Technical Report MPI-SWS-2012-002

The Transitive Composability of Relation Transition Systems

Chung-Kil Hur Georg Neis Derek Dreyer Viktor Vafeiadis

Max Planck Institute for Software Systems (MPI-SWS)
Kaiserslautern and Saarbrücken, Germany
E-mail: {gil, neis, dreyer, viktor}@mpi-sws.org

May 2012

Abstract

Relation Transition Systems (RTSs) have recently been proposed as a foundation for reasoning effectively about program equivalence in higher-order imperative languages like ML. RTSs fruitfully synthesize the coinductive style of bisimulation-based methods with the treatment of local state in recent work on step-indexed Kripke logical relations (SKLRs). Like SKLRs, RTSs are designed to have the potential to scale to *inter-language reasoning*; but unlike SKLRs, RTS proofs are also *transitively composable*, which is of critical importance for applications such as multi-stage verified compilation.

In a POPL'12 paper [6], we presented the first RTS model for an ML-like core language, $\mathsf{F}^{\mu!}$, supporting higher-order functions, recursive types, abstract types, and general mutable references, and we proved soundness of the model w.r.t. contextual equivalence. In addition, we briefly sketched the proof that RTSs are transitively composable, but our proof only covered a restricted fragment of the language/model omitting abstract types and mutable state. Here, we present the transitivity proof for the full RTS model of the full $\mathsf{F}^{\mu!}$ language. The proof is highly intricate, requiring a number of technical innovations. We have mechanized all our results in Coq.

CONTENTS

I Introduction 3

II The Language $\mathsf{F}^{\mu!}$ 3

III Relation Transition Systems 4

IV Structure of the Transitivity Proof 6

V First Part: Constructing the Full World W 7
- V-A High-Level Explanation . . . 7
- V-B The Gory Details . . . 8

VI Second Part: Constructing the Corresponding Local World w 9
- VI-A World Isomorphisms . . . 10
- VI-B Defining w . . . 10
- VI-C Showing w's Stability . . . 11
- VI-D Proving W and $w{\uparrow}$ Isomorphic . . . 12

VII Conclusion 12

References 12

Appendix 13
- A Language . . . 13
  - A1 Syntax . . . 13
  - A2 Dynamic Semantics . . . 13
  - A3 Static Semantics . . . 13
  - A4 Contextual Equivalence . . . 15
- B Model . . . 16
- C Metatheory . . . 19
  - C1 Basic Properties . . . 19
  - C2 Compatibility . . . 26
  - C3 Soundness . . . 35
  - C4 Symmetry . . . 35
- D Examples . . . 38
  - D1 World Generator . . . 38
  - D2 Substitutivity . . . 40
  - D3 Expansion . . . 40
  - D4 Beta Law . . . 41
  - D5 Awkward Example . . . 41
  - D6 Well-Bracketed State Change . . . 42
  - D7 Twin Abstraction . . . 44
- E Weak Isomorphism Theorem . . . 46
  - E1 Weak Isomorphisms . . . 46
  - E2 Global Knowledge Constructions . . . 46
  - E3 Category of Worlds . . . 47
  - E4 Isomorphism Theorem . . . 48
  - E5 Examples . . . 50
- F Transitivity . . . 51
  - F1 Constructing a Full World That Relates e_1 and e_3 . . . 51
  - F2 Constructing an Isomorphic Lifted World . . . 58

I. Introduction

A longstanding problem in semantics is to find effective methods for reasoning about program equivalence in ML-like languages supporting both functional and imperative features. In recent years, considerable progress has been made on this problem, primarily by advancements to two different classes of proof methods—*bisimulations* [12, 8, 9] and *step-indexed Kripke logical relations (SKLRs)* [2, 4].

In a paper appearing in POPL'12 [6], we proposed a new method for proving equivalences in ML-like languages, which we call *Relation Transition Systems (RTSs)*. RTSs draw inspiration from—and join together some of the best features of—bisimulations and SKLRs. In particular, RTSs support reasoning about recursive features in a convenient (step-index-free) *coinductive* style, as bisimulations do; but they also provide a very flexible treatment of "local" state, closely following recent work on SKLRs, in which invariants on the evolution of a piece of local state are expressed and enforced using a *state transition system* [2, 4].

Our ulterior motivation for developing RTSs was to overcome some basic limitations of bisimulations and SKLRs with regards to their potential for *inter-language reasoning*, *i.e.,* reasoning compositionally about equivalences between programs written in different languages, such as the source and target of a verified compiler [3, 5]. Existing bisimulation methods for higher-order stateful languages—*e.g., environmental* and *normal form* bisimulations [8, 10, 9]—rely crucially on "syntactic" devices (*e.g.,* context closure) in order to deal properly with unknown higher-order values that may be passed in as function arguments. These syntactic devices are appropriate for proving "contextual" properties—including but not limited to contextual equivalence [11]—but they bake in the assumption that the programs being related share a common syntactic notion of "context", which is clearly not a valid assumption in the inter-language setting.

In contrast, SKLRs *have* been successfully generalized to the inter-language setting—specifically, to the goal of establishing "compositional compiler correctness" [3, 5]—but they suffer from an orthogonal limitation, namely that in general they are not *transitively composable*. Ahmed grappled with this issue in her first paper on binary step-indexed logical relations [1]: her solution involved building the model over syntactically well-typed terms, an option that is not available, in general, when constructing relational models over low-level languages (*e.g.,* assembly). Moreover, her technique only helped in proving transitivity of her model for a simply-typed λ-calculus with recursive types, and has not been shown to scale to richer languages/models.

SKLRs' lack of transitivity has not been a major point of concern in prior work on proving contextual equivalences, since the latter are (by definition) transitively composable. However, in the inter-language setting, one can no longer rely on contextual equivalence as a crutch. For example, the correctness of a realistic, multi-stage compiler is only feasible to establish by transitively composing the correctness results for its constituent stages, but those correctness results cannot generally be phrased as contextual equivalences.

RTSs avoid the aforementioned limitations by means of a new technique, which we call *global vs. local knowledge*. The idea is to distinguish one's "local knowledge" about program equivalence (*i.e.,* the terms whose equivalence one wishes to prove) from the "global knowledge" (*i.e.,* the relation defining when unknown higher-order values passed in from the context are equivalent), and to parameterize the proof of correctness for the former over the latter. By *parameterizing over* the global knowledge instead of attempting to characterize it directly, RTSs (a) sidestep the need for any "syntactic" devices that would preclude inter-language reasoning, and (b) become transitively composable.

In our previous paper [6], we presented an RTS model for an ML-like core language, $\mathsf{F}^{\mu!}$, supporting higher-order functions, recursive types, abstract types, and general mutable references. We proved soundness of the model w.r.t. contextual equivalence, and gave several interesting examples of its use. We also briefly sketched the proof that RTSs are transitively composable, but our proof only covered a restricted fragment of the language/model omitting abstract types and mutable state. Extending the proof to handle those features turns out (unsurprisingly) to be highly non-trivial.

In this paper, we generalize the proof of RTS transitivity to account for the full RTS model of the full $\mathsf{F}^{\mu!}$ language. This is a critical stepping stone on the path toward generalizing RTSs to support effective inter-language reasoning. We begin in Sections II and III by reviewing the details of our language/model. In Section IV, we describe the high-level structure of our transitivity proof. The proof divides into two major parts, presented in Sections V and VI, respectively. The proof is highly intricate, requiring several tricky auxiliary constructions. In these sections, we highlight the key technical challenges, explain carefully the central constructions and the intuitions behind them, and sketch the proofs of the main lemmas. The complete proof is then given in the appendix. It has been fully machine-checked in Coq, and our Coq source files are available at the following URL:

`http://www.mpi-sws.org/~dreyer/papers/rts-trans/`

To give a rough sense of the complexity of the transitivity proof, it required approximately 3200 lines of Coq, versus 1500 lines to formalize the language, 400 lines to formalize the model, and 2000 lines to prove soundness of the model w.r.t. contextual equivalence.

II. The Language $\mathsf{F}^{\mu!}$

Figure 1 gives the syntax of $\mathsf{F}^{\mu!}$, along with its static and dynamic semantics judgment forms. $\mathsf{F}^{\mu!}$ is equipped with a standard type system, as well as a standard CBV dynamic semantics using evaluation contexts (aka continuations) K,

$$
\begin{array}{lll}
\tau_{\text{base}} & ::= & \mathsf{unit} \mid \mathsf{int} \mid \mathsf{bool} \\
\tau \in \text{Type} & ::= & \alpha \mid \tau_{\text{base}} \mid \tau_1 \times \tau_2 \mid \tau_1 + \tau_2 \mid \tau_1 \to \tau_2 \mid \mu\alpha.\,\tau \mid \\
 & & \forall\alpha.\,\tau \mid \exists\alpha.\,\tau \mid \mathsf{ref}\,\tau \mid \mathbf{n} \qquad (\mathbf{n} \in \text{TyNam}) \\
v \in \text{Val} & ::= & x \mid \langle\rangle \mid n \mid \mathsf{tt} \mid \mathsf{ff} \mid \langle v_1, v_2\rangle \mid \mathsf{inj}^i\, v \mid \mathsf{roll}\ v \mid \\
 & & \mathsf{fix}\, f(x).\, e \mid \Lambda.\, e \mid \mathsf{pack}\ v \mid \ell \\
e \in \text{Exp} & ::= & v \mid \mathsf{if}\ e_0\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \langle e_1, e_2\rangle \mid e.i \mid \\
 & & \mathsf{inj}^i\, e \mid (\mathsf{case}\, e\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_1 \mid \mathsf{inj}^2\, x \Rightarrow e_2) \mid \\
 & & \mathsf{roll}\ e \mid \mathsf{unroll}\ e \mid e_1\ e_2 \mid e[] \mid \\
 & & \mathsf{pack}\ e \mid \mathsf{unpack}\ e_1\ \mathsf{as}\ x\ \mathsf{in}\ e_2 \mid \\
 & & \mathsf{ref}\ e \mid\ !e \mid e_1 := e_2 \mid e_1 == e_2 \\
K \in \text{Cont} & ::= & \bullet \mid \mathsf{if}\ K\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \langle K, e\rangle \mid \langle v, K\rangle \mid K.i \mid \\
 & & \mathsf{inj}^i\, K \mid (\mathsf{case}\, K\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_1 \mid \mathsf{inj}^2\, x \Rightarrow e_2) \mid \\
 & & \mathsf{roll}\ K \mid \mathsf{unroll}\ K \mid K\ e \mid v\ K \mid K[] \mid \\
 & & \mathsf{pack}\ K \mid \mathsf{unpack}\ K\ \mathsf{as}\ x\ \mathsf{in}\ e \mid \mathsf{ref}\ K \mid\ !K \mid \\
 & & K := e \mid v := K \mid K == e \mid v == K \\
h \in \text{Heap} & ::= & \text{Loc} \xrightarrow{\text{fin}} \text{CVal} \qquad \text{Loc} = \{\ell_1, \ell_2, \ldots\} \\
 & & \Delta ::= \cdot \mid \Delta, \alpha \qquad \Gamma ::= \cdot \mid \Gamma, x : \tau
\end{array}
$$

Typing: $\Delta; \Gamma \vdash e : \tau$ **Small-step semantics:** $h, e \hookrightarrow h', e'$

Figure 1. The language $\mathsf{F}^{\mu!}$.

$$
\begin{array}{lll}
\text{CTypeF} & := & \{\, (\tau_1 \to \tau_2) \in \text{CType} \,\} \cup \{\, (\forall\alpha.\,\tau) \in \text{CType} \,\} \cup \\
 & & \{\, \mathbf{n} \in \text{TyNam} \,\} \cup \{\, \mathsf{ref}\,\tau \in \text{CType} \,\} \\
\text{VRel} & := & \text{CType} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\
\text{VRelF} & := & \text{CTypeF} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\
\text{ERel} & := & \text{CType} \to \mathbb{P}(\text{CExp} \times \text{CExp})
\end{array}
$$

Figure 2. Flexible types (CTypeF) and other semantic domains.

and finite heaps h. Memory allocation is deterministic, according to an unknown strategy (see [6] for details).

Here, following Ahmed [1], we only show the syntax of *type-erased* terms (aka expressions) e, over which both the dynamic semantics and our RTS model are constructed. The typeful syntax of $\mathsf{F}^{\mu!}$ programs p is given in the appendix. We distinguish between *type variables* (α) and *type names* ($\mathbf{n}$). The latter appear only in the model and are like type constants with no primitive intro/elim forms. CType is the set of closed types (with no free *variables*).

III. Relation Transition Systems

Figures 2–7 display our relation transition systems (RTS) model for $\mathsf{F}^{\mu!}$. We only provide here a brief review of the model. For a fuller exposition, see [6].

Worlds. Proving that two terms are equivalent using our model ($\Delta; \Gamma \vdash e_1 \sim e_2 : \tau$) involves constructing a "world" W, which codifies (a) the invariants on the state maintained by e_1 and e_2, and (b) the relational interpretations of any abstract types they define. In order to model equivalence of terms whose local state *evolves* over time (*e.g.,* "generative" classes/ADTs, whose instances/inhabitants grow dynamically when certain of their methods are invoked), the world W takes the form of a state transition system (STS). As shown in Figure 4, this consists of a preorder $\sqsubseteq$ on some state set S, together with a set of "owned" type names N (recording which abstract types are defined semantically

$$
\begin{array}{lll}
\overline{R}(\tau) & := & R(\tau) \qquad \text{if } \tau \in \text{CTypeF} \\
\overline{R}(\tau_{\text{base}}) & := & \{\, (v, v) \mid \vdash v : \tau_{\text{base}} \,\} \\
\overline{R}(\tau_1 \times \tau_2) & := & \{\, ((v_1, v_1'), (v_2, v_2')) \mid \\
 & & \quad (v_1, v_2) \in \overline{R}(\tau_1) \wedge (v_1', v_2') \in \overline{R}(\tau_2) \,\} \\
\overline{R}(\tau_1 + \tau_2) & := & \{\, (\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_1) \,\} \cup \\
 & & \{\, (\mathsf{inj}^2\, v_1, \mathsf{inj}^2\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_2) \,\} \\
\overline{R}(\mu\alpha.\,\tau) & := & \{\, (\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \mid (v_1, v_2) \in \overline{R}(\tau[\mu\alpha.\,\tau/\alpha]) \,\} \\
\overline{R}(\exists\alpha.\,\tau) & := & \{\, (\mathsf{pack}\, v_1, \mathsf{pack}\, v_2) \mid \exists\tau'.\, (v_1, v_2) \in \overline{R}(\tau[\tau'/\alpha]) \,\}
\end{array}
$$

Figure 3. Inductive def. of value closure (if $R \in \text{VRelF}$, then $\overline{R} \in \text{VRel}$).

$$
\begin{array}{l}
beta(e) := \begin{cases} e' & \text{if } \forall h.\ h, e \hookrightarrow h, e' \\ \text{undef} & \text{otherwise} \end{cases} \\
\text{WfKnow}(\mathcal{N}) := \{\, R \in \text{VRelF} \mid \forall \mathbf{n} \notin \mathcal{N}.\ R(\mathbf{n}) = \emptyset \\
\quad \wedge\ (\forall\tau_1, \tau_2.\ \forall (f_1, f_2) \in R(\tau_1 \to \tau_2).\ \forall i, v.\ beta(f_i\ v) \text{ defined}) \\
\quad \wedge\ (\forall\alpha, \tau.\ \forall (f_1, f_2) \in R(\forall\alpha.\,\tau).\ \forall i.\ beta(f_i[]) \text{ defined}) \,\} \\
\text{World} := \{\, W = (\mathsf{S}, \sqsubseteq, \mathsf{N}, \mathsf{L}, \mathsf{H}) \in \text{Set} \times \text{Preord}(\mathsf{S}) \times \mathbb{P}(\text{TyNam}) \times \\
\quad (\mathsf{S} \to \text{VRelF} \to \text{VRelF}) \times (\mathsf{S} \to \text{VRelF} \to \text{HRel}) \mid \\
\quad \mathsf{L} \text{ monotone in 1st, 2nd args w.r.t. } \sqsubseteq, \subseteq \ \wedge \\
\quad \forall s, R.\ \mathsf{L}(s)(R) \in \text{WfKnow}(\mathsf{N}) \wedge \\
\quad \mathsf{H} \text{ monotone in 2nd arg w.r.t. } \subseteq \ \}
\end{array}
$$

Figure 4. Definition of worlds.

by the world) and two state-dependent relations: H, which says what heaps are related (*i.e.,* obey the "current" state invariant), and L, which describes what values are known to be equivalent, at any given state $s \in \mathsf{S}$. (We call L the "local knowledge" of W, and discuss it in more detail below.)

In our original RTS model [6], worlds actually contain two preorders on the state set S—one "public" and one "private". As Dreyer *et al.* [4] have shown, this is useful for reasoning about "well-bracketed" state change. We have chosen to drop the second preorder here in this extended abstract to streamline the presentation, and because it does not introduce any challenges into the proof of RTS transitivity, our present focus. (The proof in the appendix handles the full public/private model.)

Local Worlds and W_{ref}**.** To account for the ref type of $\mathsf{F}^{\mu!}$, we require that the world $W \in \text{World}$ be a combination of a fixed "shared world" W_{ref} and a proof-specific "local world" $w \in \text{LWorld}$ (Figure 5). The idea is that W_{ref} governs the semantics and invariants of the ref type, which are the same in all proofs; whereas w describes the invariants associated with e_1's and e_2's *local* state, as well as the relational interpretations of any abstract types they define. The local w is joined together with W_{ref} to form the full W by the "lifting" operator $w{\uparrow}$, which is defined in Figure 6 using a simple product construction of w's and W_{ref}'s STSs.

An important point of note here is that the local world w is allowed to depend on the state s^{rf} of the shared world W_{ref}. The shared state s^{rf} is a partial bijection between (globally visible) memory locations, with each pair of related locations associated with the type τ of their contents, and the L and H components of w take $s^{\text{rf}} \in W_{\text{ref}}.\mathsf{S}$ as a parameter in addition to the local state $s \in w.\mathsf{S}$. Consequently, the definition of RTS equivalence (bottom of Figure 7) includes

$\mathrm{dom}_{[1]}(s^{\mathrm{rf}}) := \{\, \ell_1 \mid \exists \tau, \ell_2.\ (\tau, \ell_1, \ell_2) \in s^{\mathrm{rf}} \,\}$
$\mathrm{dom}_{[2]}(s^{\mathrm{rf}}) := \{\, \ell_2 \mid \exists \tau, \ell_1.\ (\tau, \ell_1, \ell_2) \in s^{\mathrm{rf}} \,\}$

$W_{\mathrm{ref}}.\mathsf{S} := \{\, s^{\mathrm{rf}} \in \mathbb{P}_{\mathrm{fin}}(\mathrm{CType} \times \mathrm{Loc} \times \mathrm{Loc}) \mid$
$\forall (\tau, \ell_1, \ell_2), (\tau', \ell_1', \ell_2') \in s^{\mathrm{rf}}.\ (\ell_1 = \ell_1' \implies \tau = \tau' \wedge \ell_2 = \ell_2') \wedge$
$(\ell_2 = \ell_2' \implies \tau = \tau' \wedge \ell_1 = \ell_1') \,\}$

$W_{\mathrm{ref}}.\sqsubseteq := \subseteq \qquad W_{\mathrm{ref}}.\mathsf{N} := \emptyset$

$W_{\mathrm{ref}}.\mathsf{L}(s^{\mathrm{rf}})(R)(\mathsf{ref}\ \tau) := \{\, (\ell_1, \ell_2) \mid (\tau, \ell_1, \ell_2) \in s^{\mathrm{rf}} \,\}$

$W_{\mathrm{ref}}.\mathsf{H}(s^{\mathrm{rf}})(R) := \{\, (h_1, h_2) \mid \forall i.\ \mathrm{dom}(h_i) = \mathrm{dom}_{[i]}(s^{\mathrm{rf}}) \wedge$
$\forall (\tau, \ell_1, \ell_2) \in s^{\mathrm{rf}}.\ (h_1(\ell_1), h_2(\ell_2)) \in \overline{R}(\tau) \,\}$

$\mathrm{LWorld} := \{\, w = (\mathsf{S}, \sqsubseteq, \mathsf{N}, \mathsf{L}, \mathsf{H}) \in \mathrm{Set} \times \mathrm{Preord}(\mathsf{S}) \times \mathbb{P}(\mathrm{TyNam}) \times$
$(W_{\mathrm{ref}}.\mathsf{S} \to \mathsf{S} \to \mathrm{VRelF} \to \mathrm{VRelF}) \times (W_{\mathrm{ref}}.\mathsf{S} \to \mathsf{S} \to \mathrm{VRelF} \to \mathrm{HRel}) \mid$
L monotone in 1st, 2nd, 3rd args w.r.t. $W_{\mathrm{ref}}.\sqsubseteq$, $\sqsubseteq$, $\subseteq$ $\wedge$
$\forall s^{\mathrm{rf}}, s, R.\ \mathsf{L}(s^{\mathrm{rf}})(s)(R) \in \mathrm{WfKnow}(\mathsf{N}) \wedge$
H monotone in 3rd arg w.r.t. $\subseteq$ $\}$

Figure 5. Definitions of W_{ref} and local worlds.

$H \otimes H' := \{(h_1 \uplus h_1', h_2 \uplus h_2') \mid (h_1, h_2) \in H \wedge (h_1', h_2') \in H'\}$

$w{\uparrow}.\mathsf{S} := W_{\mathrm{ref}}.\mathsf{S} \times w.\mathsf{S}$
$w{\uparrow}.\sqsubseteq := \{\, (p, p') \mid p.1 \sqsubseteq p'.1 \wedge p.2 \sqsubseteq p'.2 \,\}$
$w{\uparrow}.\mathsf{N} := w.\mathsf{N}$
$w{\uparrow}.\mathsf{L}(s^{\mathrm{rf}}, s)(R) := W_{\mathrm{ref}}.\mathsf{L}(s^{\mathrm{rf}})(R) \cup w.\mathsf{L}(s^{\mathrm{rf}})(s)(R)$
$w{\uparrow}.\mathsf{H}(s^{\mathrm{rf}}, s)(R) := W_{\mathrm{ref}}.\mathsf{H}(s^{\mathrm{rf}})(R) \otimes w.\mathsf{H}(s^{\mathrm{rf}})(s)(R)$

Figure 6. Lifting ($\uparrow \in \mathrm{LWorld} \to \mathrm{World}$) of worlds.

a side condition checking that w is *stable—i.e.,* roughly, that if two "local" heaps are related by $w.\mathsf{H}(s^{\mathrm{rf}})(s)$, and the shared state s^{rf} advances to some $\hat{s}^{\mathrm{rf}} \sqsupseteq s^{\mathrm{rf}}$, then there must exist some $\hat{s} \sqsupseteq s$ such that the local heaps continue to be related by $w.\mathsf{H}(\hat{s}^{\mathrm{rf}})(\hat{s})$. This stability condition is needed to ensure that, when different modules in a program update the state of the shared W_{ref}, they do not cause bad "interference" with one another's local state invariants. Although for most practical purposes the extra parameterization of w over s^{rf} is unnecessary—in which case stability of w is trivial to show by choosing $\hat{s} := s$—it will turn out to be critically useful in our transitivity proof (see Section VI).

Global vs. Local Knowledge. RTS proofs are much like bisimulation proofs in that they require one to declare up front all the equivalences between terms/values that one needs to know in order to establish the equivalence of the terms e_1 and e_2 in question. We call this set of putative equivalences the "local knowledge" of the proof, which constitutes the L component of the world W.

The object is then to demonstrate that this local knowledge is "consistent," as defined in Figure 7, which implies that the equivalence is semantically justified. In particular, for any function values (f_1, f_2) related by $W.\mathsf{L}$ (at any given state $s \in W.\mathsf{S}$), we must show that f_1 and f_2 behave equivalently when applied to "related arguments". But from what relation do we draw these "related arguments"?

Since the related arguments are passed in from somewhere in the program context, they might very well not be related by our local knowledge. Rather, we say they are drawn from the "global knowledge" about program equivalence. In the higher-order setting, characterizing this global knowledge directly is quite difficult; intuitively, it is as hard as coming up with a good model of program equivalence in the first place! Bisimulation-based approaches [8, 9] deal with this challenge by giving a *syntactic* characterization of the global knowledge, which (as we explained in the introduction) we do not want to do. Our approach instead is to avoid the problem altogether: rather than try to define the global knowledge directly, we *parameterize* our model over it.

We only require that the global knowledge G "respect" the world ($G \in \mathrm{GK}(W)$, Figure 7), namely that: it must include the local knowledge, it must be monotone w.r.t. state changes, and it must not alter the meaning of the reference type nor of any abstract type name owned by the world. Otherwise, we place no restrictions on G. Notably, G may relate two *arbitrary* values at *any* function type, even values that are not functions! This seemingly perverse liberality is in fact essential to our transitivity proof (see Section V-A).

Flexible Types and Value Closure. The local and global knowledges only declare which values are related at the so-called "flexible" types, CTypeF, which include type names, as well as function, universal, and reference types (Figure 2). Such value equivalences at flexible types, $R \in \mathrm{VRelF}$, are extended to all (closed) types by the inductively-constructed value closure, $\overline{R} \in \mathrm{VRel}$, in Figure 3, which defines the meaning of the remaining "rigid" type constructors. Note that while existentials ($\exists \alpha.\, \tau$) are rigid, the witness τ' for α can be a type *name*, which $W.\mathsf{L}$ can define semantically via an arbitrary state-dependent value relation. In this way, RTSs support relationally parametric reasoning [7, 12].

Local Term Equivalence. We say that two closed terms e_1 and e_2 are *locally equivalent* at a given type τ w.r.t. a world W, a global knowledge G, and the current state of the world s—and denote this as $(e_1, e_2) \in \mathbf{E}_W(G)(s)(\tau)$—if, when they are executed with related initial heaps (*i.e.,* satisfying the world's invariants), one of these cases holds:

(**Case** $\Uparrow$) they both diverge; or

(**Case** $\Downarrow$) they both reduce to related values; or

(**Case** $\lightning$) they both reduce to related "stuck" configurations (**S**), such as function calls, where related function values are applied to related argument values inside locally equivalent evaluation contexts, *i.e.,* contexts which, when filled with related values, result (coinductively) in locally equivalent terms. In all cases, "related" values are drawn from the value closure of the global knowledge, $\overline{G}$, and we require that the final heaps also satisfy the world's invariants.

Observe that, in cases $\Downarrow$ and $\lightning$, we are permitted to advance to a future state $s' \sqsupseteq s$. Correspondingly, in the $\lightning$ case, we must show that the continuations K_1 and K_2 are related in any future state $s'' \sqsupseteq s'$—as the function call may further advance the state of the world—and in any (pointwise) larger global knowledge. Also note that our definition bakes in a notion of "framing" (like in separation logic) by quantifying over frame heaps h_1^{F} and h_2^{F}.

Two open terms are locally equivalent ($\mathbf{OE}_W$) if, for

$$
\begin{array}{ll}
R' \geq^{\mathcal{N}}_{\mathrm{ref}} R & := R' \supseteq R \wedge \forall \tau.\ R'(\mathsf{ref}\,\tau) = R(\mathsf{ref}\,\tau) \wedge \forall \mathbf{n} \in \mathcal{N}.\ R'(\mathbf{n}) = R(\mathbf{n}) \\
\mathrm{GK}(W) & := \{\, G \in W.\mathsf{S} \to \mathrm{VRelF} \mid G \text{ is monotone w.r.t. } \sqsubseteq \wedge \forall s.\ G(s) \geq^{W.\mathsf{N}}_{\mathrm{ref}} W.\mathsf{L}(s)(G(s)) \,\} \\
\mathbf{E}_W(G)(s)(\tau) & := \{\, (e_1, e_2) \mid \forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)).\ \forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.\ h_1 \uplus h_1^{\mathrm{F}} \text{ defined} \wedge h_2 \uplus h_2^{\mathrm{F}} \text{ defined} \implies \\
& \qquad \exists h_1', h_2', v_1, v_2, K_1, K_2, e_1', e_2', s', \tau'. \\
& \qquad\quad \textbf{Case } \Uparrow\textbf{:}\ (h_1 \uplus h_1^{\mathrm{F}}, e_1) \hookrightarrow^{\omega} \wedge\ (h_2 \uplus h_2^{\mathrm{F}}, e_2) \hookrightarrow^{\omega} \\
& \qquad \vee\ \textbf{Case } \Downarrow\textbf{:}\ (h_1 \uplus h_1^{\mathrm{F}}, e_1) \hookrightarrow^{*} (h_1' \uplus h_1^{\mathrm{F}}, v_1)\ \wedge\ (h_2 \uplus h_2^{\mathrm{F}}, e_2) \hookrightarrow^{*} (h_2' \uplus h_2^{\mathrm{F}}, v_2) \\
& \qquad\qquad \wedge\ s' \sqsupseteq s\ \wedge\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s'))\ \wedge\ (v_1, v_2) \in \overline{G(s')}(\tau) \\
& \qquad \vee\ \textbf{Case } \lightning\textbf{:}\ (h_1 \uplus h_1^{\mathrm{F}}, e_1) \hookrightarrow^{*} (h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'])\ \wedge\ (h_2 \uplus h_2^{\mathrm{F}}, e_2) \hookrightarrow^{*} (h_2' \uplus h_2^{\mathrm{F}}, K_2[e_2']) \\
& \qquad\qquad \wedge\ s' \sqsupseteq s\ \wedge\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s'))\ \wedge\ (e_1', e_2') \in \mathbf{S}(G(s'), G(s'))(\tau') \\
& \qquad\qquad \wedge\ \forall s'' \sqsupseteq s'.\ \forall G' \supseteq G.\ \forall (v_1', v_2') \in \overline{G'(s'')}(\tau').\ (K_1[v_1'], K_2[v_2']) \in \mathbf{E}_W(G')(s'')(\tau) \,\} \\
\mathbf{S}(R_f, R_v)(\tau) & := \{\, (f_1\ v_1, f_2\ v_2) \mid \exists \tau'.\ (f_1, f_2) \in R_f(\tau' \to \tau) \wedge (v_1, v_2) \in \overline{R_v}(\tau') \,\} \cup \\
& \quad \{\, (f_1[], f_2[]) \mid \exists \tau', \sigma.\ \tau = \tau'[\sigma/\alpha] \wedge (f_1, f_2) \in R_f(\forall \alpha.\, \tau') \,\} \\
\mathbf{OE}_W(G)(s)(\Delta; \Gamma \vdash \tau) & := \{\, (e_1, e_2) \mid \forall \delta \in \Delta \to \mathrm{CType}.\ \forall \gamma_1, \gamma_2 \in \mathrm{dom}(\Gamma) \to \mathrm{CVal}. \\
& \qquad (\forall x{:}\tau' \in \Gamma.\ (\gamma_1(x), \gamma_2(x)) \in \overline{G(s)}(\delta\tau')) \implies (\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_W(G)(s)(\delta\tau) \,\} \\
\mathit{inhabited}(W) & := \forall G \in \mathrm{GK}(W).\ \exists s_0.\ (\emptyset, \emptyset) \in W.\mathsf{H}(s_0)(G(s_0)) \\
\mathit{consistent}(W) & := \forall G \in \mathrm{GK}(W).\ \forall s.\ \forall \tau.\ \forall (e_1, e_2) \in \mathbf{S}(W.\mathsf{L}(s)(G(s)), G(s))(\tau).\ (\mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_W(G)(s)(\tau) \\
\mathit{stable}(w) & := \forall G \in \mathrm{GK}(w{\uparrow}).\ \forall s^{\mathrm{rf}}, s.\ \forall (h_1, h_2) \in w.\mathsf{H}(s^{\mathrm{rf}})(s)(G(s^{\mathrm{rf}}, s)). \\
& \quad \forall \hat{s}^{\mathrm{rf}} \sqsupseteq s^{\mathrm{rf}}.\ \forall (h_1^{\mathrm{rf}}, h_2^{\mathrm{rf}}) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}^{\mathrm{rf}})(G(\hat{s}^{\mathrm{rf}}, s)).\ h_1^{\mathrm{rf}} \uplus h_1 \text{ defined} \wedge h_2^{\mathrm{rf}} \uplus h_2 \text{ defined} \implies \\
& \quad \exists \hat{s} \sqsupseteq s.\ (h_1, h_2) \in w.\mathsf{H}(\hat{s}^{\mathrm{rf}})(\hat{s})(G(\hat{s}^{\mathrm{rf}}, \hat{s})) \\
\Delta; \Gamma \vdash e_1 \sim_W e_2 : \tau & := \mathit{inhabited}(W) \wedge \mathit{consistent}(W) \wedge \forall G \in \mathrm{GK}(W).\ \forall s.\ (e_1, e_2) \in \mathbf{OE}_W(G)(s)(\Delta; \Gamma \vdash \tau) \\
\Delta; \Gamma \vdash e_1 \sim e_2 : \tau & := \forall \mathcal{N} \in \mathbb{P}(\mathrm{TyNam}).\ \mathcal{N} \text{ countably infinite} \implies \exists w.\ w.\mathsf{N} \subseteq \mathcal{N} \wedge \mathit{stable}(w) \wedge \Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_2 : \tau
\end{array}
$$

Figure 7. Coinductive definition of local term equivalence, $\mathbf{E}_W \in \mathrm{GK}(W) \to W.\mathsf{S} \to \mathrm{ERel}$, plus definitions of world inhabitation, world consistency, local world stability, and program equivalence.

all closing substitutions of related values at the appropriate types, the substituted (closed) terms are locally equivalent.

Program Equivalence. Finally, two *programs* are equivalent ($\Delta; \Gamma \vdash e_1 \sim e_2 : \tau$) iff there exists a local world w such that (a) w is parametric in the particular choice of names to represent its abstract types; (b) w is stable; and (c) $w{\uparrow}$ is inhabited and consistent, and relates e_1 and e_2 under any global knowledge $G \in \mathrm{GK}(w{\uparrow})$. A world is inhabited iff its heap invariant is satisfied by the empty heaps in some state; it is consistent iff any functions it relates do indeed behave locally equivalently when applied to $\overline{G}$-related arguments.

We conclude this section with a key lemma about $\mathbf{E}$. Given a consistent world, if the global knowledge extends the world's local knowledge $W.\mathsf{L}$ with some additional external knowledge $\boldsymbol{\mathcal{R}}$, then the third case in the definition of $\mathbf{E}$ can be restricted so that it applies only to external function calls (*i.e.,* calls to functions related by $\boldsymbol{\mathcal{R}}$, not by $W.\mathsf{L}$). This holds essentially because we can "inline" the equivalence proofs for any internal calls.

Lemma 1 (External call)**.** For any W s.t. $\mathit{consistent}(W)$, $G \in \mathrm{GK}(W)$ and $\boldsymbol{\mathcal{R}} \in W.\mathsf{S} \to \mathrm{VRelF}$, we have

$$(\forall s.\ G(s) = W.\mathsf{L}(s)(G(s)) \cup \boldsymbol{\mathcal{R}}(s)) \implies \mathbf{E}_W(G) = \mathbf{E}^{\boldsymbol{\mathcal{R}}}_W(G)$$

where the definition of $\mathbf{E}^{\boldsymbol{\mathcal{R}}}_W$ is the same as $\mathbf{E}_W$ except that $\mathbf{S}(G(s'), G(s'))$ is replaced by $\mathbf{S}(\boldsymbol{\mathcal{R}}(s'), G(s'))$.

IV. Structure of the Transitivity Proof

Given that $\Delta; \Gamma \vdash e_1 \sim e_2 : \tau$ and $\Delta; \Gamma \vdash e_2 \sim e_3 : \tau$, our goal is to show $\Delta; \Gamma \vdash e_1 \sim e_3 : \tau$. Unfolding the definition of our goal, we are given a countably infinite set of type names $\mathcal{N}$ and must construct a stable local world w such that (a) $\Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_3 : \tau$ and (b) $w.\mathsf{N} \subseteq \mathcal{N}$ (*i.e.,* $w.\mathsf{L}$ defines no names outside of $\mathcal{N}$). To do so, we split $\mathcal{N}$ into three disjoint (and also countably infinite) pieces: $\mathcal{N}_1$, $\mathcal{N}_2$, and $\mathcal{N}_\exists$. The first two pieces will be used to instantiate the assumptions regarding $e_1 \sim e_2$ and $e_2 \sim e_3$, respectively, thus yielding two stable local worlds w_1 and w_2 such that

$$\Delta; \Gamma \vdash e_1 \sim_{w_1\uparrow} e_2 : \tau \tag{1}$$

$$\text{and} \quad \Delta; \Gamma \vdash e_2 \sim_{w_2\uparrow} e_3 : \tau \tag{2}$$

as well as $w_1.\mathsf{N} \subseteq \mathcal{N}_1$ and $w_2.\mathsf{N} \subseteq \mathcal{N}_2$. Keeping $\mathcal{N}_1$ and $\mathcal{N}_2$ disjoint is a matter of basic hygiene: it ensures that w_1 and w_2, which we will be using in the construction of w, do not step on each other's toes by defining the same type name in incompatible ways. As for the names in $\mathcal{N}_\exists$, we reserve them for a special purpose to be explained later.

At this point, the proof divides into two separate parts. In the first part, we use w_1 and w_2 to directly construct a full world W such that $\Delta; \Gamma \vdash e_1 \sim_W e_3 : \tau$ (and $W.\mathsf{N} \subseteq \mathcal{N}$). While the proof of this part is quite subtle, it is essentially an extension of the transitivity proof for a restricted fragment of $\mathsf{F}^{\mu!}$ that we sketched in our previous paper [6], and which we present here in much greater detail. The main novelty over that previous proof is that we now deal with abstract types; reference types do not cause much of a problem.

However, the second part of the proof has all to do with references. Specifically, the world W that we create in the first part does not have the required shape of a lifted local world $w{\uparrow}$. Thus, in the second part, we (i) develop a theory of *weak isomorphisms* between worlds and prove that they preserve term equivalence, and (ii) construct a stable local world w such that $w{\uparrow}$ is weakly isomorphic to W.

V. First Part: Constructing the Full World W

A. High-Level Explanation

As mentioned above, this first part of the proof is essentially agnostic as to whether the language/model supports mutable state. To ease the presentation, we therefore gloss over any state-related details at first; we will be more precise in Section V-B. We also write W_i as shorthand for $w_i{\uparrow}$.

We want to construct W such that $\Delta;\Gamma \vdash e_1 \sim_W e_3 : \tau$. The proofs of consistency of W and relatedness of (e_1, e_3) by **OE** turn out to be very similar, so let us focus on the latter here. We are given a global knowledge $G \in \mathrm{GK}(W)$ and related substitutions γ_1 and γ_3. These substitutions map each variable bound in Γ to related values $(v_1, v_3) \in \overline{G}(\tau')$. In order to make use of (1) and (2), we want to be able to: (i) "decompose" G into global knowledges $G_{(1)} \in \mathrm{GK}(W_1)$ and $G_{(2)} \in \mathrm{GK}(W_2)$ that would be suitable for instantiating (1) and (2), and (ii) find a mediating substitution γ_2 s.t. for each $x \in \mathrm{dom}(\Gamma)$, it is the case that $\overline{G_{(1)}}$ relates $(\gamma_1 x, \gamma_2 x)$ and $\overline{G_{(2)}}$ relates $(\gamma_2 x, \gamma_3 x)$. Formally, we want:

$$\overline{G}(\tau) \subseteq \overline{G_{(1)}}(\tau_{(1)}) \circ \overline{G_{(2)}}(\tau_{(2)}) \tag{3}$$

where $\circ$ is ordinary relational composition. (Pretend *for now* that $\tau_{(i)} = \tau$. We will soon see why that's not good enough.)

If we have this, we can instantiate (1) and (2), thus obtaining $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}(G_{(1)})(\tau_{(1)})$ and $(\gamma_2 e_2, \gamma_3 e_3) \in \mathbf{E}(G_{(2)})(\tau_{(2)})$. It thus remains for us to show $(\gamma_1 e_1, \gamma_3 e_3) \in \mathbf{E}(G)(\tau)$. In other words, we must (unsurprisingly) show some kind of transitivity property for $\mathbf{E}$:

$$\mathbf{E}_{W_1}(G_{(1)})(\tau_{(1)}) \circ \mathbf{E}_{W_2}(G_{(2)})(\tau_{(2)}) \subseteq \mathbf{E}_W(G)(\tau) \tag{4}$$

Proving this will certainly require us to prove the analogous transitivity property for values, which is the inverse of (3):

$$\overline{G}(\tau) \supseteq \overline{G_{(1)}}(\tau_{(1)}) \circ \overline{G_{(2)}}(\tau_{(2)}) \tag{5}$$

Since global knowledges extend the corresponding local ones, this in turn means that $W.\mathsf{L}$ must at least include the composition of $W_1.\mathsf{L}$ and $W_2.\mathsf{L}$:

$$W.\mathsf{L}(G)(\tau) \supseteq W_1.\mathsf{L}(G_{(1)})(\tau_{(1)}) \circ W_2.\mathsf{L}(G_{(2)})(\tau_{(2)}) \tag{6}$$

In order to see what else we want to put into W, and how to define $G_{(i)}$ and $\tau_{(i)}$, let us consider proving (3) and (5). For a flexible type τ' the conjunction of (3) and (5) is:

$$G(\tau') = G_{(1)}(\tau'_{(1)}) \circ G_{(2)}(\tau'_{(2)}).$$

One simple (but inadequate) choice for $G_{(i)}$ would be to define it as the minimal global knowledge in $\mathrm{GK}(W_i)$—*i.e.,* as the least fixed-point of $W_i.\mathsf{L}$. But there is no reason to believe that for any $(v_1, v_3) \in G(\tau')$, there magically happens to be a "mediating" value v_2 such that $W_1.\mathsf{L}$ relates (v_1, v_2) and $W_2.\mathsf{L}$ relates (v_2, v_3), as required by the $\subseteq$ part of the above equation. To work this magic, we will explicitly *add* such mediating values to $G_{(1)}$ and $G_{(2)}$! Concretely, we define $G_{(1)}$ as the smallest global knowledge in $\mathrm{GK}(W_1)$ that relates $(v_1, \mathbf{I}(\tau, v_1, v_3))$ at $\tau_{(1)}$ whenever G relates (v_1, v_3) at τ, and similarly $G_{(2)}$ as the smallest global knowledge in $\mathrm{GK}(W_2)$ that relates $(\mathbf{I}(\tau, v_1, v_3), v_3)$ at $\tau_{(2)}$ whenever G relates (v_1, v_3) at τ.

Now, what is this magic $\mathbf{I}$? For proving (3), it could be anything that maps to CVal. But for (5), it is crucial that each mediating value *uniquely* encodes the corresponding value pair (v_1, v_3). We therefore require $\mathbf{I}$ to be *injective*. Since all involved sets are countably infinite, such an encoding function exists and we do not care about the particular choice—except that we will choose its range to be of *rigid* type, specifically int, for reasons we will explain shortly.

The proofs of (3) and (5) are by induction on the value closure (recall that it is constructed as a least fixed-point). The reason why we must add more to $W.\mathsf{L}$ than just the composition in (6), and why $\tau_{(i)}$ cannot just be τ in general, has to do with abstract types. We illustrate the issue here for existential types, but the same problem arises for universals (although in a different place, namely in the proof of (4)).

Suppose $\tau_{(i)}$ were the identity and consider (5) at some type $\exists\alpha.\,\tau$: We would have to show that if $(\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \in \overline{G_{(1)}}(\exists\alpha.\,\tau)$ and $(\mathsf{pack}\ v_2, \mathsf{pack}\ v_3) \in \overline{G_{(2)}}(\exists\alpha.\,\tau)$, then $(\mathsf{pack}\ v_1, \mathsf{pack}\ v_3) \in \overline{G}(\exists\alpha.\,\tau)$. Unfolding the value closure, this means: Given some τ'_1, τ'_2 such that $(v_1, v_2) \in \overline{G_{(1)}}(\tau[\tau'_1/\alpha])$ and $(v_2, v_3) \in \overline{G_{(2)}}(\tau[\tau'_2/\alpha])$, we must come up with τ' such that $(v_1, v_3) \in \overline{G}(\tau[\tau'/\alpha])$. Now, if the two given representation types happen to be the same ($\tau'_1 = \tau'_2$), then we could proceed by just picking $\tau' := \tau'_1$. But of course in general τ'_1 and τ'_2 will be different!

The intuition behind our solution is quite simple: we pick τ' to be a fresh *type name*, which we use to represent the semantic composition of τ'_1 and τ'_2. More concretely, we use a type name $\mathbf{n}$ from $\mathcal{N}_\exists$ (which we reserved for exactly this purpose) to uniquely encode τ'_1 and τ'_2, then define $\mathbf{n}$'s meaning in W to be precisely $\overline{G_{(1)}}(\tau'_1) \circ \overline{G_{(2)}}(\tau'_2)$, and finally choose τ' to be $\mathbf{n}$. Since we don't know what τ'_1 and τ'_2 are, we simply have to encode all pairs of types this way. To pick the names, we use an injective function

$$\mathbf{A} \in \mathrm{CType} \times \mathrm{CType} \to \mathcal{N}_\exists$$

which, like $\mathbf{I}$, exists because all involved sets are countably infinite (and, as with $\mathbf{I}$, we do not care about its concrete definition). It should be clear by now what $\tau'_{(i)}$ does and that it is crucial for making the induction go through: it *decodes* τ' by traversing its structure and replacing each type name $\mathbf{n}$ that equals $\mathbf{A}(\tau_1, \tau_2)$—for some τ_1, τ_2—with τ_i.

That's the intuition; the reality is a bit more complex. It turns out that, in order to prove (3) and (5), the decoding must in fact be *bijective*, but the one sketched above is not injective. For instance, $\mathbf{A}(\mathsf{int}, \mathsf{int})$ and int are obviously distinct types but both decode to int (by either projection). Fortunately, there is an easy way to obtain the desired bijectivity: we only encode a type pair (τ_1, τ_2) directly as a name $\mathbf{A}(\tau_1, \tau_2)$ if τ_1 and τ_2 are "sufficiently different". If they share some structure, however, we keep the parts that are the same and only apply $\mathbf{A}$ to the parts that are

different. To take a simple example: to encode $(\mathsf{int}, \mathsf{bool})$, we would use the type name $\mathbf{A}(\mathsf{int}, \mathsf{bool})$, but to encode $(\mathsf{int} \to \mathsf{int}, \mathsf{int} \to \mathsf{bool})$, we would pick $\mathsf{int} \to \mathbf{A}(\mathsf{int}, \mathsf{bool})$ instead of $\mathbf{A}(\mathsf{int} \to \mathsf{int}, \mathsf{int} \to \mathsf{bool})$.

Finally, property (4) is shown by coinduction. Recalling that $\mathbf{E}$ comprises three cases ($\Uparrow$, $\Downarrow$, and $\lightning$), the key here is that the case of $\mathbf{E}$ by which the first and second terms—call them e_1' and e_2'—are related should match the case by which the second and third terms—e_2' and e_3'—are related. In other words, out of the 3×3 possible cases, 6 should never arise. As a representative example, consider the situation where e_1' and e_2' are related because they reduce to related values (case $\Downarrow$), and e_2' and e_3' because they reduce to related function calls with related continuations (case $\lightning$). By Lemma 1 we can assume that these calls are to *external* functions related by $G_{(2)}$. But this means that the function called in e_2' must be of the form $\mathbf{I}(\tau, v_1, v_3)$, *i.e.,* not a function at all (recall that we required $\mathbf{I}$ to map to *rigid* values)! Hence, e_2' gets stuck, contradicting the assumption that it reduced to a value.

The remaining possibilities (where the cases of relatedness for (e_1', e_2') and (e_2', e_3') match) are handled as follows:

Case $\Uparrow$. Then both e_1' and e_3' diverge, so we are done.

Case $\Downarrow$. Then e_1', e_2', and e_3' reduce to values v_1, v_2, and v_3, such that $\overline{G_{(1)}}$ relates (v_1, v_2) and $\overline{G_{(2)}}$ relates (v_2, v_3). Thus, by (5), $\overline{G}$ relates (v_1, v_3) and we are done.

Case $\lightning$. We know that e_1' and e_2' reduce to related function calls in related continuations, and that the same applies to e_2' and e_3'. Using Lemma 1 as above, we know that all four function calls are actually stuck. Since, by determinacy, e_2' cannot get stuck in two different ways, we have a unique function call and a unique continuation in the middle. So, it suffices to show a corresponding transitivity property for $\mathbf{S}$ and for continuations. The one for continuations follows from (3) and the coinductive hypothesis. The one for $\mathbf{S}$ follows from (5) and injectivity of $\mathbf{I}$; when reasoning about type instantiations ($f_i[]$), we must also make use of our type encoding $\mathbf{A}$—dually to how we handle pack in proving (5).

B. The Gory Details

We first formalize the syntactic encoding of types. The previously motivated notion of two types being "sufficiently different" is defined as the negation of *similarity*.

Definition 1. Similarity, written $\approx$, is defined inductively:

$$\frac{\mathbf{n} \notin \mathcal{N}_\exists}{\mathbf{n} \approx \mathbf{n}} \quad \frac{}{\alpha \approx \alpha} \quad \frac{}{\tau_{\mathsf{base}} \approx \tau_{\mathsf{base}}} \quad \frac{\tau \sim \sigma}{\mathsf{ref}\,\tau \approx \mathsf{ref}\,\sigma} \quad \frac{\tau \sim \sigma \ (\star = \mu, \forall, \exists)}{\star\alpha.\,\tau \approx \star\alpha.\,\sigma}$$

$$\frac{\tau \sim \sigma \quad \tau' \sim \sigma' \quad (\star = \times, +, \to)}{\tau \star \tau' \approx \sigma \star \sigma'} \quad \frac{\tau, \sigma \in \mathrm{CType}}{\tau \sim \sigma} \quad \frac{\tau \approx \sigma}{\tau \sim \sigma}$$

Two closed dissimilar types are encoded as a type name from $\mathcal{N}_\exists$ using a bijection

$$\mathbf{A} \in \{\, (\tau_1, \tau_2) \in \mathrm{CType} \times \mathrm{CType} \mid \tau_1 \not\approx \tau_2 \,\} \to \mathcal{N}_\exists.$$

The encoding of two arbitrary closed types is a natural lifting of $\mathbf{A}$. Instead of defining it explicitly, we find it simpler to define the decoding and then state the existence of a corresponding encoding.

Definition 2. We recursively define *decoding projections* $(-)_{(i)} \in \mathrm{Type} \to \mathrm{Type}$ for $i = 1, 2$ as follows. Note that if τ is closed, then so is $\tau_{(i)}$.

$$\mathbf{n}_{(i)} := \begin{cases} \tau_i & \text{if } \mathbf{n} = \mathbf{A}(\tau_1, \tau_2) \text{ for some } \tau_1, \tau_2 \\ \mathbf{n} & \text{otherwise, } \textit{i.e.,}\ \mathbf{n} \notin \mathcal{N}_\exists \end{cases}$$

$$\alpha_{(i)} := \alpha \qquad \tau_{\mathsf{base}\,(i)} := \tau_{\mathsf{base}} \qquad (\mathsf{ref}\,\tau)_{(i)} := \mathsf{ref}\,\tau_{(i)}$$

$$(\star\alpha.\,\tau)_{(i)} := \star\alpha.\,\tau_{(i)} \quad (\text{where } \star = \mu, \forall, \exists)$$

$$(\tau \star \tau')_{(i)} := \tau_{(i)} \star \tau'_{(i)} \quad (\text{where } \star = \times, +, \to)$$

The encoding of two arbitrary closed types is now implicit in the surjectivity part of the next lemma.

Lemma 2. $\langle (-)_{(1)}, (-)_{(2)} \rangle \in \mathrm{CType} \to \mathrm{CType} \times \mathrm{CType}$ is bijective.

Proof: Injectivity (generalized to open types) can be easily shown by induction on types using two sub-lemmas:

(a) $\forall\tau.\ \tau_{(1)} \sim \tau_{(2)}$, which is shown by straightforward induction on τ.

(b) $\forall\tau.\ \tau_{(1)} \approx \tau_{(2)} \iff \tau \notin \mathcal{N}_\exists$, which is shown by case analysis on τ using (a).

Surjectivity is generalized as follows:

$$\forall\tau_1, \tau_2.\ \tau_1 \sim \tau_2 \implies \exists\tau.\ \tau_{(1)} = \tau_1 \wedge \tau_{(2)} = \tau_2$$

(Note that if τ_1 and τ_2 are closed, the premise holds trivially.) This property can be proven by induction on τ_1. In each case we ask if $\tau_1 \approx \tau_2$ holds. If it does, we use the inductive hypothesis; otherwise, the premise implies that τ_1, τ_2 are closed and thus we can pick τ to be $\mathbf{A}(\tau_1, \tau_2)$. ∎

Now, let us define the *decomposition* of value relations. This will eventually be used to decompose a global knowledge that respects the yet-to-be-defined W into one that respects W_1 and one that respects W_2.

