A Relational Logic for Higher-Order Programs (Additional material)

ALEJANDRO AGUIRRE, IMDEA Software Institute, Spain
GILLES BARTHE, IMDEA Software Institute, Spain
MARCO GABOARDI, University at Buffalo, SUNY, USA
DEEPAK GARG, MPI-SWS, Germany
PIERRE-YVES STRUB, École Polytechnique, France

ACM Reference format:
Alejandro Aguirre, Gilles Barthe, Marco Gaboardi, Deepak Garg, and Pierre-Yves Strub. 2017. A Relational Logic for Higher-Order Programs (Additional material). *Proc. ACM Program. Lang.* 1, 1, Article 21 (September 2017), 31 pages.
https://doi.org/10.1145/3110265

A SEMANTICS

Semantics of HOL

Types. The interpretation for the types corresponds directly to the usual representation of pairs, lists and functions in set theory.

$$
\begin{aligned}
[\![\mathbb{B}]\!] &\triangleq \{\mathsf{ff}, \mathsf{tt}\} \\
[\![\mathbb{N}]\!] &\triangleq \mathbb{N} \\
[\![\mathsf{list}_\tau]\!] &\triangleq \mathsf{list}_{[\![\tau]\!]} \\
[\![\tau_1 \times \tau_2]\!] &\triangleq [\![\tau_1]\!] \times [\![\tau_2]\!] \\
[\![\tau_1 \to \tau_2]\!] &\triangleq [\![\tau_1]\!] \to [\![\tau_2]\!]
\end{aligned}
$$

Terms. The terms are given an interpretation with respect to a valuation ρ which is a partial function mapping variables to elements in the interpretation of their type. Given ρ, we use the notation $\rho[v/x]$ to denote the unique extension of ρ such that if $y = x$ then $\rho[v/x](y) = v$ and, otherwise, $\rho[v/x](y) = \rho(y)$.

2475-1421/2017/9-ART21
https://doi.org/10.1145/3110265

$$(\!|x|\!)_\rho \triangleq \rho(x) \qquad (\!|\langle t,u\rangle|\!)_\rho := \langle (\!|t|\!)_\rho, (\!|u|\!)_\rho\rangle \qquad (\!|\pi_i\ t|\!)_\rho \triangleq \pi_i((\!|t|\!)_\rho) \qquad (\!|\lambda x:\tau.t|\!)_\rho \triangleq \lambda v : [\![\tau]\!].(\!|x|\!)_{\rho[(\!|v|\!)_\rho/v]}$$

$$(\!|c|\!)_\rho \triangleq c \qquad (\!|S\ t|\!)_\rho \triangleq S\ (\!|t|\!)_\rho \qquad (\!|t :: u|\!)_\rho \triangleq (\!|t|\!)_\rho :: (\!|u|\!)_\rho$$

$$(\!|\text{case } t \text{ of } [] \mapsto u; \_ :: \_ \mapsto v|\!)_\rho \triangleq \begin{cases} (\!|u|\!)_\rho & \text{if } (\!|t|\!)_\rho = [] \\ (\!|v|\!)_\rho\ M\ N & \text{if } (\!|t|\!)_\rho = M :: N \end{cases}$$

$$(\!|\text{letrec } f\ x = t|\!)_\rho \triangleq F \ \ \text{where } F \text{ is the unique solution of the fixpoint equation}$$

Formulas. We assume that for predicate P of arity $\tau_1 \times \cdots \times \tau_n$, we have an interpretation $[\![P]\!] \in [\![\tau_1]\!] \times \cdots \times [\![\tau_n]\!]$ that satisfies the axioms for P. The interpretation of a formula is defined as follows:

$$\begin{array}{rcl}
(\!|P(t_1,\ldots,t_n)|\!)_\rho & \triangleq & ([\![t_1]\!]_\rho, \ldots, [\![t_n]\!]_\rho) \in [\![P]\!] \\
(\!|\top|\!)_\rho & \triangleq & \tilde{\top} \\
(\!|\bot|\!)_\rho & \triangleq & \tilde{\bot} \\
(\!|\phi_1 \wedge \phi_2|\!)_\rho & \triangleq & (\!|\phi_1|\!)_\rho \mathrel{\tilde{\wedge}} (\!|\phi_2|\!)_\rho \\
(\!|\phi_1 \Rightarrow \phi_2|\!)_\rho & \triangleq & (\!|\phi_1|\!)_\rho \mathrel{\tilde{\Rightarrow}} (\!|\phi_2|\!)_\rho \\
(\!|\forall x:\tau.\phi|\!)_\rho & \triangleq & \tilde{\forall} v. v \in [\![\tau]\!] \mathrel{\tilde{\Rightarrow}} (\!|\phi|\!)_{\rho[v/x]}
\end{array}$$

where we use the tilde ($\sim$) to distinguish between the (R)HOL connectives and the meta-level connectives.

Soundness. We have the following result:

Theorem 2 (Soundness of set-theoretical semantics)**.** If $\Gamma \mid \Psi \vdash \phi$, then for every valuation $\rho \models \Gamma$, $\bigwedge_{\psi\in\Psi}(\!|\psi|\!)_\rho$ implies $(\!|\phi|\!)_\rho$.

Proof. By induction on the length of the derivation of $\Gamma \mid \Psi \vdash \phi$. □

Semantics of UHOL

The intended meaning of a UHOL judgment $\Gamma \mid \Psi \vdash t : \tau \mid \phi$ is:

$$\text{for all } \rho.\text{ s.t. } \rho \models \Gamma,\ (\!|\bigwedge \Psi|\!)_\rho \ \text{ implies } \ (\!|\phi|\!)_{\rho[(\!|t|\!)_\rho/\mathbf{r}]}$$

We have the following result:

Corollary 4 (Set-theoretical soundness and consistency of UHOL)**.** If $\Gamma \mid \Psi \vdash t : \sigma \mid \phi$, then for every valuation $\rho \models \Gamma$, $\bigwedge_{\psi\in\Psi}(\!|\psi|\!)_\rho$ implies $(\!|\phi|\!)_{\rho[(\!|t|\!)_\rho/\mathbf{r}]}$. In particular, there is no proof of $\Gamma \mid \emptyset \vdash t : \sigma \mid \bot$ in UHOL.

Proof. It is a direct consequence of the embedding from UHOL into HOL and the soundness of HOL. □

Semantics of RHOL

The intended meaning of a RHOL judgment $\Gamma \mid \Psi \vdash t_1 : \tau_1 \sim t_2 : \tau_2 \mid \phi$ is:

$$\text{for all } \rho.\text{ s.t. } \rho \models \Gamma,\ (\!|\bigwedge \Psi|\!)_\rho \ \text{ implies } \ (\!|\phi|\!)_{\rho[(\!|t_1|\!)_\rho/\mathbf{r}_1][(\!|t_2|\!)_\rho/\mathbf{r}_2]}$$

We have the following result:

Corollary 7 (Set-theoretical soundness and consistency of RHOL). If $\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi$, then for every valuation $\rho \models \Gamma$, $\bigwedge_{\psi \in \Psi} (\!|\psi|\!)_\rho$ implies $(\!|\phi|\!)_{\rho[(\!|t_1|\!)_\rho/\mathbf{r}_1],[(\!|t_2|\!)_\rho/\mathbf{r}_2]}$. In particular, there is no proof of $\Gamma \mid \emptyset \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \bot$ for any Γ.

Proof. It is a direct consequence of the embedding of RHOL into HOL and the soundness of HOL. □

B ADDITIONAL RULES

For reasons of space, we have omitted some derivable and admissible rules in HOL, UHOL and RHOL. These are useful to prove some theorems and examples. We now discuss the most interesting among them:

HOL

The following rules are derivable in HOL:

- A cut rule can be derived from $[\Rightarrow_I]$ and $[\Rightarrow_E]$:

$$\frac{\Gamma \mid \Psi, \phi' \vdash \phi \quad \Gamma \mid \Psi \vdash \phi'}{\Gamma \mid \Psi \vdash \phi}\ \mathsf{CUT}$$

- A rule for case analysis can be derived from [LIST]:

$$\frac{\Gamma \vdash l : \mathsf{list}_\tau \quad \Gamma \mid \Psi, l = [] \vdash \phi \quad \Gamma, h : \tau, t : \mathsf{list}_\tau \mid \Psi, l = h :: t \vdash \phi}{\Gamma \mid \Psi \vdash \phi}\ \mathsf{DESTR-LIST}$$

- A rule for strong induction can be derived from [LIST]:

$$\frac{\Gamma \mid \Psi \vdash \phi[[]/t] \quad \Gamma, h : \tau, t : \mathsf{list}_\tau \mid \Psi, \forall u : \mathsf{list}_\tau . |u| \leq |t| \Rightarrow \phi[u/t] \vdash \phi[h :: t/t]}{\Gamma \mid \Psi \vdash \forall t : \mathsf{list}_\tau . \phi}\ \mathsf{S-LIST}$$

- A rule for (weak) double induction can be derived by applying [LIST] twice:

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash \phi[[]/l_1][[]/l_2] \\ \Gamma, h_1 : \tau_1, t_1 : \mathsf{list}_{\tau_1} \mid \Psi, \phi[t_1/l_1][[]/l_2] \vdash \phi[h_1 :: t_1/l_1][[]/l_2] \\ \Gamma, h_2 : \tau_2, t_2 : \mathsf{list}_{\tau_2} \mid \Psi, \phi[[]/l_1][t_2/l_2] \vdash \phi[[]/l_1][h_2 :: t_2/l_2] \\ \Gamma, h_1 : \tau_1, t_2 : \mathsf{list}_{\tau_2}, h_2 : \tau_2, t_2 : \mathsf{list}_{\tau_2} \mid \Psi, \phi[t_1/l_1][t_2/l_2] \vdash \phi[h_1 :: t_1/l_1][h_2 :: t_2/l_2]\end{array}}{\Gamma \mid \Psi \vdash \forall l_1 l_2 . \phi}\ \mathsf{D-LIST}$$

- A rule for strong double induction can be derived from [D-LIST]:

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash \phi[[]/l_1][[]/l_2] \\ \Gamma, h_1 : \tau_1, t_1 : \mathsf{list}_{\tau_1} \mid \Psi, \forall m_1 . |m_1| \leq |t_1| \Rightarrow \phi[m_1/l_1][[]/l_2] \vdash \phi[h_1 :: t_1/l_1][[]/l_2] \\ \Gamma, h_2 : \tau_2, t_2 : \mathsf{list}_{\tau_2} \mid \Psi, \forall m_2 . |m_2| \leq |t_2| \Rightarrow \phi[[]/l_1][m_2/l_2] \vdash \phi[[]/l_1][h_2 :: t_2/l_2] \\ \Gamma, h_1 : \tau_1, t_1 : \mathsf{list}_{\tau_1}, h_2 : \tau_2, t_2 : \mathsf{list}_{\tau_2} \mid \\ \Psi, \forall m_1 m_2 . (|m_1|, |m_2|) < (|h_1 :: t_1|, |h_2 :: t_2|) \Rightarrow \phi[m_1/l_1][m_2/l_2] \vdash \phi[h_1 :: t_1/l_1][h_2 :: t_2/l_2]\end{array}}{\Gamma \mid \Psi \vdash \forall l_1 l_2 . \phi}\ \mathsf{S-D-LIST}$$

RHOL

The following version of the case rule is admissible:

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathsf{list}_{\tau_1} \sim t_2 : \mathsf{list}_{\tau_2} \mid \phi' \land (\mathbf{r}_1 = 0 \Leftrightarrow \mathbf{r}_2 = 0)\\ \Gamma \mid \Psi, \phi'[0/\mathbf{r}_1][0/\mathbf{r}_2] \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \mathbb{N} \to \sigma_1 \sim v_2 : \mathbb{N} \to \sigma_2 \mid \forall x_1 x_2 . \phi'[Sx_1/\mathbf{r}_1][Sx_2/\mathbf{r}_2] \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ 0 \mapsto u_1; S \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ 0 \mapsto u_2; S \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{NATCASE}*$$

and the one sided version:

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathsf{list}_{\tau_1} \sim t_2 : \sigma_2 \mid \phi'\\ \Gamma \mid \Psi, \phi'[0/\mathbf{r}_1][t_2/\mathbf{r}_2] \vdash u_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \mathbb{N} \to \sigma_1 \sim t_2 : \sigma_2 \mid \forall x_1 . \phi'[Sx_1/\mathbf{r}_1] \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ 0 \mapsto u_1; S \mapsto v_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}\ \textsf{NATCASE} * -\textsf{L}$$

Notice that we can always recover the initial version of the rule by instantiating ϕ' as $t_1 = \mathbf{r}_1 \land t_2 = \mathbf{r}_2$.

C PROOFS

Proof of Theorem 6

Theorem 6 (Equivalence with HOL). For every context Γ, simple types σ_1 and σ_2, terms t_1 and t_2, set of assertions Ψ and assertion ϕ, if $\Gamma \vdash t_1 : \sigma_1$ and $\Gamma \vdash t_2 : \sigma_2$, then the following are equivalent:

- $\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi$
- $\Gamma \mid \Psi \vdash \phi[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2]$

Proof. The easier direction is the reverse implication. To prove it, one just notices that we can trivially apply [SUB] instantiating ϕ' as a tautology that matches the structure of the types. For instance, for a base type $\mathbb{N}$ we would use $\top$, for an arrow type $\mathbb{N} \to \mathbb{N}$ we would use $\forall x. \bot \Rightarrow \top$, and so on.

We now prove the direct implication by induction on the derivation of $\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi$. Suppose the last rule is:

Case. [VAR] (similarly, [NIL] and [PROJ])
The premise of the rule is already the judgment we want to prove.

Case. [ABS] $\dfrac{\Gamma, x_1 : \tau_1, x_2 : \tau_2 \mid \Psi, \phi' \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}{\Gamma \mid \Psi \vdash \lambda x_1 . t_1 : \tau_1 \to \sigma_1 \sim \lambda x_2 . t_2 : \tau_2 \to \sigma_2 \mid \forall x_1, x_2 . \phi' \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]}$

By applying the induction hypothesis on the premise:

$$\Gamma, x_1 : \tau_1, x_2 : \tau_2 \mid \Psi, \phi' \vdash \phi[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2] \tag{1}$$

By applying $[\Rightarrow_I]$ on (1):

$$\Gamma, x_1 : \tau_1, x_2 : \tau_2 \mid \Psi \vdash \phi' \Rightarrow \phi[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2]$$

By applying $[\forall_I]$ twice on (2):

$$\Gamma \mid \Psi \vdash \forall x_1 x_2 . \phi' \Rightarrow \phi[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2] \tag{3}$$

Finally, by applying CONV on (3):

$$\Gamma \mid \Psi \vdash \forall x_1 x_2 . \phi' \Rightarrow \phi[(\lambda x_1 . t_1)\ x_1/\mathbf{r}_1][(\lambda x_2 . t_2)\ x_2/\mathbf{r}_2]$$

Proof for [ABS-L] (and [ABS-R]) is analogous.

Case. [APP] $\dfrac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \tau_1 \to \sigma_1 \sim t_2 : \tau_2 \to \sigma_2 \mid \forall x_1, x_2 . \phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]\\ \Gamma \mid \Psi \vdash u_1 : \tau_1 \sim u_2 : \tau_2 \mid \phi'\end{array}}{\Gamma \mid \Psi \vdash t_1 u_1 : \sigma_1 \sim t_2 u_2 : \sigma_2 \mid \phi[u_1/x_1][u_2/x_2]}$

By applying the induction hypothesis on the premises we have:
$\Gamma \mid \Psi \vdash \forall x_1 x_2 . \phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi[t_1\ x_1/\mathbf{r}_1][t_2\ x_2/\mathbf{r}_2]$ (1)
and
$\Gamma \mid \Psi \vdash \phi'[u_1/\mathbf{r}_1][u_2/\mathbf{r}_2]$ (2)
By applying twice $[\forall_E]$ to (1) with u_1, u_2:
$\Gamma \mid \Psi \vdash \phi'[u_1/\mathbf{r}_1][u_2/\mathbf{r}_2] \Rightarrow \phi[t_1\ u_1/\mathbf{r}_1][t_2\ u_2/\mathbf{r}_2]$ (3)
and by applying $[\Rightarrow_E]$ to (3) and (2):
$\Gamma \mid \Psi \vdash \phi[t_1\ u_1/\mathbf{r}_1][t_2\ u_2/\mathbf{r}_2]$
Proof for [APP-L] (and APP-R) is analogous, and it uses the UHOL embedding for the premise about the argument. Proofs for [CONS] and [PAIR] are very similar as well.

Case. [SUB] $\dfrac{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi' \qquad \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi'[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2] \Rightarrow \phi[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}$

Applying the inductive hypothesis on the premises we have:
$\Gamma \mid \Psi \vdash \phi'[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2]$
and
$\Gamma \mid \Psi \vdash \phi'[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2] \Rightarrow \phi[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2]$
The proof is simply applying $[\Rightarrow_E]$.

Case. [LETREC] $\dfrac{\mathcal{D}ef(f_1, x_1, e_1) \ \ \mathcal{D}ef(f_2, x_2, e_2) \qquad \begin{array}{c} \Gamma, x_1 : I_1, x_2 : I_2, f_1 : I_1 \to \sigma, f_2 : I_2 \to \sigma_2 \mid \Psi, \phi', \\ \forall m_1 m_2 . (|m_1|, |m_2|) < (|x_1|, |x_2|) \Rightarrow \phi'[m_1/x_1][m_2/x_2] \Rightarrow \\ \phi[m_1/x_1][m_2/x_2][f_1\ m_1/\mathbf{r}_1][f_2\ m_2/\mathbf{r}_2] \vdash \\ e_1 : \sigma_1 \sim e_2 : \sigma_2 \mid \phi \end{array}}{\begin{array}{c} \Gamma \mid \Psi \vdash \text{letrec } f_1\ x_1 \ = e_1 : I_1 \to \sigma_2 \sim \text{letrec } f_2\ x_2 \ = e_2 : I_2 \to \sigma_2 \mid \\ \forall x_1 x_2 . \phi' \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2] \end{array}}$

As an example, we prove the list and nat case, but for other datatypes the proof is similar. Applying the inductive hypothesis on the premise we have:

$$\Gamma, l_1, n_2, f_1, f_2 \mid \Psi, \forall m_1 m_2 . (|m_1|, |m_2|) < (|l_1|, |n_2|) \Rightarrow \phi[f_1 m_1/\mathbf{r}_1][f_2 m_2/\mathbf{r}_2] \vdash \phi[e_1/\mathbf{r}_1][e_2/\mathbf{r}_2]$$

By $[\forall_I]$ we derive:

$$\Gamma \mid \Psi \vdash \forall f_1, f_2, l_1, n_2 . (\forall m_1 m_2 . (|m_1|, |m_2|) < (|l_1|, |n_2|) \Rightarrow \phi[f_1 m_1/\mathbf{r}_1][f_2 m_2/\mathbf{r}_2]) \Rightarrow \phi[e_1/\mathbf{r}_1][e_2/\mathbf{r}_2]. \qquad (\Phi)$$

We want to prove

$$\Gamma \mid \Psi \vdash \forall l_1 n_2 . \phi[F_1\ l_1/\mathbf{r}_1][F_2\ n_2/\mathbf{r}_2]$$

where we use the abbreviations

$$\begin{array}{rcl} F_1 & := & \text{letrec } f_1\ x_1 = e_1 \\ F_2 & := & \text{letrec } f_2\ x_2 = e_2 \end{array}$$

We will use strong double induction over natural numbers and lists. We need to prove four premises. Since we can prove (Φ) from Γ, Ψ, we can add it to the axioms:

(A) $\Gamma \mid \Psi, \Phi \vdash \phi[F_1\ []/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2]$
(B) $\Gamma, h_1, t_1 \mid \Psi, \Phi, \forall m_1 . |m_1| \leq |t_1| \Rightarrow \phi[F_1\ m_1/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2] \vdash \phi[F_1\ (h_1 :: t_1)/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2]$
(C) $\Gamma, x_2 \mid \Psi, \Phi, \forall m_2 . |m_2| \leq |x_2| \Rightarrow \phi[F_1\ []/\mathbf{r}_1][F_2\ m_2/\mathbf{r}_2] \vdash \phi[F_1\ []/\mathbf{r}_1][F_2\ (S x_2)/\mathbf{r}_2]$

(D) $\Gamma, h_1, t_1, x_2 \mid \Psi, \Phi, \forall m_1 m_2.(|m_1|, |m_2|) < (|h_1 :: t_1|, |Sx_2|) \Rightarrow$
$\phi[F_1\ m_1/\mathbf{r}_1][F_2\ m_2/\mathbf{r}_2] \vdash \phi[F_1\ (h_1 :: t_1)/\mathbf{r}_1][F_2\ (Sx_2)/\mathbf{r}_2]$

To prove them, we will instantiate the quantifiers in Φ with the appropriate variables.

