_2(\mathbf{e_2}))) \in \mathcal{E}[\![\boldsymbol{\tau}^{\langle\mathcal{A}\rangle}]\!]\rho.$$

By the bridge lemma,

$$(W, {}^{\rho_1(\tau)}\mathcal{CA}\,\rho_1(\gamma_1(\mathbf{e_1})), {}^{\rho_2(\tau)}\mathcal{CA}\,\rho_2(\gamma_2(\mathbf{e_2}))) = (W, \rho_1(\gamma_1({}^{\tau}\mathcal{CA}\,\mathbf{e_1})), \rho_2(\gamma_2({}^{\tau}\mathcal{CA}\,\mathbf{e_2}))) \in \mathcal{E}[\![\boldsymbol{\tau}]\!]\rho,$$

as desired. □

We omit proofs of the remaining compatibility lemmas for C, as they are identical to the proofs of the corresponding F compatibility lemmas.

Lemma 10.28 (C Variable)
If $\mathbf{x} : \boldsymbol{\tau} \in \Gamma$, then $\Psi;\Delta;\Gamma \vdash \mathbf{x} \approx \mathbf{x} : \boldsymbol{\tau}$.

Lemma 10.29 (C Unit)

- $\Psi;\Delta;\Gamma \vdash () \approx () : \mathbf{unit}$
- $\Psi;\Delta;\Gamma \vdash () \approx_{\mathrm{v}} () : \mathbf{unit}$.

Lemma 10.30 (C Int)

- $\Psi;\Delta;\Gamma \vdash \mathbf{n} \approx \mathbf{n} : \mathbf{int}$
- $\Psi;\Delta;\Gamma \vdash \mathbf{n} \approx_{\mathrm{v}} \mathbf{n} : \mathbf{int}$.

Lemma 10.31 (C Primitive)
If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \mathbf{int}$ and $\Psi;\Delta;\Gamma \vdash \mathbf{t_1'} \approx \mathbf{t_2'} : \mathbf{int}$, then $\Psi;\Delta;\Gamma \vdash \mathbf{t_1\ p\ t_1'} \approx \mathbf{t_2\ p\ t_2'} : \mathbf{int}$.

Lemma 10.32 (C If0)
If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \mathbf{int}$, $\Psi;\Delta;\Gamma \vdash \mathbf{t_1'} \approx \mathbf{t_2'} : \boldsymbol{\tau}$, and $\Psi;\Delta;\Gamma \vdash \mathbf{t_1''} \approx \mathbf{t_2''} : \boldsymbol{\tau}$, then

$$\Psi;\Delta;\Gamma \vdash \mathbf{if0\ t_1\ t_1'\ t_1''} \approx \mathbf{if0\ t_2\ t_2'\ t_2''} : \boldsymbol{\tau}.$$

Lemma 10.33 (C Pack)

- If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \boldsymbol{\tau}[\boldsymbol{\tau'}/\boldsymbol{\alpha}]$, then $\Psi;\Delta;\Gamma \vdash \mathbf{pack}\langle\boldsymbol{\tau'},\mathbf{t_1}\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau} \approx \mathbf{pack}\langle\boldsymbol{\tau'},\mathbf{t_2}\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau} : \exists\boldsymbol{\alpha}.\boldsymbol{\tau}$
- If $\Psi;\Delta;\Gamma \vdash \mathbf{v_1} \approx_{\mathrm{v}} \mathbf{v_2} : \boldsymbol{\tau}[\boldsymbol{\tau'}/\boldsymbol{\alpha}]$, then $\Psi;\Delta;\Gamma \vdash \mathbf{pack}\langle\boldsymbol{\tau'},\mathbf{v_1}\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau} \approx_{\mathrm{v}} \mathbf{pack}\langle\boldsymbol{\tau'},\mathbf{v_2}\rangle\ \mathbf{as}\ \exists\boldsymbol{\alpha}.\boldsymbol{\tau} : \exists\boldsymbol{\alpha}.\boldsymbol{\tau}$.

Lemma 10.34 (C Unpack)
If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \exists\boldsymbol{\alpha}.\boldsymbol{\tau}$ and $\Psi;(\Delta,\boldsymbol{\alpha});(\Gamma,\mathbf{x}:\boldsymbol{\tau}) \vdash \mathbf{t_1'} \approx \mathbf{t_2'} : \boldsymbol{\tau'}$, then

$$\Psi;\Delta;\Gamma \vdash \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{t_1}\ \mathbf{in}\ \mathbf{t_1'} \approx \mathbf{unpack}\ \langle\boldsymbol{\alpha},\mathbf{x}\rangle = \mathbf{t_2}\ \mathbf{in}\ \mathbf{t_2'} : \boldsymbol{\tau'}.$$

Lemma 10.35 (C Fold)

- If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \boldsymbol{\tau}[\mu\boldsymbol{\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}]$, then $\Psi;\Delta;\Gamma \vdash \mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{t_1} \approx \mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{t_2} : \mu\boldsymbol{\alpha}.\boldsymbol{\tau}$
- If $\Psi;\Delta;\Gamma \vdash \mathbf{v_1} \approx_{\mathrm{v}} \mathbf{v_2} : \boldsymbol{\tau}[\mu\boldsymbol{\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}]$, then $\Psi;\Delta;\Gamma \vdash \mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{v_1} \approx_{\mathrm{v}} \mathbf{fold}_{\mu\boldsymbol{\alpha}.\boldsymbol{\tau}}\ \mathbf{v_2} : \mu\boldsymbol{\alpha}.\boldsymbol{\tau}$.

Lemma 10.36 (C Unfold)
If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \mu\boldsymbol{\alpha}.\boldsymbol{\tau}$, then $\Psi;\Delta;\Gamma \vdash \mathbf{unfold\ t_1} \approx \mathbf{unfold\ t_2} : \boldsymbol{\tau}[\mu\boldsymbol{\alpha}.\boldsymbol{\tau}/\boldsymbol{\alpha}]$.

Lemma 10.37 (C Tuple)

- If $\overline{\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \boldsymbol{\tau}}$, then $\Psi;\Delta;\Gamma \vdash \langle\overline{\mathbf{t_1}}\rangle \approx \langle\overline{\mathbf{t_2}}\rangle : \langle\overline{\boldsymbol{\tau}}\rangle$
- If $\overline{\Psi;\Delta;\Gamma \vdash \mathbf{v_1} \approx_{\mathrm{v}} \mathbf{v_2} : \boldsymbol{\tau}}$, then $\Psi;\Delta;\Gamma \vdash \langle\overline{\mathbf{v_1}}\rangle \approx_{\mathrm{v}} \langle\overline{\mathbf{v_2}}\rangle : \langle\overline{\boldsymbol{\tau}}\rangle$.

Lemma 10.38 (C Projection)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t_1} \approx \mathsf{t_2} : \langle \overline{\tau} \rangle$, then $\Psi;\Delta;\Gamma \vdash \pi_i(\mathsf{t_1}) \approx \pi_i(\mathsf{t_2}) : \tau_i$.

Lemma 10.39 (A Heap Fragment)
If $(\Psi, \ell : {}^{\mathsf{box}}\psi);\Delta;\Gamma \vdash (\mathsf{t_1}, \mathsf{H_1}) \approx (\mathsf{t_2}, \mathsf{H_2}) : \tau$ and for any $W \in \mathcal{H}[\![\Psi]\!]$, $(W, \mathsf{h_1}, \mathsf{h_2}) \in \mathcal{HV}[\![\psi]\!]\emptyset$, then

$$\Psi;\Delta;\Gamma \vdash (\mathsf{t_1}, (\mathsf{H_1}, \ell \mapsto \mathsf{h_1})) \approx (\mathsf{t_2}, (\mathsf{H_2}, \ell \mapsto \mathsf{h_2})) : \tau.$$

Proof

Note that $\Psi;\Delta;\Gamma \vdash (\mathsf{t_1}, (\mathsf{H_1}, \ell \mapsto \mathsf{h_1})) : \tau$ and $\Psi;\Delta;\Gamma \vdash (\mathsf{t_2}, (\mathsf{H_2}, \ell \mapsto \mathsf{h_2})) : \tau$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1((\mathsf{t_1}, (\mathsf{H_1}, \ell \mapsto \mathsf{h_1})))), \rho_2(\gamma_2((\mathsf{t_2}, (\mathsf{H_2}, \ell \mapsto \mathsf{h_2})))) \\ = (W, (\rho_1(\gamma_1(\mathsf{t_1})), (\mathsf{H_1}, \ell \mapsto \mathsf{h_1})), (\rho_2(\gamma_2(\mathsf{t_2})), (\mathsf{H_2}, \ell \mapsto \mathsf{h_2}))) \in \mathcal{E}[\![\tau]\!]\rho.$$

By Lemma 8.14, it suffices to show that

$$(W \boxplus (\ell \mapsto \mathsf{h_1}, \ell \mapsto \mathsf{h_2}), \rho_1(\gamma_1((\mathsf{t_1}, \mathsf{H_1}))), \rho_2(\gamma_2((\mathsf{t_2}, \mathsf{H_2})))) \in \mathcal{E}[\![\tau]\!]\rho.$$

We can apply our first assumption to get exactly this as long as $W \boxplus (\ell \mapsto \mathsf{h_1}, \ell \mapsto \mathsf{h_2}) \in \mathcal{H}[\![\Psi, \ell : {}^{\mathsf{box}}\psi]\!]$. But this follows from our second assumption. □

Lemma 10.40 (A Ref)
If $\ell : {}^{\mathsf{ref}}\psi \in \Psi$, then

- $\Psi;\Delta;\Gamma \vdash \ell \approx \ell : \mathsf{ref}\ \psi$
- $\Psi;\Delta;\Gamma \vdash \ell \approx_{\mathrm{v}} \ell : \mathsf{ref}\ \psi$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \ell : \mathsf{ref}\ \psi$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By definition of $W \in \mathcal{H}[\![\Psi]\!]$,

$$(W, \rho_1(\gamma_1(\ell)), \rho_2(\gamma_2(\ell))) = (W, \ell, \ell) \in \mathcal{V}[\![\mathsf{ref}\ \psi]\!]\emptyset = \mathcal{V}[\![\mathsf{ref}\ \psi]\!]\rho,$$

so we are done. □

Lemma 10.41 (A Box)
If $\ell : {}^{\mathsf{box}}\psi \in \Psi$, then

- $\Psi;\Delta;\Gamma \vdash \ell \approx \ell : \mathsf{box}\ \psi$
- $\Psi;\Delta;\Gamma \vdash \ell \approx_{\mathrm{v}} \ell : \mathsf{box}\ \psi$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \ell : \mathsf{box}\ \psi$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By definition of $W \in \mathcal{H}[\![\Psi]\!]$,

$$(W, \rho_1(\gamma_1(\ell)), \rho_2(\gamma_2(\ell))) = (W, \ell, \ell) \in \mathcal{V}[\![\mathsf{box}\ \psi]\!]\emptyset = \mathcal{V}[\![\mathsf{box}\ \psi]\!]\rho,$$

so we are done. □

Lemma 10.42 (A Application)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t_1} \approx \mathsf{t_2} : \mathsf{box}\ \forall[].(\overline{\tau}) \to \tau'$ and $\overline{\Psi;\Delta;\Gamma \vdash \mathsf{t_1'} \approx \mathsf{t_2'} : \tau}$, then $\Psi;\Delta;\Gamma \vdash \mathsf{t_1}\ []\ \overline{\mathsf{t_1'}} \approx \mathsf{t_2}\ []\ \overline{\mathsf{t_2'}} : \tau'$.

Proof

First note that $\Psi;\Delta;\Gamma \vdash \mathbf{t_1}\ []\ \overline{\mathbf{t'_1}} : \tau'$ and $\Psi;\Delta;\Gamma \vdash \mathbf{t_2}\ []\ \overline{\mathbf{t'_2}} : \tau'$.
Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathbf{t_1}\ []\ \overline{\mathbf{t'_1}})), \rho_2(\gamma_2(\mathbf{t_2}\ []\ \overline{\mathbf{t'_2}}))) = (W, \rho_1(\gamma_1(\mathbf{t_1}))\ []\ \overline{\rho_1(\gamma_1(\mathbf{t'_1}))}, \rho_2(\gamma_2(\mathbf{t_2}))\ []\ \overline{\rho_2(\gamma_2(\mathbf{t'_2}))}) \in \mathcal{E}[\![\tau']\!]\rho.$$

Let $W_0 \sqsupseteq_{\text{pub}} W$ and $(W_0, \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\mathbf{box}\,\forall[].(\overline{\tau}) \to \tau']\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W_0, \mathbf{v_1}\ []\ \overline{\rho_1(\gamma_1(\mathbf{t'_1}))}, \mathbf{v_2}\ []\ \overline{\rho_2(\gamma_2(\mathbf{t'_2}))}) \in \mathcal{E}[\![\tau']\!]\rho.$$

Let $W_i \sqsupseteq_{\text{pub}} W_{i-1}$ and $\overline{(W_i, \mathbf{v'_{1i}}, \mathbf{v'_{2i}}) \in \mathcal{V}[\![\tau]\!]\rho}$. By further applications of 8.20, it suffices to show that

$$(W_n, \mathbf{v_1}\ []\ \overline{\mathbf{v'_1}}, \mathbf{v_2}\ []\ \overline{\mathbf{v'_2}}) \in \mathcal{E}[\![\tau']\!]\rho.$$

By definition of $\mathcal{V}[\![\mathbf{box}\,\forall[].(\overline{\tau}) \to \tau']\!]\rho$, we know $\mathbf{v_1} = \ell_1[\overline{\hat{\tau}_1}]$, $\mathbf{v_2} = \ell_2[\overline{\hat{\tau}_2}]$, and for any $(M_1, M_2) : W_0$,

$$M_1(\ell_1) = \boldsymbol{\lambda}[\overline{\alpha_1}]\,(\overline{\tau_1}).\mathbf{t_1}, \qquad \overline{\tau_1[\overline{\hat{\tau}_1/\alpha_1}] = \rho_1(\overline{\tau})},$$
$$M_2(\ell_2) = \boldsymbol{\lambda}[\overline{\alpha_2}]\,(\overline{\tau_2}).\mathbf{t_2}, \qquad \overline{\tau_2[\overline{\hat{\tau}_2/\alpha_2}] = \rho_2(\overline{\tau})},$$

and $(W_n, \boldsymbol{\lambda}[]\,(\overline{\mathbf{x} : \rho_1(\tau)}).\mathbf{t_1}[\overline{\hat{\tau}_1/\alpha_1}], \boldsymbol{\lambda}[]\,(\overline{\mathbf{x} : \rho_2(\tau)}).\mathbf{t_2}[\overline{\hat{\tau}_2/\alpha_2}]) \in \mathcal{HV}[\![\boldsymbol{\lambda}[]\,(\overline{\tau}).\tau']\!]\rho$. By Lemma 8.15, it suffices to show that

$$(W_n, \mathbf{t_1}[\overline{\hat{\tau}_1/\alpha_1}][\overline{\mathbf{v'_1}/\mathbf{x}}], \mathbf{t_2}[\overline{\hat{\tau}_2/\alpha_2}][\overline{\mathbf{v'_2}/\mathbf{x}}]) \in \mathcal{E}[\![\tau']\!]\rho.$$

Since $W_n \sqsupseteq W_0$ and $\overline{(W_n, \mathbf{v'_1}, \mathbf{v'_2}) \in \mathcal{V}[\![\tau]\!]\rho}$, we can instantiate $\mathcal{HV}[\![\boldsymbol{\lambda}[]\,(\overline{\tau}).\tau']\!]\rho$ to get exactly the needed result. □

Lemma 10.43 (A Type Application)
If $\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \mathbf{box}\,\forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau'$ and $\Delta \vdash \hat{\tau}$, then

$$\Psi;\Delta;\Gamma \vdash \mathbf{t_1}[\hat{\tau}] \approx \mathbf{t_2}[\hat{\tau}] : \mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta].$$

Proof

First note that $\Psi;\Delta;\Gamma \vdash \mathbf{t_i}[\hat{\tau}] : \mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]$ for $i \in \{1,2\}$.
Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathbf{t_1}[\hat{\tau}])), \rho_2(\gamma_2(\mathbf{t_2}[\hat{\tau}])))$$
$$= (W, \rho_1(\gamma_1(\mathbf{t_1}))[\rho_1(\hat{\tau})], \rho_2(\gamma_2(\mathbf{t_2}))[\rho_2(\hat{\tau})]) \in \mathcal{E}[\![\mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]]\!]\rho.$$

By our assumption, $(W, \rho_1(\gamma_1(\mathbf{t_1})), \rho_2(\gamma_2(\mathbf{t_2}))) \in \mathcal{E}[\![\mathbf{box}\,\forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho$. Let $W' \sqsupseteq_{\text{pub}} W$ and

$$(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\mathbf{box}\,\forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho.$$

By Lemma 8.20, it suffices to show that

$$(W', \mathbf{v_1}[\rho_1(\hat{\tau})], \mathbf{v_2}[\rho_2(\hat{\tau})]) \in \mathcal{E}[\![\mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]]\!]\rho.$$

Let $\mathrm{VR} = (\rho_1(\hat{\tau}), \rho_2(\hat{\tau}), \mathcal{V}[\![\hat{\tau}]\!]\rho)$. By Lemma 8.9 and Lemma 10.5, it suffices to show that

$$(W', \mathbf{v_1}[\rho_1(\hat{\tau})], \mathbf{v_2}[\rho_2(\hat{\tau})]) \in \mathcal{V}[\![\mathbf{box}\,\forall[\overline{\alpha}].(\overline{\tau[\hat{\tau}/\beta]}) \to \tau'[\hat{\tau}/\beta]]\!]\rho = \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho[\beta \mapsto \mathrm{VR}].$$

We can reach this easily from our hypothesis that $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\mathbf{box}\,\forall[\beta, \overline{\alpha}].(\overline{\tau}) \to \tau']\!]\rho$. □

Lemma 10.44 (A Allocate Ref)
If $\overline{\Psi;\Delta;\Gamma \vdash \mathbf{t_1} \approx \mathbf{t_2} : \tau}$, then $\Psi;\Delta;\Gamma \vdash \mathbf{ralloc}\ \langle\overline{\mathbf{t_1}}\rangle \approx \mathbf{ralloc}\ \langle\overline{\mathbf{t_2}}\rangle : \mathbf{ref}\ \langle\overline{\tau}\rangle$.

Proof

Note that $\Psi; \Delta; \Gamma \vdash \mathsf{ralloc}\ \langle \overline{\mathsf{t_1}} \rangle : \mathsf{ref}\ \langle \overline{\tau} \rangle$ and $\Psi; \Delta; \Gamma \vdash \mathsf{ralloc}\ \langle \overline{\mathsf{t_2}} \rangle : \mathsf{ref}\ \langle \overline{\tau} \rangle$.
Let $W_0 \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W_0, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W_0, \rho_1(\gamma_1(\mathsf{ralloc}\ \langle \overline{\mathsf{t_1}} \rangle)), \rho_2(\gamma_2(\mathsf{ralloc}\ \langle \overline{\mathsf{t_2}} \rangle))) \\ = (W_0, \mathsf{ralloc}\ \langle \overline{\rho_1(\gamma_1(\mathsf{t_1}))} \rangle, \mathsf{ralloc}\ \langle \overline{\rho_1(\gamma_1(\mathsf{t_1}))} \rangle) \in \mathcal{E}[\![\mathsf{ref}\ \langle \overline{\tau} \rangle]\!]\rho.$$

Let $W_i \sqsupseteq_{\text{pub}} W_{i-1}$ and $\overline{(W_i, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho}$. By repeated application of Lemma 8.20, it suffices to show that

$$(W_n, \mathsf{ralloc}\ \langle \overline{\mathsf{v_1}} \rangle, \mathsf{ralloc}\ \langle \overline{\mathsf{v_2}} \rangle) \in \mathcal{E}[\![\mathsf{ref}\ \langle \overline{\tau} \rangle]\!]\rho.$$

Let $(M_1, M_2) : W_n$. Note that

$$\langle M_1 \mid \mathsf{ralloc}\ \langle \overline{\mathsf{v_1}} \rangle \rangle \longmapsto \langle M_1, \ell_1 \mapsto \langle \overline{\mathsf{v_1}} \rangle \mid \ell_1 \rangle \quad \text{and} \quad \langle M_2 \mid \mathsf{ralloc}\ \langle \overline{\mathsf{v_2}} \rangle \rangle \longmapsto \langle M_2, \ell_2 \mapsto \langle \overline{\mathsf{v_2}} \rangle \mid \ell_2 \rangle.$$

Thus, by Lemma 8.14 and Lemma 8.9, it suffices to find some $W' \sqsupseteq W_n$ such that

$$(M_1, \ell_1 \mapsto \langle \overline{\mathsf{v_1}} \rangle, M_2, \ell_2 \mapsto \langle \overline{\mathsf{v_2}} \rangle) : W' \quad \text{and} \quad (W', \ell_1, \ell_2) \in \mathcal{V}[\![\mathsf{ref}\ \langle \overline{\tau} \rangle]\!]\rho.$$

We can do this by constructing an island that satisfies the requirements of $\mathcal{V}[\![\mathsf{ref}\ \langle \overline{\tau} \rangle]\!]\rho$ and adding it to W_n. In particular, let

$$W' = (W_n.k, ((W_n.\Psi_1), \ell_1 : {}^{\mathsf{ref}}\langle \overline{\tau} \rangle), ((W_n.\Psi_2), \ell_2 : {}^{\mathsf{ref}}\langle \overline{\tau} \rangle), ((W_n.\Theta), \theta)),$$

where

$$\theta = (\bullet, \{\bullet\}, \{\}, \{\}, \lambda s.\{(\widetilde{W}, \{\ell_1 \mapsto \mathsf{h_1}\}, \{\ell_2 \mapsto \mathsf{h_2}\}) \mid (\widetilde{W}, \mathsf{h_1}, \mathsf{h_2}) \in \mathcal{HV}[\![\langle \overline{\tau} \rangle]\!]\rho\}, \lambda s.\{(\ell_1, \ell_2)\}).$$

From here it suffices to show that $(\triangleright W', \langle \overline{\mathsf{v_1}} \rangle, \langle \overline{\mathsf{v_2}} \rangle) \in \mathcal{HV}[\![\langle \overline{\tau} \rangle]\!]\rho$. But this follows from monotonicity and our assumption that $\overline{(W_i, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho}$. □

Lemma 10.45 (A Allocate Box)
If $\overline{\Psi; \Delta; \Gamma \vdash \mathsf{t_1} \approx \mathsf{t_2} : \tau}$, then $\Psi; \Delta; \Gamma \vdash \mathsf{balloc}\ \langle \overline{\mathsf{t_1}} \rangle \approx \mathsf{balloc}\ \langle \overline{\mathsf{t_2}} \rangle : \mathsf{box}\ \langle \overline{\tau} \rangle$.

Proof

Note that $\Psi; \Delta; \Gamma \vdash \mathsf{balloc}\ \langle \overline{\mathsf{t_1}} \rangle : \mathsf{box}\ \langle \overline{\tau} \rangle$ and $\Psi; \Delta; \Gamma \vdash \mathsf{balloc}\ \langle \overline{\mathsf{t_2}} \rangle : \mathsf{box}\ \langle \overline{\tau} \rangle$.
Let $W_0 \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W_0, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W_0, \rho_1(\gamma_1(\mathsf{balloc}\ \langle \overline{\mathsf{t_1}} \rangle)), \rho_2(\gamma_2(\mathsf{balloc}\ \langle \overline{\mathsf{t_2}} \rangle))) \\ = (W_0, \mathsf{balloc}\ \langle \overline{\rho_1(\gamma_1(\mathsf{t_1}))} \rangle, \mathsf{balloc}\ \langle \overline{\rho_1(\gamma_1(\mathsf{t_1}))} \rangle) \in \mathcal{E}[\![\mathsf{box}\ \langle \overline{\tau} \rangle]\!]\rho.$$

Let $W_i \sqsupseteq_{\text{pub}} W_{i-1}$ and $\overline{(W_i, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho}$. By repeated application of Lemma 8.20, it suffices to show that

$$(W_n, \mathsf{balloc}\ \langle \overline{\mathsf{v_1}} \rangle, \mathsf{balloc}\ \langle \overline{\mathsf{v_2}} \rangle) \in \mathcal{E}[\![\mathsf{box}\ \langle \overline{\tau} \rangle]\!]\rho.$$

Let $(M_1, M_2) : W_n$. Note that

$$\langle M_1 \mid \mathsf{balloc}\ \langle \overline{\mathsf{v_1}} \rangle \rangle \longmapsto \langle M_1, \ell_1 \mapsto \langle \overline{\mathsf{v_1}} \rangle \mid \ell_1 \rangle \quad \text{and} \quad \langle M_2 \mid \mathsf{balloc}\ \langle \overline{\mathsf{v_2}} \rangle \rangle \longmapsto \langle M_2, \ell_2 \mapsto \langle \overline{\mathsf{v_2}} \rangle \mid \ell_2 \rangle.$$

Thus, by Lemma 8.14 and Lemma 8.9, it suffices to show that

$$(M_1, \ell_1 \mapsto \langle \overline{\mathsf{v_1}} \rangle, M_2, \ell_2 \mapsto \langle \overline{\mathsf{v_2}} \rangle) : W_n \boxplus (\ell_1 \mapsto \langle \overline{\mathsf{v_1}} \rangle, \ell_2 \mapsto \langle \overline{\mathsf{v_2}} \rangle)$$

and

$$(W_n \boxplus (\ell_1 \mapsto \langle \overline{\mathsf{v_1}} \rangle, \ell_2 \mapsto \langle \overline{\mathsf{v_2}} \rangle), \ell_1, \ell_2) \in \mathcal{V}[\![\mathsf{box}\ \langle \overline{\tau} \rangle]\!]\rho.$$

This amounts to showing that $(W_n \boxplus (\ell_1 \mapsto \langle \overline{\mathsf{v_1}} \rangle, \ell_2 \mapsto \langle \overline{\mathsf{v_2}} \rangle), \langle \overline{\mathsf{v_1}} \rangle, \langle \overline{\mathsf{v_2}} \rangle) \in \mathcal{HV}[\![\langle \overline{\tau} \rangle]\!]\rho$. But this follows from monotonicity and our assumption that $\overline{(W_i, \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho}$. □

Lemma 10.46 (A Read from Ref)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \mathsf{ref}\ \langle\overline{\tau}\rangle$, then $\Psi;\Delta;\Gamma \vdash \mathsf{read[i]}\ \mathsf{t}_1 \approx \mathsf{read[i]}\ \mathsf{t}_2 : \tau_\mathsf{i}$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathsf{read[i]}\ \mathsf{t}_1 : \tau_\mathsf{i}$ and $\Psi;\Delta;\Gamma \vdash \mathsf{read[i]}\ \mathsf{t}_2 : \tau_\mathsf{i}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{read[i]}\ \mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{read[i]}\ \mathsf{t}_2))) = (W, \mathsf{read[i]}\ \rho_1(\gamma_1(\mathsf{t}_1)), \mathsf{read[i]}\ \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\tau_\mathsf{i}]\!]\rho.$$

By our hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\mathsf{ref}\ \langle\overline{\tau}\rangle]\!]\rho$. Let $W' \sqsupseteq W$ and

$$(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mathsf{ref}\ \langle\overline{\tau}\rangle]\!]\rho.$$

By Lemma 8.20, it suffices to show that

$$(W', \mathsf{read[i]}\ \mathsf{v}_1, \mathsf{read[i]}\ \mathsf{v}_2) \in \mathcal{E}[\![\tau_\mathsf{i}]\!]\rho.$$

By definition of $\mathcal{V}[\![\mathsf{ref}\ \langle\overline{\tau}\rangle]\!]\rho$ and $\mathcal{H}\mathcal{V}[\![\langle\overline{\tau}\rangle]\!]\rho$, we know that $\mathsf{v}_1 = \ell_1$ and $\mathsf{v}_2 = \ell_2$, where for any $(M_1, M_2) : W$, $M_1(\ell_1) = \langle\hat{\mathsf{v}}_1\rangle$, $M_2(\ell_2) = \langle\hat{\mathsf{v}}_2\rangle$, and $(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho$. By the operational semantics and by Lemma 8.15, it suffices to show that

$$(W', \hat{\mathsf{v}}_{1\mathsf{i}}, \hat{\mathsf{v}}_{2\mathsf{i}}) \in \mathcal{E}[\![\tau_\mathsf{i}]\!]\rho.$$

