Transfinite Step-indexing: Decoupling Concrete and Logical Steps **(Technical Appendix)**

Kasper Svendsen, Filip Sieczkowski and Lars Birkedal

October 30, 2015

Contents

1 Complete ordered families of equivalences over ω^2 **1**
1.1 Uniform predicates 2
1.2 Solving Recursive Domain Equations in $\mathcal{U}$ 6

2 Syntax and operational semantics **11**

3 Logical relation **13**
3.1 Compatibility lemmas 16
3.2 Soundness 23
3.3 Example 23

1 Complete ordered families of equivalences over ω^2

Definition 1 (o.f.e.)**.** *An ordered family of equivalence relations (o.f.e.) over ω^2 is a pair $(X, (\overset{a}{=})_{a\in\omega^2})$, consisting of a set X and an ω^2-indexed set of equivalence relations $\overset{a}{=}$, satisfying*

- $\forall x, y \in X.\ x \overset{0,0}{=} y$
- $\forall x, y \in X.\ \forall a, b \in \omega^2.\ a \leq b \wedge x \overset{b}{=} y \Rightarrow x \overset{a}{=} y$
- $\forall x, y \in X.\ (\forall a \in \omega^2.\ x \overset{a}{=} y) \Rightarrow x = y$

Definition 2. *Let $(X, (\overset{a}{=}_X)_{a\in\omega^2})$ and $(Y, (\overset{a}{=}_Y)_{a\in\omega^2})$ be o.f.e's. A function $f : X \to Y$ is* non-expansive *if*

$$\forall x_1, x_2 \in X.\ \forall a \in \omega^2.\ x_1 \overset{a}{=}_X x_2 \Rightarrow f(x_1) \overset{a}{=}_Y f(x_2)$$

and is contractive *if*

$$\forall x_1, x_2 \in X.\ \forall a \in \omega^2.\ (\forall b < a.\ x_1 \overset{b}{=}_X x_2) \Rightarrow f(x_1) \overset{a}{=}_Y f(x_2)$$

Definition 3 (Coherent families and limits)**.** *Let $(X, (\overset{a}{=})_{a\in\omega^2})$ be an o.f.e., I a subset of ω^2 and $(x_a)_{a\in I}$ an I-indexed sequence of elements in X. Then $(x_a)_{a\in I}$ is a coherent family if*

$$\forall a, b \in I.\ a \leq b \Rightarrow x_a \overset{a}{=} x_b$$

An element $x \in X$ is a limit of the sequence $(x_a)_{a\in I}$ if

$$\forall a \in I.\ x \overset{a}{=} x_a$$

Definition 4. *An o.f.e.* $(X, (\overset{a}{=})_{a\in\omega^2})$ *has chosen partial limits iff for any* $b \in \omega^2$ *there exists a function* $\lim_{a<b} x_a$ *that maps a* $b{\downarrow}$*-indexed coherent family* $(x_a)_{a<b}$ *to a limit, such that for any two* $b{\downarrow}$*-indexed coherent families* $(x_a)_{a<b}$ *and* $(y_a)_{a<b}$*,*

$$(\forall a < b.\ x_a \overset{a}{=} y_a) \Rightarrow \lim_{a<b} x_a = \lim_{a<b} y_a$$

Definition 5 (Completeness)**.** *An o.f.e.* $(X, (\overset{a}{=})_{a\in\omega^2})$ *is complete iff all* ω^2*-indexed coherent families have limits and it has chosen partial limits.*

Definition 6 ($\mathcal{U}$)**.** *Let* $\mathcal{U}$ *denote the category of complete ordered family of equivalence relations and non-expansive maps.*

1.1 Uniform predicates

Definition 7 (Uniform predicates, $\mathbf{UPred}(X)$)**.** *A uniform predicate,* $\mathbf{UPred}(X)$*, over a set* X *is defined as*

$$\mathbf{UPred}(X) \overset{def}{=} \{p \in \mathcal{P}(\omega^2 \times X) \mid \forall (a,x) \in p.\ \forall b \le a.\ (b,x) \in p\}$$

with the following A*-indexed equivalence relations:*

$$p \overset{a}{=} q \quad \textit{iff} \quad \lfloor p \rfloor_a = \lfloor q \rfloor_a \qquad\qquad \textit{where} \qquad\qquad \lfloor p \rfloor_a \overset{def}{=} \{(b,x) \in p \mid b < a\}$$

Lemma 1. $\mathbf{UPred}(X)$ *is an o.f.e.*

Proof. The first o.f.e. condition follows from the fact that $\lfloor p \rfloor_{0,0} = \emptyset$ for all $p \in \mathbf{UPred}(X)$. The second o.f.e. condition follows easily from the fact that $\lfloor \lfloor p \rfloor_b \rfloor_a = \lfloor p \rfloor_a$ for all $p \in \mathbf{UPred}(X)$ and $a, b \in \omega^2$ such that $a \le b$. Lastly, the third o.f.e. condition follows easily from the fact that for every $a \in \omega^2$ there exists an $b \in \omega^2$ such that $a < b$. □

Lemma 2. $\mathbf{UPred}(X)$ *has chosen partial limits.*

Proof. Let $b \in \omega^2$ and define $\lim_{-<b}$ as follows:

$$\lim_{a<b} p_a \overset{def}{=} \{(a,x) \in \omega^2 \times X \mid a+1 < b \wedge (a,x) \in p_{a+1}\}$$

Let $(p_a)_{a<b}$ and $(q_a)_{a<b}$ be two coherent families such that $\forall a < b.\ p_a \overset{a}{=} q_a$. To show that $\lim_{a<b} p_a = \lim_{a<b} q_a$ assume $(a,x) \in \lim_{a<c} p_a$. Then $a+1 < c$ and $(a,x) \in p_{a+1}$. Hence, $p_{a+1} \overset{a+1}{=} q_{a+1}$ and thus $(a,x) \in q_{a+1}$. It follows that $(a,x) \in \lim_{a<c} q_a$ as required. $\lim_{a<b} q_a \subseteq \lim_{a<b} p_a$ follows by a symmetric argument.

We also need to show that $\lim_{a<b} p_a \in \mathbf{UPred}(X)$ for a coherent family $(p_a)_{a<b}$. To that end, let $(c,x) \in \lim_{a<b} p_a$ and $d \le c$. By definition, $c+1 < b$ and $(c,x) \in p_{c+1}$. Since p_{c+1} is a uniform predicate, it follows that $(d,x) \in p_{c+1}$. Furthermore, since $d \le c$ it follows that $d+1 \le c+1$ and thus by the coherent property that $p_{d+1} \overset{d+1}{=} p_{c+1}$. Hence, $(d,x) \in p_{d+1}$ and thus $(d,x) \in \lim_{a<b} p_a$ as required.

Lastly, it remains to show that $\lim_{a<b} p_a$ is a limit for a coherent family $(p_a)_{a<b}$. Let $c < b$. To show that $\lfloor \lim_{a<b} p_a \rfloor_c \subseteq \lfloor p_c \rfloor_c$, assume $(d,x) \in \lfloor \lim_{a<b} p_a \rfloor_c$. Then $d < c$, $d+1 < b$ and $(d,x) \in p_{d+1}$. Since $d < c$ it follows that $d+1 \le c$ and thus by the coherent property that $p_{d+1} \overset{d+1}{=} p_c$. Thus, $(d,x) \in p_c$ and $(d,x) \in \lfloor p_c \rfloor_c$. To show that $\lfloor p_c \rfloor_c \subseteq \lfloor \lim_{a<b} p_a \rfloor_c$, assume $(d,x) \in \lfloor p_c \rfloor_c$. Then $d < c$ and $(d,x) \in p_c$. Thus $d+1 \le c$ and by the coherence property that $p_{d+1} \overset{d+1}{=} p_c$. It thus follows that $(d,x) \in p_{d+1}$. Lastly, since $d+1 \le c < b$ we have that $(d,x) \in \lim_{a<b} p_a$. □

Lemma 3. $\mathbf{UPred}(X)$ *has limits of* ω^2*-indexed coherent families.*

Proof. Let $(p_a)_{a\in\omega^2}$ be a coherent family in $\mathbf{UPred}(X)$. Let $\lim_a p_a = \{(a,x) \in \omega^2 \times X \mid (a,x) \in p_{a+1}\}$.

To show that $p \in \mathbf{UPred}(X)$, assume $(a,x) \in p$, $b \leq a$. Hence, by definition of p, $(a,x) \in p_{a+1}$. Since $p_{a+1} \in \mathbf{UPred}(X)$ it follows that $(b,y) \in p_{a+1}$. Since $b \leq a$ it follows that $b+1 \leq a+1$ and thus $p_{b+1} \overset{b+1}{=} p_{a+1}$. Hence, $(b,y) \in p_{b+1}$ and $(b,y) \in \lim_a p_a$.

It thus remains to show that $\lim_a p_a$ is a limit of $(p_a)_{a\in\omega^2}$. Let $b \in \omega^2$. To show that $\lfloor \lim_a p_a \rfloor_b \subseteq \lfloor p_b \rfloor_b$ assume that $(c,x) \in \lfloor \lim_a p_a \rfloor_b$. Then $c < b$ and $(c,x) \in p_{c+1}$. Since $c < b$ it follows that $c+1 \leq b$ and thus $p_{c+1} \overset{c+1}{=} p_b$. Hence, $(c,x) \in p_b$ and $(c,x) \in \lfloor p_b \rfloor_b$, as required. To show that $\lfloor p_b \rfloor_b \subseteq \lfloor \lim_a p_a \rfloor_b$, assume that $(c,x) \in \lfloor p_b \rfloor_b$. Then, $c < b$ and $(c,x) \in p_b$. Since $c < b$ it follows that $c+1 \leq b$ and by coherence, $p_{c+1} \overset{c+1}{=} p_b$. Hence, $(c,x) \in p_{c+1}$ and $(c,x) \in \lim_a p_a$, as required. □

Lemma 4. *The chosen partial limits in* $\mathbf{UPred}(X)$ *respect the partial order* $\subseteq$ *on* $\mathbf{UPred}(X)$*. In particular, for any coherent families* $(p_a)_{a<b}$ *and* $(q_a)_{a<b}$*,*

$$(\forall a < b.\ p_a \subseteq q_a) \Rightarrow \lim_{a<b} p_a \subseteq \lim_{a<b} q_a$$

Proof. Assume $(c,x) \in \lim_{a<b} p_a$. Then $c+1 < b$ and $(c,x) \in p_{c+1} \subseteq q_{c+1}$. Thus, $(c,x) \in \lim_{a<b} q_a$, as required. □

Lemma 5. *Limits in* $\mathbf{UPred}(X)$ *for* ω^2*-indexed coherent families respect the partial order* $\subseteq$ *on* $\mathbf{UPred}(X)$*. In particular, for any coherent families* $(p_a)_{a\in\omega^2}$ *and* $(q_a)_{a\in\omega^2}$*,*

$$(\forall a \in \omega^2.\ p_a \subseteq q_a) \Rightarrow \lim_{a} p_a \subseteq \lim_{a} q_a$$

Lemma 6. $(\mathbf{UPred}(X), \subseteq)$ *is a complete Heyting algebra with meets and joins given by*

$$\bigwedge S \overset{def}{=} \bigcap S = \{(a,x) \in \omega^2 \times X \mid \forall p \in S.\ (a,x) \in p\}$$
$$\bigvee S \overset{def}{=} \bigcup S = \{(a,x) \in \omega^2 \times X \mid \exists p \in S.\ (a,x) \in p\}$$

and implication given by

$$p \Rightarrow q \overset{def}{=} \{(a,x) \mid \forall b \leq a.\ (b,x) \in p \Rightarrow (b,x) \in q\}$$

Constructions

Definition 8. *Let* $\mathcal{X} = (X, (\overset{a}{=}_X)_{a\in\omega^2})$ *and* $\mathcal{Y} = (Y, (\overset{a}{=}_Y)_{a\in\omega^2})$ *be o.f.e. Then the o.f.e. of non-expansive functions* $\mathcal{X} \to_{ne} \mathcal{Y}$ *is defined as follows:*

$$\mathcal{X} \to_{ne} \mathcal{Y} \overset{def}{=} (\{f : X \to Y \mid f \text{ is non-expansive}\}, (\overset{a}{=}_{X\to_{ne}Y})_{a\in\omega^2})$$

where $f \overset{a}{=}_{X\to_{ne}Y} g \overset{def}{=} \forall x \in X.\ f(x) \overset{a}{=}_Y g(x)$.

Lemma 7. *If* $\mathcal{X}$ *and* $\mathcal{Y}$ *are o.f.e.s and* $\mathcal{Y}$ *has chosen partial limits then* $\mathcal{X} \to_{ne} \mathcal{Y}$ *has chosen partial limits.*

Proof. Let $b \in \omega^2$ and define the chosen limits function for a coherent family $(f_a)_{a<b}$,

$$\lim_{a<b} f_a = \lambda x \in X.\ \lim_{a<b} f_a(x)$$

By the definition of $\overset{a}{=}_{X\to_{ne}Y}$ it follows that $(f_a(x))_{a<b}$ is a coherent family in $\mathcal{Y}$ for any $x \in X$ and thus that $\lim_{a<b} f_a$ is well-defined.

To show that $\lim_{a<b} f_a$ is non-expansive and thus an element of $\mathcal{X} \to_{ne} \mathcal{Y}$, assume $x_1 \overset{c}{=} x_2$. If $c < b$ then

$$(\lim_{a<b} f_a)(x_1) = \lim_{a<b} f_a(x_1) \overset{c}{=} f_c(x_1) \overset{c}{=} f_c(x_2) \overset{c}{=} \lim_{a<b} f_a(x_2) = (\lim_{a<b} f_a)(x_2)$$

by non-expansiveness of f_c, as required. If $b \leq c$ then $f_a(x_1) \overset{a}{=} f_a(x_2)$ for all $a \leq b$ and thus,

$$(\lim_{a<b} f_a)(x_1) = \lim_{a<b} f_a(x_1) = \lim_{a<b} f_a(x_2) = (\lim_{a<b} f_a)(x_2)$$

To show that $\lim_{a<b} f_a$ is a limit, let $a \in \omega^2$ such that $a < b$ and $x \in X$. Then,

$$(\lim_{a<b} f_a)(x) = \lim_{a<b} f_a(x) \overset{a}{=} f_a(x) = (f_a)(x)$$

as required.