To prove (A), we instantiate Φ at $F_1, F_2, [], 0$:

$$(\forall m_1 m_2.(|m_1|, |m_2|) < (|[]|, |0|) \Rightarrow \phi[F_1 m_1/\mathbf{r}_1][F_2 m_2/\mathbf{r}_2]) \Rightarrow \phi[e_1/\mathbf{r}_1][e_2/\mathbf{r}_2][[]/l_1][0/n_2][F_1/f_1][F_2/f_2]$$

and, since $(|m_1|, |m_2|) < (|[]|, |0|)$ is trivially false, then

$$\phi[e_1/\mathbf{r}_1][e_2/\mathbf{r}_2][[]/l_1][0/n_2][F_1/f_1][F_2/f_2]$$

and by beta-expansion and [CONV]:

$$\phi[F_1\ []/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2]$$

.

To prove (B), we instantiate Φ at $F_1, F_2, h_1 :: t_1, 0$

$$(\forall m_1 m_2.(|m_1|, |m_2|) < (|h_1 :: t_1|, |0|) \Rightarrow \phi[F_1 m_1/\mathbf{r}_1][F_2 m_2/\mathbf{r}_2]) \Rightarrow \phi[e_1/\mathbf{r}_1][e_2/\mathbf{r}_2][h_1 :: t_1/l_1][0/n_2][F_1/f_1][F_2/f_2]$$

by beta-expansion:

$$(\forall m_1 m_2.(|m_1|, |m_2|) < (|h_1 :: t_1|, |0|) \Rightarrow \phi[F_1 m_1/\mathbf{r}_1][F_2 m_2/\mathbf{r}_2]) \Rightarrow \phi[F_1\ h_1 :: t_1/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2]$$

Since $(|m_1|, |m_2|) < (|h_1 :: t_1|, |0|)$ is only satisfied if $|m_1| \le |t_1| \wedge m_2 = 0$, we can write it as:

$$(\forall m_1 m_2.(|m_1| \le |t_1| \wedge m_2 = 0) \Rightarrow \phi[F_1 m_1/\mathbf{r}_1][F_2 m_2/\mathbf{r}_2]) \Rightarrow \phi[F_1\ h_1 :: t_1/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2]$$

On the other hand, one of the antecedents of (B) is $\forall m_1.|m_1| \le |t_1| \Rightarrow \phi[F_1\ m_1/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2]$, so by $[\Rightarrow_E]$ we prove $\phi[F_1\ h_1 :: t_1/\mathbf{r}_1][F_2\ 0/\mathbf{r}_2]$, which is the consequent of (B).

The proof of (C) is symmetrical to the proof of (B).

To prove (D), we instantiate Φ at $F_1, F_2, h_1 :: t_1, Sx_2$

$$\begin{gathered}(\forall m_1 m_2.(|m_1|, |m_2|) < (|h_1 :: t_1|, |Sx_2|) \Rightarrow \phi[F_1 m_1/\mathbf{r}_1][F_2 m_2/\mathbf{r}_2]) \Rightarrow \\ \phi[e_1/\mathbf{r}_1][e_2/\mathbf{r}_2][h_1 :: t_1/l_1][Sx_2/n_2][F_1/f_1][F_2/f_2]\end{gathered}$$

by beta-expansion:

$$(\forall m_1 m_2.(|m_1|, |m_2|) < (|h_1 :: t_1|, |Sx_2|) \Rightarrow \phi[F_1 m_1/\mathbf{r}_1][F_2 m_2/\mathbf{r}_2]) \Rightarrow \phi[F_1\ h_1 :: t_1/\mathbf{r}_1][F_2\ (Sx_2)/\mathbf{r}_2]$$

One of the antecedents of (D) is exactly $\forall m_1 m_2.(|m_1|, |m_2|) < (|h_1 :: t_1|, |Sx_2|) \Rightarrow \phi[F_1\ m_1/\mathbf{r}_1][F_2\ m_2/\mathbf{r}_2]$, so by $[\Rightarrow_E]$ we prove $\phi[F_1\ h_1 :: t_1/\mathbf{r}_1][F_2\ (Sx_2)/\mathbf{r}_2]$, which is the consequent of (D).

Proof of [LETREC-L] (and [LETREC-R]) is analogous, and uses simple strong induction.

Case. [CASE]
$$\frac{\begin{gathered}\Gamma \mid \Psi \vdash l_1 : \mathsf{list}_{\tau_1} \sim l_2 : \mathsf{list}_{\tau_2} \mid \mathbf{r}_1 = [] \Leftrightarrow \mathbf{r}_2 = [] \qquad \Gamma \mid \Psi, l_1 = [], l_2 = [] \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \tau_1 \to \mathsf{list}_{\tau_1} \to \sigma_1 \sim v_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \\ \forall h_1 h_2 t_1 t_2. l_1 = h_1 :: t_1 \Rightarrow l_2 = h_2 :: t_2 \Rightarrow \phi[\mathbf{r}_1\ h_1\ t_1/\mathbf{r}_1][\mathbf{r}_2\ h_2\ t_2/\mathbf{r}_2]\end{gathered}}{\Gamma \mid \Psi \vdash \mathsf{case}\ l_1\ \mathsf{of}\ [] \mapsto u_1; \_ :: \_ \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ l_2\ \mathsf{of}\ [] \mapsto u_2; \_ :: \_ \mapsto v_2 : \sigma_2 \mid \phi}$$

We prove the rule for natural numbers. Applying the induction hypothesis to the premises of the rule, we have:

(A) $\Gamma \mid \Psi \vdash t_1 = 0 \Leftrightarrow t_2 = 0$
(B) $\Gamma \mid \Psi, t_1 = 0, t_2 = 0 \vdash \phi[u_1/\mathbf{r}_1][u_2/\mathbf{r}_2]$
(C) $\Gamma \mid \Psi \vdash \forall x_1, x_2. t_1 = Sx_1 \Rightarrow t_2 = Sx_2 \Rightarrow \phi[v_1\ x_1/\mathbf{r}_1][v_2\ x_2/\mathbf{r}_2]$

We want to prove:

$$\Gamma \mid \Psi \vdash \phi[(\text{case } t_1 \text{ of } 0 \mapsto u_1; S \mapsto v_1)/\mathbf{r}_1][(\text{case } t_2 \text{ of } 0 \mapsto u_2; S \mapsto v_2)/\mathbf{r}_2]$$

By applying [DESTR-NAT] twice, we get four premises:

(1) $\Gamma \mid \Psi, t_1 = 0, t_2 = 0 \vdash \phi[(\text{case } t_1 \text{ of } 0 \mapsto u_1; S \mapsto v_1)/\mathbf{r}_1][(\text{case } t_2 \text{ of } 0 \mapsto u_2; S \mapsto v_2)/\mathbf{r}_2]$
(2) $\Gamma, m_2 \mid \Psi, t_1 = 0, t_2 = Sm_2 \vdash \phi[(\text{case } t_1 \text{ of } 0 \mapsto u_1; S \mapsto v_1)/\mathbf{r}_1][(\text{case } t_2 \text{ of } 0 \mapsto u_2; S \mapsto v_2)/\mathbf{r}_2]$
(3) $\Gamma, m_1 \mid \Psi, t_1 = Sm_1, t_2 = 0 \vdash \phi[(\text{case } t_1 \text{ of } 0 \mapsto u_1; S \mapsto v_1)/\mathbf{r}_1][(\text{case } t_2 \text{ of } 0 \mapsto u_2; S \mapsto v_2)/\mathbf{r}_2]$
(4) $\Gamma, m_1, m_2 \mid \Psi, t_1 = Sm_1, t_2 = Sm_2 \vdash \phi[(\text{case } t_1 \text{ of } 0 \mapsto u_1; S \mapsto v_1)/\mathbf{r}_1][(\text{case } t_2 \text{ of } 0 \mapsto u_2; S \mapsto v_2)/\mathbf{r}_2]$

We can prove (2) and (3) by deriving a contradiction with [NC] and (A). After beta-reducing in (1) and (4) we can easily derive them from (B) and (C) respectively.

Proof of [CASE-L] (and [CASE-R]) is analogous.

□

Proof of Lemma 10

Lemma 10 (Embedding lemma)**.** Assume that:

- $\Gamma \mid \Psi \vdash t_1 : \sigma_1 \mid \phi$
- $\Gamma \mid \Psi \vdash t_2 : \sigma_2 \mid \phi'$

Then $\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi[\mathbf{r}_1/\mathbf{r}] \wedge \phi'[\mathbf{r}_2/\mathbf{r}]$.

Proof. By the embedding into HOL, we have:

- $\Gamma \mid \Psi \vdash \phi[t_1/\mathbf{r}]$
- $\Gamma \mid \Psi \vdash \phi'[t_2/\mathbf{r}]$

and by the $[\wedge_I]$ rule,

$$\Gamma \mid \Psi \vdash \phi[t_1/\mathbf{r}] \wedge \phi'[t_2/\mathbf{r}].$$

Finally, by undoing the embedding:

$$\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi.$$

□

Proof of Theorem 11

Theorem 11. If $\Gamma \vdash t : \tau$ is derivable in the refinement type system, then $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t : |\tau| \mid \lfloor\tau\rfloor(\mathbf{r})$ is derivable in UHOL.

Proof. By induction on the derivation:

Case. $x : \tau, \Gamma \vdash x : \tau$
To prove : $x : |\tau|, |\Gamma| \vdash \lfloor\tau\rfloor(x), \lfloor\Gamma\rfloor \vdash x : |\tau| \mid \lfloor\tau\rfloor(\mathbf{r})$. Directly by [VAR].

Case. $\dfrac{\Gamma, x : \tau \vdash t : \sigma}{\Gamma \vdash \lambda x.t : \Pi(x : \tau).\sigma}$
To prove: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash \lambda x.t : |\Pi(x : \tau).\sigma| \mid \lfloor\Pi(x : \tau).\sigma\rfloor(\mathbf{r})$.
Expanding the definitions:
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash \lambda x.t : |\tau| \to |\sigma| \mid \forall x. \lfloor\tau\rfloor(x) \Rightarrow \lfloor\sigma\rfloor(\mathbf{r}x)$
By induction hypothesis on the premise:
$|\Gamma|, x : |\tau| \mid \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(x) \vdash t : |\sigma| \mid \lfloor\sigma\rfloor(\mathbf{r})$
Directly by [ABS].

Case. $\dfrac{\Gamma \vdash t : \Pi(x:\tau).\sigma \qquad \Gamma \vdash u : \tau}{\Gamma \vdash t\ u : \sigma[u/x]}$
To prove: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t\ u : |\sigma[u/x]| \mid \lfloor\sigma[u/x]\rfloor(\mathbf{r})$.
Expanding the definitions:
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t\ e_2 : |\sigma| \mid \lfloor\sigma\rfloor(\mathbf{r})[u/x]$
By induction hypothesis on the premise:
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t : |\tau| \to |\sigma| \mid \forall x.\lfloor\tau\rfloor(x) \Rightarrow \lfloor\sigma\rfloor(\mathbf{r}x)$
and
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash u : |\tau| \mid \lfloor\tau\rfloor(\mathbf{r})$
We get the result directly by [APP].

Case. $\dfrac{\Gamma \vdash t : \mathsf{list}_\tau \qquad \Gamma \vdash u : \sigma \qquad \Gamma \vdash v : \tau \to \mathsf{list}_\tau \to \sigma}{\Gamma \vdash \mathsf{case}\ t\ \mathsf{of}\ [] \mapsto u; \_ :: \_ \mapsto v : \sigma}$
To prove: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash \mathsf{case}\ t\ \mathsf{of}\ [] \mapsto u; \_ :: \_ \mapsto v : |\sigma| \mid \lfloor\sigma\rfloor(\mathbf{r})$
By induction hypothesis on the premises:
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t : |\mathsf{list}_\tau| \mid \lfloor\mathsf{list}_\tau\rfloor(\mathbf{r}),$ (1)
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash u : |\sigma| \mid \lfloor\sigma\rfloor(\mathbf{r}),$ (2)
and
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash v : |\tau \to \mathsf{list}_\tau \to \sigma| \mid \lfloor\tau \to \mathsf{list}_\tau \to \sigma\rfloor(\mathbf{r})$ (3)
Expanding the definitions on (3) we get:
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash v : |\tau| \to |\mathsf{list}_\tau| \to |\sigma| \mid \forall x.\lfloor\tau\rfloor(x) \Rightarrow \forall y.\lfloor\mathsf{list}_\tau\rfloor(y) \Rightarrow \lfloor\sigma\rfloor(\mathbf{r}\ x\ y)$ (4)
And from (1), (2) and (4) we apply [LISTCASE*] and we get the result. Notice that (2) and (4) are stronger than the premises of the rule, so we will first need to apply [SUB] to weaken them

Case. $\dfrac{\Gamma \vdash \tau}{\Gamma \vdash [] : \mathsf{list}_\tau}$
To prove: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash [] : |\mathsf{list}_\tau| \mid \lfloor\mathsf{list}_\tau\rfloor(\mathbf{r})$
Expanding the definitions: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash [] : \mathsf{list}_{|\tau|} \mid \mathrm{All}(\mathbf{r}, x, \lfloor\tau\rfloor(x))$
And by the definition of All for the empty case, trivially $\mathrm{All}([], x, \lfloor\tau\rfloor(x))$, so we apply the [NIL] rule and we get the result.

Case. $\dfrac{\Gamma \vdash h : \tau \qquad \Gamma \vdash t : \mathsf{list}_\tau}{\Gamma \vdash h :: t : \mathsf{list}_\tau}$
To prove: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash h :: t : |\mathsf{list}_\tau| \mid \lfloor\mathsf{list}_\tau\rfloor(\mathbf{r})$.
Expanding the definitions: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash h :: t : \mathsf{list}_{|\tau|} \mid \mathrm{All}(\mathbf{r}, \lambda x.\lfloor\tau\rfloor(x))$.
By induction hypothesis on the premises, we have:
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash h : |\tau| \mid \lfloor\tau\rfloor(\mathbf{r})$
and
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t : \mathsf{list}_{|\tau|} \mid \mathrm{All}(\mathbf{r}, \lambda x.\lfloor\tau\rfloor(x))$.
We complete the proof by the [CONS] rule and the definition of All in the inductive case.

Case. $\dfrac{\Gamma \vdash \tau \preceq \sigma \qquad \Gamma \vdash t : \tau}{\Gamma \vdash t : \sigma}$
To prove: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t : |\sigma| \mid \lfloor\sigma\rfloor(\mathbf{r})$
and, since $|\sigma| \equiv |\tau|$, it is the same as writing

$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t : |\tau| \mid \lfloor\tau\rfloor(\mathbf{r})$
By induction hypothesis on the premises:
$|\Gamma|, x : |\tau| \mid \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(x) \vdash \lfloor\sigma\rfloor(x)$
and
$|\Gamma| \mid \lfloor\Gamma\rfloor \vdash t : |\tau| \mid \lfloor\tau\rfloor(\mathbf{r})$
The proof is completed by applying $[\Rightarrow_I]$ to the first premise, and then [SUB].

Case. $\dfrac{\Gamma, x : \tau, f : \Pi(y : \{\mathbf{r} : \tau \mid y < x\}).\sigma[y/x] \vdash t : \sigma \qquad \mathcal{D}ef(f, x, t)}{\Gamma \vdash \text{letrec } f\ x = t : \Pi(x : \tau).\sigma}$
To prove: $|\Gamma| \mid \lfloor\Gamma\rfloor \vdash \text{letrec } f\ x = t : |\Pi(x : \tau).\sigma| \mid \lfloor\Pi(x : \tau).\sigma\rfloor(\mathbf{r})$
By induction hypothesis on the premise:
$|\Gamma|, x : |\tau|, f : |\tau| \to |\sigma| \mid \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(x), \forall y. \lfloor\tau\rfloor(y) \wedge y < x \Rightarrow \lfloor\sigma[y/x]\rfloor(f y) \vdash t : |\sigma| \mid \lfloor\sigma\rfloor(\mathbf{r})$
Directly by [LETREC].

□

Proof of Theorem 12

Theorem 12. If $\Gamma \vdash \tau \preceq \sigma$ is derivable in a refinement type system, then $|\Gamma|, x : |\tau| \mid \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(x) \vdash \lfloor\sigma\rfloor(x)$ is derivable in HOL.

We will use without proof the following results:

Lemma 21. If $\Gamma \vdash \tau \preceq \sigma$ in refinement types, then $|\tau| \equiv |\sigma|$.

Proof. By induction on the derivation. □

Lemma 22. For every type τ and expression e and variable $x \notin FV(\tau, e)$, $\lfloor\tau\rfloor(e) = \lfloor\tau\rfloor(x)[e/x]$

Proof. By structural induction. □

Now we proceed with the proof of the theorem.

Proof. By induction on the derivation:

Case. $\dfrac{\Gamma \vdash \tau}{\Gamma \vdash \tau \preceq \tau}$
To show: $|\Gamma|, x : |\tau| \mid \lfloor\tau\rfloor(x) \vdash \lfloor\tau\rfloor(x)$. Directly by [AX].

Case. $\dfrac{\Gamma \vdash \tau_1 \preceq \tau_2 \qquad \Gamma \vdash \tau_2 \preceq \tau_3}{\Gamma \vdash \tau_1 \preceq \tau_3}$
To show: $|\Gamma|, x : |\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\tau_1\rfloor(x) \vdash \lfloor\tau_3\rfloor(x)$.
By induction hypothesis on the premises,
$|\Gamma|, x : |\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\tau_1\rfloor(x) \vdash \lfloor\tau_2\rfloor(x)$
and
$|\Gamma|, x : |\tau_2| \mid \lfloor\Gamma\rfloor, \lfloor\tau_2\rfloor(x) \vdash \lfloor\tau_3\rfloor(x)$.
We complete the proof by [CUT]. Notice that $|\tau_1| \equiv |\tau_2| \equiv |\tau_3|$.

Case. $\dfrac{\Gamma \vdash \tau_1 \preceq \tau_2}{\Gamma \vdash \mathsf{list}_{\tau_1} \preceq \mathsf{list}_{\tau_2}}$
To show: $|\Gamma|, x : |\mathsf{list}_{\tau_1}| \mid \lfloor\Gamma\rfloor, \lfloor\mathsf{list}_{\tau_1}\rfloor(x) \vdash \lfloor\mathsf{list}_{\tau_2}\rfloor(\mathbf{r})$

Expanding the definitions: $|\Gamma|, x : \mathsf{list}_{|\tau_1|} \mid \lfloor\Gamma\rfloor, \top \vdash \top$,
which is trivial.

Case. $\dfrac{\Gamma \vdash \{\mathbf{r} : \tau \mid \phi\}}{\Gamma \vdash \{\mathbf{r} : \tau \mid \phi\} \preceq \tau}$
To show: $|\Gamma|, x : |\{\mathbf{r} : \tau \mid \phi\}| \mid \lfloor\{\mathbf{r} : \tau \mid \phi\}\rfloor(x) \vdash \lfloor\tau\rfloor(x)$.
Expanding the definitions: $|\Gamma|, x : |\{\mathbf{r} : \tau \mid \phi\}| \mid \lfloor\tau\rfloor(x) \wedge \phi[x/\mathbf{r}] \vdash \lfloor\tau\rfloor(x)$
and now the proof is completed trivially by $[\wedge_E]$ and [AX].