But this follows from Lemma 8.9. □

Lemma 10.47 (A Read from Box)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \mathsf{box}\ \langle\overline{\tau}\rangle$, then $\Psi;\Delta;\Gamma \vdash \mathsf{read[i]}\ \mathsf{t}_1 \approx \mathsf{read[i]}\ \mathsf{t}_2 : \tau_\mathsf{i}$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathsf{read[i]}\ \mathsf{t}_1 : \tau_\mathsf{i}$ and $\Psi;\Delta;\Gamma \vdash \mathsf{read[i]}\ \mathsf{t}_2 : \tau_\mathsf{i}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{read[i]}\ \mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{read[i]}\ \mathsf{t}_2))) = (W, \mathsf{read[i]}\ \rho_1(\gamma_1(\mathsf{t}_1)), \mathsf{read[i]}\ \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\tau_\mathsf{i}]\!]\rho.$$

By our hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t}_1)), \rho_2(\gamma_2(\mathsf{t}_2))) \in \mathcal{E}[\![\mathsf{box}\ \langle\overline{\tau}\rangle]\!]\rho$. Let $W' \sqsupseteq W$ and

$$(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\mathsf{box}\ \langle\overline{\tau}\rangle]\!]\rho.$$

By Lemma 8.20, it suffices to show that

$$(W', \mathsf{read[i]}\ \mathsf{v}_1, \mathsf{read[i]}\ \mathsf{v}_2) \in \mathcal{E}[\![\tau_\mathsf{i}]\!]\rho.$$

By definition of $\mathcal{V}[\![\mathsf{box}\ \langle\overline{\tau}\rangle]\!]\rho$ and $\mathcal{H}\mathcal{V}[\![\langle\overline{\tau}\rangle]\!]\rho$, we know that $\mathsf{v}_1 = \ell_1$ and $\mathsf{v}_2 = \ell_2$, where for any $(M_1, M_2) : W$, $M_1(\ell_1) = \langle\hat{\mathsf{v}}_1\rangle$, $M_2(\ell_2) = \langle\hat{\mathsf{v}}_2\rangle$, and $(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho$. By the operational semantics and by Lemma 8.15, it suffices to show that

$$(W', \hat{\mathsf{v}}_{1\mathsf{i}}, \hat{\mathsf{v}}_{2\mathsf{i}}) \in \mathcal{E}[\![\tau_\mathsf{i}]\!]\rho.$$

But this follows from Lemma 8.9. □

Lemma 10.48 (A Write to Ref)
If $\Psi;\Delta;\Gamma \vdash \mathsf{t}_1 \approx \mathsf{t}_2 : \mathsf{ref}\ \langle\overline{\tau}\rangle$ and $\Psi;\Delta;\Gamma \vdash \mathsf{t}'_1 \approx \mathsf{t}'_2 : \tau_\mathsf{i}$, then

$$\Psi;\Delta;\Gamma \vdash \mathsf{write}\ \mathsf{t}_1\ [\mathsf{i}] \leftarrow \mathsf{t}'_1 \approx \mathsf{write}\ \mathsf{t}_1\ [\mathsf{i}] \leftarrow \mathsf{t}'_2 : \mathsf{unit}.$$

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathsf{write}\,\mathsf{t_1}\,[\mathsf{i}] \leftarrow \mathsf{t_1'} : \mathsf{unit}$ and $\Psi;\Delta;\Gamma \vdash \mathsf{write}\,\mathsf{t_2}\,[\mathsf{i}] \leftarrow \mathsf{t_2'} : \mathsf{unit}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{write}\,\mathsf{t_1}\,[\mathsf{i}] \leftarrow \mathsf{t_1'})), \rho_2(\gamma_2(\mathsf{write}\,\mathsf{t_2}\,[\mathsf{i}] \leftarrow \mathsf{t_2'}))) \\ = (W, \mathsf{write}\,\rho_1(\gamma_1(\mathsf{t_1}))\,[\mathsf{i}] \leftarrow \rho_1(\gamma_1(\mathsf{t_1'})), \mathsf{write}\,\rho_2(\gamma_2(\mathsf{t_2}))\,[\mathsf{i}] \leftarrow \rho_2(\gamma_2(\mathsf{t_2'}))) \in \mathcal{E}[\![()]\!]\rho.$$

By our hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t_1})), \rho_2(\gamma_2(\mathsf{t_2}))) \in \mathcal{E}[\![\mathsf{ref}\,\langle\overline{\tau}\rangle]\!]\rho$ and $(W, \rho_1(\gamma_1(\mathsf{t_1'})), \rho_2(\gamma_2(\mathsf{t_2'}))) \in \mathcal{E}[\![\tau_i]\!]\rho$. Let $W' \sqsupseteq_{\mathrm{pub}} W$ and $(W', \mathsf{v_1}, \mathsf{v_2}) \in \mathcal{V}[\![\mathsf{ref}\,\langle\overline{\tau}\rangle]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{write}\,\mathsf{v_1}\,[\mathsf{i}] \leftarrow \rho_1(\gamma_1(\mathsf{t_1'})), \mathsf{write}\,\mathsf{v_2}\,[\mathsf{i}] \leftarrow \rho_2(\gamma_2(\mathsf{t_2'}))) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho.$$

Let $W'' \sqsupseteq_{\mathrm{pub}} W'$ and $(W'', \mathsf{v_1'}, \mathsf{v_2'}) \in \mathcal{V}[\![\tau_i]\!]\rho$. By another application of Lemma 8.20, it suffices to show that

$$(W'', \mathsf{write}\,\mathsf{v_1}\,[\mathsf{i}] \leftarrow \mathsf{v_1'}, \mathsf{write}\,\mathsf{v_2}\,[\mathsf{i}] \leftarrow \mathsf{v_2'}) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho.$$

Let $(M_1, M_2) : W''$. By definition of $\mathcal{V}[\![\mathsf{ref}\,\langle\overline{\tau}\rangle]\!]\rho$ and $\mathcal{HV}[\![\langle\overline{\tau}\rangle]\!]\rho$, we know that $\mathsf{v_1} = \ell_1$ and $\mathsf{v_2} = \ell_2$, where $M_1(\ell_1) = \langle \hat{\mathsf{v}}_{11}, \ldots, \hat{\mathsf{v}}_{1i}, \ldots, \hat{\mathsf{v}}_{1n}\rangle$, $M_2(\ell_2) = \langle \hat{\mathsf{v}}_{21}, \ldots, \hat{\mathsf{v}}_{2i}, \ldots, \hat{\mathsf{v}}_{2n}\rangle$, and $(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho$. Note that

$$\langle M_1 \mid \mathsf{write}\,\mathsf{v_1}\,[\mathsf{i}] \leftarrow \mathsf{v_1'}\rangle \longmapsto \langle M_1[\ell_1 \mapsto \langle \hat{\mathsf{v}}_{11}, \ldots, \mathsf{v_1'}, \ldots, \hat{\mathsf{v}}_{1n}\rangle] \mid ()\rangle$$

and

$$\langle M_2 \mid \mathsf{write}\,\mathsf{v_2}\,[\mathsf{i}] \leftarrow \mathsf{v_2'}\rangle \longmapsto \langle M_2[\ell_2 \mapsto \langle \hat{\mathsf{v}}_{21}, \ldots, \mathsf{v_2'}, \ldots, \hat{\mathsf{v}}_{2n}\rangle] \mid ()\rangle.$$

To apply Lemma 8.15, we need to show that

$$(M_1[\ell_1 \mapsto \langle \hat{\mathsf{v}}_{11}, \ldots, \mathsf{v_1'}, \ldots, \hat{\mathsf{v}}_{1n}\rangle], M_2[\ell_2 \mapsto \langle \hat{\mathsf{v}}_{21}, \ldots, \mathsf{v_2'}, \ldots, \hat{\mathsf{v}}_{2n}\rangle]) : W''.$$

But this follows from the definition of $\mathcal{V}[\![\mathsf{ref}\,\langle\overline{\tau}\rangle]\!]\rho$ and from

$$(W'', \langle \hat{\mathsf{v}}_{11}, \ldots, \mathsf{v_1'}, \ldots, \hat{\mathsf{v}}_{1n}\rangle, \langle \hat{\mathsf{v}}_{21}, \ldots, \mathsf{v_2'}, \ldots, \hat{\mathsf{v}}_{2n}\rangle) \in \mathcal{HV}[\![\langle\overline{\tau}\rangle]\!]\rho,$$

so we can indeed apply Lemma 8.15, by which it suffices to show that $(W'', (), ()) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho$. This follows from Lemma 8.9. □

Lemma 10.49 (AC Boundary)
If $\Psi;\Delta;\Gamma \vdash \mathsf{e_1} \approx \mathsf{e_2} : \tau$, then $\Psi;\Delta;\Gamma \vdash \mathcal{AC}^{\tau}\,\mathsf{e_1} \approx \mathcal{AC}^{\tau}\,\mathsf{e_2} : \tau^{\langle\mathcal{A}\rangle}$.

Proof

Note that $\Psi;\Delta;\Gamma \vdash \mathcal{AC}^{\tau}\,\mathsf{e_1} : \tau^{\langle\mathcal{A}\rangle}$ and $\Psi;\Delta;\Gamma \vdash \mathcal{AC}^{\tau}\,\mathsf{e_2} : \tau^{\langle\mathcal{A}\rangle}$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By our assumption,

$$(W, \rho_1(\gamma_1(\mathsf{e_1})), \rho_2(\gamma_2(\mathsf{e_2}))) \in \mathcal{E}[\![\tau]\!]\rho.$$

By the bridge lemma,

$$(W, \mathcal{AC}^{\rho_1(\tau)}\,\rho_1(\gamma_1(\mathsf{e_1})), \mathcal{AC}^{\rho_2(\tau)}\,\rho_2(\gamma_2(\mathsf{e_2}))) = (W, \rho_1(\gamma_1(\mathcal{AC}^{\tau}\,\mathsf{e_1})), \rho_2(\gamma_2(\mathcal{AC}^{\tau}\,\mathsf{e_2}))) \in \mathcal{E}[\![\tau^{\langle\mathcal{A}\rangle}]\!]\rho,$$

as desired. □

The next two compatibility lemmas have a slightly different shape, as they cover the two type rules for heap values.

Lemma 10.50 (A Function)
If $\Psi;\overline{\alpha};\overline{\mathsf{x}:\tau} \vdash \mathsf{t_1} \approx \mathsf{t_2} : \tau'$, then $\Psi \vdash \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\tau}).\mathsf{t_1} \approx_{\mathrm{hv}} \lambda[\overline{\alpha}]\,(\overline{\mathsf{x}:\tau}).\mathsf{t_2} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$.

Proof

Note that $\Psi \vdash \lambda[\overline{\alpha}](\overline{x:\tau}).t_1 : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ and $\Psi \vdash \lambda[\overline{\alpha}](\overline{x:\tau}).t_2 : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$.

Let $W \in \mathcal{H}[\![\Psi]\!]$. We need to show that $(W, \lambda[\overline{\alpha}](\overline{x:\tau}).t_1, \lambda[\overline{\alpha}](\overline{x:\tau}).t_2) \in \mathcal{HV}[\![\forall[\overline{\alpha}].(\overline{\tau}) \to \tau']\!]\emptyset$.

Let $W' \sqsupseteq W$, $\overline{\mathrm{VR} \in \mathrm{AValRel}}$, and $\overline{(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]}$.

We need to show that

$$(W', t_1\overline{[\mathrm{VR}.\tau_1/\alpha][v_1/x]}, t_2\overline{[\mathrm{VR}.\tau_2/\alpha][v_2/x]}) \in \mathcal{E}[\![\tau']\!]\emptyset\overline{[\alpha \mapsto \mathrm{VR}]}.$$

We have $W' \in \mathcal{H}[\![\Psi]\!]$, $\emptyset\overline{[\alpha \mapsto \mathrm{VR}]} \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W', \cdot\overline{[x \mapsto (v_1, v_2)]}) \in \mathcal{G}[\![\overline{x:\tau}]\!]\emptyset\overline{[\alpha \mapsto \mathrm{VR}]}$. Applying our assumption gives the result. □

Lemma 10.51 (A Tuple)
If $\overline{\Psi; \cdot; \cdot \vdash v_1 \approx_v v_2 : \tau}$, then $\Psi \vdash \langle\overline{v_1}\rangle \approx_{hv} \langle\overline{v_2}\rangle : \langle\overline{\tau}\rangle$.

Proof

Note that $\Psi \vdash \langle\overline{v_1}\rangle : \langle\overline{\tau}\rangle$ and $\Psi \vdash \langle\overline{v_2}\rangle : \langle\overline{\tau}\rangle$.

Let $W \in \mathcal{H}[\![\Psi]\!]$. By our assumption, $\overline{(W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\emptyset}$, which is exactly what we need. □

The remaining compatibility lemmas for A are identical to cases from F and C, so we omit their proofs.

Lemma 10.52 (A Variable)
If $x:\tau \in \Gamma$, then $\Psi; \Delta; \Gamma \vdash x \approx x : \tau$.

Lemma 10.53 (A Unit)

- $\Psi; \Delta; \Gamma \vdash () \approx () : \mathsf{unit}$
- $\Psi; \Delta; \Gamma \vdash () \approx_v () : \mathsf{unit}$.

Lemma 10.54 (A Int)

- $\Psi; \Delta; \Gamma \vdash n \approx n : \mathsf{int}$
- $\Psi; \Delta; \Gamma \vdash n \approx_v n : \mathsf{int}$.

Lemma 10.55 (A Primitive)
If $\Psi; \Delta; \Gamma \vdash t_1 \approx t_2 : \mathsf{int}$ and $\Psi; \Delta; \Gamma \vdash t_1' \approx t_2' : \mathsf{int}$, then $\Psi; \Delta; \Gamma \vdash t_1\ p\ t_1' \approx t_2\ p\ t_2' : \mathsf{int}$.

Lemma 10.56 (A If0)
If $\Psi; \Delta; \Gamma \vdash t_1 \approx t_2 : \mathsf{int}$, $\Psi; \Delta; \Gamma \vdash t_1' \approx t_2' : \tau$, and $\Psi; \Delta; \Gamma \vdash t_1'' \approx t_2'' : \tau$, then

$$\Psi; \Delta; \Gamma \vdash \mathsf{if0}\ t_1\ t_1'\ t_1'' \approx \mathsf{if0}\ t_2\ t_2'\ t_2'' : \tau.$$

Lemma 10.57 (A Pack)

- If $\Psi; \Delta; \Gamma \vdash t_1 \approx t_2 : \tau[\tau'/\alpha]$, then $\Psi; \Delta; \Gamma \vdash \mathsf{pack}\langle\tau', t_1\rangle\ \mathsf{as}\ \exists\alpha.\tau \approx \mathsf{pack}\langle\tau', t_2\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau$
- If $\Psi; \Delta; \Gamma \vdash v_1 \approx_v v_2 : \tau[\tau'/\alpha]$, then $\Psi; \Delta; \Gamma \vdash \mathsf{pack}\langle\tau', v_1\rangle\ \mathsf{as}\ \exists\alpha.\tau \approx_v \mathsf{pack}\langle\tau', v_2\rangle\ \mathsf{as}\ \exists\alpha.\tau : \exists\alpha.\tau$.

Lemma 10.58 (A Unpack)
If $\Psi; \Delta; \Gamma \vdash t_1 \approx t_2 : \exists\alpha.\tau$ and $\Psi; (\Delta, \alpha); (\Gamma, x:\tau) \vdash t_1' \approx t_2' : \tau'$, then

$$\Psi; \Delta; \Gamma \vdash \mathsf{unpack}\ \langle\alpha, x\rangle = t_1\ \mathsf{in}\ t_1' \approx \mathsf{unpack}\ \langle\alpha, x\rangle = t_2\ \mathsf{in}\ t_2' : \tau'.$$

Lemma 10.59 (A Fold)

- If $\Psi; \Delta; \Gamma \vdash t_1 \approx t_2 : \tau[\mu\alpha.\tau/\alpha]$, then $\Psi; \Delta; \Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\ t_1 \approx \mathsf{fold}_{\mu\alpha.\tau}\ t_2 : \mu\alpha.\tau$
- If $\Psi; \Delta; \Gamma \vdash v_1 \approx_v v_2 : \tau[\mu\alpha.\tau/\alpha]$, then $\Psi; \Delta; \Gamma \vdash \mathsf{fold}_{\mu\alpha.\tau}\ v_1 \approx_v \mathsf{fold}_{\mu\alpha.\tau}\ v_2 : \mu\alpha.\tau$.

Lemma 10.60 (A Unfold)
If $\Psi; \Delta; \Gamma \vdash t_1 \approx t_2 : \mu\alpha.\tau$, then $\Psi; \Delta; \Gamma \vdash \mathsf{unfold}\ t_1 \approx \mathsf{unfold}\ t_2 : \tau[\mu\alpha.\tau/\alpha]$.

10.4 Fundamental Property and Soundness

Lemma 10.61 (Fundamental Property)

- If $\Psi; \Delta; \Gamma \vdash e : \tau$, then $\Psi; \Delta; \Gamma \vdash e \approx e : \tau$
- If $\Psi; \Delta; \Gamma \vdash v : \tau$, then $\Psi; \Delta; \Gamma \vdash v \approx_{\mathrm{v}} v : \tau$
- If $\Psi \vdash \mathsf{h} : \psi$, then $\Psi \vdash \mathsf{h} \approx_{\mathrm{hv}} \mathsf{h} : \psi$.

Proof

We prove all three claims simultaneously, by induction on the typing derivations, using the compatibility lemmas. □

Lemma 10.62 (Weakening)
If $\Psi; \Delta; \Gamma \vdash e_1 \approx e_2 : \tau$ and $\Psi \subseteq \Psi'$, $\Delta \subseteq \Delta'$, $\Gamma \subseteq \Gamma'$, then $\Psi'; \Delta'; \Gamma' \vdash e_1 \approx e_2 : \tau$.

Proof

Let $W \in \mathcal{H}[\![\Psi']\!]$, $\rho' \in \mathcal{D}[\![\Delta']\!]$, and $(W, \gamma') \in \mathcal{G}[\![\Gamma']\!]\rho$.

Let $\rho = \rho'|_\Delta$ and $\gamma = \gamma'|_\Gamma$. Note that $W \in \mathcal{H}[\![\Psi]\!]$ and $\rho \in \mathcal{D}[\![\Delta]\!]$ immediately. By our hypothesis, it suffices to show that $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. Clearly, $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho'$. Since the free type variables of Γ are all in Δ, $\mathcal{G}[\![\Gamma]\!]\rho' = \mathcal{G}[\![\Gamma]\!]\rho$, so we are done. □

Lemma 10.63 (Congruence)
If $\Psi; \Delta; \Gamma \vdash e_1 \approx e_2 : \tau$ and $\vdash C : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \Delta'; \Gamma' \vdash \tau')$, then $\Psi'; \Delta'; \Gamma' \vdash C[e_1] \approx C[e_2] : \tau'$.

Proof

By induction on the type derivation for C, using Lemma 10.62 for the cases where C is empty, and the compatibility lemmas for all other cases. □

Lemma 10.64 (Canonical World)
If $\vdash M : \Psi$, then for any k, $\exists W.\ W.k = k \ \wedge\ W \in \mathcal{H}[\![\Psi]\!] \ \wedge\ (M, M) : W$.

Proof

Say that $\Psi = \mathbf{\Psi'}, \ell_1 : {}^{\mathsf{ref}}\psi_1, \ldots, \ell_n : {}^{\mathsf{ref}}\psi_n$, where $\mathrm{boxheap}(\mathbf{\Psi'})$. Let

$$\theta_i = (\bullet, \{\bullet\}, \{\}, \{\}, \lambda s.\{(W', M_1, M_2) \in \mathrm{MemAtom}_k \mid (W', M_1(\ell_i), M_2(\ell_i)) \in \mathcal{HV}[\![\psi_i]\!]\emptyset\}, \lambda s.\{(\ell_i, \ell_i)\})$$

for $1 \le i \le n$. We construct

$$W = (k, \Psi, \Psi, (\mathrm{island}_{\mathrm{box}}(k, M|_{\mathrm{dom}(\mathbf{\Psi'})}), \theta_1, \ldots, \theta_n)).$$

We need to show the following:

- For each $\ell : {}^{\mathsf{box}}\psi \in \mathbf{\Psi'}$, $(W, \ell, \ell) \in \mathcal{V}[\![\mathsf{box}\,\psi]\!]\emptyset$,
- For each i, $(W, \ell_i, \ell_i) \in \mathcal{V}[\![\mathsf{ref}\ \psi_i]\!]\emptyset$,
- $(M, M) : W$.

The first two conditions follow directly from the definitions. The last condition amounts to showing that $(\triangleright W, M(\ell_i), M(\ell_i)) \in \mathcal{HV}[\![\psi_i]\!]\emptyset$. This follows from the Fundamental Property for heap values. □

Lemma 10.65 (Adequacy)
If $\Psi; \cdot; \cdot \vdash e_1 \approx e_2 : \tau$, $\vdash M : \Psi$, then $\langle M \mid e_1 \rangle \downarrow$ if and only if $\langle M \mid e_2 \rangle \downarrow$.

Proof

We show that $\langle M \mid e_1\rangle \downarrow$ implies $\langle M \mid e_2\rangle \downarrow$, and the converse holds by an identical argument.

Suppose $\langle M \mid e_1\rangle \downarrow^k$. By Lemma 10.64, there is some $W \in \mathcal{H}[\![\Psi]\!]$ such that $(M, M) : W$ and $W.k \geq k$. So by our assumption, $(W, e_1, e_2) \in \mathcal{E}[\![\tau]\!]\emptyset$. We claim that $(W, E, E) \in \mathcal{K}[\![\tau]\!]\emptyset$, where

$$E = \begin{cases} [\cdot] & \tau = \tau \\ [\cdot] & \tau = \boldsymbol{\tau} \\ ([\cdot], \cdot) & \tau = \boldsymbol{\tau}. \end{cases}$$

If the claim holds, then $(W, E[e_1], E[e_2]) = (W, e_1, e_2) \in \mathcal{O}$. Since running$(W.k, \langle M \mid e_1\rangle)$ contradicts our assumption, we must have $\langle M \mid e_2\rangle \downarrow$, as desired.

To prove the claim, let $W' \sqsupseteq_{\text{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\emptyset$. But then

$$(W', E[v_1], E[v_2]) = (W', v_1, v_2) \in \mathcal{O}$$

trivially, so we are done. □

Lemma 10.66 (Logical Equivalence Implies Contextual Equivalence)
If $\Psi; \Delta; \Gamma \vdash e_1 \approx e_2 : \tau$, then $\Psi; \Delta; \Gamma \vdash e_1 \approx^{ctx} e_2 : \tau$.

Proof

Let $\vdash C : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \cdot; \cdot \vdash \tau')$ and $\vdash M : \Psi'$. By congruence, $\Psi'; \cdot; \cdot \vdash C[e_1] \approx C[e_2] : \tau'$. By adequacy, $\langle M \mid C[e_1]\rangle \downarrow$ if and only if $\langle M \mid C[e_2]\rangle \downarrow$, as desired. □

10.5 Completeness

Lemma 10.67 (Contextual Equivalence Implies CIU Equivalence)
If $\Psi; \Delta; \Gamma \vdash e_1 \approx^{ctx} e_2 : \tau$, then $\Psi; \Delta; \Gamma \vdash e_1 \approx^{ciu} e_2 : \tau$.

Proof

We have that $\Psi; \Delta; \Gamma \vdash e_1 : \tau$, $\Psi; \Delta; \Gamma \vdash e_2 : \tau$, and

$$\begin{aligned} \forall C, M, \Psi', \tau'.\ \vdash C : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi'; \cdot; \cdot \vdash \tau')\ \wedge\ \vdash M : \Psi' \\ \implies (\langle M \mid C[e_1]\rangle \downarrow \iff \langle M \mid C[e_2]\rangle \downarrow). \end{aligned}$$

We need to show that

$$\begin{aligned} \forall \delta, \gamma, E, M, \Psi_E, \tau_E.\ \cdot \vdash \delta : \Delta\ \wedge\ \Psi_E; \cdot; \cdot \vdash \gamma : \delta(\Gamma)\ \wedge\ \vdash E : (\Psi; \cdot; \cdot \vdash \tau) \rightsquigarrow (\Psi_E; \cdot; \cdot \vdash \tau_E)\ \wedge\ \vdash M : \Psi_E \\ \implies (\langle M \mid E[\delta(\gamma(e_1))]\rangle \downarrow \iff \langle M \mid E[\delta(\gamma(e_2))]\rangle \downarrow). \end{aligned}$$

Assume all of the premises in that implication. It suffices to find some C such that co-termination of $\langle M \mid C[e_1]\rangle$ and $\langle M \mid C[e_2]\rangle$ is equivalent to co-termination of $\langle M \mid E[\delta(\gamma(e_1))]\rangle$ and $\langle M \mid E[\delta(\gamma(e_2))]\rangle$. We will need a C such that

$$\vdash C : (\Psi; \Delta; \Gamma \vdash \tau) \rightsquigarrow (\Psi_E; \cdot; \cdot \vdash \tau_E).$$

Let

$$\tau_{\mathsf{E}} = \begin{cases} \tau & \tau_E = \tau \\ \mathsf{L}\langle\tau\rangle & \tau_E = \boldsymbol{\tau} \\ \mathsf{L}\langle\mathbf{L}\langle\tau\rangle\rangle & \tau_E = \boldsymbol{\tau} \end{cases} \qquad \boldsymbol{\tau}_{\mathbf{E}} = \begin{cases} \tau^{\langle\mathcal{C}\rangle} & \tau_E = \tau \\ \boldsymbol{\tau} & \tau_E = \boldsymbol{\tau} \\ \mathbf{L}\langle\tau\rangle & \tau_E = \boldsymbol{\tau} \end{cases} \qquad \boldsymbol{\tau}_{\mathbf{E}} = \begin{cases} \tau^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle} & \tau_E = \tau \\ \boldsymbol{\tau}^{\langle\mathcal{A}\rangle} & \tau_E = \boldsymbol{\tau} \\ \boldsymbol{\tau} & \tau_E = \boldsymbol{\tau}, \end{cases}$$

$\Delta = \Delta, \boldsymbol{\Delta}, \boldsymbol{\Delta}$, $\Gamma = \Gamma, \boldsymbol{\Gamma}, \boldsymbol{\Gamma}$, $\delta^{FC} = \delta|_{\Delta, \boldsymbol{\Delta}}$, and $\delta^{F} = \delta|_{\Delta}$.

