Computational Higher Type Theory (CHTT)

Robert Harper

Lecture Notes of Week 5 by Farzaneh Derakhshan and Di Wang

1 Setting the Scene

Thus far in the course, we have explored *closed term computation* and *open term calculation* for the simply typed lambda calculus (STLC) augmented with inductive types, with the goal to prove that all well-typed programs terminate as well as all well-typed terms normalize. We also have studied closed term computation for polymorphism, i.e., the type-level quantification. Our exploration led us to rediscover *Tait's method* and *Girard's method*.

From now on, we are going to study *equality*. Before developing *behavioral equality* (i.e., *exact equality*) in computational type theory, we first recall traditional *structural equality* (i.e., *definitional equality*) in formal type theory.

2 Structural Equality

Recall the STLC augmented with an answer type ans and a natural number type nat:

$$\begin{array}{rcl} A & ::= & \mathsf{ans} \mid \mathsf{nat} \mid A_1 \to A_2 \\ M & ::= & \uparrow \mid \downarrow \mid x \mid \lambda x : A.M \mid M_1\ M_2 \mid \mathsf{z} \mid \mathsf{s}(M) \mid \mathsf{rec}_A\{M_z; x.M_s\}(M) \end{array}$$

The typing judgment is defined as follows:

$$\frac{}{\Gamma \vdash \uparrow : \mathsf{ans}} \qquad \frac{}{\Gamma \vdash \downarrow : \mathsf{ans}} \qquad \frac{}{\Gamma, x : A \vdash x : A}$$

$$\frac{\Gamma, x : A_1 \vdash M : A_2}{\Gamma \vdash \lambda x : A_1.M : A_1 \to A_2} \qquad \frac{\Gamma \vdash M_1 : A_1 \to A_2 \qquad \Gamma \vdash M_2 : A_1}{\Gamma \vdash M_1\ M_2 : A_2}$$

$$\frac{}{\Gamma \vdash \mathsf{z} : \mathsf{nat}} \qquad \frac{\Gamma \vdash M : \mathsf{nat}}{\Gamma \vdash \mathsf{s}(M) : \mathsf{nat}} \qquad \frac{\Gamma \vdash M : \mathsf{nat} \qquad \Gamma \vdash M_z : A \qquad \Gamma, x : A \vdash M_s : A}{\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(M) : A}$$

Structural equality for STLC, written $\Gamma \vdash M \equiv M' : A$, is the strongest congruence respecting β-principles:

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash M \equiv M : A} \qquad \frac{\Gamma \vdash M' \equiv M : A}{\Gamma \vdash M \equiv M' : A} \qquad \frac{\Gamma \vdash M \equiv M' : A \qquad \Gamma \vdash M' \equiv M'' : A}{\Gamma \vdash M \equiv M'' : A}$$

$$\frac{\Gamma, x : A_1 \vdash M \equiv M' : A_2}{\Gamma \vdash \lambda x : A_1.M \equiv \lambda x : A_1.M' : A_1 \to A_2} \qquad \frac{\Gamma \vdash M \equiv M' : A_1 \to A_2 \qquad \Gamma \vdash N \equiv N' : A_1}{\Gamma \vdash M\ N \equiv M'\ N' : A_2}$$

$$\frac{\Gamma \vdash M \equiv M' : \mathsf{nat}}{\Gamma \vdash \mathsf{s}(M) \equiv \mathsf{s}(M') : \mathsf{nat}} \qquad \frac{\Gamma, x : A_1 \vdash M : A_2 \qquad \Gamma \vdash N : A_1}{\Gamma \vdash (\lambda x : A.M)\ N \equiv [N/x]M : A_2}$$

$$\frac{\Gamma \vdash M \equiv M' : \mathsf{nat} \qquad \Gamma \vdash M_z \equiv M'_z : A \qquad \Gamma, x : A \vdash M_s \equiv M'_s : A}{\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(M) \equiv \mathsf{rec}_A\{M'_z; x.M'_s\}(M') : A}$$

$$\frac{\Gamma \vdash M_z : A \qquad \Gamma, x : A \vdash M_s : A}{\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(\mathsf{z}) \equiv M_z : A}$$

$$\frac{\Gamma \vdash M : \mathsf{nat} \qquad \Gamma \vdash M_z : A \qquad \Gamma, x : A \vdash M_s : A}{\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(\mathsf{s}(M)) \equiv [\mathsf{rec}_A\{M_z; x.M_s\}(M)/x]M_s : A}$$

Methodologically, structural equality is intended to be decidable. However, this approach never turns out to be efficient and the decidability could be very hard to prove.