Case. $\dfrac{\Gamma \vdash \tau \preceq \sigma \qquad \Gamma, \mathbf{r} : \tau \vdash \phi}{\Gamma \vdash \tau \preceq \{\mathbf{r} : \sigma \mid \phi\}}$
To show: $|\Gamma|, \mathbf{r} : |\tau| \vdash \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(\mathbf{r}) \vdash \lfloor\{\mathbf{r} : \sigma \mid \phi\}\rfloor(\mathbf{r})$
Expanding the definition: $|\Gamma|, \mathbf{r} : |\tau| \mid \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(\mathbf{r}) \vdash \lfloor\sigma\rfloor(\mathbf{r}) \wedge \phi$
By induction hypothesis on the premises we have:
$|\Gamma|, \mathbf{r} : |\tau| \mid \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(\mathbf{r}) \vdash \lfloor\sigma\rfloor(\mathbf{r})$
and:
$|\Gamma|, \mathbf{r} : |\tau| \mid \lfloor\Gamma\rfloor, \lfloor\tau\rfloor(\mathbf{r}) \vdash \phi$
We complete the proof by applying the $[\wedge_I]$ rule.

Case. $\dfrac{\Gamma \vdash \sigma_2 \preceq \sigma_1 \qquad \Gamma, x : \sigma_2 \vdash \tau_1 \preceq \tau_2}{\Gamma \vdash \Pi(x : \sigma_1).\tau_1 \preceq \Pi(x : \sigma_2).\tau_2}$
To show: $|\Gamma|, f : |\Pi(x : \sigma_1).\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\Pi(x : \sigma_1).\tau_1\rfloor(f) \vdash \lfloor\Pi(x : \sigma_2).\tau_2\rfloor(f)$
Expanding the definitions:
$|\Gamma|, f : |\Pi(x : \sigma_1).\tau_1| \mid \lfloor\Gamma\rfloor, \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x) \vdash \forall x. \lfloor\sigma_2\rfloor(x) \Rightarrow \lfloor\tau_2\rfloor(f x)$
By the rules $[\forall_I]$ and $[\Rightarrow_I]$ it suffices to prove:
$|\Gamma|, f : |\Pi(x : \sigma_1).\tau_1|, x : |\sigma_2| \mid \lfloor\Gamma\rfloor, \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x), \lfloor\sigma_2\rfloor(x) \vdash \lfloor\tau_2\rfloor(f x)$ (1)
On the other hand, by induction hypothesis on the premises:
$|\Gamma|, x : |\sigma_2| \mid \lfloor\Gamma\rfloor, \lfloor\sigma_2\rfloor(x) \vdash \lfloor\sigma_1\rfloor(x)$ (2)
and
$|\Gamma|, x : |\sigma_2|, y : |\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\sigma_2\rfloor(x), \lfloor\tau_1\rfloor(y) \vdash \lfloor\tau_2\rfloor(y)$ (3)
which we can weaken respectively to:
$|\Gamma|, x : |\sigma_2|, f : |\Pi(x : \sigma_1).\tau_1| \mid |\Gamma|, \lfloor\sigma_2\rfloor(x), \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x) \vdash \lfloor\sigma_1\rfloor(x)$ (4)
and
$|\Gamma|, x : |\sigma_2|, y : |\tau_1|, f : |\Pi(x : \sigma_1).\tau_1| \mid |\Gamma|, \lfloor\sigma_2\rfloor(x), \lfloor\tau_1\rfloor(y), \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x) \vdash \lfloor\tau_2\rfloor(y)$ (5)
From (4), by doing a cut with its own premise $\forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x)$, we derive:
$|\Gamma|, x : |\sigma_2|, f : |\Pi(x : \sigma_1).\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\sigma_2\rfloor(x), \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x) \vdash \lfloor\tau_1\rfloor(f x)$ (6)
From (5), by $[\Rightarrow_I]$ and $[\forall_I]$ we can derive:
$|\Gamma|, x : |\sigma_2|, f : |\Pi(x : \sigma_1).\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\sigma_2\rfloor(x), , \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x) \vdash \forall y. \lfloor\tau_1\rfloor(y) \Rightarrow \lfloor\tau_2\rfloor(y)$
And by $[\forall_E]$
$|\Gamma|, x : |\sigma_2|, f : |\Pi(x : \sigma_1).\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\sigma_2\rfloor(x), , \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x) \vdash \lfloor\tau_1\rfloor(f x) \Rightarrow \lfloor\tau_2\rfloor(f x)$ (7)
Finally, from (6) and (7) by $[\Rightarrow_E]$ we get:
$|\Gamma|, x : |\sigma_2|, f : |\Pi(x : \sigma_1).\tau_1| \mid \lfloor\Gamma\rfloor, \lfloor\sigma_2\rfloor(x), \forall x. \lfloor\sigma_1\rfloor(x) \Rightarrow \lfloor\tau_1\rfloor(f x) \vdash \lfloor\tau_2\rfloor(f x)$
and by one last application of $[\Rightarrow_I]$ we get what we wanted to prove.

□

Proof of Theorem 13

Theorem 13 (Soundness of embedding of relational refinement types). If $\Gamma \vdash t_1 \sim t_2 :: T$, then $|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash t_1 : |T| \sim t_2 : |T| \mid \llbracket T \rrbracket(\mathbf{r}_1, \mathbf{r}_2)$ Also, if $\Gamma \vdash T \leq U$ then $|\Gamma|, x_1, x_2 : |T| \mid \llbracket \Gamma \rrbracket, \llbracket T \rrbracket(x_1, x_2) \vdash \llbracket U \rrbracket(x_1.x_2)$.

We can recover the lemma from the unary case:

Lemma 23. For every type τ, expressions t_1, t_2 and variables $x_1, x_2 \notin FV(\tau, t_1, t_2)$,

$$\llbracket \tau \rrbracket(t_1, t_2) = \llbracket \tau \rrbracket(x_1, x_2)[t_1/x_1][t_2/x_2]$$

Proof. Most cases are very similar to the unary case, so we will only show the most interesting ones:

Case. $\dfrac{\Gamma \vdash T}{\Gamma \vdash [] \sim [] :: \mathsf{list}_T}$

To show: $|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash [] : |\mathsf{list}_T| \sim [] : |\mathsf{list}_T| \mid \llbracket \mathsf{list}_T \rrbracket(\mathbf{r}_1, \mathbf{r}_2)$.
There are two options. If T is a unary type, we have to prove:
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash [] : |\mathsf{list}_T| \sim [] : |\mathsf{list}_T| \mid \bigwedge_{i \in \{1,2\}} \mathrm{All}(\mathbf{r}_i, \lambda x. \lfloor \tau \rfloor(x))$
And by the definition of All we can directly prove:
$\emptyset \mid \emptyset \vdash \mathrm{All}([], \lambda x. \lfloor \tau \rfloor(x)) \wedge \mathrm{All}([], \lambda x. \lfloor \tau \rfloor(x))$
If T is a relational type, we have to prove:
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash [] : |\mathsf{list}_T| \sim [] : |\mathsf{list}_T| \mid \mathrm{All2}(\mathbf{r}_1, \mathbf{r}_2, \lambda x_1. \lambda x_2. \llbracket T \rrbracket(x_1, x_2))$
And by the definition of All2 we can directly prove:
$\emptyset \mid \emptyset \vdash \mathrm{All2}([], [], \lambda x_1. \lambda x_2. \llbracket T \rrbracket(x_1, x_2))$

Case. $\dfrac{\Gamma \vdash h_1 \sim h_2 :: T \qquad \Gamma \vdash t_1 \sim t_2 :: \mathsf{list}_T}{\Gamma \vdash h_1 :: t_1 \sim h_2 :: t_2 :: \mathsf{list}_T}$

To show: $|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash h_1 :: t_2 : |\mathsf{list}_T| \sim h_2 :: t_2 : |\mathsf{list}_T| \mid \mathsf{list}_T$.
There are two options. If T is a unary type, we have to prove:
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash h_1 :: t_1 : |\mathsf{list}_T| \sim h_2 :: t_2 : |\mathsf{list}_T| \mid \bigwedge_{i \in \{1,2\}} \mathrm{All}(\mathbf{r}_i, \lambda x. \lfloor T \rfloor(x))$
By induction hypothesis we have:
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash h_1 : |T| \sim h_2 :: t_2 : |T| \mid \bigwedge_{i \in \{1,2\}} \lfloor T \rfloor(\mathbf{r}_i)$
and
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash t_1 : |\mathsf{list}_T| \sim t_2 : |\mathsf{list}_T| \mid \bigwedge_{i \in \{1,2\}} \mathrm{All}(\mathbf{r}_i, \lambda x. \lfloor T \rfloor(x))$
And by the definition of All we can directly prove:
$\bigwedge_{i \in \{1,2\}} \lfloor T \rfloor(h_i) \Rightarrow \bigwedge_{i \in \{1,2\}} \mathrm{All}(t_i, \lambda x. \lfloor T \rfloor(x)) \Rightarrow \bigwedge_{i \in \{1,2\}} \mathrm{All}(h_i :: t_i, \lambda x. \lfloor T \rfloor(x))$
So by the [CONS] rule, we prove the result. If T is a relational type, we have to prove:
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash h_1 :: t_1 : |\mathsf{list}_T| \sim h_2 :: t_2 : |\mathsf{list}_T| \mid \mathrm{All2}(\mathbf{r}_1, \mathbf{r}_2, \lambda x_1. \lambda x_2. \llbracket T \rrbracket(x_1, x_2))$
By induction hypothesis we have:
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash h_1 : |T| \sim h_2 :: t_2 : |T| \mid \llbracket T \rrbracket(\mathbf{r}_1, \mathbf{r}_2)$
and
$|\Gamma| \mid \llbracket \Gamma \rrbracket \vdash t_1 : |\mathsf{list}_T| \sim t_2 : |\mathsf{list}_T| \mid \mathrm{All2}(\mathbf{r}_1, \mathbf{r}_2, \lambda x_1. \lambda x_2. \llbracket T \rrbracket(x_1, x_2))$
And by the definition of All2 we can directly prove:
$\llbracket T \rrbracket(h_1, h_2) \Rightarrow \mathrm{All2}(t_1, t_2, \lambda x_1. \lambda x_2. \llbracket T \rrbracket(x_1, x_2)) \Rightarrow \mathrm{All}(h_1 :: t_1, h_1 :: h_2, \lambda x_1. \lambda x_2. \llbracket T \rrbracket(x_1, x_2))$
So by the [CONS] rule, we prove the result.

Case. $\dfrac{\Gamma \vdash t_1 \sim t_2 :: \mathsf{list}_T \qquad \Gamma \vdash t_1 = [] \Leftrightarrow t_2 = [] \qquad \Gamma \vdash u_1 \sim u_2 :: U \qquad \Gamma \vdash v_1 \sim v_2 :: \Pi(h :: T). \Pi(t :: \mathsf{list}_T). U}{\Gamma \vdash \mathrm{case}\ t_1\ \mathrm{of}\ [] \mapsto u_1; \_ :: \_ \mapsto v_1 \sim \mathrm{case}\ t_2\ \mathrm{of}\ [] \mapsto u_2; \_ :: \_ \mapsto v_2 :: U}$

To show:

$|\Gamma| \mid \llbracket\Gamma\rrbracket \vdash \text{case } t_1 \text{ of } [] \mapsto u_1; \_ :: \_ \mapsto v_1 : |U| \sim \text{case } t_2 \text{ of } [] \mapsto u_2; \_ :: \_ \mapsto r_2 : |U| \mid \llbracket U\rrbracket(\mathbf{r}_1, \mathbf{r}_2)$
By induction hypothesis we have:
$|\Gamma| \mid \llbracket\Gamma\rrbracket \vdash t_1 = [] \Leftrightarrow t_2 = []$,
$|\Gamma| \mid \llbracket\Gamma\rrbracket \vdash u_1 : |U| \sim u_2 : |U| \mid \llbracket U\rrbracket(\mathbf{r}_1, \mathbf{r}_2)$
and
$|\Gamma| \mid \llbracket\Gamma\rrbracket \vdash v_1 : T \to \text{list}_T \to U \sim v_2 : T \to \text{list}_T \to U \mid \forall h_1 h_2. \llbracket T\rrbracket(h_1, h_2) \Rightarrow \forall t_1 t_2. \llbracket \text{list}_T\rrbracket(t_1, t_2) \Rightarrow \llbracket U\rrbracket(\mathbf{r}_1 h_1 t_1,\ h_2 t_2 \mathbf{r}_2)$
By applying the [LISTCASE*] rule to the three premises we get the result.

Case. $$\frac{\Gamma, x :: T, f :: \Pi(y :: \{y :: T \mid (y_1, y_2) < (x_1, x_2)\}). U[y/x] \vdash t_1 \sim t_2 :: U \qquad \Gamma \vdash \Pi(x :: T). U \qquad \mathcal{Def}(f_1, x_1, t_1) \qquad \mathcal{Def}(f_2, x_2, t_2)}{\Gamma \vdash \text{letrec } f_1\ x_1 = t_1 \sim \text{letrec } f_2\ x_2 = t_2 :: \Pi(x :: T). U}$$
To show:
$|\Gamma| \mid \llbracket\Gamma\rrbracket \vdash \text{letrec } f_1\ x_1 = t_1 : |\Pi(x :: T). U| \sim \text{letrec } f_2\ x_2 = t_2 : |\Pi(x :: T). U| \mid \llbracket \Pi(x :: T). U\rrbracket(\mathbf{r}_1, \mathbf{r}_2)$
Expanding the definitions:
$|\Gamma| \mid \llbracket\Gamma\rrbracket \vdash \text{letrec } f_1\ x_1 = t_1 : |T| \to |U| \sim \text{letrec } f_2\ x_2 = t_2 : |T| \to |U| \mid \forall x_1 x_2. \llbracket T\rrbracket(x_1, x_2) \Rightarrow \llbracket U\rrbracket(\mathbf{r}_1 x_1,\ \mathbf{r}_2 x_2)$
By induction hypothesis on the premise:
$|\Gamma|, x_1, x_2 : |T|, f_1, f_2 : |T| \to |U| \mid \llbracket\Gamma\rrbracket, \llbracket T\rrbracket(x_1, x_2), \forall y_1, y_2. (\llbracket T\rrbracket(y_1, y_2) \wedge (y_1, y_2) < (x_1, x_2)) \Rightarrow \llbracket U\rrbracket(f_1 x_1,\ f_2 x_2) \vdash t_1 : |U| \sim t_2 : |U| \mid \llbracket U\rrbracket(\mathbf{r}_1, \mathbf{r}_2)$
And we apply the [LETREC] rule to get the result.

□

Proof of Lemma 15

Lemma 15. If $\ell \not\sqsubseteq a$ and $\tau \searrow \ell$, then $\vdash \forall x, y. (\lfloor \tau \rfloor_a(x, y) \equiv \top)$ in HOL.

Proof. By induction on the derivation of $\tau \searrow \ell$.

Case. $$\frac{\ell \sqsubseteq \ell'}{\mathbb{T}_{\ell'}(\tau) \searrow \ell}$$
Since $\ell \not\sqsubseteq a$ (given) and $\ell \sqsubseteq \ell'$ (premise), it must be the case that $\ell' \not\sqsubseteq a$. Hence, by definition, $\lfloor \mathbb{T}_{\ell'}(\tau) \rfloor_a(x, y) = \top$.

Case. $$\frac{\tau \searrow \ell}{\mathbb{T}_{\ell'}(\tau) \searrow \ell}$$
We consider two cases:

If $\ell' \not\sqsubseteq a$, then $\lfloor \mathbb{T}_{\ell'}(\tau) \rfloor_a(x, y) = \top$ by definition.

If $\ell' \sqsubseteq a$, then $\lfloor \mathbb{T}_{\ell'}(\tau) \rfloor_a(x, y) = \lfloor \tau \rfloor_a(x, y)$ by definition. By i.h. on the premise, we have $\lfloor \tau \rfloor_a(x, y) \equiv \top$. Composing, $\lfloor \mathbb{T}_{\ell'}(\tau) \rfloor_a(x, y) \equiv \top$.

Case. $$\frac{\tau_1 \searrow \ell \qquad \tau_2 \searrow \ell}{\tau_1 \times \tau_2 \searrow \ell}$$
By i.h. on the premises, we have $\lfloor \tau_i \rfloor_a(x, y) \equiv \top$ for $i = 1, 2$ and all x, y. Therefore, $\lfloor \tau_1 \times \tau_2 \rfloor_a(x, y) \triangleq \lfloor \tau_1 \rfloor_a(\pi_1(x), \pi_1(y)) \wedge \lfloor \tau_2 \rfloor_a(\pi_2(x), \pi_2(y)) \equiv \top \wedge \top \equiv \top$.

Case. $\dfrac{\tau_2 \searrow \ell}{\tau_1 \to \tau_2 \searrow \ell}$

By i.h. on the premise, we have $\lfloor \tau_2 \rfloor_a(x, y) \equiv \top$ for all x, y. Hence, $\lfloor \tau_1 \to \tau_2 \rfloor_a(x, y) \triangleq (\forall v, w.\, \lfloor \tau_1 \rfloor_a(v, w) \Rightarrow \lfloor \tau_2 \rfloor_a(x\ v, y\ w)) \equiv (\forall v, w.\, \lfloor \tau_1 \rfloor_a(v, w) \Rightarrow \top) \equiv \top$.

□

Proof of Theorem 16

Theorem 16 (Soundness of embedding)**.** If $\Gamma \vdash e : \tau$ in DCC, then for all $a \in \{L, H\}$: $|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash |e|_1 : |\tau| \sim |e|_2 : |\tau| \mid \lfloor \tau \rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.

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

Case. $\dfrac{}{\Gamma \vdash \mathsf{tt} : \mathbb{B}}$

To show: $|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash \mathsf{tt} : \mathbb{B} \sim \mathsf{tt} : \mathbb{B} \mid (\mathbf{r}_1 = \mathsf{tt} \wedge \mathbf{r}_2 = \mathsf{tt}) \vee (\mathbf{r}_1 = \mathsf{ff} \wedge \mathbf{r}_2 = \mathsf{ff})$.

By rule TRUE, it suffices to show $(\mathsf{tt} = \mathsf{tt} \wedge \mathsf{tt} = \mathsf{tt}) \vee (\mathsf{tt} = \mathsf{ff} \wedge \mathsf{tt} = \mathsf{ff})$ in HOL, which is trivial.

Case. $\dfrac{\Gamma \vdash e : \mathbb{B} \qquad \Gamma \vdash e_t : \tau \qquad \Gamma \vdash e_f : \tau}{\Gamma \vdash \text{case } e \text{ of } \mathsf{tt} \mapsto e_t; \mathsf{ff} \mapsto e_f : \tau}$

To show: $|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash (\text{case } |e|_1 \text{ of } \mathsf{tt} \mapsto |e_t|_1; \mathsf{ff} \mapsto |e_f|_1) : |\tau| \sim (\text{case } |e|_2 \text{ of } \mathsf{tt} \mapsto |e_t|_2; \mathsf{ff} \mapsto |e_f|_2) : |\tau| \mid \lfloor \tau \rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.

By i.h. on the first premise:

$|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash |e|_1 : \mathbb{B} \sim |e|_2 : \mathbb{B} \mid (\mathbf{r}_1 = \mathsf{tt} \wedge \mathbf{r}_2 = \mathsf{tt}) \vee (\mathbf{r}_1 = \mathsf{ff} \wedge \mathbf{r}_2 = \mathsf{ff})$

By i.h. on the second premise:

$|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash |e_t|_1 : |\tau| \sim |e_t|_2 : |\tau| \mid \lfloor \tau \rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$

By i.h. on the third premise:

$|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash |e_f|_1 : |\tau| \sim |e_f|_2 : |\tau| \mid \lfloor \tau \rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$

Applying rule BOOLCASE to the past three statements yields the required result.

Case. $\dfrac{}{\Gamma, x : \tau \vdash x : \tau}$

To show: $|\Gamma|, x_1 : |\tau|, x_2 : |\tau| \mid \lfloor \Gamma \rfloor_a, \lfloor \tau \rfloor_a(x_1, x_2) \vdash x_1 : |\tau| \sim x_2 : |\tau| \mid \lfloor \tau \rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.

This follows immediately from rule VAR.

Case. $\dfrac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x.e : \tau_1 \to \tau_2}$

To show: $|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash \lambda x_1.|e|_1 : |\tau_1| \to |\tau_2| \sim \lambda x_2.|e|_2 : |\tau_1| \to |\tau_2| \mid \forall x_1, x_2.\, \lfloor \tau_1 \rfloor_a(x_1, x_2) \Rightarrow \lfloor \tau_2 \rfloor_a(\mathbf{r}_1\ x_1, \mathbf{r}_2\ x_2)$.