Now choose C as follows:

$$C = (\ell\,[\delta(\mathbf{\Delta})]\,\delta(\gamma(\mathrm{dom}(\mathbf{\Gamma}))), \ell \mapsto \boldsymbol{\lambda}[\mathbf{\Delta}]\,(\delta(\mathbf{\Gamma})).\mathbf{C_t})$$
$$\mathbf{C_t} = \mathcal{AC}^{\delta^{FC}(\tau_E)}\ ((\boldsymbol{\lambda}[\mathbf{\Delta}]\,(\delta^{FC}(\mathbf{\Gamma})).\mathbf{C})\ [\delta(\mathbf{\Delta})]\ \delta^{FC}(\gamma(\mathrm{dom}(\mathbf{\Gamma}))))$$
$$\mathbf{C} = \mathcal{CF}^{\delta^{F}(\tau_E)}\ ((\lambda[\Delta]\,(\delta^{F}(\Gamma)).\mathsf{C})\ [\delta(\Delta)]\ \delta^{F}(\gamma(\mathrm{dom}(\Gamma))))$$
$$\mathsf{C} = \begin{cases} \mathsf{E} & E = \mathsf{E} \\ {}^{\tau_E}\mathcal{FC}\ \mathbf{E} & E = \mathbf{E} \\ {}^{\tau_E}\mathcal{FC}\ {}^{\tau_E}\mathcal{CA}\ \mathsf{E} & E = \mathsf{E} \end{cases}$$

By inspection of the operational semantics,

$$\langle M \mid C[e_i]\rangle \longmapsto^* \langle M, \ell \mapsto \boldsymbol{\lambda}[\mathbf{\Delta}]\,(\delta(\mathbf{\Gamma})).\mathbf{C_t} \mid \mathcal{AC}^{\delta(\tau_E)}\ (\mathcal{CF}^{\delta(\tau_E)}\ (\mathsf{C}[\delta(\gamma(e_i))]))\rangle.$$

Since this is just a fixed sequence of boundary terms around $E[\delta(\gamma(e_i))]$, we can see that this configuration co-terminates with $\langle M \mid E[\delta(\gamma(e_i))]\rangle$, as desired. □

Lemma 10.68 (CIU Equivalence Implies Logical Equivalence)
If $\Psi; \Delta; \Gamma \vdash e_1 \approx^{ciu} e_2 : \tau$, then $\Psi; \Delta; \Gamma \vdash e_1 \approx e_2 : \tau$.

Proof

We have that $\Psi; \Delta; \Gamma \vdash e_1 : \tau$, $\Psi; \Delta; \Gamma \vdash e_2 : \tau$, and

$$\forall \delta, \gamma, E, M, \Psi_E, \tau_E.\ \cdot \vdash \delta : \Delta\ \wedge\ \Psi_E; \cdot; \cdot \vdash \gamma : \delta(\Gamma)\ \wedge\ \vdash E : (\Psi; \Delta; \cdot \vdash \tau) \rightsquigarrow (\Psi_E; \cdot; \cdot \vdash \tau_E)\ \wedge\ \vdash M : \Psi_E$$
$$\implies (\langle M \mid E[\delta(\gamma(e_1))]\rangle \downarrow \iff \langle M \mid E[\delta(\gamma(e_2))]\rangle \downarrow).$$

We need to show that

$$\forall W, \rho, \gamma.\ W \in \mathcal{H}[\![\Psi]\!]\ \wedge\ \rho \in \mathcal{D}[\![\Delta]\!]\ \wedge\ (W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho\ \implies\ (W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_2))) \in \mathcal{E}[\![\tau]\!]\rho.$$

Assume all the premises of this implication.
Let $(W, E_1, E_2) \in \mathcal{K}[\![\tau]\!]\rho$. We need to show that $(W, E_1[\rho_1(\gamma_1(e_1))], E_2[\rho_2(\gamma_2(e_2))]) \in \mathcal{O}$.
Let $(M_1, M_2) : W$. It suffices to show that

$$\langle M_1 \mid E_1[\rho_1(\gamma_1(e_1))]\rangle \downarrow \iff \langle M_2 \mid E_2[\rho_2(\gamma_2(e_2))]\rangle \downarrow.$$

By the Fundamental Property, $\Psi; \Delta; \Gamma \vdash e_1 \approx e_1 : \tau$. Therefore

$$(W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_1))) \in \mathcal{E}[\![\tau]\!]\rho$$

and thus

$$\langle M_1 \mid E_1[\rho_1(\gamma_1(e_1))]\rangle \downarrow \iff \langle M_2 \mid E_2[\rho_2(\gamma_2(e_1))]\rangle \downarrow.$$

It remains to show that

$$\langle M_2 \mid E_2[\rho_2(\gamma_2(e_1))]\rangle \downarrow \iff \langle M_2 \mid E_2[\rho_2(\gamma_2(e_2))]\rangle \downarrow.$$

But this follows from our hypothesis that $\Psi; \Delta; \Gamma \vdash e_1 \approx^{ciu} e_2 : \tau$. □

11 Proofs: Compiler Correctness

Lemma 11.1

- If $\Psi; \Delta; \Gamma \vdash \mathsf{e} : \tau$, then $\Psi; \Delta; \Gamma \vdash \mathsf{e} \approx {}^{\tau}\mathcal{FC}\,\mathcal{CF}^{\tau}\,\mathsf{e} : \tau$.
- If $\Psi; \Delta; \Gamma \vdash \mathbf{e} : \tau^{\langle \mathcal{C} \rangle}$, then $\Psi; \Delta; \Gamma \vdash \mathbf{e} \approx \mathcal{CF}^{\tau}\,{}^{\tau}\mathcal{FC}\,\mathbf{e} : \tau^{\langle \mathcal{C} \rangle}$.
- If $\Psi; \Delta; \Gamma \vdash \mathbf{e} : \boldsymbol{\tau}$, then $\Psi; \Delta; \Gamma \vdash \mathbf{e} \approx {}^{\boldsymbol{\tau}}\mathcal{CA}\,\mathcal{AC}^{\boldsymbol{\tau}}\,\mathbf{e} : \boldsymbol{\tau}$.
- If $\Psi; \Delta; \Gamma \vdash \mathbf{e} : \boldsymbol{\tau}^{\langle \mathcal{A} \rangle}$, then $\Psi; \Delta; \Gamma \vdash \mathbf{e} \approx \mathcal{AC}^{\boldsymbol{\tau}}\,{}^{\boldsymbol{\tau}}\mathcal{CA}\,\mathbf{e} : \boldsymbol{\tau}^{\langle \mathcal{A} \rangle}$.

Proof

We prove the first claim; the others can be proven analogously.

First, note that $\Psi; \Delta; \Gamma \vdash {}^{\tau}\mathcal{FC}\,\mathcal{CF}^{\tau}\,\mathsf{e} : \tau$.

Let $W \in \mathcal{H}[\![\Psi]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. By the fundamental property, $\Psi; \Delta; \Gamma \vdash \mathsf{e} \approx \mathsf{e} : \tau$, so $(W, \rho_1(\gamma_1(\mathsf{e})), \rho_2(\gamma_2(\mathsf{e}))) \in \mathcal{E}[\![\tau]\!]\rho$. By boundary cancellation,

$$(W, \rho_1(\gamma_1(\mathsf{e})), {}^{\rho_2(\tau)}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau)}\,\rho_2(\gamma_2(\mathsf{e}))) \in \mathcal{E}[\![\tau]\!]\rho,$$

as desired. □

Lemma 11.2

- $\Psi; \Delta; \Gamma \vdash e_1 \approx C[\mathsf{e}_2] : \tau$ if and only if $\Psi; \Delta; \Gamma \vdash e_1 \approx C[{}^{\tau'}\mathcal{FC}\,\mathcal{CF}^{\tau'}\,\mathsf{e}_2] : \tau$.
- $\Psi; \Delta; \Gamma \vdash e_1 \approx C[\mathbf{e_2}] : \tau$ if and only if $\Psi; \Delta; \Gamma \vdash e_1 \approx C[\mathcal{CF}^{\tau'}\,{}^{\tau'}\mathcal{FC}\,\mathbf{e_2}] : \tau$.
- $\Psi; \Delta; \Gamma \vdash e_1 \approx C[\mathbf{e_2}] : \tau$ if and only if $\Psi; \Delta; \Gamma \vdash e_1 \approx C[{}^{\boldsymbol{\tau}'}\mathcal{CA}\,\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{e_2}] : \tau$.
- $\Psi; \Delta; \Gamma \vdash e_1 \approx C[\mathbf{e_2}] : \tau$ if and only if $\Psi; \Delta; \Gamma \vdash e_1 \approx C[\mathcal{AC}^{\boldsymbol{\tau}'}\,{}^{\boldsymbol{\tau}'}\mathcal{CA}\,\mathbf{e_2}] : \tau$.

Proof

We prove the first claim; the others can be proven analogously. By Lemma 11.1 and congruence, $\Psi; \Delta; \Gamma \vdash C[\mathsf{e}_2] \approx C[{}^{\tau'}\mathcal{FC}\,\mathcal{CF}^{\tau'}\,\mathsf{e}_2] : \tau$. The result follows by transitivity. □

11.1 Correctness of Closure Conversion

Lemma 11.3 (Variable)
If $\mathsf{x} : \tau \in \Gamma$, then $\cdot; \Delta; \Gamma \vdash \mathsf{x} \approx {}^{\tau}\mathcal{FC}\,(\mathcal{CF}^{\tau}\,\mathsf{x}) : \tau$.

Proof

Follows immediately from Lemma 11.1. □

Lemma 11.4 (Unit)
$\cdot; \Delta; \Gamma \vdash () \approx {}^{\mathsf{unit}}\mathcal{FC}\,() : \mathsf{unit}$.

Proof

Follows from Lemmas 8.15 and 8.9. □

Lemma 11.5 (Int)
$\cdot; \Delta; \Gamma \vdash \mathsf{n} \approx {}^{\mathsf{int}}\mathcal{FC}\,\mathbf{n} : \mathsf{int}$.

Proof

Follows from Lemmas 8.15 and 8.9. □

Lemma 11.6 (Primitive)
If $\cdot; \overline{\alpha}; \overline{\mathsf{x} : \tau'} \vdash \mathsf{t} \approx {}^{\mathsf{int}}\mathcal{FC}\,\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \mathsf{int}$ and $\cdot; \overline{\alpha}; \overline{\mathsf{x} : \tau'} \vdash \mathsf{t}' \approx {}^{\mathsf{int}}\mathcal{FC}\,\mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \mathsf{int}$, then $\cdot; \overline{\alpha}; \overline{\mathsf{x} : \tau'} \vdash \mathsf{t}\ \mathsf{p}\ \mathsf{t}' \approx {}^{\mathsf{int}}\mathcal{FC}\,(\mathbf{t}\ \mathbf{p}\ \mathbf{t}')\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \mathsf{int}$.

Proof

By Lemma 11.2, it suffices to show that

$$\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{t}\ \mathsf{p}\ \mathsf{t}' \approx {}^{\mathsf{int}}\mathcal{FC}\ (\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}))\ \mathbf{p}\ (\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]})) : \mathsf{int}.$$

Note that $\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{t}\ \mathsf{p}\ \mathsf{t}' : \mathsf{int}$ and

$$\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash {}^{\mathsf{int}}\mathcal{FC}\ (\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}))\ \mathbf{p}\ (\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]})) : \mathsf{int}.$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathsf{t}\ \mathsf{p}\ \mathsf{t}')),\\ &\quad \rho_2(\gamma_2({}^{\mathsf{int}}\mathcal{FC}\ (\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}))\ \mathbf{p}\ (\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}))))\\ &= (W, \rho_1(\gamma_1(\mathsf{t}))\ \mathsf{p}\ \rho_1(\gamma_1(\mathsf{t}')),\\ &\qquad {}^{\mathsf{int}}\mathcal{FC}\ \rho_2(\gamma_2(\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]})))\ \mathbf{p}\ \rho_2(\gamma_2(\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}))))\\ &\qquad\qquad \in \mathcal{E}[\![\mathsf{int}]\!]\rho.\end{aligned}$$

By our hypotheses,

$$(W, \rho_1(\gamma_1(\mathsf{t})), \rho_2(\gamma_2({}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]})))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho$$

and

$$(W, \rho_1(\gamma_1(\mathsf{t}')), \rho_2(\gamma_2({}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]})))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho.$$

Let $W' \sqsupseteq W$, $(W', \mathsf{m}, \mathsf{m}) \in \mathcal{V}[\![\mathsf{int}]\!]\rho$, and $(W', \mathsf{n}, \mathsf{n}) \in \mathcal{V}[\![\mathsf{int}]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{m}\ \mathsf{p}\ \mathsf{n}, {}^{\mathsf{int}}\mathcal{FC}\ (\mathcal{CF}^{\mathsf{int}}\ \mathsf{m}\ \mathbf{p}\ \mathcal{CF}^{\mathsf{int}}\ \mathsf{n})) \in \mathcal{E}[\![\mathsf{int}]\!]\rho.$$

Since boundary translations at type int produce the same integers they are given, and since the semantics of primitive operations are the same in F and C, from this point it is clear that we can complete the proof using Lemma 8.15 and Lemma 8.9. □

Lemma 11.7 (If0)
If $\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\mathsf{int}}\mathcal{FC}\ \mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]} : \mathsf{int}$,

$$\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{t}' \approx {}^{\tau}\mathcal{FC}\ \mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]} : \tau, \quad \text{and} \quad \cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{t}'' \approx {}^{\tau}\mathcal{FC}\ \mathbf{t}''\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]} : \tau,$$

then $\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{if0}\ \mathsf{t}\ \mathsf{t}'\ \mathsf{t}'' \approx {}^{\tau}\mathcal{FC}\ (\mathbf{if0}\ \mathbf{t}\ \mathbf{t}'\ \mathbf{t}'')\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]} : \tau$.

Proof

By Lemma 11.2, it suffices to show that

$$\begin{aligned}\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{if0}\ \mathsf{t}\ \mathsf{t}'\ \mathsf{t}'' \approx {}^{\tau}\mathcal{FC}\ (\mathbf{if0}\ &\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]})\\ &(\mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]})\\ &(\mathbf{t}''\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}))\qquad : \tau.\end{aligned}$$

For brevity, let $\hat{\mathbf{t}} = \mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}$, $\hat{\mathbf{t}}' = \mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}$, and $\hat{\mathbf{t}}'' = \mathbf{t}''\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}$.
Note that $\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash \mathsf{if0}\ \mathsf{t}\ \mathsf{t}'\ \mathsf{t}'' : \mathsf{int}$ and $\cdot;\overline{\alpha};\overline{\mathsf{x}:\tau'} \vdash {}^{\tau}\mathcal{FC}\ (\mathbf{if0}\ \mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ \hat{\mathbf{t}}\ \hat{\mathbf{t}}'\ \hat{\mathbf{t}}'') : \tau$.
Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathsf{if0}\ \mathsf{t}\ \mathsf{t}'\ \mathsf{t}'')), \rho_2(\gamma_2({}^{\tau}\mathcal{FC}\ (\mathbf{if0}\ (\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ \hat{\mathbf{t}})\ \hat{\mathbf{t}}'\ \hat{\mathbf{t}}''))))\\ &= (W, \mathsf{if0}\ \rho_1(\gamma_1(\mathsf{t}))\ \rho_1(\gamma_1(\mathsf{t}'))\ \rho_1(\gamma_1(\mathsf{t}'')), {}^{\tau}\mathcal{FC}\ \mathbf{if0}\ \rho_2(\gamma_2(\mathcal{CF}^{\mathsf{int}}\mathcal{FC}\ \hat{\mathbf{t}}))\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))) \in \mathcal{E}[\![\tau]\!]\rho.\end{aligned}$$

By our first hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t})), \rho_2(\gamma_2({}^{\mathsf{int}}\mathcal{FC}\,\hat{\mathbf{t}}))) \in \mathcal{E}[\![\mathsf{int}]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \mathsf{n}, \mathsf{n}) \in \mathcal{V}[\![\mathsf{int}]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{if0}\,\mathsf{n}\ \rho_1(\gamma_1(\mathsf{t}'))\ \rho_1(\gamma_1(\mathsf{t}'')), {}^{\tau}\mathcal{FC}\ (\mathbf{if0}\ (\mathcal{CF}^{\mathsf{int}}\,\mathsf{n})\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))\ \rho_2(\gamma_2(\hat{\mathbf{t}}'')))) \in \mathcal{E}[\![\tau]\!]\rho.$$

We can complete the proof using a case split on whether $n = 0$, and then applying Lemma 8.15 and the appropriate one of our hypotheses. □

Lemma 11.8 (Pack)
If $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\tau[\hat{\tau}/\beta]}\mathcal{FC}\ \mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \tau[\hat{\tau}/\beta]$, then

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{pack}\langle\hat{\tau},\mathsf{t}\rangle\ \mathsf{as}\ \exists\beta.\tau \approx {}^{\exists\beta.\tau}\mathcal{FC}\ (\mathbf{pack}\langle\hat{\tau}^{\mathcal{C}},\mathbf{t}\rangle\ \mathbf{as}\ \exists\beta.\tau^{\mathcal{C}})\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \exists\beta.\tau.$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{pack}\langle\hat{\tau},\mathsf{t}\rangle\ \mathsf{as}\ \exists\beta.\tau \approx {}^{\exists\beta.\tau}\mathcal{FC}\ (\mathbf{pack}\langle\hat{\tau}^{\mathcal{C}}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}, \mathcal{CF}^{\tau[\hat{\tau}/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})\rangle) : \exists\beta.\tau.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{pack}\langle\hat{\tau},\mathsf{t}\rangle\ \mathsf{as}\ \exists\beta.\tau : \exists\beta.\tau$ and

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash {}^{\exists\beta.\tau}\mathcal{FC}\ (\mathbf{pack}\langle\hat{\tau}^{\mathcal{C}}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}, \mathcal{CF}^{\tau[\hat{\tau}/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})\rangle\ \mathbf{as}\ \exists\beta.\tau^{\mathcal{C}}) : \exists\beta.\tau.$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}
&(W, \rho_1(\gamma_1(\mathsf{pack}\langle\hat{\tau},\mathsf{t}\rangle\ \mathsf{as}\ \exists\beta.\tau)),\\
&\quad \rho_2(\gamma_2({}^{\exists\beta.\tau}\mathcal{FC}\ (\mathbf{pack}\langle\hat{\tau}^{\mathcal{C}}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}, \mathcal{CF}^{\tau[\hat{\tau}/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})\rangle\ \mathbf{as}\ \exists\beta.\tau^{\mathcal{C}}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]})))\\
&= (W, \mathsf{pack}\langle\rho_1(\hat{\tau}),\rho_1(\gamma_1(\mathsf{t}))\rangle\ \mathsf{as}\ \rho_1(\exists\beta.\tau),\\
&\qquad {}^{\rho_2(\exists\beta.\tau)}\mathcal{FC}\ \mathbf{pack}\langle\rho_2(\hat{\tau}^{\langle\mathcal{C}\rangle}), \mathcal{CF}^{\rho_2(\tau[\hat{\tau}/\beta])}\mathcal{FC}\ (\rho_2(\gamma_2(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})))\rangle\ \mathbf{as}\ \rho_2(\exists\beta.\tau^{\langle\mathcal{C}\rangle}))\\
&\qquad\qquad \in \mathcal{E}[\![\exists\beta.\tau]\!]\rho.
\end{aligned}$$

By our hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t})), \rho_2(\gamma_2({}^{\tau[\hat{\tau}/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\tau[\hat{\tau}/\beta]]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau[\hat{\tau}/\beta]]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{pack}\langle\rho_1(\hat{\tau}),\mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\beta.\tau), {}^{\rho_2(\exists\beta.\tau)}\mathcal{FC}\ \mathbf{pack}\langle\rho_2(\hat{\tau}^{\langle\mathcal{C}\rangle}), \mathcal{CF}^{\rho_2(\tau[\hat{\tau}/\beta])}\ \mathsf{v}_2\rangle\ \mathbf{as}\ \rho_2(\exists\beta.\tau^{\langle\mathcal{C}\rangle})) \in \mathcal{E}[\![\exists\beta.\tau]\!]\rho.$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\mathbf{v_2}$ and v_2' such that

$$\mathbf{CF}^{\rho_2(\tau[\hat{\tau}/\beta])}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2) \quad \text{and} \quad {}^{\mathsf{L}\langle\rho_2(\tau[\hat{\tau}/\beta]^{\langle\mathcal{C}\rangle})\rangle}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathsf{v}_2', M_2).$$

By the operational semantics,

$$\langle M_2 \mid {}^{\rho_2(\exists\beta.\tau)}\mathcal{FC}\ \mathbf{pack}\langle\rho_2(\hat{\tau}^{\langle\mathcal{C}\rangle}), \mathcal{CF}^{\rho_2(\tau[\hat{\tau}/\beta])}\ \mathsf{v}_2\rangle\ \mathbf{as}\ \rho_2(\exists\beta.\tau)\rangle \longmapsto^2 \langle M_2 \mid \mathsf{pack}\langle\mathsf{L}\langle\rho_2(\hat{\tau}^{\langle\mathcal{C}\rangle})\rangle, \mathsf{v}_2'\rangle\ \mathsf{as}\ \rho_2(\exists\beta.\tau^{\langle\mathcal{C}\rangle})\rangle.$$

Thus, by Lemma 8.15 and Lemma 8.9, it suffices to show that

$$(W', \mathsf{pack}\langle\rho_1(\hat{\tau}),\mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\beta.\tau), \mathsf{pack}\langle\mathsf{L}\langle\rho_2(\hat{\tau}^{\langle\mathcal{C}\rangle})\rangle, \mathsf{v}_2'\rangle\ \mathsf{as}\ \rho_2(\exists\beta.\tau)) \in \mathcal{V}[\![\exists\beta.\tau]\!]\rho.$$

To show this, we need to find some $\mathrm{VR} \in \mathrm{FValRel}$ such that $\mathrm{VR}.\tau_1 = \rho_1(\hat{\tau})$, $\mathrm{VR}.\tau_2 = \mathsf{L}\langle\rho_2(\hat{\tau}^{\langle\mathcal{C}\rangle})\rangle$, and $(W', \mathsf{v}_1, \mathsf{v}_2') \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto \mathrm{VR}]$. We use

$$\mathrm{VR} = \mathrm{opaqueR}(\rho_1(\hat{\tau}), \rho_2(\hat{\tau}), \mathcal{V}[\![\hat{\tau}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{C}\rangle}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle}]\!]\rho).$$

That this $\mathrm{VR} \in \mathrm{FValRel}$ follows from Lemma 10.4 and Lemma 8.35. The types match by definition of opaqueR. For the last condition, note that

$$(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto (\rho_1(\hat{\tau}), \rho_2(\hat{\tau}), \mathcal{V}[\![\hat{\tau}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{C}\rangle}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle}]\!]\rho)]$$

by Lemma 10.7. The result follows directly from boundary cancellation. □

Lemma 11.9 (Unpack)
If $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\exists\beta.\tau}\mathcal{FC}\ \mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]} : \exists\beta.\tau$ and

$$\cdot; \overline{\alpha}, \beta; \overline{\mathsf{x}:\tau'}, \mathsf{y}:\tau \vdash \mathsf{t}' \approx {}^{\hat{\tau}}\mathcal{FC}\ \mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}[\lceil\beta\rceil/\boldsymbol{\beta}]\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]}[\mathcal{CF}^{\tau}\ \mathsf{y}/\mathbf{y}] : \hat{\tau},$$

then $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{unpack}\ \langle\beta, \mathsf{y}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t}' \approx {}^{\hat{\tau}}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t}')\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]} : \hat{\tau}$.

Proof

For brevity, let $\hat{\mathbf{t}} = \mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]}$ and $\hat{\mathbf{t}}' = \mathbf{t}'\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]}$. By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{unpack}\ \langle\beta, \mathsf{y}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t}' \approx {}^{\hat{\tau}}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = (\mathcal{CF}^{\exists\beta.\tau}\mathcal{FC}\ \hat{\mathbf{t}})\ \mathbf{in}\ \hat{\mathbf{t}}'[\mathcal{CF}^{\tau}\mathcal{FC}\ \mathbf{y}/\mathbf{y}]) : \hat{\tau}.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{unpack}\ \langle\beta, \mathsf{y}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t}' : \hat{\tau}$ and

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash {}^{\hat{\tau}}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = (\mathcal{CF}^{\exists\beta.\tau}\mathcal{FC}\ \hat{\mathbf{t}})\ \mathbf{in}\ \hat{\mathbf{t}}'[\mathcal{CF}^{\tau}\mathcal{FC}\ \mathbf{y}/\mathbf{y}]) : \hat{\tau}.$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}
&(W, \rho_1(\gamma_1(\mathsf{unpack}\ \langle\beta, \mathsf{y}\rangle = \mathsf{t}\ \mathsf{in}\ \mathsf{t}')),\\
&\quad \rho_2(\gamma_2({}^{\hat{\tau}}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = (\mathcal{CF}^{\exists\beta.\tau}\mathcal{FC}\ \hat{\mathbf{t}})\ \mathbf{in}\ \hat{\mathbf{t}}'[\mathcal{CF}^{\tau}\mathcal{FC}\ \mathbf{y}/\mathbf{y}]))))\\
&= (W, \mathsf{unpack}\ \langle\beta, \mathsf{y}\rangle = \rho_1(\gamma_1(\mathsf{t}))\ \mathsf{in}\ \rho_1(\gamma_1(\mathsf{t}')),\\
&\qquad {}^{\rho_2(\hat{\tau})}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = (\mathcal{CF}^{\rho_2(\exists\beta.\tau)}\mathcal{FC}\ \rho_2(\gamma_2(\hat{\mathbf{t}})))\ \mathbf{in}\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))[\mathcal{CF}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{y}/\mathbf{y}]))\\
&\qquad\qquad \in \mathcal{E}[\![\hat{\tau}]\!]\rho.
\end{aligned}$$

By our first hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t})), {}^{\rho_2(\exists\beta.\tau)}\mathcal{FC}\ \rho_2(\gamma_2(\hat{\mathbf{t}}))) \in \mathcal{E}[\![\exists\beta.\tau]\!]\rho$. Let $W' \sqsupseteq W$ and

$$(W', \mathsf{pack}\langle\tau_1, \mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\beta.\tau), \mathsf{pack}\langle\tau_2, \mathsf{v}_2\rangle\ \mathsf{as}\ \rho_2(\exists\beta.\tau)) \in \mathcal{V}[\![\exists\beta.\tau]\!]\rho.$$

By Lemma 8.20, it suffices to show that

$$\begin{aligned}
&(W', \mathsf{unpack}\ \langle\beta, \mathsf{y}\rangle = (\mathsf{pack}\langle\tau_1, \mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\beta.\tau))\ \mathsf{in}\ \rho_1(\gamma_1(\mathsf{t}')),\\
&\quad {}^{\rho_2(\hat{\tau})}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = (\mathcal{CF}^{\rho_2(\exists\beta.\tau)}\ \mathsf{pack}\langle\tau_2, \mathsf{v}_2\rangle)\ \mathbf{in}\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))[\mathcal{CF}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{y}/\mathbf{y}])) \in \mathcal{E}[\![\hat{\tau}]\!]\rho.
\end{aligned}$$

By Lemma 8.3, for any $(M_1, M_2) : W$, there are some $\mathbf{v_2}$ and v_2' such that

$$\mathbf{CF}^{\rho_2(\tau[\tau_2/\beta])}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2) \quad \text{and} \quad {}^{\rho_2(\tau[\tau_2/\beta])}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathsf{v}_2', M_2).$$

Note that

$$\langle M_1 \mid \mathsf{unpack}\ \langle\beta, \mathsf{y}\rangle = (\mathsf{pack}\langle\tau_1, \mathsf{v}_1\rangle\ \mathsf{as}\ \rho_1(\exists\beta.\tau))\ \mathsf{in}\ \rho_1(\gamma_1(\mathsf{t}'))\rangle \longmapsto \langle M_1 \mid \rho_1(\gamma_1(\mathsf{t}'))[\tau_1/\beta][\mathsf{v}_1/\mathsf{y}]\rangle$$

and

$$\begin{aligned}
&\langle M_2 \mid {}^{\rho_2(\hat{\tau})}\mathcal{FC}\ (\mathbf{unpack}\ \langle\boldsymbol{\beta}, \mathbf{y}\rangle = (\mathcal{CF}^{\rho_2(\exists\beta.\tau)}\ \mathsf{pack}\langle\tau_2, \mathsf{v}_2\rangle)\ \mathbf{in}\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))[\mathcal{CF}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{y}/\mathbf{y}])\rangle\\
&\qquad\qquad \longmapsto^2 \langle M_2 \mid {}^{\rho_2(\hat{\tau})}\mathcal{FC}\ (\rho_2(\gamma_2(\hat{\mathbf{t}}'))[\tau_2{}^{\langle\mathcal{C}\rangle}/\beta][\mathcal{CF}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{v_2}/\mathbf{y}])\rangle.
\end{aligned}$$