Lastly, let $(f_a)_{a<b}$ and $(g_a)_{a<b}$ be two coherent families such that

$$\forall a < b.\ f_a \overset{a}{=} g_a$$

To show that $\lim_{a<b} f_a = \lim_{a<b} g_a$, let $x \in X$. Then, it follows that $f_a(x) \overset{a}{=} g_a(x)$ for all $a < b$ and thus

$$(\lim_{a<b} f_a)(x) = \lim_{a<b} f_a(x) = \lim_{a<b} g_a(x) = (\lim_{a<b} g_a)(x)$$

□

Lemma 8. *If $\mathcal{X}$ and $\mathcal{Y}$ are o.f.e.s and $\mathcal{Y}$ has limits for ω^2-indexed coherent families then so does $\mathcal{X} \to_{ne} \mathcal{Y}$.*

Proof. Let $(f_a)_{a\in\omega^2}$ be a coherent family in $\mathcal{X} \to_{ne} \mathcal{Y}$. Define the limit as follows,

$$\lim_a f_a = \lambda x \in X.\ \lim_a f_a(x)$$

This is well-defined as $(f_a(x))_{a\in\omega^2}$ defines a coherent family in $\mathcal{Y}$ for all $x \in X$. To show that $\lim_a f_a$ is non-expansive, assume $x_1 \overset{b}{=} x_2$. Then,

$$(\lim_a f_a)(x_1) = \lim_a f_a(x_1) \overset{b}{=} f_b(x_1) \overset{b}{=} f_b(x_2) \overset{b}{=} \lim_a f_a(x_2) = (\lim_a f_a)(x_2)$$

by non-expansiveness of f_b and the limit property of $\mathcal{Y}$.

Lastly, to show that $\lim_a f_a$ is a limit let $b \in \omega^2$ and $x \in X$. Then

$$(\lim_a f_a)(x) = \lim_a f_a(x) \overset{b}{=} f_b(x) = (f_b)(x)$$

by the limit property of $\mathcal{Y}$. □

Definition 9. *Let $\mathcal{X} = (X, (\overset{a}{=}_X)_{a\in\omega^2})$ and $\mathcal{Y} = (Y, (\overset{a}{=}_Y)_{a\in\omega^2})$ be partially ordered o.f.e.s Then the o.f.e. of monotone non-expansive functions $\mathcal{X} \overset{mon}{\to} \mathcal{Y}$ is defined as follows:*

$$\mathcal{X} \overset{mon}{\to} \mathcal{Y} \overset{def}{=} (\{f : X \overset{mon}{\to} Y \mid f \text{ is non-expansive}\}, (\overset{a}{=}_{X\to_{ne}Y})_{a\in\omega^2})$$

where $f \overset{a}{=}_{X\to_{ne}Y} g \overset{def}{=} \forall x \in X.\ f(x) \overset{a}{=}_Y g(x)$.

Lemma 9. *Let $\mathcal{X}$ and $\mathcal{Y}$ be partially ordered o.f.e.s. If $\mathcal{Y}$ has chosen partial limits such that for any two coherent families $(x_a)_{a<b}$ and $(y_a)_{a<b}$ in $\mathcal{Y}$ such that*

$$(\forall a < b.\ x_a \leq_Y y_a) \Rightarrow \lim_{a<b} x_a \leq_Y \lim_{a<b} y_a$$

then $\mathcal{X} \overset{mon}{\to} \mathcal{Y}$ has chosen partial limits.

Proof. Let $b \in \omega^2$ and define the chosen limits function as follows for a coherent family $(f_a)_{a<b}$,

$$\lim_{a<b} f_a = \lambda x \in X.\ \lim_{a<b} f_a(x)$$

We need to show that $\lim_{a<b} f_a$ is monotone. Thus, assume $x_1 \leq_X x_2$. Then by monotonicity of f_a it follows that $f_a(x_1) \leq_Y f_a(x_2)$ for all $a < b$. Thus, by assumption $\lim_{a<b} f_a(x_1) \leq_Y \lim_{a<b} f_a(x_2)$, as required.

The proof that $\lim_{a<b} f_a$ is well-defined, a limit and sufficiently unique is the same as in Lemma 8. □

Lemma 10. *Let $\mathcal{X}$ and $\mathcal{Y}$ be partially ordered o.f.e.s. If $\mathcal{Y}$ has limits for all ω^2-indexed coherent families such that for any two coherent families $(x_a)_{a\in\omega^2}$ and $(y_a)_{a\in\omega^2}$ in $\mathcal{Y}$ such that*

$$(\forall a.\ x_a \leq_Y y_a) \Rightarrow \lim_a x_a \leq_Y \lim_a y_a$$

then $\mathcal{X} \overset{mon}{\to} \mathcal{Y}$ has limits for all ω^2-indexed coherent families.

Definition 10. *Let X be a set. Then $\Delta(X) = (X, (\overset{a}{=})_{a\in\omega^2})$ where $\overset{0,0}{=}$ is the total relation and $\overset{n,m}{=}$ is the identity for $(n, m) \neq (0, 0)$.*

Lemma 11. *$\Delta(X)$ is a c.o.f.e. for any non-empty set X.*

Proof. The proof that $\Delta(X)$ is an o.f.e. is trivial. To show that $\Delta(X)$ has chosen partial limits, let $(x_a)_{a<b}$ be a coherent family in $\Delta(X)$ and pick an element $x \in X$. Now, define

$$\lim_{a<b} x_a = \begin{cases} x & \text{if } b = (0,0) \text{ or } b = (0,1) \\ x_{(0,1)} & \text{if } b > (0,1) \end{cases}$$

If $b = (0, 0)$ this is vacuously a limit as $a \not< b$ for all a. If $b = (0, 1)$ this is also vacuously a limit as $\overset{0,0}{=}$ is the total relation. Lastly, if $b > (0, 1)$ this is vacuously a limit as $x_{(0,1)} = x_a$ for all $(0, 1) \leq a < b$ by the coherence property. Furthermore, for any two coherent families $(x_a)_{a<b}$ and $(y_a)_{a<b}$ such that $x_a \overset{a}{=} y_a$ for all $a < b$ we clearly have that $\lim_{a<b} x_a = \lim_{a<b} y_a$.

Finally, $\Delta(X)$ obviously has limits for all ω^2-indexed coherent families, by taking the limit of $(x_a)_{a\in\omega^2}$ to be $x_{(0,1)}$. □

Definition 11 (Locally non-expansive and locally contractive functor)**.** *A bi-functor $F : \mathcal{U}^{op} \times \mathcal{U} \to \mathcal{U}$ is locally non-expansive iff*

$$\forall \mathcal{X}, \mathcal{X}', \mathcal{Y}, \mathcal{Y}' \in obj(\mathcal{U}).\ \forall f, f' : Hom_{\mathcal{U}}(\mathcal{X}, \mathcal{X}').\ \forall g, g' : Hom_{\mathcal{U}}(\mathcal{Y}', \mathcal{Y}).$$
$$\forall a \in \omega^2.\ f \overset{a}{=} f' \wedge g \overset{a}{=} g' \Rightarrow F(f, g) \overset{a}{=} F(f', g')$$

and locally contractive iff

$$\forall \mathcal{X}, \mathcal{X}', \mathcal{Y}, \mathcal{Y}' \in obj(\mathcal{U}).\ \forall f, f' : Hom_{\mathcal{U}}(\mathcal{X}, \mathcal{X}').\ \forall g, g' : Hom_{\mathcal{U}}(\mathcal{Y}', \mathcal{Y}).$$
$$\forall a \in \omega^2.\ (\forall b \in \omega^2.\ b < a \Rightarrow f \overset{b}{=} f' \wedge g \overset{b}{=} g') \Rightarrow F(f, g) \overset{a}{=} F(f', g')$$

Definition 12 (▶)**.** *Let $\blacktriangleright : \mathcal{U} \to \mathcal{U}$ denote the following functor,*

$$\blacktriangleright\left(X, (\overset{a}{=})_{a\in\omega^2})\right) \overset{def}{=} \left(X, (\overset{a}{\equiv})_{a\in\omega^2}\right) \qquad \blacktriangleright(f) \overset{def}{=} f$$

where $\overset{0,0}{\equiv}$ is the total relation on X, $\overset{n,m+1}{\equiv}$ is $\overset{n,m}{=}$ and $\overset{n+1,0}{\equiv}$ is defined as follows

$$x_1 \overset{n+1,0}{\equiv} x_2 \quad \textit{iff} \quad \forall m \in \mathbb{N}.\ x_1 \overset{n,m}{=} x_2$$

Lemma 12. *If $F : \mathcal{U}^{op} \times \mathcal{U} \to \mathcal{U}$ is locally non-expansive then $\blacktriangleright \circ F$ is locally contractive.*

Proof. Let $a \in \omega^2$, $f, f' \in Hom_{\mathcal{U}}(\mathcal{X}, \mathcal{X}')$ and $g, g' \in Hom_{\mathcal{U}}(\mathcal{Y}', \mathcal{Y})$ such that

$$\forall b \in \omega^2.\ b < a \Rightarrow f \overset{b}{=} f' \wedge g \overset{b}{=} g'$$

By local non-expansiveness of F it follows that

$$\forall b \in \omega^2.\ b < a \Rightarrow F(f,g) \overset{b}{=}_{F(\mathcal{X}',\mathcal{Y}') \to_{ne} F(\mathcal{X},\mathcal{Y})} F(f',g')$$

To show that $F(f,g) \overset{a}{=}_{\blacktriangleright F(\mathcal{X}',\mathcal{Y}') \to_{ne} \blacktriangleright F(\mathcal{X},\mathcal{Y})} F(f',g')$ take an $x \in |\blacktriangleright F(\mathcal{X}',\mathcal{Y}')|$. By definition of $\blacktriangleright$ to show that $F(f,g)(x) \overset{a}{=}_{\blacktriangleright F(\mathcal{X},\mathcal{Y})} F(f',g')(x)$ it suffices to prove that $F(f,g)(x) \overset{b}{=}_{F(\mathcal{X},\mathcal{Y})} F(f',g')(x)$ for all $b < a$. This follows easily from the assumption. □

1.2 Solving Recursive Domain Equations in $\mathcal{U}$

In this section we give the explicit construction of a solution of recursive domain equations in the category of cofes indexed over ω^2. We proceed by building a fixed-point of a locally contractive bifunctor $F : (\mathcal{U}^{op} \times \mathcal{U}) \to \mathcal{U}$.

The construction will proceed in two stages. First, we will construct *partial* limits that are indistinguishable for *logical* steps (this construction is analogous to the construction of the solution in ω-indexed spaces), and afterwards we will use these to construct the overall fixed-point of the functor.

Lemma 13 (partial limits)**.** *For any space $S \in \mathcal{U}$, a natural number n and two functions $p_S : F(S,S) \to S$ and $e_S : S \to F(S,S)$ such that $p_S \circ e_S = \mathrm{id}_S$ and $e_S \circ p_S \overset{n,0}{=} \mathrm{id}_{F(S,S)}$, there exists a space $X \in \mathcal{U}$ and maps $p_X : F(X,X) \to X$ and $e_X : X \to F(X,X)$ such that $p_X \circ e_X = \mathrm{id}_X$ and $e_X \circ p_X \overset{n,m}{=} \mathrm{id}_{F(X,X)}$ for any m. Additionally, there are maps $\pi_X : X \to S$ and $\iota_X : S \to X$ such that $\pi_X \circ \iota_X = \mathrm{id}_S$ and $\iota_X \circ \pi_X \overset{n,0}{=} \mathrm{id}_X$, and that $\pi_X \circ p_X = p_S \circ F(\iota_X, \pi_X)$.*

Proof. The proof follows the outline of the construction of the solution for the ω-indexed cofes. We begin by constructing F_i, together with projections $p_i : F_{i+1} \to F_i$ and embeddings $e_i : F_i \to F_{i+1}$ as:

$$\begin{array}{lll} F_0 = S & p_0 = p_S & e_0 = e_S \\ F_{k+1} = F(F_k, F_k) & p_{k+1} = F(e_k, p_k) & e_{k+1} = F(p_k, e_k) \end{array}$$

First, we claim that the properties of p_S and e_S extend to the whole sequence:

$$\forall k.\ p_k \circ e_k = \mathrm{id}_{F_k} \tag{1}$$

$$\forall k.\ e_k \circ p_k \overset{n,k}{=} \mathrm{id}_{F_{k+1}} \tag{2}$$

We prove these properties by induction. For (1), the base case holds by our assumption, while for the inductive step we have:

$$p_{k+1} \circ e_{k+1} = F(e_k, p_k) \circ F(p_k, e_k) = F(p_k \circ e_k, p_k \circ e_k) \overset{IH}{=} F(\mathrm{id}_{F_k}, \mathrm{id}_{F_k}) = \mathrm{id}_{F_{k+1}}\ .$$

Similarly, for (2) the base case we already assumed. For the inductive step, we proceed similarly:

$$e_{k+1} \circ p_{k+1} = F(p_k, e_k) \circ F(e_k, p_k) = F(e_k \circ p_k, e_k \circ p_k) \overset{n,k+1}{=} F(\mathrm{id}_{F_{k+1}}, \mathrm{id}_{F_{k+1}}) = \mathrm{id}_{F_{k+2}},$$

where the crucial $(n, k+1)$-equality holds by induction hypthesis (for (n,k) on the arguments) and local contractiveness of F.