By i.h. on the premise: $|\Gamma|, x_1 : |\tau_1|, x_2 : |\tau_2| \mid \lfloor \Gamma \rfloor_a, \lfloor \tau_1 \rfloor_a(x_1, x_2) \vdash |e|_1 : |\tau_2| \sim |e|_2 : |\tau_2| \mid \lfloor \tau_2 \rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.

Applying rule ABS immediately yields the required result.

Case. $\dfrac{\Gamma \vdash e : \tau_1 \to \tau_2 \qquad \Gamma \vdash e' : \tau_1}{\Gamma \vdash e\ e' : \tau_2}$

To show: $|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash |e|_1\ |e'|_1 : |\tau_2| \sim |e|_2\ |e'|_2 : |\tau_2| \mid \lfloor \tau_2 \rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.

By i.h. on the first premise:

$|\Gamma| \mid \lfloor \Gamma \rfloor_a \vdash |e|_1 : |\tau_1| \to |\tau_2| \sim |e|_2 : |\tau_1| \to |\tau_2| \mid \forall x_1, x_2.\, \lfloor \tau_1 \rfloor_a(x_1, x_2) \Rightarrow \lfloor \tau_2 \rfloor_a(\mathbf{r}_1\ x_1, \mathbf{r}_2\ x_2)$

By i.h. on the second premise:

$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e'|_1 : |\tau_1| \sim |e'|_2 : |\tau_1| \mid \lfloor\tau_1\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$
Applying rule APP immediately yields the required result.

Case. $\dfrac{\Gamma \vdash e : \tau \qquad \Gamma \vdash e' : \tau'}{\Gamma \vdash \langle e, e'\rangle : \tau \times \tau'}$
To show: $|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash \langle |e|_1, |e'|_1\rangle : |\tau| \times |\tau'| \sim \langle |e|_2, |e'|_2\rangle : |\tau| \times |\tau'| \mid \lfloor\tau\rfloor_a(\pi_1(\mathbf{r}_1), \pi_1(\mathbf{r}_2)) \wedge \lfloor\tau'\rfloor_a(\pi_2(\mathbf{r}_1), \pi_2(\mathbf{r}_2))$.
By i.h. on the first premise:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \sim |e|_2 : |\tau| \mid \lfloor\tau\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$
By i.h. on the second premise:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e'|_1 : |\tau'| \sim |e'|_2 : |\tau'| \mid \lfloor\tau'\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$
The required result follows from the rule PAIR. We only need to show the third premise of the rule, i.e., the following in HOL:

$$\forall x_1 x_2 y_1 y_2. \lfloor\tau\rfloor_a(x_1, x_2) \Rightarrow \lfloor\tau'\rfloor_a(y_1, y_2) \Rightarrow (\lfloor\tau\rfloor_a(\pi_1\langle x_1, y_1\rangle, \pi_1\langle x_2, y_2\rangle) \wedge \lfloor\tau'\rfloor_a(\pi_2\langle x_1, y_1\rangle, \pi_2\langle x_2, y_2\rangle))$$

Since $\pi_1\langle x_1, y_1\rangle = x_1$, etc., this implication simplifies to:

$$\forall x_1 x_2 y_1 y_2. \lfloor\tau\rfloor_a(x_1, x_2) \Rightarrow \lfloor\tau'\rfloor_a(y_1, y_2) \Rightarrow (\lfloor\tau\rfloor_a(x_1, x_2) \wedge \lfloor\tau'\rfloor_a(y_1, y_2))$$

which is an obvious tautology.

Case. $\dfrac{\Gamma \vdash e : \tau \times \tau'}{\Gamma \vdash \pi_1(e) : \tau}$
To show: $|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash \pi_1(|e|_1) : |\tau| \sim \pi_1(|e|_2) : |\tau| \mid \lfloor\tau\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.
By i.h. on the premise:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \times |\tau'| \sim |e|_2 : |\tau| \times |\tau'| \mid \lfloor\tau\rfloor_a(\pi_1(\mathbf{r}_1), \pi_1(\mathbf{r}_2)) \wedge \lfloor\tau'\rfloor_a(\pi_2(\mathbf{r}_1), \pi_2(\mathbf{r}_2))$
By rule SUB:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \times |\tau'| \sim |e|_2 : |\tau| \times |\tau'| \mid \lfloor\tau\rfloor_a(\pi_1(\mathbf{r}_1), \pi_1(\mathbf{r}_2))$
By rule PROJ$_1$, we get the required result.

Case. $\dfrac{\Gamma \vdash e : \tau}{\Gamma \vdash \eta_\ell(e) : \mathbb{T}_\ell(\tau)}$
To show: $|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \sim |e|_2 : |\tau| \mid \lfloor\mathbb{T}_\ell(\tau)\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.
By i.h. on the premise: $|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \sim |e|_2 : |\tau| \mid \lfloor\tau\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$ (1)
If $\ell \sqsubseteq a$, then $\lfloor\mathbb{T}_\ell(\tau)\rfloor_a(\mathbf{r}_1, \mathbf{r}_2) \triangleq \lfloor\tau\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$, so the required result is the same as (1).
If $\ell \not\sqsubseteq a$, then $\lfloor\mathbb{T}_\ell(\tau)\rfloor_a(\mathbf{r}_1, \mathbf{r}_2) \triangleq \top$ and the required result follows from rule SUB applied to (1).

Case. $\dfrac{\Gamma \vdash e : \mathbb{T}_\ell(\tau) \qquad \Gamma, x : \tau \vdash e' : \tau' \qquad \tau' \searrow \ell}{\Gamma \vdash \mathsf{bind}(e, x.e') : \tau'}$
To show: $|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash (\lambda x.|e'|_1)\ |e|_1 : |\tau'| \sim (\lambda x.|e'|_2)\ |e|_2 : |\tau'| \mid \lfloor\tau'\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$.
By i.h. on the first premise:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \sim |e|_2 : |\tau| \mid \lfloor\mathbb{T}_\ell(\tau)\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$ (1)
By i.h. on the second premise:
$|\Gamma|, x_1 : |\tau|, x_2 : |\tau| \mid \lfloor\Gamma\rfloor_a, \lfloor\tau\rfloor_a(x_1, x_2) \vdash |e'|_1 : |\tau'| \sim |e'|_2 : |\tau'| \mid \lfloor\tau'\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$ (2)
We consider two cases:
Subcase. $\ell \sqsubseteq a$. Here, $\lfloor\mathbb{T}_\ell(\tau)\rfloor_a(\mathbf{r}_1, \mathbf{r}_2) \triangleq \lfloor\tau\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$, so (1) can be rewritten to:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \sim |e|_2 : |\tau| \mid \lfloor\tau\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$ (3)
Applying rule ABS to (2) yields:

$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash \lambda x_1.|e'|_1 : |\tau| \to |\tau'| \sim \lambda x_2.|e'|_2 : |\tau| \to |\tau'| \mid \forall x_1 x_2. \lfloor\tau\rfloor_a(x_1, x_2) \Rightarrow \lfloor\tau'\rfloor_a(\mathbf{r}_1\ x_1, \mathbf{r}_2\ x_2)$ (4)
Applying rule APP to (4) and (3) yields:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash (\lambda x_1.|e'|_1)\ |e|_1 : |\tau'| \sim (\lambda x_2.|e'|_2)\ |e|_2 : |\tau'| \mid \lfloor\tau'\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$
which is what we wanted to prove.
Subcase. $\ell \not\sqsubseteq a$. Here, $\lfloor\mathbb{T}_\ell(\tau)\rfloor_a(\mathbf{r}_1, \mathbf{r}_2) \triangleq \lfloor\tau\rfloor_a(\mathbf{r}_1, \mathbf{r}_2)$, so (1) can be rewritten to:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash |e|_1 : |\tau| \sim |e|_2 : |\tau| \mid \top$ (5)
Applying rule ABS to (2) yields:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash \lambda x_1.|e'|_1 : |\tau| \to |\tau'| \sim \lambda x_2.|e'|_2 : |\tau| \to |\tau'| \mid \forall x_1 x_2. \lfloor\tau\rfloor_a(x_1, x_2) \Rightarrow \lfloor\tau'\rfloor_a(\mathbf{r}_1\ x_1, \mathbf{r}_2\ x_2)$
By Lemma 15 applied to the subcase assumption $\ell \not\sqsubseteq a$ and the premise $\tau' \searrow \ell$, we have $\lfloor\tau'\rfloor_a(\mathbf{r}_1\ x_1, \mathbf{r}_2\ x_2) \equiv \top$.
So, by rule SUB:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash \lambda x_1.|e'|_1 : |\tau| \to |\tau'| \sim \lambda x_2.|e'|_2 : |\tau| \to |\tau'| \mid \forall x_1 x_2. \lfloor\tau\rfloor_a(x_1, x_2) \Rightarrow \top$
Since $(\forall x_1 x_2. \lfloor\tau\rfloor_a(x_1, x_2) \Rightarrow \top) \equiv \top \equiv (\forall x_1, x_2. \top \Rightarrow \top)$, we can use SUB again to get:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash \lambda x_1.|e'|_1 : |\tau| \to |\tau'| \sim \lambda x_2.|e'|_2 : |\tau| \to |\tau'| \mid \forall x_1, x_2. \top \Rightarrow \top$ (6)
Applying rule APP to (6) and (5) yields:
$|\Gamma| \mid \lfloor\Gamma\rfloor_a \vdash (\lambda x_1.|e'|_1)\ |e|_1 : |\tau'| \sim (\lambda x_2.|e'|_2)\ |e|_2 : |\tau'| \mid \top$
which is the same as our goal since $\lfloor\tau'\rfloor_a(\mathbf{r}_1, \mathbf{r}_2) \equiv \top$.

□

Proof of Theorem 17

Theorem 17. If $\Delta; \Phi; \Omega \vdash_k^l t : A$, then: $(\!|\,|\Omega|\,|\!), \Delta \mid \Phi, \lfloor\Omega\rfloor \vdash (\!|t|\!) : (\!|\,|A|\,|\!)_e \mid \lfloor A\rfloor_e^{k,l}(\mathbf{r})$

Proof. By induction on the derivation of $\Delta; \Phi; \Omega \vdash_k^l t : A$. We will show few cases.

Case. $\dfrac{}{\Delta; \Phi_a; \Omega, x : A \vdash_0^0 x : A}$
We can conclude by the following derivation:

$$\dfrac{\dfrac{}{(\!|\,|\Omega|\,|\!), x : (\!|\,|A|\,|\!)_v, \Delta \mid \Phi_a, \lfloor\Omega\rfloor, \lfloor A\rfloor_v(x) \vdash x : (\!|\,|A|\,|\!)_v \mid \lfloor A\rfloor_v(\mathbf{r})}\text{VAR} \qquad \dfrac{}{(\!|\,|\Omega|\,|\!), x : (\!|\,|A|\,|\!)_v, \Delta \mid \Phi_a, \lfloor\Omega\rfloor, \lfloor A\rfloor_v(x) \vdash 0 : \mathbb{N} \mid 0 \leq \mathbf{r} \leq 0}\text{NAT}}{(\!|\,|\Omega|\,|\!), x : (\!|\,|A|\,|\!)_v, \Delta \mid \Phi_a, \lfloor\Omega\rfloor, \lfloor A\rfloor_v(x) \vdash (x, 0) : (\!|\,|A|\,|\!)_v \times \mathbb{N} \mid \lfloor A\rfloor_v(\pi_1\mathbf{r}) \wedge 0 \leq \pi_2\mathbf{r} \leq 0}\text{PAIR-L}$$

where the additional proof conditions that is needed for the [PAIR-L] rule can be easily proved in HOL.

Case. $\dfrac{}{\Delta; \Phi_a; \Omega \vdash_0^0 \mathsf{n} : \mathsf{int}}$
Then we can conclude by the following derivation:

$$\dfrac{\dfrac{}{(\!|\,|\Omega|\,|\!), \Delta \mid \Phi_a, \lfloor\Omega\rfloor \vdash \mathsf{n} : \mathbb{N} \mid \top}\text{NAT} \qquad \dfrac{}{(\!|\,|\Omega|\,|\!), \Delta \mid \Phi_a, \lfloor\Omega\rfloor \vdash 0 : \mathbb{N} \mid 0 \leq \mathbf{r} \leq 0}\text{NAT}}{(\!|\,|\Omega|\,|\!), \Delta \mid \Phi_a, \lfloor\Omega\rfloor \vdash (\mathsf{n}, 0) : \mathbb{N} \times \mathbb{N} \mid 0 \leq \pi_2\mathbf{r} \leq 0}\text{PAIR-L}$$

where the additional proof conditions that is needed for the [PAIR-L] rule can be easily proved in HOL.

Case. $\dfrac{\Delta; \Phi_a; x : A_1, \Omega \vdash_k^l t : A_2}{\Delta; \Phi_a; \Omega \vdash_0^0 \lambda x.t : A_1 \xrightarrow{\text{exec}(k,l)} A_2}$

By induction hypothesis we have $(\!|\,|\Omega|\,|\!), x : (\!|\,|A_1|\,|\!)_v, \Delta \mid \Phi, \lfloor\Omega\rfloor, \lfloor A_1\rfloor_v(x) \vdash (\!|t|\!) : (\!|\,|A_2|\,|\!)_e \mid \lfloor A\rfloor_e^{k,l}(\mathbf{r})$ and we can conclude by the following derivation:

$$\dfrac{\dfrac{\begin{array}{c}(\!|\,|\Omega|\,|\!), x : (\!|\,|A_1|\,|\!)_v, \Delta \mid \Phi, \lfloor\Omega\rfloor, \lfloor A_1\rfloor_v(x) \vdash (\!|t|\!) : \\ (\!|\,|A_2|\,|\!)_e \mid \lfloor A_2\rfloor_e^{k,l}(\mathbf{r})\end{array}}{\begin{array}{c}(\!|\,|\Omega|\,|\!), \Delta \mid \Phi, \lfloor\Omega\rfloor \vdash \lambda x.(\!|t|\!) : (\!|\,|A_1|\,|\!)_v \to (\!|\,|A_2|\,|\!)_e \mid \\ \forall x.\lfloor A_1\rfloor_v(x) \Rightarrow \lfloor A_2\rfloor_e^{k,l}(\mathbf{r}x)\end{array}}\text{ABS} \qquad (\!|\,|\Omega|\,|\!), \Delta \mid \Phi, \lfloor\Omega\rfloor \vdash 0 : \mathbb{N} \mid 0 \le \mathbf{r} \le 0}{(\!|\,|\Omega|\,|\!), \Delta \mid \Phi, \lfloor\Omega\rfloor \vdash (\lambda x.(\!|t|\!), 0) : ((\!|\,|A_1|\,|\!)_v \to (\!|\,|A_2|\,|\!)_e) \times \mathbb{N} \mid \forall x.\lfloor A_1\rfloor_v(x) \Rightarrow \lfloor A_2\rfloor_e^{k,l}((\pi_1\mathbf{r})x) \wedge 0 \le \pi_2\mathbf{r} \le 0}\text{PAIR-L}$$

where the additional proof conditions that is needed for the [PAIR-L] rule can be easily proved in HOL.

Case $\dfrac{\Delta; \Phi_a; \Omega \vdash_{k_1}^{l_1} t_1 : A_1 \xrightarrow{\text{exec}(k,l)} A_2 \qquad \Delta; \Phi_a; \Omega \vdash_{k_2}^{l_2} t_2 : A_1}{\Delta; \Phi_a; \Omega \vdash_{k_1+k_2+k+c_{app}}^{l_1+l_2+l+c_{app}} t_1\, t_2 : A_2}$

By induction hypothesis and unfolding some some definitions we have

$$\begin{array}{l}(\!|\,|\Omega|\,|\!), \Delta \mid \Phi_a, \lfloor\Omega\rfloor \vdash (\!|t_1|\!) : ((\!|\,|A_1|\,|\!)_v \to ((\!|\,|A_2|\,|\!)_v \times \mathbb{N})) \times \mathbb{N} \mid \\ \qquad \forall h.\lfloor A_1\rfloor_v(h) \Rightarrow (\lfloor A_2\rfloor_v(\pi_1((\pi_1(\mathbf{r}))h)) \wedge k \le \pi_2((\pi_1(\mathbf{r}))h) \le l) \wedge k_1 \le \pi_2(\mathbf{r}) \le l_1\end{array}$$

and $(\!|\,|\Omega|\,|\!), \Delta \mid \Phi_a, \lfloor\Omega\rfloor \vdash (\!|t_2|\!) : (\!|\,|A_1|\,|\!)_v \times \mathbb{N} \mid \lfloor A_1\rfloor_v(\pi_1(\mathbf{r})) \wedge k_2 \le \pi_2(\mathbf{r}) \le l_2$. So, we can prove:

$$\begin{array}{l}(\!|\,|\Omega|\,|\!), \Delta \mid \Phi_a, \lfloor\Omega\rfloor \vdash \mathsf{let}\ x = (\!|t_1|\!)\ \mathsf{in}\ \mathsf{let}\ y = (\!|t_2|\!)\ \mathsf{in}\ \pi_1(x)\ \pi_1(y) : (\!|\,|A_2|\,|\!)_v \times \mathbb{N} \mid \\ \qquad \lfloor A_2\rfloor_v(\pi_1(\mathbf{r})) \wedge k \le \pi_2(\mathbf{r}) \le l \wedge k_1 \le \pi_2(x) \le l_1 \wedge k_2 \le \pi_2(y)\mathbf{r} \le l_2\end{array}$$

This combined with the definition of the cost-passing translation $(\!|t_1\, t_2|\!) \triangleq \mathsf{let}\ x = (\!|t_1|\!)\ \mathsf{in}\ \mathsf{let}\ y = (\!|t_2|\!)\ \mathsf{in}\ \mathsf{let}\ z = \pi_1(x)\ \pi_1(y)\ \mathsf{in}\ (\pi_1(z), \pi_2(x) + \pi_2(y) + \pi_2(z) + c_{app})$ allows us to prove as required the following:

$$(\!|\,|\Omega|\,|\!), \Delta \mid \Phi_a, \lfloor\Omega\rfloor \vdash (\!|t_1\, t_2|\!) : (\!|\,|A_2|\,|\!)_v \times \mathbb{N} \mid \lfloor A_2\rfloor_v(\pi_1(\mathbf{r})) \wedge k + k_1 + k_2 + c_{app} \le \pi_2(\mathbf{r}) \le l + l_1 + l_2 + c_{app}.$$

□

Proof of Theorem 18

Theorem 18. If $\Delta; \Phi; \Gamma \vdash t_1 \ominus t_2 \lesssim l : \tau$, then: $\|\Gamma\|, \Delta \mid \Phi, \llbracket\Gamma\rrbracket \vdash (\!|t_1|\!)_1 : (\!|\,|\tau|\,|\!)_e \sim (\!|t_2|\!)_2 : (\!|\,|\tau|\,|\!)_e \mid \llbracket\tau\rrbracket_e^l(\mathbf{r}_1, \mathbf{r}_2)$, where $(\!|t_i|\!)_j$ is a copy of t_i where each variable x is replaced by a variable x_j for $j \in \{1, 2\}$.

To prove Theorem 18, we need three lemmas.

Lemma C.1. *Suppose* $\Delta; \Phi \vdash \tau$ wf.[1] *Then, the following hold:*

(1) $\Delta \mid \Phi \vdash \forall xy.\, \llbracket\tau\rrbracket_v(x, y) \Rightarrow \lfloor\overline{\tau}\rfloor_v(x) \wedge \lfloor\overline{\tau}\rfloor_v(y)$
(2) $\Delta \mid \Phi \vdash \forall xy.\, \llbracket\tau\rrbracket_e^t(x, y) \Rightarrow \lfloor\overline{\tau}\rfloor_e^{0,\infty}(x) \wedge \lfloor\overline{\tau}\rfloor_e^{0,\infty}(y)$

Also, (3) $\llbracket\Gamma\rrbracket \Rightarrow \lfloor\overline{\Gamma}_1\rfloor \wedge \lfloor\overline{\Gamma}_2\rfloor$ *where* $\overline{\Gamma}_1$ *and* $\overline{\Gamma}_2$ *are obtained by replacing each variable* x *in* $\overline{\Gamma}$ *with* x_1 *and* x_2*, respectively.*

Proof. (1) and (2) follow by a simultaneous induction on the given judgment. (3) follows immediately from (1). □

Lemma C.2. *If* $\Delta; \Phi_a; \Gamma \vdash e_1 \ominus e_2 \lesssim t : \tau$ *in RelCost, then* $\Delta; \Phi; \overline{\Gamma} \vdash_0^\infty e_i : \overline{\tau}$ *for* $i \in \{1, 2\}$ *in RelCost.*

Proof. By induction on the given derivation. □

[1] This judgment simply means that τ is well-formed in the context $\Delta; \Phi$. It is defined in the original RelCost paper [Çiçek et al. 2017].