By Lemma 8.15, it suffices to show that

$$(W', \rho_1(\gamma_1(\mathsf{t}'))[\tau_1/\beta][\mathsf{v}_1/\mathsf{y}], {}^{\rho_2(\hat{\tau})}\mathcal{FC}\ (\rho_2(\gamma_2(\hat{\mathbf{t}}'))[\tau_2{}^{\langle\mathcal{C}\rangle}/\beta][\mathcal{CF}^{\rho_2(\tau)}\mathcal{FC}\ \mathbf{v_2}/\mathbf{y}])) \in \mathcal{E}[\![\hat{\tau}]\!]\rho.$$

By Lemma 8.17, it suffices to show that

$$(W', \rho_1(\gamma_1(\mathsf{t}'))[\tau_1/\beta][\mathsf{v}_1/\mathsf{y}], {}^{\rho_2(\hat{\tau})}\mathcal{FC}\ (\rho_2(\gamma_2(\hat{\mathbf{t}}'))[\tau_2{}^{\langle\mathcal{C}\rangle}/\beta][\mathcal{CF}^{\rho_2(\tau)}\ \mathsf{v}_2'/\mathbf{y}])) \in \mathcal{E}[\![\hat{\tau}]\!]\rho.$$

By definition of $\mathcal{V}[\![\exists\beta.\tau]\!]\rho$, there is some $\mathrm{VR} \in \mathrm{FValRel}$ such that $\mathrm{VR}.\tau_1 = \tau_1$, $\mathrm{VR}.\tau_2 = \tau_2$, and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto \mathrm{VR}]$. By boundary cancellation, $(W', \mathsf{v}_1, \mathsf{v}_2') \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto \mathrm{VR}]$. Therefore $\rho[\beta \mapsto \mathrm{VR}] \in \mathcal{D}[\![\overline{\alpha}, \beta]\!]$ and $(W', \gamma[\mathsf{y} \mapsto (\mathsf{v}_1, \mathsf{v}_2')]) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau'}, \mathsf{y}:\tau]\!]\rho$. Hence we can apply our second hypothesis to get exactly this result. □

Lemma 11.10 (Fold)
If $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\tau[\mu\alpha.\tau/\alpha]}\mathcal{FC}\ \mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]} : \tau[\mu\alpha.\tau/\alpha]$, then

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{fold}_{\mu\alpha.\tau}\ \mathsf{t} \approx {}^{\mu\alpha.\tau}\mathcal{FC}\ (\mathbf{fold}_{\mu\alpha.\tau\boldsymbol{\mathcal{C}}}\ \mathbf{t})\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]} : \mu\alpha.\tau.$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{fold}_{\mu\beta.\tau}\ \mathsf{t} \approx {}^{\mu\beta.\tau}\mathcal{FC}\ (\mathbf{fold}_{\mu\beta.\tau\langle\boldsymbol{\mathcal{C}}\rangle}\ \mathcal{CF}^{\tau[\mu\beta.\tau/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]})) : \mu\beta.\tau.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{fold}_{\mu\beta.\tau}\ \mathsf{t} : \mu\beta.\tau$ and

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash {}^{\mu\beta.\tau}\mathcal{FC}\ (\mathbf{fold}_{\mu\beta.\tau\langle\boldsymbol{\mathcal{C}}\rangle}\ \mathcal{CF}^{\tau[\mu\beta.\tau/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]})) : \mu\beta.\tau.$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathsf{fold}_{\mu\beta.\tau}\ \mathsf{t})), \rho_2(\gamma_2({}^{\mu\beta.\tau}\mathcal{FC}\ (\mathbf{fold}_{\mu\beta.\tau\langle\boldsymbol{\mathcal{C}}\rangle}\ \mathcal{CF}^{\tau[\mu\beta.\tau/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]})))))\\ &\quad = (W, \mathsf{fold}_{\rho_1(\mu\beta.\tau)}\ \rho_1(\gamma_1(\mathsf{t})),\\ &\qquad {}^{\rho_2(\mu\beta.\tau)}\mathcal{FC}\ \mathbf{fold}_{\rho_2(\mu\beta.\tau\langle\boldsymbol{\mathcal{C}}\rangle)}\ \mathcal{CF}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{FC}\ (\rho_2(\gamma_2(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\mu\beta.\tau]\!]\rho.\end{aligned}$$

By our hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t})), \rho_2(\gamma_2({}^{\tau[\mu\beta.\tau/\beta]}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{fold}_{\rho_1(\mu\beta.\tau)}\ \mathsf{v}_1, {}^{\rho_2(\mu\beta.\tau)}\mathcal{FC}\ \mathbf{fold}_{\rho_2(\mu\beta.\tau\langle\boldsymbol{\mathcal{C}}\rangle)}\ \mathcal{CF}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\ \mathsf{v}_2) \in \mathcal{E}[\![\mu\beta.\tau]\!]\rho.$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\mathbf{v_2}$ and v_2' such that

$$\mathbf{CF}^{\rho_2(\tau[\mu\alpha.\tau/\beta])}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2) \quad \text{and} \quad {}^{\rho_2(\tau[\mu\alpha.\tau/\beta])}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathsf{v}_2', M_2).$$

By the operational semantics,

$$\langle M_2 \mid {}^{\rho_2(\mu\beta.\tau)}\mathcal{FC}\ \mathbf{fold}_{\rho_2(\mu\beta.\tau)}\ \mathcal{CF}^{\rho_2(\tau[\mu\alpha.\tau/\beta])}\ \mathsf{v}_2\rangle \longmapsto^2 \langle M_2 \mid \mathsf{fold}_{\rho_2(\mu\beta.\tau\langle\boldsymbol{\mathcal{C}}\rangle)}\ \mathsf{v}_2'\rangle.$$

Thus, by Lemma 8.15 and Lemma 8.9, it suffices to show that

$$(W', \mathsf{fold}_{\rho_1(\mu\beta.\tau)}\ \mathsf{v}_1, \mathsf{fold}_{\rho_2(\mu\beta.\tau)}\ \mathsf{v}_2') \in \mathcal{V}[\![\mu\beta.\tau]\!]\rho.$$

This follows from our hypothesis that $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau[\mu\beta.\tau/\beta]]\!]$, by monotonicity and boundary cancellation. □

Lemma 11.11 (Unfold)
If $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\mu\alpha.\tau}\mathcal{FC}\ \mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]} : \mu\alpha.\tau$, then

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{unfold}\ \mathsf{t} \approx {}^{\tau[\mu\alpha.\tau/\alpha]}\mathcal{FC}\ (\mathbf{unfold}\ \mathbf{t})\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]} : \tau[\mu\alpha.\tau/\alpha].$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{unfold}\ \mathsf{t} \approx {}^{\tau[\mu\beta.\tau/\beta]}\mathcal{FC}\ (\mathbf{unfold}\ \mathcal{CF}^{\mu\beta.\tau}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]})) : \tau[\mu\beta.\tau/\beta].$$

Note that $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{unfold}\ \mathsf{t} : \tau[\mu\beta.\tau/\beta]$ and

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash {}^{\tau[\mu\beta.\tau/\beta]}\mathcal{FC}\ (\mathbf{unfold}\ \mathcal{CF}^{\mu\beta.\tau}\mathcal{FC}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}]})) : \tau[\mu\beta.\tau/\beta].$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathsf{unfold}\,\mathsf{t})), \rho_2(\gamma_2({}^{\tau[\mu\beta.\tau/\beta]}\mathcal{FC}\,(\mathbf{unfold}\,\mathcal{CF}^{\mu\beta.\tau}\mathcal{FC}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]}))))))$$
$$= (W, \mathsf{unfold}\,\rho_1(\gamma_1(\mathsf{t})),$$
$${}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{FC}\,\mathbf{unfold}\,\mathcal{CF}^{\rho_2(\mu\beta.\tau)}\mathcal{FC}\,(\rho_2(\gamma_2(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]}))))) \in \mathcal{E}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho.$$

By our hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t})), \rho_2(\gamma_2({}^{\mu\beta.\tau}\mathcal{FC}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\mu\beta.\tau]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \mathsf{fold}_{\rho_1(\mu\beta.\tau)}\,\mathsf{v}_1, \mathsf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathsf{v}_2) \in \mathcal{V}[\![\mu\beta.\tau]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{unfold}\,(\mathsf{fold}_{\rho_1(\mu\beta.\tau)}\,\mathsf{v}_1), {}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{FC}\,\mathbf{unfold}\,\mathcal{CF}^{\rho_2(\mu\beta.\tau)}\,\mathsf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathsf{v}_2) \in \mathcal{E}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho.$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\mathbf{v_2}$ and v_2' such that

$$\mathbf{CF}^{\rho_2(\mu\beta.\tau)}(\mathsf{v}_2, M_2) = (\mathbf{v_2}, M_2) \quad \text{and} \quad {}^{\rho_2(\mu\beta.\tau)}\mathbf{FC}(\mathbf{v_2}, M_2) = (\mathsf{v}_2', M_2).$$

By the operational semantics,

$$\langle M_2 \mid {}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{FC}\,\mathbf{unfold}\,\mathcal{CF}^{\rho_2(\mu\beta.\tau)}\,\mathsf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathsf{v}_2\rangle \longmapsto^3 \langle M_2 \mid \mathsf{v}_2'\rangle.$$

The result follows by Lemma 8.15, Lemma 8.9, and boundary cancellation. □

Lemma 11.12 (Tuple)
If $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\tau}\mathcal{FC}\,\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \tau$, then $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \langle\overline{\mathsf{t}}\rangle \approx {}^{\langle\overline{\tau}\rangle}\mathcal{FC}\,\langle\overline{\mathbf{t}}\rangle\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \langle\overline{\tau}\rangle$.

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \langle\overline{\mathsf{t}}\rangle \approx {}^{\langle\overline{\tau}\rangle}\mathcal{FC}\,(\langle\overline{\mathcal{CF}^{\tau}\mathcal{FC}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})}\rangle) : \langle\overline{\tau}\rangle.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \langle\overline{\mathsf{t}}\rangle : \langle\overline{\tau}\rangle$ and

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash {}^{\langle\overline{\tau}\rangle}\mathcal{FC}\,(\langle\overline{\mathcal{CF}^{\langle\overline{\tau}\rangle}\mathcal{FC}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})}\rangle) : \langle\overline{\tau}\rangle.$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\langle\overline{\mathsf{t}}\rangle)), \rho_2(\gamma_2({}^{\langle\overline{\tau}\rangle}\mathcal{FC}\,(\langle\overline{\mathcal{CF}^{\tau}\mathcal{FC}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})}\rangle))))$$
$$= (W, \langle\overline{\rho_1(\gamma_1(\mathsf{t}))}\rangle, {}^{\rho_2(\langle\overline{\tau}\rangle)}\mathcal{FC}\,\langle\overline{\mathcal{CF}^{\rho_2(\tau)}\mathcal{FC}\,(\rho_2(\gamma_2(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]})))}\rangle) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

By our hypothesis,

$$\overline{(W, \rho_1(\gamma_1(\mathsf{t})), \rho_2(\gamma_2({}^{\tau}\mathcal{FC}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]}))))} \in \mathcal{E}[\![\tau]\!]\rho.$$

Let $W' \sqsupseteq W$ and $\overline{(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\rho}$. By Lemma 8.20, it suffices to show that

$$(W', \langle\overline{\mathsf{v}_1}\rangle, {}^{\rho_2(\langle\overline{\tau}\rangle)}\mathcal{FC}\,\langle\overline{\mathcal{CF}^{\rho_2(\tau)}\,\mathsf{v}_2}\rangle) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

We have this by Lemma 8.15, Lemma 8.9, and boundary cancellation. □

Lemma 11.13 (Projection)
If $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\langle\overline{\tau}\rangle}\mathcal{FC}\,\mathbf{t}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \langle\overline{\tau}\rangle$, then $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \pi_i(\mathsf{t}) \approx {}^{\tau_i}\mathcal{FC}\,\boldsymbol{\pi_i}(\mathbf{t})\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \tau_i$.

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \pi_i(\mathsf{t}) \approx {}^{\tau_i}\mathcal{FC}\ (\boldsymbol{\pi_i}(\mathcal{CF}^{\langle\overline{\tau}\rangle}\mathcal{FC}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\boldsymbol{\alpha}}][\overline{\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}}]))) : \tau_i.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \pi_i(\mathsf{t}) : \tau_i$ and $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash {}^{\tau_i}\mathcal{FC}\ (\boldsymbol{\pi_i}(\mathcal{CF}^{\langle\overline{\tau}\rangle}\mathcal{FC}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\boldsymbol{\alpha}}][\overline{\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}}]))) : \tau_i$.
Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1(\gamma_1(\pi_i(\mathsf{t}))), \rho_2(\gamma_2({}^{\tau_i}\mathcal{FC}\ (\boldsymbol{\pi_i}(\mathcal{CF}^{\langle\overline{\tau}\rangle}\mathcal{FC}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\boldsymbol{\alpha}}][\overline{\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}}])))))) \\ = (W, \pi_i(\rho_1(\gamma_1(\mathsf{t}))), {}^{\rho_2(\tau_i)}\mathcal{FC}\ \boldsymbol{\pi_i}(\mathcal{CF}^{\rho_2(\langle\overline{\tau}\rangle)}\mathcal{FC}\ (\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\boldsymbol{\alpha}}][\overline{\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}}]))))) \in \mathcal{E}[\![\tau_i]\!]\rho.\end{aligned}$$

By our hypothesis, $(W, \rho_1(\gamma_1(\mathsf{t})), \rho_2(\gamma_2({}^{\langle\overline{\tau}\rangle}\mathcal{FC}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\boldsymbol{\alpha}}][\overline{\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathbf{x}}])))) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho$. Let $W' \sqsupseteq W$ and $(W', \langle\overline{\mathsf{v}_1}\rangle, \langle\overline{\mathsf{v}_2}\rangle) \in \mathcal{V}[\![\langle\overline{\tau}\rangle]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \pi_i((\langle\overline{\mathsf{v}_1}\rangle)), {}^{\rho_2(\tau_i)}\mathcal{FC}\ \boldsymbol{\pi_i}(\mathcal{CF}^{\rho_2(\langle\overline{\tau}\rangle)}\ \langle\overline{\mathsf{v}_2}\rangle)) \in \mathcal{E}[\![\tau_i]\!]\rho.$$

We have this by Lemma 8.15, Lemma 8.9, and boundary cancellation. □

Lemma 11.14 (Function)
Let $k' \geq k$, $m' \geq m$, $\Delta = \beta_1, \ldots, \beta_{\mathsf{k}'}$, and $\Gamma = \mathsf{y}_1 : \tau_1, \ldots, \mathsf{y}_{\mathsf{m}'} : \tau_{\mathsf{m}'}$.
If $\mathrm{fv}(\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t}) = \mathsf{y}_1, \ldots, \mathsf{y}_{\mathsf{m}}$, $\mathrm{ftv}(\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t}) = \beta_1, \ldots, \beta_{\mathsf{k}}$, $\boldsymbol{\tau_{\mathbf{env}}} = \langle \tau_1{}^{\boldsymbol{\mathcal{C}}}, \ldots, \tau_{\mathsf{m}}{}^{\boldsymbol{\mathcal{C}}} \rangle$,

$$\begin{aligned}\cdot; (\Delta, \overline{\alpha}); (\Gamma, \overline{\mathsf{x}:\tau}) \vdash \mathsf{t} \approx {}^{\tau'}\mathcal{FC}\ \mathbf{t}[\lceil\beta_1\rceil/\boldsymbol{\beta_1}] \cdots [\lceil\beta_{\mathsf{k}'}\rceil/\boldsymbol{\beta_{\mathbf{k}'}}][\overline{\lceil\alpha\rceil/\boldsymbol{\alpha}}] \\ [\mathcal{CF}^{\tau_1}\ \mathsf{y}_1/\mathbf{y}_1] \cdots [\mathcal{CF}^{\tau_{\mathsf{m}'}}\ \mathsf{y}_{\mathsf{m}'}/\mathbf{y}_{\mathbf{m}'}][\overline{\mathcal{CF}^{\tau}\ \mathsf{x}/\mathbf{x}}] : \tau',\end{aligned}$$

$\mathbf{v_f} = \boldsymbol{\lambda}[\boldsymbol{\beta_1}, \ldots, \boldsymbol{\beta_k}, \overline{\boldsymbol{\alpha}}](\mathbf{z} : \boldsymbol{\tau_{\mathbf{env}}}, \overline{\mathbf{x} : \tau^{\boldsymbol{\mathcal{C}}}}).\mathbf{t}[\boldsymbol{\pi_1}(\mathbf{z})/\mathbf{y}_1] \cdots [\boldsymbol{\pi_m}(\mathbf{z})/\mathbf{y}_m]$, and

$$\mathbf{v} = \mathbf{pack}\langle \boldsymbol{\tau_{\mathbf{env}}}, \langle \mathbf{v_f}[\boldsymbol{\beta_1}] \cdots [\boldsymbol{\beta_k}], \langle \mathbf{y}_1, \ldots, \mathbf{y}_m \rangle \rangle \rangle\ \mathbf{as}\ \exists \boldsymbol{\alpha'}.\langle (\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\alpha'}, \overline{\tau^{\boldsymbol{\mathcal{C}}}}) \to \tau'^{\boldsymbol{\mathcal{C}}}), \boldsymbol{\alpha'} \rangle,$$

then

$$\begin{aligned}\cdot; \Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} \approx {}^{\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}\mathcal{FC}\ \mathbf{v}[\lceil\beta_1\rceil/\boldsymbol{\beta_1}] \cdots [\lceil\beta_{\mathsf{k}'}\rceil/\boldsymbol{\beta_{\mathbf{k}'}}] \\ [\mathcal{CF}^{\tau_1}\ \mathsf{y}_1/\mathbf{y}_1] \cdots [\mathcal{CF}^{\tau_{\mathsf{m}'}}\ \mathsf{y}_{\mathsf{m}'}/\mathbf{y}_{\mathbf{m}'}] : \forall[\overline{\alpha}].(\overline{\mathsf{x}:\tau}) \to \tau'.\end{aligned}$$

Proof

Let

$$\mathbf{v'_f} = \boldsymbol{\lambda}[\boldsymbol{\beta_1}, \ldots, \boldsymbol{\beta_k}, \overline{\boldsymbol{\alpha}}](\mathbf{z} : \boldsymbol{\tau_{\mathbf{env}}}, \overline{\mathbf{x} : \tau^{\boldsymbol{\mathcal{C}}}}).\mathbf{t}[\mathcal{CF}^{\tau_1}\ \mathcal{FC}\ \boldsymbol{\pi_1}(\mathbf{z})/\mathbf{y}_1] \cdots [\mathcal{CF}^{\tau_m}\ \mathcal{FC}\ \boldsymbol{\pi_m}(\mathbf{z})/\mathbf{y}_m][\overline{\mathcal{CF}^{\tau}\ \mathcal{FC}\ \mathbf{x}/\mathbf{x}}]$$

and

$$\mathbf{v'} = \mathbf{pack}\langle \boldsymbol{\tau_{\mathbf{env}}}, \langle \mathbf{v'_f}[\boldsymbol{\beta_1}] \cdots [\boldsymbol{\beta_k}], \langle \mathbf{y}_1, \ldots, \mathbf{y}_m \rangle \rangle \rangle\ \mathbf{as}\ \exists \boldsymbol{\alpha'}.\langle (\forall[\overline{\boldsymbol{\alpha}}].(\boldsymbol{\alpha'}, \overline{\tau^{\boldsymbol{\mathcal{C}}}}) \to \tau'^{\boldsymbol{\mathcal{C}}}), \boldsymbol{\alpha'} \rangle.$$

By Lemma 11.2, it suffices to show that

$$\begin{aligned}\cdot; \Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} \approx {}^{\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}\mathcal{FC}\ \mathbf{v'}[\lceil\beta_1\rceil/\boldsymbol{\beta_1}] \cdots [\lceil\beta_{\mathsf{k}'}\rceil/\boldsymbol{\beta_{\mathbf{k}'}}] \\ [\mathcal{CF}^{\tau_1}\ \mathsf{y}_1/\mathbf{y}_1] \cdots [\mathcal{CF}^{\tau_{\mathsf{m}'}}\ \mathsf{y}_{\mathsf{m}'}/\mathbf{y}_{\mathbf{m}'}] : \forall[\overline{\alpha}].(\overline{\mathsf{x}:\tau}) \to \tau'.\end{aligned}$$

Note that $\cdot; \Delta; \Gamma \vdash \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ and

$$\begin{aligned}\cdot; \Delta; \Gamma \vdash {}^{\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}\mathcal{FC}\ \mathbf{v'}[\lceil\beta_1\rceil/\boldsymbol{\beta_1}] \cdots [\lceil\beta_{\mathsf{k}'}\rceil/\boldsymbol{\beta_{\mathbf{k}'}}] \\ [\mathcal{CF}^{\tau_1}\ \mathsf{y}_1/\mathbf{y}_1] \cdots [\mathcal{CF}^{\tau_{\mathsf{m}'}}\ \mathsf{y}_{\mathsf{m}'}/\mathbf{y}_{\mathbf{m}'}] : \forall[\overline{\alpha}].(\overline{\mathsf{x}:\tau}) \to \tau'.\end{aligned}$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1(\gamma_1(\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\mathsf{t})), \rho_2(\gamma_2(^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}\mathcal{FC}\,\mathbf{v'}[\lceil\beta_1\rceil/\beta_1]\cdots[\lceil\beta_{k'}\rceil/\beta_{k'}]\\ [\mathcal{CF}^{\tau_1}\,\mathsf{y_1}/\mathbf{y_1}]\cdots[\mathcal{CF}^{\tau_{m'}}\,\mathsf{y_{m'}}/\mathbf{y_{m'}}])))\\ = (W, \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\rho_1(\gamma_1(\mathsf{t})), {}^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}\mathcal{FC}\,\mathbf{v'}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}/\beta_1]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}/\beta_{k'}]\\ [\mathcal{CF}^{\rho_2(\tau_1)}\,\gamma_2(\mathsf{y_1})/\mathbf{y_1}]\cdots[\mathcal{CF}^{\rho_2(\tau_{m'})}\,\gamma_2(\mathsf{y_{m'}})/\mathbf{y_{m'}}])\\ \in \mathcal{E}[\![\forall[\overline{\alpha}].(\overline{\tau})\to\tau']\!]\rho.\end{aligned}$$

Note that

$$\begin{aligned}&\mathbf{v'}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}/\beta_1]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}/\beta_{k'}][\mathcal{CF}^{\rho_2(\tau_1)}\,\gamma_2(\mathsf{y_1})/\mathbf{y_1}]\cdots[\mathcal{CF}^{\rho_2(\tau_{m'})}\,\gamma_2(\mathsf{y_{m'}})/\mathbf{y_{m'}}]\\ &\quad= \mathbf{pack}\langle\boldsymbol{\tau}_{\mathbf{env}}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}/\beta_1]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}/\beta_{k'}],\\ &\qquad\langle\mathbf{v'_f}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}], \langle\mathcal{CF}^{\rho_2(\tau_1)}\,\gamma_2(\mathsf{y_1}),\ldots,\mathcal{CF}^{\rho_2(\tau_1)}\,\gamma_2(\mathsf{y_m})\rangle\rangle\rangle.\end{aligned}$$

Call this term $\hat{\mathbf{t}}'$. By Lemma 8.3, there are some $\mathbf{v_1},\ldots,\mathbf{v_m}$ and $\mathsf{v}'_1,\ldots,\mathsf{v}'_m$ such that for each $1 \le i \le m$ and any $(M_1,M_2):W$,

$$\mathbf{CF}^{\tau_i}(\gamma_1(\mathsf{y_i}),M_2) = (\mathbf{v_i},M_2) \quad\text{and}\quad {}^{\tau_i}\mathbf{FC}(\mathbf{v_i},M_2) = (\mathsf{v}'_i,M_2).$$

Let

$$\hat{\mathbf{v}}' = \mathbf{pack}\langle\boldsymbol{\tau}_{\mathbf{env}}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}/\beta_1]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}/\beta_{k'}],\langle\mathbf{v'_f}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}],\langle\mathbf{v_1},\ldots,\mathbf{v_m}\rangle\rangle\rangle.$$

By Lemma 8.15 and Lemma 8.9, it suffices to show that

$$\begin{aligned}&(W, \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\rho_1(\gamma_1(\mathsf{t})), \lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).({}^{\tau'}\mathcal{FC}\,\mathbf{unpack}\,\langle\boldsymbol{\beta}',\mathbf{z}\rangle = \hat{\mathbf{v}}'\ \mathbf{in}\ \boldsymbol{\pi}_1(\mathbf{z})\,[\overline{\lceil\alpha\rceil}]\,\boldsymbol{\pi}_2(\mathbf{z}),\overline{\mathcal{CF}^{\tau}\,\mathsf{x}}))\\ &\qquad\in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau})\to\tau']\!]\rho.\end{aligned}$$

Let $W' \sqsupseteq W$, $\overline{\mathrm{VR} \in \mathrm{FValRel}}$, and $\overline{(W',\hat{\mathsf{v}}_1,\hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau]\!]\rho[\alpha \mapsto \mathrm{VR}]}$. For convenience, let $\overline{\hat{\tau}_1 = \mathrm{VR}.\tau_1}$ and $\overline{\hat{\tau}_2 = \mathrm{VR}.\tau_2}$. We need to show that

$$\begin{aligned}&(W', (\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).\rho_1(\gamma_1(\mathsf{t})))\,\overline{[\hat{\tau}_1]}\,\overline{\hat{\mathsf{v}}_1},\\ &\quad(\lambda[\overline{\alpha}](\overline{\mathsf{x}:\tau}).{}^{\tau'}\mathcal{FC}\,\mathbf{unpack}\,\langle\boldsymbol{\beta}',\mathbf{z}\rangle = \hat{\mathbf{v}}'\ \mathbf{in}\ \boldsymbol{\pi}_1(\mathbf{z})\,[\overline{\lceil\alpha\rceil}]\,\boldsymbol{\pi}_2(\mathbf{z}),\overline{\mathcal{CF}^{\tau}\,\mathsf{x}})\,\overline{[\hat{\tau}_2]}\,\overline{\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho[\alpha \mapsto \mathrm{VR}].\end{aligned}$$

By Lemma 8.15, it suffices to show that

$$\begin{aligned}&(W', \rho_1(\gamma_1(\mathsf{t}))\overline{[\hat{\tau}_1/\alpha][\hat{\mathsf{v}}_1/\mathsf{x}]},\\ &\quad{}^{\tau'\overline{[\hat{\tau}_2/\alpha]}}\mathcal{FC}\,(\mathbf{v'_f}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}]\,\overline{[\hat{\tau}_2{}^{\langle\mathcal{C}\rangle}]}\,\langle\mathbf{v_1},\ldots,\mathbf{v_m}\rangle,\overline{\mathcal{CF}^{\tau[\hat{\tau}_2/\alpha]}\,\hat{\mathsf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho\overline{[\alpha \mapsto \mathrm{VR}]}.\end{aligned}$$

By Lemma 8.3, for any $(M'_1,M'_2):W'$, there are some $\overline{\hat{\mathbf{v}}_2}$ and $\overline{\hat{\mathsf{v}}'_2}$ such that

$$\overline{\mathbf{CF}^{\tau[\hat{\tau}_2/\alpha]}(\hat{\mathsf{v}}_2,M'_2) = (\hat{\mathbf{v}}_2,M_2)} \quad\text{and}\quad \overline{{}^{\tau[\hat{\tau}_2/\alpha]}\mathbf{FC}(\hat{\mathbf{v}}_2,M_2) = (\hat{\mathsf{v}}'_2,M_2)}.$$

By Lemma 8.15, it suffices to show that

$$\begin{aligned}&(W', \rho_1(\gamma_1(\mathsf{t}))\overline{[\hat{\tau}_1/\alpha][\hat{\mathsf{v}}_1/\mathsf{x}]},\\ &\quad{}^{\tau'\overline{[\hat{\tau}_2/\alpha]}}\mathcal{FC}\,(\mathbf{v'_f}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}]\,\overline{[\hat{\tau}_2{}^{\langle\mathcal{C}\rangle}]}\,\langle\mathbf{v_1},\ldots,\mathbf{v_m}\rangle,\overline{\hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\tau']\!]\rho\overline{[\alpha \mapsto \mathrm{VR}]}.\end{aligned}$$