We can define a helpful, iterated versions of projections and embeddings, written $p_k^l : F_{k+l} \to F_k$ and $e_k^l : F_k \to F_{k+l}$, as

$$\begin{aligned} p_k^0 &= \mathrm{id}_{F_k} & e_k^0 &= \mathrm{id}_{F_k} \\ p_k^{l+1} &= p_k^l \circ p_{k+l} & e_k^{l+1} &= e_{k+l} \circ e_k^l. \end{aligned}$$

We immediately get the following observations:

$$\forall k, l.\ p_k^l \circ e_k^l = \mathrm{id}_{F_k} \tag{3}$$

$$\forall k, l.\ e_k^l \circ p_k^l \overset{n,k}{=} \mathrm{id}_{F_{k+l}}\ . \tag{4}$$

Now we are ready to define X. Let

$$X = \left\{ x \in \prod_{k \in \mathbb{N}} F_k \;\middle|\; \forall k.\ x_k = p_k(x_{k+1}) \right\},$$

with equality defined pointwise, i.e., $x \overset{p}{=}_X x'$ *iff* $\forall k.\ x_k \overset{p}{=}_{F_k} x'_k$, for $p \in \omega^2$. Clearly, X is and object of $\mathcal{U}$.

We can now extend projections and embeddings to X: we define $\pi_k : X \to F_k$ and $\iota_k : F_k \to X$ as

$$\pi_k(x) = x_k \qquad\qquad (\iota_k(s))_i = \begin{cases} e_k^{i-k}(s) & \text{if } i \geq k \\ p_i^{k-i}(s) & \text{if } i \leq k \end{cases}$$

Again we can use (3) to show that both these maps are well-defined.

Now we are finally ready to define the maps p_X and e_X. We take

$$(p_X(z))_k = p_k(F(\iota_k, \pi_k)(z)) \qquad\qquad e_X(x) = \lim_{k \in \mathbb{N}} F(\pi_k, \iota_k)(e_k x_k)$$

First, we need to check that these maps are well-defined. For p_X, this amounts to checking that $p_X(z) \in X$, since it is clearly non-expansive. Thus, we have

$$\begin{aligned} p_k((p_X(z))_{k+1}) = p_k(p_{k+1}(F(\iota_{k+1}, \pi_{k+1})(z))) = p_k(F(e_k, p_k)F(\iota_{k+1}, \pi_{k+1})(z)) = \\ p_k(F(\iota_{k+1} \circ e_k, p_k \circ \pi_{k+1})(z)) = p_k(F(\iota_k, \pi_k)(z)) = (p_X(z))_k, \end{aligned}$$

where the identities $\iota_{k+1} \circ e_k = \iota_k$ and $p_k \circ \pi_{k+1} = p_k$ are easy to check.

For e_X, we need to check that the limit actually exists. Since we are working in $\mathcal{U}$, it is enough to show that the chain is Cauchy: we proceed by showing that $F(\pi_k, \iota_k)(e_k x_k) \overset{n,k+1}{=} F(\pi_{k+1}, \iota_{k+1})(e_{k+1} x_{k+1})$, with the Cauchy condition (up to n) following by simple induction. We have:

$$\begin{aligned} F(\pi_{k+1}, \iota_{k+1})(e_{k+1} x_{k+1}) \overset{n,k+1}{=} F(e_k \circ \pi_k, \iota_k \circ p_k)(e_{k+1} x_{k+1}) = F(\pi_k, \iota_k)(F(e_k, p_k)(e_{k+1} x_{k+1})) = \\ F(\pi_k, \iota_k)(p_{k+1}(e_{k+1} x_{k+1})) = F(\pi_k, \iota_k)(x_{k+1}) \overset{n,k+1}{=} F(\pi_k, \iota_k)(e_k(p_k(x_{k+1}))) = F(\pi_k, \iota_k)(e_k x_k). \end{aligned}$$

The $(n, k+1)$-equalities follow ultimately (easy check) from $e_k \circ p_k \overset{n,k}{=} \mathrm{id}$, (2) and contractiveness of F. Like with p_X, it is an easy check that e_X is non-expansive.

Finally, we can prove the two required properties: $p_X \circ e_X = \mathrm{id}_X$, and $\forall m.\ e_X \circ p_X \overset{n,m}{=} \mathrm{id}_{F(X,X)}$. For the first one, we compute as follows:

$$p_X(e_X(x))_k = p_k(F(\iota_k, \pi_k)(\lim_{m \in \mathbb{N}} F(\pi_m, \iota_m)(e_m x_m))) = p_k \lim_{m \in \mathbb{N}} F(\pi_{m+k} \circ \iota_k, \pi_k \circ \iota_{m+k})(e_{m+k} x_{m+k}),$$

where we only considered the tail of the chain past its k-th element in the second equation, and used the fact that nonexpansive maps preserve limits. Since, as it is easy to check, $\pi_{k+m} \circ \iota_k = e_k^m$, $\pi_k \circ \iota m + k = p_k^m$ and $F(e_k^m, p_k^m) = p_{k+1}^m$, we get:

$$\begin{aligned} p_k \lim_{m \in \mathbb{N}} F(\pi_{m+k} \circ \iota_k, \pi_k \circ \iota_{m+k})(e_{m+k} x_{m+k}) = p_k \lim_{m \in \mathbb{N}} F(e_k^m, p_k^m)(e_{k+m} x_{k+m}) = \\ p_k \lim_{m \in \mathbb{N}} p_{k+1}^m(e_{k+m} x_{k+m}) = p_k \lim_{m \in \mathbb{N}} x_{k+1} = p_k(x_{k+1}) = x_k \end{aligned}$$

For the other direction, we want to show that for any m and z, $e_X(p_X(z)) \overset{n,m}{=} z$. Unfolding the definitions, we get

$$e_X(p_X(z)) = \lim_{k\in\mathbb{N}}(F(\pi_k, \iota_k) \circ e_k \circ p_k \circ F(\iota_k, \pi_k))(z)$$

It suffices to show that k-th element of this chain is (n, k)-equal to z: then by the similarity of chains their limits will be (n, m)-equal for any m. Thus, we have

$$F(\pi_k, \iota_k) \circ e_k \circ p_k \circ F(\iota_k, \pi_k) \overset{n,k}{=} F(\pi_k, \iota_k) \circ F(\iota_k, \pi_k) = F(\iota_k \circ \pi_k, \iota_k \circ \pi_k) \overset{n,k}{=} F(\mathrm{id}_X, \mathrm{id}_X) = \mathrm{id}_X$$

The first of the (n, k)-equal steps follows by (2), while the second follows from $\iota_k \circ \pi_k \overset{n,k}{=} \mathrm{id}_X$, which in turn depends on (4).

Finally, we take $\pi_X = \pi_0$ and $\iota_X = \iota_0$; the properties follow trivially from the definition and (4), while the final property is exactly the definition of p_X at index 0. □

Theorem 1 (solutions of recursive domain equations)**.** *For any locally contractive functor $F : (\mathcal{U} \times \mathcal{U}) \to \mathcal{U}$ such that $F(1, 1)$ is inhabited (by $*_{F(1,1)}$) there exists a space $X : \mathcal{U}$ such that $X \cong F(X, X)$.*

Proof. The idea behind the construction is to iterate the construction from Lemma 13 to construct a tower of progressively closer approximations of the solution, and then to construct a limit of it. To this end, we write $\mathcal{G}(S, p_S, e_S)$ to denote the construction of the lemma, i.e., a quintuple $(X, p_X, e_X, \pi_X, \iota_X)$ whose existence the lemma shows.

Next, we proceed with the construction of a sequence of spaces $(X_i : \mathcal{U})_{i\in\mathbb{N}}$ together with maps $\pi_i : X_{i+1} \to X_i$, $\iota_i : X_i \to X_{i+1}$, $p_i : F(X_i, X_i) \to X_i$ and $e_i : X_i \to F(X_i, X_i)$. First, let

$$(X_0, p_0, e_0, \_, \_) = \mathcal{G}(1, !_{F(1,1)}, *_1 \mapsto *_{F(1,1)}),$$

where $!_{F(1,1)} : F(1, 1) \to 1$ is the unique map into the unit type. Next, we proceed by induction, taking:

$$(X_{n+1}, p_{n+1}, e_{n+1}, \pi^\circ_n, \iota^\circ_n) = \mathcal{G}(F(X_n, X_n), F(e_n, p_n), F(p_n, e_n)),$$

and setting $\pi_n = p_n \circ \pi^\circ_n$, $\iota_n = \iota^\circ_n \circ e_n$.

In order for this definition to be valid, we have to check several properties. Firstly, for the first application of $\mathcal{G}$, we need $!_{F(1,1)} \circ (*_1 \mapsto *_{F(1,1)}) = \mathrm{id}_1$, which holds trivially, and $(*_1 \mapsto *_{F(1,1)}) \circ !_{F(1,1)} \overset{0,0}{=} \mathrm{id}_{F(1,1)}$, which also holds trivially, since any two objects are $(0, 0)$-equal.

Next, we need to check that these conditions also hold for the inductive step. We have

$$F(e_n, p_n) \circ F(p_n, e_n) = F(p_n \circ e_n, p_n \circ e_n) = F(\mathrm{id}_{X_n}, \mathrm{id}_{X_n}) = \mathrm{id}_{F(X_n,X_n)},$$

where we use the fact that $p_n \circ e_n = \mathrm{id}_{X_n}$, which comes from Lemma 13. Similarly, we have

$$F(p_n, e_n) \circ F(e_n, p_n) = F(e_n \circ p_n, e_n \circ p_n) \overset{n+1,0}{=} F(\mathrm{id}_{F(X_n,X_n)}, \mathrm{id}_{F(X_n,X_n)}) = \mathrm{id}_{F(F(X_n,X_n),F(X_n,X_n))}\ .$$

Here, the crucial $(n+1, 0)$-equivalence comes from local contractiveness of F: it means we only need to show that $e_n \circ p_n \overset{n,m}{=} \mathrm{id}_{F(X_n,X_n)}$ for any m, which is precisely what Lemma 13 gives us.

Finally, we also check that $\pi_n : X_{n+1} \to X_n$ and $\iota_n : X_n \to X_{n+1}$. The construction gives us $\pi^\circ_n : X_{n+1} \to F(X_n, X_n)$, so the composition $p_n \circ \pi^\circ_n$ indeed has the right type; similarly for ι_n. We claim that

$$\forall n.\ \pi_n \circ \iota_n = \mathrm{id}_{X_n} \tag{5}$$

$$\forall n.\ \iota_n \circ \pi_n \overset{n,0}{=} \mathrm{id}_{X_{n+1}}, \tag{6}$$

which is easily checked by unfolding the definitions and using properties of p_n, e_n, π°_n and ι°_n. Furthermore, we prove an additional claims, and its two simple corrolaries

$$\forall n.\ F(\iota_n, \pi_n) = \pi^\circ_n \circ p_{n+1} \tag{7}$$

$$\forall n.\ \pi_n \circ p_{n+1} = p_n \circ F(\iota_n, \pi_n) \tag{8}$$

$$\forall n.\ F(\iota_n, \pi_n) \circ e_{n+1} = \pi^\circ_n \tag{9}$$

The first property, which is a restatement of the final property of Lemma 13 is proved as follows:

$$F(\iota_n, \pi_n) = F(\iota_n^\circ \circ e_n, p_n \circ \pi_n^\circ) = F(e_n, p_n) \circ F(\iota_n^\circ, \pi_n^\circ) = \pi_n^\circ \circ p_{n+1},$$

where the last equality is the direct application of the property from the lemma with the definitions used in the inductive step of the construction. The two corollaries follow using definitions and, in the second case, (5).

As for the previous construction, we define iterated versions of π and ι:

$$\begin{aligned} \pi_n^0 &= \mathrm{id}_{X_n} & \iota_n^0 &= \mathrm{id}_{X_n} \\ \pi_n^{k+1} &= \pi_n^k \circ \pi_{n+k} & \iota_n^{k+1} &= \iota_{n+k} \circ \iota_n^k, \end{aligned}$$

and prove, by simple induction, the iterated versions of properties:

$$\forall n, k.\ \pi_n^k \circ \iota_n^k = \mathrm{id}_{X_n} \tag{10}$$

$$\forall n, k.\ \iota_n^k \circ \pi_n^k \overset{n,0}{=} \mathrm{id}_{X_{n+k}} \tag{11}$$

Now we can construct what we claim to be the fixed-point of the recursive domain equation. We take $X \in \mathcal{U}$ as:

$$X = \left\{ x \in \prod_{n \in \mathbb{N}} X_n \;\middle|\; \forall k.\ x_k = \pi_k(x_{k+1}) \right\},$$

again, with equality defined pointwise.

Similarly to the previous construction, we extend the projections and embeddings to X: we define $\pi_k^X : X \to X_k$ and $\iota_k^X : X_k \to X$ as

$$\pi_k^X(x) = x_k \qquad\qquad (\iota_k^X(s))_i = \begin{cases} \iota_k^{i-k}(s) & \text{if } i \geq k \\ \pi_k^{k-i}(s) & \text{if } i \leq k \end{cases}$$

Finally, we can define $p_X : F(X, X) \to X$ and $e_X : X \to F(X, X)$. We take

$$(p_X(z))_k = p_k(F(\iota_k^X, \pi_k^X)(z)) \qquad\qquad e_X(x) = \lim_{k \in \mathbb{N}} F(\pi_k^X, \iota_k^X)(e_k(x_k))$$

First, we check that these maps are well-defined. For p_X, we only need to show that $p_X(z) \in X$. We compute

$$\begin{aligned} &\pi_k((p_X(z))_{k+1}) = \pi_k(p_{k+1}(F(\iota_{k+1}^X, \pi_{k+1}^X)(z))) = p_k(F(\iota_k, \pi_k)(F(\iota_{k+1}^X, \pi_{k+1}^X)(z))) = \\ &\quad p_k(F(\iota_{k+1}^X \circ \iota_k, \pi_k \circ \pi_{k+1}^X)) = p_k(F(\iota_k^X, \pi_k^X)(z)) = (p_X(z))_k. \end{aligned}$$

In the computation above, the identities $\iota_k^X = \iota_{k+1}^X \circ \iota_k$ and $\pi_k \circ \pi_{k+1}^X = \pi_k^X$ are easy to check, and the remaining one needed is (8).