Lemma C.3. *If* $\Delta; \Phi \models \tau_1 \sqsubseteq \tau_2$*, then* $\Delta; \Phi \vdash \forall xy. \llbracket \tau_1 \rrbracket_v(x, y) \Rightarrow \llbracket \tau_2 \rrbracket_v(x, y)$.

Proof. By induction on the given derivation of $\Delta; \Phi \models \tau_1 \sqsubseteq \tau_2$. □

Proof of Theorem 18. The proof is by induction on the given derivation of $\Delta; \Phi; \Gamma \vdash t_1 \ominus t_2 \lesssim k : \tau$. We show only a few representative cases here.

Case: $$\frac{i :: S, \Delta; \Phi_a; \Gamma \vdash e \ominus e' \lesssim t : \tau \qquad i \notin \text{FIV}(\Phi_a; \Gamma)}{\Delta; \Phi_a; \Gamma \vdash \Lambda e \ominus \Lambda e' \lesssim 0 : \forall i \overset{\text{diff}(t)}{::} S. \tau} \text{ r-iLam}$$

To show: $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\lambda\_.(\!|e|\!)_1, 0) : (\mathbb{N} \to (\!|\|\tau\||\!)_e) \times \mathbb{N} \sim (\lambda\_.(\!|e'|\!)_2, 0) : (\mathbb{N} \to (\!|\|\tau\||\!)_e) \times \mathbb{N} \mid \llbracket\forall i \overset{\text{diff}(t)}{::} S. \tau\rrbracket_e^0(\mathbf{r}_1, \mathbf{r}_2)$.

Expand $\llbracket\forall i \overset{\text{diff}(t)}{::} S. \tau\rrbracket_e^0(\mathbf{r}_1, \mathbf{r}_2)$ to $\llbracket\forall i \overset{\text{diff}(t)}{::} S. \tau\rrbracket_v(\pi_1\, \mathbf{r}_1, \pi_1\, \mathbf{r}_2) \land \pi_2 \mathbf{r}_1 - \pi_2\, \mathbf{r}_2 \leq 0$, and apply the rule [PAIR] to reduce to two proof obligations:

(A) $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash \lambda\_.(\!|e|\!)_1 : \mathbb{N} \to (\!|\|\tau\||\!)_e \sim \lambda\_.(\!|e'|\!)_2 : \mathbb{N} \to (\!|\|\tau\||\!)_e \mid \llbracket\forall i \overset{\text{diff}(t)}{::} S. \tau\rrbracket_v(\mathbf{r}_1, \mathbf{r}_2)$
(B) $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash 0 : \mathbb{N} \sim 0 : \mathbb{N} \mid \mathbf{r}_1 - \mathbf{r}_2 \leq 0$

(B) follows immediately by rule [ZERO]. To prove (A), expand $\llbracket\forall i \overset{\text{diff}(t)}{::} S. \tau\rrbracket_v(\mathbf{r}_1, \mathbf{r}_2)$ and apply rule [$\land_I$]. We get three proof obligations.

(C) $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash \lambda\_.(\!|e|\!)_1 : \mathbb{N} \to (\!|\|\tau\||\!)_e \sim \lambda\_.(\!|e'|\!)_2 : \mathbb{N} \to (\!|\|\tau\||\!)_e \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_v(\mathbf{r}_1)$
(D) $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash \lambda\_.(\!|e|\!)_1 : \mathbb{N} \to (\!|\|\tau\||\!)_e \sim \lambda\_.(\!|e'|\!)_2 : \mathbb{N} \to (\!|\|\tau\||\!)_e \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_v(\mathbf{r}_2)$
(E) $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash \lambda\_.(\!|e|\!)_1 : \mathbb{N} \to (\!|\|\tau\||\!)_e \sim \lambda\_.(\!|e'|\!)_2 : \mathbb{N} \to (\!|\|\tau\||\!)_e \mid \forall z_1 z_2. \top \Rightarrow \forall i. \llbracket\tau\rrbracket_e^t(\mathbf{r}_1\, z_1, \mathbf{r}_2\, z_2)$

To prove (C), apply Lemma C.2 to the given derivation (not just the premise), obtaining a RelCost derivation for $\Delta; \Phi_a; \overline{\Gamma} \vdash_0^\infty \Lambda e : (\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau})$. Applying Theorem 17 to this yields $(\!|\overline{\Gamma}|\!), \Delta \mid \Phi_a, \lfloor\overline{\Gamma}\rfloor \vdash (\lambda\_.(\!|e|\!), 0) : (\mathbb{N} \to (\!|\|\overline{\tau}\||\!)_e) \times \mathbb{N} \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_e^{0,\infty}(\mathbf{r})$ in UHOL, which is the same as $(\!|\overline{\Gamma}|\!), \Delta \mid \Phi_a, \lfloor\overline{\Gamma}\rfloor \vdash (\lambda\_.(\!|e|\!), 0) : (\mathbb{N} \to (\!|\|\overline{\tau}\||\!)_e) \times \mathbb{N} \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_v(\pi_1\, \mathbf{r}) \land 0 \leq \pi_2\, \mathbf{r} \leq \infty$. Applying rule [PROJ$_1$], we get $(\!|\overline{\Gamma}|\!), \Delta \mid \Phi_a, \lfloor\overline{\Gamma}\rfloor \vdash \pi_1(\lambda\_.(\!|e|\!), 0) : \mathbb{N} \to (\!|\|\overline{\tau}\||\!)_e \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_v(\mathbf{r})$. By subject conversion, $(\!|\overline{\Gamma}|\!), \Delta \mid \Phi_a, \lfloor\overline{\Gamma}\rfloor \vdash \lambda\_.(\!|e|\!) : \mathbb{N} \to (\!|\|\overline{\tau}\||\!)_e \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_v(\mathbf{r})$. Renaming variables, we get $(\!|\overline{\Gamma}|\!)_1, \Delta \mid \Phi_a, \lfloor\overline{\Gamma}_1\rfloor \vdash \lambda\_.(\!|e|\!)_1 : \mathbb{N} \to (\!|\|\overline{\tau}\||\!)_e \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_v(\mathbf{r})$.

Now note that by definition, $\|\Gamma\| \supseteq (\!|\overline{\Gamma}|\!)_1$ and by Lemma C.1(3), $\llbracket\Gamma\rrbracket \Rightarrow \lfloor\overline{\Gamma}_1\rfloor$. Hence, we also get $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash \lambda\_.(\!|e|\!)_1 : \mathbb{N} \to (\!|\|\overline{\tau}\||\!)_e \mid \lfloor\forall i \overset{\text{exec}(0,\infty)}{::} S. \overline{\tau}\rfloor_v(\mathbf{r})$. (C) follows immediately by rule [UHOL-L].

(D) has a similar proof.

To prove (E), apply the rule [ABS], getting the obligation:
$\|\Gamma\|, \Delta, z_1, z_2 : \mathbb{N} \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e'|\!)_2 : (\!|\|\tau\||\!)_e \mid \forall i. \llbracket\tau\rrbracket_e^t(\mathbf{r}_1, \mathbf{r}_2)$
Since z_1, z_2 do not appear anywhere else, we can strengthen the context to remove them, thus reducing to:
$\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e'|\!)_2 : (\!|\|\tau\||\!)_e \mid \forall i. \llbracket\tau\rrbracket_e^t(\mathbf{r}_1, \mathbf{r}_2)$
Next, we transpose to HOL using Theorem 6. We get the obligation:
$\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash \forall i. \llbracket\tau\rrbracket_e^t((\!|e|\!)_1, (\!|e'|\!)_2)$
This is equivalent to:
$\|\Gamma\|, \Delta, i : S \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash \llbracket\tau\rrbracket_e^t((\!|e|\!)_1, (\!|e'|\!)_2)$
The last statement follows immediately from i.h. on the premise, followed by transposition to HOL using Theorem 6.

Case: $$\frac{\Delta; \Phi_a; \Gamma \vdash e \ominus e \lesssim t : \tau \qquad \forall x \in dom(\Gamma).\ \Delta; \Phi_a \models \Gamma(x) \sqsubseteq \Box\,\Gamma(x)}{\Delta; \Phi_a; \Gamma, \Gamma'; \Omega \vdash e \ominus e \lesssim 0 : \Box\,\tau} \text{ nochange}$$

To show: $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e|\!)_2 : (\!|\|\tau\||\!)_e \mid \llbracket\Box\,\tau\rrbracket^0_e(\mathbf{r}_1, \mathbf{r}_2)$.
Expanding the definition of $\llbracket\Box\,\tau\rrbracket^0_e$, this is equivalent to:
$\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e|\!)_2 : (\!|\|\tau\||\!)_e \mid \llbracket\tau\rrbracket_v(\pi_1\,\mathbf{r}_1, \pi_2\,\mathbf{r}_2) \wedge (\pi_1\,\mathbf{r}_1 = \pi_1\,\mathbf{r}_2) \wedge (\pi_2\,\mathbf{r}_1 - \pi_2\,\mathbf{r}_2 \leq 0)$
Using rule [$\wedge_I$], we reduce this to two obligations:
(A) $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e|\!)_2 : (\!|\|\tau\||\!)_e \mid \llbracket\tau\rrbracket_v(\pi_1\,\mathbf{r}_1, \pi_2\,\mathbf{r}_2)$
(B) $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e|\!)_2 : (\!|\|\tau\||\!)_e \mid (\pi_1\,\mathbf{r}_1 = \pi_1\,\mathbf{r}_2) \wedge (\pi_2\,\mathbf{r}_1 - \pi_2\,\mathbf{r}_2 \leq 0)$

By i.h. on the first premise,
$\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e|\!)_2 : (\!|\|\tau\||\!)_e \mid \llbracket\tau\rrbracket_v(\pi_1\,\mathbf{r}_1, \pi_2\,\mathbf{r}_2) \wedge (\pi_2\,\mathbf{r}_1 - \pi_2\,\mathbf{r}_2 \leq t)$
By rule [SUB],
$\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e|\!)_2 : (\!|\|\tau\||\!)_e \mid \llbracket\tau\rrbracket_v(\pi_1\,\mathbf{r}_1, \pi_2\,\mathbf{r}_2)$
which is the same as (A).

To prove (B), apply Lemma C.3 to the second premise to get for every $x \in dom(\Gamma)$ that $\Delta \mid \Phi_a \vdash \llbracket\Gamma(x)\rrbracket_v(x_1, x_2) \Rightarrow \llbracket\Box\,\Gamma(x)\rrbracket_v(x_1, x_2)$. Since $\llbracket\Box\,\Gamma(x)\rrbracket_v(x_1, x_2) \Rightarrow x_1 = x_2$ and from $\llbracket\Gamma\rrbracket$ we know that $\llbracket\Gamma(x)\rrbracket_v(x_1, x_2)$, it follows that $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash x_1 = x_2$. Since this holds for every $x \in dom(\Gamma)$, it follows immediately that $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 = (\!|e|\!)_2$. By Theorem 6, $\|\Gamma\|, \Delta \mid \Phi_a, \llbracket\Gamma\rrbracket \vdash (\!|e|\!)_1 : (\!|\|\tau\||\!)_e \sim (\!|e|\!)_2 : (\!|\|\tau\||\!)_e \mid \mathbf{r}_1 = \mathbf{r}_2$. (B) follows immediately by rule [SUB].

□

D EXAMPLES

Factorial

This example shows that the two following implementations of factorial, with and without accumulator, are equivalent:

$$\mathrm{fact}_1 \triangleq \text{letrec } f_1\ n_1 = \text{case } n_1 \text{ of } 0 \mapsto 1; S \mapsto \lambda x_1.Sx_1 * (f_1\ x_1)$$
$$\mathrm{fact}_2 \triangleq \text{letrec } f_2\ n_2 = \lambda acc.\text{case } n_2 \text{ of } 0 \mapsto acc; S \mapsto \lambda x_2.f_2\ x_2\ (Sx_2 * acc)$$

Our goal is to prove that:

$$\emptyset \mid \emptyset \vdash \mathrm{fact}_1 : \mathbb{N} \to \mathbb{N} \sim \mathrm{fact}_2 : \mathbb{N} \to \mathbb{N} \to \mathbb{N} \mid \forall n_1 n_2. n_1 = n_2 \Rightarrow \forall acc.(\mathbf{r}_1\ n_1) * acc = \mathbf{r}_2\ n_2\ acc$$

Since both programs do the same number of iterations, we can do synchronous reasoning for the recursion at the head of the programs. However, the bodies of the functions have different types since fact_2 receives an extra argument, the accumulator. Therefore, we will need a one-sided application of [ABS-R], before we can go back to reasoning synchronously. We will then apply the [CASE] rule, knowing that both terms reduce to the same branch, since $n_1 = n_2$. On the zero branch, we will need to prove the trivial equality $1 * acc = acc$. On the successor branch, we will need to prove that $Sx * (\text{fact } x) * acc = \mathrm{fact}_2\ x_2\ (Sx_2 * acc)$, knowing by induction hypothesis that such a property holds for every m less that x.

Now we will expand on the details. We start the proof applying the [LETREC] rule, which has 2 premises:

(1) Both functions are well-defined
(2) $n_1 = n_2, \forall y_1 y_2.(y_1, y_2) < (n_1, n_2) \Rightarrow y_1 = y_2 \Rightarrow \forall acc.(f_1\ y_1) * acc = f_2\ y_2\ acc \vdash \text{case } n_1 \text{ of } 0 \mapsto 1; S \mapsto \lambda x_1.Sx_1 * (f_1\ x_1) \sim \lambda acc.\text{case } n_2 \text{ of } 0 \mapsto acc; S \mapsto \lambda x_2.f_2\ x_2\ (Sx_2 * acc) \mid n_1 = n_2 \Rightarrow \forall acc.\mathbf{r}_1 * acc = \mathbf{r}_2\ acc$

We assume that the first premise is provable.

To prove the second premise, we start by applying ABS-R, which leaves the following proof obligation:

$$n_1 = n_2, \forall y_1 y_2.(y_1, y_2) < (n_1, n_2) \Rightarrow y_1 = y_2 \Rightarrow \forall acc.(f_1\ y_1) * acc = f_2\ y_2\ acc, n_1 = n_2 \vdash$$
$$\text{case } n_1 \text{ of } 0 \mapsto 1; S \mapsto \lambda x_1.Sx_1 * (f_1\ x_1) \sim \text{case } n_2 \text{ of } 0 \mapsto acc; S \mapsto \lambda x_2.f_2\ x_2\ (Sx_2 * acc) \mid \mathbf{r}_1 * acc = \mathbf{r}_2$$

Now we can apply [CASE], and we have 3 premises, where Ψ denotes the axioms of the previous judgment:

- $\Psi \vdash n_1 \sim n_2 \mid \mathbf{r}_1 = 0 \Leftrightarrow \mathbf{r}_2 = 0$
- $\Psi, n_1 = 0, n_2 = 0 \vdash 1 \sim acc \mid \mathbf{r}_1 * acc = \mathbf{r}_2$
- $\Psi \vdash \lambda x_1.Sx_1 * (f_1\ x_1) \sim \lambda x_2.f_2\ x_2\ (Sx_2 * acc) \mid \forall x_1 x_2.n_1 = Sx_1 \Rightarrow n_2 = Sx_2 \Rightarrow (\mathbf{r}_1\ x_1) * acc = \mathbf{r}_2\ x_2$

Premise 1 is a direct consequence of $n_1 = n_2$. Premise 2 is a trivial arithmetic identity. To prove premise 3, we first apply the ABS rule:

$$\Psi, n_1 = Sx_1, n_2 = Sx_2 \vdash Sx_1 * (f_1\ x_1) \sim f_2\ x_2\ (Sx_2 * acc) \mid \mathbf{r}_1 * acc = \mathbf{r}_2$$

and then by Theorem 6 we can finish the proof in HOL by deriving.

$$\Psi, n_1 = Sx_1, n_2 = Sx_2 \vdash Sx_1 * (f_1\ x_1) * acc = f_2\ x_2\ (Sx_2 * acc)$$

From the premises we can first prove that $(x_1, x_2) < (n_1, n_2)$ so by the inductive hypothesis from the [LETREC] rule, and the $[\Rightarrow_E]$ rule, we get

$$\forall acc.(f_1\ x_1) * acc = f_2\ x_2\ acc,$$

which we then instantiate with $Sx_1 * acc$ to get

$$(f_1\ x_1) * Sx_1 * acc = f_2\ x_2\ (Sx_1 * acc).$$

On the other hand, from the hypotheses we also have $x_1 = x_2$, so by [CONV] we finally prove

$$(f_1\ x_1) * Sx_1 * acc = f_2\ x_2\ (Sx_2 * acc)$$

List reversal

A related example for lists is the equivalence of reversal with and without accumulator. The structure of the proof is the same as in the factorial example, but we will briefly show it to illustrate how the LISTCASE rule is used. The functions are written:

$$\begin{array}{lll} \text{rev}_1 & \triangleq & \text{letrec } f_1\ l_1 = \text{case } l_1 \text{ of } [\,] \mapsto [\,]; \_ :: \_ \mapsto \lambda h_1.\lambda t_1.(f_1\ t_1) ++[x_1] \\ \text{rev}_2 & \triangleq & \text{letrec } f_2\ l_2 = \lambda acc.\text{case } l_2 \text{ of } [\,] \mapsto acc; \_ :: \_ \mapsto \lambda h_2.\lambda t_2.f_2\ t_2\ (h_2 :: acc) \end{array}$$

We want to prove they are related by the following judgment:

$$\emptyset \mid \emptyset \vdash \text{rev}_1 : \text{list}_\tau \to \text{list}_\tau \sim \text{rev}_2 : \text{list}_\tau \to \text{list}_\tau \mid \forall l_1, l_2.l_1 = l_2 \Rightarrow \forall acc.\ (\mathbf{r}_1\ l_1) + +acc = \mathbf{r}_2\ l_2\ acc$$

By the [LETREC] rule, we have to prove 2 premises:

(1) Both functions are well-defined.
(2) $l_1 = l_2, \forall m_1 m_2.(|m_1|, |m_2|) < (|l_1|, |l_2|) \Rightarrow m_1 = m_2 \Rightarrow \forall acc.(f_1\ m_1) + +acc = f_2\ m_2\ acc \vdash \text{case } l_1 \text{ of } [\,] \mapsto [\,]; \_ :: \_ \mapsto \lambda h_1.\lambda t_1.(f_1\ t_1) ++[x_1] \sim \lambda acc.\text{case } l_2 \text{ of } [\,] \mapsto acc; \_ :: \_ \mapsto \lambda h_2.\lambda t_2.f_2\ t_2\ (h_2 :: acc) \mid \forall acc.\ \mathbf{r}_1 + +acc = \mathbf{r}_2\ acc$

For the second premise, similarly as in factorial, we apply ABS-R. We have the following premise, where Ψ denotes the axioms in the previous judgment:

$$\Psi \vdash \text{case } l_1 \text{ of } [\,] \mapsto [\,]; \_ :: \_ \mapsto \lambda h_1.\lambda t_1.(f_1\ t_1) ++[x_1] \sim \text{case } t_2 \text{ of } [\,] \mapsto acc; \_ :: \_ \mapsto \lambda h_2.\lambda t_2.f_2\ t_2\ (h_2 :: acc) \mid \mathbf{r}_1 + +acc = \mathbf{r}_2$$

and then LISTCASE, which has three premises:

- $\Psi \vdash l_1 \sim l_2 \mid \mathbf{r}_1 = [\,] \Leftrightarrow \mathbf{r}_2 = [\,]$
- $\Psi, l_1 = [\,], l_2 = [\,] \vdash [\,] \sim acc \mid \mathbf{r}_1 + +acc = \mathbf{r}_2$
- $\Psi \vdash \lambda h_1.\lambda t_1.(f_1\ t_1) ++[x_1] \sim \lambda h_2.\lambda t_2.f_2\ t_2\ (h_2 :: acc) \mid$
  $\forall h_1 t_1 h_2 t_2.l_1 = h_1 :: t_1 \Rightarrow l_2 = h_2 :: t_2 \Rightarrow \mathbf{r}_1 + +acc = \mathbf{r}_2$

We complete the proof in a similar way as in the factorial example.