Definition 3. Given $R \in \mathrm{VRelF}$, we define $R_{\{i\}} \in \mathrm{VRelF}$ and $R^*_{(i)} \in W_i.\mathsf{S} \to \mathrm{VRelF}$ (for $i = 1, 2$) as follows.

$$R_{\{1\}} := \{(\tau_{(1)}, v_1, \mathbf{I}(\tau, v_1, v_3)) \mid \tau \in \mathrm{CTyF}^{\setminus\mathcal{N}}_{\setminus\mathsf{ref}} \wedge (v_1, v_3) \in R(\tau)\}$$

$$R_{\{2\}} := \{(\tau_{(2)}, \mathbf{I}(\tau, v_1, v_3), v_3) \mid \tau \in \mathrm{CTyF}^{\setminus\mathcal{N}}_{\setminus\mathsf{ref}} \wedge (v_1, v_3) \in R(\tau)\}$$

$$R^*_{(i)}(s) := [W_i.\mathsf{L}(s)]^*_{(R_{\{i\}})}$$

Here,

- $\mathrm{CTyF}^{\setminus\mathcal{N}}_{\setminus\mathsf{ref}}$ means $\mathrm{CTypeF} \setminus (\mathcal{N} \cup \{\mathsf{ref}\,\tau \in \mathrm{CType}\})$,
- $[F]^*_R$ denotes the least fixed-point of the monotone function $F(-) \cup R$, thus making $R^*_{(i)}$ the smallest global knowledge that both respects W_i and contains $R_{\{i\}}$, and
- $\mathbf{I}$ is an injective function in $\mathrm{CType} \times \mathrm{CVal} \times \mathrm{CVal} \to \mathbb{N}$.

With the help of this, we can now construct the world W in Figure 8. Its well-formedness is easy to check. Note that, although W only actually defines names from $\mathcal{N}_\exists$, we declare that it owns the larger set $\mathcal{N}$ in order to reduce the set of global knowledges that we have to worry about.

Next, some notation for decomposing a global knowledge.

Definition 4. Given $G \in \mathrm{GK}(W)$, we define

$$
\begin{array}{ll}
W.\mathsf{N} & := \mathcal{N} \\
W.\mathsf{S} & := W_1.\mathsf{S} \times W_2.\mathsf{S} \\
W.\sqsubseteq & := \{\, (p,p') \mid p.1 \sqsubseteq p'.1 \wedge p.2 \sqsubseteq p'.2 \,\} \\
W.\mathsf{L}(s_1,s_2)(R)(\tau) & := \begin{cases} \overline{R^*_{(1)}(s_1)}(\tau_{(1)}) \circ \overline{R^*_{(2)}(s_2)}(\tau_{(2)}) & \text{if } \tau \in \mathcal{N}_\exists \\ W_1.\mathsf{L}(s_1)(R^*_{(1)}(s_1))(\tau_{(1)}) \\ \quad \circ W_2.\mathsf{L}(s_2)(R^*_{(2)}(s_2))(\tau_{(2)}) & \text{if } \tau \notin \mathcal{N}_\exists \end{cases} \\
W.\mathsf{H}(s_1,s_2)(R) & := W_1.\mathsf{H}(s_1)(R^*_{(1)}(s_1)) \circ W_2.\mathsf{H}(s_2)(R^*_{(2)}(s_2))
\end{array}
$$

Figure 8. Construction of $W \in \text{World}$.

$G^{s_2}_{(1)} \in W_1.\mathsf{S} \to \text{VRelF}$ for $s_2 \in W_2.\mathsf{S}$,
and $G^{s_1}_{(2)} \in W_2.\mathsf{S} \to \text{VRelF}$ for $s_1 \in W_1.\mathsf{S}$ as follows:

$$G^{s_2}_{(1)}(s) := G(s,s_2)^*_{(1)}(s) \qquad G^{s_1}_{(2)}(s) := G(s_1,s)^*_{(2)}(s)$$

Note that if the global knowledge argument R in the definition of $W.\mathsf{L}$ and $W.\mathsf{H}$ is of the form $G(s_1,s_2)$ for $G \in \text{GK}(W)$, then the global knowledge passed to $W_1.\mathsf{L}$ and $W_1.\mathsf{H}$ is exactly $G^{s_2}_{(1)}(s_1)$ (and similarly for W_2). It remains to show that $G^{s_2}_{(1)}(s_1)$ and $G^{s_1}_{(2)}(s_2)$ are in fact valid global knowledges that respect W_1 and W_2, respectively:

Lemma 3. $\forall G \in \text{GK}(W)$.

$$\forall s_2.\ G^{s_2}_{(1)} \in \text{GK}(W_1) \ \wedge\ \forall s_1.\ G^{s_1}_{(2)} \in \text{GK}(W_2)$$

Proof: We show the first conjunct (the second is analogous). Monotonicity of $G^{s_2}_{(1)}$ is proven by fixed-point induction using the fact that G, $(-)_{\{1\}}$ and $W_1.\mathsf{L}$ are monotone. $G^{s_2}_{(1)}(s_1) \geq^{W_1.\mathsf{N}}_{\text{ref}} W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))$ follows from $G^{s_2}_{(1)}(s_1)(\tau) = W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau) \cup G(s_1,s_2)_{\{1\}}(\tau)$. (Note that $G(s_1,s_2)_{\{1\}}(\tau) = \emptyset$ if τ is a reference type or a name in $W_1.\mathsf{N} = \mathcal{N}_1 \subseteq \mathcal{N}$.) ∎

We now come to the main lemma of this part, namely the conjunction of properties (3) and (5) from Section V-A:

Lemma 4. $\forall G \in \text{GK}(W).\ \forall \tau \in \text{CType}.\ \forall s_1, s_2.$

$$\overline{G^{s_2}_{(1)}(s_1)}(\tau_{(1)}) \circ \overline{G^{s_1}_{(2)}(s_2)}(\tau_{(2)}) = \overline{G(s_1,s_2)}(\tau)$$

Proof: The $\supseteq$ part is proven by fixed-point induction on $\overline{G(s_1,s_2)}$ (recall that $\overline{(-)}$ is defined as a least fixed-point). The $\subseteq$ part is equivalent to

$$\begin{array}{l}
\overline{G^{s_2}_{(1)}(s_1)}(\tau) \quad\subseteq\quad \{(v_1,v_2) \mid \forall \sigma, v_3. \\
\quad (\tau = \sigma_{(1)} \wedge (v_2,v_3) \in \overline{G^{s_1}_{(2)}(s_2)}(\sigma_{(2)})) \Longrightarrow (v_1,v_3) \in \overline{G(s_1,s_2)}(\sigma)\}
\end{array}$$

which is proven by (generalized) induction on $\overline{G^{s_2}_{(1)}(s_1)}$.

Base cases. In both parts, the base cases follow from

$$\begin{array}{l}
\forall G \in \text{GK}(W).\ \forall \tau \in \text{CTypeF}.\ \forall s_1, s_2. \\
\quad \overline{G^{s_2}_{(1)}(s_1)}(\tau_{(1)}) \circ \overline{G^{s_1}_{(2)}(s_2)}(\tau_{(2)}) = G(s_1,s_2)(\tau)
\end{array}$$

which we now show by case analysis on τ. If $\tau \in \mathcal{N}_\exists$, then

$$\begin{array}{lll}
G(s_1,s_2)(\tau) & = W.\mathsf{L}(s_1,s_2)(G(s_1,s_2))(\tau) & (G \in \text{GK}(W)) \\
& = \overline{G^{s_2}_{(1)}(s_1)}(\tau_{(1)}) \circ \overline{G^{s_1}_{(2)}(s_2)}(\tau_{(2)}) & (\text{def. of } W.\mathsf{L})
\end{array}$$

and we are done. Otherwise ($\tau \in \text{CTypeF} \setminus \mathcal{N}_\exists$), we have:

$$\begin{array}{l}
\quad \overline{G^{s_2}_{(1)}(s_1)}(\tau_{(1)}) \circ \overline{G^{s_1}_{(2)}(s_2)}(\tau_{(2)}) \\
= G^{s_2}_{(1)}(s_1)(\tau_{(1)}) \circ G^{s_1}_{(2)}(s_2)(\tau_{(2)}) \\
= (W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \cup G(s_1,s_2)_{\{1\}}(\tau_{(1)})) \circ \\
\quad (W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)}) \cup G(s_1,s_2)_{\{2\}}(\tau_{(2)})) \qquad (7)
\end{array}$$

Now, if τ is a reference type or a name from $\mathcal{N}_1 \uplus \mathcal{N}_2$, we finish by rewriting (7) as follows:

$$\begin{array}{lll}
& (W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \cup \emptyset) \circ \\
& \quad (W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)}) \cup \emptyset) & (\text{def. of } (-)_{\{i\}}) \\
= & W.\mathsf{L}(s_1,s_2)(G(s_1,s_2))(\tau) & (\text{def. of } W.\mathsf{L}) \\
= & G(s_1,s_2)(\tau) & (G \in \text{GK}(W))
\end{array}$$

Otherwise ($\tau \in \text{CTyF}^{\setminus\mathcal{N}}_{\setminus\text{ref}}$), we continue by distributing $\circ$ over $\cup$ in (7):

$$\begin{array}{l}
\quad (W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \circ W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)})) \\
\cup\ (G(s_1,s_2)_{\{1\}}(\tau_{(1)}) \circ G(s_1,s_2)_{\{2\}}(\tau_{(2)})) \\
\cup\ (W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \circ G(s_1,s_2)_{\{2\}}(\tau_{(2)})) \\
\cup\ (G(s_1,s_2)_{\{1\}}(\tau_{(1)}) \circ W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)}))
\end{array} \qquad (8)$$

The first disjunct equals $W.\mathsf{L}(s_1,s_2)(G(s_1,s_2))(\tau)$ by construction of W; the second equals $G(s_1,s_2)(\tau)$ by construction of $(-)_{\{i\}}$, injectivity of $\mathbf{I}$ and the injectivity part of Lemma 2; and the third and the fourth are empty by construction of $(-)_{\{i\}}$ and the fact that $W_i.\mathsf{L}(s)(R) \in \text{WfKnow}(W_i.\mathsf{N})$ for any s, R. So, (8) becomes $W.\mathsf{L}(s_1,s_2)(G(s_1,s_2))(\tau) \cup G(s_1,s_2)(\tau)$. As $G \in \text{GK}(W)$, the second disjunct contains the first, and we are done.

Inductive cases. In both parts, the inductive cases boil down to showing that for any $R_1, R_2, R \in \text{VRelF}$ and $S_1, S_2 \in \text{VRel}$ and $\tau \notin \text{CTypeF}$ the equation

$$F_{R_1}(S_1)(\tau_{(1)}) \circ F_{R_2}(S_2)(\tau_{(2)}) = F_R(S_1 \bullet S_2)(\tau)$$

holds, where $F_R \in \text{VRel} \to \text{VRel}$ denotes the monotone generating function of $\overline{R}$ (*i.e.,* the function of which $\overline{R}$ is least fixed-point), and $(S_1 \bullet S_2)(\tau) := S_1(\tau_{(1)}) \circ S_2(\tau_{(2)})$. This is straightforward to show by case analysis on τ. The only really interesting case is for existential types, where (in one direction) we are given two witness types τ_1 and τ_2 and then apply Lemma 2 to find a witness type τ satisfying $\tau_{(1)} = \tau_1$ and $\tau_{(2)} = \tau_2$. ∎

Finally, we can prove transitivity of $\mathbf{E}$ and then the original goal of this first part.

Lemma 5. $\forall G \in \text{GK}(W).\ \forall \tau \in \text{CType}.\ \forall s_1, s_2.$

$$\mathbf{E}_{W_1}(G^{s_2}_{(1)})(s_1)(\tau_{(1)}) \circ \mathbf{E}_{W_2}(G^{s_1}_{(2)})(s_2)(\tau_{(2)}) \subseteq \mathbf{E}_W(G)(s_1,s_2)(\tau)$$

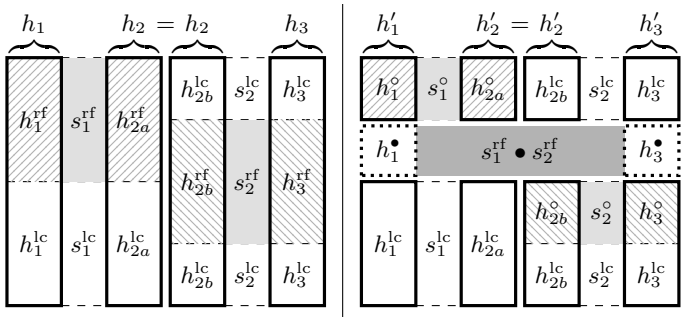
Proof: By coinduction, following the sketch in Section V-A (and choosing the middle frame heap, h^{F}_2, to be empty). ∎

Lemma 6. $\Delta; \Gamma \vdash e_1 \sim_W e_3 : \tau$

Proof: Inhabitation of W follows easily from that of W_1 and W_2 and the construction of $W.\mathsf{H}$. The proofs of consistency and relatedness of (e_1, e_3) by $\mathbf{OE}_W$ are very similar and straightforward, using Lemmas 4 and 5. ∎

VI. Second Part: Constructing the Corresponding Local World w

We now come to the second part of our transitivity proof. Conceptually it is quite simple, but the formal details are very subtle. Recall that we basically want to create a world that relates the same things as W from the previous section, but has the shape of a lifted world, *i.e.,* has the form $w\uparrow$.



Heap structure enforced by W | Heap structure enforced by $w\!\uparrow$

$w.\mathsf{N} := W.\mathsf{N} \qquad w.\mathsf{S} := W.\mathsf{S} \qquad w.\sqsubseteq := W.\sqsubseteq$
$w.\mathsf{L}(s^{\mathrm{rf}})(s)(R)(\tau) := \{(v_1, v_3) \in W.\mathsf{L}(s)(R)(\tau) \mid \tau \neq \mathsf{ref}\,(\_)\}$
$w.\mathsf{H}(s^{\mathrm{rf}})(s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}}, s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}})(R) := \{\,(h_1', h_3') \mid s^{\mathrm{rf}} = s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}} \wedge$
$\exists h_1^\circ, h_1^{\mathrm{lc}}, h_{2a}^\circ, h_{2a}^{\mathrm{lc}}, h_{2b}^\circ, h_{2b}^{\mathrm{lc}}, h_3^\circ, h_3^{\mathrm{lc}}.$
$h_1' = h_1^\circ \uplus h_1^{\mathrm{lc}} \wedge h_{2a}^\circ \uplus h_{2a}^{\mathrm{lc}} = h_{2b}^\circ \uplus h_{2b}^{\mathrm{lc}} \wedge h_3' = h_3^\circ \uplus h_3^{\mathrm{lc}} \wedge$
$\mathrm{dom}(h_{2a}^{\mathrm{lc}}) \cap \mathrm{dom}_{[2]}(s_1^{\mathrm{rf}}) = \mathrm{dom}(h_{2b}^{\mathrm{lc}}) \cap \mathrm{dom}_{[1]}(s_2^{\mathrm{rf}}) = \emptyset \wedge$
$(h_1^\circ, h_{2a}^\circ) \in W_{\mathrm{ref}}.\mathsf{H}(s_1^\circ)(R^*_{(1)}(s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}})) \wedge$
$(h_{2b}^\circ, h_3^\circ) \in W_{\mathrm{ref}}.\mathsf{H}(s_2^\circ)(R^*_{(2)}(s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}})) \wedge$
$(h_1^{\mathrm{lc}}, h_{2a}^{\mathrm{lc}}) \in w_1.\mathsf{H}(s_1^{\mathrm{rf}})(s_1^{\mathrm{lc}})(R^*_{(1)}(s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}})) \wedge$
$(h_{2b}^{\mathrm{lc}}, h_3^{\mathrm{lc}}) \in w_2.\mathsf{H}(s_2^{\mathrm{rf}})(s_2^{\mathrm{lc}})(R^*_{(2)}(s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}}))\,\}$
where $s_i^\circ = \{(\tau, \ell_1, \ell_2) \in s_i^{\mathrm{rf}} \mid \ell_i \notin \mathrm{dom}_{[i]}(s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}})\}$ for $i = 1,2$

Figure 9. Construction of a stable local world $w \in \mathrm{LWorld}$ such that $w\!\uparrow$ is weakly isomorphic to W.

By definition, the state space of a lifted world is of the form $W_{\mathrm{ref}}.\mathsf{S} \times \ldots$, and thus cannot be the same as W's state space $(W_{\mathrm{ref}}.\mathsf{S} \times w_1.\mathsf{S}) \times (W_{\mathrm{ref}}.\mathsf{S} \times w_2.\mathsf{S})$. Recall further that a world's local knowledge and heap relation are state-dependent. So, in order to characterize what it means for two worlds with different state spaces to "relate the same things", we need to introduce a notion of *world isomorphism*.

A. World Isomorphisms

Roughly, two (full) worlds W_a, W_b are isomorphic iff they declare the same type names, and each state of W_a corresponds to a state of W_b (and vice versa) such that the the same values and heaps are related at corresponding states. Different kinds of isomorphism arise depending on what counts as a correspondence. For our purpose, a one-to-one correspondence is too strong. If, say, W_b contains an "inconsistent" state (*i.e.,* a state at which W_b's heap relation is empty), then we should not have to worry about finding a similarly irrelevant state in W_a. So, instead of a full one-to-one correspondence, we use a *partial* one, wherein a state s in one world is permitted to have no correspondent in the other iff s is inconsistent. This plays a crucial role in our transitivity proof, as we will see in a moment.

Definition 5. For any $W_a, W_b \in \mathrm{World}$, a pair of functions $\phi \in W_a.\mathsf{S} \to \mathbb{P}(W_b.\mathsf{S})$ and $\psi \in W_b.\mathsf{S} \to \mathbb{P}(W_a.\mathsf{S})$ form a *weak isomorphism*, written $\phi : W_a \cong W_b : \psi$, if:

(1) $W_a.\mathsf{N} = W_b.\mathsf{N}$
(2a) $\forall s_a, s_a'.\forall s_b \in \phi(s_a), s_b' \in \phi(s_a').\ s_a \sqsubseteq s_a' \implies s_b \sqsubseteq s_b'$
(3a) $\forall s_a.\forall s_b \in \phi(s_a).\ W_a.\mathsf{L}(s_a) = W_b.\mathsf{L}(s_b)$
(4a) $\forall s_a.\forall G \in \mathrm{GK}(W_a).$
$W_b.\mathsf{H}(s_a)(G(s_a)) \subseteq \bigcup_{s_b \in \phi(s_a)} W_b.\mathsf{H}(s_b)(G(s_a))$
(5a) $\forall s_a.\forall s_b \in \phi(s_a).\forall s_a' \in \psi(s_b).\ s_a \sqsubseteq s_a'$

(2b)–(5b) symmetric to (2a)–(5a)

Note that full worlds and weak morphisms—*i.e.,* ϕ satisfying (1), (2a), (3a), and (4a)—form a category.

Theorem 7. If $\phi : W_a \cong W_b : \psi$, then: $\forall \Delta, \Gamma, \tau, e_1, e_2.$

$$\Delta; \Gamma \vdash e_1 \sim_{W_a} e_2 : \tau \iff \Delta; \Gamma \vdash e_1 \sim_{W_b} e_2 : \tau$$

Proof: See Theorem 84 in the appendix. ∎

B. Defining w

Recall that lifting a local world means linking it with the shared world W_{ref}, which provides the meaning of reference types. Accordingly, the to-be-constructed local world w's knowledge must not relate anything at reference types, and, in order for $w\!\uparrow$ to be isomorphic to W, must correspond to $W.\mathsf{L}$ at all other types. This is easy to achieve by just choosing w's state space to be the same as W's and then defining $w.\mathsf{L}(s^{\mathrm{rf}})(s)$ to be $W.\mathsf{L}(s)$ for non-reference types. Regarding reference types, we have to satisfy (by the definition of lifting):

$$W_{\mathrm{ref}}.\mathsf{L}(s^{\mathrm{rf}})(R)(\mathsf{ref}\,\tau) = W.\mathsf{L}(s)(R)(\mathsf{ref}\,\tau)$$

This is problematic. Note that s really has the form $((s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}}), (s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}}))$ (we will later omit the inner parentheses for convenience), with $s_1^{\mathrm{rf}}, s_2^{\mathrm{rf}}$ being states of W_{ref}, and $s_1^{\mathrm{lc}}, s_2^{\mathrm{lc}}$ being states of w_1, w_2, respectively. Unfolding the definition of $W.\mathsf{L}$, the above equation is equivalent to

$$W_{\mathrm{ref}}.\mathsf{L}(s^{\mathrm{rf}})(R)(\mathsf{ref}\,\tau) = W_{\mathrm{ref}}.\mathsf{L}(s_1^{\mathrm{rf}})(R^*_{(1)}(s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}}))(\mathsf{ref}\,\tau_{(1)}) \circ W_{\mathrm{ref}}.\mathsf{L}(s_2^{\mathrm{rf}})(R^*_{(2)}(s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}}))(\mathsf{ref}\,\tau_{(2)})$$

which in turn reduces to $s^{\mathrm{rf}} = s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}}$, where

$$s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}} := \{(\tau, \ell_1, \ell_3) \mid \exists \ell_2.\ (\tau_{(1)}, \ell_1, \ell_2) \in s_1^{\mathrm{rf}} \wedge (\tau_{(2)}, \ell_2, \ell_3) \in s_2^{\mathrm{rf}}\}.$$

This clearly cannot be true in general as all three states may be arbitrary. Remember, however, that we do not have to worry about inconsistent states! So the solution is easy: in the states where the equation holds—*i.e.,* where s^{rf} and s are *coherent*—we are fine; we just need to make sure that in any other case the heap relation is empty. And since w's heap relation may depend on the shared state s^{rf}, this can be easily done. Accordingly, the $w\!\uparrow$ state corresponding to s will be $(s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}}, s)$, and the W state corresponding to (s^{rf}, s) will be s—but only if s^{rf} happens to be $s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}}$.

What should $w.\mathsf{H}$ relate when $s^{\mathrm{rf}} = s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}}$ *does* hold? For such states, we want the following equation to be true (ignoring the global knowledge parameter to avoid clutter):

$$w\!\uparrow.\mathsf{H}(s^{\mathrm{rf}}, s) = W.\mathsf{H}(s) \tag{9}$$

Let us look at what we know about heaps (h_1, h_3) related by $W.\mathsf{H}(s)$. First, by construction of W, there is some h_2 mediating between $w_1\!\uparrow$ and $w_2\!\uparrow$. By definition of lifting, h_1 and h_2 can be split between $W_{\mathrm{ref}}.\mathsf{H}(s_1^{\mathrm{rf}})$ and $w_1.\mathsf{H}(s_1^{\mathrm{rf}})(s_1^{\mathrm{lc}})$,

and similarly h_2 and h_3 can be split between $W_{\text{ref}}.\mathsf{H}(s_2^{\text{rf}})$ and $w_2.\mathsf{H}(s_2^{\text{rf}})(s_2^{\text{lc}})$. Of course, in general the two splits of h_2 may be arbitrarily different. This situation is depicted in the first diagram of Figure 9.

Note that $w{\uparrow}.\mathsf{H}(s^{\text{rf}}, s)$ in (9) unfolds to $W_{\text{ref}}.\mathsf{H}(s^{\text{rf}}) \otimes w.\mathsf{H}(s^{\text{rf}})(s)$. So basically all we have to do is to define $w.\mathsf{H}(s^{\text{rf}})(s)$ to be the "septraction" [13] of $W_{\text{ref}}.\mathsf{H}(s^{\text{rf}})$ from $W.\mathsf{H}(s)$. The way we do this is essentially by describing, in the definition of $w.\mathsf{H}$, the situation from the figure but leaving out the pieces related by $W_{\text{ref}}.\mathsf{H}(s^{\text{rf}})$. This is shown in the second diagram of Figure 9: $w.\mathsf{H}$ relates heaps h_1', h_3' iff $h_i' = h_i^{\text{lc}} \uplus h_i^{\circ}$, where h_i° is the sub-heap of h_i^{rf} not covered by $s^{\text{rf}} = s_1^{\text{rf}} \bullet s_2^{\text{rf}}$. The missing pieces, $h_1^{\bullet}$ and $h_3^{\bullet}$, are then going to be related by $W_{\text{ref}}.\mathsf{H}(s^{\text{rf}})$ when w is lifted.

Formally, $w.\mathsf{H}$ is defined as shown on the right in Figure 9, together with the other components of w. As explained, it is empty whenever s^{rf} is not compatible with s_1^{rf} and s_2^{rf}. The sub-heap h_1° (and similarly h_3°) is characterized by saying that it is related by W_{ref} to a sub-heap h_{2a}° of h_{2a}^{rf} at the state obtained by essentially subtracting those parts from s_1^{rf} that are involved in $s_1^{\text{rf}} \bullet s_2^{\text{rf}}$.

C. Showing w's Stability

The well-formedness of w is fairly easy to check, but proving w stable is non-trivial (because $w.\mathsf{H}$'s dependency on s^{rf} is non-trivial). Recall that stability is crucial for soundness, as it ensures that a local world's dependency on the shared state is compatible with any changes to that state.

Definition 6. For $G \in \text{GK}(w{\uparrow})$, we define $\overleftarrow{G} \in W.\mathsf{S} \to \text{VRelF}$ as follows:

$$\overleftarrow{G}(s_1^{\text{rf}}, s_1^{\text{lc}}, s_2^{\text{rf}}, s_2^{\text{lc}}) := G(s_1^{\text{rf}} \bullet s_2^{\text{rf}}, (s_1^{\text{rf}}, s_1^{\text{lc}}, s_2^{\text{rf}}, s_2^{\text{lc}}))$$

Note that the fact that $s_1^{\text{rf}} \bullet s_2^{\text{rf}}$ is a valid W_{ref} state (*i.e.,* a partial bijection) relies on the injectivity part of Lemma 2.

Lemma 8. $\forall G \in \text{GK}(w{\uparrow}).\ \overleftarrow{G} \in \text{GK}(W)$

Lemma 9. $stable(w)$

Proof: Suppose that $G \in \text{GK}(w{\uparrow})$, $s = (s_1^{\text{rf}}, s_1^{\text{lc}}, s_2^{\text{rf}}, s_2^{\text{lc}})$, $\hat{s}^{\text{rf}} \sqsupseteq s^{\text{rf}}$, $\text{defined}(h_1' \uplus \hat{h}_1^{\bullet})$, $\text{defined}(h_3' \uplus \hat{h}_3^{\bullet})$,

$$(h_1', h_3') \in w.\mathsf{H}(s^{\text{rf}})(s)(G(s^{\text{rf}}, s)) \quad (10)$$

$$\text{and} \quad (\hat{h}_1^{\bullet}, \hat{h}_3^{\bullet}) \in W_{\text{ref}}.\mathsf{H}(\hat{s}^{\text{rf}})(G(\hat{s}^{\text{rf}}, s)). \quad (11)$$

Our goal is to find $\hat{s} = (\hat{s}_1^{\text{rf}}, \hat{s}_1^{\text{lc}}, \hat{s}_2^{\text{rf}}, \hat{s}_2^{\text{lc}}) \sqsupseteq s$ such that $(h_1', h_3') \in w.\mathsf{H}(\hat{s}^{\text{rf}})(\hat{s})(G(\hat{s}^{\text{rf}}, \hat{s}))$. The main idea is to use $stable(w_i)$ to obtain $\hat{s}_i^{\text{lc}}$ for $i = 1, 2$.

In order to do so, we must first construct states and heaps needed for instantiation. From (10) we know $s^{\text{rf}} = s_1^{\text{rf}} \bullet s_2^{\text{rf}}$ and that h_1', h_3' are structured as depicted in the diagram of Figure 10. From $\hat{s}^{\text{rf}} \sqsupseteq s^{\text{rf}}$ we know $\hat{s}^{\text{rf}} = s^{\text{rf}} \uplus s^{+}$ for some s^{+}. Thus by (11), $\hat{h}_1^{\bullet}, \hat{h}_3^{\bullet}$ can be split as $\hat{h}_i^{\bullet} = h_i^{\bullet} \uplus h_i^{+}$ such that

$$(h_1^{\bullet}, h_3^{\bullet}) \in W_{\text{ref}}.\mathsf{H}(s^{\text{rf}})(G(\hat{s}^{\text{rf}}, s)) \quad (12)$$

$$\text{and} \quad (h_1^{+}, h_3^{+}) \in W_{\text{ref}}.\mathsf{H}(s^{+})(G(\hat{s}^{\text{rf}}, s)), \quad (13)$$

as depicted in the left part of the diagram in Figure 10.

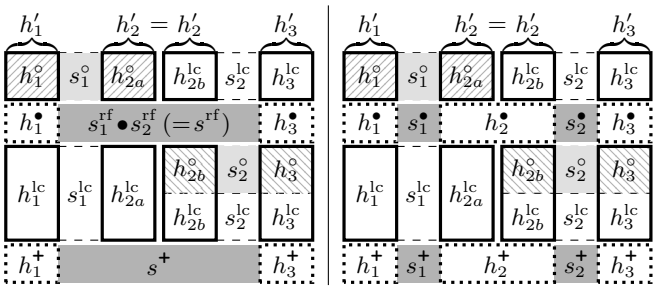


Figure 10. "Horizontal" decomposition of $\hat{s}^{\text{rf}}$ in proof of $stable(w)$.

We will now "horizontally" decompose s^{+} and s^{rf}, as shown in the right part of Figure 10. Since $s_i^{\text{rf}} \sqsupseteq s_i^{\circ}$, there is $s_i^{\bullet}$ such that $s_i^{\text{rf}} = s_i^{\circ} \uplus s_i^{\bullet}$; consequently we have $\text{dom}_{[2]}(s_1^{\bullet}) = \text{dom}_{[1]}(s_2^{\bullet})$ and $s_1^{\bullet} \bullet s_2^{\bullet} = s_1^{\text{rf}} \bullet s_2^{\text{rf}} = s^{\text{rf}}$. To decompose s^{+}, we choose a set of fresh locations L (of appropriate size) for the middle, *i.e.,* we define s_i^{+} such that $s_1^{+} \bullet s_2^{+} = s^{+}$ and $\text{dom}_{[2]}(s_1^{+}) = \text{dom}_{[1]}(s_2^{+}) = L$. We can then define $\hat{s}_i^{\text{rf}}$ (used to instantiate $stable(w_i)$) as $\hat{s}_i^{\text{rf}} := s_i^{\circ} \uplus s_i^{\bullet} \uplus s_i^{+}$, so we have $\hat{s}_1^{\text{rf}} \bullet \hat{s}_2^{\text{rf}} = s^{\text{rf}} \uplus s^{+} = \hat{s}^{\text{rf}}$.

The mediating heaps h_2^{+} (with domain L) and $h_2^{\bullet}$ are constructed as follows. Since $\hat{s}_i^{\text{rf}} \sqsupseteq s_i^{\text{rf}}$, we know

$$\overleftarrow{G}(\hat{s}_1^{\text{rf}}, s_1^{\text{lc}}, \hat{s}_2^{\text{rf}}, s_2^{\text{lc}}) = G(\hat{s}^{\text{rf}}, (\hat{s}_1^{\text{rf}}, s_1^{\text{lc}}, \hat{s}_2^{\text{rf}}, s_2^{\text{lc}})) \sqsupseteq G(\hat{s}^{\text{rf}}, s) \quad (14)$$

by monotonicity of G. From (12), (13), (14), monotonicity of $W_{\text{ref}}.\mathsf{H}$, and Lemmas 8 and 4, we can then find mediating values to construct $h_2^{\bullet}$ and h_2^{+} satisfying (for $\star \in \{\bullet, +\}$)

$$(h_1^{\star}, h_2^{\star}) \in W_{\text{ref}}.\mathsf{H}(s_1^{\star})(\overleftarrow{G}_{(1)}^{(\hat{s}_2^{\text{rf}}, s_2^{\text{lc}})}(\hat{s}_1^{\text{rf}}, s_1^{\text{lc}})) \quad (15)$$

$$\text{and} \quad (h_2^{\star}, h_3^{\star}) \in W_{\text{ref}}.\mathsf{H}(s_2^{\star})(\overleftarrow{G}_{(2)}^{(\hat{s}_1^{\text{rf}}, s_1^{\text{lc}})}(\hat{s}_2^{\text{rf}}, s_2^{\text{lc}})). \quad (16)$$

We will now prepare to instantiate $stable(w_i)$, starting with $stable(w_1)$. First, observe that $\overleftarrow{G}_{(1)}^{(\hat{s}_2^{\text{rf}}, s_2^{\text{lc}})} \in \text{GK}(w_1{\uparrow})$, thanks to Lemmas 8 and 3. Next, by monotonicity of G, we have that (for $\star \in \{\hat{s}_1^{\text{rf}}, s_1^{\text{rf}}\}$)

$$\overleftarrow{G}_{(1)}^{(\hat{s}_2^{\text{rf}}, s_2^{\text{lc}})}(\star, s_1^{\text{lc}}) = \overleftarrow{G}(\star, s_1^{\text{lc}}, \hat{s}_2^{\text{rf}}, s_2^{\text{lc}})_{(1)}^{*} \sqsupseteq G(s^{\text{rf}}, s)_{(1)}^{*}$$

and thus (10), along with monotonicity of $W_{\text{ref}}.\mathsf{H}$ and $w_1.\mathsf{H}$ and the definition of $w.\mathsf{H}$ in Figure 9, gives us:

$$(h_1^{\circ}, h_{2a}^{\circ}) \in W_{\text{ref}}.\mathsf{H}(s_1^{\circ})(\overleftarrow{G}_{(1)}^{(\hat{s}_2^{\text{rf}}, s_2^{\text{lc}})}(\hat{s}_1^{\text{rf}}, s_1^{\text{lc}})) \quad (17)$$

$$\text{and} \quad (h_1^{\text{lc}}, h_{2a}^{\text{lc}}) \in w_1.\mathsf{H}(s_1^{\text{rf}})(s_1^{\text{lc}})(\overleftarrow{G}_{(1)}^{(\hat{s}_2^{\text{rf}}, s_2^{\text{lc}})}(s_1^{\text{rf}}, s_1^{\text{lc}})). \quad (18)$$

Thus, by (15), (17), (18), and $\hat{s}_1^{\text{rf}} \sqsupseteq s_1^{\text{rf}}$, we can instantiate $stable(w_1)$, yielding $\hat{s}_1^{\text{lc}} \sqsupseteq s_1^{\text{lc}}$ such that

$$(h_1^{\text{lc}}, h_{2a}^{\text{lc}}) \in w_1.\mathsf{H}(\hat{s}_1^{\text{rf}})(\hat{s}_1^{\text{lc}})(\overleftarrow{G}_{(1)}^{(\hat{s}_2^{\text{rf}}, s_2^{\text{lc}})}(\hat{s}_1^{\text{rf}}, \hat{s}_1^{\text{lc}})). \quad (19)$$

In a similar manner, $stable(w_2)$ yields $\hat{s}_2^{\text{lc}} \sqsupseteq s_2^{\text{lc}}$ such that

$$(h_{2b}^{\text{lc}}, h_3^{\text{lc}}) \in w_2.\mathsf{H}(\hat{s}_2^{\text{rf}})(\hat{s}_2^{\text{lc}})(\overleftarrow{G}_{(2)}^{(\hat{s}_1^{\text{rf}}, s_1^{\text{lc}})}(\hat{s}_2^{\text{rf}}, \hat{s}_2^{\text{lc}})). \quad (20)$$

Let $\hat{s} := (\hat{s}_1^{\text{rf}}, \hat{s}_1^{\text{lc}}, \hat{s}_2^{\text{rf}}, \hat{s}_2^{\text{lc}})$. Finally, by monotonicity of G, $W_{\text{ref}}.\mathsf{H}$, and $w_i.\mathsf{H}$, and by definition of $w.\mathsf{H}$, we get $(h_1', h_3') \in w.\mathsf{H}(\hat{s}^{\text{rf}})(\hat{s})(\overleftarrow{G}(\hat{s})) = w.\mathsf{H}(\hat{s}^{\text{rf}})(\hat{s})(G(\hat{s}^{\text{rf}}, \hat{s}))$ from (10), (19), and (20), as desired. ∎

D. Proving W and $w\uparrow$ Isomorphic

We now show that W and $w\uparrow$ are weakly isomorphic, and then put all the pieces together, arriving at our goal and thereby finishing the proof of transitivity.

Lemma 10. $\exists \phi, \psi.\ \phi : W \cong w\uparrow : \psi$

Proof: We define $\phi \in W.\mathsf{S} \to \mathbb{P}(w\uparrow.\mathsf{S})$ and $\psi \in w\uparrow.\mathsf{S} \to \mathbb{P}(W.\mathsf{S})$ as follows.

$$\phi(s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}}, s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}}) := \{\, (s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}}, (s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}}, s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}})) \,\}$$

$$\psi(s^{\mathrm{rf}}, (s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}}, s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}})) := \begin{cases} \{(s_1^{\mathrm{rf}}, s_1^{\mathrm{lc}}, s_2^{\mathrm{rf}}, s_2^{\mathrm{lc}})\} & \text{if } s^{\mathrm{rf}} = s_1^{\mathrm{rf}} \bullet s_2^{\mathrm{rf}} \\ \emptyset & \text{otherwise} \end{cases}$$

Showing that ϕ and ψ form a weak isomorphism is mostly straightforward, but for conditions (4a) and (4b) quite tedious. The key idea behind the proofs of these is the same as that behind Lemma 9: splitting the given heaps as depicted in the diagrams of Figure 9. In particular, the proof of (4b) is very similar to that of Lemma 9 in the way it uses the construction $\overleftarrow{G}$ and Lemma 8. ■

Theorem 11 (Transitivity)**.** $\Delta; \Gamma \vdash e_1 \sim e_3 : \tau$

Proof: We have $\Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_3 : \tau$ by Lemmas 6 and 10 and Theorem 7. The result then follows from Lemma 9. ■

VII. Conclusion

In this paper, we have focused on establishing transitive composability of RTSs in a traditional single-language setting—because it is already challenging enough!—but our ultimate goal is to provide a foundation for *inter-language* reasoning. We believe strongly that RTSs should be generalizable to inter-language reasoning because, like SKLRs, RTSs are inherently "semantic" (or "relational"), always quantifying over "related" terms/values without assuming that the related entities share a common syntax. As a starting point, we believe it should be possible (straightforward, even) to adapt Hur and Dreyer's SKLR relating ML and assembly programs [5] to a formulation using RTSs instead.

As for generalizing our RTS transitivity proof to the inter-language setting, we are quite optimistic. The transitivity proof is *direct—i.e.,* it does not exploit contextual equivalence internally—and the first part of the proof makes few assumptions about the "middle" language (from which e_2 is drawn) except that it is capable of encoding the $\mathbf{I}$ function from Section V-A. The key challenge will be in adapting the second part of the proof to the case where the W_{ref}'s in the proofs of $e_1 \sim e_2$ and $e_2 \sim e_3$ are of different shapes (because the languages involved have different memory models).

References

[1] A. Ahmed, "Step-indexed syntactic logical relations for recursive and quantified types," in *ESOP*, 2006.

[2] A. Ahmed, D. Dreyer, and A. Rossberg, "State-dependent representation independence," in *POPL*, 2009.

[3] N. Benton and C.-K. Hur, "Biorthogonality, step-indexing and compiler correctness," in *ICFP*, 2009.

[4] D. Dreyer, G. Neis, and L. Birkedal, "The impact of higher-order state and control effects on local relational reasoning," in *ICFP*, 2010.

[5] C.-K. Hur and D. Dreyer, "A Kripke logical relation between ML and assembly," in *POPL*, 2011.

[6] C.-K. Hur, D. Dreyer, G. Neis, and V. Vafeiadis, "The marriage of bisimulations and Kripke logical relations," in *POPL*, 2012.

[7] J. C. Reynolds, "Types, abstraction, and parametric polymorphism," *Information Processing*, 1983.

[8] D. Sangiorgi, N. Kobayashi, and E. Sumii, "Environmental bisimulations for higher-order languages," *TOPLAS*, vol. 33, no. 1, pp. 1–69, Jan. 2011.

[9] K. Støvring and S. Lassen, "A complete, co-inductive syntactic theory of sequential control and state," in *POPL*, 2007.

[10] E. Sumii, "A complete characterization of observational equivalence in polymorphic λ-calculus with general references," in *CSL*, 2009.

[11] E. Sumii, "A bisimulation-like proof method for contextual properties in untyped λ-calculus with references and deallocation," *TCS*, vol. 411, no. 51–52, pp. 4358–4378, Dec. 2011.

[12] E. Sumii and B. Pierce, "A bisimulation for type abstraction and recursion," *JACM*, vol. 54, no. 5, pp. 1–43, Oct. 2007.

[13] V. Vafeiadis and M. Parkinson, "A marriage of rely/guarantee and separation logic," in *CONCUR*, 2007.

APPENDIX

A. Language

We define the language $\mathsf{F}^{\mu!}$.

1) Syntax.

$\ell \in \mathrm{Loc}$
$x \in \mathrm{Var}$
$\alpha \in \mathrm{TyVar}$

$$\begin{aligned}
\sigma \in \mathrm{Typ} \quad &::= \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \mathsf{bool} \mid \sigma_1 \times \sigma_2 \mid \sigma_1 + \sigma_2 \mid \sigma_1 \to \sigma_2 \mid \mu\alpha.\,\sigma \mid \forall\alpha.\,\sigma \mid \exists\alpha.\,\sigma \mid \mathsf{ref}\,\sigma \\
v \in \mathrm{Val} \quad &::= x \mid \langle\rangle \mid n \mid \mathsf{tt} \mid \mathsf{ff} \mid \langle v_1, v_2\rangle \mid \mathsf{inj}^1\, v \mid \mathsf{inj}^2\, v \mid \mathsf{roll}\ v \mid \\
&\quad \mathsf{fix}\, f(x).\, e \mid \Lambda.\, e \mid \mathsf{pack}\ v \mid \ell \\
e \in \mathrm{Exp} \quad &::= v \mid \mathsf{if}\ e_0\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \langle e_1, e_2\rangle \mid e.1 \mid e.2 \mid \mathsf{inj}^1\, e \mid \mathsf{inj}^2\, e \mid \\
&\quad (\mathsf{case}\, e\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_1 \,|\, \mathsf{inj}^2\, x \Rightarrow e_2) \mid \mathsf{roll}\ e \mid \mathsf{unroll}\ e \mid e_1\ e_2 \mid e[] \mid \mathsf{pack}\ e \mid \\
&\quad \mathsf{unpack}\ e_1\ \mathsf{as}\ x\ \mathsf{in}\ e_2 \mid \mathsf{ref}\ e \mid\ !e \mid e_1 := e_2 \mid e_1 == e_2 \\
K \in \mathrm{Cont} \quad &::= \bullet \mid \mathsf{if}\ K\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \langle K, e\rangle \mid \langle v, K\rangle \mid K.1 \mid K.2 \mid \mathsf{inj}^1\, K \mid \mathsf{inj}^2\, K \mid \\
&\quad \mathsf{case}\, K\, \mathsf{of}[\mathsf{inj}^i\, x \Rightarrow e_i] \mid \mathsf{roll}\ K \mid \mathsf{unroll}\ K \mid K\ e \mid v\ K \mid K[] \mid \mathsf{pack}\ K \mid \\
&\quad \mathsf{unpack}\ K\ \mathsf{as}\ x\ \mathsf{in}\ e \mid \mathsf{ref}\ K \mid\ !K \mid K := e \mid v := K \mid K == e \mid v == K \\
p \in \mathrm{Prog} \quad &::= x \mid \langle\rangle \mid n \mid \mathsf{tt} \mid \mathsf{ff} \mid \mathsf{if}\ p_0\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2 \mid \langle p_1, p_2\rangle \mid p.1 \mid p.2 \mid \mathsf{inj}^1_\sigma\, p \mid \mathsf{inj}^2_\sigma\, p \mid \\
&\quad (\mathsf{case}\, p\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow p_1 \,|\, \mathsf{inj}^2\, x \Rightarrow p_2) \mid \mathsf{roll}_\sigma\ p \mid \mathsf{unroll}\ p \mid \mathsf{fix}\, f(x{:}\sigma_1){:}\sigma_2.\, p \mid p_1\ p_2 \mid \Lambda\alpha.\, p \mid \\
&\quad p[\sigma] \mid \mathsf{pack}\ \langle \sigma, p\rangle\ \mathsf{as}\ \exists\alpha.\,\sigma' \mid \mathsf{unpack}\ p_1\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ p_2 \mid \mathsf{ref}\ p \mid\ !p \mid p_1 := p_2 \mid p_1 == p_2 \\
h \in \mathrm{Heap} \quad &:= \mathrm{Loc} \xrightarrow{\text{fin}} \mathrm{CVal}
\end{aligned}$$

2) Dynamic Semantics.

$$\begin{aligned}
h, \mathsf{if}\ \mathsf{tt}\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 &\hookrightarrow h, e_1 \\
h, \mathsf{if}\ \mathsf{ff}\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 &\hookrightarrow h, e_2 \\
h, \langle v_1, v_2\rangle.i &\hookrightarrow h, v_i \\
h, \mathsf{case}\, \mathsf{inj}^j\, v\, \mathsf{of}[\mathsf{inj}^i\, x \Rightarrow e_i] &\hookrightarrow h, e_j[v/x] \\
h, (\mathsf{fix}\, f(x).\, e)\ v &\hookrightarrow h, e[(\mathsf{fix}\, f(x).\, e)/f, v/x] \\
h, (\Lambda.\, e)[] &\hookrightarrow h, e \\
h, \mathsf{unpack}\ (\mathsf{pack}\ v)\ \mathsf{as}\ x\ \mathsf{in}\ e &\hookrightarrow h, e[v/x] \\
h, \mathsf{unroll}\ (\mathsf{roll}\ v) &\hookrightarrow h, v \\
h, \mathsf{ref}\ v &\hookrightarrow h \uplus [\ell{\mapsto}v], \ell \qquad \text{where } \ell \notin \mathrm{dom}(h) \\
h \uplus [\ell{\mapsto}v], !\ell &\hookrightarrow h \uplus [\ell{\mapsto}v], v \\
h \uplus [\ell{\mapsto}v], \ell := v' &\hookrightarrow h \uplus [\ell{\mapsto}v'], \langle\rangle \\
h, \ell == \ell &\hookrightarrow h, \mathsf{tt} \\
h, \ell == \ell' &\hookrightarrow h, \mathsf{ff} \qquad \text{where } \ell \neq \ell' \\
h, K[e] &\hookrightarrow h', K[e'] \qquad \text{where } h, e \hookrightarrow h', e'
\end{aligned}$$

3) Static Semantics.

$$\begin{array}{lrcl}
\text{Type environments} & \Delta & ::= & \cdot \mid \Delta, \alpha \\
\text{Term environments} & \Gamma & ::= & \cdot \mid \Gamma, x{:}\sigma
\end{array}$$

$\boxed{\Delta \vdash \sigma}$

$$\frac{\mathrm{fv}(\sigma) \subseteq \Delta \quad \mathrm{names}(\sigma) = \emptyset}{\Delta \vdash \sigma}$$

$\boxed{\Delta \vdash \Gamma}$

$$\frac{\forall x{:}\sigma \in \Gamma.\ \Delta \vdash \sigma}{\Delta \vdash \Gamma}$$

$\boxed{\Delta; \Gamma \vdash p : \sigma}$

$$\frac{\Delta \vdash \Gamma \quad x{:}\sigma \in \Gamma}{\Delta; \Gamma \vdash x : \sigma} \qquad \frac{\Delta \vdash \Gamma}{\Delta; \Gamma \vdash c : \tau_{\text{base}}}$$

$$\frac{\Delta;\Gamma \vdash p_1 : \sigma_1 \quad \Delta;\Gamma \vdash p_2 : \sigma_2}{\Delta;\Gamma \vdash \langle p_1, p_2\rangle : \sigma_1 \times \sigma_2} \qquad \frac{\Delta;\Gamma \vdash p : \sigma_1 \times \sigma_2}{\Delta;\Gamma \vdash p.1 : \sigma_1} \qquad \frac{\Delta;\Gamma \vdash p : \sigma_1 \times \sigma_2}{\Delta;\Gamma \vdash p.2 : \sigma_2}$$

$$\frac{\Delta;\Gamma, x{:}\sigma_1 \vdash p : \sigma_2}{\Delta;\Gamma \vdash \lambda x{:}\sigma_1.\, p : \sigma_1 \to \sigma_2} \qquad \frac{\Delta;\Gamma \vdash p_1 : \sigma_1 \to \sigma_2 \quad \Delta;\Gamma \vdash p_2 : \sigma_1}{\Delta;\Gamma \vdash p_1\ p_2 : \sigma_2}$$

$$\frac{\Delta, \alpha;\Gamma \vdash p : \sigma}{\Delta;\Gamma \vdash \Lambda\alpha.\, p : \forall\alpha.\, \sigma} \qquad \frac{\Delta;\Gamma \vdash p : \forall\alpha.\, \sigma_1 \quad \Delta \vdash \sigma_2}{\Delta;\Gamma \vdash p[\sigma_2] : \sigma_1[\sigma_2/\alpha]}$$

$$\frac{\Delta \vdash \sigma_1 \quad \Delta;\Gamma \vdash p : \sigma_2[\sigma_1/\alpha]}{\Delta;\Gamma \vdash \mathsf{pack}\ \langle \sigma_1, p\rangle\ \mathsf{as}\ \exists\alpha.\, \sigma_2 : \exists\alpha.\, \sigma_2} \qquad \frac{\Delta;\Gamma \vdash p_1 : \exists\alpha.\, \sigma_1 \quad \Delta, \alpha;\Gamma, x{:}\sigma_1 \vdash p_2 : \sigma_2 \quad \Delta \vdash \sigma_2}{\Delta;\Gamma \vdash \mathsf{unpack}\ p_1\ \mathsf{as}\ \langle \alpha, x\rangle\ \mathsf{in}\ p_2 : \sigma_2}$$

$$\frac{\Delta;\Gamma \vdash p : \sigma[\mu\alpha.\, \sigma/\alpha]}{\Delta;\Gamma \vdash \mathsf{roll}_{\mu\alpha.\,\sigma}\ p : \mu\alpha.\, \sigma} \qquad \frac{\Delta;\Gamma \vdash p : \mu\alpha.\, \sigma}{\Delta;\Gamma \vdash \mathsf{unroll}\ p : \sigma[\mu\alpha.\, \sigma/\alpha]}$$

$$\frac{\Delta;\Gamma \vdash p : \sigma}{\Delta;\Gamma \vdash \mathsf{ref}\ p : \mathsf{ref}\ \sigma} \qquad \frac{\Delta;\Gamma \vdash p_1 : \mathsf{ref}\ \sigma \quad \Delta;\Gamma \vdash p_2 : \sigma}{\Delta;\Gamma \vdash p_1 := p_2 : \mathsf{unit}}$$

$$\frac{\Delta;\Gamma \vdash p : \mathsf{ref}\ \sigma}{\Delta;\Gamma \vdash !p : \sigma} \qquad \frac{\Delta;\Gamma \vdash p_1 : \mathsf{ref}\ \sigma \quad \Delta;\Gamma \vdash p_2 : \mathsf{ref}\ \sigma}{\Delta;\Gamma \vdash p_1 == p_2 : \mathsf{bool}}$$

$$\ldots$$

$\boxed{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma')}$

$$\frac{\Delta \subseteq \Delta' \quad \Gamma \subseteq \Gamma'}{\vdash \bullet : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1) \quad \Delta';\Gamma' \vdash p_2 : \sigma_2}{\vdash \langle C, p_2\rangle : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1 \times \sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1 \times \sigma_2)}{\vdash C.1 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1)} \qquad \frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1 \times \sigma_2)}{\vdash C.2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma', x{:}\sigma_1;\sigma_2)}{\vdash \lambda x{:}\sigma_1.\, C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1 \to \sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1 \to \sigma_2) \quad \Delta';\Gamma' \vdash p_2 : \sigma_1}{\vdash C\ p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1) \quad \Delta';\Gamma' \vdash p_1 : \sigma_1 \to \sigma_2}{\vdash p_1\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta', \alpha;\Gamma';\sigma_1)}{\vdash \Lambda\alpha.\, C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\forall\alpha.\, \sigma_1)} \qquad \frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\forall\alpha.\, \sigma_1)}{\vdash C[\sigma_2] : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1[\sigma_2/\alpha])}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2[\sigma_1/\alpha])}{\vdash \mathsf{pack}\ \langle \sigma_1, C\rangle\ \mathsf{as}\ \exists\alpha.\, \sigma_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\exists\alpha.\, \sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\exists\alpha.\,\sigma_1) \quad \Delta',\alpha;\Gamma',x{:}\sigma_1 \vdash p_2 : \sigma_2 \quad \Delta' \vdash \sigma_2}{\vdash \mathsf{unpack}\ C\ \mathsf{as}\ \langle\alpha,x\rangle\ \mathsf{in}\ p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\Delta';\Gamma' \vdash p_1 : \exists\alpha.\,\sigma_1 \quad \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta',\alpha;\Gamma',x{:}\sigma_1;\sigma_2) \quad \Delta' \vdash \sigma_2}{\vdash \mathsf{unpack}\ p_1\ \mathsf{as}\ \langle\alpha,x\rangle\ \mathsf{in}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1[\mu\alpha.\,\sigma_1/\alpha])}{\vdash \mathsf{roll}_{\mu\alpha.\,\sigma_1}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mu\alpha.\,\sigma_1)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mu\alpha.\,\sigma_1)}{\vdash \mathsf{unroll}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1[\mu\alpha.\,\sigma_1/\alpha])}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1)}{\vdash \mathsf{ref}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1) \quad \Delta';\Gamma' \vdash p_2 : \sigma_1}{\vdash C := p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{unit})}$$

$$\frac{\Delta';\Gamma' \vdash p_1 : \mathsf{ref}\,\sigma_1 \quad \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1)}{\vdash p_1 := C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{unit})}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1)}{\vdash\, !C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1) \quad \Delta';\Gamma' \vdash p_2 : \mathsf{ref}\,\sigma_1}{\vdash C == p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{bool})}$$

$$\frac{\Delta';\Gamma' \vdash p_1 : \mathsf{ref}\,\sigma_1 \quad \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1)}{\vdash p_1 == C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{bool})}$$

...