In order for e_X to be well-defined, we need to check that the limit exists. To this end, it is enough to show that the sequence is Cauchy: we are going to show that $F(\pi_k^X, \iota_k^X)(e_k(x_k)) \overset{k,0}{=} F(\pi_{k+1}^X, \iota_{k+1}^X)(e_{k+1}(x_{k+1}))$. We have:

$$F(\pi_{k+1}^X, \iota_{k+1}^X)(e_{k+1}(x_{k+1})) \overset{k,0}{=} F(\iota_k \circ \pi_k^X, \iota_k^X \circ \pi_k)(e_{k+1}(x_{k+1})) = F(\pi_k^X, \iota_k^X)(F(\iota_k, \pi_k)(e_{k+1}(x_{k+1}))),$$

where the $(k, 0)$-equality follows from contractiveness and (6). By (9) we have $F(\iota_k, \pi_k) \circ e_{k+1} = \pi_k^\circ$, and so

$$F(\pi_k^X, \iota_k^X)(F(\iota_k, \pi_k)(e_{k+1}(x_{k+1}))) = F(\pi_k^X, \iota_k^X)(\pi_k^\circ(x_{k+1})) \overset{k,0}{=} F(\pi_k^X, \iota_k^X)((e_k \circ p_k \circ \pi_k^\circ)(x_{k+1})) = F(\pi_k^X, \iota_k^X)(e_k(x_k)).$$

We now turn to showing that p_X and e_X form an isomorphism. First, we claim that $p_X(e_X(x)) = x$. To show this, we pick an index k and compute:

$$\begin{aligned} &p_X(e_X(x))_k = p_k(F(\iota_k^X, \pi_k^X) \lim_{n \in \mathbb{N}} F(\pi_n^X, \iota_n^X)(e_n(x_n))) = \lim_{n \in \mathbb{N}} (p_k \circ F(\iota_k^X, \pi_k^X) \circ F(\pi_{k+n}^X, \iota_{k+n}^X) \circ e_{k+n})(x_{k+n}) = \\ &\quad \lim_{n \in \mathbb{N}} (p_k \circ F(\pi_{k+n}^X \circ \iota_k^X, \pi_k^X \circ \iota_{k+n}^X) \circ e_{k+n})(x_{k+n}) = \lim_{n \in \mathbb{N}} (p_k \circ F(\iota_k^n, \pi_k^n) \circ e_{n+k})(x_{n+k}) = \\ &\quad \lim_{n \in \mathbb{N}} (\pi_k^n \circ p_{n+k} \circ e_{n+k})(x_{n+k}) = \lim_{n \in \mathbb{N}} \pi_k^n(x_{n+k}) = \lim x_k = x_k \end{aligned}$$

The identities $\pi^X_{n+k} \circ \iota^X_k = \iota^n_k$ and $\pi^X_k \circ \iota^X_{n+k} = \pi^n_k$ are easy to check and analogous to the case in Lemma 13. The remaining identity $p_k \circ F(\iota^n_k, \pi^n_k) = \pi^n_k \circ p_{k+n}$ we prove by induction on n as follows. The base case holds trivially, since $\iota^0_k = \pi^0_k = \mathrm{id}_{X_k}$. For the inductive case, we have

$$p_k \circ F(\iota^{n+1}_k, \pi^{n+1}_k) = p_k \circ F(\iota^n_k \circ \iota_{k+n}, \pi_{k+n} \circ \pi^n_k) = p_k \circ F(\iota^n_k, \pi^n_k) \circ F(\iota_{k+n}, \pi_{k+n}) =$$
$$\pi^n_k \circ p_{k+n} \circ F(\iota_{k+n}, \pi_{k+n}) = \pi^n_k \circ \pi_{k+n} \circ p_{k+n+1} = \pi^{n+1}_k \circ p_{k+n+1},$$

where the second-to-last equality follows by (8).

We are left with the final obligation, showing that $e_X(p_X(z)) = z$. To this end we show that

$$e_X(p_X(z)) = \lim_{n\in\mathbb{N}}(F(\pi^X_k, \iota^X_k) \circ e_k \circ p_k \circ F(\iota^X_k, \pi^X_k))(z) = \lim_{n\in\mathbb{N}} z = z.$$

We show that the two chains under the limit approximate each other, at progressively greater, unbounded ordinals, and so the limits are equal. Precisely, we show that k-th elements of the chain are $(k, 0)$ equal:

$$F(\pi^X_k, \iota^X_k) \circ e_k \circ p_k \circ F(\iota^X_k, \pi^X_k) \overset{k,0}{=} F(\pi^X_k, \iota^X_k) \circ F(\iota^X_k, \pi^X_k) = F(\iota^X_k \circ \pi^X_k, \iota^X_k \circ \pi^X_k) \overset{k,0}{=} F(\mathrm{id}_X, \mathrm{id}_X) = \mathrm{id}_{F(X,X)}\ .$$

Similarly to the first construction, the first $(k, 0)$-equality follows from (6), and the second — from (11). □

2 Syntax and operational semantics

$$
\begin{array}{rcl}
\tau, \sigma & ::= & 1 \mid \tau \times \sigma \mid \tau \to \sigma \mid \tau \ \mathit{ref} \mid \exists \alpha.\ \tau \mid \alpha \\
\Delta & ::= & \Delta, \alpha \mid \varepsilon \\
\Gamma & ::= & \Gamma, x : \tau \mid \varepsilon
\end{array}
$$

$$
\begin{array}{rcl}
v \in \mathit{Val} & ::= & * \mid \mathit{fix}\ f(x).\ e \mid l \mid \mathit{pack}\ v \mid (v_1, v_2) \\
e \in \mathit{Exp} & ::= & v \mid e_1\ e_2 \mid (e_1, e_2) \mid \mathit{fst}\ e \mid \mathit{snd}\ e \\
& \mid & !\, e \mid e_1 := e_2 \mid \mathit{ref}\ e \\
& \mid & \mathit{pack}\ e \mid \mathit{unpack}\ e_1\ \mathit{as}\ x\ \mathit{in}\ e_2 \\
K \in \mathit{ECtx} & ::= & \bullet \mid K\ e \mid v\ K \mid (K, e) \mid (v, K) \mid \mathit{fst}\ K \mid \mathit{snd}\ K \\
& \mid & !\, K \mid K := e \mid v := K \mid \mathit{ref}\ K \\
& \mid & \mathit{pack}\ K \mid \mathit{unpack}\ K\ \mathit{as}\ x\ \mathit{in}\ e
\end{array}
$$

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

$$\frac{}{\Delta \vdash 1} \qquad \frac{\Delta \vdash \tau \qquad \Delta \vdash \sigma}{\Delta \vdash \tau \times \sigma} \qquad \frac{\Delta \vdash \tau \qquad \Delta \vdash \sigma}{\Delta \vdash \tau \to \sigma} \qquad \frac{\Delta \vdash \tau}{\Delta \vdash \tau\ \ \mathit{ref}} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \exists \alpha.\ \tau} \qquad \frac{}{\Delta, \alpha \vdash \alpha}$$

$$\frac{\Delta \vdash \tau}{\Delta; \Gamma, x : \tau \vdash x : \tau} \qquad \frac{}{\Delta; \Gamma \vdash * : 1} \qquad \frac{\Delta; \Gamma, f : \tau \to \sigma, x : \tau \vdash e : \sigma}{\Delta; \Gamma \vdash \mathit{fix}\ f(x).\ e : \tau \to \sigma} \qquad \frac{\Delta; \Gamma \vdash e_1 : \tau \to \sigma \qquad \Delta; \Gamma \vdash e_2 : \tau}{\Delta; \Gamma \vdash e_1\ e_2 : \sigma}$$

$$\frac{\Delta; \Gamma \vdash e : \tau\ \mathit{ref}}{\Delta; \Gamma \vdash !\, e : \tau} \qquad \frac{\Delta; \Gamma \vdash e_1 : \tau\ \mathit{ref} \qquad \Delta; \Gamma \vdash e_2 : \tau}{\Delta; \Gamma \vdash e_1 := e_2 : 1} \qquad \frac{\Delta; \Gamma \vdash e : \tau}{\Delta; \Gamma \vdash \mathit{ref}\ e : \tau\ \mathit{ref}} \qquad \frac{\Delta; \Gamma \vdash e : \sigma[\tau/\alpha]}{\Delta; \Gamma \vdash \mathit{pack}\ e : \exists \alpha.\ \sigma}$$

$$\frac{\Delta; \Gamma \vdash e_1 : \exists \alpha.\ \tau \qquad \Delta, \alpha; \Gamma, x : \tau \vdash e_2 : \sigma \qquad \Delta \vdash \sigma}{\Delta; \Gamma \vdash \mathit{unpack}\ e_1\ \mathit{as}\ x\ \mathit{in}\ e_2 : \sigma} \qquad \frac{\Delta; \Gamma \vdash e_1 : \tau \qquad \Delta; \Gamma \vdash e_2 : \sigma}{\Delta; \Gamma \vdash (e_1, e_2) : \tau \times \sigma} \qquad \frac{\Delta; \Gamma \vdash e : \tau \times \sigma}{\Delta; \Gamma \vdash \mathit{fst}\ e : \tau}$$

$$\frac{\Delta; \Gamma \vdash e : \tau \times \sigma}{\Delta; \Gamma \vdash \mathit{snd}\ e : \sigma}$$

Operational semantics $\boxed{e, h \to e', h'}$

EvalFix

$$\frac{}{(\mathit{fix}\ f(x).\ e)\ v, h \to e[\mathit{fix}\ f(x).\ e/f, v/x], h}$$

EvalUnpack

$$\frac{}{\mathit{unpack}\ (\mathit{pack}\ v)\ \mathit{as}\ x\ \mathit{in}\ e, h \to e[v/x], h}$$

EvalRead

$$\frac{l \in \mathit{dom}(h)}{!\, l, h \to h(l), h}$$

EvalWrite

$$\frac{l \in \mathit{dom}(h)}{l := v, h \to *, h[l \mapsto v]}$$

EvalAlloc

$$\frac{l \notin \mathit{dom}(h)}{\mathit{ref}\ v, h \to l, h[l \mapsto v]}$$

EvalFst

$$\frac{}{\mathit{fst}\ (v_1, v_2), h \to v_1, h}$$

EvalSnd

$$\frac{}{\mathit{snd}\ (v_1, v_2), h \to v_2, h}$$

EvalCtx

$$\frac{e, h \to e', h'}{K[e], h \to K[e'], h'}$$

and

$$\frac{}{e, h \to^0 e, h} \qquad \frac{e, h \to e', h' \qquad e', h' \to^n e'', h''}{e, h \to^{n+1} e'', h''}$$

Lemma 14. *If* $K[e], h \to^i e', h' \not\to$ *then there exists* i_1, i_2, e'' *and* h'' *such that*

$$e, h \to^{i_1} e'', h'' \not\to \qquad\qquad K[e''], h'' \to^{i_2} e', h' \not\to \qquad\qquad i = i_1 + i_2$$

Proof. By induction on i.

If $i = 0$ then take $i_1 = i_2 = 0$, $e'' = e$ and $h'' = h$. Otherwise, $K[e], h \to e'', h''$ and $e'', h'' \to^{i-1} e', h' \not\to$. If $K = \bullet$ then we simply take $i_1 = i$, $i_2 = 0$, $e'' = e$ and $h'' = h'$. Otherwise, we proceed by case analysis on the $K[e], h \to e'', h''$ derivation:

Case EvalCtx: then $e'' = K[e''']$ and $e, h \to e''', h''$. Thus, by the induction hypothesis, there exists i_1, i_2, e'''' and h''' such that $e''', h'' \to^{i_1} e'''', h''' \not\to$, $K[e'''']$, $h''' \to^{i_2} e', h' \not\to$ and $i - 1 = i_1 + i_2$. We thus have that, $K[e], h \to^{i_1+1} K[e'''']$, $h''' \not\to$ and $K[e'''']$, $h''' \to^{i_2} e', h' \not\to$.

Case EvalFix, EvalRead, EvalWrite, EvalAlloc, EvalUnpack, EvalFst, EvalSnd: then $e \in$ *Val*. Thus, $e, h \to^0 e, h \not\to$ and $K[e], h \to^i e', h' \not\to$. □

3 Logical relation

Assume a c.o.f.e. Inv over ω^2 and isomorphism

$$\xi : \mathit{Inv} \cong \blacktriangleright((\mathbb{N} \xrightarrow{\mathit{fin}} \mathit{Inv}) \xrightarrow{\mathit{mon}} \mathbf{UPred}(\mathit{Heap} \times \mathit{Heap})))$$

Define Type, World and $\widehat{\mathit{Inv}}$ as follows

$$\mathit{World} \stackrel{\mathit{def}}{=} \mathbb{N} \xrightarrow{\mathit{fin}} \mathit{Inv} \qquad \mathit{Type} \stackrel{\mathit{def}}{=} \mathit{World} \xrightarrow{\mathit{mon}} \mathbf{UPred}(\mathit{Val} \times \mathit{Val}) \qquad \widehat{\mathit{Inv}} \stackrel{\mathit{def}}{=} \mathit{World} \xrightarrow{\mathit{mon}} \mathbf{UPred}(\mathit{Heap} \times \mathit{Heap})$$