Proof of Theorem 19

Theorem 19. $l_1, l_2 : \mathsf{list}_{\mathbb{N}}, n_1, n_2 : \mathbb{N}, g_1, g_2 : \mathbb{N} \to \mathbb{N} \mid l_1 = l_2, n_1 = n_2, g_1 = g_2 \vdash$
$map\ (take\ l_1\ n_1)\ g_1 : \mathsf{list}_{\mathbb{N}} \sim take\ (map\ l_2\ g_2)\ n_2 : \mathsf{list}_{\mathbb{N}} \mid \mathbf{r}_1 = \mathbf{r}_2$

We will use without proof two unary lemmas:

Lemma 24. $\bullet \mid \bullet \vdash take : \mathsf{list}_{\mathbb{N}} \to \mathbb{N} \to \mathsf{list}_{\mathbb{N}} \mid \forall ln.|r\ l\ n| = min(n, |l|)$

Lemma 25. $\bullet \mid \bullet \vdash map : \mathsf{list}_{\mathbb{N}} \to (\mathbb{N} \to \mathbb{N}) \to \mathsf{list}_{\mathbb{N}} \mid \forall lf.|r\ l\ f| = |l|$

Now we proceed with the proof of the theorem

Proof. We want to prove

$l_1 = l_2, n_1 = n_2, g_1 = g_2 \vdash map\,(take\,l_1\,n_1)\,g_1 \sim take\,(map\,l_2\,g_2)\,n_2 \mid \mathbf{r}_1 \sqsubseteq \mathbf{r}_2 \wedge |\mathbf{r}_1| = \min(n_1, |l_1|) \wedge |\mathbf{r}_2| = \min(n_2, |l_2|)$

where $\mathbf{r}_1 \sqsubseteq \mathbf{r}_2$ is the prefix ordering and is defined as an inductive predicate:

$$\forall l.[] \sqsubseteq l \qquad\qquad \forall hl_1l_2.l_1 \sqsubseteq l_2 \Rightarrow h :: l_1 \sqsubseteq h :: l_2$$

By the helping lemmas and Lemma 10, it suffices to prove just the first conjunct:

$$l_1 = l_2, n_1 = n_2, g_1 = g_2 \vdash map\ (take\ l_1\ n_1)\ g_1 \sim take\ (map\ l_2\ g_2)\ n_2 \mid \mathbf{r}_1 \sqsubseteq \mathbf{r}_2$$

The derivation begins by applying the APP-R rule. We get the following judgment on n_2:

$$l_1 = l_2, n_1 = n_2, g_1 = g_2 \vdash n_2 \mid \mathbf{r} \geq |take\ l_1\ n_1| \tag{1}$$

and a main premise:

$$l_1 = l_2, n_1 = n_2, g_1 = g_2 \vdash map\ (take\ l_1\ n_1)\ g_1 \sim take\ (map\ l_2\ g_2) \mid \forall x_2.x_2 \geq |take\ l_1\ n_1| \Rightarrow \mathbf{r}_1 \sqsubseteq (\mathbf{r}_2\ x_2) \tag{2}$$

Notice that we have chosen the premise $x_2 \geq |take\ l_1\ n_1|$ because we are trying to prove $\mathbf{r}_1 \sqsubseteq (\mathbf{r}_2\ x_2)$, which is only true if we take a larger prefix on the right than on the left. The judgment (1) is easily proven from the fact that $|take\ l_1\ n_1| = min(n_1, |l_1|) \leq n_1 = n_2$, which we get from the lemmas. To prove (2) we first apply APP-L with a trivial condition $g_1 = g_2$ on g_1. Then we apply APP and we have two premises:

(A) $\Psi \vdash take\ l_1\ n_1 \sim map\ l_2\ g_2 \mid \mathbf{r}_1 \sqsubseteq_{g_2} \mathbf{r}_2$
(B) $\Psi \vdash map \sim take \mid \forall m_1m_2.m_1 \sqsubseteq_{g_2} m_2 \Rightarrow (\forall g_1.g_1 = g_2 \Rightarrow \forall x_2.x_2 \geq |m_1| \Rightarrow (\mathbf{r}_1\ m_1\ g_1) \sqsubseteq (\mathbf{r}_2\ m_2\ x_2))$

where $\sqsubseteq_g$ is defined as an inductive predicate parametrized by g:

$$\forall l.[] \sqsubseteq_g l \qquad\qquad \forall hl_1l_2.l_1 \sqsubseteq_g l_2 \Rightarrow h :: l_1 \sqsubseteq_g (gh) :: l_2$$

We first show how to prove (A). We start by applying APP with a trivial condition for the arguments to get:

$$\Psi \vdash take\ l_1 \sim map\ l_2 \mid \forall x_1g_2.(\mathbf{r}_1\ x_1) \sqsubseteq_{g_2} (\mathbf{r}_2\ g_2)$$

We then apply APP, which has two premises, one of them equating l_1 and l_2. The other one is:

$$\Psi \vdash take \sim map \mid \forall m_1m_2.m_1 = m_2 \Rightarrow \forall x_1g_2.(\mathbf{r}_1\ m_1\ x_1) \sqsubseteq_{g_2} (\mathbf{r}_2\ m_2\ g_2)$$

To complete this branch of the proof, we apply LETREC. We need to prove the following premise:

$$\Psi, m_1 = m_2, \forall k_1k_2.(k_1, k_2) < (m_1, m_2) \Rightarrow k_1 = k_2 \Rightarrow \forall x_1g_2.(f_1\ k_1\ x_1) \sqsubseteq_{g_2} (f_2\ k_2\ g_2) \vdash$$
$$\lambda n_1.e_1 \sim \lambda g_2.e_2 \mid \forall x_1g_2.(\mathbf{r}_1\ x_1) \sqsubseteq_{g_2} (\mathbf{r}_2\ g_2)$$

Where e_1, e_2 abbreviate the bodies of the functions:

$$\begin{aligned} e_1 \triangleq\ & \text{case } m_1 \text{ of } [] \mapsto [] \\ & ;\_ :: \_ \mapsto \quad \lambda h_1 t_1.\text{case } x_1 \text{ of } 0 \mapsto \quad [] \\ & \qquad\qquad\qquad ;S \mapsto \quad \lambda y_1.h_1 :: f_1\ t_1\ y_1 \end{aligned}$$

$$e_2 \triangleq \begin{array}{l} \text{case } m_2 \text{ of } [] \mapsto \quad [] \\ \quad ;\_ :: \_ \mapsto \quad \lambda h_2 t_2.(g_2\ h_2) :: (f_2\ t_2\ g_2) \end{array}$$

If we apply ABS we get a premise:

$$\Psi, m_1 = m_2, \forall k_1 k_2.(k_1,k_2) < (m_1,m_2) \Rightarrow k_1 = k_2 \Rightarrow \forall x_1 g_2.(f_1\ k_1\ x_1) \sqsubseteq_{g_2} (f_2\ k_2\ g_2) \vdash e_1 \sim e_2 \mid \mathbf{r}_1 \sqsubseteq_f \mathbf{r}_2$$

And now we can apply a synchronous CASE rule, since we have a premise $m_1 = m_2$. This yields 3 proof obligations, where Ψ' is the set of axioms in the previous judgment:

(A.1) $\Psi' \vdash m_1 \sim m_2 \mid \mathbf{r}_1 = [] \Leftrightarrow \mathbf{r}_2 = []$
(A.2) $\Psi' \vdash [] \sim [] \mid \mathbf{r}_1 \sqsubseteq_f \mathbf{r}_2$
(A.3) $\Psi' \vdash \lambda h_1 t_1.\text{case } x_1 \text{ of } 0 \mapsto []; S \mapsto \lambda y_1.h_1 :: f_1\ t_1\ y_1 \sim$
$\lambda h_2 t_2.(g_2\ h_2) :: (f_2\ t_2\ g_2) \mid \forall h_1 t_1 h_2 t_2.m_1 = h_1 :: t_1 \Rightarrow m_2 = h_2 :: t_2 \Rightarrow (\mathbf{r}_1\ h_1\ t_1) \sqsubseteq_{g_2} (\mathbf{r}_2\ h_2\ t_2)$

Premises (A.1) and (A.2) are trivial. To prove (A.3) we first apply ABS twice:

$$\Psi', m_1 = h_1 :: t_1, m_2 = h_2 :: t_2 \vdash \text{case } n_1 \text{ of } 0 \mapsto []; S \mapsto \lambda y_1.h_1 :: f_1\ t_1\ y_1 \sim (g_2\ h_2) :: (f_2\ t_2\ g_2) \mid \mathbf{r}_1 \sqsubseteq_{g_2} \mathbf{r}_2$$

Next, we apply CASE-L, which has the following two premises:

(A.3.i) $\Psi', m_1 = h_1 :: t_1, m_2 = h_2 :: t_2, n_1 = 0 \vdash [] \sim (g_2\ h_2) :: (f_2\ t_2\ g_2) \mid \mathbf{r}_1 \sqsubseteq_{g_2} \mathbf{r}_2$
(A.3.ii) $\Psi', m_1 = h_1 :: t_1, m_2 = h_2 :: t_2 \vdash \lambda y_1.h_1 :: f_1\ t_1\ y_1 \sim (g_2\ h_2) :: (f_2\ t_2\ g_2) \mid \forall y_1.n_1 = S y_1 \Rightarrow (\mathbf{r}_1\ y_1) \sqsubseteq_{g_2} \mathbf{r}_2$

Premise (A.3.i) can be directly derived in HOL from the definition of $\sqsubseteq_{g_2}$. To prove (A.3.ii) we need to make use of our inductive hypothesis:

$$\forall k_1 k_2.(k_1,k_2) < (m_1,m_2) \Rightarrow k_1 = k_2 \Rightarrow \forall x_1 g_2.(f_1\ k_1\ x_1) \sqsubseteq_{g_2} (f_2\ k_2\ g_2)$$

In particular, from the premises $m_1 = h_1 :: t_1$ and $m_2 = h_2 :: t_2$ we can deduce $(t_1,t_2) < (m_1,m_2)$. Additionally, from the premise $m_1 = m_2$ we prove $t_1 = t_2$. Therefore, from the inductive hypothesis we derive $\forall x_1 g_2.(f_1\ t_1\ x_1) \sqsubseteq_{g_2} (f_2\ t_2\ g_2)$, and by definition of $\sqsubseteq_{g_2}$, and the fact that $h_1 = h_2$, for every y we can prove $h_1 :: (f_1\ t_1\ y) \sqsubseteq_{g_2} (g_2\ h_2) :: f_2\ t_2$. By Theorem 6, we can prove (A.3.ii).

We will now show how to prove (B) :

$$\Psi \vdash map \sim take \mid \forall m_1 m_2.m_1 \sqsubseteq_{g_2} m_2 \Rightarrow (\forall g_1.g_1 = g_2 \Rightarrow \forall x_2.x_2 \geq |m_1| \Rightarrow (\mathbf{r}_1\ m_1\ g_1) \sqsubseteq (\mathbf{r}_2\ m_2\ x_2))$$

On this branch we will also use LETREC. We have to prove a premise:

$$\Psi, \Phi \vdash \lambda g_1.e_2 \sim \lambda x_2.e_1 \mid \forall g_1.g_1 = g_2 \Rightarrow \forall x_2.x_2 \geq |m_1| \Rightarrow (\mathbf{r}_1\ g_1) \sqsubseteq (\mathbf{r}_2\ x_2)$$

where

$$\Phi \triangleq \begin{array}{c} m_1 \sqsubseteq_{g_2} m_2, \\ \forall k_1 k_2.(k_1,k_2) < (m_1,m_2) \Rightarrow k_1 \sqsubseteq_{g_2} k_2 \Rightarrow (\forall g_1.g_1 = g_2 \Rightarrow \forall x_2.x_2 \geq |k_1| \Rightarrow (\mathbf{r}_1\ k_1\ g_1) \sqsubseteq (\mathbf{r}_2\ k_2\ x_2)) \end{array}$$

We start by applying ABS. Our goal is to prove:

$$\Psi, \Phi, x_2 \geq |m_1|, g_1 = g_2 \vdash \begin{array}{l} \text{case } m_1 \text{ of } [] \mapsto [] \\ ;\_ :: \_ \mapsto \lambda h_1 t_1.(g_1\ h_1) :: (f_1\ t_1\ g_1) \end{array} \sim \begin{array}{l} \text{case } m_2 \text{ of } [] \mapsto [] \\ ;\_ :: \_ \mapsto \lambda h_2 t_2.\text{case } x_2 \text{ of } 0 \mapsto [] \\ ;S \mapsto \lambda y_2.h_2 :: f_2\ t_2\ y_2 \end{array} \mid \mathbf{r}_1 \sqsubseteq \mathbf{r}_2$$

Notice that we have α-renamed the variables to have the appropriate subscript. Now we want to apply a CASE rule, but the lists over which we are matching are not necessarily of the same length. Therefore, we use the asynchronous LISTCASE-A rule. We have to prove four premises:

(B.1) $\Psi, \Phi, x_2 \geq |m_1|, g_1 = g_2, m_1 = [], m_2 = [] \vdash [] \sim [] \mid \mathbf{r}_1 \sqsubseteq \mathbf{r}_2$
(B.2) $\Psi, \Phi, x_2 \geq |m_1|, g_1 = g_2, m_1 = [] \vdash [] \sim$
$\lambda h_2 t_2.\text{case } x_2 \text{ of } 0 \mapsto []; S \mapsto \lambda y_2.h_2 :: f_2\ t_2\ y_2 \mid \forall h_2 t_2.m_2 = h_2 :: t_2 \Rightarrow \mathbf{r}_1 \sqsubseteq (\mathbf{r}_2\ h_2\ t_2)$

(B.3) $\Psi, \Phi, x_2 \geq |m_1|, g_1 = g_2, m_2 = [] \vdash \lambda h_1 t_1.(g_1\ h_1) :: (f_1\ t_1\ g_1) \sim [] \mid \forall h_1 t_1.m_1 = h_1 :: t_1 \Rightarrow (\mathbf{r}_1\ h_1\ t_1) \sqsubseteq \mathbf{r}_2$

(B.4) $\Psi, \Phi, x_2 \geq |m_1|, g_1 = g_2 \vdash \lambda h_1 t_1.(g_1\ h_1) :: (f_1\ t_1\ g_1) \sim$
$\lambda h_2 t_2.\text{case } x_2 \text{ of } 0 \mapsto []; S \mapsto \lambda y_2.h_2 :: f_2\ t_2\ y_2 \mid$
$\forall h_1 t_1 h_2 t_2.m_1 = h_1 :: t_1 \Rightarrow m_2 = h_1 :: t_1 \Rightarrow (\mathbf{r}_1\ h_1\ t_1) \sqsubseteq (\mathbf{r}_2\ h_2\ t_2)$

Premises (B.1) and (B.2) are trivially derived from the definition of the $\sqsubseteq$ predicate. To prove premise (B.3) we see that we have premises $m_1 \sqsubseteq_{g_2} m_2$, $m_2 = []$, and $m_1 = h_1 :: t_2$, from which we can derive a contradiction.

It remains to prove (B.4). To do so, we apply ABS twice and then NATCASE-R, which has two premises:

(B.4.i) $\Psi, \Phi, x_2 \geq |m_1|, g_1 = g_2, m_1 = h_1 :: t_1, m_2 = h_1 :: t_1, x_2 = 0 \vdash (g_1\ h_1) :: (f_1\ t_1\ g_1) \sim [] \mid \mathbf{r}_1 \sqsubseteq \mathbf{r}_2$

(B.4.ii) $\Psi, \Phi, x_2 \geq |m_1|, g_1 = g_2, m_1 = h_1 :: t_1, m_2 = h_1 :: t_1 \vdash (g_1\ h_1) :: (f_1\ t_1\ g_1) \sim \lambda y_2.h_2 :: f_2\ t_2\ y_2 \mid$
$\forall y_2.x_2 = S y_2 \Rightarrow \mathbf{r}_1 \sqsubseteq (\mathbf{r}_2\ y_2)$

To prove (B.4.i) we derive a contradiction between the premises. From $x_2 = 0$ and the premise $x_2 \geq |m_1|$ we derive $m_1 = []$ and, together with $m_1 = h_1 :: t_1$ we arrive at a contradiction by applying NC.

To prove (B.4.ii) we need to use the induction hypothesis. From $m_1 = h_1 :: t_1, m_2 = h_1 :: t_1$ we can prove that $|t_1| < |m_1|$ and $|t_2| < |m_2|$, so we can do a CUT with the i.h. and derive:

$$t_1 \sqsubseteq_{g_2} t_2 \Rightarrow (\forall g_1.g_1 = g_2 \Rightarrow \forall x_2.x_2 \geq |t_1| \Rightarrow (f_1\ t_1\ g_1) \sqsubseteq (f_2\ t_2\ x_2))$$

By assumption, $m_1 \sqsubseteq_{g_2} m_2$, so $t_1 \sqsubseteq_{g_2} t_2$. Moreover, also by assumption $g_1 = g_2$, and $S y_2 = x_2 \geq |m_1| = S|t_1|$, so $y_2 \geq |t_1|$. So if we instantiate the i.h. with g_1 and y_2, and apply CUT again, we can prove:

$$(f_1\ t_1\ g_1) \sqsubseteq (f_2\ t_2\ y_2)$$

On the other hand, since $h_1 :: t_1 \sqsubseteq_{g_2} h_2 :: t_2$, then (by elimination of $\sqsubseteq_{g_2}$) we can derive $g_1 h_1 = h_2$ and by definition of $\sqsubseteq$, $(g_1\ h_1) :: (f_1\ t_1\ g_1) \sqsubseteq h_2 :: (f_2\ t_2\ y_2)$. So we can apply Theorem 6 and prove (B.4.ii). This ends the proof. □

□

Proof of Theorem 20

Theorem 20. Let $\tau \triangleq \mathsf{list}_{\mathbb{N}} \to \mathsf{list}_{\mathbb{N}}$. Then, $\bullet \mid \bullet \vdash \mathsf{isort} : \tau \sim \mathsf{isort} : \tau \mid \forall x_1\, x_2.\, (\mathsf{sorted}(x_1) \wedge |x_1| = |x_2|) \Rightarrow \pi_2(\mathbf{r}_1\ x_1) \leq \pi_2(\mathbf{r}_2\ x_2)$.

We need two straightforward lemmas in UHOL. The lemmas state that sorting preserves the length and minimum element of a list.

Lemma 26. Let $\tau \triangleq \mathsf{list}_{\mathbb{N}} \to \mathsf{list}_{\mathbb{N}}$. Then, (1) $\bullet \mid \bullet \vdash \mathsf{insert} : \mathbb{N} \to \tau \mid \forall x\, l.\, |\pi_1(\mathbf{r}\ x\ l)| = 1 + |l|$, and (2) $\bullet \mid \bullet \vdash \mathsf{isort} : \tau \mid \forall x.\, |\pi_1(\mathbf{r}\ x)| = |x|$.

Lemma 27. Let $\tau \triangleq \mathsf{list}_{\mathbb{N}} \to \mathsf{list}_{\mathbb{N}}$. Then, (1) $\bullet \mid \bullet \vdash \mathsf{insert} : \mathbb{N} \to \tau \mid \forall x\, l.\, \mathsf{lmin}(\pi_1(\mathbf{r}\ x\ l)) = \mathsf{min}(x, \mathsf{lmin}(l))$, and (2) $\bullet \mid \bullet \vdash \mathsf{isort} : \tau \mid \forall x.\, \mathsf{lmin}(\pi_1(\mathbf{r}\ x)) = \mathsf{lmin}(x)$.