4) Contextual Equivalence.

Definition 7 (Contextual equivalence)**.**
Let $\Delta;\Gamma \vdash p_1 : \sigma$ and $\Delta;\Gamma \vdash p_2 : \sigma$. Then:
$\Delta;\Gamma \vdash p_1 \sim_{\mathrm{ctx}} p_2 : \sigma := \forall C, h, \tau.\ \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\cdot;\cdot;\tau) \Longrightarrow (h, |C[p_1]| \hookrightarrow^{\omega} \iff h, |C[p_2]| \hookrightarrow^{\omega})$

B. Model

Various Relations..

$$\begin{array}{lcl} beta(e) & := & \begin{cases} e' & \text{if } \forall h.\ \ h, e \hookrightarrow^1 h, e' \\ \text{undef} & \text{otherwise} \end{cases} \\ \text{FunVal} & := & \{\, f \in \text{CVal} \mid \forall v.\ beta(f\ v) \text{ defined} \,\} \\ \text{GenVal} & := & \{\, v \in \text{CVal} \mid beta(v[]) \text{ defined} \,\} \end{array}$$

$$\begin{array}{lcl} \mathbf{n} \in \text{TyNam} & & \\ \text{Names} & := & \{\, \mathcal{N} \in \mathbb{P}(\text{TyNam}) \mid \mathcal{N} \text{ is countably infinite} \,\} \\ \sigma \in \text{Type} & ::= & \mathbf{n} \mid \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \mathsf{bool} \mid \sigma_1 \times \sigma_2 \mid \sigma_1 + \sigma_2 \mid \sigma_1 \to \sigma_2 \mid \mu\alpha.\,\sigma \mid \forall\alpha.\,\sigma \mid \exists\alpha.\,\sigma \mid \mathsf{ref}\,\sigma \\ \text{CType} & := & \{\, \tau \in \text{Type} \mid \text{ftv}(\tau) = \emptyset \,\} \\ \text{CTypeF} & := & \{\, (\tau_1 \to \tau_2) \in \text{CType} \,\} \cup \{\, \mathsf{ref}\,\tau \in \text{CType} \,\} \cup \{\, (\forall\alpha.\,\sigma) \in \text{CType} \,\} \cup \text{TyNam} \\ \text{VRelF} & := & \text{CTypeF} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\ \text{VRel} & := & \text{CType} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\ \text{ERel} & := & \text{CType} \to \mathbb{P}(\text{CExp} \times \text{CExp}) \\ \text{KRel} & := & \text{CType} \times \text{CType} \to \mathbb{P}(\text{CCont} \times \text{CCont}) \\ \text{HRel} & := & \mathbb{P}(\text{Heap} \times \text{Heap}) \end{array}$$

Note that as a notational convention we use σ to range over possibly open types and τ over closed types.

Value Closure.. We define the closure $\overline{R} \in \text{VRel}$ for $R \in \text{VRelF}$ as the least fixpoint of the following equation.

$$\begin{array}{lcl} \overline{R}(\tau_{\text{base}}) & := & \text{ID}_{\tau_{\text{base}}} \\ \overline{R}(\tau_1 \times \tau_2) & := & \{\, ((v_1, v_1'), (v_2, v_2')) \mid (v_1, v_2) \in \overline{R}(\tau_1) \wedge (v_1', v_2') \in \overline{R}(\tau_2) \,\} \\ \overline{R}(\tau_1 + \tau_2) & := & \{\, (\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_1) \,\} \cup \{\, (\mathsf{inj}^2\, v_1, \mathsf{inj}^2\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_2) \,\} \\ \overline{R}(\mu\alpha.\,\sigma) & := & \{\, (\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \mid (v_1, v_2) \in \overline{R}(\sigma[\mu\alpha.\,\sigma/\alpha]) \,\} \\ \overline{R}(\exists\alpha.\,\sigma) & := & \{\, (\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \mid \exists\tau \in \text{CType}.\ (v_1, v_2) \in \overline{R}(\sigma[\tau/\alpha]) \,\} \\ \overline{R}(\tau_1 \to \tau_2) & := & R(\tau_1 \to \tau_2) \\ \overline{R}(\mathsf{ref}\,\tau) & := & R(\mathsf{ref}\,\tau) \\ \overline{R}(\mathbf{n}) & := & R(\mathbf{n}) \\ \overline{R}(\forall\alpha.\,\sigma) & := & R(\forall\alpha.\,\sigma) \end{array}$$

Dependent World.. For a preordered set $P = (\mathsf{S}_P, \sqsubseteq_P)$ we define

$$\begin{array}{l} \text{DepWorld}(P) \quad := \\ \{\, (\mathsf{N}, \mathsf{S}, \sqsubseteq, \sqsubseteq_{\text{pub}}, \mathsf{L}, \mathsf{H}) \\ \quad \in \mathbb{P}(\text{TyNam}) \times \text{Set} \times \mathbb{P}(\mathsf{S} \times \mathsf{S}) \times \mathbb{P}(\mathsf{S} \times \mathsf{S}) \times \\ \qquad (\mathsf{S}_P \to \mathsf{S} \to \text{VRelF} \to \text{VRelF}) \times (\mathsf{S}_P \to \mathsf{S} \to \text{VRelF} \to \text{HRel}) \mid \\ \quad \sqsubseteq, \sqsubseteq_{\text{pub}} \text{ are preorders } \wedge \\ \quad \sqsubseteq_{\text{pub}} \text{ is a subset of } \sqsubseteq \wedge \\ \quad \mathsf{L} \text{ is monotone in the first argument w.r.t. } \sqsubseteq_P, \text{ in the second w.r.t. } \sqsubseteq, \text{ in the third w.r.t. } \subseteq \wedge \\ \quad \mathsf{H} \text{ is monotone in the third argument w.r.t. } \subseteq \wedge \\ \quad (\forall s_1, s_2.\ \forall R.\ \forall \mathbf{n} \notin \mathsf{N}.\ \mathsf{L}(s_1)(s_2)(R)(\mathbf{n}) = \emptyset) \wedge \\ \quad (\forall s_1, s_2.\ \forall R.\ \forall (\tau_1 \to \tau_2, f_1, f_2) \in \mathsf{L}(s_1)(s_2)(R).\ f_1, f_2 \in \text{FunVal}) \wedge \\ \quad (\forall s_1, s_2.\ \forall R.\ \forall (\forall\alpha.\,\sigma, v_1, v_2) \in \mathsf{L}(s_1)(s_2)(R).\ v_1, v_2 \in \text{GenVal}) \quad \} \end{array}$$

Here we write $\subseteq$ for the pointwise lifting of the usual subset ordering $\subseteq$ to function spaces.
Also we write $\cup$ for the pointwise lifting of the usual set union $\cup$ to function spaces.

Full World.. We define

$$\text{World} := \{\, W \in \text{DepWorld}(\{*\}, \{(*,*)\}) \,\}$$

and for $W \in \text{World}$ and $s \in W.\mathsf{S}$ often write just $W.\mathsf{H}(s)$ for $W.\mathsf{H}(*)(s)$ (and similar for the L component).

World for Mutable References.. We define the reference world $W_{\mathrm{ref}} \in \mathrm{World}$ as follows.

$$
\begin{array}{lll}
W_{\mathrm{ref}}.\mathsf{N} & := & \emptyset \\
W_{\mathrm{ref}}.\mathsf{S} & := & \{\, s_{\mathrm{rf}} \in \mathbb{P}_{\mathrm{fin}}(\mathrm{CType} \times \mathrm{Loc} \times \mathrm{Loc}) \mid \\
 & & \quad \forall (\tau, \ell_1, \ell_2), (\tau', \ell_1', \ell_2') \in s_{\mathrm{rf}}. \\
 & & \quad (\ell_1 = \ell_1' \implies \tau = \tau' \wedge \ell_2 = \ell_2') \wedge (\ell_2 = \ell_2' \implies \tau = \tau' \wedge \ell_1 = \ell_1') \,\} \\
s_{\mathrm{rf}}' \sqsupseteq s_{\mathrm{rf}} & \text{iff} & s_{\mathrm{rf}}' \supseteq s_{\mathrm{rf}} \\
s_{\mathrm{rf}}' \sqsupseteq_{\mathrm{pub}} s_{\mathrm{rf}} & \text{iff} & s_{\mathrm{rf}}' \supseteq s_{\mathrm{rf}} \\
W_{\mathrm{ref}}.\mathsf{L}(s_{\mathrm{rf}})(R) & := & \{\, (\mathsf{ref}\,\tau, \ell_1, \ell_2) \mid (\tau, \ell_1, \ell_2) \in s_{\mathrm{rf}} \,\} \\
W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(R) & := & \{\, (h_1, h_2) \mid \mathrm{dom}(h_1) = \mathrm{dom}_{[1]}(s_{\mathrm{rf}}) \wedge \mathrm{dom}(h_2) = \mathrm{dom}_{[2]}(s_{\mathrm{rf}}) \wedge \\
 & & \qquad \forall (\tau, \ell_1, \ell_2) \in s_{\mathrm{rf}}.\ (\tau, h_1(\ell_1), h_2(\ell_2)) \in \overline{R} \,\}
\end{array}
$$

where

$$
\begin{array}{lll}
\mathrm{dom}_{[1]}(s) & := & \{\, \ell_1 \mid \exists \tau, \ell_2.\ (\tau, \ell_1, \ell_2) \in s \,\}\ , \\
\mathrm{dom}_{[2]}(s) & := & \{\, \ell_2 \mid \exists \tau, \ell_1.\ (\tau, \ell_1, \ell_2) \in s \,\}\ .
\end{array}
$$

Local World.. We define

$$\mathrm{LWorld} := \{\, w \in \mathrm{DepWorld}(W_{\mathrm{ref}}.\mathsf{S}, W_{\mathrm{ref}}.\sqsubseteq) \mid \forall s_{\mathrm{rf}}, s, R, \tau.\ w.\mathsf{L}(s_{\mathrm{rf}})(s)(R)(\mathsf{ref}\,\tau) = \emptyset \,\}$$

Product World.. For $w_1, w_2 \in \mathrm{LWorld}$, we define $w_1 \otimes w_2 \in \mathrm{LWorld}$ as follows.

$$
\begin{array}{lll}
\mathsf{N} & := & w_1.\mathsf{N} \uplus w_2.\mathsf{N} \\
\mathsf{S} & := & w_1.\mathsf{S} \times w_2.\mathsf{S} \\
(s_1', s_2') \sqsupseteq (s_1, s_2) & \text{iff} & s_1' \sqsupseteq s_1 \wedge s_2' \sqsupseteq s_2 \\
(s_1', s_2') \sqsupseteq_{\mathrm{pub}} (s_1, s_2) & \text{iff} & s_1' \sqsupseteq_{\mathrm{pub}} s_1 \wedge s_2' \sqsupseteq_{\mathrm{pub}} s_2 \\
\mathsf{L}(s_{\mathrm{rf}})(s_1, s_2)(R) & := & w_1.\mathsf{L}(s_{\mathrm{rf}})(s_1)(R) \cup w_2.\mathsf{L}(s_{\mathrm{rf}})(s_2)(R) \\
\mathsf{H}(s_{\mathrm{rf}})(s_1, s_2)(R) & := & w_1.\mathsf{H}(s_{\mathrm{rf}})(s_1)(R) \otimes w_2.\mathsf{H}(s_{\mathrm{rf}})(s_2)(R)
\end{array}
$$

where

$$H_1 \otimes H_2 \quad := \quad \{\, (h_1 \uplus h_1', h_2 \uplus h_2') \mid (h_1, h_2) \in H_1 \wedge (h_1', h_2') \in H_2 \,\}$$

Note that $w_1 \otimes w_2$ is undefined iff $w_1.\mathsf{N}$ and $w_2.\mathsf{N}$ is not disjoint.

Lifting of a Local World.. For $w \in \mathrm{LWorld}$, we define $w{\uparrow} \in \mathrm{World}$ as follows.

$$
\begin{array}{lll}
\mathsf{N} & := & w.\mathsf{N} \\
\mathsf{S} & := & W_{\mathrm{ref}}.\mathsf{S} \times w.\mathsf{S} \\
(s_{\mathrm{rf}}', s') \sqsupseteq (s_{\mathrm{rf}}, s) & \text{iff} & s_{\mathrm{rf}}' \sqsupseteq s_{\mathrm{rf}} \wedge s' \sqsupseteq s \\
(s_{\mathrm{rf}}', s') \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s) & \text{iff} & s_{\mathrm{rf}}' \sqsupseteq_{\mathrm{pub}} s_{\mathrm{rf}} \wedge s' \sqsupseteq_{\mathrm{pub}} s \\
\mathsf{L}(s_{\mathrm{rf}}, s)(R) & := & W_{\mathrm{ref}}.\mathsf{L}(s_{\mathrm{rf}})(R) \cup w.\mathsf{L}(s_{\mathrm{rf}})(s)(R) \\
\mathsf{H}(s_{\mathrm{rf}}, s)(R) & := & W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(R) \otimes w.\mathsf{H}(s_{\mathrm{rf}})(s)(R)
\end{array}
$$

Single-State Worlds.. Given a local knowledge $L \in \mathrm{VRelF} \xrightarrow{\mathrm{mon}} \mathrm{VRelF}$ and a heap relation $H \in \mathrm{VRelF} \xrightarrow{\mathrm{mon}} \mathrm{HRel}$ such that

$$
\begin{array}{l}
\forall R.\ \forall (\tau_1 \to \tau_2, f_1, f_2) \in L(R).\ f_1, f_2 \in \mathrm{FunVal} \wedge \\
\forall R.\ \forall (\forall \alpha.\, \tau, f_1, f_2) \in L(R).\ f_1, f_2 \in \mathrm{GenVal}
\end{array}
$$

we define the single-state local world $w_{\mathrm{single}}(L, H) \in \mathrm{LWorld}$ as follows.

$$
\begin{array}{lll}
w_{\mathrm{single}}(L,H).\mathsf{N} & := & \emptyset \\
w_{\mathrm{single}}(L,H).\mathsf{S} & := & \{\, * \,\} \\
* \sqsupseteq * & & \\
* \sqsupseteq_{\mathrm{pub}} * & & \\
w_{\mathrm{single}}(L,H).\mathsf{L}(s_{\mathrm{rf}})(*)(R) & := & \{\, (\tau' \to \tau, f_1, f_2) \in L(R) \,\} \cup \{\, (\forall \alpha.\, \tau, f_1, f_2) \in L(R) \,\} \\
w_{\mathrm{single}}(L,H).\mathsf{H}(s_{\mathrm{rf}})(*)(R) & := & H(R)
\end{array}
$$

Global Knowledge.. We define the ref-name-preserving order $\geq_{\mathrm{ref}}^{\mathcal{N}}$ between $R, R' \in \mathrm{VRelF}$ as follows.

$$
\begin{array}{lll}
R' \geq_{\mathrm{ref}}^{\mathcal{N}} R & \text{iff} & \forall \tau.\ R'(\tau) \supseteq R(\tau) \wedge \\
 & & \forall \tau.\ R'(\mathsf{ref}\,\tau) = R(\mathsf{ref}\,\tau) \wedge \\
 & & \forall \mathbf{n} \in \mathcal{N}.\ R'(\mathbf{n}) = R(\mathbf{n})
\end{array}
$$

Note that $R' \geq_{\mathrm{ref}}^{\mathcal{N}} R \implies R' \supseteq R$.

We define $\mathrm{GK}(W)$ for $W \in \mathrm{World}$ as follows.

$$\mathrm{GK}(W) \quad := \quad \{\, G \in W.\mathsf{S} \to \mathrm{VRelF} \mid G \text{ is monotone w.r.t. } \sqsubseteq \ \wedge \forall s.\ G(s) \geq^{W.\mathsf{N}}_{\mathrm{ref}} W.\mathsf{L}(s)(G(s)) \,\}$$

Expression and Continuation Equivalence.. We define the following notation.

$$s' \sqsupseteq [s_0, s] \quad \text{iff} \quad s' \sqsupseteq_{\mathrm{pub}} s_0 \wedge s' \sqsupseteq s$$

For $W \in \mathrm{World}$, we coinductively define $\mathbf{E}_W \in \mathrm{GK}(W) \to W.\mathsf{S} \times W.\mathsf{S} \to \mathrm{ERel}$ and $\mathbf{K}_W \in \mathrm{GK}(W) \to W.\mathsf{S} \times W.\mathsf{S} \to \mathrm{KRel}$ as follows.

$$\begin{aligned}
\mathbf{E}_W(G)(s_0,s)(\tau) &:= \{\, (e_1,e_2) \mid \forall (h_1,h_2) \in W.\mathsf{H}(s)(G(s)).\ \forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}. \\
&\qquad ((h_1,h_1^{\mathrm{F}},e_1),(h_2,h_2^{\mathrm{F}},e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0,s)(\tau) \,\} \\
\mathbf{K}_W(G)(s_0,s)(\tau_1,\tau_2) &:= \{\, (K_1,K_2) \mid \forall (v_1,v_2) \in \overline{G(s)}(\tau_1).\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s_0,s)(\tau_2) \,\} \\
\mathbf{O}_W(R^{\mathbf{K}})(G)(s_0,s)(\tau) &:= \{\, ((h_1,h_1^{\mathrm{F}},e_1),(h_2,h_2^{\mathrm{F}},e_2)) \mid h_1 \uplus h_1^{\mathrm{F}} \text{ defined} \wedge h_2 \uplus h_2^{\mathrm{F}} \text{ defined} \implies \\
&\qquad (h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{\omega} \wedge\ h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^{\omega}) \\
&\qquad \vee\ (\exists h_1', h_2', v_1, v_2.\ h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, v_2 \wedge \\
&\qquad\quad \exists s' \sqsupseteq [s_0, s].\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (v_1,v_2) \in \overline{G(s')}(\tau)) \\
&\qquad \vee\ (\exists h_1', h_2', \tau', K_1, K_2, e_1', e_2'. \\
&\qquad\quad h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'] \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[e_2'] \wedge \\
&\qquad\quad \exists s' \sqsupseteq s.\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (\tau', e_1', e_2') \in \mathbf{S}(G(s'), G(s')) \wedge \\
&\qquad\quad \forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \supseteq G.\ (K_1,K_2) \in R^{\mathbf{K}}(G')(s_0,s'')(\tau',\tau)) \,\} \\
\mathbf{S}(R_f,R_v) &:= \{\, (\tau, f_1\ v_1, f_2\ v_2) \mid \exists \tau'.\ (f_1,f_2) \in R_f(\tau' \to \tau) \wedge (v_1,v_2) \in \overline{R_v}(\tau') \,\} \\
&\quad \cup \{\, (\sigma[\tau/\alpha], f_1[], f_2[]) \mid \tau \in \mathrm{CType} \wedge (f_1,f_2) \in R_f(\forall \alpha.\, \sigma) \,\}
\end{aligned}$$

Program Equivalence..

For $w \in \mathrm{LWorld}$, we define:

$$\begin{aligned}
\mathit{stable}(w) \quad := \quad & \forall G \in \mathrm{GK}(w{\uparrow}).\ \forall s_{\mathrm{rf}}, s.\ \forall (h_1,h_2) \in w.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}},s)). \\
& \forall s'_{\mathrm{rf}} \sqsupseteq s_{\mathrm{rf}}.\ \forall (h^1_{\mathrm{ref}}, h^2_{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s'_{\mathrm{rf}})(G(s'_{\mathrm{rf}}, s)).\ h^1_{\mathrm{ref}} \uplus h_1 \text{ defined} \wedge h^2_{\mathrm{ref}} \uplus h_2 \text{ defined} \implies \\
& \exists s' \sqsupseteq_{\mathrm{pub}} s.\ (h_1,h_2) \in w.\mathsf{H}(s'_{\mathrm{rf}})(s')(G(s'_{\mathrm{rf}}, s'))
\end{aligned}$$

For $W \in \mathrm{World}$, we define:

$$\begin{aligned}
\mathit{inhabited}(W) \quad &:= \quad \forall G \in \mathrm{GK}(W).\ \exists s_0.\ (\emptyset,\emptyset) \in W.\mathsf{H}(s_0)(G(s_0)) \\
\mathit{consistent}(W) \quad &:= \quad \forall G \in \mathrm{GK}(W).\ \forall s.\ \forall (\tau, e_1, e_2) \in \mathbf{S}(W.\mathsf{L}(s)(G(s)), G(s)). \\
&\qquad\qquad (\tau, \mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_W(G)(s,s)
\end{aligned}$$

We define program equivalence $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$.

$$\begin{aligned}
&\mathrm{TyEnv}(\Delta) && := \{\, \delta \mid \delta \in \Delta \to \mathrm{CType} \,\} \\
&\mathrm{Env}(\Gamma, R) && := \{\, (\gamma_1,\gamma_2) \mid \gamma_1,\gamma_2 \in \mathrm{dom}(\Gamma) \to \mathrm{CVal} \wedge \forall x.\ (\Gamma(x), \gamma_1(x), \gamma_2(x)) \in \overline{R} \,\} \\
&\Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma && := \mathit{inhabited}(W) \wedge \mathit{consistent}(W) \wedge \\
&&& \quad \forall G \in \mathrm{GK}(W).\ \forall s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1,\gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)). \\
&&& \quad (\delta\sigma, \gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_W(G)(s,s) \\
&\Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma && := \mathit{stable}(w) \wedge \Delta; \Gamma \vdash e_1 \sim_{w{\uparrow}} e_2 : \sigma \\
&\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma && := \forall \mathcal{N} \in \mathrm{Names}.\ \exists w \in \mathrm{LWorld}.\ w.\mathsf{N} \subseteq \mathcal{N} \wedge \Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma
\end{aligned}$$

C. Metatheory

1) Basic Properties.

***Notation.*.** For a monotone function $F \in \mathrm{VRelF} \to \mathrm{VRelF}$ and $R \in \mathrm{VRelF}$, we define $[F]^*_R$ as the least fixpoint of the monotone function $F(-) \cup R$:

$$[F]^*_R := \mu X.\ F(X) \cup R\ .$$

For $W \in \mathrm{World}$, we define $[W] \in W.\mathsf{S} \to \mathrm{VRelF}$ as follows:

$$[W](s) := [W.\mathsf{L}(s)]^*_\emptyset\ .$$

Lemma 12. If $G' \supseteq G$ and $s' \sqsupseteq s$, then:

1) $G'(s') \supseteq G(s)$
2) $\mathrm{Env}(\Gamma, G'(s')) \supseteq \mathrm{Env}(\Gamma, G(s))$

Proof:

1) By definition of GK we know $G'(s') \supseteq G'(s)$. And since $G' \supseteq G$ we also know $G'(s) \supseteq G(s)$.
2) Follows immediately from (1).

■

Lemma 13. $\forall W \in \mathrm{World}.\ [W] \in \mathrm{GK}(W)$

Proof: We must establish four properties:

a) To show: $[W]$ is monotone w.r.t. $\sqsubseteq$.
   Follows from monotonicity of $W.\mathsf{L}$.
b) To show: $\forall s, \tau.\ [W](s)(\tau) \supseteq W.\mathsf{L}(s)([W](s))(\tau)$.
   Immediate after unrolling fixpoint once.
c) To show: $\forall s, \tau.\ [W](s)(\mathsf{ref}\,\tau) = W.\mathsf{L}(s)([W](s))(\mathsf{ref}\,\tau)$.
   Easy fixpoint induction.
d) To show: $\forall s, \mathbf{n} \in W.\mathsf{N}.\ [W](s)(\mathbf{n}) = W.\mathsf{L}(s)([W](s))(\mathbf{n})$.
   Easy fixpoint induction.

■

Lemma 14. $\forall W \in \mathrm{World}, G \in \mathrm{GK}(W).\ [W] \subseteq G$

Proof: Easy fixpoint induction. ■

Lemma 15. If

- $h_1 \uplus h^f_1, e_1 \hookrightarrow^* h'_1 \uplus h^f_1, e'_1$,
- $h_2 \uplus h^f_2, e_2 \hookrightarrow^* h'_2 \uplus h^f_2, e'_2$,
- $s' \sqsupseteq s$, and
- $(\tau, (h'_1, h^f_1, e'_1), (h'_2, h^f_2, e'_2)) \in \mathbf{O}_W(R^{\mathbf{K}})(s_0, s')$,

then $(\tau, (h_1, h^f_1, e_1), (h_2, h^f_2, e_2)) \in \mathbf{O}_W(R^{\mathbf{K}})(s_0, s)$.

Proof: Follows easily from the definition of $\mathbf{O}_W$. ■

Lemma 16. $G(s) \subseteq \overline{G(s)} \subseteq \mathbf{E}_W(G)(s, s)$

Proof: The first inclusion holds immediately by definition; the second by choosing the final state to be s. ■

Lemma 17. $(\tau, \tau, \bullet, \bullet) \in \mathbf{K}_W(G)(s, s)$

Proof: We need to show $(\tau, v_1, v_2) \in \mathbf{E}_W(G)(s, s)$ for $(\tau, v_1, v_2) \in \overline{G(s)}$, which holds by Lemma 16. ■

Lemma 18. If $s'_0 \sqsupseteq_{\mathrm{pub}} s_0$, then:

1) $\mathbf{E}_W(G)(s'_0, s) \subseteq \mathbf{E}_W(G)(s_0, s)$
2) $\mathbf{K}_W(G)(s'_0, s) \subseteq \mathbf{K}_W(G)(s_0, s)$

Proof: We define $\mathbf{E}'_W$ and $\mathbf{K}'_W$ as follows:

$$\mathbf{E}'_W(G)(s_0, s) = \{\, (\tau, e_1, e_2) \mid \exists s'_0.\ s'_0 \sqsupseteq_{\mathrm{pub}} s_0 \wedge (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s) \,\}$$
$$\mathbf{K}'_W(G)(s_0, s) = \{\, (\tau_1, \tau_2, K_1, K_2) \mid \exists s'_0.\ s'_0 \sqsupseteq_{\mathrm{pub}} s_0 \wedge (\tau_1, \tau_2, K_1, K_2) \in \mathbf{K}_W(G)(s'_0, s) \,\}$$

If $\mathbf{E}'_W \subseteq \mathbf{E}_W$ and $\mathbf{K}'_W \subseteq \mathbf{K}_W$, then for $s'_0 \sqsupseteq_{\text{pub}} s_0$ we have

$$\mathbf{E}_W(G)(s'_0, s) \subseteq \mathbf{E}'_W(G)(s_0, s) \subseteq \mathbf{E}_W(G)(s_0, s)$$

(and similar for $\mathbf{K}_W$).

We now prove $\mathbf{E}'_W \subseteq \mathbf{E}_W$ and $\mathbf{K}'_W \subseteq \mathbf{K}_W$ by coinduction. Concretely, we have to show:

1) $\forall e_1, e_2, G, s_0, s, \tau.$
   $(e_1, e_2) \in \mathbf{E}'_W(G)(s_0, s)(\tau) \implies$
   $\forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)).\forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.\ ((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$
2) $\forall K_1, K_2, G, s_0, s, \tau', \tau.$
   $(K_1, K_2) \in \mathbf{K}'_W(G)(s_0, s)(\tau', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s)}(\tau').\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$ and $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$.
- We must show $((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$.
- By definition of $\mathbf{E}'_W$ we know $(e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s)(\tau)$ for some $s'_0 \sqsupseteq_{\text{pub}} s_0$.
- Hence $((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s'_0, s)(\tau)$.
- It is easy to see that this implies $((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$.

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_W(G)(s_0, s)(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s)}(\tau')$.
- We must show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$.
- By definition of $\mathbf{K}'_W$ we know $(K_1, K_2) \in \mathbf{K}_W(G)(s'_0, s)(\tau', \tau)$ for some $s'_0 \sqsupseteq_{\text{pub}} s_0$.
- Hence $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s'_0, s)(\tau) \subseteq \mathbf{E}'_W(G)(s_0, s)(\tau)$.

■

Lemma 19. If $w_1, w_2 \in \text{LWorld}$, then $\forall G \in \text{GK}((w_1 \otimes w_2)\uparrow).\ \forall s_2 \in w_2.\mathsf{S}.\ G(-, -, s_2) \in \text{GK}(w_1\uparrow)$.

Proof: We must establish four properties:

a) To show: $G(-, -, s_2)$ is monotone w.r.t. $\sqsubseteq$.
   This follows directly from the definition of $\uparrow, \otimes$ and the monotonicity of G.
b) To show: $\forall s_{\text{rf}}, s_1, \tau.\ G(s_{\text{rf}}, s_1, s_2)(\tau) \supseteq w_1\uparrow.\mathsf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\tau)$.
   We know $G(s_{\text{rf}}, s_1, s_2)(\tau) \supseteq (w_1 \otimes w_2)\uparrow.\mathsf{L}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))(\tau)$.
   By definition, the latter equals $w_1\uparrow.\mathsf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\tau) \cup w_2.\mathsf{L}(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))(\tau)$.
c) To show: $\forall s_{\text{rf}}, s_1, \tau.\ G(s_{\text{rf}}, s_1, s_2)(\mathsf{ref}\,\tau) = w_1\uparrow.\mathsf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\mathsf{ref}\,\tau)$.
   We know $G(s_{\text{rf}}, s_1, s_2)(\mathsf{ref}\,\tau) = (w_1 \otimes w_2)\uparrow.\mathsf{L}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))(\mathsf{ref}\,\tau)$.
   By definition, the latter equals $w_1\uparrow.\mathsf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\mathsf{ref}\,\tau) \cup w_2.\mathsf{L}(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))(\mathsf{ref}\,\tau)$.
   Since $w_2 \in \text{LWorld}$, we are done.
d) To show: $\forall s_{\text{rf}}, s_1, \mathbf{n} \in w_1\uparrow.\mathsf{N}.\ G(s_{\text{rf}}, s_1, s_2)(\mathbf{n}) = w_1\uparrow.\mathsf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n})$.
   We know $G(s_{\text{rf}}, s_1, s_2)(\mathbf{n}) = (w_1 \otimes w_2)\uparrow.\mathsf{L}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n})$.
   By definition, the latter equals $w_1\uparrow.\mathsf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n}) \cup w_2.\mathsf{L}(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n})$.
   Since $\mathbf{n} \notin w_2.\mathsf{N}$ by definition of $\uparrow, \otimes$, we are done.

■

Lemma 20. If $w_1, w_2 \in \text{LWorld}$, then $\forall G \in \text{GK}((w_1 \otimes w_2)\uparrow).\ \forall s_1 \in w_1.\mathsf{S}.\ G(-, s_1, -) \in \text{GK}(w_2\uparrow)$.

Proof: Similar to Lemma 19. ■

Lemma 21. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in \text{LWorld}$ and $\mathit{stable}(w_2)$, then for all $G \in \text{GK}(w\uparrow)$ and for all $s^0_{\text{rf}}, s_{\text{rf}} \in W_{\text{ref}}.\mathsf{S}$, $s^0_1, s_1 \in w_1.\mathsf{S}$, $s^0_2, s_2 \in w_2.\mathsf{S}$ with $s_2 \sqsupseteq_{\text{pub}} s^0_2$:

1) $\mathbf{E}_{w_1\uparrow}(G(-, -, s_2))((s^0_{\text{rf}}, s^0_1), (s_{\text{rf}}, s_1)) \subseteq \mathbf{E}_{w\uparrow}(G)((s^0_{\text{rf}}, s^0_1, s^0_2), (s_{\text{rf}}, s_1, s_2))$
2) $\mathbf{K}_{w_1\uparrow}(G(-, -, s_2))((s^0_{\text{rf}}, s^0_1), (s_{\text{rf}}, s_1) \subseteq \mathbf{K}_{w\uparrow}(G)((s^0_{\text{rf}}, s^0_1, s^0_2), (s_{\text{rf}}, s_1, s_2))$

Proof: We define $\mathbf{E}'_{w\uparrow}$ and $\mathbf{K}'_{w\uparrow}$ as follows:

$$\mathbf{E}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2)) = \{\, (\tau, e_1, e_2) \mid s_2 \sqsupseteq_{\mathrm{pub}} s^0_2 \wedge (\tau, e_1, e_2) \in \mathbf{E}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\mathrm{rf}}, s^0_1), (s_{\mathrm{rf}}, s_1)) \,\}$$

$$\mathbf{K}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2)) = \{\, (\tau', \tau, K_1, K_2) \mid s_2 \sqsupseteq_{\mathrm{pub}} s^0_2 \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\mathrm{rf}}, s^0_1), (s_{\mathrm{rf}}, s_1)) \,\}$$

We now prove $\mathbf{E}'_{w\uparrow} \subseteq \mathbf{E}_{w\uparrow}$ and $\mathbf{K}'_{w\uparrow} \subseteq \mathbf{K}_{w\uparrow}$ by coinduction. Concretely, we have to show:

1) $\forall e_1, e_2, G, s^0_{\mathrm{rf}}, s_{\mathrm{rf}}, s^0_1, s^0_2, s_1, s_2, \tau.$
   $(e_1, e_2) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau) \implies$
   $\forall (h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s_1, s_2)(G(s_{\mathrm{rf}}, s_1, s_2)).\forall h^{\mathrm{F}}_1, h^{\mathrm{F}}_2.$
   $((h_1, h^{\mathrm{F}}_1, e_1), (h_2, h^{\mathrm{F}}_2, e_2)) \in \mathbf{O}_{w\uparrow}(\mathbf{K}'_{w\uparrow})(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau)$
2) $\forall K_1, K_2, G, s^0_{\mathrm{rf}}, s_{\mathrm{rf}}, s^0_1, s^0_2, s_1, s_2, \tau', \tau.$
   $(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s_1, s_2)}(\tau').\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau)$ and $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s_1, s_2)(G(s_{\mathrm{rf}}, s_1, s_2))$.
- By definition of $\mathbf{E}'_{w\uparrow}$ we know $s_2 \sqsupseteq_{\mathrm{pub}} s^0_2$ and $(e_1, e_2) \in \mathbf{E}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\mathrm{rf}}, s^0_1), (s_{\mathrm{rf}}, s_1))(\tau)$.
- We must show $((h_1, h^{\mathrm{F}}_1, e_1), (h_2, h^{\mathrm{F}}_2, e_2)) \in \mathbf{O}_{w\uparrow}(\mathbf{K}'_{w\uparrow})(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau)$.
- So suppose $\mathrm{defined}(h_1 \uplus h^{\mathrm{F}}_1)$ and $\mathrm{defined}(h_2 \uplus h^{\mathrm{F}}_2)$.
- From $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s_1, s_2)(G(s_{\mathrm{rf}}, s_1, s_2))$ and the definition of $\uparrow, \otimes$, we know $h_1 = h'_1 \uplus h''_1$ and $h_2 = h'_2 \uplus h''_2$ with $(h'_1, h'_2) \in w_1\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s_1)(G(s_{\mathrm{rf}}, s_1, s_2))$ and $(h''_1, h''_2) \in w_2.\mathsf{H}(s_{\mathrm{rf}})(s_2)(G(s_{\mathrm{rf}}, s_1, s_2))$.
- Hence $((h'_1, h''_1 \uplus h^{\mathrm{F}}_1, e_1), (h'_2, h''_2 \uplus h^{\mathrm{F}}_2, e_2)) \in \mathbf{O}_{w_1\uparrow}(\mathbf{K}_{w_1\uparrow})(G(-,-,s_2))((s^0_{\mathrm{rf}}, s^0_1), (s_{\mathrm{rf}}, s_1))(\tau)$.
- Consequently at least one of the following three properties holds:

A) $h_1 \uplus h^{\mathrm{F}}_1, e_1 \hookrightarrow^{\omega}$ and $h_2 \uplus h^{\mathrm{F}}_2, e_2 \hookrightarrow^{\omega}$

B) a) $h_1 \uplus h^{\mathrm{F}}_1, e_1 \hookrightarrow^{*} \widetilde{h'_1} \uplus h''_1 \uplus h^{\mathrm{F}}_1, v_1$ and $h_2 \uplus h^{\mathrm{F}}_2, e_2 \hookrightarrow^{*} \widetilde{h'_2} \uplus h''_2 \uplus h^{\mathrm{F}}_2, v_2$
   b) $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}) \sqsupseteq [(s^0_{\mathrm{rf}}, s^0_1), (s_{\mathrm{rf}}, s_1)]$
   c) $(\widetilde{h'_1}, \widetilde{h'_2}) \in \overline{w_1\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, s_2))}$
   d) $(v_1, v_2) \in \overline{G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, s_2)}(\tau)$

C) a) $h_1 \uplus h^{\mathrm{F}}_1, e_1 \hookrightarrow^{*} \widetilde{h'_1} \uplus h''_1 \uplus h^{\mathrm{F}}_1, K_1[e'_1]$ and $h_2 \uplus h^{\mathrm{F}}_2, e_2 \hookrightarrow^{*} \widetilde{h'_2} \uplus h''_2 \uplus h^{\mathrm{F}}_2, K_2[e'_2]$
   b) $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}) \sqsupseteq (s_{\mathrm{rf}}, s_1)$
   c) $(\widetilde{h'_1}, \widetilde{h'_2}) \in w_1\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, s_2))$
   d) $(e'_1, e'_2) \in \mathbf{S}(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}, s_2), G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}, s_2))(\widetilde{\tau})$
   e) $\forall (\widehat{s_{\mathrm{rf}}}, \widehat{s_1}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}).\ \forall G' \supseteq G(-,-,s_2).\ (K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G')((s^0_{\mathrm{rf}}, s^0_1), (\widehat{s_{\mathrm{rf}}}, \widehat{s_1}))(\widetilde{\tau}, \tau)$

- If (A) holds, then we are done.
- If (B) holds:
  - By $\mathit{stable}(w_2)$ there is $\widetilde{s_2} \sqsupseteq_{\mathrm{pub}} s_2$ such that
    $$(h''_1, h''_2) \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(\widetilde{s_2})(G(s_{\mathrm{rf}}, s_1, s_2))\ .$$
  - By monotonicity of $w_2.\mathsf{H}$, from $G(s_{\mathrm{rf}}, s_1, s_2) \subseteq G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{st_2})$, we have
    $$(h''_1, h''_2) \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(\widetilde{s_2})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{st_2}))\ .$$
  - From (Bc) and monotonicity we also know $(\widetilde{h'_1}, \widetilde{h'_2}) \in w_1\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2}))$.
  - Thus by the definition of $\uparrow, \otimes$, we get $(\widetilde{h'_1} \uplus h''_1, \widetilde{h'_2} \uplus h''_2) \in w\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2}))$.
  - From (Bb) and the definition of $\uparrow, \otimes$, we get $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2}) \sqsupseteq [(s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2)]$.
  - Together with (Ba) (Bd) we are done.
- If (C) holds:
  - By $\mathit{stable}(w_2)$ there is $\widetilde{s_2} \sqsupseteq_{\mathrm{pub}} s_2$ such that
    $$(h''_1, h''_2) \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(\widetilde{s_2})(G(s_{\mathrm{rf}}, s_1, s_2))\ .$$
  - By monotonicity of $w_2.\mathsf{H}$, from $G(s_{\mathrm{rf}}, s_1, s_2) \subseteq G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{st_2})$, we have
    $$(h''_1, h''_2) \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(\widetilde{s_2})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{st_2}))\ .$$

– From (Cc) and monotonicity we also know $(\widetilde{h_1'}, \widetilde{h_2'}) \in w_1{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2}))$.
– Thus by the definition of $\uparrow, \otimes$, we get $(\widetilde{h_1'} \uplus h_1'', \widetilde{h_2'} \uplus h_2'') \in w{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2}))$.
– From (Cb) and the definition of $\uparrow, \otimes$, we get $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2}) \sqsupseteq [(s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2)]$.
– Now it remains to show:

$$\forall(\widehat{s_{\mathrm{rf}}}, \widehat{s_1}, \widehat{s_2}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2}).\ \forall G' \supseteq G.\ (K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G')((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (\widehat{s_{\mathrm{rf}}}, \widehat{s_1}, \widehat{s_2}))(\widetilde{\tau}, \tau)$$

– So suppose $(\widehat{s_{\mathrm{rf}}}, \widehat{s_1}, \widehat{s_2}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1}, \widetilde{s_2})$ and $G' \supseteq G$.
– Note that $(\widehat{s_{\mathrm{rf}}}, \widehat{s_1}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1})$ and, by monotonicity, $G'(-, -, \widehat{s_2}) \supseteq G(-, -, s_2)$.
– From (Ce) we therefore get $(K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G'(-, -, \widehat{s_2}))((s^0_{\mathrm{rf}}, s^0_1), (\widehat{s_{\mathrm{rf}}}, \widehat{s_1}))(\widetilde{\tau}, \tau)$.
– By definition of $\mathbf{K}'_{w\uparrow}$ this implies

$$(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G')((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (\widehat{s_{\mathrm{rf}}}, \widehat{s_1}, \widehat{s_2}))(\widetilde{\tau}, \tau)$$

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s_1, s_2)}(\tau')$.
- By definition of $\mathbf{K}'_{w\uparrow}$ we know $s_2 \sqsupseteq_{\mathrm{pub}} s^0_2$ and $(K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G(-, -, s_2))((s^0_{\mathrm{rf}}, s^0_1), (s_{\mathrm{rf}}, s_1))(\tau', \tau)$.
- We must show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))(\tau)$.
- By definition of $\mathbf{E}'_{w\uparrow}$ it suffices to show

$$(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{w_1\uparrow}(G(-, -, s_2))((s^0_{\mathrm{rf}}, s^0_1), (s_{\mathrm{rf}}, s_1))(\tau).$$

- Since $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s_1, s_2)}(\tau')$, we are done.

■

Lemma 22. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in \mathrm{LWorld}$ and $\mathit{stable}(w_1)$, then for all $G \in \mathrm{GK}(w\uparrow)$ and for all $s^0_{\mathrm{rf}}, s_{\mathrm{rf}} \in W_{\mathrm{ref}}.\mathsf{S}$, $s^0_1, s_1 \in w_1.\mathsf{S}$, $s^0_2, s_2 \in w_2.\mathsf{S}$ with $s_1 \sqsupseteq_{\mathrm{pub}} s^0_1$:

1) $\mathbf{E}_{w_2\uparrow}(G(-, s_1, -))((s^0_{\mathrm{rf}}, s^0_2), (s_{\mathrm{rf}}, s_2)) \subseteq \mathbf{E}_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))$
2) $\mathbf{K}_{w_2\uparrow}(G(-, s_1, -))((s^0_{\mathrm{rf}}, s^0_2), (s_{\mathrm{rf}}, s_2) \subseteq \mathbf{K}_{w\uparrow}(G)((s^0_{\mathrm{rf}}, s^0_1, s^0_2), (s_{\mathrm{rf}}, s_1, s_2))$

Proof: Similar to Lemma 21. ■

Lemma 23. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in \mathrm{LWorld}$ and $\mathit{stable}(w_1), \mathit{stable}(w_2)$, then:

1) $\mathit{stable}(w)$
2) If $\mathit{inhabited}(w_1\uparrow)$ and $\mathit{inhabited}(w_2\uparrow)$, then $\mathit{inhabited}(w\uparrow)$.
3) If $\mathit{consistent}(w_1\uparrow)$ and $\mathit{consistent}(w_2\uparrow)$, then $\mathit{consistent}(w\uparrow)$.

Proof:

1) • Suppose $G \in \mathrm{GK}((w_1 \otimes w_2)\uparrow)$, $(h_1, h_2) \in (w_1 \otimes w_2).\mathsf{H}(s_{\mathrm{rf}})(s_1, s_2)(G(s_{\mathrm{rf}}, s_1, s_2))$ and $s'_{\mathrm{rf}} \sqsupseteq s_{\mathrm{rf}}$.
   • Further suppose $(h'_1, h'_2) \in W_{\mathrm{ref}}.\mathsf{H}(s'_{\mathrm{rf}})(G(s'_{\mathrm{rf}}, s))$ and $\mathrm{defined}(h'_1 \uplus h_1)$ and $\mathrm{defined}(h'_2 \uplus h_2)$.
   • We must show that there is $(s'_1, s'_2) \sqsupseteq_{\mathrm{pub}} (s_1, s_2)$ such that

$$(h_1, h_2) \in (w_1 \otimes w_2).\mathsf{H}(s'_{\mathrm{rf}})(s'_1, s'_2)(G(s'_{\mathrm{rf}}, s'_1, s'_2)).$$

   • Decomposing $(w_1 \otimes w_2).\mathsf{H}$ gives us $h^1_1, h^1_2, h^2_1, h^2_2$ such that:
     – $h_1 = h^1_1 \uplus h^2_1$ and $h_2 = h^1_2 \uplus h^2_2$
     – $(h^1_1, h^1_2) \in w_1.\mathsf{H}(s_{\mathrm{rf}})(s_1)(G(s_{\mathrm{rf}}, s_1, s_2))$
     – $\mathrm{defined}(h'_1 \uplus h^1_1)$ and $\mathrm{defined}(h'_2 \uplus h^1_2)$
     – $(h^2_1, h^2_2) \in w_2.\mathsf{H}(s_{\mathrm{rf}})(s_2)(G(s_{\mathrm{rf}}, s_1, s_2))$
     – $\mathrm{defined}(h'_1 \uplus h^2_1)$ and $\mathrm{defined}(h'_2 \uplus h^2_2)$
   • From this, Lemmas 19–22, and the assumptions, we get $s'_1 \sqsupseteq_{\mathrm{pub}} s_1$ and $s'_2 \sqsupseteq_{\mathrm{pub}} s_2$ such that:
     a) $(h^1_1, h^1_2) \in w_1.\mathsf{H}(s'_{\mathrm{rf}})(s'_1)(G(s'_{\mathrm{rf}}, s'_1, s_2))$
     b) $(h^2_1, h^2_2) \in w_2.\mathsf{H}(s'_{\mathrm{rf}})(s'_2)(G(s'_{\mathrm{rf}}, s_1, s'_2))$
   • Using monotonicity and then composing this gives us

$$(h_1, h_2) \in (w_1 \otimes w_2).\mathsf{H}(s'_{\mathrm{rf}})(s'_1, s'_2)(G(s'_{\mathrm{rf}}, s'_1, s'_2)).$$

2) • Suppose $G \in \mathrm{GK}(w\uparrow)$.
   • From the assumptions, Lemma 13, and definition of $\uparrow$ and W_{ref} we get s_1, s_2 such that
   $(\emptyset, \emptyset) \in w_1.\mathsf{H}(\emptyset)(s_1)([w_1\uparrow](\emptyset, s_1))$ and
   $(\emptyset, \emptyset) \in w_2.\mathsf{H}(\emptyset)(s_2)([w_2\uparrow](\emptyset, s_2))$.

- From Lemmas 13, 14, 19, 20, we know $[w_1\uparrow] \subseteq [w\uparrow](-,(-,s_2))$ and $[w_2\uparrow] \subseteq [w\uparrow](-,(s_1,-))$.
- Hence $(\emptyset,\emptyset) \in w\uparrow.\mathsf{H}(\emptyset,(s_1,s_2))([w\uparrow](\emptyset,(s_1,s_2)))$ by monotonicity and definition of $\otimes,\uparrow$.

3) • We suppose
   a) $s = (s_{\mathrm{rf}}, s_1, s_2) \in w\uparrow.\mathsf{S}$
   b) $G \in \mathrm{GK}(w\uparrow)$
   c) $(\tau, e_1, e_2) \in \mathbf{S}(w\uparrow.\mathsf{L}(s)(G(s)), G(s))$

   and must show $(\tau, beta(e_1), beta(e_2)) \in \mathbf{E}_{w\uparrow}(G)(s,s))$.
- From (c) and the definitions of $\uparrow$, $\otimes$ and $\mathbf{S}$ we know:

$$(\tau, e_1, e_2) \in \mathbf{S}(W_{\mathrm{ref}}.\mathsf{L}(s_{\mathrm{rf}})(G(s)), G(s)) \vee$$
$$(\tau, e_1, e_2) \in \mathbf{S}(w_1.\mathsf{L}(s_{\mathrm{rf}})(s_1)(G(s)), G(s)) \vee$$
$$(\tau, e_1, e_2) \in \mathbf{S}(w_2.\mathsf{L}(s_{\mathrm{rf}})(s_2)(G(s)), G(s))$$

- This implies:

$$(\tau, e_1, e_2) \in \mathbf{S}(w_1\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s_1)(G(s)), G(s)) \vee$$
$$(\tau, e_1, e_2) \in \mathbf{S}(w_2\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s_2)(G(s)), G(s))$$

- If the former is true, the goal follows from $consistent(w_1\uparrow)$ with the help of Lemmas 19 and 21.
- If the latter is true, the goal follows from $consistent(w_2\uparrow)$ with the help of Lemmas 20 and 22.

■

Lemma 24. For $G \in \mathrm{GK}(W)$, $s_0, s_0', s \in W.\mathsf{S}$, $\tau, \tau' \in \mathrm{CType}$, $K_1, K_2 \in \mathrm{Cont}$, if

$$\forall s' \sqsupseteq [s_0', s].\forall G' \supseteq G.\ (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')\,,$$

then:

1) $(\tau', e_1, e_2) \in \mathbf{E}_W(G)(s_0', s)$ implies $(\tau, K_1[e_1], K_2[e_2]) \in \mathbf{E}_W(G)(s_0, s)$.
2) $(\tau'', \tau', K_1', K_2') \in \mathbf{K}_W(G)(s_0', s)$ implies $(\tau'', \tau, K_1[K_1'], K_2[K_2']) \in \mathbf{K}_W(G)(s_0, s)$.