Value relation $\boxed{\mathcal{V}[\![\Delta \vdash \tau]\!] : \mathit{Type}^{\Delta} \to \mathit{Type}}$

$$\begin{aligned}
\mathcal{V}[\![\Delta \vdash 1]\!]_\rho(W) &\stackrel{\mathit{def}}{=} \{(n, m, *, *)\} \\
\mathcal{V}[\![\Delta \vdash \tau \times \sigma]\!]_\rho(W) &\stackrel{\mathit{def}}{=} \{(n, m, v_I, v_S) \mid \exists v_{1I}, v_{2I}, v_{1S}, v_{2S}.\ v_I = (v_{1I}, v_{2I}) \wedge v_S = (v_{1S}, v_{2S}) \wedge \\
&\qquad (n, m, v_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W') \wedge (n, m, v_{2I}, v_{2S}) \in \mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho(W')\} \\
\mathcal{V}[\![\Delta \vdash \tau \to \sigma]\!]_\rho(W) &\stackrel{\mathit{def}}{=} \{(n, _, v_I, v_S) \mid \forall n' < n.\ \forall W' \geq W. \\
&\qquad (\forall m.\ (n', m, u_I, u_S) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W')) \Rightarrow (n' + 1, v_I\ u_I, v_S\ u_S) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho)(W')\} \\
\mathcal{V}[\![\Delta \vdash \tau\ \mathit{ref}]\!]_\rho(W) &\stackrel{\mathit{def}}{=} \{(n, m, l_I, l_S) \mid \exists \iota \in \mathit{dom}(W).\ \xi(W(\iota)) \stackrel{n,m}{=}_{\blacktriangleright \widehat{\mathit{Inv}}} \mathit{inv}(\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho, l_I, l_S)\} \\
\mathcal{V}[\![\Delta, \alpha \vdash \alpha]\!]_\rho(W) &\stackrel{\mathit{def}}{=} \rho(\alpha)(W) \\
\mathcal{V}[\![\Delta \vdash \exists \alpha.\ \tau]\!]_\rho(W) &\stackrel{\mathit{def}}{=} \{(n, m, \mathit{pack}\ v_I, \mathit{pack}\ v_S) \mid \exists \nu \in \mathit{Type}.\ (n, m, v_I, v_S) \in \mathcal{V}[\![\Delta, \alpha \vdash \tau]\!]_{\rho[\alpha \mapsto \nu]}(W)\}
\end{aligned}$$

Reference invariant $\boxed{\mathit{inv} : \mathit{Type} \times \mathcal{L} \times \mathcal{L} \to \mathit{World} \xrightarrow{\mathit{mon}} \mathbf{UPred}(\mathit{Heap} \times \mathit{Heap})}$

$$\mathit{inv}(\nu, l_I, l_S) \stackrel{\mathit{def}}{=} \lambda W.\ \{(n, m, h_I, h_S) \mid l_I \in \mathit{dom}(h_I) \wedge l_S \in \mathit{dom}(h_S) \wedge (n, m, h_I(l_I), h_S(l_S)) \in \nu(W)\}$$

World satisfaction

$$\begin{aligned}
\lfloor W \rfloor \stackrel{\mathit{def}}{=} \{(n, h_I, h_S) \mid\ & n = 0 \vee \exists r_I, r_S : \mathit{dom}(W) \to \mathit{Heap}.\ h_I = \Pi_\iota r_I(\iota) \wedge h_S = \Pi_\iota r_S(\iota) \wedge \\
& \forall \iota \in \mathit{dom}(W).\ \forall m.\ (n - 1, m, r_I(\iota), r_S(\iota)) \in \xi(W(\iota))(W)\}
\end{aligned}$$

Expression closure

$$\begin{aligned}
\mathcal{E}(\nu) \stackrel{\mathit{def}}{=} \lambda W.\ \{(n, e_I, e_S) \mid\ & \forall n' \leq n.\ \forall i < n'.\ \forall h_I, h_S \in \mathit{Heap}.\ \forall W' \geq W. \\
& (n', h_I, h_S) \in \lfloor W' \rfloor \wedge e_I, h_I \to^i e_I', h_I' \not\to \ \Rightarrow \\
& \exists v_S, h_S'.\ \exists W'' \geq W'.\ e_S, h_S \to^* v_S, h_S' \wedge e_I' \in \mathit{Val} \wedge \\
& (n' - i, h_I', h_S') \in \lfloor W'' \rfloor \wedge \forall m.\ (n' - i, m, e_I', v_S) \in \nu(W'')\}
\end{aligned}$$

Context relation $\boxed{\mathcal{V}[\![\Delta \vdash \Gamma]\!] : \mathit{Type}^{\Delta} \to \mathit{World} \xrightarrow{\mathit{mon}} \mathbf{UPred}(\mathit{Val}^{\Gamma} \times \mathit{Val}^{\Gamma})}$

$$\mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W) \stackrel{\mathit{def}}{=} \{(n, m, \sigma_I, \sigma_S) \mid \forall (x : \tau) \in \Gamma.\ (n, m, \sigma_I(x), \sigma_S(x)) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W)\}$$

Logical relation $\boxed{\Delta;\Gamma \models e_I \leq_{log} e_S : \tau}$

$$\Delta;\Gamma \models e_I \leq_{log} e_S : \tau \stackrel{def}{=} \forall n \in \mathbb{N}.\ \forall W \in \mathit{World}.\ \forall \sigma_I, \sigma_S \in \mathit{Val}^{\Gamma}.\ \forall \rho \in \mathit{Type}^{\Delta}.$$
$$(\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W))$$
$$\Rightarrow\ (n, \sigma_I(e_I), \sigma_S(e_S)) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho)(W)$$

Lemma 15.

$$\forall W_1, W_2 \in \mathit{World}.\ \forall h_I, h_S \in \mathit{Heap}.\ \forall n, m \in \mathbb{N}.$$
$$W_1 \stackrel{n,m}{=}_{\mathit{World}} W_2 \wedge (n, h_I, h_S) \in \lfloor W_1 \rfloor \Rightarrow (n, h_I, h_S) \in \lfloor W_2 \rfloor$$

Proof. Since the conclusion is trivial for $n = 0$, assume $n > 0$. By assumption, there exists $r_I, r_S : \mathit{dom}(W_1) \to \mathit{Heap}$ such that

$$h_I = \Pi_{\iota \in \mathit{dom}(W_1)} r_I(\iota) \qquad\qquad h_S = \Pi_{\iota \in \mathit{dom}(W_1)} r_S(\iota)$$

and

$$\forall \iota \in \mathit{dom}(W_1).\ \forall m.\ (n-1, m, r_I(\iota), r_S(\iota)) \in \xi(W_1(\iota))(W_1).$$

Since $W_1 \stackrel{n,m}{=} W_2$ it follows that $\mathit{dom}(W_1) = \mathit{dom}(W_2)$. Let $\iota \in \mathit{dom}(W_2)$ and $m' \in \mathbb{N}$. Thus, by assumption, $(n-1, m', r_I(\iota), r_S(\iota)) \in \xi(W_1(\iota))(W_1)$. Since $W_1 \stackrel{n,m}{=} W_2$ it follows that

$$\xi(W_1(\iota)) \stackrel{n,m}{=}_{\blacktriangleright \widehat{Inv}} \xi(W_2(\iota))$$

and thus $\xi(W_1(\iota))(W_1) \stackrel{n-1,m'+1}{=} \xi(W_2(\iota))(W_2)$. Hence, $(n'-1, m'+1, r_I(\iota), r_S(\iota)) \in \xi(W_2(\iota))(W_2)$. □

Lemma 16.

$$\forall W_1, W_2 \in \mathit{World}.\ \forall \nu \in \mathit{Type}.\ \forall n, m \in \mathbb{N}.\ \forall e_I, e_S \in \mathit{Exp}.$$
$$W_1 \stackrel{n,m}{=}_{\mathit{World}} W_2 \wedge (n, e_I, e_S) \in \mathcal{E}(\nu)(W_1) \Rightarrow (n, e_I, e_S) \in \mathcal{E}(\nu)(W_2)$$

Proof. Assume

$$i < k \leq n \qquad W_2' \geq W_2 \qquad (k, h_I, h_S) \in \lfloor W_2' \rfloor \qquad e_I, h_I \to^i e_I', h_I' \not\to$$

Then there exists a W_1' such that $W_1' \geq W_1$ and $W_1' \stackrel{n,m}{=} W_2'$. Hence, by Lemma 15, $(k, h_I, h_S) \in \lfloor W_1' \rfloor$. There thus exists v_S, h_S', and $W_1'' \geq W_1'$ such that

$$e_I' \in \mathit{Val} \qquad e_S, h_S \to^* v_S, h_S' \qquad (k-i, h_I', h_S') \in \lfloor W_1'' \rfloor \qquad \forall m.\ (k-i, m, e_I', v_S) \in \nu(W_1'')$$

Hence, there exists a W_2'' such that $W_2'' \geq W_2'$ and $W_1'' \stackrel{n,m}{=} W_2''$ from which it follows that

$$(k-i, h_I', h_S') \in \lfloor W_2'' \rfloor \qquad\qquad \forall m.\ (k-i, m, e_I', v_S) \in \nu(W_2'')$$

by Lemma 15 and non-expansiveness. □

Lemma 17.

$$\forall \nu \in \mathit{Type}.\ \forall l_I, l_S \in \mathit{Loc}.\ \mathit{inv}(\nu, l_I, l_S) \in \mathit{World} \stackrel{mon}{\to} \mathbf{UPred}(\mathit{Heap} \times \mathit{Heap})$$

Lemma 18. *The value relation is well-defined. In particular,*

- $\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho$ *is non-expansive for all* $\rho \in \mathit{Type}^{\Delta}$,

- $\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho$ *is monotone for all* $\rho \in \mathit{Type}^\Delta$,
- $\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W)$ *is downwards-closed for all* $\rho \in \mathit{Type}^\Delta$ *and* $W \in \mathit{World}$.

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

- Case $\tau = 1$: trivial.
- Case $\tau = \sigma\ \mathit{ref}$: to show that the value relation is non-expansive, assume $W_1 \overset{n,m}{=} W_2$, $(n', m') < (n, m)$, and $(n', m', l_I, l_S) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W_1)$. Hence, there an $\iota \in \mathit{dom}(W_1)$ such that

  $$\xi(W_1(\iota)) \overset{n',m'}{=}_{\blacktriangleright \widehat{Inv}} inv(\mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho, l_I, l_S)$$

  Since ξ is non-expansive, $\xi(W_1(\iota)) \overset{n,m}{=}_{\blacktriangleright \widehat{Inv}} \xi(W_2(\iota))$. By transivity it follows that

  $$\xi(W_2(\iota)) \overset{n',m'}{=}_{\blacktriangleright \widehat{Inv}} inv(\mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho, l_I, l_S)$$

  and thus, $(n', m', l_I, l_S) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W_2)$. The value relation is easily seen to be monotone in worlds and downwards-closed in the step-index.
- Case $\tau = \sigma_1 \to \sigma_2$: to show that the value relation is non-expansive, assume $W_1 \overset{n,m}{=} W_2$, $(n', m') < (n, m)$, and $(n', m', v_I, v_S) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W_1)$. Hence,

  $$\begin{array}{l}\forall k < n'.\ \forall W_1' \geq W_1. \\ \quad (\forall m.\ (k, m, u_I, u_S) \in \mathcal{V}[\![\Delta \vdash \sigma_1]\!]_\rho(W_1')) \Rightarrow (k+1, v_I\ u_I, v_S\ u_S) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \sigma_2]\!]_\rho)(W_1')\end{array}$$

  To show that $(n', m', v_I, v_S) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W_2)$, let $k < n'$, $W_2' \geq W_2$ such that $\forall m.\ (k, m, u_I, u_S) \in \mathcal{V}[\![\Delta \vdash \sigma_1]\!]_\rho(W_2')$. Hence, there exists a W_1' such that $W_1' \geq W_1$ and $W_1' \overset{n,m}{=} W_2'$. Hence, $\forall m.\ (k, m, u_I, u_S) \in \mathcal{V}[\![\Delta \vdash \sigma_1]\!]_\rho(W_1')$, since $\mathcal{V}[\![\Delta \vdash \sigma_1]\!]_\rho$ is non-expansive by the induction hypothesis. It thus follows that $(k+1, v_I\ u_I, v_S\ u_S) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \sigma_2]\!]_\rho)(W_1')$ and, by Lemma 16, $(k+1, v_I\ u_I, v_S\ u_S) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \sigma_2]\!]_\rho)(W_2')$. The value relation is clearly monotone and downwards-closed in the step-index.
- Case $\tau = \exists\alpha.\ \sigma$: follows easily from the induction hypothesis.
- Case $\tau = \alpha$: follows from the type of ρ.

□

Lemma 19.

$$\begin{array}{l}\forall n \in \mathbb{N}.\ \forall v_I, v_S \in \mathit{Val}.\ \forall W \in \mathit{World}.\ \forall \nu \in \mathit{Type}. \\ \quad (\forall m.\ (n, m, v_I, v_S) \in \nu(W)) \Rightarrow (n, v_I, v_S) \in \mathcal{E}(\nu)(W)\end{array}$$

Proof. Assume

$$0 < n' \leq n \qquad i < n' \qquad W' \geq W \qquad (n', h_I, h_S) \in W' \qquad v_I, h_I \to^i e_I', h_I' \not\to$$

Since v_I is a value it follows that $i = 0$, $e_I' = v_I$, and $h_I' = h_I$. Thus, we pick $W'' = W'$, $v_S' = v_S$ and $h_S' = h_S$. By downwards-closure it follows that

$$(n' - i, h_I, h_S) \in \lfloor W' \rfloor \qquad \forall m.\ (n' - i, m, e_I', v_S) \in \nu(W')$$

as required. □

Lemma 20. $\Delta; \Gamma, x : \tau \models x \leq x : \tau$.

Proof. Assume

$$\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma, x : \tau]\!]_\rho(W)$$

Thus, $\forall m.\ (n, m, \sigma_I(x), \sigma_S(x)) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W)$ and by Lemma 19,

$$(n, \sigma_I(x), \sigma_S(x)) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho)(W)$$

as required. □

3.1 Compatibility lemmas

Lemma 21. *If* $\Delta; \Gamma, f : \tau \to \sigma, x : \tau \models e_I \leq e_S : \sigma$ *then* $\Delta; \Gamma \models \mathit{fix}\ f(x).\ e_I \leq \mathit{fix}\ f(x).\ e_S : \tau \to \sigma$.

Proof. We prove by induction on n that

$$\begin{array}{l}\forall n \in \mathbb{N}.\ \forall W \in \mathit{World}.\ \forall \rho \in \mathit{Type}^\Delta.\ \forall \sigma_I, \sigma_S \in \mathit{Val}^\Gamma. \\ \quad (\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)) \\ \qquad \Rightarrow\ (\forall m.\ (n, m, \sigma_I(\mathit{fix}\ f(x).\ e_I), \sigma_S(\mathit{fix}\ f(x).\ e_S)) \in \mathcal{V}[\![\Delta \vdash \tau \to \sigma]\!]_\rho(W))\end{array}$$

from which the conclusion follows easily, by Lemma 19, as $\mathit{fix}\ f(x).\ e_I$ and $\mathit{fix}\ f(x).\ e_S$ are values.