Proof of Theorem 20. We prove the theorem using LETREC. We actually show the following stronger theorem, which yields a stronger induction hypothesis in the proof.

$$\begin{array}{l}\bullet \mid \bullet \vdash \mathsf{isort} : \tau \sim \mathsf{isort} : \tau \mid \forall x_1\, x_2.\, (\mathsf{sorted}(x_1) \wedge |x_1| = |x_2|) \Rightarrow \\ (\pi_2(\mathbf{r}_1\ x_1) \leq \pi_2(\mathbf{r}_2\ x_2)) \wedge \underline{(\mathbf{r}_1\ x_1 = \mathsf{isort}\ x_1) \wedge (\mathbf{r}_2\ x_2 = \mathsf{isort}\ x_2)}\end{array}$$

Let ι denote the inductive hypothesis:

$$\begin{array}{l}\iota \triangleq \forall m_1\, m_2.\, (|m_1|, |m_2|) < (|x_1|, |x_2|) \Rightarrow (\mathsf{sorted}(m_1) \wedge |m_1| = |m_2|) \\ \qquad \Rightarrow \pi_2(isort_1\ m_1) \leq \pi_2(isort_2\ m_2) \wedge (isort_1\ m_1 = \mathsf{isort}\ m_1) \wedge (isort_2\ m_2 = \mathsf{isort}\ m_2)\end{array}$$

and e denote the body of the function isort:

$$\begin{aligned} e \triangleq\ & \text{case } l \text{ of } [] \mapsto ([], 0); \\ & \_ :: \_ \mapsto \lambda h\, t.\ \ \text{let } s = isort\ t \\ & \qquad\qquad\qquad \text{let } s' = \text{insert } h\ (\pi_1\ s) \text{ in} \\ & \qquad\qquad\qquad (\pi_1\ s', (\pi_2\ s) + (\pi_2\ s')) \end{aligned}$$

By LETREC, it suffices to prove the following (we omit simple types for easier reading; they play no essential role in the proof).

$$isort_1, isort_2, x_1, x_2 \mid \text{sorted}(x_1), |x_1| = |x_2|, \iota \vdash e[isort_1/isort][x_1/l] \sim e[isort_2/isort][x_2/l] \mid \begin{pmatrix} \pi_2\ \mathbf{r}_1 \leq \pi_2\ \mathbf{r}_2 \\ \wedge\ \mathbf{r}_1 = \text{isort } x_1 \\ \wedge\ \mathbf{r}_2 = \text{isort } x_2 \end{pmatrix}$$

Following the structure of e, we next apply the rule LISTCASE. This yields the following two main proof obligations, corresponding to the two case branches (the third proof obligation, $x_1 = [] \Leftrightarrow x_2 = []$ follows immediately from the assumption $|x_1| = |x_2|$).

$$\begin{array}{c} isort_1, isort_2, x_1, x_2 \mid \text{sorted}(x_1), |x_1| = |x_2|, \iota, x_1 = x_2 = [] \vdash ([], 0) \sim ([], 0) \mid \\ (\pi_2\ \mathbf{r}_1 \leq \pi_2\ \mathbf{r}_2) \wedge (\mathbf{r}_1 = \text{isort } x_1) \wedge (\mathbf{r}_2 = \text{isort } x_2) \end{array} \tag{1}$$

$$\frac{\begin{array}{l} isort_1, isort_2, \\ x_1, x_2, h_1, t_1, h_2, t_2 \mid \\ \text{sorted}(x_1), |x_1| = |x_2|, \iota, \\ x_1 = h_1 :: t_1, x_2 = h_2 :: t_2 \end{array}}{} \vdash \begin{array}{l} \text{let } s = isort_1\ t_1 \\ \text{let } s' = \text{insert } h_1\ (\pi_1\ s) \text{ in} \\ (\pi_1\ s', (\pi_2\ s) + (\pi_2\ s')) \end{array} \sim \begin{array}{l} \text{let } s = isort_2\ t_2 \\ \text{let } s' = \text{insert } h_2\ (\pi_1\ s) \text{ in} \\ (\pi_1\ s', (\pi_2\ s) + (\pi_2\ s')) \end{array} \left| \begin{array}{l} \pi_2\ \mathbf{r}_1 \leq \pi_2\ \mathbf{r}_2 \\ \wedge\ \mathbf{r}_1 = \text{isort } x_1 \\ \wedge\ \mathbf{r}_2 = \text{isort } x_2 \end{array} \right. \tag{2}$$

(1) is immediate: By Theorem 6, it suffices to show that $(\pi_2([], 0) \leq \pi_2([], 0)) \wedge (([], 0) = \text{isort } x_1) \wedge (([], 0) = \text{isort } x_2)$. Since $x_1 = x_2 = []$ by assumption here, this is equivalent to $(\pi_2([], 0) \leq \pi_2([], 0)) \wedge (([], 0) = \text{isort } []) \wedge (([], 0) = \text{isort } [])$, which is trivial by direct computation.

To prove (2), we expand the outermost occurrences of let in both to function applications using the definition let $x = e_1$ in $e_2 \triangleq (\lambda x.e_2)\ e_1$. Applying the rules APP and ABS, it suffices to prove the following for any ϕ of our choice.

$$isort_1, isort_2, x_1, x_2, h_1, t_1, h_2, t_2 \left| \begin{array}{l} \text{sorted}(x_1), |x_1| = |x_2|, \\ \iota, x_1 = h_1 :: t_1, x_2 = h_2 :: t_2 \end{array} \right. \vdash isort_1\ t_1 \sim isort_2\ t_2 \mid \phi \tag{3}$$

$$\frac{\begin{array}{l} isort_1, isort_2, x_1, x_2, \\ h_1, t_1, h_2, t_2, s_1, s_2 \mid \\ \text{sorted}(x_1), |x_1| = |x_2|, \iota, \\ x_1 = h_1 :: t_1, x_2 = h_2 :: t_2 \\ \phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2] \end{array}}{} \vdash \begin{array}{l} \text{let } s' = \text{insert } h_1\ (\pi_1\ s_1) \text{ in} \\ (\pi_1\ s', (\pi_2\ s_1) + (\pi_2\ s')) \end{array} \sim \begin{array}{l} \text{let } s' = \text{insert } h_2\ (\pi_1\ s_2) \text{ in} \\ (\pi_1\ s', (\pi_2\ s_2) + (\pi_2\ s')) \end{array} \left| \begin{array}{l} \pi_2\ \mathbf{r}_1 \leq \pi_2\ \mathbf{r}_2 \\ \wedge\ \mathbf{r}_1 = \text{isort } x_1 \\ \wedge\ \mathbf{r}_2 = \text{isort } x_2 \end{array} \right. \tag{4}$$

We choose ϕ as follows:

$$\phi \triangleq \pi_2\ \mathbf{r}_1 \leq \pi_2\ \mathbf{r}_2 \wedge \mathbf{r}_1 = \text{isort}(t_1) \wedge \mathbf{r}_2 = \text{isort}(t_2) \wedge |\pi_1\ \mathbf{r}_1| = |\pi_1\ \mathbf{r}_2| \wedge \text{lmin}(t_1) = \text{lmin}(\pi_1\ \mathbf{r}_1)$$

Proof of (3): By Theorem 6, it suffices to prove the following five statements in HOL under the context of (3). These statements correspond to the five conjuncts of ϕ.

$$\pi_2(isort_1\ t_1) \leq \pi_2(isort_2\ t_2) \tag{5}$$

$$isort_1\ t_1 = \mathsf{isort}\ t_1 \tag{6}$$

$$isort_1\ t_2 = \mathsf{isort}\ t_2 \tag{7}$$

$$|\pi_1(isort_1\ t_1)| = |\pi_1(isort_2\ t_2)| \tag{8}$$

$$\mathsf{lmin}(t_1) = \mathsf{lmin}(\pi_1(isort_1\ t_1)) \tag{9}$$

(5)–(7) follow from the induction hypothesis ι instantiated with $m_1 := t_1, m_2 := t_2$. Note that because $x_1 = h_1 :: t_1$ and $x_2 = h_2 :: t_2$, we can prove (in HOL) that $(|t_1|, |t_2|) < (|x_1|, |x_2|)$. Since, $|x_1| = |x_2|, x_1 = h_1 :: t_1$ and $x_2 = h_2 :: t_2$, we can also prove that $|t_1| = |t_2|$. Finally, from the axiomatic definition of sorted and the assumption $\mathsf{sorted}(x_1)$ it follows that $\mathsf{sorted}(t_1)$. These together allow us to instantiate the i.h. ι and immediately derive (5)–(7).

To prove (8), we use (6) and (7), which reduces (8) to $|\pi_1(\mathsf{isort}\ t_1)| = |\pi_1(\mathsf{isort}\ t_2)|$. To prove this, we apply Theorem 3 to Lemma 26, yielding $\forall x.\ |\pi_1(\mathsf{isort}\ x)| = |x|$. Hence, we can further reduce our goal to proving $|t_1| = |t_2|$, which we already did above.

To prove (9), we use (6), which reduces (9) to $\mathsf{lmin}(t_1) = \mathsf{lmin}(\pi_1(\mathsf{isort}\ t_1))$. This follows immediately from Theorem 3 applied to Lemma 27.

This proves (3).

Proof of (4): We expand the definition of let and apply the rules APP and ABS to reduce (4) to proving the following for any ϕ'.

$$\begin{array}{l} isort_1, isort_2, x_1, x_2, \\ h_1, t_1, h_2, t_2, s_1, s_2 \end{array} \left| \begin{array}{l} \mathsf{sorted}(x_1), |x_1| = |x_2|, \\ \iota, x_1 = h_1 :: t_1, x_2 = h_2 :: t_2, \\ \phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2] \end{array} \right. \vdash \mathsf{insert}\ h_1\ (\pi_1\ s_1) \sim \mathsf{insert}\ h_2\ (\pi_1\ s_2) \left|\ \phi' \right. \tag{10}$$

$$\begin{array}{l} isort_1, isort_2, x_1, x_2, \\ h_1, t_1, h_2, t_2, s_1, s_2, s_1', s_2' \mid \\ \mathsf{sorted}(x_1), |x_1| = |x_2|, \\ \iota, x_1 = h_1 :: t_1, x_2 = h_2 :: t_2 \\ \phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2], \\ \phi'[s_1'/\mathbf{r}_1][s_2'/\mathbf{r}_2] \end{array} \vdash (\pi_1\ s_1', (\pi_2\ s_1) + (\pi_2\ s_1')) \sim (\pi_1\ s_2', (\pi_2\ s_2) + (\pi_2\ s_2')) \left| \begin{array}{l} \pi_2\ \mathbf{r}_1 \leq \pi_2\ \mathbf{r}_2 \\ \wedge\ \mathbf{r}_1 = \mathsf{isort}\ x_1 \\ \wedge\ \mathbf{r}_2 = \mathsf{isort}\ x_2 \end{array} \right. \tag{11}$$

We pick the following ϕ':

$$\phi' \triangleq \pi_2\ \mathbf{r}_1 \leq \pi_2\ \mathbf{r}_2 \wedge \mathbf{r}_1 = \mathsf{insert}\ h_1\ (\pi_1\ s_1) \wedge \mathbf{r}_2 = \mathsf{insert}\ h_2\ (\pi_1\ s_2)$$

Proof of (10): We start by applying Theorem 6. This yields three subgoals in HOL, corresponding to the three conjuncts in ϕ':

$$\pi_2(\mathsf{insert}\ h_1\ (\pi_1\ s_1)) \leq \pi_2(\mathsf{insert}\ h_2\ (\pi_1\ s_2)) \tag{12}$$

$$\mathsf{insert}\ h_1\ (\pi_1\ s_1) = \mathsf{insert}\ h_1\ (\pi_1\ s_1) \tag{13}$$

$$\mathsf{insert}\ h_2\ (\pi_1\ s_2) = \mathsf{insert}\ h_2\ (\pi_1\ s_2) \tag{14}$$

(13) and (14) are trivial, so we only have to prove (12). Since $s_1 = \text{isort } t_1$ and $s_2 = \text{isort } t_2$ are conjuncts in the assumption $\phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2]$, (12) is equivalent to:

$$\pi_2(\text{insert } h_1\ (\pi_1(\text{isort } t_1))) \leq \pi_2(\text{insert } h_2\ (\pi_1(\text{isort } t_2))) \tag{15}$$

To prove this, we split cases on the shapes of $\pi_1(\text{isort } t_1)$ and $\pi_1(\text{isort } t_2)$. From the conjuncts in $\phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2]$, it follows immediately that $|\pi_1(\text{isort } t_1)| = |\pi_1(\text{isort } t_2)|$. Hence, only two cases apply:
Case: $\pi_1(\text{isort } t_1) = \pi_1(\text{isort } t_2) = []$. In this case, by direct computation, $\pi_2(\text{insert } h_1\ (\pi_1(\text{isort } t_1))) = \pi_2(\text{insert } h_1\ []) = \pi_2([h_1], 0) = 0$. Similarly, and $\pi_2(\text{insert } h_2\ (\pi_1(\text{isort } t_2))) = 0$. So, the result follows trivially.
Case: $\pi_1(\text{isort } t_1) = h_1' :: t_1'$ and $\pi_1(\text{isort } t_2) = h_2' :: t_2'$. We first argue that $h_1 \leq h_1'$. Note that from the second and fifth conjuncts in $\phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2]$, it follows that $\text{lmin}(t_1) = \text{lmin}(\pi_1(\text{isort } t_1))$. Since $\pi_1(\text{isort } t_1) = h_1' :: t_1'$, we further get $\text{lmin}(t_1) = \text{lmin}(\pi_1(\text{isort } t_1)) = \text{lmin}(h_1' :: t_1') = \min(h_1', \text{lmin}(t_1')) \leq h_1'$. Finally, from the axiomatic definition of $\text{sorted}(x_1)$ and $x_1 = h_1 :: t_1$, we derive $h_1 \leq \text{lmin}(t_1)$. Combining, we get $h_1 \leq \text{lmin}(t_1) \leq h_1'$.

Next, $\pi_2(\text{insert } h_1\ (\pi_1(\text{isort } t_1))) = \pi_2(\text{insert } h_1\ (h_1' :: t_1'))$. Expanding the definition of insert and using $h_1 \leq h_1'$, we immediately get $\pi_2(\text{insert } h_1\ (\pi_1(\text{isort } t_1))) = \pi_2(\text{insert } h_1\ (h_1' :: t_1')) = \pi_2(h_1 :: h_1' :: t_1', 1) = 1$. On the other hand, it is fairly easy to prove (by case analyzing the result of $h_2 \leq h_2'$) that $\pi_2(\text{insert } h_2\ (\pi_1(\text{isort } t_2))) = \pi_2(\text{insert } h_2\ (h_2' :: t_2')) \geq 1$. Hence, $\pi_2(\text{insert } h_1\ (\pi_1(\text{isort } t_1))) = 1 \leq \pi_2(\text{insert } h_2\ (\pi_1(\text{isort } t_2)))$.
This proves (15) and, hence, (12) and (10).

Proof of (11): By Theorem 6, it suffices to show the following in HOL, under the assumptions of (11):

$$\pi_2(\pi_1\ s_1', (\pi_2\ s_1) + (\pi_2\ s_1')) \leq \pi_2(\pi_1\ s_2', (\pi_2\ s_2) + (\pi_2\ s_2')) \tag{16}$$

$$(\pi_1\ s_1', (\pi_2\ s_1) + (\pi_2\ s_1')) = \text{isort } x_1 \tag{17}$$

$$(\pi_1\ s_2', (\pi_2\ s_2) + (\pi_2\ s_2')) = \text{isort } x_2 \tag{18}$$

By computation, (16) is equivalent to $(\pi_2\ s_1) + (\pi_2\ s_1') \leq (\pi_2\ s_2) + (\pi_2\ s_2')$. Using the definition of ϕ, it is easy to see that $\pi_2\ s_1 \leq \pi_2\ s_2$ is a conjunct in the assumption $\phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2]$. Similarly, using the definition of ϕ', $\pi_2\ s_1' \leq \pi_2\ s_2'$ is a conjunct in the assumption $\phi'[s_1'/\mathbf{r}_1][s_2'/\mathbf{r}_2]$. (16) follows immediately from these.

To prove (17), note that since $x_1 = h_1 :: t_1$, expanding the definition of isort, we get

$$\text{isort } x_1 = (\pi_1(\text{insert } h_1\ (\pi_1(\text{isort } t_1))), \pi_2(\text{isort } t_1) + \pi_2(\text{insert } h_1\ (\pi_1(\text{isort } t_1))))$$

Matching with the left side of (17), it suffices to show that $s_1' = \text{insert } h_1\ (\pi_1(\text{isort } t_1))$ and $s_1 = \text{isort } t_1$. These are immediate: $s_1 = \text{isort } t_1$ is a conjunct in the assumption $\phi[s_1/\mathbf{r}_1][s_2/\mathbf{r}_2]$, while $s_1' = \text{insert } h_1\ (\pi_1(\text{isort } t_1))$ follows trivially from this and the conjunct $s_1' = \text{insert } h_1\ (\pi_1\ s_1)$ in $\phi'[s_1'/\mathbf{r}_1][s_2'/\mathbf{r}_2]$. This proves (17).

The proof of (18) is similar to that of (17).
This proves (11) and, hence, (4). □

E FULL RHOL RULES

The full set of RHOL rules is in the following figures:

REFERENCES

Ezgi Çiçek, Gilles Barthe, Marco Gaboardi, Deepak Garg, and Jan Hoffmann. 2017. Relational cost analysis. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*, Giuseppe Castagna and Andrew D. Gordon (Eds.). ACM, 316–329. http://dl.acm.org/citation.cfm?id=3009858

$$\frac{\Gamma, x_1 : \tau_1, x_2 : \tau_2 \mid \Psi, \phi' \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}{\Gamma \mid \Psi \vdash \lambda x_1.t_1 : \tau_1 \to \sigma_1 \sim \lambda x_2.t_2 : \tau_2 \to \sigma_2 \mid \forall x_1, x_2.\phi' \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]}\ \textsf{ABS}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \tau_1 \to \sigma_1 \sim t_2 : \tau_2 \to \sigma_2 \mid \forall x_1, x_2.\phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2] \\ \Gamma \mid \Psi \vdash u_1 : \tau_1 \sim u_2 : \tau_2 \mid \phi'\end{array}}{\Gamma \mid \Psi \vdash t_1 u_1 : \sigma_1 \sim t_2 u_2 : \sigma_2 \mid \phi[u_1/x_1][u_2/x_2]}\ \textsf{APP}$$

$$\frac{\Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi[0/\mathbf{r}_1][0/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash 0 : \mathbb{N} \sim 0 : \mathbb{N} \mid \phi}\ \textsf{ZERO} \qquad \frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{N} \sim t_2 : \mathbb{N} \mid \phi' \\ \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \forall x_1 x_2 \phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi[Sx_1/\mathbf{r}_1][Sx_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash St_1 : \mathbb{N} \sim St_2 : \mathbb{N} \mid \phi}\ \textsf{SUCC}$$

$$\frac{\Gamma \mid \Psi \vdash \phi[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \quad \Gamma \vdash x_1 : \sigma_1 \quad \Gamma \vdash x_1 : \sigma_1}{\Gamma \mid \Psi \vdash x_1 : \sigma_1 \sim x_2 : \sigma_2 \mid \phi}\ \textsf{VAR} \qquad \frac{\Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi[\mathsf{tt}/\mathbf{r}_1][\mathsf{tt}/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash \mathsf{tt} : \mathbb{B} \sim \mathsf{tt} : \mathbb{B} \mid \phi}\ \textsf{TRUE}$$

$$\frac{\Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi[\mathsf{ff}/\mathbf{r}_1][\mathsf{ff}/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash \mathsf{ff} : \mathbb{B} \sim \mathsf{ff} : \mathbb{B} \mid \phi}\ \textsf{FALSE} \qquad \frac{\Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi[[]/\mathbf{r}_1][[]/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash [] : \mathsf{list}_{\sigma_1} \sim [] : \mathsf{list}_{\sigma_2} \mid \phi}\ \textsf{NIL}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash h_1 : \sigma_1 \sim h_2 : \sigma_2 \mid \phi' \qquad \Gamma \mid \Psi \vdash t_1 : \mathsf{list}_{\sigma_1} \sim t_2 : \mathsf{list}_{\sigma_2} \mid \phi'' \\ \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \forall x_1 x_2 y_1 y_2.\phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi''[y_1/\mathbf{r}_1][y_2/\mathbf{r}_2] \Rightarrow \phi[x_1 :: y_1/\mathbf{r}_1][x_2 :: y_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash h_1 :: t_1 : \mathsf{list}_{\sigma_1} \sim h_2 :: t_2 : \mathsf{list}_{\sigma_2} \mid \phi}\ \textsf{CONS}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi' \qquad \Gamma \mid \Psi \vdash u_1 : \tau_1 \sim u_2 : \tau_2 \mid \phi'' \\ \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \forall x_1 x_2 y_1 y_2.\phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi''[y_1/\mathbf{r}_1][y_2/\mathbf{r}_2] \Rightarrow \phi[\langle x_1, y_1\rangle/\mathbf{r}_1][\langle x_2, y_2\rangle/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \langle t_1, u_1\rangle : \sigma_1 \times \tau_1 \sim \langle t_2, u_2\rangle : \sigma_2 \times \tau_2 \mid \phi}\ \textsf{PAIR}$$

$$\frac{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \times \tau_1 \sim t_2 : \sigma_2 \times \tau_2 \mid \phi[\pi_i(\mathbf{r}_1)/\mathbf{r}_1][\pi_i(\mathbf{r}_2)/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash \pi_i(t_1) : \sigma_1 \sim \pi_i(t_2) : \sigma_2 \mid \phi}\ \textsf{PROJ}_\mathsf{i}$$