Proof: We define $\mathbf{E}'_W$ and $\mathbf{K}'_W$ as follows:

$$\mathbf{E}'_W(G)(s_0,s) = \{\, (\tau, K_1[e_1], K_2[e_2]) \mid \exists \tau', s_0'.\ (\tau', e_1, e_2) \in \mathbf{E}_W(G)(s_0', s) \wedge \forall s' \sqsupseteq [s_0', s].\forall G' \supseteq G.\ (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')\,\}$$

$$\mathbf{K}'_W(G)(s_0,s) = \{\, (\tau'', \tau, K_1[K_1'], K_2[K_2']) \mid \exists \tau', s_0'.\ (\tau'', \tau', K_1', K_2') \in \mathbf{K}_W(G)(s_0', s) \wedge \forall s' \sqsupseteq [s_0', s].\forall G' \supseteq G.\ (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')\,\}$$

It suffices to show $\mathbf{E}'_W \subseteq \mathbf{E}_W$ and $\mathbf{K}'_W \subseteq \mathbf{K}_W$, which we do by coinduction. Concretely, we have to show:

1) $\forall K_1, K_2, e_1, e_2, G, s_0, s, \tau.$
   $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'_W(G)(s_0,s)(\tau) \implies$
   $\forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)).\forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.$
   $((h_1, h_1^{\mathrm{F}}, K_1[e_1]), (h_2, h_2^{\mathrm{F}}, K_2[e_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0,s)(\tau)$
2) $\forall K_1, K_2, K_1', K_2', G, s_0, s, \tau'', \tau.$
   $(K_1[K_1'], K_2[K_2']) \in \mathbf{K}'_W(G)(s_0,s)(\tau'', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s)}(\tau'').\ (K_1[K_1'][v_1], K_2[K_2'][v_2]) \in \mathbf{E}'_W(G)(s_0,s)(\tau)$

For (1):

- Suppose $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'_W(G)(s_0,s)(\tau)$ and $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$.
- By definition of $\mathbf{E}'_W$ we know $(e_1, e_2) \in \mathbf{E}_W(G)(s_0', s)(\tau')$ and

$$\forall s' \sqsupseteq [s_0', s].\forall G' \supseteq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$

  for some s_0' and τ'.
- We must show $((h_1, h_1^{\mathrm{F}}, K_1[e_1]), (h_2, h_2^{\mathrm{F}}, K_2[e_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0,s)(\tau)$.
- So suppose $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- We know $((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0', s)(\tau')$.
- Hence at least one of the following three properties holds:

A) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{\omega}$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^{\omega}$
B) a) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{*} h_1' \uplus h_1^{\mathrm{F}}, v_1$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^{*} h_2' \uplus h_2^{\mathrm{F}}, v_2$
   b) $s' \sqsupseteq [s_0', s]$
   c) $(h_1', h_2') \in W.\mathsf{H}(s')(G(s'))$

d) $(v_1, v_2) \in \overline{G(s')}(\tau')$

C) a) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1'[e_1']$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2'[e_2']$

b) $s' \sqsupseteq s$

c) $(h_1', h_2') \in W.\mathsf{H}(s')(G(s'))$

d) $(e_1', e_2') \in \mathbf{S}(G(s'), G(s'))(\widetilde{\tau})$

e) $\forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \supseteq G.\ (K_1', K_2') \in \mathbf{K}_W(G')(s_0', s'')(\widetilde{\tau}, \tau')$

- If (A) holds:
  - Then $h_1 \uplus h_1^{\mathrm{F}}, K_1[e_1] \hookrightarrow^\omega$ and $h_2 \uplus h_2^{\mathrm{F}}, K_2[e_2] \hookrightarrow^\omega$, so we are done.
- If (B) holds:
  - Then $h_1 \uplus h_1^{\mathrm{F}}, K_1[e_1] \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[v_1]$ and $h_2 \uplus h_2^{\mathrm{F}}, K_2[e_2] \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[v_2]$ from (Ba).
  - Since $(K_1, K_2) \in \mathbf{K}_W(G)(s_0, s')(\tau', \tau)$ from (Bb), we get $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s_0, s')(\tau)$ from (Bd).
  - Using (Bc), this implies $((h_1', h_1^{\mathrm{F}}, K_1[v_1]), (h_2', h_2^{\mathrm{F}}, K_2[v_2])) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0, s')(\tau)$.
  - We show $\mathbf{O}_W(\mathbf{K}_W)(G)(s_0, s')(\tau) \subseteq \mathbf{O}_W(\mathbf{K}_W')(G)(s_0, s')(\tau)$:
    - It suffices to show $\mathbf{K}_W \subseteq \mathbf{K}_W'$.
    - By definition of the latter, this follows from Lemmas 18 and 17.
  - Consequently, $((h_1', h_1^{\mathrm{F}}, K_1[v_1]), (h_2', h_2^{\mathrm{F}}, K_2[v_2])) \in \mathbf{O}_W(\mathbf{K}_W')(G)(s_0, s')(\tau)$.
  - We are done by (Bb) and Lemma 15.
- If (C) holds:
  - Then $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[K_1'][e_1']$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[K_2'][e_2']$ from (Ca).
  - Due to (Cb–d) it remains to show:
    $$\forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \supseteq G.\ (K_1[K_1'], K_2[K_2']) \in \mathbf{K}_W'(G')(s_0, s'')(\widetilde{\tau}, \tau)$$
  - So suppose $s'' \sqsupseteq_{\mathrm{pub}} s'$ and $G' \supseteq G$.
  - By definition of $\mathbf{K}_W'$ it suffices to show $(K_1', K_2') \in \mathbf{K}_W(G')(s_0', s'')(\widetilde{\tau}, \tau')$ and
    $$\forall s''' \sqsupseteq [s_0', s''].\forall G'' \supseteq G'.\ (K_1, K_2) \in \mathbf{K}_W(G'')(s_0, s''')(\tau', \tau).$$
  - The former follows from (Ce).
  - For the latter, recall that
    $$\forall s' \sqsupseteq [s_0', s].\forall G' \supseteq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau).$$
  - Since $s'' \sqsupseteq_{\mathrm{pub}} s' \sqsupseteq s$ and $G'' \supseteq G' \supseteq G$, we are done.

For (2):

- Suppose $(K_1[K_1'], K_2[K_2']) \in \mathbf{K}_W'(G)(s_0, s)(\tau'', \tau)$ and $(v_1, v_2) \in \overline{G(s)}(\tau'')$.
- By definition of $\mathbf{K}_W'$ we know $(K_1', K_2') \in \mathbf{K}_W(G)(s_0', s)(\tau'', \tau')$ and
  $$\forall s' \sqsupseteq [s_0', s].\forall G' \supseteq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$
  for some s_0' and τ'.
- We must show $(K_1[K_1'][v_1], K_2[K_2'][v_2]) \in \mathbf{E}_W'(G)(s_0, s)(\tau)$.
- By definition of $\mathbf{E}_W'$ it suffices to show $(K_1'[v_1], K_2'[v_2]) \in \mathbf{E}_W(G)(s_0', s)(\tau')$ and
  $$\forall s' \sqsupseteq [s_0', s].\forall G' \supseteq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau).$$
- The latter is given and the former follows from $(K_1', K_2') \in \mathbf{K}_W(G)(s_0', s)(\tau'', \tau')$ and $(v_1, v_2) \in \overline{G(s)}(\tau'')$.

■

Lemma 25. If $\mathit{inhabited}(w_2{\uparrow})$, $\mathit{consistent}(w_2{\uparrow})$, $\mathit{stable}(w_2)$, and $\mathrm{defined}(w_1 \otimes w_2)$, then:

$$\Delta; \Gamma \vdash e_1 \sim_{w_1} e_2 : \sigma \quad \Longrightarrow \quad \Delta; \Gamma \vdash e_1 \sim_{w_1 \otimes w_2} e_2 : \sigma$$

Proof:

- Using the assumptions and Lemma 23, we get $\mathit{inhabited}((w_1 \otimes w_2){\uparrow})$ and $\mathit{consistent}((w_1 \otimes w_2){\uparrow})$ as well as $\mathit{stable}(w_1 \otimes w_2)$.
- Now suppose $G \in \mathrm{GK}((w_1 \otimes w_2){\uparrow})$ and $\delta \in \mathrm{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$.
- We must show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{(w_1 \otimes w_2){\uparrow}}(G)((s_{\mathrm{rf}}, s, s'), (s_{\mathrm{rf}}, s, s'))(\delta\sigma)$.
- From $\Delta; \Gamma \vdash e_1 \sim_{w_1} e_2 : \sigma$ and Lemma 19 we know:
  $$(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{w_1{\uparrow}}(G(-, -, s'))((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\delta\sigma)$$

- We are done by Lemma 21.

■

Lemma 26. If $\forall w.\ \big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim_w e_i' : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim_{w\uparrow} e' : \sigma$, then
$$\big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim e_i' : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim e' : \sigma\ .$$

Proof:

- Suppose $\forall w.\ \big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim_w e_i' : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim_{w\uparrow} e' : \sigma$ and $\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim e_i' : \sigma_i$.
- Given $\mathcal{N} \in \mathrm{Names}$, since $\mathcal{N}$ is countably infinite, we can split it into $\mathcal{N}_i$'s such that $\mathcal{N} = \mathcal{N}_1 \uplus \dots \uplus \mathcal{N}_n$.
- Thus by the premise we have w_i's such that for all i, $w_i.\mathsf{N} \subseteq \mathcal{N}_i$ and $\Delta_i; \Gamma_i \vdash e_i \sim_{w_i} e_i' : \sigma_i$.
- Since $w_i.\mathsf{N}$'s are disjoint, by applying Lemma 25 repeatedly, we have $\Delta_i; \Gamma_i \vdash e_i \sim_{w_1 \otimes \dots \otimes w_n} e_i' : \sigma_i$ for all i.
- By the assumption we thus have $\Delta; \Gamma \vdash e \sim_{(w_1 \otimes \dots \otimes w_n)\uparrow} e' : \sigma$.
- Using Lemma 23 we get $\mathit{stable}(w_1 \otimes \dots \otimes w_n)$ and thus $\Delta; \Gamma \vdash e \sim_{w_1 \otimes \dots \otimes w_n} e' : \sigma$
- By definition of $\otimes$, we have $(w_1 \otimes \dots \otimes w_n).\mathsf{N} \subseteq \mathcal{N}_1 \uplus \dots \uplus \mathcal{N}_n = \mathcal{N}$, and thus $\Delta; \Gamma \vdash e \sim e' : \sigma$.

■

Lemma 27. If $\forall W.\ \big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim_W e_i' : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim_W e' : \sigma$, then:
$$\big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim e_i' : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim e' : \sigma$$

Proof: Immediate consequence of Lemma 26. ■

Lemma 28. If $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)).\ (\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G)(s,s)(\delta\sigma', \delta\sigma)$ then
$$\Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma' \quad \implies \quad \Delta; \Gamma \vdash K_1[e_1] \sim_W K_2[e_2] : \sigma$$

Proof:

- Suppose $G \in \mathrm{GK}(W)$, $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$.
- We must show $((\gamma_1 K_1)[\gamma_1 e_1], (\gamma_2 K_2)[\gamma_2 e_2]) \in \mathbf{E}_W(G)(s,s)(\delta\sigma)$.
- From the premise we get $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_W(G)(s,s)(\delta\sigma')$.
- By Lemma 24 it suffices to show
$$(\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G')(s, s^\circ)(\delta\sigma', \delta\sigma)$$
for $s^\circ \sqsupseteq_{\mathrm{pub}} s$ and $G' \supseteq G$.
- By Lemma 18 it then suffices to show
$$(\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G')(s^\circ, s^\circ)(\delta\sigma', \delta\sigma),$$
which follows from Lemma 12 and the assumption.

■

Lemma 29 (External call)**.** For any $G \in \mathrm{GK}(W)$ and $\boldsymbol{\mathcal{R}} \in W.\mathsf{S} \to \mathrm{VRelF}$, if
$$\mathit{consistent}(W)\ \wedge\ \forall s.\ G(s) = W.\mathsf{L}(s)(G(s)) \cup \boldsymbol{\mathcal{R}}(s)\ ,$$
then we have
$$\begin{array}{l}
\forall (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0, s).\ \forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)).\\
\forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.\ h_1 \uplus h_1^{\mathrm{F}} \text{ defined} \wedge h_2 \uplus h_2^{\mathrm{F}} \text{ defined} \implies \\
\qquad (h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^\omega \wedge\ h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^\omega)\\
\qquad \vee\ (\exists h_1', h_2', v_1, v_2.\ h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, v_2 \wedge\\
\qquad\quad \exists s' \sqsupseteq [s_0, s].\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (v_1, v_2) \in \overline{G(s')}(\tau))\\
\qquad \vee\ (\exists h_1', h_2', \tau', K_1, K_2, e_1', e_2'.\\
\qquad\quad h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'] \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[e_2'] \wedge\\
\qquad\quad \exists s' \sqsupseteq s.\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (\tau', e_1', e_2') \in \mathbf{S}(\boldsymbol{\mathcal{R}}(s'), G(s')) \wedge\\
\qquad\quad \forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \supseteq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'')(\tau', \tau))
\end{array}$$

Proof:

- We prove the following proposition by induction on n.

$$\begin{array}{l}\forall(\tau,e_1,e_2)\in\mathbf{E}_W(G)(s_0,s).\ \forall(h_1,h_2)\in W.\mathsf{H}(s)(G(s)).\\ \forall h_1^{\mathrm{F}},h_2^{\mathrm{F}}.\ h_1\uplus h_1^{\mathrm{F}}\text{ defined}\wedge h_2\uplus h_2^{\mathrm{F}}\text{ defined}\implies\\ \qquad (h_1\uplus h_1^{\mathrm{F}},e_1\hookrightarrow^n\wedge\ h_2\uplus h_2^{\mathrm{F}},e_2\hookrightarrow^n)\\ \quad\vee\ (\exists h_1',h_2',v_1,v_2.\ h_1\uplus h_1^{\mathrm{F}},e_1\hookrightarrow^* h_1'\uplus h_1^{\mathrm{F}},v_1\wedge h_2\uplus h_2^{\mathrm{F}},e_2\hookrightarrow^* h_2'\uplus h_2^{\mathrm{F}},v_2\wedge\\ \qquad \exists s'\sqsupseteq[s_0,s].\ (h_1',h_2')\in W.\mathsf{H}(s')(G(s'))\wedge(v_1,v_2)\in\overline{G(s')}(\tau))\\ \quad\vee\ (\exists h_1',h_2',\tau',K_1,K_2,e_1',e_2'.\\ \qquad h_1\uplus h_1^{\mathrm{F}},e_1\hookrightarrow^* h_1'\uplus h_1^{\mathrm{F}},K_1[e_1']\wedge h_2\uplus h_2^{\mathrm{F}},e_2\hookrightarrow^* h_2'\uplus h_2^{\mathrm{F}},K_2[e_2']\wedge\\ \qquad \exists s'\sqsupseteq s.\ (h_1',h_2')\in W.\mathsf{H}(s')(G(s'))\wedge(\tau',e_1',e_2')\in\mathbf{S}(\boldsymbol{\mathcal{R}}(s'),G(s'))\wedge\\ \qquad \forall s''\sqsupseteq_{\mathrm{pub}}s'.\ \forall G'\supseteq G.\ (K_1,K_2)\in\mathbf{K}_W(G')(s_0,s'')(\tau',\tau))\end{array}\tag{21}$$

- When $n=0$, the first case holds vacuously.
- When $n>0$, we assume that the goal (21) holds for $n-1$. Then we need to show that the goal (21) holds for n.
- By definition of $\mathbf{E}_W(G)(s_0,s)$, we have three cases.
- In the first two cases, the goal (21) is trivially satisfied.
- In the third case, we have

$$\begin{array}{l}\exists h_1',h_2',\tau',K_1,K_2,e_1',e_2'.\\ \quad h_1\uplus h_1^{\mathrm{F}},e_1\hookrightarrow^* h_1'\uplus h_1^{\mathrm{F}},K_1[e_1']\wedge h_2\uplus h_2^{\mathrm{F}},e_2\hookrightarrow^* h_2'\uplus h_2^{\mathrm{F}},K_2[e_2']\wedge\\ \quad \exists s'\sqsupseteq s.\ (h_1',h_2')\in W.\mathsf{H}(s')(G(s'))\wedge(\tau',e_1',e_2')\in\mathbf{S}(G(s'),G(s'))\wedge\\ \quad \forall s''\sqsupseteq_{\mathrm{pub}}s'.\ \forall G'\supseteq G.\ (K_1,K_2)\in\mathbf{K}_W(G')(s_0,s'')(\tau',\tau)\end{array}$$

- As $G(s')=W.\mathsf{L}(s')(G(s'))\cup\boldsymbol{\mathcal{R}}(s')$, by definition of $\mathbf{S}$, we have

$$(\tau',e_1',e_2')\in\mathbf{S}(G(s'),G(s'))=\mathbf{S}(W.\mathsf{L}(s')(G(s')),G(s'))\cup\mathbf{S}(\boldsymbol{\mathcal{R}}(s'),G(s'))\ .$$

- If $(\tau',e_1',e_2')\in\mathbf{S}(\boldsymbol{\mathcal{R}}(s'),G(s'))$, then the goal (21) is satisfied.
- If $(\tau',e_1',e_2')\in\mathbf{S}(W.\mathsf{L}(s')(G(s')),G(s'))$, then by $consistent(W)$, we have that $h_1'\uplus h_1^{\mathrm{F}},K_1[e_1']\hookrightarrow^1 h_1'\uplus h_1^{\mathrm{F}},K_1[beta(e_1')]$ and $h_2'\uplus h_2^{\mathrm{F}},K_2[e_2']\hookrightarrow^1 h_2'\uplus h_2^{\mathrm{F}},K_2[beta(e_2')]$ and $(\tau',beta(e_1'),beta(e_2'))\in\mathbf{E}_W(G)(s',s')$.
- By Lemma 24, we have $(\tau,K_1[beta(e_1')],K_2[beta(e_2')])\in\mathbf{E}_W(G)(s_0,s')$.
- As $(h_1',h_2')\in W.\mathsf{H}(s')(G(s'))$, by induction hypothesis we have that $h_1'\uplus h_1^{\mathrm{F}},K_1[beta(e_1')]$ and $h_2'\uplus h_2^{\mathrm{F}},K_2[beta(e_2')]$ satisfy the goal (21) for $n-1$ w.r.t. (s_0,s').
- As $h_1\uplus h_1^{\mathrm{F}},e_1\hookrightarrow^+ h_1'\uplus h_2^{\mathrm{F}},K_1[beta(e_1')]\wedge h_2\uplus h_2^{\mathrm{F}},e_2\hookrightarrow^+ h_2'\uplus h_2^{\mathrm{F}},K_2[beta(e_2')]$ and $s'\sqsupseteq s$, we have that $h_1\uplus h_1^{\mathrm{F}},e_1$ and $h_2\uplus h_2^{\mathrm{F}},e_2$ satisfy the goal (21) for n w.r.t. (s_0,s), so we are done.
- The original goal is obtained from the sub-goal (21) by pushing the quantification over n inside the first case and then observing that $\forall n.\ h,e\hookrightarrow^n$ is equivalent to $h,e\hookrightarrow^\omega$.

■

Corollary 30. If

- $consistent(W)$
- $\forall s.\ G(s)=W.\mathsf{L}(s)(G(s))$
- $(\tau,e_1,e_2)\in\mathbf{E}_W(G)(s_0,s)$
- $(h_1,h_2)\in W.\mathsf{H}(s)(G(s))$ and $h_1\uplus h_1^{\mathrm{F}}\ ,h_2\uplus h_2^{\mathrm{F}}$ defined

then one of the following holds:

1) $h_1\uplus h_1^{\mathrm{F}},e_1\hookrightarrow^\omega\wedge\ h_2\uplus h_2^{\mathrm{F}},e_2\hookrightarrow^\omega$
2) $\exists h_1',h_2',v_1,v_2,s'.$
   $h_1\uplus h_1^{\mathrm{F}},e_1\hookrightarrow^* h_1'\uplus h_1^{\mathrm{F}},v_1\wedge h_2\uplus h_2^{\mathrm{F}},e_2\hookrightarrow^* h_2'\uplus h_2^{\mathrm{F}},v_2\wedge$
   $s'\sqsupseteq_{\mathrm{pub}}[s_0,s]\wedge(h_1',h_2')\in W.\mathsf{H}(s')(G(s'))\wedge(\tau,v_1,v_2)\in\overline{G(s')}$

Proof: Follows from Lemma 29 for $\mathcal{R}=\lambda s.\emptyset$. ■

2) Compatibility.

Lemma 31 (Compatibility: Var)**.**

$$\frac{\Delta\vdash\Gamma\quad x{:}\sigma\in\Gamma}{\Delta;\Gamma\vdash x\sim x:\sigma}$$

Proof:

- Let $w_{\mathrm{id}}=w_{\mathrm{single}}(\lambda R.\emptyset,\lambda R.\{(\emptyset,\emptyset)\})$ (so $w_{\mathrm{id}}.\mathsf{N}\subseteq\mathcal{N}$ for any $\mathcal{N}$).

- We are done if we can show $\Delta;\Gamma \vdash x \sim_{w_{\mathrm{id}}} x : \sigma$.
- It is obvious that $\mathit{stable}(w_{\mathrm{id}})$ (the dependency is vacuous) and that $\mathit{consistent}(w_{\mathrm{id}}\uparrow)$ (neither W_{ref} nor w_{id} relates any functions).
- $\mathit{inhabited}(w_{\mathrm{id}}\uparrow)$ is witnessed by state $(\emptyset, *)$.
- Now suppose $G \in \mathrm{GK}(w_{\mathrm{id}}\uparrow)$ and $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$.
- We must show $(\gamma_1(x), \gamma_2(x)) \in \mathbf{E}_{w_{\mathrm{id}}\uparrow}(G)(s,s)(\delta\sigma)$.
- From $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$ we know $(\gamma_1(x), \gamma_2(x)) \in \overline{G(s)}(\delta\sigma)$.
- We are done by Lemma 16.

■

Lemma 32.

1) If $(\tau, v_1, v_2) \in \overline{G(s)}$, then $(\tau', \tau \times \tau', \langle v_1, \bullet\rangle, \langle v_2, \bullet\rangle) \in \mathbf{K}_W(G)(s,s)$.
2) If $(\tau', e_1', e_2') \in \mathbf{E}_W(G)(s_0, s)$, then $(\tau, \tau \times \tau', \langle \bullet, e_1'\rangle, \langle \bullet, e_2'\rangle) \in \mathbf{K}_W(G)(s_0, s)$.

Proof:

1) • Suppose $(v_1', v_2') \in \overline{G(s)}(\tau')$.
   • We need to show $(\langle v_1, v_1'\rangle, \langle v_2, v_2'\rangle) \in \mathbf{E}_W(G)(s,s)(\tau \times \tau')$.
   • By Lemma 16 it suffices to show $(\langle v_1, v_1'\rangle, \langle v_2, v_2'\rangle) \in \overline{G(s)}(\tau \times \tau')$.
   • Hence it suffices to show $(v_1, v_2) \in \overline{G(s)}(\tau)$ and $(v_1', v_2') \in \overline{G(s)}(\tau')$, which we both already have.
2) • Suppose $(v_1, v_2) \in \overline{G(s)}(\tau)$.
   • We need to show $(\langle v_1, e_1'\rangle, \langle v_2, e_2'\rangle) \in \mathbf{E}_W(G)(s_0, s)(\tau \times \tau')$.
   • By Lemma 24 it suffices to show
   $$(\langle v_1, \bullet\rangle, \langle v_2, \bullet\rangle) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau \times \tau')$$
   for $s' \sqsupseteq [s_0, s]$ and $G' \supseteq G$.
   • By Lemma 18 it suffices to show $(\langle v_1, \bullet\rangle, \langle v_2, \bullet\rangle) \in \mathbf{K}_W(G')(s', s')(\tau', \tau \times \tau')$.
   • By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(s')}(\tau)$, which follows from $(v_1, v_2) \in \overline{G(s)}(\tau)$ by Lemma 12.

■

Lemma 33 (Compatibility: Pair)**.**

$$\frac{\Delta;\Gamma \vdash e_1 \sim e_2 : \sigma \qquad \Delta;\Gamma \vdash e_1' \sim e_2' : \sigma'}{\Delta;\Gamma \vdash \langle e_1, e_1'\rangle \sim \langle e_2, e_2'\rangle : \sigma \times \sigma'}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\langle \bullet, \gamma_1 e_1'\rangle, \langle \bullet, \gamma_2 e_2'\rangle) \in \mathbf{K}_W(G)(s,s)(\delta\sigma, \delta\sigma \times \delta\sigma')$$
assuming $\Delta;\Gamma \vdash e_1' \sim_W e_2' : \sigma'$.
- By Lemma 32 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_W(G)(s,s)(\delta\sigma')$, which follows from the assumption.

■

Lemma 34 (Compatibility: Fst (Snd analogously))**.**

$$\frac{\Delta;\Gamma \vdash e_1 \sim e_2 : \sigma \times \sigma'}{\Delta;\Gamma \vdash e_1.1 \sim e_2.1 : \sigma}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\bullet.1, \bullet.1) \in \mathbf{K}_W(G)(s,s)(\delta\sigma \times \delta\sigma', \delta\sigma)\ .$$
- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\delta\sigma \times \delta\sigma')$.
- We need to show $(v_1^\circ.1, v_2^\circ.1) \in \mathbf{E}_W(G)(s,s)(\delta\sigma)$.
- Suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- We know $v_1^\circ = \langle v_1, v_1'\rangle$ and $v_2^\circ = \langle v_2, v_2'\rangle$ with $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.
- Hence $h_1 \uplus h_1^{\mathrm{F}}, v_1^\circ.1 \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, v_1$ and $h_2 \uplus h_2^{\mathrm{F}}, v_2^\circ.1 \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, v_2$.
- Since $s \sqsupseteq [s, s]$, we are done.

■

Lemma 35 (Compatibility: Inl (Inr analogously))**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \mathsf{inj}^1\, e_1 \sim \mathsf{inj}^1\, e_2 : \sigma + \sigma'}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)),$
$$(\mathsf{inj}^1\, \bullet, \mathsf{inj}^1\, \bullet) \in \mathbf{K}_W(G)(s,s)(\delta\sigma, \delta\sigma + \delta\sigma')\ .$$
- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.
- We need to show $(\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \in \mathbf{E}_W(G)(s,s)(\delta\sigma + \delta\sigma')$.
- By Lemma 16 it suffices to show $(\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \in \overline{G(s)}(\delta\sigma + \delta\sigma')$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.

■

Lemma 36 (Compatibility: Case)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma' + \sigma'' \qquad \Delta; \Gamma, x{:}\sigma' \vdash e_1' \sim e_2' : \sigma \qquad \Delta; \Gamma, x{:}\sigma'' \vdash e_1'' \sim e_2'' : \sigma}{\Delta; \Gamma \vdash \mathsf{case}\, e_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_1' \mid \mathsf{inj}^2\, x \Rightarrow e_1'' \sim \mathsf{case}\, e_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_2' \mid \mathsf{inj}^2\, x \Rightarrow e_2'' : \sigma}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)),$
$$(\mathsf{case}\ \bullet\ \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \mid \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'', \mathsf{case}\ \bullet\ \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \mid \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'') \in \mathbf{K}_W(G)(s,s)(\delta\sigma' + \delta\sigma'', \delta\sigma)\ .$$
assuming $\Delta; \Gamma, x{:}\sigma' \vdash e_1' \sim_W e_2' : \sigma$ and $\Delta; \Gamma, x{:}\sigma'' \vdash e_1'' \sim_W e_2'' : \sigma$.
- Thus it suffices to show that $\forall (v_1, v_2) \in \overline{G(s)}(\delta\sigma' + \delta\sigma''),$
$$(\mathsf{case}\, v_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \mid \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'', \mathsf{case}\, v_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \mid \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'') \in \mathbf{E}_W(G)(s,s)(\delta\sigma)$$
- By definition of $\overline{G(s)}(\delta\sigma' + \delta\sigma'')$, we have v_1', v_2' such that either
1) $v_1 = \mathsf{inj}^1\, v_1' \wedge v_2 = \mathsf{inj}^1\, v_2' \wedge (v_1', v_2') \in \overline{G(s)}(\delta\sigma')$; or
2) $v_1 = \mathsf{inj}^2\, v_1' \wedge v_2 = \mathsf{inj}^2\, v_2' \wedge (v_1', v_2') \in \overline{G(s)}(\delta\sigma'')$.
- We show the former case (the latter case can be done analogousely).
- Let $\gamma_1' := \gamma_1, x{\mapsto}v_1'$ and $\gamma_2' := \gamma_2, x{\mapsto}v_2'$.
- Now suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ and $h_1^{\mathrm{F}}, h_2^{\mathrm{F}} \in \mathrm{Heap}$ with $h_1 \uplus h_1^{\mathrm{F}}, h_2 \uplus h_2^{\mathrm{F}}$ defined.
- We have
$$h_1 \uplus h_1^{\mathrm{F}}, \mathsf{case}\, v_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \mid \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'' \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, \gamma_1' e_1'$$
and
$$h_2 \uplus h_2^{\mathrm{F}}, \mathsf{case}\, v_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \mid \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'' \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, \gamma_2' e_2'$$
- Thus by Lemma 15, it suffices to show
$$(\delta\sigma', (h_1, h_1^{\mathrm{F}}, \gamma_1' e_1'), (h_2, h_2^{\mathrm{F}}, \gamma_2' e_2')) \in \mathbf{O}_W(\mathbf{E}_W)(G)(s,s)\ .$$
- This follows from the assumption and $(\gamma_1', \gamma_2') \in \mathrm{Env}(\delta(\Gamma, x : \sigma'), G(s))$.

■

Lemma 37 (Compatibility: Fix)**.**

$$\frac{\Delta; \Gamma, f{:}\sigma' \to \sigma, x{:}\sigma' \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \mathsf{fix}\, f(x).\, e_1 \sim \mathsf{fix}\, f(x).\, e_2 : \sigma' \to \sigma}$$

Proof:

- For any $\mathcal{N}$, from the premise we have w such that $w.\mathsf{N} \subseteq \mathcal{N}$ and $\Delta; \Gamma, f{:}\sigma' \to \sigma, x{:}\sigma' \vdash e_1 \sim_w e_2 : \sigma$.
- Let $w' = w_{\mathrm{single}}(\lambda R.\ \{(\delta\sigma' \to \delta\sigma, \gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \mid \delta \in \mathrm{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, R)\}, \lambda R.\ \{(\emptyset, \emptyset)\})$.
- Since $(w \otimes w').\mathsf{N} = w.\mathsf{N} \subseteq \mathcal{N}$, it suffices to show $\Delta; \Gamma \vdash \mathsf{fix}\, f(x).\, e_1 \sim_{w \otimes w'} \mathsf{fix}\, f(x).\, e_2 : \sigma' \to \sigma$.
- To do so, we first prove $\mathit{inhabited}((w \otimes w')\uparrow)$ and $\mathit{consistent}((w \otimes w')\uparrow)$:
  - $\mathit{inhabited}(w'\uparrow)$ is witnessed by state $(\emptyset, *)$, so $\mathit{inhabited}((w \otimes w')\uparrow)$ holds by Lemma 23.
  - The part of $\mathit{consistent}((w \otimes w')\uparrow)$ concerning universal types follows from $\mathit{consistent}(w\uparrow)$ by Lemma 23, because $w'.\mathsf{L}$ doesn't relate anything at universal types.

– Regarding the part concerning arrow types, we suppose
  1) $G \in \mathrm{GK}((w \otimes w')\uparrow)$
  2) $(v_1, v_2) \in \overline{(w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s, s')(G(s_{\mathrm{rf}}, s, s'))}(\widetilde{\sigma'} \to \widetilde{\sigma})$
  3) $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s, s')}(\widetilde{\sigma'})$

  and must show:
$$(beta(v_1\ v_1'), beta(v_2\ v_2')) \in \mathbf{E}_{(w\otimes w')\uparrow}(G)((s_{\mathrm{rf}}, s, s'), (s_{\mathrm{rf}}, s, s'))(\widetilde{\sigma})$$
– From (2) and the definition of $\uparrow$ and $\otimes$ we know:
$$(v_1, v_2) \in w\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s, s'))(\widetilde{\sigma'} \to \widetilde{\sigma}) \vee$$
$$(v_1, v_2) \in w'.\mathsf{L}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s, s'))(\widetilde{\sigma'} \to \widetilde{\sigma})$$
– If the former is true, the claim follows from $consistent(w\uparrow)$ with the help of Lemmas 19 and 21.
– So suppose the latter.
– Then $\sigma' \to \widetilde{\sigma} = \delta\sigma' \to \delta\sigma$ and $v_1 = \gamma_1 \mathsf{fix}\, f(x).\, e_1$ and $v_2 = \gamma_2 \mathsf{fix}\, f(x).\, e_2$ for $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$.
– Let $\gamma_1' = \gamma_1, f{\mapsto}\gamma_1 \mathsf{fix}\, f(x).\, e_1, x{\mapsto}v_1'$ and $\gamma_2' = \gamma_2, f{\mapsto}\gamma_2 \mathsf{fix}\, f(x).\, e_2, x{\mapsto}v_2'$
– It remains to show $(\gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_{(w\otimes w')\uparrow}(G)((s_{\mathrm{rf}}, s, s'), (s_{\mathrm{rf}}, s, s'))(\delta\sigma)$.
– By Lemmas 19 and 21 it suffices to show $(\gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_{w\uparrow}(G(-, -, s'))((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\delta\sigma)$.
– This follows from the premise if we can show $(\gamma_1', \gamma_2') \in \mathrm{Env}((\delta\Gamma, f{:}\delta\sigma' \to \delta\sigma, x{:}\delta\sigma'), G(s_{\mathrm{rf}}, s, s'))$.
– This reduces to showing $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s, s')}(\delta\sigma')$ and
$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in \overline{G(s_{\mathrm{rf}}, s, s')}(\delta\sigma' \to \delta\sigma).$$
– The former is given as (3).
– For the latter, note that by definition of GK it suffices to show
$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s, s')(G(s_{\mathrm{rf}}, s, s'))(\delta\sigma' \to \delta\sigma).$$
– By definition of $\uparrow$ and $\otimes$ it then suffices to show
$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in w'.\mathsf{L}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s, s'))(\delta\sigma' \to \delta\sigma).$$
– Since $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$, this holds by construction.

- Now suppose $G \in \mathrm{GK}((w \otimes w')\uparrow)$ and $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$.
- We must show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in \mathbf{E}_{(w\otimes w')\uparrow}(G)((s_{\mathrm{rf}}, s, s'), (s_{\mathrm{rf}}, s, s'))(\delta\sigma' \to \delta\sigma)$.
- By Lemma 16 it suffices to show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in G(s_{\mathrm{rf}}, s, s')(\delta\sigma' \to \delta\sigma)$.
- By definition of GK it suffices to show:
$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s, s')(G(s_{\mathrm{rf}}, s, s'))(\delta\sigma' \to \delta\sigma)$$
- By definition of $\uparrow$ and $\otimes$ it suffices to show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in w'.\mathsf{L}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s, s'))(\delta\sigma' \to \delta\sigma)$.
- Since $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$, this holds by construction of w'.

■

Lemma 38.

1) If $(\tau' \to \tau, v_1, v_2) \in \overline{G(s)}$, then $(\tau', \tau, v_1\ \bullet, v_2\ \bullet) \in \mathbf{K}_W(G)(s, s)$.
2) If $(\tau', e_1', e_2') \in \mathbf{E}_W(G)(s_0, s)$, then $(\tau' \to \tau, \tau, \bullet\ e_1', \bullet\ e_2') \in \mathbf{K}_W(G)(s_0, s)$.

Proof:

1) • Suppose $(v_1', v_2') \in \overline{G(s)}(\tau')$.
   • We need to show $(v_1\ v_1', v_2\ v_2') \in \mathbf{E}_W(G)(s, s)(\tau)$.
   • By definition of $\mathbf{E}_W$ it suffices to show the following:
     a) $(v_1, v_2) \in \overline{G(s)}(\tau' \to \tau)$
     b) $(v_1', v_2') \in \overline{G(s)}(\tau')$
     c) $\forall s' \sqsupseteq_{\mathrm{pub}} s.\forall G' \supseteq G.\ (\bullet, \bullet) \in \mathbf{K}_W(G')(s, s')(\tau, \tau)$
   • (a) and (b) are already given.
   • (c) follows by Lemmas 17 and 18.
2) • Suppose $(v_1, v_2) \in \overline{G(s)}(\tau' \to \tau)$.
   • We need to show $(v_1\ e_1', v_2\ e_2') \in \mathbf{E}_W(G)(s_0, s)(\tau)$.

- By Lemma 24 it suffices to show
$$(v_1 \bullet, v_2 \bullet) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$
for $s' \sqsupseteq [s_0, s]$ and $G' \supseteq G$.
- By Lemma 18 it suffices to show $(v_1 \bullet, v_2 \bullet) \in \mathbf{K}_W(G')(s', s')(\tau', \tau)$.
- By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(s')}(\tau' \to \tau)$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\tau' \to \tau)$ by Lemma 12.

■

Lemma 39 (Compatibility: App)**.**
$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma' \to \sigma \qquad \Delta; \Gamma \vdash e_1' \sim e_2' : \sigma'}{\Delta; \Gamma \vdash e_1\ e_1' \sim e_2\ e_2' : \sigma}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\bullet\ \gamma_1 e_1', \bullet\ \gamma_2 e_2') \in \mathbf{K}_W(G)(s, s)(\delta\sigma' \to \delta\sigma, \delta\sigma)$$
assuming $\Delta; \Gamma \vdash e_1' \sim_W e_2' : \sigma'$.
- By Lemma 38 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_W(G)(s, s)(\delta\sigma')$, which follows from the assumption.

■

Lemma 40 (Compatibility: Roll)**.**
$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma[\mu\alpha.\, \sigma/\alpha]}{\Delta; \Gamma \vdash \mathsf{roll}\ e_1 \sim \mathsf{roll}\ e_2 : \mu\alpha.\, \sigma}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\mathsf{roll}\ \bullet, \mathsf{roll}\ \bullet) \in \mathbf{K}_W(G)(s, s)(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha], \mu\alpha.\, \delta\sigma)\ .$$
- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.
- We need to show $(\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \in \mathbf{E}_W(G)(s, s)(\mu\alpha.\, \delta\sigma)$.
- By Lemma 16 it suffices to show $(\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \in \overline{G(s)}(\mu\alpha.\, \delta\sigma)$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.

■

Lemma 41 (Compatibility: Unroll)**.**
$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mu\alpha.\, \sigma}{\Delta; \Gamma \vdash \mathsf{unroll}\ e_1 \sim \mathsf{unroll}\ e_2 : \sigma[\mu\alpha.\, \sigma/\alpha]}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\mathsf{unroll}\ \bullet, \mathsf{unroll}\ \bullet) \in \mathbf{K}_W(G)(s, s)(\mu\alpha.\, \delta\sigma, \delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])\ .$$
- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\mu\alpha.\, \delta\sigma)$.
- We need to show $(\mathsf{unroll}\ v_1^\circ, \mathsf{unroll}\ v_2^\circ) \in \mathbf{E}_W(G)(s, s)(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.
- Suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- We know $v_1^\circ = \mathsf{roll}\ v_1$ and $v_2^\circ = \mathsf{roll}\ v_2$ with $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.
- Hence $h_1 \uplus h_1^{\mathrm{F}}, \mathsf{unroll}\ v_1^\circ \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, v_1$ and $h_2 \uplus h_2^{\mathrm{F}}, \mathsf{unroll}\ v_2^\circ \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, v_2$.
- Since $s \sqsupseteq [s, s]$, we are done.

■

Lemma 42 (Compatibility: Ref)**.**
$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \mathsf{ref}\ e_1 \sim \mathsf{ref}\ e_2 : \mathsf{ref}\ \sigma}$$

Proof:

- By Lemmas 26 and 28, it suffices to show $\forall G, s_{\mathrm{rf}}, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\mathsf{ref}\ \bullet, \mathsf{ref}\ \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\delta\sigma, \mathsf{ref}\ \delta\sigma)\ .$$

- Suppose $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\delta\sigma)$.
- We need to show $(\mathsf{ref}\ v_1, \mathsf{ref}\ v_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\mathsf{ref}\ \delta\sigma)$.
- Suppose $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- We know $h_1 \uplus h_1^{\mathrm{F}}, \mathsf{ref}\ v_1 \hookrightarrow h_1 \uplus [\ell_1 \mapsto v_1] \uplus h_1^{\mathrm{F}}, \ell_1$ for $\ell_1 \notin \mathrm{dom}(h_1 \uplus h_1^{\mathrm{F}})$.
- Similarly, $h_2 \uplus h_2^{\mathrm{F}}, \mathsf{ref}\ v_2 \hookrightarrow h_2 \uplus [\ell_2 \mapsto v_2] \uplus h_2^{\mathrm{F}}, \ell_2$ for $\ell_2 \notin \mathrm{dom}(h_2 \uplus h_2^{\mathrm{F}})$.
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) \sqsupseteq [(s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s)]$ such that:
  1) $(h_1 \uplus [\ell_1 \mapsto v_1], h_2 \uplus [\ell_2 \mapsto v_2]) \in w\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))$
  2) $(\ell_1, \ell_2) \in \overline{G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\mathsf{ref}\ \delta\sigma)$
- From $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ we know $h_i = h_i' \uplus h_i''$ for some h_1', h_1'', h_2', h_2'' with $(h_1', h_2') \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}}, s))$ and $(h_1'', h_2'') \in w.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}}, s))$.
- Since $\ell_1 \notin \mathrm{dom}(h_1')$ and $\ell_2 \notin \mathrm{dom}(h_2')$, we therefore know that $s_{\mathrm{rf}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\}$ is well-defined and that $s_{\mathrm{rf}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\} \in W_{\mathrm{ref}}.\mathsf{S}$.
- We choose $\widetilde{s_{\mathrm{rf}}} = s_{\mathrm{rf}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\}$.
- Note that $\widetilde{s_{\mathrm{rf}}} \sqsupseteq_{\mathrm{pub}} s_{\mathrm{rf}}$ and that $(h_1' \uplus [\ell_1 \mapsto v_1], h_2' \uplus [\ell_2 \mapsto v_2]) \in W_{\mathrm{ref}}.\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(G(s_{\mathrm{rf}}, s))$.
- By dependent monotonicity we also get $\widetilde{s} \sqsupseteq_{\mathrm{pub}} s$ such that $(h_1'', h_2'') \in w.\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(\widetilde{s})(G(s_{\mathrm{rf}}, s))$.
- Together this yields $(h_1 \uplus [\ell_1 \mapsto v_1], h_2 \uplus [\ell_2 \mapsto v_2]) \in w\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})(G(s_{\mathrm{rf}}, s))$ and then (1) by monotonicity.
- To show (2) it suffices, by definition of GK, to show $(\ell_1, \ell_2) \in w\uparrow.\mathsf{L}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))(\mathsf{ref}\ \delta\sigma)$.
- By definition of $\uparrow$ and W_{ref}, this in turn reduces to showing $(\delta\sigma, \ell_1, \ell_2) \in \widetilde{s_{\mathrm{rf}}}$, which holds by construction.

■

Lemma 43 (Compatibility: Deref)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mathsf{ref}\ \sigma}{\Delta; \Gamma \vdash\ !e_1 \sim\ !e_2 : \sigma}$$

Proof:

- By Lemmas 26 and 28, it suffices to show $\forall G, s_{\mathrm{rf}}, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)),$
$$(!\bullet, !\bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\mathsf{ref}\ \delta\sigma, \delta\sigma)\ .$$
- Suppose $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\ \delta\sigma)$.
- We need to show $(!v_1, !v_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\delta\sigma)$.
- Suppose $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- From $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\ \delta\sigma)$ we know by definition of GK and W_{ref} that $(\delta\sigma, v_1, v_2) \in s_{\mathrm{rf}}$.
- From $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ we know $(h_1', h_2') \in \overline{W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}}, s))}$ for some $h_1' \subseteq h_1$ and $h_2' \subseteq h_2$.
- From the definition of W_{ref} we thus get $(h_1'(v_1), h_2'(v_2)) \in \overline{G(s_{\mathrm{rf}}, s)}(\delta\sigma)$.
- Hence we know $h_1 \uplus h_1^{\mathrm{F}}, !v_1 \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, h_1'(v_1)$ and $h_2 \uplus h_2^{\mathrm{F}}, !v_2 \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, h_2'(v_2)$.
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s)$ such that:
  1) $(h_1, h_2) \in w\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))$
  2) $(h_1'(v_1), h_2'(v_2)) \in \overline{G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\delta\sigma)$
- We choose $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) = (s_{\mathrm{rf}}, s)$ and are done.

■

Lemma 44.

1) If $(\mathsf{ref}\ \tau, v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}$,
   then $(\tau, \mathsf{unit}, v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$.
2) If $(\tau, e_1', e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$,
   then $(\mathsf{ref}\ \tau, \mathsf{unit}, \bullet := e_1', \bullet := e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$.

Proof:

1) - Suppose $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s)}(\tau)$.
   - We need to show $(v_1 := v_1', v_2 := v_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\mathsf{unit})$.
   - Suppose $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
   - From $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\ \tau)$ we know by definition of GK and W_{ref} that $(\tau, v_1, v_2) \in s_{\mathrm{rf}}$.
   - From $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ we know $h_i = h_i' \uplus h_i''$ for some h_1', h_1'', h_2', h_2'' with $(h_1', h_2') \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}}, s))$ and $(h_1'', h_2'') \in w.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}}, s))$.
   - From the definition of W_{ref} we thus get $v_1 \in \mathrm{dom}(h_1')$ and $v_2 \in \mathrm{dom}(h_2')$.

- Hence $h_1 \uplus h_1^{\mathrm{F}}, v_1 := v_1' \hookrightarrow h_1[v_1 \mapsto v_1'] \uplus h_1^{\mathrm{F}}, \langle\rangle$ and $h_2 \uplus h_2^{\mathrm{F}}, v_2 := v_2' \hookrightarrow h_2[v_2 \mapsto v_2'] \uplus h_2^{\mathrm{F}}, \langle\rangle$.
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s)$ such that:
  a) $(h_1[v_1 \mapsto v_1'], h_2[v_2 \mapsto v_2']) \in w\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))$
  b) $(\langle\rangle, \langle\rangle) \in \overline{G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\mathsf{unit})$
- We choose $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) = (s_{\mathrm{rf}}, s)$.
- Note that (b) is immediate.
- Showing (a) reduces to showing $(v_1', v_2') \in \overline{G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\tau)$, which is given.

2) - Suppose $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\,\tau)$.
   - We need to show $(v_1 := e_1', v_2 := e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\mathsf{unit})$.
   - By Lemma 24 it suffices to show
   $$(v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G')((s_{\mathrm{rf}}, s), (\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))(\tau, \mathsf{unit})$$
   for $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s)$ and $G' \supseteq G$.
   - By Lemma 18 it suffices to show $(v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G')((\widetilde{s_{\mathrm{rf}}}, \widetilde{s}), (\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))(\tau, \mathsf{unit})$.
   - By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\mathsf{ref}\,\tau)$.
   - This follows from $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\,\tau)$ by Lemma 12.

■

Lemma 45 (Compatibility: Assign)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mathsf{ref}\,\sigma \qquad \Delta; \Gamma \vdash e_1' \sim e_2' : \sigma}{\Delta; \Gamma \vdash e_1 := e_1' \sim e_2 := e_2' : \mathsf{unit}}$$

Proof:

- By Lemmas 26 and 28, it suffices to show $\forall G, s_{\mathrm{rf}}, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\mathsf{ref}\,\delta\sigma, \mathsf{unit}, \bullet := \gamma_1 e_1', \bullet := \gamma_2 e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$$
assuming $\Delta; \Gamma \vdash e_1' \sim_{w\uparrow} e_2' : \sigma$.
- By Lemma 44 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\delta\sigma)$, which follows from the assumption.

■

Lemma 46.

1) If $(\mathsf{ref}\,\tau, v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}$,
then $(\mathsf{ref}\,\tau, \mathsf{bool}, v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$.
2) If $(\mathsf{ref}\,\tau, e_1', e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$,
then $(\mathsf{ref}\,\tau, \mathsf{bool}, \bullet == e_1', \bullet == e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$.

Proof:

1) - Suppose $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\,\tau)$.
   - We need to show $(v_1 == v_1', v_2 == v_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\mathsf{bool})$.
   - Suppose $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
   - From $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\,\tau)$ we know by definition of GK and W_{ref} that $(\mathsf{ref}\,\tau, v_1', v_2') \in s_{\mathrm{rf}}$.
   - From $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\,\tau)$ we know by definition of GK and W_{ref} that $(\mathsf{ref}\,\tau, v_1, v_2) \in s_{\mathrm{rf}}$.
   - By definition of $W_{\mathrm{ref}}.\mathsf{S}$ this yields $v_1 = v_1' \iff v_2 = v_2'$.
   - Hence either $h_1 \uplus h_1^{\mathrm{F}}, v_1 == v_1' \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, \mathsf{tt}$ and $h_2 \uplus h_2^{\mathrm{F}}, v_2 == v_2' \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, \mathsf{tt}$ or $h_1 \uplus h_1^{\mathrm{F}}, v_1 == v_1' \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, \mathsf{ff}$ and $h_2 \uplus h_2^{\mathrm{F}}, v_2 == v_2' \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, \mathsf{ff}$.
   - By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s)$ such that:
     a) $(h_1, h_2) \in w\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))$
     b) $(\mathsf{tt}, \mathsf{tt}) \in \overline{G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\mathsf{bool})$
     c) $(\mathsf{ff}, \mathsf{ff}) \in \overline{G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\mathsf{bool})$
   - We choose $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) = (s_{\mathrm{rf}}, s)$, and are done.

2) - Suppose $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\,\tau)$.
   - We need to show $(v_1 == e_1', v_2 == e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\mathsf{bool})$.
   - By Lemma 24 it suffices to show
   $$(v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G')((s_{\mathrm{rf}}, s), (\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))(\mathsf{ref}\,\tau, \mathsf{bool})$$

for $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s)$ and $G' \supseteq G$.
- By Lemma 18 it suffices to show $(v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G')((\widetilde{s_{\mathrm{rf}}}, \widetilde{s}), (\widetilde{s_{\mathrm{rf}}}, \widetilde{s}))(\mathsf{ref}\,\tau, \mathsf{bool})$.
- By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(\widetilde{s_{\mathrm{rf}}}, \widetilde{s})}(\mathsf{ref}\,\tau)$.
- This follows from $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{ref}\,\tau)$ by Lemma 12.

■

Lemma 47 (Compatibility: Refeq)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mathsf{ref}\,\sigma \qquad \Delta; \Gamma \vdash e_1' \sim e_2' : \mathsf{ref}\,\sigma}{\Delta; \Gamma \vdash e_1 == e_1' \sim e_2 == e_2' : \mathsf{bool}}$$

Proof:

- By Lemmas 26 and 28, it suffices to show $\forall G, s_{\mathrm{rf}}, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)),$
$$(\mathsf{ref}\,\delta\sigma, \mathsf{bool}, \bullet == \gamma_1 e_1', \bullet == \gamma_2 e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))$$
assuming $\Delta; \Gamma \vdash e_1' \sim_{w\uparrow} e_2' : \mathsf{ref}\,\sigma$.
- By Lemma 46 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\mathsf{ref}\,\delta\sigma)$, which follows from the assumption.

■

Lemma 48 (Compatibility: Gen)**.**

$$\frac{\Delta, \alpha; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \Lambda.\, e_1 \sim \Lambda.\, e_2 : \forall\alpha.\, \sigma}$$

Proof:

- For any $\mathcal{N}$, from the premise we have w such that $w.\mathsf{N} \subseteq \mathcal{N}$ and $\Delta, \alpha; \Gamma \vdash e_1 \sim_w e_2 : \sigma$.
- Let $w' = w_{\mathrm{single}}(\lambda R.\ \{\, (\forall\alpha.\, \delta\sigma, \Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \mid \delta \in \mathrm{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, R)\}, \lambda R.\ \{(\emptyset, \emptyset)\,\})$.
- Since $(w \otimes w').\mathsf{N} = w.\mathsf{N} \subseteq \mathcal{N}$, it suffices to show $\Delta; \Gamma \vdash \Lambda.\, e_1 \sim_{w \otimes w'} \Lambda.\, e_2 : \forall\alpha.\, \sigma$.
- To do so, we first prove $\mathit{inhabited}((w \otimes w')\uparrow)$ and $\mathit{consistent}((w \otimes w')\uparrow)$:
  - $\mathit{inhabited}(w'\uparrow)$ is witnessed by state $(\emptyset, *)$, so $\mathit{inhabited}((w \otimes w')\uparrow)$ holds by Lemma 23.
  - The part of $\mathit{consistent}((w \otimes w')\uparrow)$ concerning arrow types follows from $\mathit{consistent}(w\uparrow)$ by Lemma 23, because $w'.\mathsf{L}$ doesn't relate anything at arrow types.
  - Regarding the part concerning universal types, we suppose
    1) $G \in \mathrm{GK}((w \otimes w')\uparrow)$
    2) $(v_1, v_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s, s')(G(s_{\mathrm{rf}}, s, s'))(\forall\alpha.\, \widetilde{\sigma})$

    and must show:
$$\forall\tau \in \mathrm{CType}.\ (\mathit{beta}(v_1[]), \mathit{beta}(v_2[])) \in \mathbf{E}_{(w\otimes w')\uparrow}(G)((s_{\mathrm{rf}}, s, s'), (s_{\mathrm{rf}}, s, s'))(\widetilde{\sigma}[\tau/\alpha])$$
  - From (2) and the definition of $\uparrow$ and $\otimes$ we know:
$$(v_1, v_2) \in w\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s, s'))(\forall\alpha.\, \widetilde{\sigma}) \vee$$
$$(v_1, v_2) \in w'.\mathsf{L}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s, s'))(\forall\alpha.\, \widetilde{\sigma})$$
  - If the former is true, the claims follow from $\mathit{consistent}(w\uparrow)$ with the help of Lemmas 19 and 21.
  - So suppose the latter.
  - Then $\forall\alpha.\, \widetilde{\sigma} = \forall\alpha.\, \delta\sigma$ and $v_1 = \Lambda.\, \gamma_1 e_1$ and $v_2 = \Lambda.\, \gamma_2 e_2$ for $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$.
  - Let $\delta' := \delta, \alpha{\mapsto}\tau$.
  - It remains to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{(w\otimes w')\uparrow}(G)((s_{\mathrm{rf}}, s, s'), (s_{\mathrm{rf}}, s, s'))(\delta'\sigma)$ since $\widetilde{\sigma}[\tau/\alpha] = \delta\sigma[\tau/\alpha] = \delta'\sigma$.
  - By Lemmas 19 and 21 it suffices to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{w\uparrow}(G(-, -, s'))((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\delta'\sigma)$.
  - This follows from the premise since $\delta' \in \mathrm{TyEnv}(\Delta, \alpha)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s')) = \mathrm{Env}(\delta'\Gamma, G(s_{\mathrm{rf}}, s, s'))$.
- Now suppose $G \in \mathrm{GK}((w \otimes w')\uparrow)$ and $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$.
- We must show $(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in \mathbf{E}_{(w\otimes w')\uparrow}(G)((s_{\mathrm{rf}}, s, s'), (s_{\mathrm{rf}}, s, s'))(\forall\alpha.\, \delta\sigma)$.
- By Lemma 16 it suffices to show $(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in G(s_{\mathrm{rf}}, s, s')(\forall\alpha.\, \delta\sigma)$.
- By definition of GK it suffices to show:
$$(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s, s')(G(s_{\mathrm{rf}}, s, s'))(\forall\alpha.\, \delta\sigma)$$
- By definition of $\uparrow$ and $\otimes$ it suffices to show $(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in w'.\mathsf{L}(s')(G(s_{\mathrm{rf}}, s, s'))(\forall\alpha.\, \delta\sigma)$.
- Since $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s, s'))$, this holds by construction of w'.