The base case follows trivially, as $\neg(n' < 0)$ for all n'.

For the inductive case, assume

$$\forall m.\ (n+1, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$$

To show that

$$\forall m.\ (n+1, m, \sigma_I(\mathit{fix}\ f(x).\ e_I), \sigma_S(\mathit{fix}\ f(x).\ e_S)) \in \mathcal{V}[\![\Delta \vdash \tau \to \sigma]\!]_\rho(W)$$

let $n' < n+1$, $W' \geq W$ such that $\forall m.\ (n', m, u_I, u_S) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W')$. Then it remains to show that

$$(n'+1, \sigma_I(\mathit{fix}\ f(x).\ e_I)\ u_I, \sigma_S(\mathit{fix}\ f(x).\ e_S)\ u_S) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho)(W')$$

Assume

$$i < n'' \leq n' \qquad W'' \geq W' \qquad (n'', h_I, h_S) \in \lfloor W'' \rfloor \qquad \sigma_I(\mathit{fix}\ f(x).\ e_I)\ u_I, h_I \to^i e_I', h_I' \not\to$$

Hence, $i > 0$ and $\sigma_I(\mathit{fix}\ f(x).\ e_I)\ u_I, h_I \to \sigma_I(e_I)[u_I/x, \sigma_I(\mathit{fix}\ f(x).\ e_I)/f], h_I \to^{i-1} e_I', h_I'$.

Since $n'' \leq n$, by downwards closure and monotonicity, it follows that

$$\forall m.\ (n'', m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W'')$$

Thus, by the induction hypothesis,

$$\forall m.\ (n'', m, \sigma_I(\mathit{fix}\ f(x).\ e_I), \sigma_S(\mathit{fix}\ f(x).\ e_S)) \in \mathcal{V}[\![\Delta \vdash \tau \to \sigma]\!]_\rho(W'')$$

We thus have that

$$\forall m.\ (n'', m, \sigma_I', \sigma_S') \in \mathcal{V}[\![\Delta \vdash \Gamma, f : \tau \to \sigma, x : \tau]\!]_\rho(W'')$$

for $\sigma_I' = \sigma_I[x \mapsto u_I, f \mapsto \mathit{fix}\ f(x).\ e_I]$ and $\sigma_S' = \sigma_S[x \mapsto u_S, f \mapsto \mathit{fix}\ f(x).\ e_S]$.

From the $\Delta; \Gamma, f : \tau \to \sigma, x : \tau \models e_I \leq e_S : \sigma$ assumption it thus follows that

$$(n'', \sigma_I'(e_I), \sigma_S'(e_S)) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho)(W'')$$

The rest is easy. □

Lemma 22. *If* $\Delta;\Gamma \models e_{1I} \leq e_{1S} \leq \tau \to \sigma$ *and* $\Delta;\Gamma \models e_{2I} \leq e_{2S} : \tau$, *then* $\Delta;\Gamma \models e_{1I}\ e_{2I} \leq e_{1S}\ e_{2S} : \sigma$.

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(e_{1I}\ e_{2I}), h_I \to^i e'_I, h'_I \not\to$$

Hence, by Lemma 14, there exists i_1, i_2, h_{1I}, and e'_{1I} such that

$$\sigma_I(e_{1I}), h_I \to^{i_1} e'_{1I}, h_{1I} \not\to \qquad e'_{1I}\ \sigma_I(e_{2I}), h_{1I} \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

From the $\Delta;\Gamma \models e_{1I} \leq e_{1S} \leq \tau \to \sigma$ assumption there exists $W'' \geq W'$, v_{1S} and h_{1S} such that

$$\sigma_S(e_{1S}), h_S \to^* v_{1S}, h_{1S} \quad (n' - i_1, h_{1I}, h_{1S}) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau \to \sigma]\!]_\rho(W'')$$

and $e'_{1I} \in \mathit{Val}$. Thus, by Lemma 14, there exists i_3, i_4, h_{2I} and e'_{2I} such that

$$\sigma_I(e_{2I}), h_{1I} \to^{i_3} e'_{2I}, h_{2I} \not\to \qquad e'_{1I}\ e'_{2I}, h_{2I} \to^{i_4} e'_I, h'_I \not\to$$

and $i_2 = i_3 + i_4$.

From the $\Delta;\Gamma \models e_{2I} \leq e_{2S} : \tau$ assumption there exists $W''' \geq W''$, v_{2S}, and h_{2S} such that

$$\sigma_S(e_{2S}), h_{1S} \to^* v_{2S}, h_{2S} \quad (n' - i_1 - i_3, h_{2I}, h_{2S}) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1 - i_3, m, e'_{2I}, v_{2S}) \in \mathcal{V}[\![\tau]\!](W''')$$

and $e'_{2I} \in \mathit{Val}$.

By $(n' - i_1, 0, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau \to \sigma]\!]_\rho(W'')$ it follows that

$$(n' - i_1 - i_3, e'_{1I}\ e'_{2I}, v_{1S}\ v_{2S}) \in \mathcal{E}(\mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho)(W''')$$

Hence, there exists $W'''' \geq W'''$, v_S and h'_S such that

$$v_{1S}\ v_{2S}, h_{2S} \to^* v_S, h'_S \qquad (n' - i, h'_I, h'_S) \in \lfloor W'''' \rfloor \qquad \forall m.\ (n' - i, m, e'_I, v_S) \in \mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho(W'''')$$

and $e'_I \in \mathit{Val}$. Lastly, $\sigma_S(e_{1S}\ e_{2S}), h_S \to^* v_S, h'_S$. □

Lemma 23.

$$\begin{array}{l}\forall l_I, l_S \in \mathit{Loc}.\ \forall h_I, h_S \in \mathit{Heap}.\ \forall \nu \in \mathit{Type}.\ \forall \iota \in \mathbb{N}.\ \forall W \in \mathit{World}.\ \forall n, m \in \mathbb{N}.\\ \quad \mathit{inv}(\nu, l_I, l_S) \stackrel{n,m}{=}_{\blacktriangleright \widehat{Inv}} \xi(W(\iota)) \wedge (n, h_I, h_S) \in \lfloor W \rfloor \wedge n > 0\\ \qquad \Rightarrow l_I \in \mathit{dom}(h_I) \wedge l_S \in \mathit{dom}(h_S) \wedge \forall m' \in \mathbb{N}.\ (n-1, m', h_I(l_I), h_S(l_S)) \in \nu(W)\end{array}$$

Proof. By definition of heap satisfiction, there exists $r_I, r_S : \mathit{dom}(W) \to \mathit{Heap}$ such that

$$h_I = \Pi_{\iota \in \mathit{dom}(W)} r_I(\iota) \qquad h_S = \Pi_{\iota \in \mathit{dom}(W)} r_S(\iota) \qquad \forall m.\ (n-1, m, r_I(\iota), r_S(\iota)) \in \xi(W(\iota))(W)$$

Since $\mathit{inv}(\nu, l_I, l_S) \stackrel{n,m}{=}_{\blacktriangleright \widehat{Inv}} \xi(W(\iota))$ it follows that $\mathit{inv}(\nu, l_I, l_S)(W) \stackrel{n-1,1}{=}_{\blacktriangleright \widehat{Inv}} \xi(W(\iota))(W)$ and thus

$$(n-1, 0, r_I(\iota), r_S(\iota)) \in \mathit{inv}(\nu, l_I, l_S)(W)$$

Hence, $l_I \in \mathit{dom}(r_I(\iota)), l_S \in \mathit{dom}(r_S(\iota))$.

To show that $\forall m'.\ (n-1, m', r_I(\iota)(l_I), r_S(\iota)(l_S)) \in \nu(W)$, assume $m' \in \mathbb{N}$. Since $(n-1, m'+1) < (n, m)$ it follows that $\mathit{inv}(\nu, l_I, l_S)(W) \stackrel{n-1,m'+1}{=}_{\blacktriangleright \widehat{Inv}} \xi(W(\iota))(W)$ and thus

$$(n-1, m', r_I(\iota), r_S(\iota)) \in \mathit{inv}(\nu, l_I, l_S)(W)$$

Thus, $(n-1, m', r_I(\iota)(l_I), r_S(\iota)(l_S)) \in \nu(W)$. □

Lemma 24. *If* $\Delta;\Gamma \models e_I \leq e_S : \tau$ *ref then* $\Delta;\Gamma \models !\, e_I \leq !\, e_S : \tau$.

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(!\, e_I), h_I \to^i e'_I, h'_I \not\to$$

Hence, by Lemma 14, there exists i_1, i_2, v_{1I} and h_{1I} such that

$$\sigma_I(e_I), h_I \to^{i_1} e_{1I}, h_{1I} \not\to \qquad\qquad !\, e_{1I}, h_{1I} \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

From the $\Delta;\Gamma \models e_I \leq e_S : \tau$ *ref* assumption there exists $W'' \geq W'$, v_{1S} and h_{1S} such that

$$\sigma_S(e_{1S}), h_S \to^* v_{1S}, h_{1S} \quad (n' - i_1, h_{1I}, h_{1S}) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1, m, e_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau \text{ ref}]\!]_\rho(W'')$$

and $e_{1I} \in \mathit{Val}$. By the value relation there exists an $\iota \in \mathit{dom}(W'')$ such that

$$\xi(W''(\iota))\ {}^{n'-i_1,0}_{\blacktriangleright\widehat{Inv}}\ \mathit{inv}(\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho, e_{1I}, v_{1S})$$

Since $n' - i_1 > 0$ it follows by Lemma 23 that $e_{1I} \in \mathit{dom}(h_{1I})$, $v_{1S} \in \mathit{dom}(h_{1S})$ and

$$\forall m.\ (n' - i_1 - 1, m, h_{1I}(e_{1I}), h_{1S}(v_{1S})) \in \mathcal{V}[\![\Gamma \vdash \tau]\!]_\rho(W'')$$

Lastly, since $e_{1I} \in \mathit{dom}(h_{1I})$ it follows that $h'_I = h_{1I}$, $v_I = h_{1I}(e_{1I})$ and $i_2 = 1$. □

Lemma 25.

$$\begin{array}{l}\forall l_I, l_S \in \mathit{Loc}.\ \forall h_I, h_S \in \mathit{Heap}.\ \forall \nu \in \mathit{Type}.\ \forall \iota \in \mathbb{N}.\ \forall W \in \mathit{World}.\ \forall n, m \in \mathbb{N}.\\ \quad \mathit{inv}(\nu, l_I, l_S)\ {}^{n,m}_{\blacktriangleright\widehat{Inv}}\ \xi(W(\iota)) \wedge (n, h_I, h_S) \in \lfloor W \rfloor \wedge \forall m.\ (n-1, m, v_I, v_S) \in \nu(W)\\ \quad\quad \Rightarrow (n, h_I[l_I \mapsto v_I], h_S[l_S \mapsto v_S]) \in \lfloor W \rfloor\end{array}$$

Proof. As the conclusion is trivial if $n < 1$, assume $n \geq 1$. By definition of heap satisfiction, there exists $r_I, r_S : \mathit{dom}(W) \to \mathit{Heap}$ such that

$$h_I = \Pi_{\iota \in dom(W)} r_I(\iota) \qquad h_S = \Pi_{\iota \in dom(W)} r_S(\iota) \qquad \forall m.\ (n-1, m, r_I(\iota), r_S(\iota)) \in \xi(W(\iota))(W)$$

Since $\xi(W(\iota))(W)\ {}^{n-1,1}_{=}\ \mathit{inv}(\nu, l_I, l_S)$ it follows that

$$(n-1, 0, r_I(\iota), r_S(\iota)) \in \mathit{inv}(\nu, l_I, l_S)$$

and thus $l_I \in \mathit{dom}(r_I(\iota))$ and $l_S \in \mathit{dom}(r_S(\iota))$.

Let $r'_I = r_I[\iota \mapsto r_I(\iota)[l_I \mapsto v_I]]$ and $r'_S = r_S[\iota \mapsto r_S(\iota)[l_S \mapsto v_S]]$. Then,

$$h_I[l_I \mapsto v_I] = \Pi_{\iota \in dom(r'_I)} r'_I(\iota) \qquad h_S[l_S \mapsto v_S] = \Pi_{\iota \in dom(r'_S)} r'_S(\iota)$$

It thus remains to show that

$$\forall x \in \mathit{dom}(W).\ \forall m'.\ (n-1, m', r'_I(x), r'_S(x)) \in \xi(W(x))(W)$$

This holds trivially for all $x \neq \iota$. For $x = \iota$, let $m' \in \mathbb{N}$. Then by assumption $(n-1, m', v_I, v_S) \in \nu(W)$ and

$$\mathit{inv}(\nu, l_I, l_S)(W)\ {}^{n-1,m'+1}_{=}\ \xi(W(\iota))(W)$$

Thus, $(n-1, m', r'_I(x), r'_S(x)) \in \mathit{inv}(\nu, l_I, l_S)(W)$ and $(n-1, m', r'_I(x), r'_S(x)) \in \xi(W(\iota))(W)$. □

Lemma 26. *If* $\Delta;\Gamma \models e_{1I} \leq e_{1S} : \tau$ *ref and* $\Delta;\Gamma \models e_{2I} \leq e_{2S} : \tau$ *then* $\Delta;\Gamma \models e_{1I} := e_{2I} \leq e_{1S} := e_{2S} : 1$.