Fig. 1. Core two-sided rules

$$\frac{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi' \quad \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi'[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2] \Rightarrow \phi[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}\ \mathsf{SUB}$$

$$\frac{\Gamma \mid \Psi' \vdash t_1 : \sigma_2 \sim t_2 : \sigma_2 \mid \phi \quad \Gamma \mid \Psi' \vdash t_1 : \sigma_2 \sim t_2 : \sigma_2 \mid \phi'}{\Gamma \mid \Psi' \vdash t_1 : \sigma_2 \sim t_2 : \sigma_2 \mid \phi \wedge \phi'}\ \wedge_{\mathsf{I}}$$

$$\frac{\Gamma \mid \Psi', \phi'[t_1/\mathbf{r}_1][t_2/\mathbf{r}_2] \vdash t_1 : \sigma_2 \sim t_2 : \sigma_2 \mid \phi}{\Gamma \mid \Psi' \vdash t_1 : \sigma_2 \sim t_2 : \sigma_2 \mid \phi' \Rightarrow \phi}\ \Rightarrow_{\mathsf{I}}$$

$$\frac{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \mid \phi[\mathbf{r}/\mathbf{r}_1][t_2/\mathbf{r}_2]}{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_1 \mid \phi}\ \mathsf{UHOL-L}$$

Fig. 2. Structural rules

$$\frac{\Gamma, x_1 : \tau_1 \mid \Psi, \phi' \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}{\Gamma \mid \Psi \vdash \lambda x_1.t_1 : \tau_1 \to \sigma_1 \sim t_2 : \sigma_2 \mid \forall x_1.\phi' \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1]}\ \textsf{ABS-L}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \tau_1 \to \sigma_1 \sim u_2 : \sigma_2 \mid \forall x_1.\phi'[x_1/\mathbf{r}_1] \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1] \\ \Gamma \mid \Psi \vdash u_1 : \sigma_1 \mid \phi'\end{array}}{\Gamma \mid \Psi \vdash t_1 u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi[u_1/x_1]}\ \textsf{APP-L}$$

$$\frac{\begin{array}{c}\Gamma \vdash t_2 : \sigma_2 \\ \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi[0/\mathbf{r}_1][t_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash 0 : \mathbb{N} \sim t_2 : \sigma_2 \mid \phi}\ \textsf{ZERO-L} \qquad \frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{N} \sim t_2 : \sigma_2 \mid \phi' \\ \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \forall x_1 x_2 \phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi[S x_1/\mathbf{r}_1][x_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash S t_1 : \mathbb{N} \sim t_2 : \sigma_2 \mid \phi}\ \textsf{SUCC-L}$$

$$\frac{\Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi[\mathsf{tt}/\mathbf{r}_1][t_2/\mathbf{r}_2] \quad \Gamma \vdash t_2 : \sigma_2}{\Gamma \mid \Psi \vdash \mathsf{tt} : \mathbb{B} \sim t_2 : \sigma_2 \mid \phi}\ \textsf{TRUE - L} \qquad \frac{\Gamma \mid \Psi \vdash_{\mathsf{HOL}} \phi[\mathsf{ff}/\mathbf{r}_1][t_2/\mathbf{r}_2] \quad \Gamma \vdash t_2 : \sigma_2}{\Gamma \mid \Psi \vdash \mathsf{ff} : \mathbb{B} \sim t_2 : \sigma_2 \mid \phi}\ \textsf{FALSE - L}$$

$$\frac{\phi[x_1/\mathbf{r}_1] \in \Psi \quad \mathbf{r}_2 \notin FV(\phi) \quad \Gamma \vdash t_2 : \sigma_2}{\Gamma \mid \Psi \vdash x_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}\ \textsf{VAR-L} \qquad \frac{\Gamma \mid \Psi \vdash \phi[[]/\mathbf{r}_1][t_2/\mathbf{r}_2] \quad \Gamma \vdash t_2 : \sigma_2}{\Gamma \mid \Psi \vdash [] : \mathsf{list}_{\sigma_1} \sim t_2 : \sigma_2 \mid \phi}\ \textsf{NIL-L}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash h_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi' \qquad \Gamma \mid \Psi \vdash t_1 : \mathsf{list}_{\sigma_1} \sim t_2 : \sigma_2 \mid \phi'' \\ \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \forall x_1 x_2 y_1.\phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi''[y_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi[x_1 :: y_1/\mathbf{r}_1][x_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash h_1 :: t_1 : \mathsf{list}_{\sigma_1} \sim t_2 : \sigma_2 \mid \phi}\ \textsf{CONS-L}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi' \qquad \Gamma \mid \Psi \vdash u_1 : \tau_1 \sim t_2 : \sigma_2 \mid \phi'' \\ \Gamma \mid \Psi \vdash_{\mathsf{HOL}} \forall x_1 x_2 y_1.\phi'[x_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi''[y_1/\mathbf{r}_1][x_2/\mathbf{r}_2] \Rightarrow \phi[\langle x_1, y_1\rangle/\mathbf{r}_1][x_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \langle t_1, u_1\rangle : \sigma_1 \times \tau_1 \sim t_2 : \sigma_2 \mid \phi}\ \textsf{PAIR-L}$$

$$\frac{\Gamma \mid \Psi \vdash t_1 : \sigma_1 \times \tau_1 \sim t_2 : \sigma_2 \mid \phi[\pi_1(\mathbf{r}_1)/\mathbf{r}_1]}{\Gamma \mid \Psi \vdash \pi_1(t_1) : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}\ \textsf{PROJ}_1\textsf{-L}$$

Fig. 3. Core one-sided rules

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{B} \sim t_2 : \mathbb{B} \mid (\mathbf{r}_1 = \mathsf{tt} \wedge \mathbf{r}_2 = \mathsf{tt}) \vee (\mathbf{r}_1 = \mathsf{ff} \wedge \mathbf{r}_2 = \mathsf{ff}) \\ \Gamma \mid \Psi, t_1 = \mathsf{tt}, t_2 = \mathsf{tt} \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 = \mathsf{ff}, t_2 = \mathsf{ff} \vdash v_1 : \sigma_1 \sim v_2 : \sigma_2 \mid \phi\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ \mathsf{tt} \mapsto u_1; \mathsf{ff} \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ \mathsf{tt} \mapsto u_2; \mathsf{ff} \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{BOOLCASE}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{N} \sim t_2 : \mathbb{N} \mid \mathbf{r}_1 = 0 \Leftrightarrow \mathbf{r}_2 = 0 \\ \Gamma \mid \Psi, t_1 = 0, t_2 = 0 \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \mathbb{N} \to \sigma_1 \sim v_2 : \mathbb{N} \to \sigma_2 \mid \forall x_1 x_2 . t_1 = S x_1 \Rightarrow t_2 = S x_2 \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ 0 \mapsto u_1; S \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ 0 \mapsto u_2; S \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{NATCASE}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathsf{list}_{\tau_1} \sim t_2 : \mathsf{list}_{\tau_2} \mid \mathbf{r}_1 = [] \Leftrightarrow \mathbf{r}_2 = [] \\ \Gamma \mid \Psi, t_1 = [], t_2 = [] \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \tau_1 \to \mathsf{list}_{\tau_1} \to \sigma_1 \sim v_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \\ \forall h_1 h_2 l_1 l_2 . t_1 = h_1 :: l_1 \Rightarrow t_2 = h_2 :: l_2 \Rightarrow \phi[\mathbf{r}_1\ h_1\ l_1/\mathbf{r}_1][\mathbf{r}_2\ h_2\ l_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ [] \mapsto u_1; \_ :: \_ \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ [] \mapsto u_2; \_ :: \_ \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{LISTCASE}$$

Fig. 4. Synchronous case rules

$$\frac{\begin{array}{c}\Gamma \vdash t_1 : \mathbb{B} \\ \Gamma \mid \Psi, t_1 = \mathsf{tt} \vdash u_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 = \mathsf{ff} \vdash v_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ \mathsf{tt} \mapsto u_1; \mathsf{ff} \mapsto v_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}\ \textsf{BOOLCASE} - \textsf{L}$$

$$\frac{\begin{array}{c}\Gamma \vdash t_1 : \mathbb{N} \\ \Gamma \mid \Psi, t_1 = 0 \vdash u_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \mathbb{N} \to \sigma_1 \sim t_2 : \sigma_2 \mid \forall x_1 . t_1 = S x_1 \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ 0 \mapsto u_1; S \mapsto v_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}\ \textsf{NATCASE} - \textsf{L}$$

$$\frac{\begin{array}{c}\Gamma \vdash t_1 : \mathsf{list}_\tau \\ \Gamma \mid \Psi, t_1 = [] \vdash u_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \tau \to \mathsf{list}_\tau \to \sigma_1 \sim t_2 : \sigma_2 \mid \forall h_1 l_1 . t_1 = h_1 :: l_1 \Rightarrow \phi[\mathbf{r}_1\ h_1\ l_1/\mathbf{r}_1]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ [] \mapsto u_1; \_ :: \_ \mapsto v_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi}\ \textsf{LISTCASE} - \textsf{L}$$

Fig. 5. One-sided case rules

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{B} \sim t_2 : \mathbb{B} \mid \top \\ \Gamma \mid \Psi, t_1 = \mathsf{tt}, t_2 = \mathsf{tt} \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 \neq \mathsf{tt}, t_2 = \mathsf{tt} \vdash v_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 = \mathsf{tt}, t_2 \neq \mathsf{tt} \vdash u_1 : \sigma_1 \sim v_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 \neq \mathsf{tt}, t_2 \neq \mathsf{tt} \vdash v_1 : \sigma_1 \sim v_2 : \sigma_2 \mid \phi\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ \mathsf{tt} \mapsto u_1; \mathsf{ff} \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ \mathsf{tt} \mapsto u_2; \mathsf{ff} \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{BBCASE} - \textsf{A}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{B} \sim t_2 : \mathbb{N} \mid \top \\ \Gamma \mid \Psi, t_1 = \mathsf{tt}, t_2 = 0 \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 \neq \mathsf{tt}, t_2 = 0 \vdash v_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 = \mathsf{tt} \vdash u_1 : \sigma_1 \sim v_2 : \mathbb{N} \to \sigma_2 \mid \forall x_2. t_2 = S x_2 \Rightarrow \phi[\mathbf{r}_2\ x_2/\mathbf{r}_2] \\ \Gamma \mid \Psi, t_1 \neq \mathsf{tt} \vdash v_1 : \sigma_1 \sim v_2 : \mathbb{N} \to \sigma_2 \mid \forall x_2. t_2 = S x_2 \Rightarrow \phi[\mathbf{r}_2\ x_2/_2]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ \mathsf{tt} \mapsto u_1; \mathsf{ff} \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ 0 \mapsto u_2; S \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{BNCASE} - \textsf{A}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{B} \sim t_2 : \mathsf{list}_{\tau_2} \mid \top \\ \Gamma \mid \Psi, t_1 = \mathsf{tt}, t_2 = [] \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 \neq \mathsf{tt}, t_2 = [] \vdash v_1 : \sigma_1 \sim u_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_1 = \mathsf{tt} \vdash u_1 : \sigma_1 \sim v_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \forall h_2 l_2. t_2 = h_2 :: l_2 \Rightarrow \phi[\mathbf{r}_2\ h_2\ l_2/\mathbf{r}_2] \\ \Gamma \mid \Psi, t_1 \neq \mathsf{tt} \vdash v_1 : \sigma_1 \sim v_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \forall h_2 l_2. t_2 = h_2 :: l_2 \Rightarrow \phi[\mathbf{r}_2\ h_2\ l_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ \mathsf{tt} \mapsto u_1; \mathsf{ff} \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ [] \mapsto u_2; \_ :: \_ \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{BLCASE} - \textsf{A}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{N} \sim t_2 : \mathbb{N} \mid \top \\ \Gamma \mid \Psi, t_1 = 0, t_2 = 0 \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_2 = 0 \vdash v_1 : \mathbb{N} \to \sigma_1 \sim u_2 : \sigma_2 \mid \forall x_1. t_1 = S x_1 \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1] \\ \Gamma \mid \Psi, t_1 = 0 \vdash u_1 : \sigma_1 \sim v_2 : \mathbb{N} \to \sigma_2 \mid \forall x_2. t_2 = S x_2 \Rightarrow \phi[\mathbf{r}_2\ x_2/\mathbf{r}_2] \\ \Gamma \mid \Psi \vdash v_1 : \mathbb{N} \to \sigma_1 \sim v_2 : \mathbb{N} \to \sigma_2 \mid \forall x_1 x_2. t_1 = S x_1 \Rightarrow t_2 = S x_2 \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ 0 \mapsto u_1; S \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ 0 \mapsto u_2; S \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{NNCASE} - \textsf{A}$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathsf{list}_{\tau_1} \sim t_2 : \mathsf{list}_{\tau_2} \mid \top \\ \Gamma \mid \Psi, t_1 = [], t_2 = [] \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi, t_2 = [] \vdash v_1 : \tau_1 \to \mathsf{list}_{\tau_1} \to \sigma_1 \sim u_2 : \sigma_2 \mid \forall h_1 l_1. t_1 = h_1 :: l_1 \Rightarrow \phi[\mathbf{r}_1\ h_1\ l_1/\mathbf{r}_1] \\ \Gamma \mid \Psi, t_1 = [] \vdash u_1 : \tau_1 \to \mathsf{list}_{\tau_1} \to \sigma_1 \sim v_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \\ \forall h_2. t_2 = h_2 :: l_2 \Rightarrow \phi[\mathbf{r}_2\ h_2\ l_2/\mathbf{r}_2] \\ \Gamma \mid \Psi \vdash v_1 : \tau_1 \to \mathsf{list}_{\tau_1} \to \sigma_1 \sim v_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \\ \forall h_1 h_2 l_1 l_2. t_1 = h_1 :: l_1 \Rightarrow t_2 = h_2 :: l_2 \Rightarrow \phi[\mathbf{r}_1\ h_1\ l_1/\mathbf{r}_1][\mathbf{r}_2\ h_2\ l_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \mathsf{case}\ t_1\ \mathsf{of}\ [] \mapsto u_1; \_ :: \_ \mapsto v_1 : \sigma_1 \sim \mathsf{case}\ t_2\ \mathsf{of}\ [] \mapsto u_2; \_ :: \_ \mapsto v_2 : \sigma_2 \mid \phi}\ \textsf{LLCASE} - \textsf{A}$$

Fig. 6. Asynchronous case rules (selected)

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathbb{N} \sim t_2 : \mathbb{N} \mid \phi' \wedge \mathbf{r}_1 = 0 \Leftrightarrow \mathbf{r}_2 = 0 \\ \Gamma \mid \Psi, \phi'[0/\mathbf{r}_1][0/\mathbf{r}_2] \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \mathbb{N} \to \sigma_1 \sim v_2 : \mathbb{N} \to \sigma_2 \mid \forall x_1 x_2 . \phi'[Sx_1/\mathbf{r}_1][Sx_2/\mathbf{r}_2] \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \text{case } t_1 \text{ of } 0 \mapsto u_1; S \mapsto v_1 : \sigma_1 \sim \text{case } t_2 \text{ of } 0 \mapsto u_2; S \mapsto v_2 : \sigma_2 \mid \phi} \text{ NATCASE}*$$

$$\frac{\begin{array}{c}\Gamma \mid \Psi \vdash t_1 : \mathsf{list}_{\tau_1} \sim t_2 : \mathsf{list}_{\tau_2} \mid \phi' \wedge \mathbf{r}_1 = [] \Leftrightarrow \mathbf{r}_2 = [] \\ \Gamma \mid \Psi, \phi'[[]/\mathbf{r}_1][[]/\mathbf{r}_2] \vdash u_1 : \sigma_1 \sim u_2 : \sigma_2 \mid \phi \\ \Gamma \mid \Psi \vdash v_1 : \tau_1 \to \mathsf{list}_{\tau_1} \to \sigma_1 \sim v_2 : \tau_2 \to \mathsf{list}_{\tau_2} \to \sigma_2 \mid \\ \forall h_1 h_2 l_1 l_2 . \phi'[h_1 :: l_1/\mathbf{r}_1][h_2 :: l_2/\mathbf{r}_2] \Rightarrow \phi[\mathbf{r}_1\ h_1\ l_1/\mathbf{r}_1][\mathbf{r}_2\ h_2\ l_2/\mathbf{r}_2]\end{array}}{\Gamma \mid \Psi \vdash \text{case } t_1 \text{ of } [] \mapsto u_1; \_ :: \_ \mapsto v_1 : \sigma_1 \sim \text{case } t_2 \text{ of } [] \mapsto u_2; \_ :: \_ \mapsto v_2 : \sigma_2 \mid \phi} \text{ LISTCASE}*$$

Fig. 7. Alternative case rules

$$\frac{\begin{array}{c}\mathcal{D}ef(f_1, x_1, e_1) \ \ \mathcal{D}ef(f_2, x_2, e_2) \\ \Gamma, x_1 : I_1, x_2 : I_2, f_1 : I_1 \to \sigma, f_2 : I_2 \to \sigma_2 \mid \Psi, \phi', \\ \forall m_1 m_2 . (|m_1|, |m_2|) < (|x_1|, |x_2|) \Rightarrow \phi'[m_1/x_1][m_2/x_2] \Rightarrow \phi[m_1/x_1][m_2/x_2][f_1\ m_1/\mathbf{r}_1][f_2\ m_2/\mathbf{r}_2] \vdash \\ e_1 : \sigma_1 \sim e_2 : \sigma_2 \mid \phi\end{array}}{\Gamma \mid \Psi \vdash \text{letrec } f_1\ x_1\ = e_1 : I_1 \to \sigma_2 \sim \text{letrec } f_2\ x_2\ = e_2 : I_2 \to \sigma_2 \mid \forall x_1 x_2 . \phi' \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1][\mathbf{r}_2\ x_2/\mathbf{r}_2]} \text{ LETREC}$$

$$\frac{\begin{array}{c}\mathcal{D}ef(f_1, x_1, e_1) \\ \Gamma, x_1 : I_1, f_1 : I_1 \to \sigma \mid \Psi, \phi', \\ \forall m_1 . |m_1| < |x_1| \Rightarrow \phi'[m_1/x_1] \Rightarrow \phi[m_1/x_1][m_2/x_2][f_1\ m_1/\mathbf{r}_1][t_2/\mathbf{r}_2] \vdash e_1 : \sigma_1 \sim t_2 : \sigma_2 \mid \phi\end{array}}{\Gamma \mid \Psi \vdash \text{letrec } f_1\ x_1\ = e_1 : I_1 \to \sigma_2 \sim t_2 : \sigma_2 \mid \forall x_1 . \phi' \Rightarrow \phi[\mathbf{r}_1\ x_1/\mathbf{r}_1]} \text{ LETREC} - \text{L}$$

$$\text{where } I_1, I_2 \in \{\mathbb{N}, \mathsf{list}_\tau\}$$

Fig. 8. Recursion rules