Note that

$$\begin{aligned}&\langle M'_2 \mid {}^{\tau'\overline{[\hat{\tau}_2/\alpha]}}\mathcal{FC}\,(\mathbf{v'_f}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}]\,\overline{[\hat{\tau}_2{}^{\langle\mathcal{C}\rangle}]}\,\langle\mathbf{v_1},\ldots,\mathbf{v_m}\rangle,\overline{\hat{\mathbf{v}}_2})\rangle\\ &\quad\longmapsto \langle M'_2 \mid {}^{\tau'\overline{[\hat{\tau}_2/\alpha]}}\mathcal{FC}\,\mathbf{t}[\mathcal{CF}^{\tau_1}\,\mathcal{FC}\,\boldsymbol{\pi}_1(\langle\mathbf{v_1},\ldots,\mathbf{v_m}\rangle)/\mathbf{y_1}]\cdots[\mathcal{CF}^{\tau_m}\,\mathcal{FC}\,\boldsymbol{\pi}_m(\langle\mathbf{v_1},\ldots,\mathbf{v_m}\rangle)/\mathbf{y_m}]\\ &\qquad\overline{[\mathcal{CF}^{\tau}\,\mathcal{FC}\,\hat{\mathbf{v}}_2/\mathbf{x}]}[\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}/\beta_1]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}/\beta_{k'}]\overline{[\hat{\tau}_2{}^{\langle\mathcal{C}\rangle}/\alpha]}\rangle\end{aligned}$$

By Lemma 8.15 and multiple uses of Lemma 8.17, it suffices to show

$$(W', \rho_1(\gamma_1(\mathsf{t}))\overline{[\hat{\tau}_1/\alpha][\hat{\mathsf{v}}_1/\mathsf{x}]},\ {}^{\tau'\overline{[\hat{\tau}_2/\alpha]}}\mathcal{FC}\,\mathbf{t}[\mathcal{CF}^{\tau_1}\,\mathsf{v}'_1/\mathbf{y_1}]\cdots[\mathcal{CF}^{\tau_m}\,\mathsf{v}'_m/\mathbf{y_m}]\overline{[\mathcal{CF}^{\tau}\,\hat{\mathsf{v}}'_2/\mathbf{x}]}\ [\rho_2(\beta_1)^{\langle\mathcal{C}\rangle}/\boldsymbol{\beta_1}]\cdots[\rho_2(\beta_{k'})^{\langle\mathcal{C}\rangle}/\boldsymbol{\beta_{k'}}]\overline{[\hat{\tau}_2{}^{\langle\mathcal{C}\rangle}/\boldsymbol{\alpha}]}) \in \mathcal{E}[\![\tau']\!]\rho\overline{[\alpha \mapsto \mathrm{VR}]}.$$

We have that $\rho\overline{[\alpha \mapsto \mathrm{VR}]} \in \mathcal{D}[\![\Delta, \overline{\alpha}]\!]$, and by monotonicity and boundary cancellation, that

$$(W', \emptyset[\mathsf{y}_1 \mapsto (\gamma_1(\mathsf{y}_1), \mathsf{v}'_1)]\cdots[\mathsf{y}_m \mapsto (\gamma_1(\mathsf{y}_m), \mathsf{v}'_m)][\mathsf{y}_{m+1} \mapsto \gamma(\mathsf{y}_{m+1})]\cdots[\mathsf{y}_{m'} \mapsto \gamma(\mathsf{y}_{m'})]\overline{[\mathsf{x} \mapsto (\hat{\mathsf{v}}_1, \hat{\mathsf{v}}'_2)]}) \in \mathcal{G}[\![\Gamma, \overline{\mathsf{x}:\tau}]\!]\rho\overline{[\alpha \mapsto \mathrm{VR}]}.$$

Therefore we can apply our hypothesis to get exactly the needed result. □

Lemma 11.15 (Application)
If $\cdot; \overline{\beta}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t}_0 \approx {}^{\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2}\mathcal{FC}\,\mathbf{t_0}\overline{[\lceil\beta\rceil/\boldsymbol{\beta}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2$, $\overline{\overline{\beta} \vdash \tau}$, and

$$\overline{\cdot; \overline{\beta}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t} \approx {}^{\tau_1\overline{[\tau/\alpha]}}\mathcal{FC}\,\mathbf{t}\overline{[\lceil\beta\rceil/\boldsymbol{\beta}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \tau_1\overline{[\tau/\alpha]}},$$

then

$$\cdot; \overline{\beta}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t}_0\,\overline{[\tau]}\,\overline{\mathsf{t}} \approx {}^{\tau_2\overline{[\tau/\alpha]}}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta'}, \mathbf{z}\rangle = \mathbf{t_0}\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi_2}(\mathbf{z}), \overline{\mathbf{t}})\overline{[\lceil\beta\rceil/\boldsymbol{\beta}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]} : \tau_2\overline{[\tau/\alpha]}.$$

Proof

Let $\hat{\mathbf{t}}_0 = \mathbf{t_0}\overline{[\lceil\beta\rceil/\boldsymbol{\beta}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]}$ and $\overline{\hat{\mathbf{t}} = \mathbf{t}\overline{[\lceil\beta\rceil/\boldsymbol{\beta}]}\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]}}$. By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\beta}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t}_0\,\overline{[\tau]}\,\overline{\mathsf{t}} \approx {}^{\tau_2\overline{[\tau/\alpha]}}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta'}, \mathbf{z}\rangle = \mathcal{CF}^{\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2}\,\mathcal{FC}\,\hat{\mathbf{t}}_0\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi_2}(\mathbf{z}), \overline{\mathcal{CF}^{\tau_1\overline{[\tau/\alpha]}}\,\mathcal{FC}\,\hat{\mathbf{t}}}) : \tau_2\overline{[\tau/\alpha]}.$$

Note that $\cdot; \overline{\beta}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{t}_0\,\overline{[\tau]}\,\overline{\mathsf{t}} : \tau_2$ and

$$\cdot; \overline{\beta}; \overline{\mathsf{x}:\tau'} \vdash {}^{\tau_2\overline{[\tau/\alpha]}}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta'}, \mathbf{z}\rangle = \mathcal{CF}^{\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2}\,\mathcal{FC}\,\hat{\mathbf{t}}_0\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi_2}(\mathbf{z}), \overline{\mathcal{CF}^{\tau_1\overline{[\tau/\alpha]}}\,\mathcal{FC}\,\hat{\mathbf{t}}}) : \tau_2\overline{[\tau/\alpha]}.$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\beta}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathsf{x}:\tau'}]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1(\gamma_1(\mathsf{t}_0\,\overline{[\tau]}\,\overline{\mathsf{t}})), \rho_2(\gamma_2({}^{\tau_2\overline{[\tau/\alpha]}}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta'}, \mathbf{z}\rangle = \mathcal{CF}^{\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2}\,\mathcal{FC}\,\hat{\mathbf{t}}_0\\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi_2}(\mathbf{z}), \overline{\mathcal{CF}^{\tau_1\overline{[\tau/\alpha]}}\,\mathcal{FC}\,\hat{\mathbf{t}}})))\\ = (W, \rho_1(\gamma_1(\mathbf{t_0}))\,\overline{[\tau]}\,\overline{\rho_1(\gamma_1(\mathbf{t}))}, {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta'}, \mathbf{z}\rangle = \rho_2(\gamma_2(\mathcal{CF}^{\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2}\,\mathcal{FC}\,\hat{\mathbf{t}}_0))\\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi_2}(\mathbf{z}), \overline{\rho_2(\gamma_2(\mathcal{CF}^{\tau_1\overline{[\tau/\alpha]}}\,\mathcal{FC}\,\hat{\mathbf{t}}))}))))\\ \in \mathcal{E}[\![\tau_2]\!]\rho.\end{aligned}$$

Let $W' \sqsupseteq W$, $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2]\!]\rho$, and $\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2) \in \mathcal{V}[\![\tau_1\overline{[\tau/\alpha]}]\!]\rho}$. By Lemma 8.20, it suffices to show that

$$(W', \mathsf{v}_1\,\overline{[\tau]}\,\overline{\hat{\mathsf{v}}_1}, {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta'}, \mathbf{z}\rangle = \mathcal{CF}^{\rho_2(\forall[\overline{\alpha}].(\overline{\tau_1}) \to \tau_2)}\,\mathsf{v}_2\ \mathbf{in}\ \boldsymbol{\pi_1}(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi_2}(\mathbf{z}), \overline{\mathcal{CF}^{\rho_2(\tau_1\overline{[\tau/\alpha]})}\,\hat{\mathsf{v}}_2})) \in \mathcal{E}[\![\tau_2\overline{[\tau/\alpha]}]\!]\rho.$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\overline{\hat{\mathbf{v}}_2}$ and $\overline{\hat{\mathsf{v}}'_2}$ such that

$$\overline{\mathbf{CF}^{\rho_2(\tau_1\overline{[\tau/\alpha]})}(\hat{\mathsf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2)} \quad \text{and} \quad \overline{{}^{\rho_2(\tau_1\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle/\alpha]})}\mathbf{FC}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathsf{v}}_2, M_2)}.$$

Let

$$\mathbf{v} = \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}](\mathbf{z}:\mathbf{unit}, \overline{\mathbf{y}:\rho_2(\tau_1)^{\mathcal{C}}}).\mathcal{CF}^{\rho_2(\tau_2)\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}}\,(\mathsf{v}_2\,\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle]}\,\overline{\mathcal{FC}^{\rho_2(\tau_1)\overline{[\mathsf{L}\langle\boldsymbol{\alpha}\rangle/\alpha]}}\,\mathbf{y}})$$

and note that

$$\begin{array}{rl}
 & \langle M_2 \mid {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta}',\mathbf{z}\rangle = \mathcal{CF}^{\rho_2(\forall[\overline{\alpha}].(\overline{\tau_1})\to\tau_2)}\,\mathsf{v}_2 \\
 & \qquad\qquad \mathbf{in}\ \boldsymbol{\pi}_1(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi}_2(\mathbf{z}), \overline{\mathcal{CF}^{\rho_2(\tau_1\overline{[\tau/\alpha]})}\,\hat{\mathsf{v}}_2}))\rangle \\
\longmapsto & \langle M_2 \mid {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,(\mathbf{unpack}\,\langle\boldsymbol{\beta}',\mathbf{z}\rangle = (\mathbf{pack}\langle\mathbf{unit},\langle\mathbf{v},()\rangle\rangle\ \mathbf{as}\ \rho_2(\forall[\overline{\alpha}].(\overline{\tau_1})\to\tau_2)^{\langle\mathcal{C}\rangle}) \\
 & \qquad\qquad \mathbf{in}\ \boldsymbol{\pi}_1(\mathbf{z})\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,\boldsymbol{\pi}_2(\mathbf{z}), \overline{\mathcal{CF}^{\rho_2(\tau_1\overline{[\tau/\alpha]})}\,\hat{\mathsf{v}}_2}))\rangle \\
\longmapsto^3 & \langle M_2 \mid {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,\mathbf{v}\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,(), \overline{\mathcal{CF}^{\rho_2(\tau_1\overline{[\tau/\alpha]})}\,\hat{\mathsf{v}}_2}\rangle \\
\longmapsto^* & \langle M_2 \mid {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,\mathbf{v}\,\overline{[\tau^{\langle\mathcal{C}\rangle}]}\,(), \overline{\hat{\mathbf{v}}_2}\rangle \\
\longmapsto & \langle M_2 \mid {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau_2)\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle/\alpha]}}\,(\mathsf{v}_2\,\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle]}\,\overline{\mathcal{FC}^{\rho_2(\tau_1)[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle/\alpha]}\,\hat{\mathbf{v}}_2})\rangle \\
\longmapsto^* & \langle M_2 \mid {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau_2)\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle/\alpha]}}\,(\mathsf{v}_2\,\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle]}\,\overline{\hat{\mathsf{v}}_2'})\rangle
\end{array}$$

By Lemma 8.14, it suffices to show that

$$(W', \mathsf{v}_1\,\overline{[\tau]}\,\overline{\hat{\mathsf{v}}_1}, {}^{\rho_2(\tau_2\overline{[\tau/\alpha]})}\mathcal{FC}\,\mathcal{CF}^{\rho_2(\tau_2)\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle/\alpha]}}\,(\mathsf{v}_2\,\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle]}\,\overline{\hat{\mathsf{v}}_2'})) \in \mathcal{E}[\![\tau_2\overline{[\tau/\alpha]}]\!]\rho.$$

From here, note that

$$\mathcal{E}[\![\tau_2\overline{[\tau/\alpha]}]\!]\rho = \mathcal{E}[\![\tau_2]\!]\rho\overline{[\alpha \mapsto (\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho, \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}]\!]\rho, \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle}]\!]\rho)]}$$

by Lemma 10.7. Let

$$\overline{\mathrm{VR} = \mathrm{opaqueR}(\rho_1(\tau), \rho_2(\tau), \mathcal{V}[\![\tau]\!]\rho, \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle}]\!]\rho, \mathcal{V}[\![\tau^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle}]\!]\rho)}.$$

Using $\overline{\mathrm{VR}}$ and $\overline{(W', \hat{\mathsf{v}}_1, \hat{\mathsf{v}}_2') \in \mathcal{V}[\![\tau_1]\!]\rho\overline{[\alpha \mapsto \mathrm{VR}]}}$ (which we have by Lemma 10.7 and boundary cancellation), we can instantiate $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\forall[\overline{\alpha}].(\overline{\tau_1})\to\tau_2]\!]\rho$ to get

$$(W', \mathsf{v}_1\,\overline{[\tau]}\,\overline{\hat{\mathsf{v}}_1}, \mathsf{v}_2\,\overline{[\mathsf{L}\langle\tau^{\langle\mathcal{C}\rangle}\rangle]}\,\overline{\hat{\mathsf{v}}_2'}) \in \mathcal{E}[\![\tau_2]\!]\rho\overline{[\alpha \mapsto \mathrm{VR}]}.$$

The result follows by boundary cancellation. □

Theorem 11.16 (Closure Conversion is Semantics-Preserving)
If $\overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e}:\tau \rightsquigarrow \mathbf{e}$, then

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e} \approx {}^{\tau}\mathcal{FC}\,(\mathbf{e}\overline{[\lceil\alpha\rceil/\boldsymbol{\alpha}]}\,\overline{[\mathcal{CF}^{\tau'}\,\mathsf{x}/\mathbf{x}]}) : \tau.$$

Proof

By induction on the compiler judgment, using the preceding lemmas. □

11.2 Correctness of Allocation

Lemma 11.17 (Variable)
If $\mathbf{x}:\boldsymbol{\tau} \in \boldsymbol{\Gamma}$, then $\cdot; \boldsymbol{\Delta}; \boldsymbol{\Gamma} \vdash \mathbf{x} \approx {}^{\tau}\mathcal{CA}\,(\mathcal{AC}^{\tau}\,\mathbf{x}) : \boldsymbol{\tau}$.

Proof

Follows immediately from Lemma 11.1. □

Lemma 11.18 (Unit)
$\cdot; \boldsymbol{\Delta}; \boldsymbol{\Gamma} \vdash () \approx {}^{\mathbf{unit}}\mathcal{CA}\,() : \mathbf{unit}$.

Proof

Follows from Lemmas 8.15 and 8.9. □

Lemma 11.19 (Int)
$\cdot; \mathbf{\Delta}; \mathbf{\Gamma} \vdash \mathbf{n} \approx {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,\mathbf{n} : \mathbf{int}$.

Proof

Follows from Lemmas 8.15 and 8.9. □

Lemma 11.20 (Primitive)
If $\cdot \vdash \mathbf{H}, \mathbf{H'} : \mathbf{\Psi}$, $\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x} : \boldsymbol{\tau}'} \vdash \mathbf{t} \approx {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \mathbf{int}$, and

$$\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x} : \boldsymbol{\tau}'} \vdash \mathbf{t}' \approx {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}'\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H'}) : \mathbf{int},$$

then $\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x} : \boldsymbol{\tau}'} \vdash \mathbf{t}\ \mathbf{p}\ \mathbf{t}' \approx {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,((\mathbf{t}\ \mathbf{p}\ \mathbf{t}')\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}, (\mathbf{H}, \mathbf{H'})) : \mathbf{int}$.

Proof

By Lemma 11.2, it suffices to show that

$$\begin{aligned}&\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x} : \boldsymbol{\tau}'} \vdash \mathbf{t}\,\mathbf{p}\,\mathbf{t}' \approx \\ &\qquad {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,((\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}))\ \mathbf{p}\ (\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}'\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]})), (\mathbf{H}, \mathbf{H'})) \\ &\qquad : \mathbf{int}.\end{aligned}$$

Note that $\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x} : \boldsymbol{\tau}'} \vdash \mathbf{t}\ \mathbf{p}\ \mathbf{t}' : \mathbf{int}$ and

$$\begin{aligned}&\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x} : \boldsymbol{\tau}'} \vdash {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,((\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}))\ \mathbf{p}\ (\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}'\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]})), (\mathbf{H}, \mathbf{H'})) \\ &\qquad : \mathbf{int}.\end{aligned}$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\boldsymbol{\alpha}}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x} : \boldsymbol{\tau}}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathbf{t}\ \mathbf{p}\ \mathbf{t}')), \\ &\quad \rho_2(\gamma_2({}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,((\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}))\ \mathbf{p}\ (\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}'\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]})), (\mathbf{H}, \mathbf{H'}))))) \\ &\qquad = (W, \rho_1(\gamma_1(\mathbf{t}))\ \mathbf{p}\ \rho_1(\gamma_1(\mathbf{t}')), \\ &\qquad\quad {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\rho_2(\gamma_2(\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}))))\ \mathbf{p} \\ &\qquad\qquad \rho_2(\gamma_2(\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}'\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}))), (\mathbf{H}, \mathbf{H'}))) \in \mathcal{E}[\![\mathbf{int}]\!]\rho.\end{aligned}$$

By Lemma 8.14, it suffices to show that

$$\begin{aligned}&(W \boxplus (\cdot, (\mathbf{H}, \mathbf{H'})), \rho_1(\gamma_1(\mathbf{t}))\ \mathbf{p}\ \rho_1(\gamma_1(\mathbf{t}')), \\ &\qquad {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\rho_2(\gamma_2(\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}))))\ \mathbf{p} \\ &\qquad\quad \rho_2(\gamma_2(\mathcal{AC}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}'\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]}))))) \in \mathcal{E}[\![\mathbf{int}]\!]\rho.\end{aligned}$$

By our hypotheses, Lemma 8.18, and monotonicity, we have

$$(W \boxplus (\cdot, (\mathbf{H}, \mathbf{H'})), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\mathbf{int}]\!]\rho$$

and

$$(W \boxplus (\cdot, (\mathbf{H}, \mathbf{H'})), \rho_1(\gamma_1(\mathbf{t}')), \rho_2(\gamma_2({}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathbf{t}'\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\boldsymbol{\tau}'}\,\mathbf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\mathbf{int}]\!]\rho.$$

Let $W' \sqsupseteq W \boxplus (\cdot, (\mathbf{H}, \mathbf{H'}))$, $(W', \mathbf{m}, \mathbf{m}) \in \mathcal{V}[\![\mathbf{int}]\!]\rho$, and $(W', \mathbf{n}, \mathbf{n}) \in \mathcal{V}[\![\mathbf{int}]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathbf{m}\ \mathbf{p}\ \mathbf{n}, {}^{\mathbf{int}}\mathcal{C}\mathcal{A}\,(\mathcal{AC}^{\mathbf{int}}\,\mathbf{m}\ \mathbf{p}\ \mathcal{AC}^{\mathbf{int}}\,\mathbf{n})) \in \mathcal{E}[\![\mathbf{int}]\!]\rho.$$

Since boundary translations at type **int** produce the same integers they are given, and since the semantics of primitive operations are the same in C and A, from this point it is clear that we can complete the proof using Lemma 8.15 and Lemma 8.9. □

Lemma 11.21 (If0)
If $\cdot \vdash \mathbf{H}, \mathbf{H'}, \mathbf{H''} : \Psi$, $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t} \approx {}^{\mathbf{int}}\mathcal{CA}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \mathbf{int}$,

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t'} \approx {}^{\tau}\mathcal{CA}\,(\mathbf{t'}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H'}) : \tau,$$

and

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t''} \approx {}^{\tau}\mathcal{CA}\,(\mathbf{t''}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H''}) : \tau,$$

then $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{if0\ t\ t'\ t''} \approx {}^{\tau}\mathcal{CA}\,((\mathbf{if0\ t\ t'\ t''})\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, (\mathbf{H}, \mathbf{H'}, \mathbf{H''})) : \tau$.

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{if0\ t\ t'\ t''} \approx {}^{\tau}\mathcal{CA}\,(\mathbf{if0}\ \mathcal{AC}^{\mathbf{int}}\mathcal{CA}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]})\ (\mathbf{t'}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]})\ (\mathbf{t''}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}), (\mathbf{H}, \mathbf{H'}, \mathbf{H''})) : \tau.$$

For brevity, let $\hat{\mathbf{t}} = \mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}$, $\hat{\mathbf{t}}' = \mathbf{t'}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}$, and $\hat{\mathbf{t}}'' = \mathbf{t''}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}$.
Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{if0\ t\ t'\ t''} : \mathbf{int}$ and $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash {}^{\tau}\mathcal{CA}\,(\mathbf{if0}\ (\mathcal{AC}^{\mathbf{int}}\mathcal{CA}\,\hat{\mathbf{t}})\ \hat{\mathbf{t}}'\ \hat{\mathbf{t}}'', (\mathbf{H}, \mathbf{H'}, \mathbf{H''})) : \tau$.
Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x} : \tau}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathbf{if0\ t\ t'\ t''})), \rho_2(\gamma_2({}^{\tau}\mathcal{CA}\,(\mathbf{if0}\ (\mathcal{AC}^{\mathbf{int}}\mathcal{CA}\,\hat{\mathbf{t}})\ \hat{\mathbf{t}}'\ \hat{\mathbf{t}}'', (\mathbf{H}, \mathbf{H'}, \mathbf{H''})))))\\ &\quad = (W, \mathbf{if0}\ \rho_1(\gamma_1(\mathbf{t}))\ \rho_1(\gamma_1(\mathbf{t'}))\ \rho_1(\gamma_1(\mathbf{t''})),\\ &\qquad {}^{\tau}\mathcal{CA}\,(\mathbf{if0}\ \rho_2(\gamma_2(\mathcal{AC}^{\mathbf{int}}\mathcal{CA}\,\hat{\mathbf{t}}))\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))\ \rho_2(\gamma_2(\hat{\mathbf{t}}')), (\mathbf{H}, \mathbf{H'}, \mathbf{H''}))) \in \mathcal{E}[\![\tau]\!]\rho.\end{aligned}$$

By Lemma 8.14, it suffices to show that

$$\begin{aligned}&(W \boxplus (\{\cdot\}, (\mathbf{H}, \mathbf{H'}, \mathbf{H''})), \mathbf{if0}\ \rho_1(\gamma_1(\mathbf{t}))\ \rho_1(\gamma_1(\mathbf{t'}))\ \rho_1(\gamma_1(\mathbf{t''})),\\ &\qquad {}^{\tau}\mathcal{CA}\,(\mathbf{if0}\ \rho_2(\gamma_2(\mathcal{AC}^{\mathbf{int}}\mathcal{CA}\,\hat{\mathbf{t}}))\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))\ \rho_2(\gamma_2(\hat{\mathbf{t}}')))) \in \mathcal{E}[\![\tau]\!]\rho.\end{aligned}$$

By our first hypothesis and Lemma 8.18, $(W \boxplus (\{\cdot\}, (\mathbf{H}, \mathbf{H'}, \mathbf{H''})), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\mathbf{int}}\mathcal{CA}\,\hat{\mathbf{t}}))) \in \mathcal{E}[\![\mathbf{int}]\!]\rho$.
Let $W' \sqsupseteq W \boxplus (\{\cdot\}, (\mathbf{H}, \mathbf{H'}, \mathbf{H''}))$ and $(W', \mathbf{n}, \mathbf{n}) \in \mathcal{V}[\![\mathbf{int}]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathbf{if0\ n}\ \rho_1(\gamma_1(\mathbf{t'}))\ \rho_1(\gamma_1(\mathbf{t''})), {}^{\tau}\mathcal{CA}\,(\mathbf{if0}\ (\mathcal{AC}^{\mathbf{int}}\ \mathbf{n})\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))\ \rho_2(\gamma_2(\hat{\mathbf{t}}'')))) \in \mathcal{E}[\![\tau]\!]\rho.$$

We can complete the proof using a case split on whether $n = 0$, and then applying Lemma 8.15 and the appropriate one of our hypotheses. □

Lemma 11.22 (Function)
If $\ell \notin \mathrm{dom}(\mathbf{H})$ and $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau} \vdash \mathbf{t} \approx {}^{\tau'}\mathcal{CA}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \tau'$, then

$$\cdot; \mathbf{\Delta}; \mathbf{\Gamma} \vdash \mathbf{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x} : \tau}).\mathbf{t} \approx {}^{\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}\mathcal{CA}\,(\ell, (\mathbf{H}, \ell \mapsto \mathbf{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x} : \tau^{\mathcal{A}}}).\mathbf{t})) : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'.$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \mathbf{\Delta}; \mathbf{\Gamma} \vdash \mathbf{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x} : \tau}).\mathbf{t} \approx {}^{\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}\mathcal{CA}\,(\ell, (\mathbf{H}, \ell \mapsto \mathbf{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x} : \tau^{\mathcal{A}}}).\mathbf{t}\overline{[\mathcal{AC}^{\tau}\,\mathcal{CA}\,\mathbf{x}/\mathbf{x}]})) : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'.$$

Note that $\cdot; \mathbf{\Delta}; \mathbf{\Gamma} \vdash \mathbf{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x} : \tau}).\mathbf{t} : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'$ and

$$\cdot; \mathbf{\Delta}; \mathbf{\Gamma} \vdash {}^{\forall[\overline{\alpha}].(\overline{\tau}) \to \tau'}\mathcal{CA}\,(\ell, (\mathbf{H}, \ell \mapsto \mathbf{\lambda}[\overline{\alpha}]\,(\overline{\mathbf{x} : \tau^{\mathcal{A}}}).\mathbf{t}\overline{[\mathcal{AC}^{\tau}\,\mathcal{CA}\,\mathbf{x}/\mathbf{x}]})) : \forall[\overline{\alpha}].(\overline{\tau}) \to \tau'.$$

Let $W \in \text{World}$, $\rho \in \mathcal{D}[\![\mathbf{\Delta}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\mathbf{\Gamma}]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1(\gamma_1(\boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{t})), \rho_2(\gamma_2(^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}\mathcal{CA}\,(\ell, (\mathbf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}^{\mathcal{A}}}).\mathbf{t}[\overline{\mathcal{AC}^{\tau}\,\mathcal{CA}\,\mathbf{x}/\mathbf{x}}])))))) \\ = (W, \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{t}, {}^{\forall[\overline{\alpha}].(\overline{\tau})\to\tau'}\mathcal{CA}\,(\ell, (\mathbf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}^{\mathcal{A}}}).\mathbf{t}[\overline{\mathcal{AC}^{\tau}\,\mathcal{CA}\,\mathbf{x}/\mathbf{x}}]))) \\ \in \mathcal{E}[\![\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau}']\!]\rho.\end{aligned}$$

By Lemma 8.14 and Lemma 8.9, it suffices to show that

$$\begin{aligned}(W \boxplus (\{\cdot\}, (\mathbf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}^{\mathcal{A}}}).\mathbf{t}[\overline{\mathcal{AC}^{\tau}\,\mathcal{CA}\,\mathbf{x}/\mathbf{x}}])), \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{t}, \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).(^{\tau'}\mathcal{CA}\,\ell\,[\overline{\lceil\boldsymbol{\alpha}\rceil}]\,\overline{\mathcal{AC}^{\tau}\,\mathbf{x}})) \\ \in \mathcal{V}[\![\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau}']\!]\rho.\end{aligned}$$