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(e_{1I} := e_{2I}), h_I \to^i e'_I, h'_I \not\to$$

Hence, by Lemma 14, there exists i_1, i_2, e'_{1I}, and h_{1I} such that

$$\sigma_I(e_{1I}), h_I \to^{i_1} e'_{1I}, h_{1I} \not\to \qquad\qquad e'_{1I} := e_{2I}, h_{1I} \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

Since $\Delta;\Gamma \models e_{1I} \leq e_{1S} : \tau$ *ref*, it follows that there exists $W'' \geq W'$, v_{1S}, and h_{1S} such that

$$\sigma_S(e_{1S}), h_S \to^* v_{1S}, h_{1S} \quad (n' - i_1, h_{1I}, h_{1S}) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau\ \mathit{ref}]\!]_\rho(W'')$$

and $e'_{1I} \in \mathit{Val}$. By Lemma 23 it thus follows that $e'_{1I} \in \mathit{dom}(h_{1I})$ and $v_{1S} \in \mathit{dom}(h_{1S})$.

By Lemma 14 there exists i_3, i_4, e'_{2I}, and h_{2I} such that

$$\sigma_I(e_{2I}), h_{1I} \to^{i_3} e'_{2I}, h_{2I} \not\to \qquad\qquad e'_{1I} := e'_{2I}, h_{2I} \to^{i_4} e'_I, h'_I \not\to$$

and $i_2 = i_3 + i_4$.

Since $\Delta;\Gamma \models e_{2I} \leq e_{2S} : \tau$, it follows that there exists $W''' \geq W''$, v_{2S}, and h_{2S} such that

$$\sigma_S(e_{2S}), h_{1S} \to^* v_{2S}, h_{2S} \quad (n' - i_1 - i_3, h_{2I}, h_{2S}) \in \lfloor W''' \rfloor \quad \forall m.\ (n' - i_1 - i_3, m, e'_{2I}, v_{2S}) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W''')$$

and $e'_{2I} \in \mathit{Val}$.

Thus $e'_{1I} \in \mathit{dom}(h_{1I}) \subseteq \mathit{dom}(h_{2I})$ and $v_{1S} \in \mathit{dom}(h_{1S}) \subseteq \mathit{dom}(h_{2S})$. Hence, by the evaluation of $e'_{1I} := e'_{2I}$, $h'_I = h_{2I}[e'_{1I} \mapsto e'_{2I}]$, $v_I = *$, and

$$v_{1S} := v_{2S}, h_{2S} \to *, h_{2S}[v_{1S} \mapsto v_{2S}]$$

Lastly, by Lemma 25, we have that $(n' - i_1 - i_3, h_{2I}[e'_{1I} \mapsto e'_{2I}], h_{2S}[v_{1S} \mapsto v_{2S}]) \in \lfloor W''' \rfloor$. □

Lemma 27.

$$\begin{array}{l}\forall l_I, l_S \in \mathit{Loc}.\ \forall h_I, h_S \in \mathit{Heap}.\ \forall \nu \in \mathit{Type}.\ \forall \iota \in \mathbb{N}.\ \forall W \in \mathit{World}.\ \forall n \in \mathbb{N}.\\ \quad (n, h_I, h_S) \in \lfloor W \rfloor \wedge \iota \notin \mathit{dom}(W) \wedge l_I \notin \mathit{dom}(h_I) \wedge l_S \notin \mathit{dom}(h_S) \wedge \forall m.\ (n-1, m, v_I, v_S) \in \nu(W)\\ \quad\Rightarrow (n, h_I[l_I \mapsto v_I], h_S[l_S \mapsto v_S]) \in \lfloor W[\iota \mapsto \xi^{-1}(\mathit{inv}(\nu, l_I, l_S))] \rfloor\end{array}$$

Proof. Since the conclusion is trivial for $n = 0$, assume $n > 0$. By definition of heap satisfiction, there exists $r_I, r_S : \mathit{dom}(W) \to \mathit{Heap}$ such that

$$h_I = \Pi_{\iota \in \mathit{dom}(W)} r_I(\iota) \qquad h_S = \Pi_{\iota \in \mathit{dom}(W)} r_S(\iota) \qquad \forall m.\ (n-1, m, r_I(\iota), r_S(\iota)) \in \xi(W(\iota))(W)$$

Let $r'_I = r_I[\iota \mapsto [l_I \mapsto v_I]]$ and $r'_S = r_S[\iota \mapsto [l_S \mapsto v_S]]$. Then,

$$h_I[l_I \mapsto v_I] = \Pi_{\iota \in \mathit{dom}(r'_I)} r'_I(\iota) \qquad\qquad h_S[l_S \mapsto v_S] = \Pi_{\iota \in \mathit{dom}(r'_S)} r'_S(\iota)$$

It thus remains to show that

$$\forall x \in \mathit{dom}(W).\ \forall m.\ (n-1, m, r'_I(x), r'_S(x)) \in \xi(W'(x))(W')$$

where $W' = W[\iota \mapsto \xi^{-1}(\mathit{inv}(\nu, l_I, l_S))$.

This holds trivially for all $x \neq \iota$. For $x = \iota$, the proof obligation reduces to,

$$\forall m.\ (n-1, m, [l_I \mapsto v_I], [l_S \mapsto v_S]) \in \mathit{inv}(\nu, l_I, l_S)(W')$$

This follows from the $\forall m.\ (n-1, m, v_I, v_S) \in \nu(W)$ assumption, by monotonicity. □

Lemma 28. *If* $\Delta;\Gamma \models e_{1I} \leq e_{1S} : \tau$ *then* $\Delta;\Gamma \models \mathit{ref}\, e_{1I} \leq \mathit{ref}\, e_{1S} : \tau$ *ref.*

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(\mathit{ref}\, e_{1I}), h_I \to^i e'_I, h'_I \not\to$$

By Lemma 14, there exists i_1, i_2, e'_{1I}, and h_{1I} such that

$$\sigma_I(e_{1I}), h_I \to^{i_1} e'_{1I}, h_{1I} \not\to \qquad\qquad \mathit{ref}\, e'_{1I}, h_{1I} \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

Since $\Delta;\Gamma \models e_{1I} \leq e_{1S} : \tau$ it follows that there exists $W'' \geq W'$, v_{1S}, and h_{1S} such that

$$\sigma_S(e_{1S}), h_S \to^* v_{1S}, h_{1S} \qquad (n' - i_1, h_{1I}, h_{1S}) \in \lfloor W'' \rfloor \qquad \forall m.\ (n' - i_1, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W'')$$

and $e'_{1I} \in \mathit{Val}$. Thus, $e'_I \in \mathit{Loc}$, $e'_I \notin \mathit{dom}(h_{1I})$, $h'_I = h_{1I}[e'_I \mapsto e'_{1I}]$ and $i_2 = 1$.

Pick $v_S \in \mathit{Loc}$ such that $v_S \notin \mathit{dom}(h_{1S})$ and $\iota \in \mathbb{N}$ such that $\iota \notin \mathit{dom}(W'')$. Let

$$W''' = W''[\iota \mapsto \xi^{-1}(\mathit{inv}(\mathcal{V}[\![\Delta \vdash \tau]\!]_\rho, e'_I, v_S))]$$

By Lemma 27,

$$(n' - i_1, h_{1I}[e'_I \mapsto e'_{1I}], h_{1S}[v_S \mapsto v_{1S}]) \in \lfloor W''' \rfloor$$

Lastly, $\forall m.\ (n' - i_1 - 1, m, e'_I, v_S) \in \mathcal{V}[\![\Delta \vdash \tau\ \mathit{ref}]\!]_\rho(W''')$ and $\mathit{ref}\, v_{1S}, h_{1S} \to v_S, h_{1S}[v_S \mapsto v_{1S}]$. □

Lemma 29.

$$\mathcal{V}[\![\Delta, \alpha \vdash \tau]\!]_{\rho[\alpha \mapsto \mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho]} = \mathcal{V}[\![\Delta \vdash \tau[\sigma/\alpha]]\!]_\rho$$

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

Case $\Delta \vdash 1$, $\Delta, \alpha \vdash \alpha$: trivial.

Case $\Delta \vdash \tau \times \sigma$, $\Delta \vdash \tau \to \sigma$, $\Delta \vdash \tau\ \mathit{ref}$, $\Delta \vdash \exists\alpha.\ \tau$: follows directly from the induction hypothesis. □

Lemma 30. *If* $\Delta \vdash \tau$ *then*

$$\forall \rho \in \mathit{Type}^\Delta.\ \forall \nu \in \mathit{Type}.\ \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho = \mathcal{V}[\![\Delta, \alpha \vdash \tau]\!]_{\rho[\alpha \mapsto \nu]}$$

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

Case $\Delta \vdash 1$, $\Delta, \alpha \vdash \alpha$: trivial.

Case $\Delta \vdash \tau \times \sigma$, $\Delta \vdash \tau \to \sigma$, $\Delta \vdash \tau\ \mathit{ref}$, $\Delta \vdash \exists\alpha.\ \tau$: follows directly from the induction hypothesis. □

Lemma 31. *If* $\Delta;\Gamma \vdash e_{1I} \leq e_{1S} : \sigma[\tau/\alpha]$ *then* $\Delta;\Gamma \vdash \mathit{pack}\, e_{1I} \leq \mathit{pack}\, e_{1S} : \exists\alpha.\ \sigma$.

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(\mathit{pack}\, e_{1I}), h_I \to^i e'_I, h'_I \not\to$$

By Lemma 14, there exists i_1, i_2, e'_{1I}, and h_{1I} such that

$$\sigma_I(e_{1I}), h_I \to^{i_1} e'_{1I}, h_{1I} \not\to \qquad\qquad \mathit{pack}\, e'_{1I}, h_{1I} \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

Since $\Delta; \Gamma \models e_{1I} \leq e_{1S} : \sigma[\tau/\alpha]$ it follows that there exists $W'' \geq W'$, v_{1S}, and h_{1S} such that

$$\sigma_S(e_{1S}), h_S \to^* v_{1S}, h_{1S} \quad (n' - i_1, h_{1I}, h_{1S}) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \sigma[\tau/\alpha]]\!]_\rho(W'')$$

and $e'_{1I} \in \mathit{Val}$. Thus, $i_2 = 0$, $e'_I = \mathit{pack}\ e'_{1I}$ and $h'_I = h_{1I}$.

By Lemma 29, $\forall m.\ (n' - i_1, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta, \alpha \vdash \sigma]\!]_{\rho[\alpha \mapsto \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho]}(W'')$ and thus

$$\forall m.\ (n' - i_1, m, \mathit{pack}\ e'_{1I}, \mathit{pack}\ v_{1S}) \in \mathcal{V}[\![\Delta \vdash \exists \alpha.\ \sigma]\!]_\rho(W'').$$

□

Lemma 32. *If* $\Delta; \Gamma \vdash e_{1I} \leq e_{1S} : \exists \alpha.\ \tau,\ \Delta, \alpha; \Gamma, x : \tau \vdash e_{2I} \leq e_{2S} : \sigma$ *and* $\Delta \vdash \sigma$ *then*

$$\Delta; \Gamma \vdash \mathit{unpack}\ e_{1I}\ \mathit{as}\ x\ \mathit{in}\ e_{2I} \leq \mathit{unpack}\ e_{1S}\ \mathit{as}\ x\ \mathit{in}\ e_{2S} : \sigma.$$

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(\mathit{unpack}\ e_{1I}\ \mathit{as}\ x\ \mathit{in}\ e_{2I}), h_I \to^i e'_I, h'_I \not\to$$

By Lemma 14, there exists i_1, i_2, e'_{1I}, and h_{1I} such that

$$\sigma_I(e_{1I}), h_I \to^{i_1} e'_{1I}, h_{1I} \not\to \qquad\qquad \mathit{unpack}\ e'_{1I}\ \mathit{as}\ x\ \mathit{in}\ \sigma_I(e_{2I}), h_{1I} \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

Since $\Delta; \Gamma \models e_{1I} \leq e_{1S} : \exists \alpha.\ \sigma$ it follows that there exists $W'' \geq W'$, v_{1S}, and h_{1S} such that

$$\sigma_S(e_{1S}), h_S \to^* v_{1S}, h_{1S} \quad (n' - i_1, h_{1I}, h_{1S}) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \exists \alpha.\ \tau]\!]_\rho(W'')$$

and $e'_{1I} \in \mathit{Val}$. Hence, $e'_{1I} = \mathit{pack}\ v_{1I}$ and $v_{1S} = \mathit{pack}\ v'_{1S}$ and there exists a $\nu \in \mathit{Type}$ such that

$$(n' - i_1, 0, v_{1I}, v'_{1S}) \in \mathcal{V}[\![\Delta, \alpha \vdash \tau]\!]_{\rho[\alpha \mapsto \nu]}(W'')$$

Furthermore,

$$\mathit{unpack}\ e'_{1I}\ \mathit{as}\ x\ \mathit{in}\ \sigma(e_{2I}), h_{1I} \to \sigma_I(e_{2I})[v_{1I}/x], h_{1I} \to^{i_2 - 1} e'_I, h'_I$$

and $i_2 \geq 1$.

By downwards-closure, monotonicity and Lemma 30, it follows that

$$\forall m.\ (n' - i_1 - 1, m, \sigma_I[x \mapsto v_{1I}], \sigma_S[x \mapsto v'_{1S}]) \in \mathcal{V}[\![\Delta, \alpha \vdash \Gamma, x : \tau]\!]_{\rho[\alpha \mapsto \nu]}(W'')$$

Since $i_2 - 1 < n' - i_1 - 1$ it follows from the $\Delta, \alpha; \Gamma, x : \tau \vdash e_{2I} \leq e_{2S} : \sigma$ assumption that there exists $W''' \geq W''$, v_S, and h'_S such that $\sigma_S[x \mapsto v'_{1S}](e_{2S}), h_{1S} \to^* v_S, h'_S$ and

$$(n' - i_1 - i_2, h'_I, h'_S) \in \lfloor W''' \rfloor \qquad \forall m.\ (n' - i_1 - i_2, m, e'_I, v_S) \in \mathcal{V}[\![\Delta, \alpha \vdash \sigma]\!]_{\rho[\alpha \mapsto \nu]}(W''')$$

and $e'_I \in \mathit{Val}$. Lastly, since $\Delta \vdash \sigma$ it follows that

$$\forall m.\ (n' - i_1 - i_2, m, e'_I, v_S) \in \mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho(W''')$$

□

Lemma 33. *If* $\Delta;\Gamma \vdash e_{1I} \leq e_{1S} : \tau$ *and* $\Delta;\Gamma \vdash e_{2I} \leq e_{2S} : \sigma$*, then* $\Delta;\Gamma \vdash (e_{1I}, e_{2I}) \leq (e_{1S}, e_{2S}) : \tau \times \sigma$.