■

Lemma 49 (Compatibility: Inst)**.**

$$\frac{\Delta;\Gamma \vdash e_1 \sim e_2 : \forall\alpha.\,\sigma \quad \Delta \vdash \sigma'}{\Delta;\Gamma \vdash e_1[] \sim e_2[] : \sigma[\sigma'/\alpha]}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall\delta \in \mathrm{TyEnv}(\Delta).\ \forall(\gamma_1,\gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\bullet[], \bullet[]) \in \mathbf{K}_W(G)(s,s)(\forall\alpha.\,\delta\sigma, \delta\sigma[\delta\sigma'/\alpha])\ .$$
- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\forall\alpha.\,\delta\sigma)$.
- We need to show $(v_1^\circ[], v_2^\circ[]) \in \mathbf{E}_W(G)(s,s)(\delta\sigma[\delta\sigma'/\alpha])$.
- Since $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\forall\alpha.\,\delta\sigma)$, by definition of $\mathbf{E}_W$, it suffices to show
$$\forall s' \sqsupseteq_{\mathrm{pub}} s.\ \forall G' \supseteq G.\ (\bullet,\bullet) \in \mathbf{K}_W(G')(s,s')(\delta\sigma[\delta\sigma'/\alpha], \delta\sigma[\delta\sigma'/\alpha])$$
which holds by Lemma 17.

■

Lemma 50 (Compatibility: Pack)**.**

$$\frac{\Delta \vdash \sigma' \quad \Delta;\Gamma \vdash e_1 \sim e_2 : \sigma[\sigma'/\alpha]}{\Delta;\Gamma \vdash \mathsf{pack}\ e_1 \sim \mathsf{pack}\ e_2 : \exists\alpha.\,\sigma}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall\delta \in \mathrm{TyEnv}(\Delta).\ \forall(\gamma_1,\gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\mathsf{pack}\ \bullet, \mathsf{pack}\ \bullet) \in \mathbf{K}_W(G)(s,s)(\delta\sigma[\delta\sigma'/\alpha], \exists\alpha.\,\delta\sigma)\ .$$
- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\delta\sigma'/\alpha])$.
- We need to show $(\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \in \mathbf{E}_W(G)(s,s)(\exists\alpha.\,\delta\sigma)$.
- By Lemma 16 it suffices to show $(\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \in \overline{G(s)}(\exists\alpha.\,\delta\sigma)$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\delta\sigma'/\alpha])$.

■

Lemma 51 (Compatibility: Unpack)**.**

$$\frac{\Delta;\Gamma \vdash e_1 \sim e_2 : \exists\alpha.\,\sigma \qquad \Delta,\alpha;\Gamma, x:\sigma \vdash e_1' \sim e_2' : \sigma' \qquad \Delta \vdash \sigma'}{\Delta;\Gamma \vdash \mathsf{unpack}\ e_1\ \mathsf{as}\ x\ \mathsf{in}\ e_1' \sim \mathsf{unpack}\ e_2\ \mathsf{as}\ x\ \mathsf{in}\ e_2' : \sigma'}$$

Proof:

- By Lemmas 27 and 28, it suffices to show $\forall G, s.\ \forall\delta \in \mathrm{TyEnv}(\Delta).\ \forall(\gamma_1,\gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
$$(\exists\alpha.\,\delta\sigma, \delta\sigma', \mathsf{unpack}\ \bullet\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_1 e_1', \mathsf{unpack}\ \bullet\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_2 e_2') \in \mathbf{K}_W(G)(s,s)$$
assuming $\Delta,\alpha;\Gamma, x:\sigma \vdash e_1' \sim_W e_2' : \sigma'$.
- Thus it suffices to show that $\forall(v_1,v_2) \in \overline{G(s)}(\exists\alpha.\,\delta\sigma)$,
$$(\delta\sigma', \mathsf{unpack}\ v_1\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_1 e_1', \mathsf{unpack}\ v_2\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_2 e_2') \in \mathbf{E}_W(G)(s,s)$$
- By definition of $\overline{G(s)}(\exists\alpha.\,\delta\sigma)$, we have v_1', v_2' and $\tau \in \mathrm{CType}$ such that
$$v_1 = \mathsf{pack}\ v_1' \wedge v_2 = \mathsf{pack}\ v_2' \wedge (v_1', v_2') \in \overline{G(s)}(\delta\sigma[\tau/\alpha])$$
- Let $\delta' := \delta, \alpha{\mapsto}\tau$ and $\gamma_1' := \gamma_1, x{\mapsto}v_1'$ and $\gamma_2' := \gamma_2, x{\mapsto}v_2'$.
- Now suppose $(h_1,h_2) \in W.\mathsf{H}(s)(G(s))$ and $h_1^{\mathrm{F}}, h_2^{\mathrm{F}} \in \mathrm{Heap}$ with $h_1 \uplus h_1^{\mathrm{F}}, h_2 \uplus h_2^{\mathrm{F}}$ defined.
- We have $h_1 \uplus h_1^{\mathrm{F}}, \mathsf{unpack}\ v_1\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_1 e_1' \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, \gamma_1' e_1'$ and $h_2 \uplus h_2^{\mathrm{F}}, \mathsf{unpack}\ v_2\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_2 e_2' \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, \gamma_2' e_2'$ and thus by Lemma 15, it suffices to show
$$(\delta\sigma', (h_1, h_1^{\mathrm{F}}, \gamma_1' e_1'), (h_2, h_2^{\mathrm{F}}, \gamma_2' e_2'')) \in \mathbf{O}_W(\mathbf{E}_W)(G)(s,s)\ .$$
- This follows from the assumption and $\delta\sigma' = \delta'\sigma'$, $\delta' \in \mathrm{TyEnv}(\Delta,\alpha)$, $(\gamma_1', \gamma_2') \in \mathrm{Env}(\delta'(\Gamma, x:\tau), G(s))$.

■

3) Soundness.

Theorem 52 (Fundamental Property)**.** If $\Delta;\Gamma \vdash p : \sigma$, then $\Delta;\Gamma \vdash |p| \sim |p| : \sigma$.

Proof: By induction on the typing derivation, in each case using the appropriate compatibility lemma. ∎

Lemma 53 (Weakening)**.** If $\Delta;\Gamma \vdash e_1 \sim e_2 : \sigma$ and $\Delta \subseteq \Delta' \wedge \Gamma \subseteq \Gamma'$, then $\Delta';\Gamma' \vdash e_1 \sim e_2 : \sigma$.

Proof: One can easily see that the goal is a direct consequence of the definition from the following observation:

$$\text{for } i = 1,2,\ \forall R.\ \forall \delta \in \mathrm{TyEnv}(\Delta').\ \forall \gamma_i \in \mathrm{Env}(\delta\Gamma', R).$$
$$\lfloor \delta \rfloor_\Delta \in \mathrm{TyEnv}(\Delta) \wedge \lfloor \gamma_i \rfloor_{\mathrm{dom}(\Gamma)} \in \mathrm{Env}(\lfloor \delta \rfloor_\Delta \Gamma, R) \wedge \gamma_i e_i = \lfloor \gamma_i \rfloor_{\mathrm{dom}(\Gamma)} e_i$$

where $\lfloor f \rfloor_d$ denotes the restriction of the function f on domain d. ∎

Lemma 54 (Congruence)**.** If $\Delta;\Gamma \vdash e_1 \sim e_2 : \sigma$ and $\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma')$, then

$$\Delta';\Gamma' \vdash |C|[e_1] \sim |C|[e_2] : \sigma' \ .$$

Proof: By induction on the derivation of the context typing: in each case using the corresponding compatibility lemma. For a context containing subterms we also need Theorem 52. The rule for an empty context requires Lemma 53. ∎

Lemma 55 (Adequacy)**.** If $\cdot;\cdot \vdash e_1 \sim e_2 : \tau$, then

1) $\forall h_1, h_2.$ neither h_1, e_1 nor h_2, e_2 gets stuck.
2) $\forall h_1, h_2.\ h_1, e_1 \hookrightarrow^\omega \iff h_2, e_2 \hookrightarrow^\omega$.

Proof:

- We know $\cdot;\cdot \vdash e_1 \sim_w e_2 : \tau$ for some w with $w.\mathsf{N} \subseteq \mathrm{TyNam}$.
- Hence we have $\mathit{consistent}(w{\uparrow})$ and $\mathit{inhabited}(w{\uparrow})$.
- Thus, using Lemma 13, there is s_0 such that $(\emptyset,\emptyset) \in w{\uparrow}.\mathsf{H}(s_0)([w{\uparrow}](s_0))$.
- We also have $(e_1, e_2) \in \mathbf{E}_{w{\uparrow}}([w{\uparrow}])(s_0, s_0)(\tau)$.
- Since $\mathit{consistent}(w{\uparrow})$, $(\emptyset,\emptyset) \in w{\uparrow}.\mathsf{H}(s_0)([w{\uparrow}](s_0))$ and $\forall s.\ [w{\uparrow}](s) = w{\uparrow}.\mathsf{L}(s)([w{\uparrow}](s))$, by Corollary 30 for any heaps h_1, h_2 both h_1, e_1 and h_2, e_2 diverge or both terminate without getting stuck.

∎

Theorem 56 (Soundness)**.** If $\Delta;\Gamma \vdash p_1 : \sigma$ and $\Delta;\Gamma \vdash p_2 : \sigma$, then:

$$\Delta;\Gamma \vdash |p_1| \sim |p_2| : \sigma \implies \Delta;\Gamma \vdash p_1 \sim_{\mathrm{ctx}} p_2 : \sigma$$

Proof:

- Suppose $\Delta;\Gamma \vdash |p_1| \sim |p_2| : \sigma$ as well as $\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\cdot;\cdot;\tau)$.
- By congruence (Lemma 54), we have $\cdot;\cdot \vdash |C[p_1]| \sim |C[p_2]| : \tau$.
- By adequacy (Lemma 55), we have $h, |C[p_1]| \hookrightarrow^\omega \iff h, |C[p_2]| \hookrightarrow^\omega$ for any h, so we are done.

∎

4) Symmetry.

Definition 8. Given $R \in \mathrm{VRel}$ (or VRelF), we define $R^{-1} \in \mathrm{VRel}$ (or VRelF) as follows:

$$R^{-1} := \lambda\tau.\ R(\tau)^{-1}$$

Lemma 57. $(\overline{R})^{-1} = \overline{R^{-1}}$

Proof: Easy to check by induction. ∎

Lemma 58. $\mathbf{S}(R_f^{-1}, R_v^{-1}) = \big(\mathbf{S}(R_f, R_v)\big)^{-1}$

Proof: Easy to check. ∎

Definition 9. Given $w \in \mathrm{LWorld}$, we define $w^{-1} \in \mathrm{LWorld}$ as follows:

$$\begin{array}{ll}
w^{-1}.\mathsf{N} & := w.\mathsf{N} \\
w^{-1}.\mathsf{S} & := w.\mathsf{S} \\
w^{-1}.\sqsupseteq & := w.\sqsupseteq \\
w^{-1}.\sqsupseteq_{\mathrm{pub}} & := w.\sqsupseteq_{\mathrm{pub}} \\
w^{-1}.\mathsf{L}(s_{\mathrm{rf}})(s)(R) & := \big(w.\mathsf{L}(s_{\mathrm{rf}}^{-1})(s)(R^{-1})\big)^{-1} \\
w^{-1}.\mathsf{H}(s_{\mathrm{rf}})(s)(R) & := \big(w.\mathsf{H}(s_{\mathrm{rf}}^{-1})(s)(R^{-1})\big)^{-1}
\end{array}$$

where $s_{\mathrm{rf}}^{-1} := \lambda\tau.\ s_{\mathrm{rf}}(\tau)^{-1}$.

Lemma 59. $w^{-1}\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(R) = \left(w\uparrow.\mathsf{H}(s_{\mathrm{rf}}^{-1}, s)(R^{-1})\right)^{-1}$

Proof:

$$\begin{aligned}
& w^{-1}\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(R) \\
= \ & W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(R) \otimes w^{-1}.\mathsf{H}(s_{\mathrm{rf}})(s)(R) \\
= \ & \left(\left(W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(R)\right)^{-1} \otimes \left(w^{-1}.\mathsf{H}(s_{\mathrm{rf}})(s)(R)\right)^{-1}\right)^{-1} \\
= \ & \left(W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}}^{-1})(R^{-1}) \otimes w.\mathsf{H}(s_{\mathrm{rf}}^{-1})(s)(R^{-1})\right)^{-1} \\
= \ & \left(w\uparrow.\mathsf{H}(s_{\mathrm{rf}}^{-1}, s)(R^{-1})\right)^{-1}
\end{aligned}$$

■

Lemma 60. $w^{-1}\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s)(R) = \left(w\uparrow.\mathsf{L}(s_{\mathrm{rf}}^{-1}, s)(R^{-1})\right)^{-1}$

Proof: Analogous to Lemma 59. ■

Definition 10. If $G \in \mathrm{GK}(w^{-1}\uparrow)$, we define $G^{-1} := \lambda s_{\mathrm{rf}}, s.\ G(s_{\mathrm{rf}}^{-1}, s)^{-1}$.

Lemma 61. If $G \in \mathrm{GK}(w^{-1}\uparrow)$, then $G^{-1} \in \mathrm{GK}(w\uparrow)$.

Proof:

1) Monotonicity of G^{-1} follows immediately from monotonicity of G.
2) It remains to show $\forall s_{\mathrm{rf}}, s.\ G^{-1}(s_{\mathrm{rf}}, s) \geq_{\mathrm{ref}}^{w\uparrow.\mathsf{N}} w\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s)(G^{-1}(s_{\mathrm{rf}}, s))$:

$$\begin{aligned}
& G^{-1}(s_{\mathrm{rf}}, s) \\
= \ & G(s_{\mathrm{rf}}^{-1}, s)^{-1} \\
\geq_{\mathrm{ref}}^{w\uparrow.\mathsf{N}} \ & \left(w^{-1}\uparrow.\mathsf{L}(s_{\mathrm{rf}}^{-1}, s)(G(s_{\mathrm{rf}}^{-1}, s))\right)^{-1} \\
= \ & w\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}^{-1}, s)^{-1}) \\
= \ & w\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s)(G^{-1}(s_{\mathrm{rf}}, s))
\end{aligned}$$

■

Lemma 62. If $\mathit{stable}(w)$, then $\mathit{stable}(w^{-1})$.

Proof:

- We suppose
  1) $G \in \mathrm{GK}(w^{-1}\uparrow)$
  2) $(h_1, h_2) \in w^{-1}.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}}, s))$
  3) $s'_{\mathrm{rf}} \sqsupseteq s_{\mathrm{rf}}$
  4) $(h^1_{\mathrm{ref}}, h^2_{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s'_{\mathrm{rf}})(G(s'_{\mathrm{rf}}, s))$
  5) $h^1_{\mathrm{ref}} \uplus h_1$ defined $\wedge$ $h^2_{\mathrm{ref}} \uplus h_2$ defined

  and must show: $\exists s' \sqsupseteq_{\mathrm{pub}} s.\ (h_1, h_2) \in w^{-1}.\mathsf{H}(s'_{\mathrm{rf}})(s')(G(s'_{\mathrm{rf}}, s'))$
- From (2) we know $(h_2, h_1) \in w.\mathsf{H}(s_{\mathrm{rf}}^{-1})(s)(G(s_{\mathrm{rf}}, s)^{-1}) = w.\mathsf{H}(s_{\mathrm{rf}}^{-1})(s)(G^{-1}(s_{\mathrm{rf}}^{-1}, s))$.
- From (3) we know $s'^{-1}_{\mathrm{rf}} \sqsupseteq s^{-1}_{\mathrm{rf}}$.
- From (4) and Lemma 57 we know $(h^2_{\mathrm{ref}}, h^1_{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s'^{-1}_{\mathrm{rf}})(G(s'_{\mathrm{rf}}, s)^{-1}) = W_{\mathrm{ref}}.\mathsf{H}(s'^{-1}_{\mathrm{rf}})(G^{-1}(s'^{-1}_{\mathrm{rf}}, s))$.
- Hence, using Lemma 61, the assumption yields $s' \sqsupseteq_{\mathrm{pub}} s$ such that
$$(h_2, h_1) \in w.\mathsf{H}(s'^{-1}_{\mathrm{rf}})(s')(G^{-1}(s'^{-1}_{\mathrm{rf}}, s')).$$
- This implies $(h_1, h_2) \in w^{-1}.\mathsf{H}(s'_{\mathrm{rf}})(s')(G(s'_{\mathrm{rf}}, s'))$.

■

Lemma 63. If $\mathit{inhabited}(w\uparrow)$, then $\mathit{inhabited}(w^{-1}\uparrow)$.

Proof:

- We suppose $G \in \mathrm{GK}(w^{-1}\uparrow)$ and must show $\exists s_0.\ (\emptyset, \emptyset) \in w^{-1}\uparrow.\mathsf{H}(s_0)(G(s_0))$.
- Using the assumption and Lemma 61, we get (s_{rf}, s) such that $(\emptyset, \emptyset) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G^{-1}(s_{\mathrm{rf}}, s))$.
- Lemma 59 implies $(\emptyset, \emptyset) \in w^{-1}\uparrow.\mathsf{H}(s_{\mathrm{rf}}^{-1}, s)(G(s_{\mathrm{rf}}^{-1}, s))$.

■

Lemma 64. If $G \in \mathrm{GK}(w^{-1}\uparrow)$, then:

$$\left(\mathbf{E}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}{}_0, s_0), (s_{\mathrm{rf}}^{-1}, s))\right)^{-1} \subseteq \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))$$

Proof: Let

$$\begin{array}{lcl} \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau) & := & \left(\mathbf{E}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}{}_0, s_0), (s_{\mathrm{rf}}^{-1}, s))(\tau)\right)^{-1}, \\ \mathbf{K}'_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau', \tau) & := & \left(\mathbf{K}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}{}_0, s_0), (s_{\mathrm{rf}}^{-1}, s))(\tau', \tau)\right)^{-1}. \end{array}$$

By coinduction, it suffices to show:

1) $\forall e_2, e_1, G, s_{\mathrm{rf}0}, s_0, s_{\mathrm{rf}}, s, \tau.$
   $(e_2, e_1) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau) \implies$
   $\forall (h_2, h_1) \in w^{-1}\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s)).\ \forall h_2^{\mathrm{F}}, h_1^{\mathrm{F}}.$
   $((h_2, h_2^{\mathrm{F}}, e_2), (h_1, h_1^{\mathrm{F}}, e_1)) \in \mathbf{O}_{w^{-1}\uparrow}(\mathbf{K}'_{w^{-1}\uparrow})(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau)$
2) $\forall K_2, K_1, G, s_{\mathrm{rf}0}, s_0, s_{\mathrm{rf}}, s, \tau', \tau.$
   $(K_2, K_1) \in \mathbf{K}'_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau', \tau) \implies$
   $\forall (v_2, v_1) \in \overline{G(s_{\mathrm{rf}}, s)}(\tau').$
   $(K_2[v_2], K_1[v_1]) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau)$

For (1):

- By definition of $\mathbf{E}'_{w^{-1}\uparrow}$ and Lemma 59, suppose $(e_1, e_2) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}{}_0, s_0), (s_{\mathrm{rf}}^{-1}, s))(\tau)$ and $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}^{-1}, s)(G^{-1}(s_{\mathrm{rf}}^{-1}, s))$.
- By definition of $\mathbf{E}_{w\uparrow}$ we have $((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_{w\uparrow}(\mathbf{K}_{w\uparrow})(G^{-1})((s_{\mathrm{rf}}^{-1}{}_0, s_0), (s_{\mathrm{rf}}^{-1}, s))(\tau)$.
- Using all the lemmas above, it is easy to check that this implies
$$((h_2, h_2^{\mathrm{F}}, e_2), (h_1, h_1^{\mathrm{F}}, e_1)) \in \mathbf{O}_{w^{-1}\uparrow}(\mathbf{K}'_{w^{-1}\uparrow})(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau)\ .$$

For (2):

- By definition of $\mathbf{K}'_{w^{-1}\uparrow}$ and Lemma 57, suppose $(K_1, K_2) \in \mathbf{K}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}{}_0, s_0), (s_{\mathrm{rf}}^{-1}, s))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G^{-1}(s_{\mathrm{rf}}^{-1}, s)}(\tau')$.
- By definition of $\mathbf{K}_{w\uparrow}$ we have $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}{}_0, s_0), (s_{\mathrm{rf}}^{-1}, s))(\tau)$.
- By definition of $\mathbf{E}'_{w^{-1}\uparrow}$, it implies that $(K_2[v_2], K_1[v_1]) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}0}, s_0), (s_{\mathrm{rf}}, s))(\tau)$.

■

Lemma 65. If $\mathit{consistent}(w\uparrow)$, then $\mathit{consistent}(w^{-1}\uparrow)$.

Proof:

- We suppose $G \in \mathrm{GK}(w^{-1}\uparrow)$ and $(e_1, e_2) \in \mathbf{S}(w^{-1}\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s)), G(s_{\mathrm{rf}}, s))(\tau)$, and must show $(\mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\tau)$.
- By Lemma 58 we know $(e_2, e_1) \in \mathbf{S}(w\uparrow.\mathsf{L}(s_{\mathrm{rf}}^{-1}, s)(G^{-1}(s_{\mathrm{rf}}^{-1}, s)), G^{-1}(s_{\mathrm{rf}}^{-1}, s))(\tau)$.
- Using the assumption and Lemma 61, we get $(\mathit{beta}(e_2), \mathit{beta}(e_1)) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}, s), (s_{\mathrm{rf}}^{-1}, s))(\tau)$.
- We are done by Lemma 64.

■

Theorem 66. If $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$, then $\Delta; \Gamma \vdash e_2 \sim e_1 : \sigma$.

Proof: Suppose $\Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma$ with $\mathit{stable}(w)$. By Lemma 62 it suffices to show $\Delta; \Gamma \vdash e_2 \sim_{w^{-1}} e_1 : \sigma$. Using Lemmas 63 and 65, this in turn reduces to showing:

$$\begin{array}{l} \forall G \in \mathrm{GK}(w^{-1}\uparrow).\ \forall s_{\mathrm{rf}}, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s)). \\ \quad (\gamma_1 e_2, \gamma_2 e_1) \in \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\delta\sigma) \end{array}$$

From $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s))$ we have $(\gamma_2, \gamma_1) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{rf}}, s)^{-1}) = \mathrm{Env}(\delta\Gamma, G^{-1}(s_{\mathrm{rf}}^{-1}, s))$. Lemma 61 and the assumption thus yield $(\gamma_2 e_1, \gamma_1 e_2) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\mathrm{rf}}^{-1}, s), (s_{\mathrm{rf}}^{-1}, s))(\delta\sigma)$. We are done by Lemma 64. ■

D. Examples

1) World Generator.

$$\mathrm{NLWorld} := \{\, \mathcal{W} \in \mathrm{Names} \to \mathrm{LWorld} \mid \forall \mathcal{N}.\ \mathcal{W}(\mathcal{N}).\mathsf{N} \subseteq \mathcal{N} \,\}$$

Definition 11. We define $\mathbf{G} : \mathrm{NLWorld} \to \mathrm{NLWorld}$ as follows.

$$\begin{array}{ll}
\mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{N} & := \mathcal{N} \\
\mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{S} & := \{\, (s_1, \ldots, s_n) \mid n \in \mathbb{N} \wedge \forall i \in \{1 \ldots n\}.\ s_i \in \mathcal{W}(\mathcal{N}_i).\mathsf{S} \,\} \\
\mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{L}(s_{\mathrm{rf}})(s_1, \ldots, s_n)(R) & := \bigcup_{i \in \{1 \ldots n\}} \mathcal{W}(\mathcal{N}_i).\mathsf{L}(s_{\mathrm{rf}})(s_i)(R) \\
\mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{H}(s_{\mathrm{rf}})(s_1, \ldots, s_n)(R) & := \otimes_{i \in \{1 \ldots n\}} \mathcal{W}(\mathcal{N}_i).\mathsf{H}(s_{\mathrm{rf}})(s_i)(R)
\end{array}$$

where $\{\, \mathcal{N}_i \,\}$ is a countably infinite splitting of $\mathcal{N}$ *i.e.,* $\mathcal{N} = \mathcal{N}_1 \uplus \mathcal{N}_2 \uplus \mathcal{N}_3 \uplus \ldots$.
The transition on $\mathbf{G}(\mathcal{W})(\mathcal{N})$ is generated by the following rule.

$$\begin{array}{rll}
(s_1, \ldots, s_k, s_{k+1}) \sqsupseteq_{\mathrm{pub}} (s_1, \ldots, s_k) & & \\
(s'_1, \ldots, s'_k) \sqsupseteq_{\mathrm{pub}} (s_1, \ldots, s_k) & \text{if} & s'_1 \sqsupseteq_{\mathrm{pub}} s_1 \wedge \ldots \wedge s'_k \sqsupseteq_{\mathrm{pub}} s_k \\
(s'_1, \ldots, s'_k) \sqsupseteq (s_1, \ldots, s_k) & \text{if} & s'_1 \sqsupseteq s_1 \wedge \ldots \wedge s'_k \sqsupseteq s_k \\
(s'_1, \ldots, s'_j) \sqsupseteq (s_1, \ldots, s_k) & \text{if} & (s'_1, \ldots, s'_j) \sqsupseteq_{\mathrm{pub}} (s_1, \ldots, s_k)
\end{array}$$

We define the following notation.

$$\begin{array}{rcl}
\{n \backslash i\} & := & \{\, 1, \ldots, i-1, i+1, \ldots, n \,\} \\
G(\{s_k\}_{k \in \{n \backslash i\}}) & := & G(-, s_1, \ldots, s_{i-1}, -, s_{i+1}, \ldots, s_n)
\end{array}$$

Lemma 67.

$$\forall G \in \mathrm{GK}(\mathbf{G}(\mathcal{W})(\mathcal{N})\!\uparrow).\ \forall s_1 \ldots s_{i-1}, s_{i+1} \ldots s_n.\ G(\{s_k\}_{k \in \{n \backslash i\}}) \in \mathrm{GK}(\mathcal{W}(\mathcal{N}_i)\!\uparrow)$$

Proof:

- We need to show $G(\{s_k\}_{k \in \{n \backslash i\}})$ is monotone w.r.t. $\sqsubseteq$, which follows directly from the definition of $\sqsubseteq$ and monotonicity of G.
- We have

$$\begin{array}{ll}
& G(\{s_k\}_{k \in \{n \backslash i\}})(s_{\mathrm{rf}}, s_i) \\
= & G(s_{\mathrm{rf}}, s_1 \ldots s_n) \\
\geq^{\mathcal{N}}_{\mathrm{ref}} & \mathbf{G}(\mathcal{W})(\mathcal{N})\!\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s_1 \ldots s_n)(G(s_{\mathrm{rf}}, s_1 \ldots s_n)) \\
\supseteq & \mathcal{W}(\mathcal{N}_i)\!\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s_i)(G(s_{\mathrm{rf}}, s_1, \ldots, s_n)) \\
= & \mathcal{W}(\mathcal{N}_i)\!\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s_i)(G(\{s_k\}_{k \in \{n \backslash i\}})(s_{\mathrm{rf}}, s_i))\ .
\end{array}$$

- Now it suffices to show that the latter inequality is contained in $\geq^{\mathcal{N}_i}_{\mathrm{ref}}$, which follows from $\forall i.\ \mathcal{W}(\mathcal{N}_i) \in \mathrm{LWorld}$ and the fact that $\mathcal{N}_1, \ldots, \mathcal{N}_n$ are disjoint.

■

Lemma 68. If $W = \mathbf{G}(\mathcal{W})(\mathcal{N})\!\uparrow$ and $\forall \mathcal{N}'.\ \mathit{stable}(\mathcal{W}(\mathcal{N}'))$ and $G \in \mathrm{GK}(W)$, then:

1) $\mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i)) \subseteq \mathbf{E}_W(G)((s^0_{\mathrm{rf}}, s_1 \ldots s_{i-1}, s^0_i, s_{i+1} \ldots s_n), (s_{\mathrm{rf}}, s_1 \ldots s_n))$
2) $\mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i)) \subseteq \mathbf{K}_W(G)((s^0_{\mathrm{rf}}, s_1 \ldots s_{i-1}, s^0_i, s_{i+1} \ldots s_n), (s_{\mathrm{rf}}, s_1 \ldots s_n))$

Proof: We define $\mathbf{E}'_W$ and $\mathbf{K}'_W$ as follows:

$$\begin{array}{l}
\mathbf{E}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \ldots s_n)) = \{\, (\tau, e_1, e_2) \mid \\
\qquad (\forall k \in \{n_0 \backslash i\}.\ s_k \sqsupseteq_{\mathrm{pub}} s^0_k) \wedge (\tau, e_1, e_2) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i)) \,\} \\
\mathbf{K}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \ldots s_n)) = \{\, (\tau', \tau, K_1, K_2) \mid \\
\qquad (\forall k \in \{n_0 \backslash i\}.\ s_k \sqsupseteq_{\mathrm{pub}} s^0_k) \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i)) \,\}
\end{array}$$

Then it suffices to show $\mathbf{E}'_W \subseteq \mathbf{E}_W$ and $\mathbf{K}'_W \subseteq \mathbf{K}_W$ by coinduction. Concretely, we have to show:

1) $\forall e_1, e_2, G, s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}, s_{\mathrm{rf}}, s_1 \ldots s_n, \tau.$
$(e_1, e_2) \in \mathbf{E}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \ldots s_n))(\tau) \implies$
$\forall (h_1, h_2) \in W.\mathsf{H}(s_{\mathrm{rf}}, s_1 \ldots s_n)(G(s_{\mathrm{rf}}, s_1 \ldots s_n)).\forall h^{\mathrm{F}}_1, h^{\mathrm{F}}_2.$
$((h_1, h^{\mathrm{F}}_1, e_1), (h_2, h^{\mathrm{F}}_2, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)((s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \ldots s_n))(\tau)$
2) $\forall K_1, K_2, G, s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}, s_{\mathrm{rf}}, s_1 \ldots s_n, \tau', \tau.$
$(K_1, K_2) \in \mathbf{K}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \ldots s_n))(\tau', \tau) \implies$
$\forall (v_1, v_2) \in G(s_{\mathrm{rf}}, s_1 \ldots s_n)(\tau').\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \ldots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \ldots s_n))(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \dots s_n))(\tau)$ and $(h_1, h_2) \in W.\mathsf{H}(s_{\mathrm{rf}}, s_1 \dots s_n)(G(s_{\mathrm{rf}}, s_1 \dots s_n))$.
- By definition of $\mathbf{E}'_W$ we have $(\forall k \in \{n_0 \backslash i\}.\ s_k \sqsupseteq_{\mathrm{pub}} s^0_k)$ and
$$(\tau, e_1, e_2) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k\in\{n\setminus i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i))\ .$$
- We must show $((h_1, h^{\mathrm{F}}_1, e_1), (h_2, h^{\mathrm{F}}_2, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)((s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \dots s_n))(\tau)$.
- So suppose $\mathrm{defined}(h_1 \uplus h^{\mathrm{F}}_1)$ and $\mathrm{defined}(h_2 \uplus h^{\mathrm{F}}_2)$.
- From $(h_1, h_2) \in W.\mathsf{H}(s_{\mathrm{rf}}, s_1 \dots s_n)(G(s_{\mathrm{rf}}, s_1 \dots s_n))$, we have $h_1 = h'_1 \uplus h''_1$ and $h_2 = h'_2 \uplus h''_2$ with $(h'_1, h'_2) \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s_i)(G(s_{\mathrm{rf}}, s_1 \dots s_n))$ and $(h''_1, h''_2) \in \otimes_{k\in\{n\setminus i\}}\mathcal{W}(\mathcal{N}_k).\mathsf{H}(s_{\mathrm{rf}})(s_k)(G(s_{\mathrm{rf}}, s_1 \dots s_n))$.
- Hence $((h'_1, h''_1 \uplus h^{\mathrm{F}}_1, e_1), (h'_2, h''_2 \uplus h^{\mathrm{F}}_2, e_2)) \in \mathbf{O}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(\mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow})(G(\{s_k\}_{k\in\{n\setminus i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i))(\tau)$.
- Consequently at least one of the following three properties holds:

A) $h_1 \uplus h^{\mathrm{F}}_1, e_1 \hookrightarrow^{\omega}$ and $h_2 \uplus h^{\mathrm{F}}_2, e_2 \hookrightarrow^{\omega}$

B) a) $h_1 \uplus h^{\mathrm{F}}_1, e_1 \hookrightarrow^{*} \widetilde{h'_1} \uplus h''_1 \uplus h^{\mathrm{F}}_1, v_1$ and $h_2 \uplus h^{\mathrm{F}}_2, e_2 \hookrightarrow^{*} \widetilde{h'_2} \uplus h''_2 \uplus h^{\mathrm{F}}_2, v_2$
b) $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_i}) \sqsupseteq [(s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i)]$
c) $(\widetilde{h'_1}, \widetilde{h'_2}) \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_i})(G(\widetilde{s_{\mathrm{rf}}}, s_1 \dots s_{i-1}, \widetilde{s_i}, s_{i+1} \dots s_n))$
d) $(v_1, v_2) \in \overline{G(\widetilde{s_{\mathrm{rf}}}, s_1 \dots s_{i-1}, \widetilde{s_i}, s_{i+1} \dots s_n)}(\tau)$

C) a) $h_1 \uplus h^{\mathrm{F}}_1, e_1 \hookrightarrow^{*} \widetilde{h'_1} \uplus h''_1 \uplus h^{\mathrm{F}}_1, v_1$ and $h_2 \uplus h^{\mathrm{F}}_2, e_2 \hookrightarrow^{*} \widetilde{h'_2} \uplus h''_2 \uplus h^{\mathrm{F}}_2, v_2$
b) $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_i}) \sqsupseteq (s_{\mathrm{rf}}, s_i)$
c) $(\widetilde{h'_1}, \widetilde{h'_2}) \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_i})(G(\widetilde{s_{\mathrm{rf}}}, s_1 \dots s_{i-1}, \widetilde{s_i}, s_{i+1} \dots s_n))$
d) $(e'_1, e'_2) \in \mathbf{S}(G(\widetilde{s_{\mathrm{rf}}}, s_1 \dots s_{i-1}, \widetilde{s_i}, s_{i+1} \dots s_n), G(\widetilde{s_{\mathrm{rf}}}, s_1 \dots s_{i-1}, \widetilde{s_i}, s_{i+1} \dots s_n))(\widetilde{\tau})$
e) $\forall(\widehat{s_{\mathrm{rf}}}, \widehat{s_i}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{rf}}}, \widetilde{s_i}).\ \forall G' \supseteq G(\{s_k\}_{k\in\{n\setminus i\}}).\ (K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G')((s^0_{\mathrm{rf}}, s^0_i), (\widehat{s_{\mathrm{rf}}}, \widehat{s_i}))(\widetilde{\tau}, \tau)$

- If (A) holds, then we are done.
- If (B) holds:
  - For all $k \in \{n \setminus i\}$, iteratively applying $stable(\mathcal{W}(\mathcal{N}_k))$ and using monotonicity gets us $\widetilde{s_k} \sqsupseteq_{\mathrm{pub}} s_k$ such that:
$$(h''_1, h''_2) \in \otimes_{k\in\{n\setminus i\}}\mathcal{W}(\mathcal{N}_k).\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(\widetilde{s_k})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n}))$$
  - Thus from (Bc), monotonicity, and the definition of W we get
$$(\widetilde{h'_1} \uplus h''_1, \widetilde{h'_2} \uplus h''_2) \in W.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n}))$$
  - From (Bb) we get $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n}) \sqsupseteq [(s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \dots s_n)]$.
  - Together with (Ba), (Bd), and monotonicity we are done.
- If (C) holds:
  - For all $k \in \{n \setminus i\}$, iteratively applying $stable(\mathcal{W}(\mathcal{N}_k))$ and using monotonicity gets us $\widetilde{s_k} \sqsupseteq_{\mathrm{pub}} s_k$ such that:
$$(h''_1, h''_2) \in \otimes_{k\in\{n\setminus i\}}\mathcal{W}(\mathcal{N}_k).\mathsf{H}(\widetilde{s_{\mathrm{rf}}})(\widetilde{s_k})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n}))$$
  - Thus from (Cc), monotonicity, and the definition of W we get
$$(\widetilde{h'_1} \uplus h''_1, \widetilde{h'_2} \uplus h''_2) \in W.\mathsf{H}(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n})(G(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n}))$$
  - From (Cb) we get $(\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n}) \sqsupseteq [(s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \dots s_n)]$.
  - After applying monotonicity to (Cd), it remains to show:
$$\forall(\widehat{s_{\mathrm{rf}}}, \widehat{s_1} \dots \widehat{s_m}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n}).\ \forall G' \supseteq G.$$
$$(K_1, K_2) \in \mathbf{K}'_W(G')((s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (\widehat{s_{\mathrm{rf}}}, \widehat{s_1} \dots \widehat{s_m}))(\widetilde{\tau}, \tau)$$
  - So suppose $(\widehat{s_{\mathrm{rf}}}, \widehat{s_1} \dots \widehat{s_m}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{rf}}}, \widetilde{s_1} \dots \widetilde{s_n})$ and $G' \supseteq G$.
  - By monotonicity we have $G'(\{\widehat{s_k}\}_{k\in\{m\setminus i\}}) \supseteq G(\{s_k\}_{k\in\{n\setminus i\}})$.
  - From (Ce) we therefore get $(K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G'(\{\widehat{s_k}\}_{k\in\{m\setminus i\}}))((s^0_{\mathrm{rf}}, s^0_i), (\widehat{s_{\mathrm{rf}}}, \widehat{s_i}))(\widetilde{\tau}, \tau)$.
  - By definition of $\mathbf{K}'_W$ this implies $(K_1, K_2) \in \mathbf{K}'_W(G')((s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (\widehat{s_{\mathrm{rf}}}, \widehat{s_1} \dots \widehat{s_m}))(\widetilde{\tau}, \tau)$.

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \dots s_n))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s_1 \dots s_n)}(\tau')$.
- By definition of $\mathbf{K}'_W$ we have $(\forall k \in \{n_0 \backslash i\}.\ s_k \sqsupseteq_{\mathrm{pub}} s^0_k)$ and
$$(\tau', \tau, K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k\in\{n\setminus i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i))\ .p$$
- We must show $(\tau, K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)((s^0_{\mathrm{rf}}, s^0_1 \dots s^0_{n_0}), (s_{\mathrm{rf}}, s_1 \dots s_n))$.
- By definition of $\mathbf{E}'_W$ it suffices to show
$$(\tau, K_1[v_1], K_2[v_2]) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k\in\{n\setminus i\}}))((s^0_{\mathrm{rf}}, s^0_i), (s_{\mathrm{rf}}, s_i))\ .$$

- Since $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s_1 \dots s_n)}(\tau')$, we are done.

■

Lemma 69. Suppose $\forall \mathcal{N}.\ \mathit{stable}(\mathcal{W}(\mathcal{N}))$.

1) $\forall \mathcal{N}.\ \mathit{stable}(\mathbf{G}(\mathcal{W})(\mathcal{N}))$
2) If $\forall \mathcal{N}.\ \mathit{consistent}(\mathcal{W}(\mathcal{N})\uparrow)$, then $\forall \mathcal{N}.\ \mathit{consistent}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$.

Proof:

- We suppose

(a) $G \in \mathrm{GK}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$

(b) $(\tau, e_1, e_2) \in \mathbf{S}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s_1 \dots s_n)(G(s_{\mathrm{rf}}, s_1 \dots s_n)), G(s_{\mathrm{rf}}, s_1 \dots s_n))$
and must show $(\tau, \mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_{\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow}(G)((s_{\mathrm{rf}}, s_1 \dots s_n), (s_{\mathrm{rf}}, s_1 \dots s_n))$.

- From (b) and the definition of $\mathbf{S}$ we know: for some i,

$$(\tau, e_1, e_2) \in \mathbf{S}(\mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{L}(s_{\mathrm{rf}}, s_i)(G(s_{\mathrm{rf}}, s_1 \dots s_n)), G(s_{\mathrm{rf}}, s_1 \dots s_n))$$

- The claim follows from $\mathit{consistent}(\mathcal{W}(\mathcal{N}_i)\uparrow)$ with the help of Lemmas 67 and 68.

■

Lemma 70. $\mathit{inhabited}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$

Proof: It is easy to check that $(\emptyset, \emptyset) \in \mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow.\mathsf{H}(\emptyset, ())(R)$ for any R. ■

2) Substitutivity.

Theorem 71.

$$\frac{\Delta; \Gamma, x{:}\sigma' \vdash e_1 \sim e_2 : \sigma \qquad \Delta; \Gamma \vdash v_1 \sim v_2 : \sigma'}{\Delta; \Gamma \vdash e_1[v_1/x] \sim e_2[v_2/x] : \sigma}$$

Proof: By Lemma 27 it suffices to show:

$$\frac{\Delta; \Gamma, x{:}\sigma' \vdash e_1 \sim_W e_2 : \sigma \qquad \Delta; \Gamma \vdash v_1 \sim_W v_2 : \sigma'}{\Delta; \Gamma \vdash e_1[v_1/x] \sim_W e_2[v_2/x] : \sigma}$$

This boils down to showing

$$(\delta\sigma, \gamma_1(e_1[v_1/x]), \gamma_2(e_2[v_2/x])) \in \mathbf{E}_W(G)(s, s)$$

for $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$.

- So suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ and $h_1^{\mathrm{F}}, h_2^{\mathrm{F}} \in \mathrm{Heap}$.
- We must show $(\delta\sigma, (h_1, h_1^{\mathrm{F}}, \gamma_1(e_1[v_1/x])), (h_2, h_2^{\mathrm{F}}, \gamma_2(e_2[v_2/x]))) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s)$.
- From the second premise we get $(\delta\sigma', \gamma_1 v_1, \gamma_2 v_2) \in \mathbf{E}_W(G)(s, s)$.
- As a consequence of this, there is $s' \sqsupseteq_{\mathrm{pub}} s$ such that:

1) $(\delta\sigma', \gamma_1 v_1, \gamma_2 v_2) \in \overline{G(s')}$
2) $(h_1, h_2) \in W.\mathsf{H}(s')(G(s'))$

- Let $\gamma_1' := \gamma_1, x \mapsto \gamma_1 v_1$ and $\gamma_2' := \gamma_2, x \mapsto \gamma_2 v_2$.
- By monotonicity and (1) we have $\gamma' \in \mathrm{Env}(\delta(\Gamma, x{:}\sigma'), G(s'))$.
- The first premise then yields $(\delta\sigma, \gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_W(G)(s', s')$.
- By Lemma 18 we get $(\delta\sigma, \gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_W(G)(s, s')$.
- This implies $(\delta\sigma, (h_1, h_1^{\mathrm{F}}, \gamma_1(e_1[v_1/x])), (h_2, h_2^{\mathrm{F}}, \gamma_2(e_2[v_2/x]))) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s')$.
- We are done by Lemma 15 and (2).

■

3) Expansion.

Theorem 72.

$$\frac{\Delta; \Gamma \vdash e_1' \sim e_2' : \sigma \qquad \forall h, \gamma.\ h, \gamma e_1 \hookrightarrow^* h, \gamma e_1' \qquad \forall h, \gamma.\ h, \gamma e_2 \hookrightarrow^* h, \gamma e_2'}{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}$$

Proof: By Lemma 27 it suffices to show:

$$\frac{\Delta; \Gamma \vdash e_1' \sim_W e_2' : \sigma \qquad \forall h, \gamma.\ h, \gamma e_1 \hookrightarrow^* h, \gamma e_1' \qquad \forall h, \gamma.\ h, \gamma e_2 \hookrightarrow^* h, \gamma e_2'}{\Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma}$$

This boils down to showing

$$(\delta\sigma, (h_1, h_1^{\mathrm{F}}, \gamma_1 e_1), (h_2, h_2^{\mathrm{F}}, \gamma_2 e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s,s)$$

in a context where the premise provides

$$(\delta\sigma, (h_1, h_1^{\mathrm{F}}, \gamma_1 e_1'), (h_2, h_2^{\mathrm{F}}, \gamma_2 e_2')) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s,s).$$

Using the side condition, we are done by Lemma 15. ∎

4) Beta Law.

Theorem 73.

$$\frac{\Delta; \Gamma, x{:}\sigma' \vdash e_1 \sim e_2 : \sigma \qquad \Delta; \Gamma \vdash v_1 \sim v_2 : \sigma'}{\Delta; \Gamma \vdash (\lambda x.\, e_1)\ v_1 \sim e_2[v_2/x] : \sigma}$$

Proof: From the premises and Theorem 71 we know $\Delta; \Gamma \vdash e_1[v_1/x] \sim e_2[v_2/x] : \sigma$. Thus the conclusion holds by Theorem 72. ∎

5) Awkward Example.

$$\begin{array}{rcl} \tau & := & (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int} \\ v_1 & := & \lambda f.\, f\ \langle\rangle; 1 \\ e_2 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\ & & \lambda f.\, x := 1; f\ \langle\rangle; !x \end{array}$$

We show $\cdot; \cdot \vdash v_1 \sim e_2 : \tau$. So let $\mathcal{N}$ be given. The proof splits conceptually into three parts:

1) Constructing a local world $\widehat{w}$ with $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$, $\mathit{stable}(\widehat{w})$, and $\mathit{inhabited}(\widehat{w}\!\uparrow)$.
2) Showing $\mathit{consistent}(\widehat{w}\!\uparrow)$. This is the meat of the proof.
3) Showing that v_1 and e_2 are related by $\mathbf{E}_{\widehat{w}\uparrow}$.

Constructing the world.. First, we define $w \in \mathrm{LWorld}$ as follows:

$$\begin{array}{lcl} w.\mathsf{N} & := & \emptyset \\ w.\mathsf{S} & := & \mathrm{Loc} \times \{0,1\} \\ w.\sqsupseteq & := & w.\sqsupseteq_{\mathrm{pub}} \\ w.\sqsupseteq_{\mathrm{pub}} & := & \{((\ell,1),(\ell,0)) \mid \ell \in \mathrm{Loc}\}^* \\ w.\mathsf{L} & := & \lambda s_{\mathrm{rf}}, (\ell, n), R.\ \{((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}, v_1, (\lambda f.\, \ell := 1; f\ \langle\rangle; !\ell))\} \\ w.\mathsf{H} & := & \lambda s_{\mathrm{rf}}, (\ell, n), R.\ \{(\emptyset, [\ell \mapsto n])\} \end{array}$$

Now let $\widehat{w} = \mathbf{G}(\lambda\mathcal{N}.w)(\mathcal{N})$. By definition of $\mathbf{G}$ we have $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 69 and 70 we know $\mathit{stable}(\widehat{w})$ and $\mathit{inhabited}(\widehat{w}\!\uparrow)$.

Showing consistency.. In order to show $\mathit{consistent}(\widehat{w}\!\uparrow)$, it suffices by Lemma 69 to just show $\mathit{consistent}(w\!\uparrow)$.

- So suppose $(s_{\mathrm{rf}}, (\ell, n)) \in w\!\uparrow.\mathsf{S}$ and $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, (\ell, n))}(\mathsf{unit} \to \mathsf{unit})$.
- We need to show:
$$((v_1'\ \langle\rangle; 1), (\ell := 1; v_2'\ \langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, (\ell, n)), (s_{\mathrm{rf}}, (\ell, n)))(\mathsf{int})$$
- So suppose $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$ as well as
$$(h_1, h_2) \in w\!\uparrow.\mathsf{H}(s_{\mathrm{rf}}, (\ell, n))(G(s_{\mathrm{rf}}, (\ell, n))).$$
- Then there are $(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}}, (\ell, n)))$ such that $h_1 = h_1^{\mathrm{ref}}$ and $h_2 = h_2^{\mathrm{ref}} \uplus [\ell \mapsto n]$.
- Therefore we know:
$$h_2 \uplus h_2^{\mathrm{F}}, (\ell := 1; v_2'\ \langle\rangle; !\ell) \hookrightarrow h_2^{\mathrm{ref}} \uplus [\ell \mapsto 1] \uplus h_2^{\mathrm{F}}, (v_2'\ \langle\rangle; !\ell)$$
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s' \sqsupseteq (\ell, n)$ such that:
  1) $(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}} \uplus [\ell \mapsto 1]) \in w\!\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s')(G(s_{\mathrm{rf}}, s'))$
  2) $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s')}(\mathsf{unit} \to \mathsf{unit})$
  3) $(\langle\rangle, \langle\rangle) \in \overline{G(s_{\mathrm{rf}}, s')}(\mathsf{unit})$
  4) $\forall (s_{\mathrm{rf}}', s'') \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s').\forall G' \supseteq G.\ ((\bullet; 1), (\bullet; !\ell)) \in \mathbf{K}_{w\uparrow}(G')((s_{\mathrm{rf}}, (\ell, n)), (s_{\mathrm{rf}}', s''))(\mathsf{unit}, \mathsf{int})$
- We pick $s' = (\ell, 1) \sqsupseteq (\ell, n)$.
- (1) follows from monotonicity and $(\emptyset, [\ell \mapsto 1]) \in w.\mathsf{H}(s')(G(s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s_{\mathrm{rf}}', s'') \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s')$ and $G' \supseteq G$.
- Then necessarily $s'' = s'$.

- We must show $((\langle\rangle;1),(\langle\rangle;!\ell)) \in \mathbf{E}_{w\uparrow}(G')((s_{\mathrm{rf}},(\ell,n)),(s'_{\mathrm{rf}},s''))(\mathsf{int})$.
- So suppose $\mathrm{defined}(h'_1 \uplus h_1^{\mathrm{F}\prime})$ and $\mathrm{defined}(h'_2 \uplus h_2^{\mathrm{F}\prime})$ as well as $(h'_1,h'_2) \in w\uparrow.\mathsf{H}(s'_{\mathrm{rf}},s'')(G'(s'_{\mathrm{rf}},s''))$.
- Then there are $h_1'^{\mathrm{ref}}, h_2'^{\mathrm{ref}}$ such that $h'_1 = h_1'^{\mathrm{ref}}$ and $h'_2 = h_2'^{\mathrm{ref}} \uplus [\ell\mapsto 1]$.
- Therefore we know:
$$h'_2 \uplus h_2^{\mathrm{F}\prime}, (\langle\rangle;!\ell) \hookrightarrow^* h'_2 \uplus h_2^{\mathrm{F}\prime}, 1$$
- Of course we also know:
$$h'_1 \uplus h_1^{\mathrm{F}\prime}, (\langle\rangle;1) \hookrightarrow^* h'_1 \uplus h_1^{\mathrm{F}\prime}, 1$$
- Since $(s'_{\mathrm{rf}},s'') \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}},(\ell,n))$, it suffices by definition of $\mathbf{E}_{w\uparrow}$ to show $(1,1) \in \overline{G(s'_{\mathrm{rf}},s'')}(\mathsf{int})$, which is immediate.

Proving the programs related.. It remains to show $(v_1,e_2) \in \mathbf{E}_{\widehat{w}\uparrow}(G)((s_{\mathrm{rf}},s),(s_{\mathrm{rf}},s))(\tau)$ for any G, s_{rf}, s.