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, (\mathbf{H}, \ell \mapsto \boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}^{\mathcal{A}}}).\mathbf{t}[\overline{\mathcal{AC}^{\tau}\,\mathcal{CA}\,\mathbf{x}/\mathbf{x}}]))$, $\overline{\text{VR} \in \text{CValRel}}$, and

$$\overline{(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\boldsymbol{\tau}]\!]\rho[\boldsymbol{\alpha} \mapsto \text{VR}]}.$$

For convenience, let $\overline{\boldsymbol{\tau_1} = \text{VR}.\boldsymbol{\tau_1}}$ and $\overline{\boldsymbol{\tau_2} = \text{VR}.\boldsymbol{\tau_2}}$. We need to show that

$$\begin{aligned}(W', (\boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).\mathbf{t})\;[\overline{\boldsymbol{\tau_1}}]\;\overline{\mathbf{v_1}}, (\boldsymbol{\lambda}[\overline{\boldsymbol{\alpha}}]\,(\overline{\mathbf{x}:\boldsymbol{\tau}}).^{\tau'[\overline{\tau_2/\alpha}]}\mathcal{CA}\,(\ell\,[\overline{\lceil\boldsymbol{\alpha}\rceil}]\,\overline{\mathcal{AC}^{\tau[\overline{\tau_2/\alpha}]}\,\mathbf{x}}))\;[\overline{\boldsymbol{\tau_2}}]\;\overline{\mathbf{v_2}}) \\ \in \mathcal{E}[\![\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau}']\!]\rho\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]} = \mathcal{E}[\![\forall[\overline{\boldsymbol{\alpha}}].(\overline{\boldsymbol{\tau}}) \to \boldsymbol{\tau}']\!]\emptyset\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]}.\end{aligned}$$

By Lemma 8.15, it suffices to show that

$$(W', \mathbf{t}\overline{[\boldsymbol{\tau_1}/\boldsymbol{\alpha}][\mathbf{v_1}/\mathbf{x}]}, {}^{\tau'\overline{[\tau_2/\alpha]}}\mathcal{CA}\,(\ell\,\overline{[\boldsymbol{\tau_2}^{\langle\mathcal{A}\rangle}]}\;\overline{\mathcal{AC}^{\tau[\overline{\tau_2/\alpha}]}\,\mathbf{v_2}})) \in \mathcal{E}[\![\boldsymbol{\tau}']\!]\emptyset\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]}.$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\mathbf{v_2}$ and $\mathbf{v_2'}$ such that

$$\mathbf{AC}^{\tau\overline{[\tau_2/\alpha]}}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2') \quad \text{and} \quad {}^{\tau\overline{[\tau_2/\alpha]}}\mathbf{CA}(\mathbf{v_2}, M_2 \uplus M_2') = (\mathbf{v_2'}, M_2 \uplus M_2').$$

By Lemma 8.14, it suffices to show that

$$(W' \boxplus (\{\cdot\}, M_2'), \mathbf{t}\overline{[\boldsymbol{\tau_1}/\boldsymbol{\alpha}][\mathbf{v_1}/\mathbf{x}]}, {}^{\tau'\overline{[\tau_2/\alpha]}}\mathcal{CA}\,(\ell\,\overline{[\boldsymbol{\tau_2}^{\langle\mathcal{A}\rangle}]}\;\overline{\mathbf{v_2}})) \in \mathcal{E}[\![\boldsymbol{\tau}']\!]\emptyset\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]}.$$

By one more application of Lemma 8.15, it suffices to show

$$\begin{aligned}(W' \boxplus (\{\cdot\}, M_2'), \mathbf{t}\overline{[\boldsymbol{\tau_1}/\boldsymbol{\alpha}][\mathbf{v_1}/\mathbf{x}]}, {}^{\tau'\overline{[\tau_2/\alpha]}}\mathcal{CA}\,\mathbf{t}\overline{[\mathcal{AC}^{\tau}\,{}^{\tau}\mathcal{CA}\,\mathbf{x}/\mathbf{x}][\boldsymbol{\tau_2}^{\langle\mathcal{A}\rangle}/\boldsymbol{\alpha}][\mathbf{v_2}/\mathbf{x}]}) \\ = (W' \boxplus (\{\cdot\}, M_2'), \mathbf{t}\overline{[\boldsymbol{\tau_1}/\boldsymbol{\alpha}][\mathbf{v_1}/\mathbf{x}]}, {}^{\tau'\overline{[\tau_2/\alpha]}}\mathcal{CA}\,\mathbf{t}\overline{[\mathcal{AC}^{\tau}\,{}^{\tau}\mathcal{CA}\,\mathbf{v_2}/\mathbf{x}][\boldsymbol{\tau_2}^{\langle\mathcal{A}\rangle}/\boldsymbol{\alpha}]}) \in \mathcal{E}[\![\boldsymbol{\tau}']\!]\emptyset\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]}.\end{aligned}$$

Finally, by Lemma 8.17, it suffices to show that

$$(W' \boxplus (\{\cdot\}, M_2'), \mathbf{t}\overline{[\boldsymbol{\tau_1}/\boldsymbol{\alpha}][\mathbf{v_1}/\mathbf{x}]}, {}^{\tau'\overline{[\tau_2/\alpha]}}\mathcal{CA}\,\mathbf{t}\overline{[\mathcal{AC}^{\tau}\,\mathbf{v_2'}/\mathbf{x}][\boldsymbol{\tau_2}^{\langle\mathcal{A}\rangle}/\boldsymbol{\alpha}]}) \in \mathcal{E}[\![\boldsymbol{\tau}']\!]\emptyset\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]},$$

which we have from our hypothesis and Lemma 8.18, since $\emptyset\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]} \in \mathcal{D}[\![\overline{\boldsymbol{\alpha}}]\!]$, and by boundary cancellation, $(W' \boxplus (\emptyset, M_2'), \emptyset\overline{[\mathbf{x} \mapsto (\mathbf{v_1}, \mathbf{v_2'})]}) \in \mathcal{G}[\![\overline{\mathbf{x}:\boldsymbol{\tau}}]\!]\emptyset\overline{[\boldsymbol{\alpha} \mapsto \text{VR}]}$. □

Lemma 11.23 (Application)
If $\cdot \vdash \mathbf{H_0}, \overline{\mathbf{H}} : \mathbf{\Psi}$, $\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x}:\boldsymbol{\tau'}} \vdash \mathbf{t_0} \approx {}^{\forall[].(\overline{\tau_1})\to\tau_2}\mathcal{CA}\,(\mathbf{t_0}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H_0}) : \forall[].(\overline{\boldsymbol{\tau_1}}) \to \boldsymbol{\tau_2}$, and

$$\overline{\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x}:\boldsymbol{\tau'}} \vdash \mathbf{t} \approx {}^{\tau_1}\mathcal{CA}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \boldsymbol{\tau_1}},$$

then $\cdot; \overline{\boldsymbol{\alpha}}; \overline{\mathbf{x}:\boldsymbol{\tau'}} \vdash \mathbf{t_0}\;[]\;\overline{\mathbf{t}} \approx {}^{\tau_2}\mathcal{CA}\,((\mathbf{t_0}\;[]\;\overline{\mathbf{t}})\overline{[\lceil\boldsymbol{\alpha}\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, (\mathbf{H_0}, \overline{\mathbf{H}})) : \boldsymbol{\tau_2}$.

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t_0}\ [\overline{\tau}]\ \overline{\mathbf{t}} \approx {}^{\tau_2}\mathcal{CA}\ ((\mathcal{AC}^{\forall[].(\overline{\tau_1})\to\tau_2}\ \mathcal{CA}\ \mathbf{t_0}\ []\ \overline{\mathcal{AC}^{\tau_1}\ \mathcal{CA}\ \mathbf{t}})\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]}, (\mathbf{H_0}, \overline{\mathbf{H}})) : \tau_2.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t_0}\ []\ \overline{\mathbf{t}} : \tau_2$ and

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash {}^{\tau_2}\mathcal{CA}\ ((\mathcal{AC}^{\forall[].(\overline{\tau_1})\to\tau_2}\ \mathcal{CA}\ \mathbf{t_0}\ []\ \overline{\mathcal{AC}^{\tau_1}\ \mathcal{CA}\ \mathbf{t}})\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]}, (\mathbf{H_0}, \overline{\mathbf{H}})) : \tau_2.$$

Let $W \in \text{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x} : \tau'}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathbf{t_0}\ []\ \overline{\mathbf{t}})), \rho_2(\gamma_2({}^{\tau_2}\mathcal{CA}\ ((\mathcal{AC}^{\forall[].(\overline{\tau_1})\to\tau_2}\ \mathcal{CA}\ \mathbf{t_0}\ []\ \overline{\mathcal{AC}^{\tau_1}\ \mathcal{CA}\ \mathbf{t}})\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]}, (\mathbf{H_0}, \overline{\mathbf{H}})))))\\ &\quad = (W, \rho_1(\gamma_1(\mathbf{t_0}))\ []\ \overline{\rho_1(\gamma_1(\mathbf{t}))}, {}^{\tau_2}\mathcal{CA}\ (\rho_2(\gamma_2(\mathcal{AC}^{\forall[].(\overline{\tau_1})\to\tau_2}\ \mathcal{CA}\ \mathbf{t_0}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]}))\\ &\qquad\qquad []\ \overline{\rho_2(\gamma_2(\mathcal{AC}^{\tau_1}\ \mathcal{CA}\ \mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]}))}, (\mathbf{H_0}, \overline{\mathbf{H}})) \in \mathcal{E}[\![\tau_2]\!]\rho.\end{aligned}$$

By Lemma 8.14, it suffices to show that

$$\begin{aligned}&(W \uplus (\cdot, (\mathbf{H_0}, \overline{\mathbf{H}})), \rho_1(\gamma_1(\mathbf{t_0}))\ []\ \overline{\rho_1(\gamma_1(\mathbf{t}))},\\ &\qquad {}^{\tau_2}\mathcal{CA}\ (\rho_2(\gamma_2(\mathcal{AC}^{\forall[].(\overline{\tau_1})\to\tau_2}\ \mathcal{CA}\ \mathbf{t_0}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]}))\\ &\qquad\quad []\ \overline{\rho_2(\gamma_2(\mathcal{AC}^{\tau_1}\ \mathcal{CA}\ \mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]}))}, (\mathbf{H_0}, \overline{\mathbf{H}})) \in \mathcal{E}[\![\tau_2]\!]\rho.\end{aligned}$$

By our hypotheses, Lemma 8.18, and monotonicity, we have

$$(W \uplus (\cdot, (\mathbf{H_0}, \overline{\mathbf{H}})), \rho_1(\gamma_1(\mathbf{t_0})), \rho_2(\gamma_2({}^{\forall[].(\overline{\tau_1})\to\tau_2}\mathcal{CA}\ (\mathbf{t_0}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\forall[].(\overline{\tau_1})\to\tau_2]\!]\rho$$

and

$$\overline{(W \uplus (\cdot, (\mathbf{H_0}, \overline{\mathbf{H}})), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\tau_1}\mathcal{CA}\ (\mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\tau_1]\!]\rho}.$$

Let $W' \sqsupseteq W \uplus (\cdot, (\mathbf{H_0}, \overline{\mathbf{H}}))$, $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[].(\overline{\tau_1})\to\tau_2]\!]\rho$, and $\overline{(W', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau_1]\!]\rho}$. By Lemma 8.20, it suffices to show that

$$(W', \mathbf{v_1}\ []\ \overline{\hat{\mathbf{v}}_1}, {}^{\rho_2(\tau_2)}\mathcal{CA}\ (\mathcal{AC}^{\rho_2(\forall[].(\overline{\tau_1})\to\tau_2)}\ \mathbf{v_2}\ []\ \overline{\mathcal{AC}^{\rho_2(\tau_1)}\ \hat{\mathbf{v}}_2})) \in \mathcal{E}[\![\tau_2]\!]\rho.$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\overline{\hat{\mathbf{v}}_2}$ and $\overline{\hat{\mathbf{v}}'_2}$ such that

$$\overline{\mathbf{AC}^{\rho_2(\tau_1)}(\hat{\mathbf{v}}_2, M_2) = (\hat{\mathbf{v}}_2, M_2 \uplus M'_2)} \quad \text{and} \quad \overline{{}^{\rho_2(\tau_1)}\mathbf{CA}(\hat{\mathbf{v}}_2, M_2 \uplus M'_2) = (\hat{\mathbf{v}}_2, M_2 \uplus M'_2)}.$$

Note that

$$\begin{aligned}&\langle M_2 \mid {}^{\rho_2(\tau_2)}\mathcal{CA}\ (\mathcal{AC}^{\rho_2(\forall[].(\overline{\tau_1})\to\tau_2)}\ \mathbf{v_2}\ []\ \overline{\mathcal{AC}^{\rho_2(\tau_1)}\ \hat{\mathbf{v}}_2})\rangle\\ \longmapsto\ &\langle M_2, \ell \mapsto (\lambda[]\,(\overline{\mathbf{y} : \rho_2(\tau_1)^{\mathcal{A}}}).\mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{{}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathbf{y}}) \mid {}^{\rho_2(\tau_2)}\mathcal{CA}\ (\ell\ []\ \overline{\mathcal{AC}^{\rho_2(\tau_1)}\ \hat{\mathbf{v}}_2})\rangle\\ \longmapsto^*\ &\langle M_2, \ell \mapsto (\lambda[]\,(\overline{\mathbf{y} : \rho_2(\tau_1)^{\mathcal{A}}}).\mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{{}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathbf{y}}), \overline{M'_2} \mid {}^{\rho_2(\tau_2)}\mathcal{CA}\ (\ell\ []\ \hat{\mathbf{v}}_2)\rangle\\ \longmapsto\ &\langle M_2, \ell \mapsto (\lambda[]\,(\overline{\mathbf{y} : \rho_2(\tau_1)^{\mathcal{A}}}).\mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{{}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathbf{y}}), \overline{M'_2} \mid {}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{{}^{\rho_2(\tau_2)}\mathcal{CA}\ \hat{\mathbf{v}}_2}\rangle\\ \longmapsto^*\ &\langle M_2, \ell \mapsto (\lambda[]\,(\overline{\mathbf{y} : \rho_2(\tau_1)^{\mathcal{A}}}).\mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{{}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathbf{y}}), \overline{M'_2} \mid {}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{\hat{\mathbf{v}}'_2}\rangle.\end{aligned}$$

Let $W'' = W' \uplus (\{\cdot\}, \{\ell \mapsto \lambda[]\,(\overline{\mathbf{y} : \rho_2(\tau_1)^{\mathcal{A}}}).\mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{{}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathbf{y}}\} \uplus \overline{M'_2})$. By Lemma 8.14, it suffices to show that

$$(W'', \mathbf{v_1}\ []\ \overline{\hat{\mathbf{v}}_1}, {}^{\rho_2(\tau_2)}\mathcal{CA}\ \mathcal{AC}^{\rho_2(\tau_2)}\ \mathbf{v_2}\ []\ \overline{\hat{\mathbf{v}}'_2}) \in \mathcal{E}[\![\tau_2]\!]\rho.$$

By monotonicity and boundary cancellation, $\overline{(W'', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}'_2) \in \mathcal{V}[\![\tau_1]\!]\rho}$, so we can instantiate our assumption that $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[].(\overline{\tau_1})\to\tau_2]\!]\rho$ to get

$$(W'', \mathbf{v_1}\ []\ \overline{\hat{\mathbf{v}}_1}, \mathbf{v_2}\ []\ \overline{\hat{\mathbf{v}}'_2}) \in \mathcal{E}[\![\tau_2]\!]\rho.$$

The result follows by another use of boundary cancellation. □

Lemma 11.24 (Type Application)
If $\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{t} \approx {}^{\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2$, and $\overline{\alpha} \vdash \tau_0$ then

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{t}[\tau_0] \approx {}^{\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']}\mathcal{CA}\,((\mathbf{t}[\tau_0{}^{\mathcal{A}}])\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta'].$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{t}[\tau_0] \approx {}^{\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']}\mathcal{CA}\,(((\mathcal{AC}^{\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2}\,\mathcal{CA}\,\mathbf{t})[\tau_0{}^{\mathcal{A}}])\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta'].$$

Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{t}[\tau_0] : \forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']$ and

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash {}^{\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']}\mathcal{CA}\,(((\mathcal{AC}^{\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2}\,\mathcal{CA}\,\mathbf{t})[\tau_0{}^{\mathcal{A}}])\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta'].$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\overline{\mathbf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathbf{t}[\tau_0])),\\ &\quad \rho_2(\gamma_2({}^{\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']}\mathcal{CA}\,(((\mathcal{AC}^{\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2}\,\mathcal{CA}\,\mathbf{t})[\tau_0{}^{\mathcal{A}}])\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}))))\\ &= (W, \rho_1(\gamma_1(\mathbf{t}))[\rho_1(\tau_0)],\\ &\qquad {}^{\rho_2(\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta'])}\mathcal{CA}\,(((\mathcal{AC}^{\rho_2(\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2)}\,\mathcal{CA}\,\rho_2(\gamma_2(\mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]})))\\ &\qquad\qquad [\rho_2(\tau_0{}^{\langle\mathcal{A}\rangle})]), \mathbf{H}))\\ &\qquad\qquad \in \mathcal{E}[\![\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']]\!]\rho.\end{aligned}$$

By Lemma 8.15, it suffices to show that

$$\begin{aligned}&(W \boxplus (\{\cdot\}, \mathbf{H}), \rho_1(\gamma_1(\mathbf{t}))[\rho_1(\tau_0)],\\ &\quad {}^{\rho_2(\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta'])}\mathcal{CA}\,((\mathcal{AC}^{\rho_2(\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2)}\,\mathcal{CA}\,\rho_2(\gamma_2(\mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]})))\\ &\quad\qquad [\rho_2(\tau_0{}^{\langle\mathcal{A}\rangle})]))\\ &\quad\qquad \in \mathcal{E}[\![\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']]\!]\rho.\end{aligned}$$

By Lemma 8.18 and our hypothesis,

$(W \boxplus (\{\cdot\}, \mathbf{H}), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2}\mathcal{CA}\,(\mathbf{t}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}]})))) \in \mathcal{E}[\![\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2]\!]\rho.$

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, \mathbf{H})$ and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2]\!]\rho$. By Lemma 8.20, it suffices to show that

$$\begin{aligned}&(W', \mathbf{v_1}[\rho_1(\tau_0)], {}^{\rho_2(\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta'])}\mathcal{CA}\,((\mathcal{AC}^{\rho_2(\forall[\beta',\overline{\beta}].(\overline{\tau_1}) \to \tau_2)}\,\mathbf{v_2})[\rho_2(\tau_0{}^{\langle\mathcal{A}\rangle})]))\\ &\qquad \in \mathcal{E}[\![\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']]\!]\rho.\end{aligned}$$

By Lemma 8.14 and Lemma 8.9, it suffices to show that

$$\begin{aligned}&(W' \boxplus (\{\cdot\}, \{\ell \mapsto \lambda[\beta',\overline{\beta}](\overline{\mathbf{y}:\rho_2(\tau_1)^{\langle\mathcal{A}\rangle}[\beta'/\lceil\beta'\rceil]\overline{[\beta/\lceil\beta\rceil]}}).\\ &\qquad\qquad \mathcal{AC}^{\rho_2(\tau_2)[\mathbf{L}\langle\beta'\rangle/\beta']\overline{[\mathbf{L}\langle\beta\rangle/\beta]}}\,\mathbf{v_2}\,[\mathbf{L}\langle\beta'\rangle, \overline{\mathbf{L}\langle\beta\rangle}]\,\overline{{}^{\rho_2(\tau_1)[\mathbf{L}\langle\beta'\rangle/\beta']\overline{[\mathbf{L}\langle\beta\rangle/\beta]}}\mathcal{CA}\,\mathbf{y}}\}),\\ &\quad \mathbf{v_1}[\rho_1(\tau_0)],\\ &\quad \lambda[\overline{\beta}](\overline{\mathbf{y}:\rho_2(\tau_1[\tau_0/\beta'])}).{}^{\rho_2(\tau_2[\tau_0/\beta'])}\mathcal{CA}\,(\ell[\rho_2(\tau_0{}^{\langle\mathcal{A}\rangle})]\,[\overline{\lceil\beta\rceil}]\,\overline{\mathcal{AC}^{\rho_2(\tau_1[\tau_0/\beta'])}\,\mathbf{y}})\\ &\qquad \in \mathcal{V}[\![\forall[\overline{\beta}].(\overline{\tau_1[\tau_0/\beta']}) \to \tau_2[\tau_0/\beta']]\!]\rho.\end{aligned}$$

Let

$$W'' \sqsupseteq W' \boxplus (\{\cdot\}, \{\ell \mapsto \lambda[\beta', \overline{\beta}]\,(\overline{\mathbf{y}:\rho_2(\tau_1)^{\langle\mathcal{A}\rangle}[\beta'/\lceil\beta'\rceil][\beta/\lceil\beta\rceil]}).\ \mathcal{AC}^{\rho_2(\tau_2)[\mathbf{L}\langle\beta'\rangle/\beta'][\mathbf{L}\langle\beta\rangle/\beta]}\ \mathbf{v_2}\ [\mathbf{L}\langle\beta'\rangle, \overline{\mathbf{L}\langle\beta\rangle}]\ \overline{{}^{\rho_2(\tau_1)[\mathbf{L}\langle\beta'\rangle/\beta'][\mathbf{L}\langle\beta\rangle/\beta]}\mathcal{CA}\ \mathbf{y}}\}),$$

$\overline{\mathrm{VR} \in \mathrm{CValRel}}$, and $\overline{(W'', \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \in \mathcal{V}[\![\tau_1[\tau_0/\beta']]\!]\rho[\beta \mapsto \mathrm{VR}]}$. For convenience, let $\overline{\hat{\tau}_1 = \mathrm{VR}.\tau_1}$ and $\overline{\hat{\tau}_2 = \mathrm{VR}.\tau_2}$. We need to show that

$$(W'', (\mathbf{v_1}[\rho_1(\tau_0)])\ [\overline{\hat{\tau}_1}]\ \overline{\hat{\mathbf{v}}_1},\ (\lambda[\overline{\beta}]\,(\overline{\mathbf{y}:\rho_2(\tau_1[\tau_0/\beta'])}).^{\rho_2(\tau_2[\tau_0/\beta'])}\mathcal{CA}\ (\ell[\rho_2(\tau_0{}^{\langle\mathcal{A}\rangle})])\ [\overline{\lceil\beta\rceil}]\ \overline{\mathcal{AC}^{\rho_2(\tau_1[\tau_0/\beta'])}\ \mathbf{y}})\ [\overline{\hat{\tau}_2}]\ \overline{\hat{\mathbf{v}}_2}) \in \mathcal{E}[\![\tau_2[\tau_0/\beta']]\!]\rho[\overline{\beta \mapsto \mathrm{VR}}].$$

Let

$$\rho' = \rho[\overline{\beta \mapsto \mathrm{VR}}][\beta' \mapsto (\rho_1(\tau_0), \rho_2(\tau_0), \mathcal{V}[\![\tau_0]\!]\rho, \mathcal{V}[\![\tau_0{}^{\langle\mathcal{A}\rangle}]\!]\rho)]$$

and

$$\hat{\rho} = \rho[\overline{\beta \mapsto \mathrm{opaqueR}\,\mathrm{VR}}][\beta' \mapsto \mathrm{opaqueR}(\rho_1(\tau_0), \rho_2(\tau_0), \mathcal{V}[\![\tau_0]\!]\rho, \mathcal{V}[\![\tau_0{}^{\langle\mathcal{A}\rangle}]\!]\rho)].$$

Note that $\overline{\mathcal{V}[\![\tau_1[\tau_0/\beta']]\!]\rho[\beta \mapsto \mathrm{VR}] = \mathcal{V}[\![\tau_1]\!]\rho'}$ and $\overline{\mathcal{E}[\![\tau_2[\tau_0/\beta']]\!]\rho[\beta \mapsto \mathrm{VR}] = \mathcal{E}[\![\tau_2]\!]\rho'}$, by Lemma 10.6. By Lemma 8.3, for any $(M_1, M_2) : W''$, there are some $\overline{\mathbf{v_2}}$ and $\overline{\mathbf{v_2'}}$ such that

$$\overline{\mathbf{AC}^{\rho_2'(\tau_1)}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2')} \quad \text{and} \quad \overline{{}^{\hat{\rho}_2(\tau_1)}\mathbf{CA}(\mathbf{v_2}, M_2 \uplus M_2') = (\mathbf{v_2}, M_2 \uplus M_2')}.$$

Note that

$$\begin{aligned}
&\langle M_2 \mid (\lambda[\overline{\beta}]\,(\overline{\mathbf{y}:\rho_2(\tau_1[\tau_0/\beta'])}).^{\rho_2(\tau_2[\tau_0/\beta'])}\mathcal{CA}\ (\ell[\rho_2(\tau_0{}^{\langle\mathcal{A}\rangle})])\ [\overline{\lceil\beta\rceil}]\ \overline{\mathcal{AC}^{\rho_2(\tau_1[\tau_0/\beta'])}\ \mathbf{y}})\ [\overline{\hat{\tau}_2}]\ \overline{\hat{\mathbf{v}}_2}\rangle \\
\longmapsto\ &\langle M_2 \mid {}^{\rho_2'(\tau_2)}\mathcal{CA}\ (\ell[\rho_2'(\tau_0{}^{\langle\mathcal{A}\rangle})])\ [\overline{\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}}]\ \overline{\mathcal{AC}^{\rho_2'(\tau_1)}\ \hat{\mathbf{v}}_2}\rangle \\
\longmapsto^*\ &\langle M_2 \uplus \overline{M_2'} \mid {}^{\rho_2'(\tau_2)}\mathcal{CA}\ (\ell[\rho_2'(\tau_0{}^{\langle\mathcal{A}\rangle})])\ [\overline{\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}}]\ \overline{\hat{\mathbf{v}}_2}\rangle \\
\longmapsto\ &\langle M_2 \uplus \overline{M_2'} \mid {}^{\rho_2'(\tau_2)}\mathcal{CA}\,\mathcal{AC}^{\hat{\rho}_2(\tau_2)}\ \mathbf{v_2}\ [\mathbf{L}\langle\rho_2'(\tau_0{}^{\langle\mathcal{A}\rangle})\rangle, \overline{\mathbf{L}\langle\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}\rangle}]\ \overline{{}^{\hat{\rho}_2(\tau_1)}\mathcal{CA}\ \hat{\mathbf{v}}_2}\rangle \\
\longmapsto^*\ &\langle M_2 \uplus \overline{M_2'} \mid {}^{\rho_2'(\tau_2)}\mathcal{CA}\,\mathcal{AC}^{\hat{\rho}_2(\tau_2)}\ \mathbf{v_2}\ [\mathbf{L}\langle\rho_2'(\tau_0{}^{\langle\mathcal{A}\rangle})\rangle, \overline{\mathbf{L}\langle\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}\rangle}]\ \overline{\hat{\mathbf{v}}_2'}\rangle.
\end{aligned}$$

By Lemma 8.14, it suffices to show that

$$(W'' \boxplus (\{\cdot\}, \overline{M_2'}), \mathbf{v_1}\ [\rho_1(\tau_0), \overline{\hat{\tau}_1}]\ \overline{\hat{\mathbf{v}}_1}, {}^{\rho_2'(\tau_2)}\mathcal{CA}\,\mathcal{AC}^{\hat{\rho}_2(\tau_2)}\ \mathbf{v_2}\ [\mathbf{L}\langle\rho_2'(\tau_0{}^{\langle\mathcal{A}\rangle})\rangle, \overline{\mathbf{L}\langle\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}\rangle}]\ \overline{\hat{\mathbf{v}}_2'}) \in \mathcal{E}[\![\tau_2]\!]\rho'.$$