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(e_{1I}, e_{2I}), h_I \to^i e'_I, h'_I \not\to$$

By Lemma 14, there exists i_1, i_2, e'_{1I}, and h_{1I} such that

$$\sigma_I(e_{1I}), h_I \to^{i_1} e'_{1I}, h_{1I} \not\to \qquad (e'_{1I}, \sigma_I(e_{2I})), h_{1I} \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

Since $\Delta;\Gamma \models e_{1I} \leq e_{1S} : \tau$ it follows that there exists $W'' \geq W'$, v_{1S}, and h_{1S} such that

$\sigma_S(e_{1S}), h_S \to^* v_{1S}, h_{1S} \quad (n' - i_1, h_{1I}, h_{1S}) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W'')$
and $e'_{1I} \in \mathit{Val}$.

By Lemma 14, there exists i_3, i_4, e'_{2I}, and h_{2I} such that

$$\sigma_I(e_{2I}), h_{1I} \to^{i_3} e'_{2I}, h_{2I} \not\to \qquad (e'_{1I}, e'_{2I}), h_{2I} \to^{i_4} e'_I, h'_I \not\to$$

and $i_2 = i_3 + i_4$.

Since $\Delta;\Gamma \models e_{2I} \leq e_{2S} : \sigma$ it follows that there exists $W''' \geq W''$, v_{2S}, and h_{2S} such that
$\sigma_S(e_{2S}), h_{1S} \to^* v_{2S}, h_{2S} \quad (n' - i_1 - i_3, h_{2I}, h_{2S}) \in \lfloor W''' \rfloor \quad \forall m.\ (n' - i_1 - i_3, m, e'_{2I}, v_{2S}) \in \mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho(W''')$
and $e'_{2I} \in \mathit{Val}$.

Thus $e'_I = (e'_{1I}, e'_{2I})$, $h'_I = h_{2I}$ and $i_4 = 0$. Lastly,

$$\forall m.\ (n' - i, m, (e'_{1I}, e'_{2I}), (v_{1S}, v_{2S})) \in \mathcal{V}[\![\Delta \vdash \tau \times \sigma]\!]_\rho(W''')$$

by downwards-closure and monotonicity. □

Lemma 34. *If* $\Delta;\Gamma \vdash e_I \leq e_S : \tau \times \sigma$ *then* $\Delta;\Gamma \vdash \mathit{fst}\ e_I \leq \mathit{fst}\ e_S : \tau$.

Proof. Assume $\forall m.\ (n, m, \sigma_I, \sigma_S) \in \mathcal{V}[\![\Delta \vdash \Gamma]\!]_\rho(W)$ and

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(\mathit{fst}\ e_I), h_I \to^i e'_I, h'_I \not\to$$

By Lemma 14, there exists i_1, i_2, e''_I, and h''_I such that

$$\sigma_I(e_I), h_I \to^{i_1} e''_I, h''_I \not\to \qquad \mathit{fst}\ e''_I, h''_I \to^{i_2} e'_I, h'_I \not\to$$

and $i = i_1 + i_2$.

Since $\Delta;\Gamma \models e_I \leq e_S : \tau$ it follows that there exists $W'' \geq W'$, v''_S, and h''_S such that

$\sigma_S(e_S), h_S \to^* v''_S, h''_S \quad (n' - i_1, h''_I, h''_S) \in \lfloor W'' \rfloor \quad \forall m.\ (n' - i_1, m, e''_I, v''_S) \in \mathcal{V}[\![\Delta \vdash \tau \times \sigma]\!]_\rho(W'')$
and $e''_I \in \mathit{Val}$.

Thus, $(n' - i_1, 0, e''_I, v''_S) \in \mathcal{V}[\![\Delta \vdash \tau \times \sigma]\!]_\rho(W'')$ and there exists v_{1I}, v_{2I} and v_{1S}, v_{2S} such that

$$e''_I = (v_{1I}, v_{2I}) \qquad v''_S = (v_{1S}, v_{2S})$$

and

$$(n' - i_1, 0, v_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W'') \qquad (n' - i_1, 0, v_{2I}, v_{2S}) \in \mathcal{V}[\![\Delta \vdash \sigma]\!]_\rho(W'')$$

Thus, by downwards-closure,

$$\forall m.\ (n' - i_1 - 1, m, v_{1I}, v_{1S}) \in \mathcal{V}[\![\Delta \vdash \tau]\!]_\rho(W'')$$

Lastly, $e'_I = v_{1I}$, $h'_I = h''_I$ and $i_2 = 1$. □

3.2 Soundness

Theorem 2 (Fundamental theorem of logical relations)**.** *If* $\Delta; \Gamma \vdash e : \tau$ *then* $\Delta; \Gamma \models e \leq e : \tau$.

Theorem 3. *If* $- \models e_I \leq e_S : 1$ *and* $e_I, [] \to^* v_I, h_I'$ *then then there exists a* h_S' *such that* $e_S, [] \to^* *, h_S'$.

Proof. Trivial. □

3.3 Example

Lemma 35. *Let* τ *denote the type*

$$\exists \alpha.\ (1 \to \alpha) \times (\alpha \to \mathbb{N})$$

Then,

$$-; x : \tau \mid x \leq_{log} f(x) : \tau$$

where f *is defined as follows*

$$f \stackrel{def}{=} \lambda x.\mathit{unpack}\ x\ \mathit{as}\ y\ \mathit{in}\ \mathit{pack}\ (\lambda z.\mathit{ref}\ (\mathit{fst}\ y\ z), \lambda z.\mathit{snd}\ y\ (!z))$$

Proof. Assume

$$(n, 0, \sigma_I, \sigma_S) \in \mathcal{V}[\![-; x : \tau]\!]_{[]}(W)$$

Thus, there exists a $\nu \in \mathit{Type}$ and v_{1I}, v_{2I}, v_{1S} and v_{2S} such that

$$\sigma_I(x) = \mathit{pack}\ (v_{1I}, v_{2I}) \qquad \sigma_S(x) = \mathit{pack}\ (v_{1S}, v_{2S}) \qquad (n, 0, v_{1I}, v_{1S}) \in \mathcal{V}[\![\alpha \vdash 1 \to \alpha]\!]_{[\alpha \mapsto \nu]}(W)$$

and $(n, 0, v_{2I}, v_{2S}) \in \mathcal{V}[\![\alpha \vdash \alpha \to \mathbb{N}]\!]_{[\alpha \mapsto \nu]}(W)$.

To show that $(n, \sigma_I(x), \sigma_S(f(x))) \in \mathcal{E}(\mathcal{V}[\![- \vdash \tau]\!]_{[]})(W)$ assume

$$i < n' \leq n \qquad W' \geq W \qquad (n', h_I, h_S) \in \lfloor W' \rfloor \qquad \sigma_I(x), h_I \to^i e_I', h_I' \not\to$$

Since $\sigma_I(x)$ is a value, $h_I' = h_I$, $e_I' = \sigma_I(x)$ and $i = 0$.

Since $\sigma_S(f(x)), h_S \to^* v_S, h_S$, where $v_S = \mathit{pack}\ (\lambda z.\mathit{ref}\ ((\mathit{fst}\ (v_{1S}, v_{2S}))(z)), \lambda z.\mathit{snd}\ (v_{1S}, v_{2S})(!z))$, it just remains to show that

$$(n', h_I, h_S) \in \lfloor W \rfloor \qquad\qquad (n', \sigma_I(x), v_S) \in \mathcal{V}[\![- \vdash \tau]\!]_{[]}(W)$$

The first proof obligation holds trivially.

For the second proof obligation, let

$$\nu' = \lambda W.\ \{(n, m, v_I, v_S) \mid \exists \iota \in \mathit{dom}(W).\ \xi(W(\iota)) \stackrel{n,m}{=}_{\blacktriangleright \widehat{Inv}} S(v_I, v_S)\}$$

and $\rho = [\alpha \mapsto \nu']$, where

$$S(v_I, l_S) \stackrel{def}{=} \lambda W.\ \{(n, m, h_I, h_S) \mid l_S \in \mathit{dom}(h_S) \wedge (n, m, v_I, h_S(l_S)) \in \nu(W)\}$$

Then it remains to show that

$$\forall m.\ (n', m, v_{1I}, \lambda z.\mathit{ref}\ ((\mathit{fst}\ (v_{1S}, v_{2S}))(z))) \in \mathcal{V}[\![\alpha \vdash 1 \to \alpha]\!]_\rho(W')$$
$$\forall m.\ (n', m, v_{2I}, \lambda z.\mathit{snd}\ (v_{1S}, v_{2S})(!z)) \in \mathcal{V}[\![\alpha \vdash \alpha \to \mathbb{N}]\!]_\rho(W')$$

First function: Assume

$$n'' < n' \qquad W'' \geq W' \qquad \forall m.\ (n'', m, u_I, u_S) \in \mathcal{V}[\![\alpha \vdash 1]\!]_\rho(W'')$$

To show that $(n''+1, v_{1I}\ u_I, (\lambda z.\mathit{ref}\ ((\mathit{fst}\ (v_{1S}, v_{2S}))(z)))\ u_S) \in \mathcal{E}(\mathcal{V}[\![\alpha \vdash \alpha]\!]_\rho)(W'')$, assume

$$j < k \leq n''+1 \qquad W_1 \geq W'' \qquad (k, h_{1I}, h_{1S}) \in \lfloor W_1 \rfloor \qquad v_{1I}\ u_I, h_{1I} \to^j e'_{1I}, h'_{1I} \not\to$$

By downwards-closure and monotonicity, it follows that $(n''+1, 0, v_{1I}, v_{1S}) \in \mathcal{V}[\![\alpha \vdash 1 \to \alpha]\!]_{[\alpha \mapsto \nu]}(W_1)$. Thus, there exists v_{1S}, h'_{1S} and $W'_1 \geq W_1$ such that $e'_{1I} \in \mathit{Val}$ and

$$v_{1S}\ u_S, h_{1S} \to^* v_{1S}, h'_{1S} \quad (k-j, h'_{1I}, h'_{1S}) \in \lfloor W'_1 \rfloor \quad \forall m.\ (k-j, m, e'_{1I}, v_{1S}) \in \mathcal{V}[\![\alpha \vdash \alpha]\!]_{[\alpha \mapsto \nu]}(W'_1) = \nu(W'_1)$$

Pick a fresh location $l_S \notin \mathit{dom}(h'_{1S})$. Then

$$(\lambda z.\mathit{ref}\ ((\mathit{fst}\ (v_{1S}, v_{2S}))(z)))\ u_S, h_{1S} \to^* l_S, h'_{1S}[l_S \mapsto v_{1S}]$$

Pick a fresh invariant name $\iota \notin \mathit{dom}(W'_1)$ and let $W''_1 = W'_1[\iota \mapsto \xi^{-1}(S(e'_{1I}, l_S))]$. Then it remains to show that

$$(k-j, h'_{1I}, h'_{1S}[l_S \mapsto v_{1S}]) \in \lfloor W''_1 \rfloor \qquad \forall m.\ (k-j, m, e'_{1I}, l_S) \in \mathcal{V}[\![\alpha \vdash \alpha]\!]_\rho(W''_1)$$

The first obligation reduces to proving that

$$\forall m.\ (k-j-1, m, [], [l_S \mapsto v_{1S}]) \in S(e'_{1I}, l_S)(W''_1)$$

which further reduces to proving that $\forall m.\ (k-j-1, m, e'_{1I}, v_{1S}) \in \nu(W''_1)$. This follows easily by downwards-closure and monotonicity.

The second proof obligation reduces to,

$$\forall m.\ \exists \iota \in \mathit{dom}(W''_1).\ \xi(W''_1(\iota))\ {}^{k-j,m}_{\blacktriangleright \widehat{\mathit{Type}}}\ S(e'_{1I}, l_S)$$

which is easily seen to hold, as ${}^{k-j,m}_{\blacktriangleright \widehat{\mathit{Type}}}$ is an equivalence relation.

Second function: Assume

$$n'' < n' \qquad W'' \geq W' \qquad \forall m.\ (n'', m, u_I, u_S) \in \mathcal{V}[\![\alpha \vdash \alpha]\!]_\rho(W'') = \nu'(W'')$$

To show that $(n''+1, v_{2I}\ u_I, (\lambda z.\mathit{snd}\ (v_{1S}, v_{2S})(!z))\ u_S) \in \mathcal{E}(\mathcal{V}[\![\alpha \vdash \mathbb{N}]\!]_\rho)(W'')$, assume

$$j < k \leq n''+1 \qquad W_2 \geq W'' \qquad (k, h_{2I}, h_{2S}) \in \lfloor W_2 \rfloor \qquad v_{2I}\ u_I, h_{2I} \to^j e'_{2I}, h'_{2I} \not\to$$

To show that $\forall m.\ (k-1, m, u_I, h'_{2S}(u_S)) \in \nu(W_2)$, assume $m \in \mathbb{N}$. By assumption, $(n'', m+1, u_I, u_S) \in \nu'(W'')$ and thus, there exists an $\iota \in \mathit{dom}(W'')$ such that $\xi(W''(\iota))\ {}^{n'',m+1}_{\blacktriangleright \widehat{\mathit{Type}}}\ S(u_I, u_S)$. Furthermore, by the extension ordering on worlds, $W_2(\iota) = W''(\iota)$ and by world satisfaction, there exists h'_{2I} and h'_{2S} such that

$$h'_{2I} \leq h_{2I} \qquad h'_{2S} \leq h_{2S} \qquad \forall m'.\ (k-1, m', h'_{2I}, h'_{2S}) \in \xi(W''(\iota))(W'')$$

Since $(k-1, m) < (n'', m+1)$ it follows that $(k-1, m, h'_{2I}, h'_{2S}) \in S(u_I, u_S)(W_2)$ and thus,

$$(k-1, m, u_I, h'_{2S}(u_S)) \in \nu(W_2)$$

□