- So suppose $(h_1,h_2) \in \widehat{w}\uparrow.\mathsf{H}(s_{\mathrm{rf}},s)(G(s_{\mathrm{rf}},s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- Then there are
$$(h_1^{\mathrm{ref}},h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}},s)) \text{ and } (\widehat{h_1},\widehat{h_2}) \in \widehat{w}.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}},s))$$
with $h_1 = h_1^{\mathrm{ref}} \uplus \widehat{h_1}$ and $h_2 = h_2^{\mathrm{ref}} \uplus \widehat{h_2}$.
- Hence we have $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell\mapsto 0] \uplus h_2^{\mathrm{F}}, v_2$, where $v_2 = \lambda f.\,\ell := 1; f\ \langle\rangle; !\ell$ and ℓ is fresh.
- We are done if we can find $s' \sqsupseteq_{\mathrm{pub}} s$ such that:
  1) $(h_1^{\mathrm{ref}} \uplus \widehat{h_1}, h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell\mapsto 0]) \in \widehat{w}\uparrow.\mathsf{H}(s_{\mathrm{rf}},s')(G(s_{\mathrm{rf}},s'))$
  2) $(v_1,v_2) \in \overline{G(s_{\mathrm{rf}},s')}(\tau)$
- We pick $s' = (s,(\ell,0)) \sqsupseteq_{\mathrm{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h_1},\widehat{h_2} \uplus [\ell\mapsto 0]) \in \widehat{w}.\mathsf{H}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}},s'))$.
- By monotonicity and construction of $\widehat{w}$ it then suffices to show $(\emptyset,[\ell\mapsto 0]) \in w.\mathsf{H}(s_{\mathrm{rf}})(\ell,0)(G(s_{\mathrm{rf}},s'))$, which holds by construction of w.
- To show (2) it suffices by definition of GK to show $(v_1,v_2) \in \widehat{w}\uparrow.\mathsf{L}(s_{\mathrm{rf}},s')(G(s_{\mathrm{rf}},s'))(\tau)$.
- By construction of $\widehat{w}$ it then suffices to show $(v_1,v_2) \in w.\mathsf{L}(\ell,0)(G(s_{\mathrm{rf}},s'))(\tau)$, which also holds by construction of w.

6) Well-Bracketed State Change.

$$\begin{array}{rcl} \tau & := & (\mathsf{unit}\to\mathsf{unit})\to\mathsf{int} \\ v_1 & := & \lambda f.\, f\ \langle\rangle; f\ \langle\rangle; 1 \\ e_2 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\ & & \lambda f.\, x := 0; f\ \langle\rangle; x := 1; f\ \langle\rangle; !x \end{array}$$

We show $\cdot;\cdot \vdash v_1 \sim e_2 : \tau$. So let $\mathcal{N}$ be given. The proof splits conceptually into three parts:

1) Constructing a local world $\widehat{w}$ with $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$, $\mathit{stable}(\widehat{w})$, and $\mathit{inhabited}(\widehat{w}\uparrow)$.
2) Showing $\mathit{consistent}(\widehat{w}\uparrow)$. This is the meat of the proof.
3) Showing that v_1 and e_2 are related by $\mathbf{E}_{\widehat{w}\uparrow}$.

Constructing the world.. First, we define $w \in \mathrm{LWorld}$ as follows:

$$\begin{array}{lcl} w.\mathsf{N} & := & \emptyset \\ w.\mathsf{S} & := & \mathrm{Loc}\times\{0,1\} \\ w.\sqsupseteq & := & w.\sqsupseteq_{\mathrm{pub}} \cup \{((\ell,0),(\ell,1)) \mid \ell \in \mathrm{Loc}\} \\ w.\sqsupseteq_{\mathrm{pub}} & := & \{((\ell,1),(\ell,0)) \mid \ell \in \mathrm{Loc}\}^* \\ w.\mathsf{L} & := & \lambda s_{\mathrm{rf}},(\ell,n),R.\ \{((\mathsf{unit}\to\mathsf{unit})\to\mathsf{int}, v_1, (\lambda f.\,\ell := 0; f\ \langle\rangle; \ell := 1; f\ \langle\rangle; !\ell))\} \\ w.\mathsf{H} & := & \lambda s_{\mathrm{rf}},(\ell,n),R.\ \{(\emptyset,[\ell\mapsto n])\} \end{array}$$

Now let $\widehat{w} = \mathbf{G}(\lambda\mathcal{N}.w)(\mathcal{N})$. By definition of $\mathbf{G}$ we have $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 69 and 70 we know $\mathit{stable}(\widehat{w})$ and $\mathit{inhabited}(\widehat{w}\uparrow)$.

Showing consistency.. In order to show $\mathit{consistent}(\widehat{w}\uparrow)$, it suffices by Lemma 69 to just show $\mathit{consistent}(w\uparrow)$.

- So suppose $(s_{\mathrm{rf}},(\ell,n)) \in w\uparrow.\mathsf{S}$ and $(v'_1,v'_2) \in \overline{G(s_{\mathrm{rf}},(\ell,n))}(\mathsf{unit}\to\mathsf{unit})$.
- We need to show:
$$((v'_1\ \langle\rangle; v'_1\ \langle\rangle; 1),(\ell := 0; v'_2\ \langle\rangle; \ell := 1; v'_2\ \langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}},(\ell,n)),(s_{\mathrm{rf}},(\ell,n)))(\mathsf{int})$$
- So suppose $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$ as well as
$$(h_1,h_2) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}},(\ell,n))(G(s_{\mathrm{rf}},(\ell,n))).$$

- Then there are $(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}}, (\ell, n)))$ such that $h_1 = h_1^{\mathrm{ref}}$ and $h_2 = h_2^{\mathrm{ref}} \uplus [\ell \mapsto n]$.
- Therefore we know:
$$h_2 \uplus h_2^{\mathrm{F}}, (\ell := 0; v_2' \ \langle\rangle; \ell := 1; v_2' \ \langle\rangle; !\ell) \hookrightarrow h_2^{\mathrm{ref}} \uplus [\ell \mapsto 0] \uplus h_2^{\mathrm{F}}, (v_2' \ \langle\rangle; \ell := 1; v_2' \ \langle\rangle; !\ell)$$
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s' \sqsupseteq (\ell, n)$ such that:
  1) $(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}} \uplus [\ell \mapsto 0]) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s')(G(s_{\mathrm{rf}}, s'))$
  2) $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s')}(\mathsf{unit} \to \mathsf{unit})$
  3) $(\langle\rangle, \langle\rangle) \in \overline{G(s_{\mathrm{rf}}, s')}(\mathsf{unit})$
  4) $\forall (s_{\mathrm{rf}}', \widetilde{s'}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s').\forall G' \supseteq G.$
  $((\bullet; v_1' \ \langle\rangle; 1), (\bullet; \ell := 1; v_2' \ \langle\rangle; !\ell)) \in \mathbf{K}_{w\uparrow}(G')((s_{\mathrm{rf}}, (\ell, n)), (s_{\mathrm{rf}}', \widetilde{s'}))(\mathsf{unit}, \mathsf{int})$
- We pick $s' = (\ell, 0) \sqsupseteq (\ell, n)$.
- (1) follows from monotonicity and $(\emptyset, [\ell \mapsto 1]) \in w.\mathsf{H}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s_{\mathrm{rf}}', \widetilde{s'}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, s')$ and $G' \supseteq G$.
- We need to show:
$$((\langle\rangle; v_1' \ \langle\rangle; 1), (\langle\rangle; \ell := 1; v_2' \ \langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G')((s_{\mathrm{rf}}, (\ell, n)), (s_{\mathrm{rf}}', \widetilde{s'}))(\mathsf{int})$$
- So suppose $\mathrm{defined}(h_1' \uplus h_1^{\mathrm{F}'})$ and $\mathrm{defined}(h_2' \uplus h_2^{\mathrm{F}'})$ as well as
$$(h_1', h_2') \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}', \widetilde{s'})(G'(s_{\mathrm{rf}}', \widetilde{s'})).$$
- Then there are $(h_1'^{\mathrm{ref}}, h_2'^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}}')(G'(s_{\mathrm{rf}}', \widetilde{s'}))$ such that $h_1' = h_1'^{\mathrm{ref}}$ and $h_2' = h_2'^{\mathrm{ref}} \uplus [\ell \mapsto n']$.
- Therefore we know:
$$\begin{aligned} h_1' \uplus h_1^{\mathrm{F}'}, (\langle\rangle; v_1' \ \langle\rangle; 1) &\hookrightarrow h_1'^{\mathrm{ref}} \uplus h_1^{\mathrm{F}'}, (v_1' \ \langle\rangle; 1) \\ h_2' \uplus h_2^{\mathrm{F}'}, (\langle\rangle; \ell := 1; v_2' \ \langle\rangle; !\ell) &\hookrightarrow h_2'^{\mathrm{ref}} \uplus [\ell \mapsto 1] \uplus h_2^{\mathrm{F}'}, (v_2' \ \langle\rangle; !\ell) \end{aligned}$$
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s'' \sqsupseteq \widetilde{s'}$ such that:
  1) $(h_1'^{\mathrm{ref}}, h_2'^{\mathrm{ref}} \uplus [\ell \mapsto 1]) \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}', s'')(G'(s_{\mathrm{rf}}', s''))$
  2) $(v_1', v_2') \in \overline{G'(s_{\mathrm{rf}}', s'')}(\mathsf{unit} \to \mathsf{unit})$
  3) $(\langle\rangle, \langle\rangle) \in \overline{G'(s_{\mathrm{rf}}', s'')}(\mathsf{unit})$
  4) $\forall (s_{\mathrm{rf}}'', \widetilde{s''}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}', s'').\forall G'' \supseteq G'.\ ((\bullet; 1), (\bullet; !\ell)) \in \mathbf{K}_{w\uparrow}(G'')((s_{\mathrm{rf}}, (\ell, n)), (s_{\mathrm{rf}}'', \widetilde{s''}))(\mathsf{unit}, \mathsf{int})$
- We pick $s'' = (\ell, 1) \sqsupseteq \widetilde{s'}$.
- (1) follows from monotonicity and $(\emptyset, [\ell \mapsto 1]) \in w.\mathsf{H}(s_{\mathrm{rf}})(s')(G'(s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s_{\mathrm{rf}}'', \widetilde{s''}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}', s'')$ and $G'' \supseteq G'$.
- Then necessarily $\widetilde{s''} = s''$.
- We must show $((\langle\rangle; 1), (\langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G'')((s_{\mathrm{rf}}, (\ell, n)), (s_{\mathrm{rf}}'', s''))(\mathsf{int})$.
- So suppose $\mathrm{defined}(h_1'' \uplus h_1^{\mathrm{F}''})$ and $\mathrm{defined}(h_2'' \uplus h_2^{\mathrm{F}''})$ as well as $(h_1'', h_2'') \in w\uparrow.\mathsf{H}(s_{\mathrm{rf}}'', s'')(G''(s_{\mathrm{rf}}'', s''))$.
- Then there are $h_1''^{\mathrm{ref}}, h_2''^{\mathrm{ref}}$ such that $h_1'' = h_1''^{\mathrm{ref}}$ and $h_2'' = h_2''^{\mathrm{ref}} \uplus [\ell \mapsto 1]$.
- Therefore we know:
$$h_2'' \uplus h_2^{\mathrm{F}''}, (\langle\rangle; !\ell) \hookrightarrow^* h_2'' \uplus h_2^{\mathrm{F}''}, 1$$
- Of course we also know:
$$h_1'' \uplus h_1^{\mathrm{F}''}, (\langle\rangle; 1) \hookrightarrow^* h_1'' \uplus h_1^{\mathrm{F}''}, 1$$
- Since $(s_{\mathrm{rf}}'', s'') \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{rf}}, (\ell, n))$, it suffices by definition of $\mathbf{E}_{w\uparrow}$ to show $(1, 1) \in \overline{G(s_{\mathrm{rf}}'', s'')}(\mathsf{int})$, which is immediate.

Proving the programs related.. It remains to show $(v_1, e_2) \in \mathbf{E}_{\widehat{w}\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\tau)$ for any G, s_{rf}, s.

- So suppose $(h_1, h_2) \in \widehat{w}\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- Then there are
$$(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}}, s)) \text{ and } (\widehat{h_1}, \widehat{h_2}) \in \widehat{w}.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}}, s))$$
with $h_1 = h_1^{\mathrm{ref}} \uplus \widehat{h_1}$ and $h_2 = h_2^{\mathrm{ref}} \uplus \widehat{h_2}$.
- Hence we have $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell \mapsto 0] \uplus h_2^{\mathrm{F}}, v_2$, where $v_2 = \lambda f.\, \ell := 0; f \ \langle\rangle; \ell := 1; f \ \langle\rangle; !\ell$ and ℓ is fresh.
- We are done if we can find $s' \sqsupseteq_{\mathrm{pub}} s$ such that:
  1) $(h_1^{\mathrm{ref}} \uplus \widehat{h_1}, h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell \mapsto 0]) \in \widehat{w}\uparrow.\mathsf{H}(s_{\mathrm{rf}}, s')(G(s_{\mathrm{rf}}, s'))$
  2) $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s')}(\tau)$

- We pick $s' = (s, (\ell, 0)) \sqsupseteq_{\text{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h_1}, \widehat{h_2} \uplus [\ell \mapsto 0]) \in \widehat{w}.\mathsf{H}(s_{\text{rf}})(s')(G(s_{\text{rf}}, s'))$.
- By monotonicity and construction of $\widehat{w}$ it then suffices to show $(\emptyset, [\ell \mapsto 0]) \in w.\mathsf{H}(s_{\text{rf}})(\ell, 0)(G(s_{\text{rf}}, s'))$, which holds by construction of w.
- To show (2) it suffices by definition of GK to show $(v_1, v_2) \in \widehat{w}\!\uparrow.\mathsf{L}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))(\tau)$.
- By construction of $\widehat{w}$ it then suffices to show $(v_1, v_2) \in w.\mathsf{L}(s_{\text{rf}})(\ell, 0)(G(s_{\text{rf}}, s'))(\tau)$, which also holds by construction of w.

7) Twin Abstraction.

$$\begin{array}{rcl}
\tau & := & \exists\alpha.\,\exists\beta.\,(\mathsf{unit} \to \alpha) \times (\mathsf{unit} \to \beta) \times (\alpha \times \beta \to \mathsf{bool}) \\
e_1 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in}\ \mathsf{pack}\ \langle \mathsf{int}, \mathsf{pack}\ \langle \mathsf{int}, \lambda_.\, x := !x + 1; !x, \\
& & \qquad\qquad\qquad\qquad \lambda_.\, x := !x + 1; !x, \\
& & \qquad\qquad\qquad\qquad \lambda p.\, p.1 = p.2 \rangle\rangle \\
e_2 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in}\ \mathsf{pack}\ \langle \mathsf{int}, \mathsf{pack}\ \langle \mathsf{int}, \lambda_.\, x := !x + 1; !x, \\
& & \qquad\qquad\qquad\qquad \lambda_.\, x := !x + 1; !x, \\
& & \qquad\qquad\qquad\qquad \lambda p.\, \mathsf{ff} \rangle\rangle
\end{array}$$

We show $\cdot;\cdot \vdash e_1 \sim e_2 : \tau$. So let $\mathcal{N}$ be given. The proof splits conceptually into three parts:

1) Constructing a world w with $w.\mathsf{N} \subseteq \mathcal{N}$, $\mathit{stable}(w)$, and $\mathit{inhabited}(w\!\uparrow)$.
2) Showing $\mathit{consistent}(w\!\uparrow)$. This is the meat of the proof.
3) Showing that e_1 and e_2 are related by $\mathbf{E}_{w\uparrow}$.

Constructing the world.. First, we define $\mathcal{W} \in \text{NLWorld}$ as follows:

$$\begin{array}{lcl}
\mathcal{W}(\mathcal{N}').\mathsf{N} & := & \{\mathcal{N}'(1), \mathcal{N}'(2)\} \\
\mathcal{W}(\mathcal{N}').\mathsf{S} & := & \{(\ell_1, \ell_2, S_1, S_2) \in \text{Loc} \times \text{Loc} \times \mathbb{P}(\mathbb{N}_{>0}) \times \mathbb{P}(\mathbb{N}_{>0}) \mid S_1 \cap S_2 = \emptyset\} \\
\mathcal{W}(\mathcal{N}').\sqsupseteq & := & \mathcal{W}(\mathcal{N}').\sqsupseteq_{\text{pub}} \\
\mathcal{W}(\mathcal{N}').\sqsupseteq_{\text{pub}} & := & \{((\ell_1', \ell_2', S_1', S_2'), (\ell_1, \ell_2, S_1, S_2) \mid \ell_1 = \ell_1' \wedge \ell_2 = \ell_2' \wedge S_1 \subseteq S_1' \wedge S_2 \subseteq S_2'\} \\
\mathcal{W}(\mathcal{N}').\mathsf{L} & := & \lambda(\ell_1, \ell_2, S_1, S_2), R.\ \{(\mathcal{N}'(1), n, n) \mid n \in S_1\} \uplus \{(\mathcal{N}'(2), n, n) \mid n \in S_2\} \uplus \\
& & \qquad \{((\mathsf{unit} \to \mathcal{N}'(1)), (\lambda_.\, \ell_1 := !\ell_1 + 1; !\ell_1), (\lambda_.\, \ell_1 := !\ell_1 + 1; !\ell_1))\} \uplus \\
& & \qquad \{((\mathsf{unit} \to \mathcal{N}'(2)), (\lambda_.\, \ell_2 := !\ell_2 + 1; !\ell_2), (\lambda_.\, \ell_2 := !\ell_2 + 1; !\ell_2))\} \uplus \\
& & \qquad \{((\mathcal{N}'(1) \times \mathcal{N}'(2) \to \mathsf{bool}), (\lambda p.\, p.1 = p.2), (\lambda p.\, \mathsf{ff}))\} \\
\mathcal{W}(\mathcal{N}').\mathsf{H} & := & \lambda(\ell_1, \ell_2, S_1, S_2), R.\ \{([\ell_1 \mapsto n], [\ell_2 \mapsto n]) \mid n = \max(\{0\} \uplus S_1 \uplus S_2)\}
\end{array}$$

where $\mathcal{N}'(1)$ and $\mathcal{N}'(2)$ denote two distinct elements of $\mathcal{N}'$.

Now let $w = \mathbf{G}(\mathcal{W})(\mathcal{N})$. By definition of $\mathbf{G}$ we have $w.\mathsf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 69 and 70 we know $\mathit{stable}(w)$ and $\mathit{inhabited}(w\!\uparrow)$.

Showing consistency.. In order to show $\mathit{consistent}(w\!\uparrow)$, it suffices by Lemma 69 to just show $\mathit{consistent}(\mathcal{W}(\mathcal{N}')\!\uparrow)$ for any $\mathcal{N}'$. This decomposes into the following subgoals (for any $G, s_{\text{rf}}, s = (\ell_1, \ell_2, S_1, S_2)$):

1) $((\ell_1 := !\ell_1 + 1; !\ell_1), (\ell_1 := !\ell_1 + 1; !\ell_1)) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\mathcal{N}'(1))$
2) $((\ell_2 := !\ell_2 + 1; !\ell_2), (\ell_2 := !\ell_2 + 1; !\ell_2)) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\mathcal{N}'(2))$
3) $\forall (v_1', v_2') \in \overline{G(s_{\text{rf}}, s)}(\mathcal{N}'(1) \times \mathcal{N}'(2)).\ (v_1'.1 = v_1'.2, \mathsf{ff}) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\mathsf{bool})$

For (1) (part (2) is analogously):

- Suppose $(h_1, h_2) \in \mathcal{W}(\mathcal{N}')\!\uparrow.\mathsf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as $\text{defined}(h_1 \uplus h_1^{\text{F}})$ and $\text{defined}(h_2 \uplus h_2^{\text{F}})$.
- Then there are
$$(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathsf{H}(s_{\text{rf}})(G(s_{\text{rf}}, s)) \text{ and } (h_1^{\circ}, h_2^{\circ}) \in \mathcal{W}(\mathcal{N}').\mathsf{H}(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$$
with $h_1 = h_1^{\text{ref}} \uplus h_1^{\circ}$ and $h_2 = h_2^{\text{ref}} \uplus h_2^{\circ}$.
- By construction of $\mathcal{W}(\mathcal{N}')$ we know $h_1^{\circ} = [\ell_1 \mapsto n]$ and $h_2^{\circ} = [\ell_2 \mapsto n]$ where $n = \max(\{0\} \uplus S_1 \uplus S_2)$.
- Hence $h_1 \uplus h_1^{\text{F}}, (\ell_1 := !\ell_1 + 1; !\ell_1) \hookrightarrow^* h_1^{\text{ref}} \uplus [\ell_1 \mapsto n+1] \uplus h_1^{\text{F}}, n+1$
and $h_2 \uplus h_2^{\text{F}}, (\ell_2 := !\ell_2 + 1; !\ell_2) \hookrightarrow^* h_2^{\text{ref}} \uplus [\ell_2 \mapsto n+1] \uplus h_2^{\text{F}}, n+1$.
- By definition of $\mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}$ it suffices to find $s' \sqsupseteq_{\text{pub}} s$ such that:
  a) $(h_1^{\text{ref}} \uplus [\ell_1 \mapsto n+1], h_1^{\text{ref}} \uplus [\ell_2 \mapsto n+1]) \in \mathcal{W}(\mathcal{N}')\!\uparrow.\mathsf{H}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))$
  b) $(n+1, n+1) \in \overline{G(s_{\text{rf}}, s')}(\mathcal{N}'(1))$
- We pick $s' = (\ell_1, \ell_2, S_1 \uplus \{n+1\}, S_2)$.
- Note that $n+1 \notin S_1 \cup S_2$ and thus $(S_1 \uplus \{n+1\}) \cap S_2 = \emptyset$, so s' is well-formed.

- Since $n{+}1 = \max\{0\} \uplus S_1 \uplus \{n+1\} \uplus S_2$, (a) follows from $([\ell_1{\mapsto}n{+}1], [\ell_2{\mapsto}n{+}1]) \in \mathcal{W}(\mathcal{N}').\mathsf{H}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s'))$ by construction of $\mathcal{W}(\mathcal{N}')$.
- To show (b) it suffices, by definition of GK, to show
$$(n+1, n+1) \in \mathcal{W}(\mathcal{N}'){\uparrow}.\mathsf{L}(s_{\mathrm{rf}}, s')(G(s_{\mathrm{rf}}, s'))(\mathcal{N}'(1)).$$
- This follows from
$$(n+1, n+1) \in \mathcal{W}(\mathcal{N}').\mathsf{L}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s'))(\mathcal{N}'(1)),$$
which in turns holds by construction of $\mathcal{W}(\mathcal{N}')$.

For (3):

- Suppose $(v_1', v_2') \in \overline{G(s_{\mathrm{rf}}, s)}(\mathcal{N}'(1) \times \mathcal{N}'(2))$.
- Then $v_1' = \langle \widehat{v_1}, \widetilde{v_1} \rangle$ and $v_2' = \langle \widehat{v_2}, \widetilde{v_2} \rangle$ with $(\widehat{v_1}, \widehat{v_2}) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathcal{N}'(1))$ and $(\widetilde{v_1}, \widetilde{v_2}) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathcal{N}'(2))$.
- By definition of GK and construction of $\mathcal{W}(\mathcal{N}')$ we know $\widehat{v_1} = \widehat{v_2} \in S_1$ and $\widetilde{v_1} = \widetilde{v_2} \in S_2$.
- Now suppose $(h_1, h_2) \in \mathcal{W}(\mathcal{N}'){\uparrow}.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- Since $S_1 \cap S_2 = \emptyset$, we get $h_1 \uplus h_1^{\mathrm{F}}, v_1'.1 = v_1'.2 \hookrightarrow^* h_1 \uplus h_1^{\mathrm{F}}, \mathsf{ff}$ and $h_2 \uplus h_2^{\mathrm{F}}, \mathsf{ff} \hookrightarrow^* h_2 \uplus h_2^{\mathrm{F}}, \mathsf{ff}$.
- Since $(\mathsf{ff}, \mathsf{ff}) \in \overline{G(s_{\mathrm{rf}}, s)}(\mathsf{bool})$, we are done.

Proving the programs related.. It remains to show $(e_1, e_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{rf}}, s), (s_{\mathrm{rf}}, s))(\tau)$ for any G, s_{rf}, s.

- So suppose $(h_1, h_2) \in w{\uparrow}.\mathsf{H}(s_{\mathrm{rf}}, s)(G(s_{\mathrm{rf}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- Then there are
$$(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{rf}})(G(s_{\mathrm{rf}}, s)) \text{ and } (\widehat{h_1}, \widehat{h_2}) \in w.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}}, s))$$
with $h_1 = h_1^{\mathrm{ref}} \uplus \widehat{h_1}$ and $h_2 = h_2^{\mathrm{ref}} \uplus \widehat{h_2}$.
- Hence we have
$$h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow h_1^{\mathrm{ref}} \uplus \widehat{h_1} \uplus [\ell_1{\mapsto}0] \uplus h_1^{\mathrm{F}}, \mathsf{pack}\ \mathsf{pack}\ v_1 \text{ and } h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell_2{\mapsto}0] \uplus h_2^{\mathrm{F}}, \mathsf{pack}\ \mathsf{pack}\ v_2$$
where ℓ_1 and ℓ_2 are fresh and v_1, v_2 are what you think they are.
- We are done if we can find $s' \sqsupseteq_{\mathrm{pub}} s$ such that:

1) $(h_1^{\mathrm{ref}} \uplus \widehat{h_1} \uplus [\ell_1{\mapsto}0], h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell_2{\mapsto}0]) \in w{\uparrow}.\mathsf{H}(s_{\mathrm{rf}}, s')(G(s_{\mathrm{rf}}, s'))$
2) $(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s')}(\tau)$

- We pick $s' = (s, (\ell_1, \ell_2, \emptyset, \emptyset)) \sqsupseteq_{\mathrm{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h_1} \uplus [\ell_1{\mapsto}0], \widehat{h_2} \uplus [\ell_2{\mapsto}0]) \in w.\mathsf{H}(s_{\mathrm{rf}})(s')(G(s_{\mathrm{rf}}, s'))$.
- By monotonicity and construction of w it then suffices to show $([\ell_1{\mapsto}0], [\ell_2{\mapsto}0]) \in \mathcal{W}(\mathcal{N}').\mathsf{H}(s_{\mathrm{rf}})(\ell_1, \ell_2, \emptyset, \emptyset)(G(s_{\mathrm{rf}}, s'))$ (for any $\mathcal{N}'$), which holds by construction of $\mathcal{W}$.
- To show (2), we pick the witness types $\mathcal{N}_n(1)$ and $\mathcal{N}_n(2)$, where $n := |s'|$.
- It thus suffices to show:
$$(v_1, v_2) \in \overline{G(s_{\mathrm{rf}}, s')}((\mathsf{unit} \to \mathcal{N}_n(1)) \times (\mathsf{unit} \to \mathcal{N}_n(2)) \times (\mathcal{N}_n(1) \times \mathcal{N}_n(2) \to \mathsf{bool}))$$
- This in turn reduces to showing the following:
  - $((\mathsf{unit} \to \mathcal{N}_n(1)), (\lambda\_.\, \ell_1 := !\ell_1 + 1; !\ell_1), (\lambda\_.\, \ell_1 := !\ell_1 + 1; !\ell_1)) \in \overline{G(s_{\mathrm{rf}}, s')}$
  - $((\mathsf{unit} \to \mathcal{N}_n(2)), (\lambda\_.\, \ell_2 := !\ell_2 + 1; !\ell_2), (\lambda\_.\, \ell_2 := !\ell_2 + 1; !\ell_2)) \in \overline{G(s_{\mathrm{rf}}, s')}$
  - $((\mathcal{N}_n(1) \times \mathcal{N}_n(2) \to \mathsf{bool}), (\lambda p.\, p.1 = p.2), (\lambda p.\, \mathsf{ff})) \in \overline{G(s_{\mathrm{rf}}, s')}$
- By definition of GK and construction of w, it suffices to show that these triples are in $\mathcal{W}(\mathcal{N}_n).\mathsf{L}(\ell_1, \ell_2, \emptyset, \emptyset)(G(s_{\mathrm{rf}}, s'))$.
- This is true by construction of $\mathcal{W}$.

E. Weak Isomorphism Theorem

1) Weak Isomorphisms.

Definition 12. Assuming $W_1, W_2 \in \mathrm{World}$, then a function $\phi \in W_1.\mathsf{S} \to \mathbb{P}(W_2.\mathsf{S})$ is a *weak morphism* from W_1 to W_2, written $\phi : W_1 \to W_2$, if:

1) $W_1.\mathsf{N} = W_2.\mathsf{N}$
2) $\forall s_1, s_1'.\ s_1 \sqsubseteq s_1' \implies \forall s_2 \in \phi(s_1), s_2' \in \phi(s_1').\ s_2 \sqsubseteq s_2'$
3) $\forall s_1, s_1'.\ s_1 \sqsubseteq_{\mathrm{pub}} s_1' \implies \forall s_2 \in \phi(s_1), s_2' \in \phi(s_1').\ s_2 \sqsubseteq_{\mathrm{pub}} s_2'$
4) $\forall s_1.\forall s_2 \in \phi(s_1).\ W_1.\mathsf{L}(s_1) = W_2.\mathsf{L}(s_2)$
5) $\forall s_1.\forall G \in \mathrm{GK}(W_1).\ W_1.\mathsf{H}(s_1)(G(s_1)) \subseteq \bigcup_{s_2 \in \phi(s_1)} W_2.\mathsf{H}(s_2)(G(s_1))$

Definition 13. The identity weak morphism id_W on W is defined as $\mathrm{id}_W(s) = \{\, s \,\}$. It is obvious that id_W forms a weak morphism.

Definition 14. The composition of weak morphisms $\psi \circ \phi$ is defined as $(\psi \circ \phi)(s) = \bigcup_{s' \in \phi(s)} \psi(s')$. We will show that $\psi \circ \phi$ forms a weak morphism in Lemma 80.

Definition 15. Between two weak morphisms $\phi_1, \phi_2 : W_1 \to W_2$, we define the following preorders $\sqsubseteq$ and $\sqsubseteq_{\mathrm{pub}}$:

$$\phi_1 \sqsupseteq \phi_2 \quad \text{iff} \quad \forall s.\ \forall s_1 \in \phi_1(s).\ \forall s_2 \in \phi_2(s).\ s_1 \sqsupseteq s_2$$
$$\phi_1 \sqsupseteq_{\mathrm{pub}} \phi_2 \quad \text{iff} \quad \forall s.\ \forall s_1 \in \phi_1(s).\ \forall s_2 \in \phi_2(s).\ s_1 \sqsupseteq_{\mathrm{pub}} s_2$$

Definition 16. A pair of weak morphisms $\phi : W_1 \to W_2$, $\psi : W_2 \to W_1$ is a weak isomorphism, written $\phi : W_1 \cong W_2 : \psi$, if $\psi \circ \phi \sqsupseteq_{\mathrm{pub}} \mathrm{id}$ and $\phi \circ \psi \sqsupseteq_{\mathrm{pub}} \mathrm{id}$.

2) Global Knowledge Constructions. Recall that for a monotone function $F \in \mathrm{VRelF} \to \mathrm{VRelF}$ and $R \in \mathrm{VRelF}$, we write $[F]^*_R$ for the least fixpoint of the monotone function $F(-) \cup R$.

Definition 17. Given $\phi : W_1 \to W_2$ and $G \in \mathrm{GK}(W_2)$, we define $\overleftarrow{G_\phi} \in W_1.\mathsf{S} \to \mathrm{VRelF}$ as follows.

$$\overleftarrow{G_\phi}(s_1) = [W_1.\mathsf{L}(s_1)]^*_{(\bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} G(s_2'))}$$

Definition 18. Given $\phi : W_1 \to W_2$ and $G \in \mathrm{GK}(W_1)$, we define $\overrightarrow{G_\phi^{s_1}} \in W_2.\mathsf{S} \to \mathrm{VRelF}$ for $s_1 \in W_1.\mathsf{S}$ as follows.

$$\overrightarrow{G_\phi^{s_1}}(s_2) = [W_2.\mathsf{L}(s_2)]^*_{(\bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} G(s_1'))}$$

Lemma 74. Given $\phi : W_1 \to W_2$ and $G \in \mathrm{GK}(W_2)$, we have $\forall s_2 \in \phi(s_1).\ \overleftarrow{G_\phi}(s_1) = G(s_2)$.

Proof:

- Suppose $s_2 \in \phi(s_1)$.
- We first show $G(s_2) = \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} G(s_2')$:
  - $G(s_2) \subseteq \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} G(s_2')$ is obvious.
  - To see the other inclusion, note that whenever $s_2' \in \phi(s_1')$ and $s_1' \sqsubseteq s_1$, then $s_2' \sqsubseteq s_2$ and thus $G(s_2') \subseteq G(s_2)$.
- Consequently we know $\overleftarrow{G_\phi}(s_1) = [W_1.\mathsf{L}(s_1)]^*_{G(s_2)} = W_1.\mathsf{L}(s_1)([W_1.\mathsf{L}(s_1)]^*_{G(s_2)}) \cup G(s_2) \supseteq G(s_2)$.
- To show $[W_1.\mathsf{L}(s_1)]^*_{G(s_2)} \subseteq G(s_2)$, it suffices by induction to show $W_1.\mathsf{L}(s_1)(G(s_2)) \cup G(s_2) \subseteq G(s_2)$.
- This follows from $W_1.\mathsf{L}(s_1)(G(s_2)) = W_2.\mathsf{L}(s_2)(G(s_2)) \subseteq G(s_2)$.

■

Lemma 75. If $\phi : W_1 \to W_2$ and $G \in \mathrm{GK}(W_2)$, then $\overleftarrow{G_\phi} \in \mathrm{GK}(W_1)$.

Proof:

- $\overleftarrow{G_\phi}$ is monotone by definition because $[W_1.\mathsf{L}(s_1)]^*_{(-)}$ is monotone.
- We have $\overleftarrow{G_\phi}(s_1) = W_1.\mathsf{L}(s_1)(\overleftarrow{G_\phi}(s_1)) \cup \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} G(s_2') \supseteq W_1.\mathsf{L}(s_1)(\overleftarrow{G_\phi}(s_1))$.

- Moreover, for any $\tau \in \mathrm{CType}$ we have $\overleftarrow{G_\phi}(s_1)(\mathsf{ref}\,\tau) = W_1.\mathsf{L}(s_1)(\overleftarrow{G_\phi}(s_1))(\mathsf{ref}\,\tau)$ because:
$$\begin{array}{rll} & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} G(s_2')(\mathsf{ref}\,\tau) & \\ = & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} W_2.\mathsf{L}(s_2')(G(s_2'))(\mathsf{ref}\,\tau) & (G \in \mathrm{GK}(W_2)) \\ = & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} W_1.\mathsf{L}(s_1')(G(s_2'))(\mathsf{ref}\,\tau) & (\phi : W_1 \to W_2) \\ = & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} W_1.\mathsf{L}(s_1')(\overleftarrow{G_\phi}(s_1'))(\mathsf{ref}\,\tau) & \text{(Lemma 74)} \\ \subseteq & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \in \phi(s_1')} W_1.\mathsf{L}(s_1)(\overleftarrow{G_\phi}(s_1))(\mathsf{ref}\,\tau) & \\ = & W_1.\mathsf{L}(s_1)(\overleftarrow{G_\phi}(s_1))(\mathsf{ref}\,\tau) & \end{array}$$
- Using an analogous argument, for any $\mathbf{n} \in W_1.\mathsf{N} = W_2.\mathsf{N}$, we have $\overleftarrow{G_\phi}(s_1)(\mathbf{n}) = W_1.\mathsf{L}(s_1)(\overleftarrow{G_\phi}(s_1))(\mathbf{n})$.

■

Lemma 76. Given $\phi : W_1 \to W_2$ and $G \in \mathrm{GK}(W_1)$, we have $\forall s_2 \in \phi(s_1).\ \overrightarrow{G_\phi^{s_1}}(s_2) = G(s_1)$.

Proof:

- Suppose $s_2 \in \phi(s_1)$.
- We first show $G(s_1) = \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} G(s_1')$:
  - $G(s_1) \subseteq \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} G(s_1')$ is obvious.
  - To see the other inclusion, note that whenever $s_1' \sqsubseteq s_1$, then $G(s_1') \subseteq G(s_1)$.
- Consequently we know $\overrightarrow{G_\phi^{s_1}}(s_2) = [W_2.\mathsf{L}(s_2)]^*_{G(s_1)} = W_2.\mathsf{L}(s_2)([W_2.\mathsf{L}(s_2)]^*_{G(s_1)}) \cup G(s_1) \supseteq G(s_1)$.
- To show $[W_2.\mathsf{L}(s_2)]^*_{G(s_1)} \subseteq G(s_1)$, it suffices by induction to show $W_2.\mathsf{L}(s_2)(G(s_1)) \cup G(s_1) \subseteq G(s_1)$.
- This follows from $W_2.\mathsf{L}(s_2)(G(s_1)) = W_1.\mathsf{L}(s_1)(G(s_1)) \subseteq G(s_1)$.

■

Lemma 77. If $\phi : W_1 \to W_2$ and $G \in \mathrm{GK}(W_1)$, then $\overrightarrow{G_\phi^{s_1}} \in \mathrm{GK}(W_2)$ for any $s_1 \in W_1.\mathsf{S}$.

Proof:

- We have the following monotonicity by definition because $[W_2.\mathsf{L}(s_2)]^*_{(-)}$ is monotone:
$$\forall \widetilde{s_1} \sqsupseteq \widehat{s_1}.\ \forall \widetilde{s_2} \sqsupseteq \widehat{s_2}.\ \overrightarrow{G_\phi^{s_1}}(\widetilde{s_2}) \supseteq \overrightarrow{G_\phi^{s_1}}(\widehat{s_2})$$
- We have $\overrightarrow{G_\phi^{s_1}}(s_2) = W_2.\mathsf{L}(s_2)(\overrightarrow{G_\phi^{s_1}}(s_2)) \cup \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} G(s_1') \supseteq W_2.\mathsf{L}(s_2)(\overrightarrow{G_\phi^{s_1}}(s_2))$.
- Moreover, for any $\tau \in \mathrm{CType}$ we have $\overrightarrow{G_\phi^{s_1}}(s_2)(\mathsf{ref}\,\tau) = W_2.\mathsf{L}(s_2)(\overrightarrow{G_\phi^{s_1}}(s_2))(\mathsf{ref}\,\tau)$ because:
$$\begin{array}{rll} & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} G(s_1')(\mathsf{ref}\,\tau) & \\ = & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_1.\mathsf{L}(s_1')(G(s_1'))(\mathsf{ref}\,\tau) & (G \in \mathrm{GK}(W_1)) \\ = & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_2.\mathsf{L}(s_2')(G(s_1'))(\mathsf{ref}\,\tau) & (\phi : W_1 \to W_2) \\ = & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_2.\mathsf{L}(s_2')(\overrightarrow{G_\phi^{s_1'}}(s_2'))(\mathsf{ref}\,\tau) & \text{(Lemma 76)} \\ \subseteq & \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_2.\mathsf{L}(s_2)(\overrightarrow{G_\phi^{s_1}}(s_2))(\mathsf{ref}\,\tau) & \text{(Monotonicity)} \\ = & W_2.\mathsf{L}(s_2)(\overrightarrow{G_\phi^{s_1}}(s_2))(\mathsf{ref}\,\tau) & \end{array}$$
- Using an analogous argument, for any $\mathbf{n} \in W_2.\mathsf{N} = W_1.\mathsf{N}$, we have $\overrightarrow{G_\phi^{s_1}}(s_2)(\mathbf{n}) = W_2.\mathsf{L}(s_2)(\overrightarrow{G_\phi^{s_1}}(s_2))(\mathbf{n})$.

■

3) Category of Worlds.

Lemma 78. If $\phi : W_1 \to W_2$, then $\phi \circ \mathrm{id}_{W_1} = \phi = \mathrm{id}_{W_2} \circ \phi$.

Proof: Obvious. ■

Lemma 79. If $\phi : W_1 \to W_2$, $\psi : W_2 \to W_3$, $\chi : W_3 \to W_4$, then $\chi \circ (\psi \circ \phi) = (\chi \circ \psi) \circ \phi$.

Proof:

$$\begin{array}{ll} & s_4 \in (\chi \circ (\psi \circ \phi))(s_1) \\ \iff & \exists s_3.\ s_4 \in \chi(s_3) \wedge s_3 \in (\psi \circ \phi)(s_1) \\ \iff & \exists s_3, s_2.\ s_4 \in \chi(s_3) \wedge s_3 \in \psi(s_2) \wedge s_2 \in \phi(s_1) \\ \iff & \exists s_2.\ s_4 \in (\chi \circ \psi)(s_2) \wedge s_2 \in \phi(s_1) \\ \iff & s_4 \in ((\chi \circ \psi) \circ \phi)(s_1) \end{array}$$

■

Lemma 80. If $\phi : W_1 \to W_2$ and $\psi : W_2 \to W_3$, then $\psi \circ \phi$ forms a weak morphism.

Proof: Conditions (1) through (4) hold vacuously. Condition (5) follows from Lemmas 76 and 77. ■

Proposition 81. Worlds with weak morphisms form a category.

Proof: It follows from Lemmas 78, 79 and 80. ■

4) Isomorphism Theorem.

Definition 19. Given $\phi : W_1 \to W_2$, we define $|-|_\phi \in \mathbb{P}(W_1.\mathsf{S}) \to \mathbb{P}(W_1.\mathsf{S})$ as follows:

$$|S|_\phi = \{\, s_1 \in S \mid \phi(s_1) \neq \emptyset \,\}$$

When ϕ is clear from context, we often just write $|S|$.

Lemma 82. If $\phi : W_1 \cong W_2 : \psi$ and $G \in \mathrm{GK}(W_2)$, then:

$$\bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1) \subseteq \mathbf{E}_{W_2}(G)(s_2^0, s_2)$$
$$\bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{K}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1) \subseteq \mathbf{K}_{W_2}(G)(s_2^0, s_2)$$

Proof: We define:

$$\mathbf{E}'_{W_2}(G)(s_2^0, s_2) = \bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)$$
$$\mathbf{K}'_{W_2}(G)(s_2^0, s_2) = \bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{K}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)$$

We prove $\mathbf{E}'_{W_2} \subseteq \mathbf{E}_{W_2}$ and $\mathbf{K}'_{W_2} \subseteq \mathbf{K}_{W_2}$ by coinduction. Concretely, we have to show:

1) $\forall e_1, e_2, G, s_2^0, s_2, \tau.$
   $(e_1, e_2) \in \mathbf{E}'_{W_2}(G)(s_2^0, s_2)(\tau) \implies$
   $\forall (h_1, h_2) \in W_2.\mathsf{H}(s_2)(G(s_2)).\forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.$
   $((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_{W_2}(\mathbf{K}'_{W_2})(G)(s_2^0, s_2)(\tau)$
2) $\forall K_1, K_2, G, s_2^0, s_2, \tau', \tau.$
   $(K_1, K_2) \in \mathbf{K}'_{W_2}(G)(s_2^0, s_2)(\tau', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s_2)}(\tau').\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{W_2}(G)(s_2^0, s_2)(\tau)$

Part (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_{W_2}(G)(s_2^0, s_2)(\tau)$, and thus $(e_1, e_2) \in \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)(\tau)$ for some $s_1^0 \in |\psi(s_2^0)|$.
- Further suppose $(h_1, h_2) \in W_2.\mathsf{H}(s_2)(G(s_2))$, and thus $(h_1, h_2) \in \bigcup_{s_1 \in \psi(s_2)} W_1.\mathsf{H}(s_1)(G(s_2))$.
- Thus there exists $s_1 \in \psi(s_2)$ such that $(h_1, h_2) \in W_1.\mathsf{H}(s_1)(G(s_2))$.
- By Lemma 76 we know $G(s_2) = \overrightarrow{G_\psi^{s_2}}(s_1)$ and thus $W_1.\mathsf{H}(s_1)(\overrightarrow{G_\psi^{s_2}}(s_1)) \neq \emptyset$.
- Since $W_1.\mathsf{H}(s_1)(\overrightarrow{G_\psi^{s_2}}(s_1)) \subseteq \bigcup_{s_2' \in \phi(s_1)} W_2.\mathsf{H}(s_2')(\overrightarrow{G_\psi^{s_2}}(s_1))$, there also exists $s_2' \in \phi(s_1)$.
- Since $s_2' \in (\phi \circ \psi)(s_2)$ and $\phi \circ \psi \sqsupseteq_{\mathrm{pub}} \mathrm{id}$, we have that $s_2' \sqsupseteq_{\mathrm{pub}} s_2$.
- Hence $(h_1, h_2) \in W_1.\mathsf{H}(s_1)(G(s_2'))$, which means $(h_1, h_2) \in W_1.\mathsf{H}(s_1)(\overleftarrow{G_\phi}(s_1))$ by Lemma 74.
- For h_1^{F} and h_2^{F} with $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$ we then get three cases from $(e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)(\tau)$:
  a) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^\omega \wedge\ h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^\omega$
     We are done.
  b) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, v_2$
     with $s_1' \sqsupseteq [s_1^0, s_1] \wedge (h_1', h_2') \in W_1.\mathsf{H}(s_1')(\overleftarrow{G_\phi}(s_1')) \wedge (v_1, v_2) \in \overline{\overleftarrow{G_\phi}(s_1')}(\tau)$
     - Since $W_1.\mathsf{H}(s_1')(\overleftarrow{G_\phi}(s_1')) \subseteq \bigcup_{s_2'' \in \phi(s_1')} W_2.\mathsf{H}(s_2'')(\overleftarrow{G_\phi}(s_1'))$, there exists $s_2'' \in \phi(s_1')$ such that $(h_1', h_2') \in W_2.\mathsf{H}(s_2'')(G(s_2''))$ by Lemma 74.
     - Also by Lemma 74 we have $(v_1, v_2) \in \overline{G(s_2'')}(\tau)$.
     - It remains to show $s_2'' \sqsupseteq [s_2^0, s_2]$.

- From $s_2'' \in \phi(s_1')$ and $s_2' \in \phi(s_1)$ we get $s_2'' \sqsupseteq s_2' \sqsupseteq s_2$.
- From $s_1^0 \in |\psi(s_2^0)|$ we know there is $s_2'^0 \in \phi(s_1^0)$.
- From $s_2'' \in \phi(s_1')$ and $s_2'^0 \in \phi(s_1^0)$ we get $s_2'' \sqsupseteq_{\text{pub}} s_2'^0$.
- Since $s_2'^0 \in (\phi \circ \psi)(s_2^0)$ we also get $s_2'^0 \sqsupseteq_{\text{pub}} s_2^0$ and thus $s_2'' \sqsupseteq_{\text{pub}} s_2^0$.

c) $h_1 \uplus h_1^{\text{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\text{F}}, K_1[e_1'] \wedge h_2 \uplus h_2^{\text{F}}, e_2 \hookrightarrow^n h_2' \uplus h_2^{\text{F}}, K_2[e_2']$
with $s_1' \sqsupseteq s_1 \wedge (h_1', h_2') \in W_1.\mathsf{H}(s_1')(\overleftarrow{G_\phi}(s_1')) \wedge (e_1', e_2') \in \mathbf{S}(\overleftarrow{G_\phi}(s_1'), \overleftarrow{G_\phi}(s_1'))(\tau')$ and
$\forall s_1'' \sqsupseteq_{\text{pub}} s_1'.\ \forall G' \supseteq \overleftarrow{G_\phi}.\ (K_1, K_2) \in \mathbf{K}_{W_1}(G')(s_1^0, s_1'')(\tau', \tau)$

- Since $W_1.\mathsf{H}(s_1')(\overleftarrow{G_\phi}(s_1')) \subseteq \bigcup_{s_2'' \in \phi(s_1')} W_2.\mathsf{H}(s_2'')(\overleftarrow{G_\phi}(s_1'))$, there exists $s_2'' \in \phi(s_1')$ such that $(h_1', h_2') \in W_2.\mathsf{H}(s_2'')(G(s_2''))$ by Lemma 74.
- Also by Lemma 74 we have $(e_1', e_2') \in \mathbf{S}(G(s_2''), G(s_2''))(\tau')$.
- From $s_2'' \in \phi(s_1')$ and $s_2' \in \phi(s_1)$ we get $s_2'' \sqsupseteq s_2' \sqsupseteq s_2$.
- It remains to show: $\forall s_2''' \sqsupseteq_{\text{pub}} s_2''.\ \forall G' \supseteq G.\ (K_1, K_2) \in \mathbf{K}'_{W_2}(G')(s_2^0, s_2''')(\tau', \tau)$
- So suppose $s_2''' \sqsupseteq_{\text{pub}} s_2''$ and $G' \supseteq G$.
- By definition of $\mathbf{K}'_{W_2}$ it suffices to show $(K_1, K_2) \in \mathbf{K}_{W_1}(G'_\phi)(s_1^0, s_1''')(\tau', \tau)$ for any $s_1''' \in |\psi(s_2''')|$.
- Since $(h_1', h_2') \in W_2.\mathsf{H}(s_2'')(G(s_2'')) \subseteq \bigcup_{s_1'' \in \psi(s_2'')} W_1.\mathsf{H}(s_1'')(G(s_2''))$, there exists $s_1'' \in \psi(s_2'')$.
- First, note that $\overleftarrow{G'_\phi} \supseteq \overleftarrow{G_\phi}$.
- Second, from $s_1''' \in |\psi(s_2''')|$ and $s_2''' \sqsupseteq_{\text{pub}} s_2''$ and $s_1'' \in \psi(s_2'')$ we get $s_1''' \sqsupseteq_{\text{pub}} s_1''$, which in turn yields $s_1''' \sqsupseteq_{\text{pub}} s_1'$ because $s_1'' \in (\psi \circ \phi)(s_1')$.
- The claim then follows from $\forall s_1'' \sqsupseteq_{\text{pub}} s_1'.\ \forall G' \supseteq \overleftarrow{G_\phi}.\ (K_1, K_2) \in \mathbf{K}_{W_1}(G')(s_1^0, s_1'')(\tau', \tau)$.

Part (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_{W_2}(G)(s_2^0, s_2)(\tau', \tau)$, *i.e.,* $(K_1, K_2) \in \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{K}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)(\tau', \tau)$ for some $s_1^0 \in |\psi(s_2^0)|$.
- Further suppose $(v_1, v_2) \in \overline{G(s_2)}(\tau')$.
- By definition of $\mathbf{E}'_{W_2}$ it suffices to show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)(\tau)$ for any $s_1 \in |\psi(s_2)|$.
- Pick $s_2' \in \phi(s_1)$, so $s_2' \in (\phi \circ \psi)(s_2)$ and thus $s_2' \sqsupseteq_{\text{pub}} s_2$.
- Hence $(v_1, v_2) \in \overline{G(s_2)}(\tau') \subseteq \overline{G(s_2')}(\tau') = \overleftarrow{G_\phi}(s_1)(\tau')$ by Lemma 74.
- The claim then follows from $(K_1, K_2) \in \mathbf{K}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)(\tau', \tau)$.

■

Corollary 83. If $\phi : W_1 \cong W_2 : \psi$ and $G \in \text{GK}(W_2)$, then:

$$\forall s_2.\ (\forall s_1 \in |\psi(s_2)|.\ (\tau, e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1, s_1)) \implies (\tau, e_1, e_2) \in \mathbf{E}_{W_2}(G)(s_2, s_2)$$

Proof:

- Suppose $\forall s_1 \in |\psi(s_2)|.\ (\tau, e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1, s_1)$.
- We need to show $(\tau, e_1, e_2) \in \mathbf{E}_{W_2}(G)(s_2, s_2)$.
- Now suppose $W_2.\mathsf{H}(s_2)(G(s_2)) \neq \emptyset$ (otherwise there is nothing to show).
- From $W_2.\mathsf{H}(s_2)(G(s_2)) \subseteq \bigcup_{s_1 \in \psi(s_2)} W_1.\mathsf{H}(s_1)(G(s_2))$ we get $s_1^0 \in \psi(s_2)$ with $W_1.\mathsf{H}(s_1^0)(G(s_2)) \neq \emptyset$.
- By Lemma 76 we know $G(s_2) = \overrightarrow{G_\psi^{s_2}}(s_1^0)$ and thus $W_1.\mathsf{H}(s_1^0)(\overrightarrow{G_\psi^{s_2}}(s_1^0)) \neq \emptyset$.
- Since also $W_1.\mathsf{H}(s_1^0)(\overrightarrow{G_\psi^{s_2}}(s_1^0)) \subseteq \bigcup_{s_2' \in \phi(s_1^0)} W_2.\mathsf{H}(s_2')(\overrightarrow{G_\psi^{s_2}}(s_1^0))$, we have $\phi(s_1^0) \neq \emptyset$ and thus $s_1^0 \in |\psi(s_2)|$.
- By Lemma 82, it suffices to show $(\tau, e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1^0, s_1)$ for any $s_1 \in |\psi(s_2)|$.
- Since $s_1, s_1^0 \in \psi(s_2)$ and thus $s_1 \sqsupseteq_{\text{pub}} s_1^0$, this follows from the assumption by Lemma 18.

■

Theorem 84 (Weak isomorphisms preserve equivalence)**.** If $\phi : W_1 \cong W_2 : \psi$, then: $\forall \Delta, \Gamma, \tau, e_1, e_2$.

$$\Delta; \Gamma \vdash e_1 \sim_{W_1} e_2 : \tau \iff \Delta; \Gamma \vdash e_1 \sim_{W_2} e_2 : \tau$$

Proof: By symmetry, it is enough to show $\Delta; \Gamma \vdash e_1 \sim_{W_1} e_2 : \tau \implies \Delta; \Gamma \vdash e_1 \sim_{W_2} e_2 : \tau$. From the premise we know:

1) $\mathit{inhabited}(W_1)$
2) $\mathit{consistent}(W_1)$
3) $\forall G \in \text{GK}(W_1).\forall s_1.\forall \delta \in \text{TyEnv}(\Delta).\forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_1)).\ (\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_1}(G)(s_1, s_1)(\delta\tau)$

a) We prove $\mathit{inhabited}(W_2)$.