Since $\overline{(W'' \boxplus (\{\cdot\}, \overline{M_2'}), \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2') \in \mathcal{V}[\![\tau_1]\!]\hat{\rho}}$ by boundary cancellation and monotonicity, we can instantiate our assumption that $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\forall[\beta', \overline{\beta}].(\overline{\tau_1}) \to \tau_2]\!]\rho$ to get

$$(W'' \boxplus (\{\cdot\}, \overline{M_2'}), \mathbf{v_1}\ [\rho_1(\tau_0), \overline{\hat{\tau}_1}]\ \overline{\hat{\mathbf{v}}_1}, \mathbf{v_2}\ [\mathbf{L}\langle\rho_2'(\tau_0{}^{\langle\mathcal{A}\rangle})\rangle, \overline{\mathbf{L}\langle\hat{\tau}_2{}^{\langle\mathcal{A}\rangle}\rangle}]\ \overline{\hat{\mathbf{v}}_2'}) \in \mathcal{E}[\![\tau_2]\!]\hat{\rho}.$$

The result follows by another use of boundary cancellation. □

Lemma 11.25 (Pack)
If $\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{t} \approx {}^{\tau[\hat{\tau}/\alpha]}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}], \mathbf{H}) : \tau[\hat{\tau}/\alpha]$, then

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{pack}\langle\hat{\tau}, \mathbf{t}\rangle\ \mathbf{as}\ \exists\alpha.\tau \approx {}^{\exists\alpha.\tau}\mathcal{CA}\ ((\mathbf{pack}\langle\hat{\tau}^{\mathcal{A}}, \mathbf{t}\rangle\ \mathbf{as}\ \exists\alpha.\tau^{\mathcal{A}})[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}], \mathbf{H}) : \exists\alpha.\tau.$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{pack}\langle\hat{\tau}, \mathbf{t}\rangle\ \mathbf{as}\ \exists\beta.\tau \approx {}^{\exists\beta.\tau}\mathcal{CA}\ (\mathbf{pack}\langle\hat{\tau}^{\mathcal{A}}[\overline{\lceil\alpha\rceil/\alpha}], \mathcal{AC}^{\tau[\hat{\tau}/\beta]}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])\rangle\ \mathbf{as}\ \exists\beta.\tau^{\mathcal{A}}, \mathbf{H}) : \exists\beta.\tau.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{pack}\langle\hat{\tau},\mathbf{t}\rangle\ \mathbf{as}\ \exists\beta.\tau : \exists\beta.\tau$ and

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash {}^{\exists\beta.\tau}\mathcal{CA}\ (\mathbf{pack}\langle\hat{\tau}^{\mathcal{A}}[\overline{\lceil\alpha\rceil/\alpha}],\mathcal{AC}^{\tau[\hat{\tau}/\beta]}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])\rangle\ \mathbf{as}\ \exists\beta.\tau^{\mathcal{A}}, \mathbf{H}) : \exists\beta.\tau.$$

Let $W \in \text{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\overline{\mathbf{x}:\tau}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathbf{pack}\langle\hat{\tau},\mathbf{t}\rangle\ \mathbf{as}\ \exists\beta.\tau)),\\ &\quad \rho_2(\gamma_2({}^{\exists\beta.\tau}\mathcal{CA}\ (\mathbf{pack}\langle\hat{\tau}^{\mathcal{A}}[\overline{\lceil\alpha\rceil/\alpha}],\mathcal{AC}^{\tau[\hat{\tau}/\beta]}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])\rangle\ \mathbf{as}\ \exists\beta.\tau^{\mathcal{A}}[\overline{\lceil\alpha\rceil/\alpha}], \mathbf{H}))))\\ &\quad = (W, \mathbf{pack}\langle\rho_1(\hat{\tau}),\rho_1(\gamma_1(\mathbf{t}))\rangle\ \mathbf{as}\ \rho_1(\exists\beta.\tau),\\ &\qquad {}^{\rho_2(\exists\beta.\tau)}\mathcal{CA}\ (\mathbf{pack}\langle\rho_2(\hat{\tau}^{\langle\mathcal{A}\rangle}),\mathcal{AC}^{\rho_2(\tau[\hat{\tau}/\beta])}\mathcal{CA}\ (\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])))\rangle, \mathbf{H}))\\ &\qquad\qquad \in \mathcal{E}[\![\exists\beta.\tau]\!]\rho.\end{aligned}$$

By Lemma 8.15, it suffices to show that

$$\begin{aligned}&(W \boxplus (\{\cdot\}, \mathbf{H}), \mathbf{pack}\langle\rho_1(\hat{\tau}),\rho_1(\gamma_1(\mathbf{t}))\rangle\ \mathbf{as}\ \rho_1(\exists\beta.\tau),\\ &\qquad {}^{\rho_2(\exists\beta.\tau)}\mathcal{CA}\ (\mathbf{pack}\langle\rho_2(\hat{\tau}^{\langle\mathcal{A}\rangle}),\mathcal{AC}^{\rho_2(\tau[\hat{\tau}/\beta])}\mathcal{CA}\ (\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])))\rangle)\\ &\qquad\qquad \in \mathcal{E}[\![\exists\beta.\tau]\!]\rho.\end{aligned}$$

By Lemma 8.18 and our hypothesis,

$$(W \boxplus (\{\cdot\}, \mathbf{H}), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\tau[\hat{\tau}/\beta]}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])))) \in \mathcal{E}[\![\tau[\hat{\tau}/\beta]]\!]\rho.$$

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, \mathbf{H})$ and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau[\hat{\tau}/\beta]]\!]\rho$. By Lemma 8.20, it suffices to show that

$$\begin{aligned}&(W', \mathbf{pack}\langle\rho_1(\hat{\tau}),\mathbf{v_1}\rangle\ \mathbf{as}\ \rho_1(\exists\beta.\tau),\\ &\quad {}^{\rho_2(\exists\beta.\tau)}\mathcal{CA}\ \mathbf{pack}\langle\rho_2(\hat{\tau}^{\langle\mathcal{A}\rangle}),\mathcal{AC}^{\rho_2(\tau[\hat{\tau}/\beta])}\ \mathbf{v_2}\rangle\ \mathbf{as}\ \rho_2(\exists\beta.\tau^{\langle\mathcal{A}\rangle})) \in \mathcal{E}[\![\exists\beta.\tau]\!]\rho.\end{aligned}$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\mathbf{v_2}$ and $\mathbf{v_2'}$ such that

$$\mathbf{AC}^{\rho_2(\tau[\hat{\tau}/\beta])}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2') \quad \text{and} \quad {}^{\mathbf{L}\langle\rho_2(\tau[\hat{\tau}/\beta]^{\langle\mathcal{A}\rangle})\rangle}\mathbf{CA}(\mathbf{v_2}, M_2 \uplus M_2') = (\mathbf{v_2'}, M_2 \uplus M_2').$$

By the operational semantics,

$$\begin{aligned}&\langle M_2 \mid {}^{\rho_2(\exists\beta.\tau)}\mathcal{CA}\ \mathbf{pack}\langle\rho_2(\hat{\tau}^{\langle\mathcal{A}\rangle}),\mathcal{AC}^{\rho_2(\tau[\hat{\tau}/\beta])}\ \mathbf{v_2}\rangle\ \mathbf{as}\ \rho_2(\exists\beta.\tau)\rangle\\ &\qquad\qquad \longmapsto^2 \langle M_2 \uplus M_2' \mid \mathbf{pack}\langle\mathbf{L}\langle\rho_2(\hat{\tau}^{\langle\mathcal{A}\rangle})\rangle,\mathbf{v_2'}\rangle\ \mathbf{as}\ \rho_2(\exists\beta.\tau^{\langle\mathcal{A}\rangle})\rangle.\end{aligned}$$

Thus, by Lemma 8.15 and Lemma 8.9, it suffices to show that

$$(W' \boxplus (\{\cdot\}, M_2'), \mathbf{pack}\langle\rho_1(\hat{\tau}),\mathbf{v_1}\rangle\ \mathbf{as}\ \rho_1(\exists\beta.\tau), \mathbf{pack}\langle\mathbf{L}\langle\rho_2(\hat{\tau}^{\langle\mathcal{A}\rangle})\rangle,\mathbf{v_2'}\rangle\ \mathbf{as}\ \rho_2(\exists\beta.\tau)) \in \mathcal{V}[\![\exists\beta.\tau]\!]\rho.$$

To show this, we need to find some $\text{VR} \in \text{CValRel}$ such that $\text{VR}.\tau_1 = \rho_1(\hat{\tau})$, $\text{VR}.\tau_2 = \mathbf{L}\langle\rho_2(\hat{\tau}^{\langle\mathcal{A}\rangle})\rangle$, and $(W' \boxplus (\{\cdot\}, M_2'), \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto \text{VR}]$. We use

$$\text{VR} = \text{opaqueR}(\rho_1(\hat{\tau}), \rho_2(\hat{\tau}), \mathcal{V}[\![\hat{\tau}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{A}\rangle}]\!]\rho).$$

That this $\text{VR} \in \text{CValRel}$ follows from Lemma 10.4 and Lemma 8.35. The types match by definition of opaqueR. For the last condition, note that

$$(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto (\rho_1(\hat{\tau}), \rho_2(\hat{\tau}), \mathcal{V}[\![\hat{\tau}]\!]\rho, \mathcal{V}[\![\hat{\tau}^{\langle\mathcal{A}\rangle}]\!]\rho)]$$

by Lemma 10.6. The result follows directly from boundary cancellation. □

Lemma 11.26 (Unpack)
If $\cdot \vdash \mathbf{H}, \mathbf{H'} : \mathbf{\Psi}$, $\cdot ; \overline{\boldsymbol{\alpha}} ; \overline{\mathbf{x} : \boldsymbol{\tau'}} \vdash \mathbf{t} \approx {}^{\exists \boldsymbol{\alpha}.\boldsymbol{\tau}}\mathcal{CA}\,(\mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{AC}^{\boldsymbol{\tau'}}\,\mathbf{x}/\mathbf{x}]}, \mathbf{H}) : \exists \boldsymbol{\alpha}.\boldsymbol{\tau}$ and

$$\cdot ; \overline{\boldsymbol{\alpha}}, \boldsymbol{\beta} ; \overline{\mathbf{x} : \boldsymbol{\tau'}}, \mathbf{y} : \boldsymbol{\tau} \vdash \mathbf{t'} \approx {}^{\hat{\boldsymbol{\tau}}}\mathcal{CA}\,(\mathbf{t'}\overline{[\lceil\boldsymbol{\alpha}\rceil/\boldsymbol{\alpha}]}[\lceil\boldsymbol{\beta}\rceil/\boldsymbol{\beta}]\overline{[\mathcal{AC}^{\boldsymbol{\tau'}}\,\mathbf{x}/\mathbf{x}]}[\mathcal{AC}^{\boldsymbol{\tau}}\,\mathbf{y}/\mathbf{y}], \mathbf{H'}) : \hat{\boldsymbol{\tau}},$$

then

$$\cdot ; \overline{\boldsymbol{\alpha}} ; \overline{\mathbf{x} : \boldsymbol{\tau'}} \vdash \mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t'} \approx {}^{\hat{\boldsymbol{\tau}}}\mathcal{CA}\,((\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t'})\overline{[\lceil\boldsymbol{\alpha}\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{AC}^{\boldsymbol{\tau'}}\,\mathbf{x}/\mathbf{x}]}, (\mathbf{H}, \mathbf{H'}) : \hat{\boldsymbol{\tau}}.$$

Proof

For brevity, let $\hat{\mathbf{t}} = \mathbf{t}\overline{[\lceil\boldsymbol{\alpha}\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{AC}^{\boldsymbol{\tau'}}\,\mathbf{x}/\mathbf{x}]}$ and $\hat{\mathbf{t}}' = \mathbf{t'}\overline{[\lceil\boldsymbol{\alpha}\rceil/\boldsymbol{\alpha}]}\overline{[\mathcal{AC}^{\boldsymbol{\tau'}}\,\mathbf{x}/\mathbf{x}]}$. By Lemma 11.2, it suffices to show that

$$\begin{aligned}&\cdot ; \overline{\boldsymbol{\alpha}} ; \overline{\mathbf{x} : \boldsymbol{\tau'}} \vdash \mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t'} \approx \\ &\qquad {}^{\hat{\boldsymbol{\tau}}}\mathcal{CA}\,(\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathcal{AC}^{\exists \boldsymbol{\beta}.\boldsymbol{\tau}}\mathcal{CA}\,\hat{\mathbf{t}})\ \mathbf{in}\ \hat{\mathbf{t}}'[\mathcal{AC}^{\boldsymbol{\tau}}\mathcal{CA}\,\mathbf{y}/\mathbf{y}], (\mathbf{H}, \mathbf{H'})) : \hat{\boldsymbol{\tau}}.\end{aligned}$$

Note that $\cdot ; \overline{\boldsymbol{\alpha}} ; \overline{\mathbf{x} : \boldsymbol{\tau'}} \vdash \mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t'} : \hat{\boldsymbol{\tau}}$ and

$$\cdot ; \overline{\boldsymbol{\alpha}} ; \overline{\mathbf{x} : \boldsymbol{\tau'}} \vdash {}^{\hat{\boldsymbol{\tau}}}\mathcal{CA}\,(\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathcal{AC}^{\exists \boldsymbol{\beta}.\boldsymbol{\tau}}\mathcal{CA}\,\hat{\mathbf{t}})\ \mathbf{in}\ \hat{\mathbf{t}}'[\mathcal{AC}^{\boldsymbol{\tau}}\mathcal{CA}\,\mathbf{y}/\mathbf{y}], (\mathbf{H}, \mathbf{H'})) : \hat{\boldsymbol{\tau}}.$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\boldsymbol{\alpha}}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x} : \boldsymbol{\tau}}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = \mathbf{t}\ \mathbf{in}\ \mathbf{t'})),\\ &\quad \rho_2(\gamma_2({}^{\hat{\boldsymbol{\tau}}}\mathcal{CA}\,(\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathcal{AC}^{\exists \boldsymbol{\beta}.\boldsymbol{\tau}}\mathcal{CA}\,\hat{\mathbf{t}})\ \mathbf{in}\ \hat{\mathbf{t}}'[\mathcal{AC}^{\boldsymbol{\tau}}\mathcal{CA}\,\mathbf{y}/\mathbf{y}], (\mathbf{H}, \mathbf{H'})))))\\ &= (W, \mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = \rho_1(\gamma_1(\mathbf{t}))\ \mathbf{in}\ \rho_1(\gamma_1(\mathbf{t'})),\\ &\qquad {}^{\rho_2(\hat{\boldsymbol{\tau}})}\mathcal{CA}\,(\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathcal{AC}^{\rho_2(\exists \boldsymbol{\beta}.\boldsymbol{\tau})}\mathcal{CA}\,\rho_2(\gamma_2(\hat{\mathbf{t}})))\ \mathbf{in}\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))[\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\mathcal{CA}\,\mathbf{y}/\mathbf{y}], (\mathbf{H}, \mathbf{H'})))\\ &\qquad\qquad \in \mathcal{E}[\![\hat{\boldsymbol{\tau}}]\!]\rho.\end{aligned}$$

By Lemma 8.14, it suffices to show that

$$\begin{aligned}&(W \boxplus (\{\cdot\}, (\mathbf{H}, \mathbf{H'})),\\ &\ \mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = \rho_1(\gamma_1(\mathbf{t}))\ \mathbf{in}\ \rho_1(\gamma_1(\mathbf{t'})),\\ &\ {}^{\rho_2(\hat{\boldsymbol{\tau}})}\mathcal{CA}\,(\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathcal{AC}^{\rho_2(\exists \boldsymbol{\beta}.\boldsymbol{\tau})}\mathcal{CA}\,\rho_2(\gamma_2(\hat{\mathbf{t}})))\ \mathbf{in}\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))[\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\mathcal{CA}\,\mathbf{y}/\mathbf{y}])) \in \mathcal{E}[\![\hat{\boldsymbol{\tau}}]\!]\rho.\end{aligned}$$

By Lemma 8.18 and our first hypothesis,

$$(W \boxplus (\{\cdot\}, (\mathbf{H}, \mathbf{H'})), \rho_1(\gamma_1(\mathbf{t})), {}^{\rho_2(\exists \boldsymbol{\beta}.\boldsymbol{\tau})}\mathcal{CA}\,\rho_2(\gamma_2(\hat{\mathbf{t}}))) \in \mathcal{E}[\![\exists \boldsymbol{\beta}.\boldsymbol{\tau}]\!]\rho.$$

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, (\mathbf{H}, \mathbf{H'}))$ and

$$(W', \mathbf{pack}\langle \boldsymbol{\tau_1}, \mathbf{v_1} \rangle\ \mathbf{as}\ \rho_1(\exists \boldsymbol{\beta}.\boldsymbol{\tau}), \mathbf{pack}\langle \boldsymbol{\tau_2}, \mathbf{v_2} \rangle\ \mathbf{as}\ \rho_2(\exists \boldsymbol{\beta}.\boldsymbol{\tau})) \in \mathcal{V}[\![\exists \boldsymbol{\beta}.\boldsymbol{\tau}]\!]\rho.$$

By Lemma 8.20, it suffices to show that

$$\begin{aligned}&(W', \mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathbf{pack}\langle \boldsymbol{\tau_1}, \mathbf{v_1} \rangle\ \mathbf{as}\ \rho_1(\exists \boldsymbol{\beta}.\boldsymbol{\tau}))\ \mathbf{in}\ \rho_1(\gamma_1(\mathbf{t'})),\\ &\quad {}^{\rho_2(\hat{\boldsymbol{\tau}})}\mathcal{CA}\,(\mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathcal{AC}^{\rho_2(\exists \boldsymbol{\beta}.\boldsymbol{\tau})}\ \mathbf{pack}\langle \boldsymbol{\tau_2}, \mathbf{v_2} \rangle)\ \mathbf{in}\ \rho_2(\gamma_2(\hat{\mathbf{t}}'))[\mathcal{AC}^{\rho_2(\boldsymbol{\tau})}\mathcal{CA}\,\mathbf{y}/\mathbf{y}])) \in \mathcal{E}[\![\hat{\boldsymbol{\tau}}]\!]\rho.\end{aligned}$$

By Lemma 8.3, for any $(M_1, M_2) : W$, there are some $\mathbf{v_2}$ and $\mathbf{v_2'}$ such that

$$\mathbf{AC}^{\rho_2(\boldsymbol{\tau}[\boldsymbol{\tau_2}/\boldsymbol{\beta}])}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2') \quad \text{and} \quad {}^{\rho_2(\boldsymbol{\tau}[\boldsymbol{\tau_2}/\boldsymbol{\beta}])}\mathbf{CA}(\mathbf{v_2}, M_2 \uplus M_2') = (\mathbf{v_2'}, M_2 \uplus M_2').$$

Note that

$$\langle M_1 \mid \mathbf{unpack}\,\langle \boldsymbol{\beta}, \mathbf{y} \rangle = (\mathbf{pack}\langle \boldsymbol{\tau_1}, \mathbf{v_1} \rangle\ \mathbf{as}\ \rho_1(\exists \boldsymbol{\beta}.\boldsymbol{\tau}))\ \mathbf{in}\ \rho_1(\gamma_1(\mathbf{t'})) \rangle \longmapsto \langle M_1 \mid \rho_1(\gamma_1(\mathbf{t'}))[\boldsymbol{\tau_1}/\boldsymbol{\beta}][\mathbf{v_1}/\mathbf{y}] \rangle$$

and

$$\langle M_2 \mid {}^{\rho_2(\hat{\tau})}\mathcal{CA}\,(\mathbf{unpack}\,\langle\beta,\mathbf{y}\rangle = (\mathcal{AC}^{\rho_2(\exists\beta.\tau)}\,\mathbf{pack}\langle\tau_2,\mathbf{v_2}\rangle)\,\mathbf{in}\,\rho_2(\gamma_2(\hat{\mathbf{t}}'))[\mathcal{AC}^{\rho_2(\tau)}\mathcal{CA}\,\mathbf{y}/\mathbf{y}])\rangle$$
$$\longmapsto^2 \langle M_2 \uplus M_2' \mid {}^{\rho_2(\hat{\tau})}\mathcal{CA}\,(\rho_2(\gamma_2(\hat{\mathbf{t}}'))[\tau_2{}^{\langle\mathcal{A}\rangle}/\beta][\mathcal{AC}^{\rho_2(\tau)}\mathcal{CA}\,\mathbf{v_2}/\mathbf{y}])\rangle.$$

By Lemma 8.15, it suffices to show that

$$(W' \boxplus (\{\cdot\}, M_2'), \rho_1(\gamma_1(\mathbf{t}'))[\tau_1/\beta][\mathbf{v_1}/\mathbf{y}], {}^{\rho_2(\hat{\tau})}\mathcal{CA}\,(\rho_2(\gamma_2(\hat{\mathbf{t}}'))[\tau_2{}^{\langle\mathcal{A}\rangle}/\beta][\mathcal{AC}^{\rho_2(\tau)}\mathcal{CA}\,\mathbf{v_2}/\mathbf{y}])) \in \mathcal{E}[\![\hat{\tau}]\!]\rho.$$

By Lemma 8.17, it suffices to show that

$$(W' \boxplus (\{\cdot\}, M_2'), \rho_1(\gamma_1(\mathbf{t}'))[\tau_1/\beta][\mathbf{v_1}/\mathbf{y}], {}^{\rho_2(\hat{\tau})}\mathcal{CA}\,(\rho_2(\gamma_2(\hat{\mathbf{t}}'))[\tau_2{}^{\langle\mathcal{A}\rangle}/\beta][\mathcal{AC}^{\rho_2(\tau)}\,\mathbf{v_2'}/\mathbf{y}])) \in \mathcal{E}[\![\hat{\tau}]\!]\rho.$$

By definition of $\mathcal{V}[\![\exists\beta.\tau]\!]\rho$, there is some VR $\in$ CValRel such that VR.$\tau_1 = \tau_1$, VR.$\tau_2 = \tau_2$, and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto \text{VR}]$. By boundary cancellation, $(W', \mathbf{v_1}, \mathbf{v_2'}) \in \mathcal{V}[\![\tau]\!]\rho[\beta \mapsto \text{VR}]$. Therefore $\rho[\beta \mapsto \text{VR}] \in \mathcal{D}[\![\overline{\alpha}, \beta]\!]$ and $(W', \gamma[\mathbf{y} \mapsto (\mathbf{v_1}, \mathbf{v_2'})]) \in \mathcal{G}[\![\overline{\mathbf{x}:\tau'}, \mathbf{y}:\tau]\!]\rho$. Hence we can apply our second hypothesis to get exactly this result. □

Lemma 11.27 (Fold)
If $\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{t} \approx {}^{\tau[\mu\alpha.\tau/\alpha]}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \tau[\mu\alpha.\tau/\alpha]$, then

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{fold}_{\mu\alpha.\tau}\,\mathbf{t} \approx {}^{\mu\alpha.\tau}\mathcal{CA}\,((\mathbf{fold}_{\mu\alpha.\tau\,\mathcal{A}}\,\mathbf{t})[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \mu\alpha.\tau.$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{fold}_{\mu\beta.\tau}\,\mathbf{t} \approx {}^{\mu\beta.\tau}\mathcal{CA}\,(\mathbf{fold}_{\mu\beta.\tau\langle\mathcal{A}\rangle}\,\mathcal{AC}^{\tau[\mu\beta.\tau/\beta]}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}) : \mu\beta.\tau.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{fold}_{\mu\beta.\tau}\,\mathbf{t} : \mu\beta.\tau$ and

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash {}^{\mu\beta.\tau}\mathcal{CA}\,(\mathbf{fold}_{\mu\beta.\tau\langle\mathcal{A}\rangle}\,\mathcal{AC}^{\tau[\mu\beta.\tau/\beta]}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}) : \mu\beta.\tau.$$

Let $W \in \text{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x}:\tau}]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\mathbf{fold}_{\mu\beta.\tau}\,\mathbf{t})), \rho_2(\gamma_2({}^{\mu\beta.\tau}\mathcal{CA}\,(\mathbf{fold}_{\mu\beta.\tau\langle\mathcal{A}\rangle}\,\mathcal{AC}^{\tau[\mu\beta.\tau/\beta]}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}))))$$
$$= (W, \mathbf{fold}_{\rho_1(\mu\beta.\tau)}\,\rho_1(\gamma_1(\mathbf{t})),$$
$${}^{\rho_2(\mu\beta.\tau)}\mathcal{CA}\,(\mathbf{fold}_{\rho_2(\mu\beta.\tau\langle\mathcal{A}\rangle)}\,\mathcal{AC}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{CA}\,(\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]))), \mathbf{H}))$$
$$\in \mathcal{E}[\![\mu\beta.\tau]\!]\rho.$$

By Lemma 8.15, it suffices to show that

$$(W \boxplus (\{\cdot\}, \mathbf{H}), \mathbf{fold}_{\rho_1(\mu\beta.\tau)}\,\rho_1(\gamma_1(\mathbf{t})),$$
$${}^{\rho_2(\mu\beta.\tau)}\mathcal{CA}\,(\mathbf{fold}_{\rho_2(\mu\beta.\tau\langle\mathcal{A}\rangle)}\,\mathcal{AC}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{CA}\,(\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}])))))$$
$$\in \mathcal{E}[\![\mu\beta.\tau]\!]\rho.$$

By Lemma 8.18 and our hypothesis,

$$(W \boxplus (\{\cdot\}, \mathbf{H}), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\tau[\mu\beta.\tau/\beta]}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}])))) \in \mathcal{E}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho.$$

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, \mathbf{H})$ and $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \mathbf{fold}_{\rho_1(\mu\beta.\tau)}\,\mathbf{v_1}, {}^{\rho_2(\mu\beta.\tau)}\mathcal{CA}\,\mathbf{fold}_{\rho_2(\mu\beta.\tau\langle\mathcal{A}\rangle)}\,\mathcal{AC}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\,\mathbf{v_2}) \in \mathcal{E}[\![\mu\beta.\tau]\!]\rho.$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\mathbf{v_2}$ and $\mathbf{v_2'}$ such that

$$\mathbf{AC}^{\rho_2(\tau[\mu\alpha.\tau/\beta])}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2') \quad \text{and} \quad {}^{\rho_2(\tau[\mu\alpha.\tau/\beta])}\mathbf{CA}(\mathbf{v_2}, M_2 \uplus M_2') = (\mathbf{v_2'}, M_2 \uplus M_2').$$

By the operational semantics,

$$\langle M_2 \mid {}^{\rho_2(\mu\beta.\tau)}\mathcal{CA}\,\mathbf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathcal{AC}^{\rho_2(\tau[\mu\alpha.\tau/\beta])}\,\mathbf{v_2}\rangle \longmapsto^2 \langle M_2 \uplus M_2' \mid \mathbf{fold}_{\rho_2(\mu\beta.\tau^{\langle\mathcal{A}\rangle})}\,\mathbf{v_2'}\rangle.$$

Thus, by Lemma 8.15 and Lemma 8.9, it suffices to show that

$$(W' \boxplus (\{\cdot\}, M_2'), \mathbf{fold}_{\rho_1(\mu\beta.\tau)}\,\mathbf{v_1}, \mathbf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathbf{v_2'}) \in \mathcal{V}[\![\mu\beta.\tau]\!]\rho.$$

This follows from our hypothesis that $(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau[\mu\beta.\tau/\beta]]\!]$, by monotonicity and boundary cancellation. □

Lemma 11.28 (Unfold)
If $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t} \approx {}^{\mu\alpha.\tau}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \mu\alpha.\tau$, then

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{unfold}\,\mathbf{t} \approx {}^{\tau[\mu\alpha.\tau/\alpha]}\mathcal{CA}\,((\mathbf{unfold}\,\mathbf{t})[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \tau[\mu\alpha.\tau/\alpha].$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{unfold}\,\mathbf{t} \approx {}^{\tau[\mu\beta.\tau/\beta]}\mathcal{CA}\,(\mathbf{unfold}\,\mathcal{AC}^{\mu\beta.\tau}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}) : \tau[\mu\beta.\tau/\beta].$$

Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{unfold}\,\mathbf{t} : \tau[\mu\beta.\tau/\beta]$ and

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash {}^{\tau[\mu\beta.\tau/\beta]}\mathcal{CA}\,(\mathbf{unfold}\,\mathcal{AC}^{\mu\beta.\tau}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}) : \tau[\mu\beta.\tau/\beta].$$

Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x} : \tau}]\!]\rho$. We need to show that

$$\begin{aligned}(W, \rho_1(\gamma_1(\mathbf{unfold}\,\mathbf{t})), \rho_2(\gamma_2({}^{\tau[\mu\beta.\tau/\beta]}\mathcal{CA}\,(\mathbf{unfold}\,\mathcal{AC}^{\mu\beta.\tau}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}))))\\ = (W, \mathbf{unfold}\,\rho_1(\gamma_1(\mathbf{t})),\\ {}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{CA}\,(\mathbf{unfold}\,\mathcal{AC}^{\rho_2(\mu\beta.\tau)}\mathcal{CA}\,(\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]))), \mathbf{H}))\\ \in \mathcal{E}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho.\end{aligned}$$

By Lemma 8.14, it suffices to show that

$$\begin{aligned}(W \boxplus (\{\cdot\}, \mathbf{H}), \mathbf{unfold}\,\rho_1(\gamma_1(\mathbf{t})),\\ {}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{CA}\,(\mathbf{unfold}\,\mathcal{AC}^{\rho_2(\mu\beta.\tau)}\mathcal{CA}\,(\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}])))))\\ \in \mathcal{E}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho.\end{aligned}$$

By Lemma 8.18 and our hypothesis,

$$(W \boxplus (\{\cdot\}, \mathbf{H}), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\mu\beta.\tau}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}])))) \in \mathcal{E}[\![\mu\beta.\tau]\!]\rho.$$

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, \mathbf{H})$ and $(W', \mathbf{fold}_{\rho_1(\mu\beta.\tau)}\,\mathbf{v_1}, \mathbf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathbf{v_2}) \in \mathcal{V}[\![\mu\beta.\tau]\!]\rho$. By Lemma 8.20, it suffices to show that

$$\begin{aligned}(W', \mathbf{unfold}\,(\mathbf{fold}_{\rho_1(\mu\beta.\tau)}\,\mathbf{v_1}),\\ {}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{CA}\,\mathbf{unfold}\,\mathcal{AC}^{\rho_2(\mu\beta.\tau)}\,\mathbf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathbf{v_2}) \in \mathcal{E}[\![\tau[\mu\beta.\tau/\beta]]\!]\rho.\end{aligned}$$

By Lemma 8.3, for any $(M_1, M_2) : W'$, there are some $\mathbf{v_2}$ and $\mathbf{v_2'}$ such that

$$\mathbf{AC}^{\rho_2(\mu\beta.\tau)}(\mathbf{v_2}, M_2) = (\mathbf{v_2}, M_2 \uplus M_2') \quad \text{and} \quad {}^{\rho_2(\mu\beta.\tau)}\mathbf{CA}(\mathbf{v_2}, M_2 \uplus M_2') = (\mathbf{v_2'}, M_2 \uplus M_2').$$

By the operational semantics,

$$\langle M_2 \mid {}^{\rho_2(\tau[\mu\beta.\tau/\beta])}\mathcal{CA}\,\mathbf{unfold}\,\mathcal{AC}^{\rho_2(\mu\beta.\tau)}\,\mathbf{fold}_{\rho_2(\mu\beta.\tau)}\,\mathbf{v_2}\rangle \longmapsto^3 \langle M_2 \uplus M_2' \mid \mathbf{v_2'}\rangle.$$

The result follows by Lemma 8.15, Lemma 8.9, and boundary cancellation. □

Lemma 11.29 (Projection)
If $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t} \approx {}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \langle\overline{\tau}\rangle$, then

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \pi_\mathbf{i}(\mathbf{t}) \approx {}^{\tau_\mathbf{i}}\mathcal{CA}\,(\mathbf{read[i]}\,\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \tau_\mathbf{i}.$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \pi_\mathbf{i}(\mathbf{t}) \approx {}^{\tau_\mathbf{i}}\mathcal{CA}\,(\mathbf{read[i]}\,\mathcal{AC}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}) : \tau_\mathbf{i}.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \pi_\mathbf{i}(\mathbf{t}) : \tau_\mathbf{i}$ and $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash {}^{\tau_\mathbf{i}}\mathcal{CA}\,(\mathbf{read[i]}\,\mathcal{AC}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}) : \tau_\mathbf{i}$.
Let $W \in \mathrm{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x} : \tau}]\!]\rho$. We need to show that

$$\begin{aligned}&(W, \rho_1(\gamma_1(\pi_\mathbf{i}(\mathbf{t}))), \rho_2(\gamma_2({}^{\tau_\mathbf{i}}\mathcal{CA}\,(\mathbf{read[i]}\,\mathcal{AC}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]), \mathbf{H}))))\\ &\quad = (W, \pi_\mathbf{i}(\rho_1(\gamma_1(\mathbf{t}))), {}^{\rho_2(\tau_\mathbf{i})}\mathcal{CA}\,(\mathbf{read[i]}\,\mathcal{AC}^{\rho_2(\langle\overline{\tau}\rangle)}\mathcal{CA}\,(\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]))), \mathbf{H})) \in \mathcal{E}[\![\tau_\mathbf{i}]\!]\rho.\end{aligned}$$

By Lemma 8.14, it suffices to show that

$$(W \boxplus (\{\cdot\}, \mathbf{H}), \pi_\mathbf{i}(\rho_1(\gamma_1(\mathbf{t}))), {}^{\rho_2(\tau_\mathbf{i})}\mathcal{CA}\,(\mathbf{read[i]}\,\mathcal{AC}^{\rho_2(\langle\overline{\tau}\rangle)}\mathcal{CA}\,(\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}]))))) \in \mathcal{E}[\![\tau_\mathbf{i}]\!]\rho.$$

By our hypothesis and Lemma 8.18,

$$(W \boxplus (\{\cdot\}, \mathbf{H}), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}])))) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

Let $W' \sqsupseteq W \boxplus (\{\cdot\}, \mathbf{H})$ and $(W', \langle\overline{\mathbf{v_1}}\rangle, \langle\overline{\mathbf{v_2}}\rangle) \in \mathcal{V}[\![\langle\overline{\tau}\rangle]\!]\rho$. By Lemma 8.20, it suffices to show that

$$(W', \pi_\mathbf{i}((\langle\overline{\mathbf{v_1}}\rangle)), {}^{\rho_2(\tau_\mathbf{i})}\mathcal{CA}\,\mathbf{read[i]}\,\mathcal{AC}^{\rho_2(\langle\overline{\tau}\rangle)}\,\langle\overline{\mathbf{v_2}}\rangle) \in \mathcal{E}[\![\tau_\mathbf{i}]\!]\rho.$$

We have this by Lemma 8.15, Lemma 8.9, and boundary cancellation. □

Lemma 11.30 (Tuple)
If $\cdot \vdash \overline{\mathbf{H}} : \Psi$ and $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \mathbf{t} \approx {}^{\tau}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \mathbf{H}) : \tau$, then

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \langle\overline{\mathbf{t}}\rangle \approx {}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{balloc}\,\langle\overline{\mathbf{t}}\rangle[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}], \overline{\mathbf{H}}) : \langle\overline{\tau}\rangle.$$

Proof

By Lemma 11.2, it suffices to show that

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \langle\overline{\mathbf{t}}\rangle \approx {}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{balloc}\,\langle\overline{\mathcal{AC}^{\tau}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}])}\rangle, \overline{\mathbf{H}}) : \langle\overline{\tau}\rangle.$$

Note that $\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash \langle\overline{\mathbf{t}}\rangle : \langle\overline{\tau}\rangle$ and

$$\cdot; \overline{\alpha}; \overline{\mathbf{x} : \tau'} \vdash {}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{balloc}\,\langle\overline{\mathcal{AC}^{\langle\overline{\tau}\rangle}\mathcal{CA}\,(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\,\mathbf{x}/\mathbf{x}}])}\rangle, \overline{\mathbf{H}}) : \langle\overline{\tau}\rangle.$$

Let $W \in \text{World}$, $\rho \in \mathcal{D}[\![\overline{\alpha}]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\overline{\mathbf{x}:\tau}]\!]\rho$. We need to show that

$$(W, \rho_1(\gamma_1(\langle \overline{\mathbf{t}} \rangle)), \rho_2(\gamma_2(\overline{{}^{\langle\tau\rangle}\mathcal{CA}\ (\mathbf{balloc}\ \langle \mathcal{AC}^{\tau}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])\rangle, \overline{\mathbf{H}})}))))$$
$$= (W, \langle \overline{\rho_1(\gamma_1(\mathbf{t}))} \rangle, \overline{{}^{\rho_2(\langle\tau\rangle)}\mathcal{CA}\ (\mathbf{balloc}\ \langle \mathcal{AC}^{\rho_2(\tau)}\mathcal{CA}\ (\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}]))))\rangle, \overline{\mathbf{H}})}) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

By Lemma 8.14, it suffices to show that

$$(W \uplus (\{\cdot\}, \overline{\mathbf{H}}), \langle \overline{\rho_1(\gamma_1(\mathbf{t}))} \rangle, \overline{{}^{\rho_2(\langle\tau\rangle)}\mathcal{CA}\ (\mathbf{balloc}\ \langle \mathcal{AC}^{\rho_2(\tau)}\mathcal{CA}\ (\rho_2(\gamma_2(\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}]))))\rangle}) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

By our hypothesis,

$$\overline{(W \uplus (\{\cdot\}, \overline{\mathbf{H}}), \rho_1(\gamma_1(\mathbf{t})), \rho_2(\gamma_2({}^{\tau}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}])))) \in \mathcal{E}[\![\tau]\!]\rho}.$$

Let $W' \sqsupseteq W \uplus (\{\cdot\}, \overline{\mathbf{H}})$ and $\overline{(W', \mathbf{v_1}, \mathbf{v_2}) \in \mathcal{V}[\![\tau]\!]\rho}$. By Lemma 8.20, it suffices to show that

$$(W', \langle \overline{\mathbf{v_1}} \rangle, {}^{\rho_2(\langle\tau\rangle)}\mathcal{CA}\ \mathbf{balloc}\ \langle \overline{\mathcal{AC}^{\rho_2(\tau)}\ \mathbf{v_2}} \rangle) \in \mathcal{E}[\![\langle\overline{\tau}\rangle]\!]\rho.$$

We have this by Lemma 8.15, Lemma 8.9, and boundary cancellation. □

Theorem 11.31 (Allocation is Semantics-Preserving)
If $\overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{e}:\tau \rightsquigarrow (\mathbf{t}, \mathbf{H}:\Psi)$, then

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'} \vdash \mathbf{e} \approx {}^{\tau}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}]\ [\overline{\mathcal{AC}^{\tau'}\ \mathbf{x}/\mathbf{x}}], \mathbf{H}):\tau.$$

Proof

By induction on the compiler judgment, using the preceding lemmas. □

11.3 Multi-Pass Correctness

Corollary 11.32 (FCA Compiler Correctness)
If $\overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e}:\tau \rightsquigarrow \mathbf{e} \rightsquigarrow \mathbf{e}$, then

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e} \approx^{ctx} {}^{\tau}\mathcal{FCA}\ (\mathbf{e}[\overline{\lceil\alpha\rceil/\alpha}][\overline{\mathcal{AC}\mathcal{F}^{\tau'}\ \mathsf{x}/\mathsf{x}}]):\tau.$$

Proof

Let $\mathbf{e} = (\mathbf{t}, \mathbf{H})$. By Theorem 11.31, we have

$$\cdot; \overline{\alpha}; \overline{\mathbf{x}:\tau'^{\mathcal{C}}} \vdash \mathbf{e} \approx {}^{\tau}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}]\ [\overline{\mathcal{AC}^{\tau'^{\mathcal{C}}}\ \mathbf{x}/\mathbf{x}}], \mathbf{H}):\tau^{\mathcal{C}}.$$

By applying the substitutions of $\overline{[\lceil\alpha\rceil/\alpha]}$ and $\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]}$, we get

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathbf{e}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]} \approx {}^{\tau}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}]\ [\overline{\mathcal{AC}^{\tau'^{\langle\mathcal{C}\rangle}}\ (\mathcal{CF}^{\tau'}\ \mathsf{x})/\mathsf{x}}], \mathbf{H}):\tau^{\langle\mathcal{C}\rangle}.$$

Applying Lemma 10.22, we have

$$\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash {}^{\tau}\mathcal{FC}\ \mathbf{e}\overline{[\lceil\alpha\rceil/\alpha]}\overline{[\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}]} \approx {}^{\tau}\mathcal{FC}\ {}^{\tau}\mathcal{CA}\ (\mathbf{t}[\overline{\lceil\alpha\rceil/\alpha}]\ [\overline{\mathcal{AC}^{\tau'^{\langle\mathcal{C}\rangle}}\ (\mathcal{CF}^{\tau'}\ \mathsf{x})/\mathsf{x}}], \mathbf{H}):\tau.$$

Finally, Theorem 11.16 tells us that $\cdot; \overline{\alpha}; \overline{\mathsf{x}:\tau'} \vdash \mathsf{e} \approx {}^{\tau}\mathcal{FC}\ (\mathbf{e}[\overline{\lceil\alpha\rceil/\alpha}]\ [\overline{\mathcal{CF}^{\tau'}\ \mathsf{x}/\mathsf{x}}]):\tau$, so by transitivity and soundness, we have the result. □

12 Examples

12.1 Example of Linking

We can use our compiler correctness theorem to make statements about linking with arbitrary A components, as long as they have translation type. In this section, we present an example showing how our framework allows linking with A components that both can and cannot be expressed in F.

Consider the component

$$\mathsf{e} = (\lambda[]\,(\mathsf{g}:\forall[].(\mathsf{unit})\to\mathsf{int}).(\mathsf{g}\;[]\;())*(\mathsf{g}\;[]\;()))\;[]\;\mathsf{x}.$$

Clearly, we have $\cdot;\cdot;(\mathsf{x}:\mathsf{unit}\to\mathsf{int})\vdash\mathsf{e}:\mathsf{int}$. In F alone, only divergent or constant functions can have type $\forall[].(\mathsf{unit})\to\mathsf{int}$, but if we are compiling to A before linking, g could be instantiated with something that makes use of A's mutable references.

If we compile e to language C by $\cdot;\mathsf{x}:\forall[].(\mathsf{unit})\to\mathsf{int}\vdash\mathsf{e}:\mathsf{int}\rightsquigarrow\mathbf{e}$, we get

$$\begin{aligned}\mathbf{e} = \mathbf{unpack}\,\langle\beta,\mathbf{z}\rangle = \mathbf{pack}\langle\langle\rangle,&\langle\boldsymbol{\lambda}[]\,(\mathbf{z}:\langle\rangle,\mathbf{g}:\exists\alpha.\langle\forall[].(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle).\mathbf{e_{body}},\langle\rangle\rangle\rangle\\ &\mathbf{as}\;\exists\beta.\langle\forall[].(\beta,\exists\alpha.\langle\forall[].(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle)\to\mathbf{int},\beta\rangle,\\ \mathbf{in}\;\pi_1(\mathbf{z})\;[]\;\pi_2(\mathbf{z}),\mathbf{x}&\end{aligned}$$

where

$$\mathbf{e_{body}} = ((\mathbf{unpack}\,\langle\beta,\mathbf{z}\rangle = \mathbf{g}\;\mathbf{in}\;\pi_1(\mathbf{z})\;[]\;\pi_2(\mathbf{z}),())*(\mathbf{unpack}\,\langle\beta,\mathbf{z}\rangle = \mathbf{g}\;\mathbf{in}\;\pi_1(\mathbf{z})\;[]\;\pi_2(\mathbf{z}),())).$$

If we compile $\mathbf{e}$ to language A by $\cdot;\cdot\vdash\mathbf{e}:\exists\beta.\langle\forall[].(\beta,\exists\alpha.\langle\forall[].(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle)\to\mathbf{int},\beta\rangle\rightsquigarrow(\mathbf{t},\mathbf{H}:\Psi)$, we get

$$\begin{aligned}\mathbf{t} = \mathbf{unpack}\,\langle\beta,\mathbf{z}\rangle &= \mathbf{pack}\langle\mathbf{box}\,\langle\rangle,\mathbf{balloc}\,\langle\ell,\mathbf{balloc}\,\langle\rangle\rangle\rangle\\ &\quad\mathbf{as}\;\exists\beta.\mathbf{box}\,\langle\forall[].(\beta,\exists\alpha.\mathbf{box}\,\langle\mathbf{box}\,\forall[].(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle)\to\mathbf{int},\beta\rangle\\ \mathbf{in}\;\pi_1(\mathbf{z})\;[]\;\pi_1(\mathbf{z}),\mathbf{x}&\\ \mathbf{H} = \{\ell\mapsto\boldsymbol{\lambda}[]\,(\mathbf{z}:\mathbf{box}\,\langle\rangle,\mathbf{g}:\exists\alpha.\mathbf{box}\,\langle\mathbf{box}\,\forall[].(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle).&\\ ((\mathbf{unpack}\,\langle\beta,\mathbf{z}\rangle = \mathbf{g}\;\mathbf{in}\;(\mathbf{read}[1]\,\mathbf{z})\;[]\;\mathbf{read}[2]\,\mathbf{z},())*&\\ (\mathbf{unpack}\,\langle\beta,\mathbf{z}\rangle = \mathbf{g}\;\mathbf{in}\;(\mathbf{read}[1]\,\mathbf{z})\;[]\;\mathbf{read}[2]\,\mathbf{z},()))\}.&\\ \Psi = \{\ell:\forall[].(\mathbf{box}\,\langle\rangle,\exists\alpha.\mathbf{box}\,\langle\mathbf{box}\,\forall[].(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle)\to\mathbf{int}\}&\\ \mathbf{e} = (\mathbf{t},\mathbf{H}).&\end{aligned}$$

By compiler correctness, we know that

$$\cdot;\cdot;(\mathsf{x}:\mathsf{unit}\to\mathsf{int})\vdash\mathsf{e}\approx^{ctx}{}^{\mathsf{int}}\mathcal{FCA}\,(\mathsf{e}[\mathcal{ACF}^{\mathsf{unit}\to\mathsf{int}}\,\mathsf{x}/\mathsf{x}]):\mathsf{int}.$$

Equivalently,

$$\cdot;\cdot;(\mathbf{x}:\tau)\vdash\mathcal{ACF}^{\mathsf{int}}\,(\mathsf{e}[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}\,\mathsf{x}/\mathsf{x}])\approx^{ctx}\mathbf{e}:\mathbf{int},$$

where

$$\tau = \mathsf{unit}\to\mathsf{int}^{\langle\mathcal{C}\rangle\langle\mathcal{A}\rangle} = \exists\alpha.\mathbf{box}\,\langle\mathbf{box}\,(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle.$$

Suppose we want to instantiate x with the following A component, which creates a function that uses a mutable reference to return the number of times it has been called:

$$\begin{aligned}\mathbf{e'} = (&\mathbf{pack}\langle\mathbf{ref}\;\mathbf{int},\mathbf{balloc}\,\langle\ell,\mathbf{ralloc}\,\langle\mathbf{0}\rangle\rangle\rangle\;\mathbf{as}\;\exists\alpha.\mathbf{box}\,\langle\mathbf{box}\,\forall[].(\alpha,\mathbf{unit})\to\mathbf{int},\alpha\rangle,\\ &\{\ell\mapsto\boldsymbol{\lambda}[]\,(\mathbf{x}:\mathbf{ref}\;\mathbf{int},\mathbf{z}:\mathbf{unit}).\mathbf{let}\;\mathbf{y}=\mathbf{read}[1]\,\mathbf{x}\;\mathbf{in}\;\mathbf{let}\;\mathbf{z}=\mathbf{write}\,\mathbf{x}\,[1]\leftarrow\mathbf{y}+\mathbf{1}\;\mathbf{in}\;\mathbf{y}+\mathbf{1}\}),\end{aligned}$$

where $\mathbf{let}\,\mathbf{x}=\mathbf{t}\;\mathbf{in}\;\mathbf{t'}\stackrel{\text{def}}{=}\mathbf{unpack}\,\langle\_,\mathbf{x}\rangle=\mathbf{pack}\langle\_,\mathbf{t}\rangle\;\mathbf{in}\;\mathbf{t'}$. We would then have

$$\cdot;\cdot;\cdot\vdash\mathcal{ACF}^{\mathsf{int}}\,(\mathsf{e}[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}\,\mathbf{e'}/\mathsf{x}])\approx^{ctx}\mathbf{e}[\mathbf{e'}/\mathsf{x}]:\mathbf{int}.$$

The right-hand side of this equivalence is exactly the pure-A program that we would ultimately run, and the left-hand side is an FCA program that models it. Note that on either side of the equation, the function exported by $\mathsf{e'}$ will be applied to the unit value twice, and it will return $\mathsf{1}$ the first time and $\mathsf{2}$ the second time. An F function could not exhibit this behavior. This demonstrates how our framework allows for linking with components that are not expressible in the source language.

If we want instead to link with a different A component $\hat{\mathsf{e}}$ that was compiled from an F component $\hat{\mathsf{e}}$, we can still make the statement

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{int}}\,(\mathsf{e}[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}\ \hat{\mathsf{e}}/\mathsf{x}]) \approx^{ctx} \mathsf{e}[\hat{\mathsf{e}}/\mathsf{x}] : \mathsf{int}.$$

But we can simplify this statement using our additional knowledge of $\hat{\mathsf{e}}$, as long as we know

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{unit}\to\mathsf{int}}\ \hat{\mathsf{e}} \approx^{ctx} \hat{\mathsf{e}} : \tau.$$

If $\hat{\mathsf{e}}$ was compiled to $\hat{\mathsf{e}}$ with our compiler, this is exactly what we have from our compiler correctness theorem. If $\hat{\mathsf{e}}$ was compiled by some other compiler, we would need some other way to get a proof of this fact. From the equivalence above, we can infer that

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{int}}\,(\mathsf{e}[{}^{\mathsf{unit}\to\mathsf{int}}\mathcal{FCA}\,(\mathcal{ACF}^{\mathsf{unit}\to\mathsf{int}}\ \hat{\mathsf{e}})/\mathsf{x}]) \approx^{ctx} \mathsf{e}[\hat{\mathsf{e}}/\mathsf{x}] : \mathsf{int}.$$

Applying boundary cancellation yields

$$\cdot;\cdot;\cdot \vdash \mathcal{ACF}^{\mathsf{int}}\,(\mathsf{e}[\hat{\mathsf{e}}/\mathsf{x}]) \approx^{ctx} \mathsf{e}[\hat{\mathsf{e}}/\mathsf{x}] : \mathsf{int}.$$

Now we are essentially equating the pure-A program with a pure-F program, since the only multi-language element in this statement is the integer boundary at the outermost level, which merely converts an n to n. This demonstrates that when we do have source-language equivalents for all our target-level components, our framework allows us to model target-level linking with source-level linking.

12.2 Example of Using the Logical Relation to Prove Contextual Equivalences

In this section, we give a simple example of how our FCA logical relation can be used to prove contextual equivalences. Other than our notion of admissible relations, which are not generally hard to construct in practice, these proofs proceed as similar proofs using a logical relations model normally would.

Lemma 12.1
Let

$$\mathsf{e}_1 = \mathsf{pack}\langle\mathsf{int}, \langle 3, \lambda[]\,(\mathsf{x}:\mathsf{int}).\mathsf{x}+2\rangle\rangle\ \mathsf{as}\ \exists\alpha.\langle\alpha, \forall[].(\alpha)\to\mathsf{int}\rangle$$

and

$$\mathsf{e}_2 = \mathsf{pack}\langle\mathsf{int}, \langle 5, \lambda[]\,(\mathsf{x}:\mathsf{int}).\mathsf{x}\rangle\rangle\ \mathsf{as}\ \exists\alpha.\langle\alpha, \forall[].(\alpha)\to\mathsf{int}\rangle.$$

Then $\cdot;\cdot;\cdot \vdash \mathsf{e}_1 \approx^{ctx} \mathsf{e}_2 : \exists\alpha.\langle\alpha, \forall[].(\alpha)\to\mathsf{int}\rangle$.

Proof

Let $W \in \text{World}$. We need to show that $(W, \mathsf{e}_1, \mathsf{e}_2) \in \mathcal{E}[\![\exists\alpha.\langle\alpha, \forall[].(\alpha)\to\mathsf{int}\rangle]\!]\emptyset$. By Lemma 8.9, it suffices to show that

$$(W, \mathsf{e}_1, \mathsf{e}_2) \in \mathcal{V}[\![\exists\alpha.\langle\alpha, \forall[].(\alpha)\to\mathsf{int}\rangle]\!]\emptyset.$$

Let $\varphi_v^F = \{(W', 3, 5) \mid W' \sqsupseteq W\}$, $\varphi_v^C = \{(W', \mathbf{3}, \mathbf{5}) \mid W' \sqsupseteq W\}$, and $\varphi_v^A = \{(W', \mathbf{3}, \mathbf{5}) \mid W' \sqsupseteq W\}$. Let

$$\text{VR} = (\mathsf{int}, \mathsf{int}, \varphi_v^F, \varphi_v^C, \varphi_v^A).$$

Note that $\text{VR} \in \text{FValRel}$. By definition of $\mathcal{V}[\![\exists\alpha.\langle\alpha, \forall[].(\alpha)\to\mathsf{int}\rangle]\!]\emptyset$, it suffices to show that

$$(W, \langle 3, \lambda[]\,(\mathsf{x}:\mathsf{int}).\mathsf{x}+2\rangle, \langle 5, \lambda[]\,(\mathsf{x}:\mathsf{int}).\mathsf{x}\rangle) \in \mathcal{V}[\![\langle\alpha, \forall[].(\alpha)\to\mathsf{int}\rangle]\!]\emptyset[\alpha \mapsto \text{VR}].$$

Clearly, $(W, 3, 5) \in \mathcal{V}[\![\alpha]\!]\emptyset[\alpha \mapsto \text{VR}]$, so it remains to show that

$$(W, \lambda[]\,(\mathsf{x}:\mathsf{int}).\mathsf{x}+2, \lambda[]\,(\mathsf{x}:\mathsf{int}).\mathsf{x}) \in \mathcal{V}[\![\forall[].(\alpha)\to\mathsf{int}]\!]\emptyset[\alpha \mapsto \text{VR}].$$

Let $W' \sqsupseteq W$ and $(W', \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\alpha]\!]\emptyset[\alpha \mapsto \mathrm{VR}]$. By definition of VR.$\varphi_v^F$, $\mathsf{v}_1 = 3$ and $\mathsf{v}_2 = 5$. We need to show that

$$(W', (\lambda[]\,(\mathsf{x}\colon \mathsf{int}).\mathsf{x} + 2)\;[]\;3, (\lambda[]\,(\mathsf{x}\colon \mathsf{int}).\mathsf{x})\;[]\;5) \in \mathcal{E}[\![\mathsf{int}]\!]\emptyset[\alpha \mapsto \mathrm{VR}].$$

But this follows easily from Lemma 8.15 and Lemma 8.9. □

As the example shows, building admissible relations for base types is easy. By extension, it is also easy to build admissible relations for types where repeated translation produces a small number of values, including tuple, existential, and recursive types. Since repeatedly translating function types adds more and more layers of wrapping boundaries, it is more difficult to build relations that satisfy boundary cancellation and bridge properties at types that involve functions. However, this can be done by explicitly closing the desired relation over all translations of its values.

To close off a relation $\mathrm{VR} = (\tau_1, \tau_2, \varphi_v^F, \varphi_v^C, \varphi_v^A)$ over all translations, we would require that for any initial value v desired to be in φ_v^F (on either side), the desired φ_v^F, φ_v^C, and φ_v^A in the final VR must also contain all the values that result from sequences of translations that match the following regular expressions:

- In φ_v^F: $(\mathcal{FC}(\mathcal{CAAC})^*\mathcal{CF})^*(\mathsf{v})$
- In φ_v^C: $((\mathcal{CAAC})^*(\mathcal{CFFC})^*)^*\mathcal{CF}(\mathsf{v})$
- In φ_v^A: $(\mathcal{AC}(\mathcal{CFFC})^*\mathcal{CA})^*\mathcal{AC}(\mathcal{CFFC})^*\mathcal{CF}(\mathsf{v})$

The necessary sets of translations can be constructed similarly for relations that need particular C and A values.