- Suppose $G \in \mathrm{GK}(W_2)$.
- From (1) we know there is s_1 such that $(\emptyset, \emptyset) \in W_1.\mathsf{H}(s_1)(\overleftarrow{G_\phi}(s_1))$.
- From $W_1.\mathsf{H}(s_1)(\overleftarrow{G_\phi}(s_1)) \subseteq \bigcup_{s_2 \in \phi(s_1)} W_2.\mathsf{H}(s_2)(\overleftarrow{G_\phi}(s_1))$ we get $s_2 \in \phi(s_1)$ with $(\emptyset, \emptyset) \in W_2.\mathsf{H}(s_2)(\overleftarrow{G_\phi}(s_1))$.
- By Lemma 74 we have $(\emptyset, \emptyset) \in W_2.\mathsf{H}(s_2)(G(s_2))$.

b) We prove $\mathit{consistent}(W_2)$.
- Let $G \in \mathrm{GK}(W_2)$ and $(e_1', e_2') \in \mathbf{S}(W_2.\mathsf{L}(s_2)(G(s_2)), G(s_2))(\tau')$.
- We need to show $(\mathit{beta}(e_1'), \mathit{beta}(e_2')) \in \mathbf{E}_{W_2}(G)(s_2, s_2)(\tau')$.
- By Corollary 83, it suffices to show $(\mathit{beta}(e_1'), \mathit{beta}(e_2')) \in \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1, s_1)(\tau')$ for any $s_1 \in |\psi(s_2)|$.
- Since $\phi(s_1) \neq \emptyset$, we have $s_2' \in \phi(s_1)$ and thus $\overleftarrow{G_\phi}(s_1) = G(s_2')$ by Lemma 74.
- Since $s_2' \in (\phi \circ \psi)(s_2)$, we have $s_2' \sqsupseteq_{\mathrm{pub}} s_2$ and thus $\overleftarrow{G_\phi}(s_1) \supseteq G(s_2)$.
- Thus we have $\mathbf{S}(W_2.\mathsf{L}(s_2)(G(s_2)), G(s_2)) \subseteq \mathbf{S}(W_2.\mathsf{L}(s_2)(\overleftarrow{G_\phi}(s_1)), \overleftarrow{G_\phi}(s_1)) \subseteq \mathbf{S}(W_1.\mathsf{L}(s_1)(\overleftarrow{G_\phi}(s_1)), \overleftarrow{G_\phi}(s_1))$.
- Consequently, the claim follows from (2).

c) We prove $\forall G \in \mathrm{GK}(W_2). \forall s_2. \forall \delta \in \mathrm{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_2)).\ (\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_2}(G)(s_2, s_2)(\delta\tau)$.
- Let $G \in \mathrm{GK}(W_2)$, $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_2))$.
- By Corollary 83, it suffices to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G_\phi})(s_1, s_1)(\delta\tau)$ for any $s_1 \in |\psi(s_2)|$.
- Since $\phi(s_1) \neq \emptyset$, we have $s_2' \in \phi(s_1)$ and thus $\overleftarrow{G_\phi}(s_1) = G(s_2')$ by Lemma 74.
- Since $s_2' \in (\phi \circ \psi)(s_2)$, we have $s_2' \sqsupseteq_{\mathrm{pub}} s_2$ and thus $\overleftarrow{G_\phi}(s_1) \supseteq G(s_2)$.
- Thus we have $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_2)) \subseteq \mathrm{Env}(\delta\Gamma, \overleftarrow{G_\phi}(s_1))$.
- Consequently, the claim follows from (3).

■

5) Examples.

Erased World.. For $W \in \mathrm{World}$, we define its erasure $|W| \in \mathrm{World}$ as follows.

$$\begin{array}{lcl} |W|.\mathsf{N} & := & W.\mathsf{N} \\ |W|.\mathsf{S} & := & \{\, s \in W.\mathsf{S} \mid \exists G \in \mathrm{GK}(W).\ W.\mathsf{H}(s)(G(s)) \neq \emptyset \,\} \\ |W|.\sqsupseteq & := & W.\sqsupseteq \\ |W|.\sqsupseteq_{\mathrm{pub}} & := & W.\sqsupseteq_{\mathrm{pub}} \\ |W|.\mathsf{L} & := & W.\mathsf{L} \\ |W|.\mathsf{H} & := & W.\mathsf{H} \end{array}$$

Note that erasing preserves inhabitance and consistency.

Theorem 85. $\exists \phi, \psi.\ \phi : W \cong |W| : \psi$

Proof: We define ϕ, ψ as follows:

$$\begin{array}{lcl} \phi(s) & := & \{\, s \,\} \cap |W|.\mathsf{S} \\ \psi(s) & := & \{\, s \,\} \end{array}$$

It is easy to check all the properties of a weak isomorphism. ■

Flattened World.. For $W \in \mathrm{World}$, we define its flattening $\mathrm{Flat}(W) \in \mathrm{World}$ as follows.

$$\begin{array}{lcl} \mathrm{Flat}(W).\mathsf{S} & := & W.\mathsf{S} \times \mathrm{Heap} \times \mathrm{Heap} \\ \mathrm{Flat}(W).\sqsupseteq & := & \{\, ((s', h_1', h_2'), (s, h_1, h_2)) \mid s' \sqsupseteq s \,\} \\ \mathrm{Flat}(W).\sqsupseteq_{\mathrm{pub}} & := & \{\, ((s', h_1', h_2'), (s, h_1, h_2)) \mid s' \sqsupseteq_{\mathrm{pub}} s \,\} \\ \mathrm{Flat}(W).\mathsf{L}(s, h_1, h_2) & := & W.\mathsf{L}(s) \\ \mathrm{Flat}(W).\mathsf{H}(s, h_1, h_2)(R) & := & \{\, (h_1, h_2) \,\} \cap W.\mathsf{H}(s)(R) \end{array}$$

Note that flattening preserves inhabitance and consistency.

Theorem 86. $\exists \phi, \psi.\ \phi : W \cong \mathrm{Flat}(W) : \psi$

Proof: We define ϕ, ψ as follows:

$$\begin{array}{lcl} \phi(s) & := & \{\, (s, h_1, h_2) \mid h_1, h_2 \in \mathrm{Heap} \,\} \\ \psi(s, h_1, h_2) & := & \{\, s \,\} \end{array}$$

It easy to check all the properties of a weak isomorphism. ■

F. Transitivity

Suppose $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$ and $\Delta; \Gamma \vdash e_2 \sim e_3 : \sigma$. The goal of this section is to prove $\Delta; \Gamma \vdash e_1 \sim e_3 : \sigma$. To this end, suppose we are given $\mathcal{N}$. We may assume $\mathcal{N} = \mathcal{N}_1 \uplus \mathcal{N}_2 \uplus \mathcal{N}_\exists$ with $\mathrm{names}(\Gamma, \sigma) \cap \mathcal{N}_\exists = \emptyset$. Then there are W_1, w_1, W_2, w_2 such that:

- $W_i = w_i{\uparrow}$
- $\mathit{stable}(w_i)$
- $w_i.\mathsf{N} \subseteq \mathcal{N}_i$
- $\Gamma \vdash e_1 \sim_{W_1} e_2 : \sigma$ and $\Gamma \vdash e_2 \sim_{W_2} e_3 : \sigma$

1) Constructing a Full World That Relates e_1 and e_3.

Type Decomposition.

Definition 20. We mutually inductively define $\sigma_1 \approx \sigma_2$ and $\sigma_1 \sim \sigma_2$ for $\sigma_1, \sigma_2 \in \mathrm{Type}$ as follows:

$$
\begin{array}{lll}
\mathbf{n} \approx \mathbf{n} & \text{if} & \mathbf{n} \notin \mathcal{N}_\exists \\
\alpha \approx \alpha & & \\
\tau_{\text{base}} \approx \tau_{\text{base}} & & \\
\sigma_1 \times \sigma_1' \approx \sigma_2 \times \sigma_2' & \text{if} & \sigma_1 \sim \sigma_2 \wedge \sigma_1' \sim \sigma_2' \\
\sigma_1 + \sigma_1' \approx \sigma_2 + \sigma_2' & \text{if} & \sigma_1 \sim \sigma_2 \wedge \sigma_1' \sim \sigma_2' \\
\sigma_1 \to \sigma_1' \approx \sigma_2 \to \sigma_2' & \text{if} & \sigma_1 \sim \sigma_2 \wedge \sigma_1' \sim \sigma_2' \\
\mu\alpha.\, \sigma_1 \approx \mu\alpha.\, \sigma_2 & \text{if} & \sigma_1 \sim \sigma_2 \\
\forall\alpha.\, \sigma_1 \approx \forall\alpha.\, \sigma_2 & \text{if} & \sigma_1 \sim \sigma_2 \\
\exists\alpha.\, \sigma_1 \approx \exists\alpha.\, \sigma_2 & \text{if} & \sigma_1 \sim \sigma_2 \\
\mathsf{ref}\, \sigma_1 \approx \mathsf{ref}\, \sigma_2 & \text{if} & \sigma_1 \sim \sigma_2
\end{array}
$$

with

$$
\sigma_1 \sim \sigma_2 \quad \text{if} \quad \sigma_1, \sigma_2 \in \mathrm{CType} \vee \sigma_1 \approx \sigma_2
$$

Definition 21. Since CType and $\mathcal{N}_\exists$ are countably infinite sets, there exists a bijective function

$$
\mathbf{A} \in \{\, (\tau_1, \tau_2) \in \mathrm{CType} \times \mathrm{CType} \mid \tau_1 \not\approx \tau_2 \,\} \to \mathcal{N}_\exists\ .
$$

Definition 22. Given $\sigma \in \mathrm{Type}$, we define $\sigma_{(1)}, \sigma_{(2)} \in \mathrm{Type}$ recursively as follows:

$$
\begin{array}{lcl}
\mathbf{n}_{(i)} & := & \begin{cases} \tau_i & \text{if } \mathbf{n} = \mathbf{A}(\tau_1, \tau_2) \text{ for some } \tau_1, \tau_2 \\ \mathbf{n} & \text{otherwise, } \textit{i.e.,}\ \mathbf{n} \notin \mathcal{N}_\exists \end{cases} \\
\alpha_{(i)} & := & \alpha \\
\tau_{\text{base}(i)} & := & \tau_{\text{base}} \\
(\sigma \times \sigma')_{(i)} & := & \sigma_{(i)} \times \sigma'_{(i)} \\
(\sigma + \sigma')_{(i)} & := & \sigma_{(i)} + \sigma'_{(i)} \\
(\sigma \to \sigma')_{(i)} & := & \sigma_{(i)} \to \sigma'_{(i)} \\
(\forall\alpha.\, \sigma)_{(i)} & := & \forall\alpha.\, \sigma_{(i)} \\
(\exists\alpha.\, \sigma)_{(i)} & := & \exists\alpha.\, \sigma_{(i)} \\
(\mu\alpha.\, \sigma)_{(i)} & := & \mu\alpha.\, \sigma_{(i)} \\
(\mathsf{ref}\, \sigma)_{(i)} & := & \mathsf{ref}\, \sigma_{(i)}
\end{array}
$$

Lemma 87. For $\sigma \in \mathrm{Type}$,

$$
\sigma_{(1)} \in \mathrm{CType} \wedge \sigma_{(2)} \in \mathrm{CType} \iff \sigma \in \mathrm{CType}
$$

Proof: By straightforward induction on σ. ∎

Lemma 88. For $\sigma \in \mathrm{Type}$,

$$
\sigma_{(1)} \sim \sigma_{(2)}
$$

Proof: By straightforward induction on σ. ∎

Lemma 89. For $\sigma \in \mathrm{Type}$,

$$
\sigma_{(1)} \approx \sigma_{(2)} \iff \sigma \notin \mathcal{N}_\exists
$$

Proof: Straightfoward to show by case analysis on σ using Lemma 88. ∎

Lemma 90 (Injectivity of Type Decomposition)**.** For $\sigma_1, \sigma_2 \in \mathrm{Type}$,

$$\sigma_{1(1)} = \sigma_{2(1)} \wedge \sigma_{1(2)} = \sigma_{2(2)} \implies \sigma_1 = \sigma_2$$

Proof: Easy to show by induction on σ_1. We just show the following representative cases.

- when $\sigma_1 = \mathbf{A}(\tau_1, \tau_2) \in \mathcal{N}_\exists$:
  - We have $\sigma_2 \in \mathcal{N}_\exists$ by Lemma 89.
  - Thus we have $\sigma_1 = \mathbf{A}(\tau_1, \tau_2) = \sigma_2$ since $\mathbf{A}$ is bijective.
- when $\sigma_1 = \mathbf{n} \notin \mathcal{N}_\exists$:
  - By case analysis on σ_2, we have $\sigma_2 \in \mathrm{TyNam}$.
  - By Lemma 89, we have $\sigma_2 \notin \mathcal{N}_\exists$.
  - Thus we have $\sigma_2 = \mathbf{n} = \sigma_1$.
- when $\sigma_1 = \sigma_1' \to \sigma_1''$:
  - By Lemmas 88 and 89, we have $\sigma_2 \notin \mathcal{N}_\exists$.
  - By case analysis on σ_2, we have $\sigma_2 = \sigma_2' \to \sigma_2''$ for some $\sigma_2', \sigma_2'' \in \mathrm{Type}$.
  - Then we have $\sigma'_{1(i)} = \sigma'_{2(i)}$ and $\sigma''_{1(i)} = \sigma''_{2(i)}$ for $i = 1, 2$.
  - Thus by induction hypothesis we have $\sigma_1' = \sigma_2' \wedge \sigma_1'' = \sigma_2''$, which yields $\sigma_1 = \sigma_2$.
- when $\sigma_1 = \exists\alpha.\, \sigma_1'$:
  - By Lemmas 88 and 89, we have $\sigma_2 \notin \mathcal{N}_\exists$.
  - By case analysis on σ_2, we have $\sigma_2 = \exists\alpha.\, \sigma_2'$ for some $\sigma_2' \in \mathrm{Type}$.
  - Then we have $\sigma'_{1(i)} = \sigma'_{2(i)}$ for $i = 1, 2$.
  - Thus by induction hypothesis we have $\sigma_1' = \sigma_2'$, which yields $\sigma_1 = \sigma_2$.

■

Lemma 91. For $\sigma_1, \sigma_2 \in \mathrm{Type}$,

$$\sigma_1 \sim \sigma_2 \implies \exists\sigma.\ \sigma_{(1)} = \sigma_1 \wedge \sigma_{(2)} = \sigma_2$$

Proof: Easy to show by induction on σ_1. We just show the following representative cases.
If $\sigma_1 \not\approx \sigma_2$, then $\sigma_1, \sigma_2 \in \mathrm{CType}$ and we are done for $\sigma = \mathbf{A}(\sigma_1, \sigma_2)$. Otherwise we proceed as follows:

- when $\sigma_1 = \mathbf{n} \in \mathrm{TyNam}$:
  - From $\sigma_1 \approx \sigma_2$, we have $\sigma_2 = \mathbf{n} \notin \mathcal{N}_\exists$.
  - Thus we are done by letting $\sigma = \mathbf{n}$.
- when $\sigma_1 = \sigma_1' \to \sigma_1''$:
  - From $\sigma_1 \approx \sigma_2$, we have $\sigma_2 = \sigma_2' \to \sigma_2''$ such that $\sigma_1' \sim \sigma_2'$ and $\sigma_1'' \sim \sigma_2''$.
  - By induction hypothesis, we have σ' and σ'' such that $\sigma'_{(i)} = \sigma_i'$ and $\sigma''_{(i)} = \sigma_i''$ for $i = 1, 2$.
  - Thus we are done by letting $\sigma = \sigma' \to \sigma''$.
- when $\sigma_1 = \exists\alpha.\, \sigma_1'$:
  - From $\sigma_1 \approx \sigma_2$, we have $\sigma_2 = \exists\alpha.\, \sigma_2'$ such that $\sigma_1' \sim \sigma_2'$.
  - By induction hypothesis, we have σ' such that $\sigma'_{(i)} = \sigma_i'$ for $i = 1, 2$.
  - Thus we are done by letting $\sigma = \exists\alpha.\, \sigma'$.

■

Corollary 92 (Surjectivity of Type Decomposition)**.** For $\tau_1, \tau_2 \in \mathrm{CType}$, we have $\tau \in \mathrm{CType}$ such that $\tau_{(1)} = \tau_1 \wedge \tau_{(2)} = \tau_2$.

Proof: Since $\tau_1 \sim \tau_2$ by definition, we have $\sigma \in \mathrm{Type}$ such that $\sigma_{(1)} = \tau_1 \wedge \sigma_{(2)} = \tau_2$ by Lemma 91. Hence $\sigma \in \mathrm{CType}$ by Lemma 87. ■

World Construction.

Definition 23. Since CType and CVal are countable sets, there exists an injective function

$$\mathbf{I} \in \mathrm{CType} \times \mathrm{CVal} \times \mathrm{CVal} \to \mathbb{N}\ .$$

Definition 24. Given $R \in \mathrm{VRelF}$, we define $R_{\{1\}}, R_{\{2\}} \in \mathrm{VRelF}$ as follows:

$$\begin{aligned} R_{\{1\}} &:= \{\, (\tau_{(1)}, v_1, \mathbf{I}(\tau, v_1, v_3)) \mid \tau \in \mathrm{CTypeF} \setminus (\mathcal{N} \cup \{\mathsf{ref}\ \tau' \in \mathrm{CType}\}) \wedge (\tau, v_1, v_3) \in R \,\} \\ R_{\{2\}} &:= \{\, (\tau_{(2)}, \mathbf{I}(\tau, v_1, v_3), v_3) \mid \tau \in \mathrm{CTypeF} \setminus (\mathcal{N} \cup \{\mathsf{ref}\ \tau' \in \mathrm{CType}\}) \wedge (\tau, v_1, v_3) \in R \,\} \end{aligned}$$

Definition 25. For $X_1, X_2 \in \mathrm{VRel}$, we define $X_1 \bullet X_2 \in \mathrm{VRel}$ as follows:

$$(X_1 \bullet X_2)(\tau) \quad := \quad X_1(\tau_{(1)}) \circ X_2(\tau_{(2)})$$

Note that this is well-defined due to Lemma 87.

Recall that for a monotone function $F \in \mathrm{VRelF} \to \mathrm{VRelF}$ and $R \in \mathrm{VRelF}$, we write $[F]^*_R$ for the least fixpoint of the monotone function $F(-) \cup R$.

Definition 26. We define $W \in \mathrm{World}$ as follows:

$$\begin{array}{lll}
W.\mathsf{N} & := & \mathcal{N} \\
W.\mathsf{S} & := & W_1.\mathsf{S} \times W_2.\mathsf{S} \\
W.\sqsubseteq & := & \{\, (p, p') \mid p.1 \sqsubseteq p'.1 \wedge p.2 \sqsubseteq p'.2 \,\} \\
W.\sqsubseteq_{\mathrm{pub}} & := & \{\, (p, p') \mid p.1 \sqsubseteq_{\mathrm{pub}} p'.1 \wedge p.2 \sqsubseteq_{\mathrm{pub}} p'.2 \,\} \\
W.\mathsf{L}(s_1, s_2)(R) & := & \{\, (\tau, v_1, v_3) \in \overline{W_1.\mathsf{L}(s_1)([W_1.\mathsf{L}(s_1)]^*_{R_{\{1\}}})} \bullet \overline{W_2.\mathsf{L}(s_2)([W_2.\mathsf{L}(s_2)]^*_{R_{\{2\}}})} \mid \tau \in \mathrm{CTypeF} \setminus \mathcal{N}_\exists \,\} \uplus \\
 & & \{\, (\mathbf{n}, v_1, v_3) \in \overline{[W_1.\mathsf{L}(s_1)]^*_{R_{\{1\}}}} \bullet \overline{[W_2.\mathsf{L}(s_2)]^*_{R_{\{2\}}}} \mid \mathbf{n} \in \mathcal{N}_\exists \,\} \\
W.\mathsf{H}(s_1, s_2)(R) & := & W_1.\mathsf{H}(s_1)([W_1.\mathsf{L}(s_1)]^*_{R_{\{1\}}}) \circ W_2.\mathsf{H}(s_2)([W_2.\mathsf{L}(s_2)]^*_{R_{\{2\}}})
\end{array}$$

It is easy to check that W is well-defined.

Transitivity of Value Equivalence.

Definition 27. Given $G \in \mathrm{GK}(W)$ and $(s_1, s_2) \in W.\mathsf{S} = W_1.\mathsf{S} \times W_2.\mathsf{S}$, we define $G^{s_2}_{(1)} \in W_1.\mathsf{S} \to \mathrm{VRelF}$ and $G^{s_1}_{(2)} \in W_2.\mathsf{S} \to \mathrm{VRelF}$ as follows:

$$\begin{array}{lll}
G^{s_2}_{(1)}(s) & := & [W_1.\mathsf{L}(s)]^*_{G(s,s_2)_{\{1\}}} \\
G^{s_1}_{(2)}(s) & := & [W_2.\mathsf{L}(s)]^*_{G(s_1,s)_{\{2\}}}
\end{array}$$

Lemma 93.

1) $\forall G \in \mathrm{GK}(W). \forall s_2 \in W_2.\mathsf{S}.\ G^{s_2}_{(1)} \in \mathrm{GK}(W_1)$
2) $\forall G \in \mathrm{GK}(W). \forall s_1 \in W_1.\mathsf{S}.\ G^{s_1}_{(2)} \in \mathrm{GK}(W_2)$

Proof: We only show part (1) since part (2) is analogous. Monotonicity of $G^{s_2}_{(1)}$ is easy to show by induction, using that G and $(-)_{\{1\}}$ and $W_1.\mathsf{L}$ are monotone.

It remains to show $G^{s_2}_{(1)}(s_1) \geq^{W_1.\mathsf{N}}_{\mathrm{ref}} W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))$ for any s_1. For $\tau \in \mathrm{CTypeF}$ we know:

$$\begin{array}{lll}
 & G^{s_2}_{(1)}(s_1)(\tau) & \\
= & [W_1.\mathsf{L}(s)]^*_{G(s_1,s_2)_{\{1\}}}(\tau) & \\
= & W_1.\mathsf{L}(s_1)([W_1.\mathsf{L}]^*_{G(s_1,s_2)_{\{1\}}})(\tau) \cup G(s_1, s_2)_{\{1\}}(\tau) & \\
= & W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau) \cup G(s_1, s_2)_{\{1\}}(\tau) &
\end{array}$$

The claim follows from this and the fact that by construction $G(s_1, s_2)_{\{1\}}(\mathbf{n}) = \emptyset = G(s_1, s_2)_{\{1\}}(\mathsf{ref}\,\tau')$ for any $\mathbf{n} \in W_1.\mathsf{N} \subseteq \mathcal{N}$ and τ'. ∎

Lemma 94. $\forall R \in \mathrm{VRelF}.\ \forall \tau \in \mathrm{CTypeF} \setminus (\mathcal{N} \cup \{\mathsf{ref}\,\tau' \in \mathrm{CType}\})$.

$$\begin{array}{l}
\forall s_1, R_1.\ W_1.\mathsf{L}(s_1)(R_1)(\tau_{(1)}) \circ R_{\{2\}}(\tau_{(2)}) = \emptyset \wedge \\
\forall s_2, R_2.\ R_{\{1\}}(\tau_{(1)}) \circ W_2.\mathsf{L}(s_2)(R_2)(\tau_{(2)}) = \emptyset
\end{array}$$

Proof: We only show the former part since the other part holds analogously.

- When $\tau \in \mathrm{TyNam} \setminus \mathcal{N}$: holds vacuously since $W_i.\mathsf{L}(s_i)(R_i)(\tau_{(i)}) = \emptyset$.
- When $\tau = \tau' \to \tau''$: holds vacuously since $v_2 \in \mathrm{FunVal}$ for any $(v_1, v_2) \in W_1.\mathsf{L}(s_1)(R_1)(\tau_{(1)})$ but $\mathbf{I}(\tau, v_1, v_3) \notin \mathrm{FunVal}$ for any τ, v_1, v_3.
- When $\tau = \forall \alpha.\, \sigma$: holds vacuously since $v_2 \in \mathrm{GenVal}$ for any $(v_1, v_2) \in W_1.\mathsf{L}(s_1)(R_1)(\tau_{(1)})$ but $\mathbf{I}(\tau, v_1, v_3) \notin \mathrm{GenVal}$ for any τ, v_1, v_3.

∎

Lemma 95. $\forall R \in \mathrm{VRelF}.\ \forall \tau \in \mathrm{CTypeF} \setminus (\mathcal{N} \cup \{\mathsf{ref}\,\tau' \in \mathrm{CType}\})$.

$$R_{\{1\}}(\tau_{(1)}) \circ R_{\{2\}}(\tau_{(2)}) = R(\tau)$$

Proof: By construction of $R_{\{1\}}$ and $R_{\{2\}}$, the injectivity of $\mathbf{I}$, and Lemma 90. ∎

Lemma 96.

$$\forall \tau \in \mathrm{CTypeF}.\ \forall G \in \mathrm{GK}(W).\ \forall (s_1, s_2) \in W.\mathsf{S}.\ \left(\overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)}\right)(\tau) = G(s_1, s_2)(\tau)$$

Proof: By case analysis on τ.

- when $\tau = \mathbf{n} \in \mathcal{N}_\exists$:

$$\begin{array}{lll} & \overline{G^{s_2}_{(1)}(s_1)}(\mathbf{n}_{(1)}) \circ \overline{G^{s_1}_{(2)}(s_2)}(\mathbf{n}_{(2)}) & \\ = & W.\mathsf{L}(s_1, s_2)(G(s_1, s_2))(\mathbf{n}) & \text{(construction of } W.\mathsf{L}) \\ = & G(s_1, s_2)(\mathbf{n}) & (G \in \mathrm{GK}(W)) \end{array}$$

- when $\tau = \mathsf{ref}\,\tau'$ or $\tau \in \mathcal{N}_1 \uplus \mathcal{N}_2$:

$$\begin{array}{lll} & \overline{G^{s_2}_{(1)}(s_1)}(\tau_{(1)}) \circ \overline{G^{s_1}_{(2)}(s_2)}(\tau_{(2)}) & \\ = & G^{s_2}_{(1)}(s_1)(\tau_{(1)}) \circ G^{s_1}_{(2)}(s_2)(\tau_{(2)}) & \\ = & (W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \cup G(s_1, s_2)_{\{1\}}(\tau_{(1)})) \circ (W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)}) \cup G(s_1, s_2)_{\{2\}}(\tau_{(2)})) & \\ & & \text{(fixpoint)} \\ = & W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \circ W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)}) & \text{(construction of } (-)_{\{i\}}) \\ = & W.\mathsf{L}(s_1, s_2)(G(s_1, s_2))(\tau) & \text{(construction of } W.\mathsf{L}(s_1, s_2)) \\ = & G(s_1, s_2)(\tau) & (G \in \mathrm{GK}(W)) \end{array}$$

- when $\tau \in \mathrm{CTypeF} \setminus (\mathcal{N} \cup \{\mathsf{ref}\,\tau' \in \mathrm{CType}\})$:

$$\begin{array}{lll} & \overline{G^{s_2}_{(1)}(s_1)}(\tau_{(1)}) \circ \overline{G^{s_1}_{(2)}(s_2)}(\tau_{(2)}) & \\ = & G^{s_2}_{(1)}(s_1)(\tau_{(1)}) \circ G^{s_1}_{(2)}(s_2)(\tau_{(2)}) & \\ = & (W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \cup G(s_1, s_2)_{\{1\}}(\tau_{(1)})) \circ (W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)}) \cup G(s_1, s_2)_{\{2\}}(\tau_{(2)})) & \\ & & \text{(fixpoint)} \\ = & (W_1.\mathsf{L}(s_1)(G^{s_2}_{(1)}(s_1))(\tau_{(1)}) \circ W_2.\mathsf{L}(s_2)(G^{s_1}_{(2)}(s_2))(\tau_{(2)})) \cup (G(s_1, s_2)_{\{1\}}(\tau_{(1)}) \circ G(s_1, s_2)_{\{2\}}(\tau_{(2)})) & \\ & & \text{(Lemma 94)} \\ = & W.\mathsf{L}(s_1, s_2)(G(s_1, s_2))(\tau) \cup (G(s_1, s_2)_{\{1\}}(\tau_{(1)}) \circ G(s_1, s_2)_{\{2\}}(\tau_{(2)})) & \text{(construction of } W.\mathsf{L}(s_1, s_2)) \\ = & W.\mathsf{L}(s_1, s_2)(G(s_1, s_2))(\tau) \cup G(s_1, s_2)(\tau) & \text{(Lemma 95)} \\ = & G(s_1, s_2)(\tau) & (G \in \mathrm{GK}(W)) \end{array}$$

■

Recall that $\overline{R}$ is the least fixpoint of the monotone function $F_R : \mathrm{VRel} \to \mathrm{VRel}$ given as follows:

$$\begin{array}{ll} F_R(X)(\tau_{\text{base}}) & := \mathrm{ID}_{\tau_{\text{base}}} \\ F_R(X)(\tau_1 \times \tau_2) & := \{\, ((v_1, v_1'), (v_2, v_2')) \mid (v_1, v_2) \in X(\tau_1) \wedge (v_1', v_2') \in X(\tau_2) \,\} \\ F_R(X)(\tau_1 + \tau_2) & := \{\, (\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \mid (v_1, v_2) \in X(\tau_1) \,\} \cup \{\, (\mathsf{inj}^2\, v_1, \mathsf{inj}^2\, v_2) \mid (v_1, v_2) \in X(\tau_2) \,\} \\ F_R(X)(\exists \alpha.\, \sigma) & := \{\, (\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \mid \exists \tau' \in \mathrm{CType}.\ (v_1, v_2) \in X(\sigma[\tau'/\alpha]) \,\} \\ F_R(X)(\mu \alpha.\, \sigma) & := \{\, (\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \mid (v_1, v_2) \in X(\sigma[\mu \alpha.\, \sigma/\alpha]) \,\} \\ F_R(X)(\tau_1 \to \tau_2) & := R(\tau_1 \to \tau_2) \\ F_R(X)(\forall \alpha.\, \sigma) & := R(\forall \alpha.\, \sigma) \\ F_R(X)(\mathbf{n}) & := R(\mathbf{n}) \\ F_R(X)(\mathsf{ref}\,\tau) & := R(\mathsf{ref}\,\tau) \end{array}$$

Lemma 97.

$$\forall \tau \in \mathrm{CType} \setminus \mathrm{CTypeF}.\ (F_{R_1}(X_1) \bullet F_{R_2}(X_2))(\tau) = F_R(X_1 \bullet X_2)(\tau)$$

Proof: Easy to check by case analysis of τ. We show the only interesting case, $\tau = \exists\alpha.\,\sigma$:

$$\begin{aligned}
& (v_1, v_3) \in (F_{R_1}(X_1) \bullet F_{R_2}(X_2))(\exists\alpha.\,\sigma) \\
\iff\ & \exists v_1', v_2', v_3'.\ v_1 = \mathsf{pack}\ v_1' \wedge v_3 = \mathsf{pack}\ v_3' \wedge (\mathsf{pack}\ v_1', \mathsf{pack}\ v_2') \in F_{R_1}(X_1)(\exists\alpha.\,\sigma_{(1)}) \wedge \\
& \qquad\qquad (\mathsf{pack}\ v_2', \mathsf{pack}\ v_3') \in F_{R_2}(X_2)(\exists\alpha.\,\sigma_{(2)}) \\
\iff\ & \exists v_1', v_2', v_3'.\ \exists \tau_1', \tau_2' \in \mathrm{CType}.\ v_1 = \mathsf{pack}\ v_1' \wedge v_3 = \mathsf{pack}\ v_3' \wedge (v_1', v_2') \in X_1(\sigma_{(1)}[\tau_1'/\alpha]) \wedge \\
& \qquad\qquad (v_2', v_3') \in X_2(\sigma_{(2)}[\tau_2'/\alpha]) \\
\iff\ & \exists v_1', v_2', v_3'.\ \exists \tau' \in \mathrm{CType}.\ v_1 = \mathsf{pack}\ v_1' \wedge v_3 = \mathsf{pack}\ v_3' \wedge (v_1', v_2') \in X_1(\sigma_{(1)}[\tau'_{(1)}/\alpha]) \wedge \\
& \qquad\qquad (v_2', v_3') \in X_2(\sigma_{(2)}[\tau'_{(2)}/\alpha]) \quad \text{(Corollary 92)} \\
\iff\ & \exists v_1', v_2', v_3'.\ \exists \tau' \in \mathrm{CType}.\ v_1 = \mathsf{pack}\ v_1' \wedge v_3 = \mathsf{pack}\ v_3' \wedge (v_1', v_2') \in X_1(\sigma[\tau'/\alpha]_{(1)}) \wedge \\
& \qquad\qquad (v_2', v_3') \in X_2(\sigma[\tau'/\alpha]_{(2)}) \\
\iff\ & \exists v_1', v_2', v_3'.\ \exists \tau' \in \mathrm{CType}.\ v_1 = \mathsf{pack}\ v_1' \wedge v_3 = \mathsf{pack}\ v_3' \wedge (v_1', v_3') \in (X_1 \bullet X_2)(\sigma[\tau'/\alpha]) \\
\iff\ & (v_1, v_3) \in F_R(X_1 \bullet X_2)(\exists\alpha.\,\sigma)
\end{aligned}$$

■

Lemma 98 (Generalized Fixed-Point Induction)**.** For a monotone function $F \in \mathrm{VRelF} \to \mathrm{VRelF}$ and $R \in \mathrm{VRelF}$,

$$F(R \cap [F]^*_\emptyset) \subseteq R \implies [F]^*_\emptyset \subseteq R$$

Proof: Suppose $F(R \cap [F]^*_\emptyset) \subseteq R$. By monotonicity of F, we have $F(R \cap [F]^*_\emptyset) \subseteq F([F]^*_\emptyset) = [F]^*_\emptyset$. Thus we have $F(R \cap [F]^*_\emptyset) \subseteq (R \cap [F]^*_\emptyset)$, *i.e.,* $R \cap [F]^*_\emptyset$ is a prefixpoint of F. Thus we have $[F]^*_\emptyset \subseteq (R \cap [F]^*_\emptyset) \subseteq R$. ■

Lemma 99 (Transitivity of Value Equivalence)**.**

$$\forall G \in \mathrm{GK}(W).\ \forall (s_1, s_2) \in W.\mathsf{S}.\ \overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)} = \overline{G(s_1, s_2)}$$

Proof: First part ($\subseteq$): It suffices to show $\overline{G^{s_2}_{(1)}(s_1)} \subseteq S$, where:

$$S = \{\, (\tau, v_1, v_2) \mid \forall \tau', v_3'.\ \tau = \tau'_{(1)} \wedge (\tau'_{(2)}, v_2, v_3') \in \overline{G^{s_1}_{(2)}(s_2)} \implies (\tau', v_1, v_3') \in \overline{G(s_1, s_2)} \,\}$$

We prove it using Lemma 98, *i.e.,* it suffices to show $F_{G^{s_2}_{(1)}(s_1)}(S') \subseteq S$ for $S' = S \cap \overline{G^{s_2}_{(1)}(s_1)}$, which is equivalent to show $F_{G^{s_2}_{(1)}(s_1)}(S') \bullet \overline{G^{s_1}_{(2)}(s_2)} \subseteq \overline{G(s_1, s_2)}$ by definition of S.

- $\tau \notin \mathrm{CTypeF}$:

$$\begin{aligned}
& (F_{G^{s_2}_{(1)}(s_1)}(S') \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau) \\
=\ & (F_{G^{s_2}_{(1)}(s_1)}(S') \bullet F_{G^{s_1}_{(2)}(s_2)}(\overline{G^{s_1}_{(2)}(s_2)}))(\tau) \\
=\ & F_{G(s_1,s_2)}(S' \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau) \qquad \text{(Lemma 97)} \\
\subseteq\ & F_{G(s_1,s_2)}(\overline{G(s_1, s_2)})(\tau) \\
=\ & \overline{G(s_1, s_2)}(\tau)
\end{aligned}$$

- $\tau \in \mathrm{CTypeF}$:

$$(F_{G^{s_2}_{(1)}(s_1)}(S') \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau) \subseteq (\overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau) = G(s_1, s_2)(\tau) = \overline{G(s_1, s_2)}(\tau) \qquad \text{(Lemma 96)}$$

Second part ($\supseteq$): By induction it suffices to show $F_{G(s_1,s_2)}(\overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)}) \subseteq \overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)}$.

- $\tau \notin \mathrm{CTypeF}$:

$$\begin{aligned}
& F_{G(s_1,s_2)}(\overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau) \\
=\ & (F_{G^{s_2}_{(1)}(s_1)}(\overline{G^{s_2}_{(1)}(s_1)}) \bullet F_{G^{s_1}_{(2)}(s_2)}(\overline{G^{s_1}_{(2)}(s_2)}))(\tau) \qquad \text{(Lemma 97)} \\
=\ & (\overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau)
\end{aligned}$$

- $\tau \in \mathrm{CTypeF}$:

$$\begin{aligned}
& F_{G(s_1,s_2)}(\overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau) \\
=\ & G(s_1, s_2)(\tau) \\
=\ & (\overline{G^{s_2}_{(1)}(s_1)} \bullet \overline{G^{s_1}_{(2)}(s_2)})(\tau) \qquad \text{(Lemma 96)}
\end{aligned}$$

■

Transitivity of Term Equivalence.

Lemma 100 (Transitivity of Term Equivalence)**.** If $G \in \mathrm{GK}(W)$ and $(s_1^0, s_2^0), (s_1, s_2) \in W.\mathsf{S}$, then:

1) $\mathbf{E}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)(\tau_{(1)}) \circ \mathbf{E}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)(\tau_{(2)}) \subseteq \mathbf{E}_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau)$
2) $\mathbf{K}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)(\tau_{(1)}, \pi_{(1)}) \circ \mathbf{K}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)(\tau_{(2)}, \pi_{(2)}) \subseteq \mathbf{K}_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau, \pi)$

Proof: Let

$$\mathbf{E}'_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau) = \mathbf{E}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)(\tau_{(1)}) \circ \mathbf{E}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)(\tau_{(2)})$$
$$\mathbf{K}'_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau, \pi) = \mathbf{K}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)(\tau_{(1)}, \pi_{(1)}) \circ \mathbf{K}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)(\tau_{(2)}, \pi_{(2)})$$

Now it suffices to show that $\mathbf{E}'_W, \mathbf{K}'_W$ forms a post-fixpoint.

We first consider $\mathbf{K}'_W$. We suppose

- $(\tau_{(1)}, \pi_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)$
- $(\tau_{(2)}, \pi_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)$
- $(\tau, v_1, v_3) \in \overline{G(s_1, s_2)}$

and must show $(\pi, K_1[v_1], K_3[v_3]) \in \mathbf{E}'_W(G)((s_1^0, s_2^0), (s_1, s_2))$. By Lemma 99 there is v_2 such that $(\tau_{(1)}, v_1, v_2) \in \overline{G^{s_2}_{(1)}(s_1)}$ and $(\tau_{(2)}, v_2, v_3) \in \overline{G^{s_1}_{(2)}(s_2)}$. Hence we get:

- $(\pi_{(1)}, K_1[v_1], K_2[v_2]) \in \mathbf{E}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)$
- $(\pi_{(2)}, K_2[v_2], K_3[v_3]) \in \mathbf{E}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)$

By definition of $\mathbf{E}'_W$ we are done.

We now consider $\mathbf{E}'_W$. Suppose $(\tau_{(1)}, e_1, e_2) \in \mathbf{E}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)$ and $(\tau_{(2)}, e_2, e_3) \in \mathbf{E}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)$. Further suppose $(h_1, h_3) \in W.\mathsf{H}(s_1, s_2)(G(s_1, s_2))$ and $h_1^{\mathrm{F}}, h_3^{\mathrm{F}} \in \mathrm{Heap}$ such that $h_1 \uplus h_1^{\mathrm{F}}, h_3 \uplus h_3^{\mathrm{F}}$ defined. By construction of $W.\mathsf{H}$, we have h_2 such that $(h_1, h_2) \in W_1.\mathsf{H}(s_1)(G^{s_2}_{(1)})$ and $(h_2, h_3) \in W_2.\mathsf{H}(s_2)(G^{s_1}_{(2)})$. By Lemma 29, from $\mathit{consistent}(W_1)$, $(\tau_{(1)}, e_1, e_2) \in \mathbf{E}_{W_1}(G^{s_2}_{(1)})(s_1^0, s_1)$ and $G^{s_2}_{(1)} = W_1.\mathsf{L}(G^{s_2}_{(1)}) \cup G(s_1, s_2)_{\{1\}}$, we get three cases by letting $h_2^{\mathrm{F}} = \emptyset$. For each of these, again by Lemma 29 and letting $h_2^{\mathrm{F}} = \emptyset$, we get another three subcases from $\mathit{consistent}(W_2)$ and $(\tau_{(2)}, e_2, e_3) \in \mathbf{E}_{W_2}(G^{s_1}_{(2)})(s_2^0, s_2)$. So there are nine cases in total.

1) (1) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{\omega} \wedge\, h_2, e_2 \hookrightarrow^{\omega}$
   (1) $h_2, e_2 \hookrightarrow^{\omega} \wedge\, h_3 \uplus h_3^{\mathrm{F}}, e_3 \hookrightarrow^{\omega}$
   We are done because $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{\omega} \wedge\, h_3 \uplus h_3^{\mathrm{F}}, e_3 \hookrightarrow^{\omega}$.
2) (1) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{\omega} \wedge\, h_2, e_2 \hookrightarrow^{\omega}$
   (2) $h_2, e_2 \hookrightarrow^{*} h_2', v_2 \wedge\, h_3 \uplus h_3^{\mathrm{F}}, e_3 \hookrightarrow^{*} h_3', v_3$
   This is a contradiction by determinacy.
3) (1) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{\omega} \wedge\, h_2, e_2 \hookrightarrow^{\omega}$
   (3) $h_2, e_2 \hookrightarrow^{*} h_2', K_2[e_2'] \wedge\, h_3 \uplus h_3^{\mathrm{F}}, e_3 \hookrightarrow^{*} h_3', K_3[e_3']$ with $(\tau', e_2', e_3') \in \mathbf{S}(G(s_1, s_2')_{\{2\}}, G^{s_1}_{(2)}(s_2'))$
   Since $e_2' = \mathbf{I}(\widetilde{\tau}, f_1, f_3)\ v_2$ or $e_2' = \mathbf{I}(\widetilde{\tau}, f_1, f_3)[]$ for some $\widetilde{\tau}, f_1, f_3, v_2$, we know by determinacy that e_2 eventually gets stuck. This is a contradiction.
4) (2) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{*} h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge\, h_2, e_2 \hookrightarrow^{*} h_2', v_2$ with $s_1' \sqsupseteq [s_1^0, s_1]$ and $(h_1', h_2') \in W_1.\mathsf{H}(s_1')(G^{s_2}_{(1)}(s_1'))$ and $(\tau_{(1)}, v_1, v_2) \in \overline{G^{s_2}_{(1)}(s_1')}$
   (2) $h_2, e_2 \hookrightarrow^{*} h_2'', v_2' \wedge\, h_3 \uplus h_3^{\mathrm{F}}, e_3 \hookrightarrow^{*} h_3' \uplus h_3^{\mathrm{F}}, v_3$ with $s_2' \sqsupseteq [s_2^0, s_2]$ and $(h_2'', h_3') \in W_2.\mathsf{H}(s_2')(G^{s_1}_{(2)}(s_2'))$ and $(\tau_{(2)}, v_2', v_3) \in \overline{G^{s_1}_{(2)}(s_2')}$
   By determinacy we have $h_2' = h_2''$ and $v_2 = v_2'$. Since $G^{s_2}_{(1)}(s_1') \subseteq G^{s_2'}_{(1)}(s_1')$ and $G^{s_1}_{(2)}(s_2') \subseteq G^{s_2'}_{(2)}(s_2')$, we have $(\tau, v_1, v_3) \in \overline{G(s_1', s_2')}$ by Lemma 99. Similarly, $(h_1', h_3') \in W.\mathsf{H}(s_1', s_2')(G(s_1', s_2'))$ by construction of $W.\mathsf{H}$. Since $(s_1', s_2') \sqsupseteq [(s_1^0, s_2^0), (s_1, s_2)]$, we are done.
5) (2) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{*} h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge\, h_2, e_2 \hookrightarrow^{*} h_2', v_2$
   (3) $h_2, e_2 \hookrightarrow^{*} h_2'', K_2[e_2'] \wedge\, h_3 \uplus h_3^{\mathrm{F}}, e_3 \hookrightarrow^{*} h_3' \uplus h_3^{\mathrm{F}}, K_3[e_3']$ with $(\tau', e_2', e_3') \in \mathbf{S}(G(s_1, s_2')_{\{2\}}, G^{s_1}_{(2)}(s_2'))$
   Since $e_2' = \mathbf{I}(\widetilde{\tau}, f_1, f_3)\ v_2$ or $e_2' = \mathbf{I}(\widetilde{\tau}, f_1, f_3)[]$ for some $\widetilde{\tau}, f_1, f_3, v_2$, we know by determinacy that e_2 eventually gets stuck. This is a contradiction.
6) (3) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^{*} h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'] \wedge\, h_2, e_2 \hookrightarrow^{*} h_2', K_2[e_2']$ with $s_1' \sqsupseteq s_1$ and $(h_1', h_2') \in W_1.\mathsf{H}(s_1')(G^{s_2}_{(1)}(s_1'))$ and $(\tau', e_1', e_2') \in \mathbf{S}(G(s_1', s_2)_{\{1\}}, G^{s_2}_{(1)}(s_1'))$ and $\forall s_1'' \sqsupseteq_{\mathrm{pub}} s_1'. \forall G' \supseteq G^{s_2}_{(1)}.\ (\tau', \tau_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G')(s_1^0, s_1'')$
   (3) $h_2, e_2 \hookrightarrow^{*} h_2'', K_2'[e_2''] \wedge\, h_3 \uplus h_3^{\mathrm{F}}, e_3 \hookrightarrow^{*} h_3' \uplus h_3^{\mathrm{F}}, K_3[e_3']$ with $s_2' \sqsupseteq s_2$ and $(h_2'', h_3') \in W_2.\mathsf{H}(s_2')(G^{s_1}_{(2)}(s_2'))$ and $(\tau'', e_2'', e_3') \in \mathbf{S}(G(s_1, s_2')_{\{2\}}, G^{s_1}_{(2)}(s_2'))$ and $\forall s_2'' \sqsupseteq_{\mathrm{pub}} s_2'. \forall G' \supseteq G^{s_1}_{(2)}.\ (\tau'', \tau_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G')(s_2^0, s_2'')$

By definition of $\mathbf{S}$, $G(s_1', s_2)_{\{1\}}$ and $G(s_1, s_2')_{\{2\}}$, there are four possibilities.

a) We have for some $\widetilde{\tau}, \widehat{\tau}, f_1, f_3, v_1, v_2$,
- $e_1' = f_1\ v_1$ and $e_2' = \mathbf{I}(\widetilde{\tau} \to \widehat{\tau}, f_1, f_3)\ v_2$ and $\tau' = \widehat{\tau}_{(1)}$
- $(\widetilde{\tau} \to \widehat{\tau}, f_1, f_3) \in G(s_1', s_2) \subseteq G(s_1', s_2')$ and $(\widetilde{\tau}_{(1)}, v_1, v_2) \in \overline{G^{s_2}_{(1)}(s_1')} \subseteq \overline{G^{s_2'}_{(1)}(s_1')}$

and for some $\widetilde{\tau}', \widehat{\tau}', f_1', f_3', v_2', v_3$,
- $e_2'' = \mathbf{I}(\widetilde{\tau}' \to \widehat{\tau}', f_1', f_3')\ v_2'$ and $e_3' = f_3'\ v_3$ and $\tau'' = \widehat{\tau}'_{(2)}$
- $(\widetilde{\tau}' \to \widehat{\tau}', f_1', f_3') \in G(s_1, s_2') \subseteq G(s_1', s_2')$ and $(\widetilde{\tau}'_{(2)}, v_2', v_3) \in \overline{G^{s_1}_{(2)}(s_2')} \subseteq \overline{G^{s_1'}_{(2)}(s_2')}$

Since both e_2' and e_2'' are stuck, we know by determinacy:
- $h_2' = h_2''$ and $K_2 = K_2'$ and $\mathbf{I}(\widetilde{\tau} \to \widehat{\tau}, f_1, f_3) = \mathbf{I}(\widetilde{\tau}' \to \widehat{\tau}', f_1', f_3')$ and $v_2 = v_2'$

Since $\mathbf{I}$ is injective, we also have:
- $\widetilde{\tau} = \widetilde{\tau}'$ and $\widehat{\tau} = \widehat{\tau}'$ and $f_1 = f_1'$ and $f_3 = f_3'$.

Since $e_3' = f_3\ v_3 \wedge (f_1, f_3) \in G(s_1', s_2')(\widetilde{\tau} \to \widehat{\tau}) \wedge (v_1, v_3) \in \overline{G(s_1', s_2')}(\widetilde{\tau})$ by Lemma 99, we have
- $(\widehat{\tau}, e_1', e_3') \in \mathbf{S}(G(s_1', s_2'), G(s_1', s_2'))$.

Since $(h_1', h_2') \in W_1.\mathsf{H}(s_1')(G^{s_2}_{(1)}(s_1')) \subseteq W_1.\mathsf{H}(s_1')(G^{s_2'}_{(1)}(s_1'))$ and $(h_2', h_3') \in W_2.\mathsf{H}(s_2')(G^{s_1}_{(2)}(s_2')) \subseteq W_2.\mathsf{H}(s_2')(G^{s_1'}_{(2)}(s_2'))$, we have
- $(s_1', s_2') \sqsupseteq (s_1, s_2)$ and $(h_1', h_3') \in W.\mathsf{H}(s_1', s_2')(G(s_1', s_2'))$ by construction of $W.\mathsf{H}$.

It remains to show that $\forall (s_1'', s_2'') \sqsupseteq_{\text{pub}} (s_1', s_2').\forall G' \supseteq G.\ (\widehat{\tau}, \tau, K_1, K_3) \in \mathbf{K}'_W(G')((s_1^0, s_2^0), (s_1'', s_2''))$.
Since $G'^{s_2''}_{(1)} \supseteq G^{s_2}_{(1)}$ and $G'^{s_1''}_{(2)} \supseteq G^{s_1}_{(2)}$, we have

$$(\tau', \tau_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G'^{s_2''}_{(1)})(s_1^0, s_1'') \ \wedge\ (\tau'', \tau_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G'^{s_1''}_{(2)})(s_2^0, s_2'')$$

Note that $\tau' = \widehat{\tau}_{(1)}$ and $\tau'' = \widehat{\tau}_{(2)}$.
Thus, by definition of $\mathbf{K}'_W$, we have $(\widehat{\tau}, \tau, K_1, K_3) \in \mathbf{K}'_W(G')((s_1^0, s_2^0), (s_1'', s_2''))$.

b) We have for some $\sigma, \widehat{\tau}_1, f_1, f_3$,
- $e_1' = f_1[]$ and $e_2' = \mathbf{I}(\forall \alpha.\, \sigma, f_1, f_3)[]$ and $\tau' = \sigma_{(1)}[\widehat{\tau}_1/\alpha]$
- $(\forall \alpha.\, \sigma, f_1, f_3) \in G(s_1', s_2) \subseteq G(s_1', s_2')$

and for some $\sigma', \widehat{\tau}_2, f_1', f_3'$,
- $e_2'' = \mathbf{I}(\forall \alpha.\, \sigma', f_1', f_3')[]$ and $e_3' = f_3'[]$ and $\tau'' = \sigma'_{(2)}[\widehat{\tau}_2/\alpha]$
- $(\forall \alpha.\, \sigma', f_1', f_3') \in G(s_1, s_2') \subseteq G(s_1', s_2')$

Since both e_2' and e_2'' are stuck, we know by determinacy:
- $h_2' = h_2''$ and $K_2 = K_2'$ and $\mathbf{I}(\forall \alpha.\, \sigma, f_1, f_3) = \mathbf{I}(\forall \alpha.\, \sigma', f_1', f_3')$.

Since $\mathbf{I}$ is injective, we also have:
- $\sigma = \sigma'$ and $f_1 = f_1'$ and $f_3 = f_3'$.

Since $e_3' = f_3[] \wedge (f_1, f_3) \in G(s_1', s_2')(\forall \alpha.\, \sigma)$, we have
- $(\sigma[\widehat{\tau}/\alpha], e_1', e_3') \in \mathbf{S}(G(s_1', s_2'), G(s_1', s_2'))$ for some $\widehat{\tau}$ with $\widehat{\tau}_{(1)} = \widehat{\tau}_1 \wedge \widehat{\tau}_{(2)} = \widehat{\tau}_2$ by Corollary 92.

Since $(h_1', h_2') \in W_1.\mathsf{H}(s_1')(G^{s_2}_{(1)}(s_1')) \subseteq W_1.\mathsf{H}(s_1')(G^{s_2'}_{(1)}(s_1'))$ and $(h_2', h_3') \in W_2.\mathsf{H}(s_2')(G^{s_1}_{(2)}(s_2')) \subseteq W_2.\mathsf{H}(s_2')(G^{s_1'}_{(2)}(s_2'))$, we have
- $(s_1', s_2') \sqsupseteq (s_1, s_2)$ and $(h_1', h_3') \in W.\mathsf{H}(s_1', s_2')(G(s_1', s_2'))$ by construction of $W.\mathsf{H}$.

It remains to show that $\forall (s_1'', s_2'') \sqsupseteq_{\text{pub}} (s_1', s_2').\forall G' \supseteq G.\ (\sigma[\widehat{\tau}/\alpha], \tau, K_1, K_3) \in \mathbf{K}'_W(G')((s_1^0, s_2^0), (s_1'', s_2''))$.
Since $G'^{s_2''}_{(1)} \supseteq G^{s_2}_{(1)}$ and $G'^{s_1''}_{(2)} \supseteq G^{s_1}_{(2)}$, we have

$$(\tau', \tau_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G'^{s_2''}_{(1)})(s_1^0, s_1'') \ \wedge\ (\tau'', \tau_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G'^{s_1''}_{(2)})(s_2^0, s_2'')$$

Note that $\tau' = \sigma_{(1)}[\widehat{\tau}_1/\alpha] = \sigma[\widehat{\tau}/\alpha]_{(1)}$ and $\tau'' = \sigma_{(2)}[\widehat{\tau}_2/\alpha] = \sigma[\widehat{\tau}/\alpha]_{(2)}$.
Thus, by definition of $\mathbf{K}'_W$, we have $(\sigma[\widehat{\tau}/\alpha], \tau, K_1, K_3) \in \mathbf{K}'_W(G')((s_1^0, s_2^0), (s_1'', s_2''))$.

c) Proceeding as in the previous two cases, we get $e_2' = \mathbf{I}(\widetilde{\tau} \to \widehat{\tau}, f_1, f_3)\ v_2$ and $e_2'' = \mathbf{I}(\forall \alpha.\, \widetilde{\tau}', f_1', f_3')[]$ and later then $e_2' = e_2''$, which is a contradiction.

d) Similar to the previous case.

7) The remaining three cases (2)(1), (3)(1) and (3)(2) are symmetric to (1)(2), (1)(3) and (2)(3), respectively.

■

Transitivity w.r.t. the Full World.

Lemma 101.

$$\Delta;\Gamma \vdash e_1 \sim_W e_3 : \sigma$$

Proof:
We show $\mathit{inhabited}(W)$.

- By Lemma 13 we have $[W_i] \in \mathrm{GK}(W_i)$ for $i = 1, 2$.
- From $\mathit{inhabited}(W_i)$ for $i = 1, 2$, we have s_i^0 such that $(\emptyset, \emptyset) \in W_i.\mathsf{H}(s_i^0)([W_i](s_i^0))$.
- Thus, for any $G \in \mathrm{GK}(W)$, we have

$$\begin{array}{rll} (\emptyset,\emptyset) \in & W_1.\mathsf{H}(s_1^0)([W_1](s_1^0)) \circ W_2.\mathsf{H}(s_2^0)([W_2](s_2^0)) & \\ \subseteq & W_1.\mathsf{H}(s_1^0)(G_{(1)}^{s_2^0}(s_1^0)) \circ W_2.\mathsf{H}(s_2^0)(G_{(2)}^{s_1^0}(s_2^0)) & \text{(Lemmas 93 and 13)} \\ = & W.\mathsf{H}(s_1^0, s_2^0)(G(s_1^0, s_2^0)) & \text{(construction of } W.\mathsf{H}) \end{array}$$

We show $\mathit{consistent}(W)$.

- Suppose $G \in \mathrm{GK}(W)$ and $(e_1', e_3') \in \mathbf{S}(W.\mathsf{L}(s_1, s_2)(G(s_1, s_2)), G(s_1, s_2))(\tau')$.
- We need to show $(\mathit{beta}(e_1'), \mathit{beta}(e_3')) \in \mathbf{E}_W(G)((s_1, s_2), (s_1, s_2))(\tau')$.
- By definition of $\mathbf{S}$ and $W.\mathsf{L}$, and by Lemma 99, there is e_2' such that
  $(e_1', e_2') \in \mathbf{S}(W_1.\mathsf{L}(s_1)(G_{(1)}^{s_2}(s_1)), G_{(1)}^{s_2}(s_1))(\tau_{(1)}')$ and
  $(e_2', e_3') \in \mathbf{S}(W_2.\mathsf{L}(s_2)(G_{(2)}^{s_1}(s_2)), G_{(2)}^{s_1}(s_2))(\tau_{(2)}')$.
- From $\mathit{consistent}(W_1)$ and $\mathit{consistent}(W_2)$, we get

$$(\tau_{(1)}', \mathit{beta}(e_1'), \mathit{beta}(e_2')) \in \mathbf{E}_{W_1}(G_{(1)}^{s_2})(s_1, s_1) \ \wedge \ (\tau_{(2)}', \mathit{beta}(e_2'), \mathit{beta}(e_3')) \in \mathbf{E}_{W_2}(G_{(2)}^{s_1})(s_2, s_2) \ .$$

- By Lemma 100 we are done.

We show $\forall G \in \mathrm{GK}(W).\forall s_1, s_2.\forall \delta \in \mathrm{TyEnv}(\Delta).\forall(\gamma_1, \gamma_3) \in \mathrm{Env}(\delta\Gamma, G(s_1, s_2))$.

$$(\delta\sigma, \gamma_1 e_1, \gamma_3 e_3) \in \mathbf{E}_W(G)((s_1, s_2), (s_1, s_2)) \ .$$

- By Lemma 99 there exists γ_2 such that

$$(\gamma_1, \gamma_2) \in \mathrm{Env}((\delta\Gamma)_{(1)}, G_{(1)}^{s_2}(s_1)) \wedge (\gamma_2, \gamma_3) \in \mathrm{Env}((\delta\Gamma)_{(2)}, G_{(2)}^{s_1}(s_2)).$$

- Since $\mathrm{names}(\Gamma) \cap \mathcal{N}_\exists = \emptyset$, we have $(\delta\Gamma)_{(i)} = \delta_{(i)}\Gamma$.
- From $\Delta;\Gamma \vdash e_1 \sim_{W_1} e_2 : \sigma$ and $\Delta;\Gamma \vdash e_2 \sim_{W_2} e_3 : \sigma$ we thus get:

$$(\delta_{(1)}\sigma, \gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_1}(G_{(1)}^{s_2})(s_1, s_1) \wedge (\delta_{(2)}\sigma, \gamma_2 e_2, \gamma_3 e_3) \in \mathbf{E}_{W_2}(G_{(2)}^{s_1})(s_2, s_2)$$

- Since $\mathrm{names}(\sigma) \cap \mathcal{N}_\exists = \emptyset$, we have $\delta_{(i)}\sigma = (\delta\sigma)_{(i)}$.
- Thus, by Lemma 100, we have $(\delta\sigma, \gamma_1 e_1, \gamma_3 e_3) \in \mathbf{E}_W(G)((s_1, s_2), (s_1, s_2))$.

■

2) Constructing an Isomorphic Lifted World. We now come to the second part of the proof. Recall that the goal is to show $\Delta;\Gamma \vdash e_1 \sim e_3 : \sigma$ and that, to this end, we already assumed a set of names $\mathcal{N}$ to be given. Hence we must find $w \in \mathrm{LWorld}$ such that:

1) $w.\mathsf{N} \subseteq \mathcal{N}$
2) $\mathit{stable}(w)$
3) $\Delta;\Gamma \vdash e_1 \sim_{w\uparrow} e_3 : \tau$

We will now construct such a w. However, instead of showing (3) directly, we will rely on Theorem 84 and Lemma 101 and just show that $w\uparrow$ is isomorphic to W.

Definition 28. For $s_{\mathrm{rf}}, s_{\mathrm{rf}}' \in W_{\mathrm{ref}}.\mathsf{S}$, we define $s_{\mathrm{rf}}\backslash_{[1]}s_{\mathrm{rf}}', s_{\mathrm{rf}}\backslash_{[2]}s_{\mathrm{rf}}' \in W_{\mathrm{ref}}.\mathsf{S}$ as follows:

$$\begin{array}{rcl} s_{\mathrm{rf}}\backslash_{[1]}s_{\mathrm{rf}}' & := & \{\, (\tau, \ell_1, \ell_2) \in s_{\mathrm{rf}} \mid \forall \tau', \ell'.\ (\tau', \ell_1, \ell') \notin s_{\mathrm{rf}}' \,\} \\ s_{\mathrm{rf}}\backslash_{[2]}s_{\mathrm{rf}}' & := & \{\, (\tau, \ell_1, \ell_2) \in s_{\mathrm{rf}} \mid \forall \tau', \ell'.\ (\tau', \ell', \ell_2) \notin s_{\mathrm{rf}}' \,\} \end{array}$$

Definition 29. We construct $w \in \mathrm{LWorld}$ as follows (recall that $W_i = w_i\!\uparrow$).

$$
\begin{array}{lcl}
w.\mathsf{N} & := & W.\mathsf{N} \\
w.\mathsf{S} & := & W.\mathsf{S} \\
w.\sqsupseteq & := & W.\sqsupseteq \\
w.\sqsupseteq_{\mathrm{pub}} & := & W.\sqsupseteq_{\mathrm{pub}} \\
w.\mathsf{L}(s_{\mathrm{rf}})(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})(R) & := & \{\, (\tau, v_1, v_3) \in W.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})(R) \mid \forall \tau'.\ \tau \neq \mathsf{ref}\ \tau' \,\} \\
w.\mathsf{H}(s_{\mathrm{rf}})(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})(R) & := & \{\, (h_1, h_3) \mid s_{\mathrm{rf}} = s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}} \wedge \exists h^\circ_1, h^\bullet_1, h^\circ_{2a}, h^\bullet_{2a}, h^\circ_{2b}, h^\bullet_{2b}, h^\circ_3, h^\bullet_3. \\
& & \quad h_1 = h^\circ_1 \uplus h^{\mathrm{lc}}_1 \wedge h^\circ_{2a} \uplus h^{\mathrm{lc}}_{2a} = h^\circ_{2b} \uplus h^{\mathrm{lc}}_{2b} \wedge h_3 = h^\circ_3 \uplus h^{\mathrm{lc}}_3 \wedge \\
& & \quad \mathrm{dom}(h^{\mathrm{lc}}_{2a}) \cap \mathrm{dom}_{[2]}(s^1_{\mathrm{rf}}) = \emptyset \wedge \mathrm{dom}(h^{\mathrm{lc}}_{2b}) \cap \mathrm{dom}_{[1]}(s^2_{\mathrm{rf}}) = \emptyset \wedge \\
& & \quad (h^\circ_1, h^\circ_{2a}) \in W_{\mathrm{ref}}.\mathsf{H}(s^1_{\mathrm{rf}} \backslash_{[1]} s_{\mathrm{rf}})([W_1.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})]^*_{R_{\{1\}}}) \wedge \\
& & \quad (h^{\mathrm{lc}}_1, h^{\mathrm{lc}}_{2a}) \in w_1.\mathsf{H}(s^1_{\mathrm{rf}})(s^1_{\mathrm{lc}})([W_1.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})]^*_{R_{\{1\}}}) \wedge \\
& & \quad (h^\circ_{2b}, h^\circ_3) \in W_{\mathrm{ref}}.\mathsf{H}(s^2_{\mathrm{rf}} \backslash_{[2]} s_{\mathrm{rf}})([W_2.\mathsf{L}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})]^*_{R_{\{2\}}}) \wedge \\
& & \quad (h^{\mathrm{lc}}_{2b}, h^{\mathrm{lc}}_3) \in w_2.\mathsf{H}(s^2_{\mathrm{rf}})(s^2_{\mathrm{lc}})([W_2.\mathsf{L}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})]^*_{R_{\{2\}}}) \,\}
\end{array}
$$

Definition 30. For $G \in \mathrm{GK}(w\!\uparrow)$, we define $\overleftarrow{G} \in W.\mathsf{S} \to \mathrm{VRelF}$ as follows:

$$\overleftarrow{G}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}) := G(s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}, s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})\ .$$

Lemma 102.

$$s^1_{\mathrm{rf}}, s^2_{\mathrm{rf}} \in W_{\mathrm{ref}}.\mathsf{S} \implies s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}} \in W_{\mathrm{ref}}.\mathsf{S}$$

Proof:

- Since s^1_{rf} and s^2_{rf} are finite by assumption, $s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}$ is finite, too.
- Now suppose $(\tau, \ell_1, \ell_3), (\tau', \ell'_1, \ell'_3) \in s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}$.
- Then there is ℓ_2 such that $(\tau_{(1)}, \ell_1, \ell_2) \in s^1_{\mathrm{rf}}$ and $(\tau_{(2)}, \ell_2, \ell_3) \in s^2_{\mathrm{rf}}$.
- Also there is ℓ'_2 such that $(\tau'_{(1)}, \ell'_1, \ell'_2) \in s^1_{\mathrm{rf}}$ and $(\tau'_{(2)}, \ell'_2, \ell'_3) \in s^2_{\mathrm{rf}}$.
- Now further suppose $\ell_1 = \ell'_1$ (the reasoning for $\ell_3 = \ell'_3$ is analogous).
- From the assumption we get $\tau_{(1)} = \tau'_{(1)}$ and $\ell_2 = \ell'_2$.
- From the latter and the assumption we get $\tau_{(2)} = \tau'_{(2)}$ and $\ell_3 = \ell'_3$.
- It thus remains to show $\tau = \tau'$, which follows by Lemma 90.

■

Lemma 103.

1) If $\hat{s}^1_{\mathrm{rf}} \sqsupseteq s^1_{\mathrm{rf}}$ and $\hat{s}^2_{\mathrm{rf}} \sqsupseteq s^2_{\mathrm{rf}}$, then $\hat{s}^1_{\mathrm{rf}} \bullet \hat{s}^2_{\mathrm{rf}} \sqsupseteq s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}$.
2) If $\hat{s}^1_{\mathrm{rf}} \sqsupseteq_{\mathrm{pub}} s^1_{\mathrm{rf}}$ and $\hat{s}^2_{\mathrm{rf}} \sqsupseteq_{\mathrm{pub}} s^2_{\mathrm{rf}}$, then $\hat{s}^1_{\mathrm{rf}} \bullet \hat{s}^2_{\mathrm{rf}} \sqsupseteq_{\mathrm{pub}} s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}$.

Proof: Easy to check. ■

Lemma 104. For $G \in \mathrm{GK}(w\!\uparrow)$, we have $\overleftarrow{G} \in \mathrm{GK}(W)$.

Proof: We know from Lemma 103 and $G \in \mathrm{GK}(w\!\uparrow)$ that $\overleftarrow{G}$ is monotone. It thus remains to show $\forall s.\ \overleftarrow{G}(s) \geq^{W.\mathsf{N}}_{\mathrm{ref}} W.\mathsf{L}(s)(\overleftarrow{G}(s))$:

- Suppose $s = (s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})$ and τ are given.
- From $G \in \mathrm{GK}(w\!\uparrow)$ we know $\overleftarrow{G}(s)(\tau) \geq^{w.\mathsf{N}}_{\mathrm{ref}} w\!\uparrow.\mathsf{L}(s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}, s)(\overleftarrow{G}(s))(\tau)$.
- Note that $w.\mathsf{N} = W.\mathsf{N}$.
- If τ is not of the form $\mathsf{ref}\ \tau'$, then we have:

$$
\begin{array}{rl}
& w\!\uparrow.\mathsf{L}(s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}, s)(\overleftarrow{G}(s))(\tau) \\
= & w.\mathsf{L}(s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}})(s)(\overleftarrow{G}(s))(\tau) \\
= & W.\mathsf{L}(s)(\overleftarrow{G}(s))(\tau)
\end{array}
$$

- If $\tau = \mathsf{ref}\,\tau'$, then we have:

$$\begin{aligned}
& w{\uparrow}.\mathsf{L}(s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}, s)(\overleftarrow{G}(s))(\tau) \\
&= W_{\mathrm{ref}}.\mathsf{L}(s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}})(\overleftarrow{G}(s))(\tau) \\
&= (s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}})(\tau') \\
&= s^1_{\mathrm{rf}}(\tau'_{(1)}) \circ s^2_{\mathrm{rf}}(\tau'_{(2)}) \\
&= W_{\mathrm{ref}}.\mathsf{L}(s^1_{\mathrm{rf}})([W_1.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})]^*_{\overleftarrow{G}(s)_{\{1\}}})(\tau_{(1)}) \circ W_{\mathrm{ref}}.\mathsf{L}(s^2_{\mathrm{rf}})([W_2.\mathsf{L}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})]^*_{\overleftarrow{G}(s)_{\{2\}}})(\tau_{(2)}) \\
&= W_1.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})([W_1.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})]^*_{\overleftarrow{G}(s)_{\{1\}}})(\tau_{(1)}) \circ W_2.\mathsf{L}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})([W_2.\mathsf{L}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})]^*_{\overleftarrow{G}(s)_{\{2\}}})(\tau_{(2)}) \\
&= (W_1.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})([W_1.\mathsf{L}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})]^*_{\overleftarrow{G}(s)_{\{1\}}}) \bullet W_2.\mathsf{L}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})([W_2.\mathsf{L}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})]^*_{\overleftarrow{G}(s)_{\{2\}}}))(\tau) \\
&= W.\mathsf{L}(s)(\overleftarrow{G}(s))(\tau)
\end{aligned}$$

■

Lemma 105. $w.\mathsf{N} \subseteq \mathcal{N}$

Proof: By construction. ■

Stability.

Definition 31. Lemma 99 gives rise to a choice function *mediate* that, given $G \in \mathrm{GK}(W)$ and $(\tau, v_1, v_3) \in \overline{G(s_1, s_2)}$, returns a value $v_2 = \mathit{mediate}(G, s_1, s_2, \tau, v_1, v_3)$ such that $(\tau_{(1)}, v_1, v_2) \in \overline{G^{s_2}_{(1)}(s_1)}$ and $(\tau_{(2)}, v_2, v_3) \in \overline{G^{s_1}_{(2)}(s_2)}$. We usually leave out some arguments of *mediate* that are clear from context.

Lemma 106 (Stability of w)**.** $\mathit{stable}(w)$

Proof:

- Suppose $G \in \mathrm{GK}(w{\uparrow})$, $s = (s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})$, $(h_1, h_3) \in w.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}}, s))$ and $\hat{s}_{\mathrm{rf}} \sqsupseteq s_{\mathrm{rf}}$.
- Further suppose $(\hat{h}^\bullet_1, \hat{h}^\bullet_3) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}_{\mathrm{rf}})(G(\hat{s}_{\mathrm{rf}}, s))$ and $\mathrm{defined}(h_1 \uplus \hat{h}^\bullet_1)$ and $\mathrm{defined}(h_3 \uplus \hat{h}^\bullet_3)$.
- We must find $\hat{s} = (\hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}}, \hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}}) \sqsupseteq_{\mathrm{pub}} s$ such that $(h_1, h_3) \in w.\mathsf{H}(\hat{s}_{\mathrm{rf}})(\hat{s})(G(\hat{s}_{\mathrm{rf}}, \hat{s}))$.
- From $(h_1, h_3) \in w.\mathsf{H}(s_{\mathrm{rf}})(s)(G(s_{\mathrm{rf}}, s))$ we know that there are $h^\circ_1, h^{\mathrm{lc}}_1, h^\circ_{2a}, h^{\mathrm{lc}}_{2a}, h^\circ_{2b}, h^{\mathrm{lc}}_{2b}, h^\circ_3, h^{\mathrm{lc}}_3$ such that:
  1) $h_1 = h^\circ_1 \uplus h^{\mathrm{lc}}_1 \wedge h^\circ_{2a} \uplus h^{\mathrm{lc}}_{2a} = h^\circ_{2b} \uplus h^{\mathrm{lc}}_{2b} \wedge h_3 = h^\circ_3 \uplus h^{\mathrm{lc}}_3$
  2) $\mathrm{dom}(h^{\mathrm{lc}}_{2a}) \cap \mathrm{dom}_{[2]}(s^1_{\mathrm{rf}}) = \emptyset \wedge \mathrm{dom}(h^{\mathrm{lc}}_{2b}) \cap \mathrm{dom}_{[1]}(s^2_{\mathrm{rf}}) = \emptyset$
  3) $(h^\circ_1, h^\circ_{2a}) \in W_{\mathrm{ref}}.\mathsf{H}(s^1_{\mathrm{rf}} \backslash_{[1]} s_{\mathrm{rf}})(G_1)$
  4) $(h^{\mathrm{lc}}_1, h^{\mathrm{lc}}_{2a}) \in w_1.\mathsf{H}(s^1_{\mathrm{rf}})(s^1_{\mathrm{lc}})(G_1)$
  5) $(h^\circ_{2b}, h^\circ_3) \in W_{\mathrm{ref}}.\mathsf{H}(s^2_{\mathrm{rf}} \backslash_{[2]} s_{\mathrm{rf}})(G_2)$
  6) $(h^{\mathrm{lc}}_{2b}, h^{\mathrm{lc}}_3) \in w_2.\mathsf{H}(s^2_{\mathrm{rf}})(s^2_{\mathrm{lc}})(G_2)$

  where G_i is short for $[W_i.\mathsf{L}(s^i_{\mathrm{rf}}, s^i_{\mathrm{lc}})]^*_{G(s_{\mathrm{rf}}, s)_{\{i\}}}$.
- We know $\hat{s}_{\mathrm{rf}} = s_{\mathrm{rf}} \uplus s^+$ for some s^+.
- For each $(\tau, \ell_1, \ell_3) \in s^+$ we pick a fresh location $\ell_{(\tau, \ell_1, \ell_3)}$.
- Now let $\hat{s}^1_{\mathrm{rf}} = s^1_{\mathrm{rf}} \uplus \{\, (\tau_{(1)}, \ell_1, \ell_{(\tau, \ell_1, \ell_3)}) \mid (\tau, \ell_1, \ell_3) \in s^+ \,\}$.
- And let $\hat{s}^2_{\mathrm{rf}} = s^2_{\mathrm{rf}} \uplus \{\, (\tau_{(2)}, \ell_{(\tau, \ell_1, \ell_3)}, \ell_3) \mid (\tau, \ell_1, \ell_3) \in s^+ \,\}$.
- Using $s_{\mathrm{rf}}, s^1_{\mathrm{rf}}, s^2_{\mathrm{rf}}, \hat{s}_{\mathrm{rf}} \in W_{\mathrm{ref}}.\mathsf{S}$ and $s_{\mathrm{rf}} = s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}$, it is easy to see that $\hat{s}^1_{\mathrm{rf}} \bullet \hat{s}^2_{\mathrm{rf}} = \hat{s}_{\mathrm{rf}}$.
- We show $\hat{s}^1_{\mathrm{rf}}, \hat{s}^2_{\mathrm{rf}} \in W_{\mathrm{ref}}.\mathsf{S}$:
  - We do only one part, the other is symmetric.
  - Suppose $(\tau', \ell_1, \ell_2) \in s^1_{\mathrm{rf}}$ and $(\tau, \ell_1, \ell_3) \in s^+$, *i.e.,* $(\tau, \ell_1, \ell_3) \in \hat{s}_{\mathrm{rf}} \setminus s_{\mathrm{rf}}$.
  - We derive a contradiction.
  - Since $\ell_1 \in \mathrm{dom}(\hat{h}^\bullet_1)$ and $\mathrm{defined}(h_1 \uplus \hat{h}^\bullet_1)$, we get $\ell_1 \notin \mathrm{dom}(h_1) \supseteq \mathrm{dom}(h^\circ_1)$.
  - From (3) we learn $\ell_1 \notin \mathrm{dom}_{[1]}(s^1_{\mathrm{rf}} \backslash_{[1]} s_{\mathrm{rf}})$, and hence $\ell_1 \in \mathrm{dom}_{[1]}(s_{\mathrm{rf}})$.
  - Consequently there is τ'', ℓ''_3 such that $(\tau'', \ell_1, \ell''_3) \in s_{\mathrm{rf}} \subseteq \hat{s}_{\mathrm{rf}}$.
  - Since $(\tau, \ell_1, \ell_3) \in s^+ \subseteq \hat{s}_{\mathrm{rf}}$, we learn $\tau = \tau''$ and $\ell_3 = \ell''_3$.
  - This contradicts $(\tau, \ell_1, \ell_3) \notin s_{\mathrm{rf}}$.
- $\hat{s}^i_{\mathrm{rf}} \sqsupseteq s^i_{\mathrm{rf}}$ holds by construction.
- From $(\hat{h}^\bullet_1, \hat{h}^\bullet_3) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}_{\mathrm{rf}})(G(\hat{s}_{\mathrm{rf}}, s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}))$ we know by monotonicity that

$(\hat{h}_1^\bullet, \hat{h}_3^\bullet) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}_{\mathrm{rf}})(\overleftarrow{G}(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, \hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}))$.

- Note that $\overleftarrow{G} \in \mathrm{GK}(W)$ by Lemma 104.
- We define:

7) $h_1^{\mathrm{rf}} = \hat{h}_1^\bullet \uplus h_1^\circ$
8) $\hat{h}_2^\bullet = \{\, \ell_2 \mapsto \mathit{mediate}(\overleftarrow{G}, \tau, \hat{h}_1^\bullet(\ell_1), \hat{h}_3^\bullet(\ell_3)) \mid (\tau_{(1)}, \ell_1, \ell_2) \in \hat{s}^1_{\mathrm{rf}} \wedge (\tau_{(2)}, \ell_2, \ell_3) \in \hat{s}^2_{\mathrm{rf}} \,\}$
9) $h_{2a}^{\mathrm{rf}} = \hat{h}_2^\bullet \uplus h_{2a}^\circ$
10) $h_{2b}^{\mathrm{rf}} = \hat{h}_2^\bullet \uplus h_{2b}^\circ$
11) $h_3^{\mathrm{rf}} = \hat{h}_3^\bullet \uplus h_3^\circ$

- It is easy to check that:
  - $\mathrm{dom}(h_1^{\mathrm{rf}}) = \mathrm{dom}_{[1]}(\hat{s}^1_{\mathrm{rf}}) \wedge \mathrm{dom}(h_{2a}^{\mathrm{rf}}) = \mathrm{dom}_{[2]}(\hat{s}^1_{\mathrm{rf}})$
  - $\mathrm{dom}(h_{2b}^{\mathrm{rf}}) = \mathrm{dom}_{[1]}(\hat{s}^2_{\mathrm{rf}}) \wedge \mathrm{dom}(h_3^{\mathrm{rf}}) = \mathrm{dom}_{[2]}(\hat{s}^2_{\mathrm{rf}})$
- Since $G(s_{\mathrm{rf}}, s) = \overleftarrow{G}(s)$ we know from (3–6) by monotonicity:

12) $(h_1^\circ, h_{2a}^\circ) \in W_{\mathrm{ref}}.\mathsf{H}(s^1_{\mathrm{rf}} \backslash_{[1]} s_{\mathrm{rf}})(\overleftarrow{G}^{(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})}_{(1)}(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}))$
13) $(h_1^{\mathrm{lc}}, h_{2a}^{\mathrm{lc}}) \in w_1.\mathsf{H}(s^1_{\mathrm{rf}})(s^1_{\mathrm{lc}})(\overleftarrow{G}^{(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})}_{(1)}(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}))$
14) $(h_{2b}^\circ, h_3^\circ) \in W_{\mathrm{ref}}.\mathsf{H}(s^2_{\mathrm{rf}} \backslash_{[2]} s_{\mathrm{rf}})(\overleftarrow{G}^{(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})}_{(2)}(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}))$
15) $(h_{2b}^{\mathrm{lc}}, h_3^{\mathrm{lc}}) \in w_2.\mathsf{H}(s^2_{\mathrm{rf}})(s^2_{\mathrm{lc}})(\overleftarrow{G}^{(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})}_{(2)}(s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}))$

- Using (6–11), (13), and $(\hat{h}_1^\bullet, \hat{h}_3^\bullet) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}_{\mathrm{rf}})(\overleftarrow{G}(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, \hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}))$, it is easy to check that:
  - $\forall(\tau_1, \ell_1, \ell_2) \in \hat{s}^1_{\mathrm{rf}}.\ (\tau_1, h_1^{\mathrm{rf}}(\ell_1), h_{2a}^{\mathrm{rf}}(\ell_2)) \in \overleftarrow{G}^{(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})}_{(1)}(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})}$
  - $\forall(\tau_2, \ell_2, \ell_3) \in \hat{s}^2_{\mathrm{rf}}.\ (\tau_2, h_{2b}^{\mathrm{rf}}(\ell_2), h_3^{\mathrm{rf}}(\ell_3)) \in \overleftarrow{G}^{(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})}_{(2)}(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})}$
- Consequently we have:

16) $(h_1^{\mathrm{rf}}, h_{2a}^{\mathrm{rf}}) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}^1_{\mathrm{rf}})(\overleftarrow{G}^{(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})}_{(1)}(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}))$
17) $(h_{2b}^{\mathrm{rf}}, h_3^{\mathrm{rf}}) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}^2_{\mathrm{rf}})(\overleftarrow{G}^{(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})}_{(2)}(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}))$

- From (1–2), (7–11), (16–17), $\mathrm{defined}(h_1 \uplus \hat{h}_1^\bullet)$ and $\mathrm{defined}(h_3 \uplus \hat{h}_3^\bullet)$ it is easy to see that:

18) $\mathrm{defined}(h_1^{\mathrm{lc}} \uplus h_1^{\mathrm{rf}}) \wedge \mathrm{defined}(h_{2a}^{\mathrm{lc}} \uplus h_{2a}^{\mathrm{rf}})$
19) $\mathrm{defined}(h_{2b}^{\mathrm{lc}} \uplus h_{2b}^{\mathrm{rf}}) \wedge \mathrm{defined}(h_3^{\mathrm{lc}} \uplus h_3^{\mathrm{rf}})$

- From (13), (16), (18), and $\mathit{stable}(w_1)$ we get $\hat{s}^1_{\mathrm{lc}} \sqsupseteq_{\mathrm{pub}} s^1_{\mathrm{lc}}$ such that $(h_1^{\mathrm{lc}}, h_{2a}^{\mathrm{lc}}) \in w_1.\mathsf{H}(\hat{s}^1_{\mathrm{rf}})(\hat{s}^1_{\mathrm{lc}})(\overleftarrow{G}^{(\hat{s}^2_{\mathrm{rf}}, s^2_{\mathrm{lc}})}_{(1)}(\hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}}))$.
- From (15), (17), (19), and $\mathit{stable}(w_2)$ we get $\hat{s}^2_{\mathrm{lc}} \sqsupseteq_{\mathrm{pub}} s^2_{\mathrm{lc}}$ such that $(h_{2b}^{\mathrm{lc}}, h_3^{\mathrm{lc}}) \in w_2.\mathsf{H}(\hat{s}^2_{\mathrm{rf}})(\hat{s}^2_{\mathrm{lc}})(\overleftarrow{G}^{(\hat{s}^1_{\mathrm{rf}}, s^1_{\mathrm{lc}})}_{(2)}(\hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}}))$.
- Thus by monotonicity we get $(h_1^{\mathrm{lc}}, h_{2a}^{\mathrm{lc}}) \in w_1.\mathsf{H}(\hat{s}^1_{\mathrm{rf}})(\hat{s}^1_{\mathrm{lc}})(\overleftarrow{G}^{(\hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}})}_{(1)}(\hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}}))$ and $(h_{2b}^{\mathrm{lc}}, h_3^{\mathrm{lc}}) \in w_2.\mathsf{H}(\hat{s}^2_{\mathrm{rf}})(\hat{s}^2_{\mathrm{lc}})(\overleftarrow{G}^{(\hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}})}_{(2)}(\hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}}))$.
- From (12) we get by monotonicity $(h_1^\circ, h_{2a}^\circ) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}^1_{\mathrm{rf}} \backslash_{[1]} \hat{s}_{\mathrm{rf}})(\overleftarrow{G}^{(\hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}})}_{(1)}(\hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}}))$ because $\hat{s}^1_{\mathrm{rf}} \backslash_{[1]} \hat{s}_{\mathrm{rf}} = s^1_{\mathrm{rf}} \backslash_{[1]} s_{\mathrm{rf}}$.
- From (14) we get by monotonicity $(h_{2b}^\circ, h_3^\circ) \in W_{\mathrm{ref}}.\mathsf{H}(\hat{s}^2_{\mathrm{rf}} \backslash_{[2]} \hat{s}_{\mathrm{rf}})(\overleftarrow{G}^{(\hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}})}_{(2)}(\hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}}))$ because $\hat{s}^2_{\mathrm{rf}} \backslash_{[2]} \hat{s}_{\mathrm{rf}} = s^2_{\mathrm{rf}} \backslash_{[2]} s_{\mathrm{rf}}$.
- Hence $(h_1, h_3) \in w.\mathsf{H}(\hat{s}_{\mathrm{rf}})(\hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}}, \hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}})(G(\hat{s}_{\mathrm{rf}}, \hat{s}^1_{\mathrm{rf}}, \hat{s}^1_{\mathrm{lc}}, \hat{s}^2_{\mathrm{rf}}, \hat{s}^2_{\mathrm{lc}}))$ by construction of w.

■

Isomorphism.

Lemma 107 (Isomorphism between W and $w\!\uparrow$)**.** $\exists \phi, \psi.\ \phi : W \cong w\!\uparrow : \psi$

Proof: We define $\phi \in W.\mathsf{S} \to \mathbb{P}(w\!\uparrow.\mathsf{S})$ and $\psi \in w\!\uparrow.\mathsf{S} \to \mathbb{P}(W.\mathsf{S})$ as follows.

$$\begin{array}{lcl} \phi(s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}) & := & \{\, (s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}}, s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}) \,\} \\ \psi(s_{\mathrm{rf}}, s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}) & := & \begin{cases} \{\, (s^1_{\mathrm{rf}}, s^1_{\mathrm{lc}}, s^2_{\mathrm{rf}}, s^2_{\mathrm{lc}}) \,\} & \text{if } s_{\mathrm{rf}} = s^1_{\mathrm{rf}} \bullet s^2_{\mathrm{rf}} \\ \emptyset & \text{otherwise} \end{cases} \end{array}$$

It is easy to see that $\phi \circ \psi \sqsupseteq_{\text{pub}} \text{id}$ and $\psi \circ \phi \sqsupseteq_{\text{pub}} \text{id}$. So it remains to show that ϕ and ψ are world morphisms:

1) To show: $\phi : W \to w\!\uparrow$
   a) To show: $W.\mathsf{N} = w\!\uparrow.\mathsf{N}$
      - $w\!\uparrow.\mathsf{N} = W_{\text{ref}}.\mathsf{N} \uplus w.\mathsf{N} = w.\mathsf{N} = W.\mathsf{N}$.
   b) To show: $\forall s_1, s_1'.\ s_1 \sqsubseteq s_1' \implies \forall s_2 \in \phi(s_1), s_2' \in \phi(s_1').\ s_2 \sqsubseteq s_2'$
      - This boils down to the fact that $s^1_{\text{rf}} \bullet s^2_{\text{rf}} \sqsubseteq \hat{s}^1_{\text{rf}} \bullet \hat{s}^2_{\text{rf}}$ if $s^1_{\text{rf}} \sqsubseteq \hat{s}^1_{\text{rf}}$ and $s^2_{\text{rf}} \sqsubseteq \hat{s}^2_{\text{rf}}$.
   c) To show: $\forall s_1, s_1'.\ s_1 \sqsubseteq_{\text{pub}} s_1' \implies \forall s_2 \in \phi(s_1), s_2' \in \phi(s_1').\ s_2 \sqsubseteq_{\text{pub}} s_2'$
      - See (1b).
   d) $\forall s_1.\forall s_2 \in \phi(s_1).\ W.\mathsf{L}(s_1) = w\!\uparrow.\mathsf{L}(s_2)$
      - In fact, we show $\forall s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}}.\ W.\mathsf{L}(s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}}) = w\!\uparrow.\mathsf{L}(s^1_{\text{rf}} \bullet s^2_{\text{rf}}, s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})$.
        For non-reference types this is immediate:

$$\begin{array}{lll} & W.\mathsf{L}(s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})(R)(\tau) & \\ = & w.\mathsf{L}(s^1_{\text{rf}} \bullet s^2_{\text{rf}})(s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})(R)(\tau) & \text{(construction of } w\text{)} \\ = & w\!\uparrow.\mathsf{L}(s^1_{\text{rf}} \bullet s^2_{\text{rf}}, s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})(R)(\tau) & \text{(construction of } W_{\text{ref}}\text{)} \end{array}$$

        For reference types we have:

$$\begin{array}{lll} & W.\mathsf{L}(s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})(R)(\mathsf{ref}\,\tau) & \\ = & W_1.\mathsf{L}(s^1_{\text{rf}}, s^1_{\text{lc}})(R_1)(\mathsf{ref}\,\tau_{(1)}) \circ W_2.\mathsf{L}(s^2_{\text{rf}}, s^2_{\text{lc}})(R_2)(\mathsf{ref}\,\tau_{(2)}) & \text{(construction of } W\text{)} \\ = & W_{\text{ref}}.\mathsf{L}(s^1_{\text{rf}})(R_1)(\mathsf{ref}\,\tau_{(1)}) \circ W_{\text{ref}}.\mathsf{L}(s^2_{\text{rf}})(R_2)(\mathsf{ref}\,\tau_{(2)}) & (W_i = w_i\!\uparrow) \\ = & s^1_{\text{rf}}(\tau_{(1)}) \circ s^2_{\text{rf}}(\tau_{(2)}) & \text{(construction of } W_{\text{ref}}\text{)} \\ = & (s^1_{\text{rf}} \bullet s^2_{\text{rf}})(\tau) & \\ = & W_{\text{ref}}.\mathsf{L}(s^1_{\text{rf}} \bullet s^2_{\text{rf}})(R)(\mathsf{ref}\,\tau) & \text{(construction of } W_{\text{ref}}\text{)} \\ = & w\!\uparrow.\mathsf{L}(s^1_{\text{rf}} \bullet s^2_{\text{rf}}, s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})(R)(\mathsf{ref}\,\tau) & \end{array}$$

        where R_i is short for $[W_i.\mathsf{L}(s^i_{\text{rf}}, s^i_{\text{lc}})]^*_{R_{\{i\}}}$.
   e) $\forall s.\forall G \in \text{GK}(W).\ W.\mathsf{H}(s)(G(s)) \subseteq \bigcup_{s' \in \phi(s)} w\!\uparrow.\mathsf{H}(s')(G(s))$
      - Let $s = (s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})$ and G be given and suppose $(h_1, h_3) \in W.\mathsf{H}(s)(G(s))$.
      - Let $s' = (s^1_{\text{rf}} \bullet s^2_{\text{rf}}, s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})$, so $s' \in \phi(s)$.
      - We will show $(h_1, h_3) \in w\!\uparrow.\mathsf{H}(s')(G(s))$.
      - We know by construction of W that there is h_2 such that
        $(h_1, h_2) \in W_1.\mathsf{H}(s^1_{\text{rf}}, s^1_{\text{lc}})(G_1)$ and
        $(h_2, h_3) \in W_2.\mathsf{H}(s^2_{\text{rf}}, s^2_{\text{lc}})(G_2)$, where G_i is short for $[W_i.\mathsf{L}(s^i_{\text{rf}}, s^i_{\text{lc}})]^*_{G(s)_{\{i\}}}$.
      - Hence there are $h_1^{\text{rf}}, h_1^{\text{lc}}, h_{2a}^{\text{rf}}, h_{2a}^{\text{lc}}, h_{2b}^{\text{rf}}, h_{2b}^{\text{lc}}, h_3^{\text{rf}}, h_3^{\text{lc}}$ such that:
        i) $h_1 = h_1^{\text{rf}} \uplus h_1^{\text{lc}}$
        ii) $h_2 = h_{2a}^{\text{rf}} \uplus h_{2a}^{\text{lc}}$
        iii) $h_2 = h_{2b}^{\text{rf}} \uplus h_{2b}^{\text{lc}}$
        iv) $h_3 = h_3^{\text{rf}} \uplus h_3^{\text{lc}}$
        v) $(h_1^{\text{rf}}, h_{2a}^{\text{rf}}) \in W_{\text{ref}}.\mathsf{H}(s^1_{\text{rf}})(G_1)$
        vi) $(h_1^{\text{lc}}, h_{2a}^{\text{lc}}) \in w_1.\mathsf{H}(s^1_{\text{rf}})(s^1_{\text{lc}})(G_1)$
        vii) $(h_{2b}^{\text{rf}}, h_3^{\text{rf}}) \in W_{\text{ref}}.\mathsf{H}(s^2_{\text{rf}})(G_2)$
        viii) $(h_{2b}^{\text{lc}}, h_3^{\text{lc}}) \in w_2.\mathsf{H}(s^2_{\text{rf}})(s^2_{\text{lc}})(G_2)$
      - Let $s_i^\circ = s^i_{\text{rf}} \setminus_{[i]} (s^1_{\text{rf}} \bullet s^2_{\text{rf}})$.
      - Let $s_i^\bullet = s^i_{\text{rf}} \setminus s_i^\circ$.
      - Note that $s^i_{\text{rf}} = s_i^\bullet \uplus s_i^\circ$.
      - Hence by (v), (vii) and construction of W_{ref} there are $h_1^\bullet, h_1^\circ, h_{2a}^\bullet, h_{2a}^\circ, h_{2b}^\bullet, h_{2b}^\circ, h_3^\bullet, h_3^\circ$ such that:
        ix) $h_1^{\text{rf}} = h_1^\bullet \uplus h_1^\circ$
        x) $h_{2a}^{\text{rf}} = h_{2a}^\bullet \uplus h_{2a}^\circ$
        xi) $h_{2b}^{\text{rf}} = h_{2b}^\bullet \uplus h_{2b}^\circ$
        xii) $h_3^{\text{rf}} = h_3^\bullet \uplus h_3^\circ$
        xiii) $(h_1^\bullet, h_{2a}^\bullet) \in W_{\text{ref}}.\mathsf{H}(s_1^\bullet)(G_1)$
        xiv) $(h_1^\circ, h_{2a}^\circ) \in W_{\text{ref}}.\mathsf{H}(s_1^\circ)(G_1)$
        xv) $(h_{2b}^\bullet, h_3^\bullet) \in W_{\text{ref}}.\mathsf{H}(s_2^\bullet)(G_2)$

xvi) $(h^\circ_{2b}, h^\circ_3) \in W_{\text{ref}}.\mathsf{H}(s^\circ_2)(G_2)$

- Also, from (ii-iii), (v), (vii) we know $\text{dom}(h^{\text{lc}}_{2a}) \cap \text{dom}_{[2]}(s^1_{\text{rf}}) = \emptyset \wedge \text{dom}(h^{\text{lc}}_{2b}) \cap \text{dom}_{[1]}(s^2_{\text{rf}}) = \emptyset$.
- We show $(h^\bullet_1, h^\bullet_3) \in W_{\text{ref}}.\mathsf{H}(s^1_{\text{rf}} \bullet s^2_{\text{rf}})(G(s))$:
  - Suppose $(\tau, \ell_1, \ell_3) \in s^1_{\text{rf}} \bullet s^2_{\text{rf}}$.
  - We must show $(\tau, h^\bullet_1(\ell_1), h^\bullet_3(\ell_3)) \in \overline{G(s)}$.
  - Observe that $s^\bullet_1 \bullet s^\bullet_2 = s^1_{\text{rf}} \bullet s^2_{\text{rf}}$.
  - So there is ℓ_2 such that $(\tau_{(1)}, \ell_1, \ell_2) \in s^\bullet_1$ and $(\tau_{(2)}, \ell_2, \ell_3) \in s^\bullet_2$.
  - From (xiii) we know $(\tau_{(1)}, h^\bullet_1(\ell_1), h^\bullet_{2a}(\ell_2)) \in \overline{G_1}$.
  - From (xv) we know $(\tau_{(2)}, h^\bullet_{2b}(\ell_2), h^\bullet_3(\ell_3)) \in \overline{G_2}$.
  - Since $h^\bullet_{2a}, h^\bullet_{2b} \subseteq h_2$, we have $h^\bullet_{2a}(\ell_2) = h^\bullet_{2b}(\ell_2)$ and thus $(\tau, h^\bullet_1(\ell_1), h^\bullet_3(\ell_3)) \in \overline{G(s)}$ by Lemma 99.
- Since $h_1 \setminus h^\bullet_1 = h^\circ_1 \uplus h^{\text{lc}}_1$ and $h_3 \setminus h^\bullet_3 = h^\circ_3 \uplus h^{\text{lc}}_3$, we know by construction of w that $(h_1 \setminus h^\bullet_1, h_3 \setminus h^\bullet_3) \in w.\mathsf{H}(s^1_{\text{rf}} \bullet s^2_{\text{rf}})(s)(G(s))$.
- Hence $(h_1, h_3) \in w{\uparrow}.\mathsf{H}(s')(G(s))$.

2) To show: $\psi : w{\uparrow} \to W$

a) To show: $w{\uparrow}.\mathsf{N} = W.\mathsf{N}$

- See (1a).

b) To show: $\forall s_1, s'_1.\ s_1 \sqsubseteq s'_1 \implies \forall s_2 \in \psi(s_1), s'_2 \in \psi(s'_1).\ s_2 \sqsubseteq s'_2$

- Easy to see.

c) To show: $\forall s_1, s'_1.\ s_1 \sqsubseteq_{\text{pub}} s'_1 \implies \forall s_2 \in \psi(s_1), s'_2 \in \psi(s'_1).\ s_2 \sqsubseteq_{\text{pub}} s'_2$

- See (2b).

d) $\forall s_1.\forall s_2 \in \psi(s_1).\ w{\uparrow}.\mathsf{L}(s_1) = W.\mathsf{L}(s_2)$

- See (1c).

e) $\forall s.\forall G \in \text{GK}(w{\uparrow}).\ w{\uparrow}.\mathsf{H}(s)(G(s)) \subseteq \bigcup_{s' \in \psi(s)} W.\mathsf{H}(s')(G(s))$

- Let $s = (s_{\text{rf}}, s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})$ and G be given and suppose $(h_1, h_3) \in w{\uparrow}.\mathsf{H}(s)(G(s))$.
- This implies $s_{\text{rf}} = s^1_{\text{rf}} \bullet s^2_{\text{rf}}$ and $s' \in \psi(s)$ for $s' = (s^1_{\text{rf}}, s^1_{\text{lc}}, s^2_{\text{rf}}, s^2_{\text{lc}})$.
- We will show $(h_1, h_3) \in W.\mathsf{H}(s')(G(s))$.
- We know there are $h^\bullet_1, h'_1, h^\bullet_3, h'_3$ such that:
  - i) $h_1 = h^\bullet_1 \uplus h'_1$
  - ii) $h_3 = h^\bullet_3 \uplus h'_3$
  - iii) $(h^\bullet_1, h^\bullet_3) \in W_{\text{ref}}.\mathsf{H}(s^1_{\text{rf}} \bullet s^2_{\text{rf}})(G(s))$
  - iv) $(h'_1, h'_3) \in w.\mathsf{H}(s^1_{\text{rf}} \bullet s^2_{\text{rf}})(s')(G(s))$.
- From (iv) we further know there are $h^\circ_1, h^{\text{lc}}_1, h^\circ_{2a}, h^{\text{lc}}_{2a}, h^\circ_{2b}, h^{\text{lc}}_{2b}, h^\circ_3, h^{\text{lc}}_3$ such that:
  - v) $h'_1 = h^\circ_1 \uplus h^{\text{lc}}_1$
  - vi) $h^\circ_{2a} \uplus h^{\text{lc}}_{2a} = h^\circ_{2b} \uplus h^{\text{lc}}_{2b}$
  - vii) $h'_3 = h^\circ_3 \uplus h^{\text{lc}}_3$
  - viii) $\text{dom}(h^{\text{lc}}_{2a}) \cap \text{dom}_{[2]}(s^1_{\text{rf}}) = \emptyset \wedge \text{dom}(h^{\text{lc}}_{2b}) \cap \text{dom}_{[1]}(s^2_{\text{rf}}) = \emptyset$
  - ix) $(h^\circ_1, h^\circ_{2a}) \in W_{\text{ref}}.\mathsf{H}(s^1_{\text{rf}} \setminus_{[1]} (s^1_{\text{rf}} \bullet s^2_{\text{rf}}))(G_1)$
  - x) $(h^{\text{lc}}_1, h^{\text{lc}}_{2a}) \in w_1.\mathsf{H}(s^1_{\text{rf}})(s^1_{\text{lc}})(G_1)$
  - xi) $(h^\circ_{2b}, h^\circ_3) \in W_{\text{ref}}.\mathsf{H}(s^2_{\text{rf}} \setminus_{[2]} (s^1_{\text{rf}} \bullet s^2_{\text{rf}}))(G_2)$
  - xii) $(h^{\text{lc}}_{2b}, h^{\text{lc}}_3) \in w_2.\mathsf{H}(s^2_{\text{rf}})(s^2_{\text{lc}})(G_2)$

  where G_i is short for $[W_i.\mathsf{L}(s^i_{\text{rf}}, s^i_{\text{lc}})]^*_{G(s)_{\{i\}}}$.
- We have $\overleftarrow{G}(s') = G(s)$. Thus by Lemmas 104 and 99, we have $\overline{G_1} \bullet \overline{G_2} = \overline{G(s)}$.
- Thus, for each $(\tau, \ell_1, \ell_3) \in s^1_{\text{rf}} \bullet s^2_{\text{rf}}$, we know from (iii) that there is $v_{(\tau,\ell_1,\ell_3)}$ such that $(\tau_{(1)}, h^\bullet_1(\ell_1), v_{(\tau,\ell_1,\ell_3)}) \in \overline{G_1}$ and $(\tau_{(2)}, v_{(\tau,\ell_1,\ell_3)}, h^\bullet_3(\ell_3)) \in \overline{G_2}$.
- Let $h^\bullet_2 := \{\ell \mapsto v_{(\tau,\ell_1,\ell_3)} \mid (\tau_{(1)}, \ell_1, \ell) \in s^1_{\text{rf}} \wedge (\tau_{(2)}, \ell, \ell_3) \in s^2_{\text{rf}}\}$.
- Let $s^\circ_i = s^i_{\text{rf}} \setminus_{[i]} (s^1_{\text{rf}} \bullet s^2_{\text{rf}})$.
- Let $s^\bullet_i = s^i_{\text{rf}} \setminus s^\circ_i$.
- Then we have $(h^\bullet_1, h^\bullet_2) \in W_{\text{ref}}.\mathsf{H}(s^\bullet_1)(G_1)$ and $(h^\bullet_2, h^\bullet_3) \in W_{\text{ref}}.\mathsf{H}(s^\bullet_2)(G_2)$.
- Observe that $s^\circ_i \uplus s^\bullet_i = s^i_{\text{rf}}$.
- Consequently, $(h^\circ_1 \uplus h^\bullet_1, h^\circ_{2a} \uplus h^\bullet_2) \in W_{\text{ref}}.\mathsf{H}(s^1_{\text{rf}})(G_1)$ and $(h^\circ_{2b} \uplus h^\bullet_2, h^\circ_3 \uplus h^\bullet_3) \in W_{\text{ref}}.\mathsf{H}(s^2_{\text{rf}})(G_2)$.

- From (viii), (x) and (xii) we get $(h_1^\circ \uplus h_1^\bullet \uplus h_1^{\mathrm{lc}}, h_{2a}^\circ \uplus h_2^\bullet \uplus h_{2a}^{\mathrm{lc}}) \in W_1.\mathsf{H}(s_{\mathrm{rf}}^1, s_{\mathrm{lc}}^1)(G_1)$ and $(h_{2b}^\circ \uplus h_2^\bullet \uplus h_{2b}^{\mathrm{lc}}, h_3^\circ \uplus h_3^\bullet \uplus h_3^{\mathrm{lc}}) \in W_2.\mathsf{H}(s_{\mathrm{rf}}^2, s_{\mathrm{lc}}^2)(G_2)$.
- By construction of W, this means $(h_1, h_3) = (h_1^\circ \uplus h_1^\bullet \uplus h_1^{\mathrm{lc}}, h_3^\circ \uplus h_3^\bullet \uplus h_3^{\mathrm{lc}}) \in W.\mathsf{H}(s')(G(s))$.

■

Transitivity.

Theorem 108 (Transitivity)**.** $\Delta; \Gamma \vdash e_1 \sim e_3 : \sigma$

Proof: We have $\Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_3 : \tau$ by Lemmas 101 and 107 and Theorem 84. The result then follows from Lemma 106.

■