3 Behavioral Equality

Under structural equality, one will not be able to prove $x : \mathsf{nat}, y : \mathsf{nat} \vdash x + y \equiv y + x : \mathsf{nat}$, where plus is defined by recursion on one of its arguments. In other words, structural equality is a very strong equality. Similar to the exploration of closed term computation, we want to develop a characterization of *behavioral equality* in terms of program behaviors.

Intuitively, we want to "binarize logical relations", written $\Gamma \gg M \doteq M' \in A$, with the following fundamental theorem:

Theorem 1 (FTLR)**.** *If $\Gamma \vdash M \equiv M' : A$, then $\Gamma \gg M \doteq M' \in A$.*

Similar to $\Gamma \gg M \in A$, $\Gamma \gg M \doteq M' \in A$ is *extensional* and *functional*. In other words, suppose we have a behavioral equality relation for closed terms $M \doteq M' \in A$ where M, M' are programs and A is a type, if $\gamma \doteq \gamma' \in \Gamma$ where γ, γ' are closed substitution mappings (i.e., for all $x \in B \in \Gamma$, $\gamma(x) \doteq \gamma'(x) \in B$), then $\widehat{\gamma}(M) \doteq \widehat{\gamma'}(M') \in A$. Now we develop the logical relation $M \doteq M' \in A$, which can be seen as a binary version of hereditary termination relation.

Definition 2. *$M \doteq M' \in A$ is defined inductively on the structure of A.*

- *$M \doteq M' \in \mathsf{ans}$ iff either $M \Downarrow \uparrow$ and $M' \Downarrow \uparrow$, or $M \Downarrow \downarrow$ and $M' \Downarrow \downarrow$.*
- *$M \doteq M' \in \mathsf{nat}$ iff either $M \Downarrow \mathsf{z}$ and $M' \Downarrow \mathsf{z}$, or $M \Downarrow \mathsf{s}(N)$, $M' \Downarrow \mathsf{s}(N')$, and $N \doteq N' \in \mathsf{nat}$ (following the horizontal induction principle).*
- *$M \doteq M' \in A_1 \to A_2$ iff $M \Downarrow \lambda x : A_1.M_1$, $M' \Downarrow \lambda x : A_1.M_1'$, and for all N, N' such that $N \doteq N' \in A_1$, $[N/x]M_1 \doteq [N'/x]M_1' \in A_2$.*

The first property we want to establish is that $M \doteq M' \in A$ is symmetric and transitive.

Lemma 3. *For any type A,*

- *$M \doteq M' \in A$ implies $M' \doteq M \in A$.*
- *$M \doteq M' \in A$ and $M' \doteq M'' \in A$ imply $M \doteq M'' \in A$.*

Proof. By induction on the structure of A:

- Case $A = \mathsf{ans}$:
  - Symmetry: By inversion we know that either $M \Downarrow \uparrow$, $M' \Downarrow \uparrow$, or $M \Downarrow \downarrow$, $M' \Downarrow \downarrow$. In either case it is straightforward to show $M' \doteq M \in \mathsf{ans}$.
  - Transitivity: By inversion on $M \doteq M' \in \mathsf{ans}$ we know that either $M \Downarrow \uparrow$, $M' \Downarrow \uparrow$, or $M \Downarrow \downarrow$, $M' \Downarrow \downarrow$. If M, M' evaluates to $\uparrow$, then by the determinism of evaluation and inversion on $M' \doteq M'' \in \mathsf{ans}$, we know that M'' also evaluates to $\uparrow$, hence by definition we know $M \doteq M'' \in \mathsf{ans}$. It is similar to prove for the case where M, M' evaluates to $\downarrow$.

- Case $A = \mathsf{nat}$:
  - Symmetry: By inversion and then a case analysis:
    - Subcase $M \Downarrow \mathsf{z}, M' \Downarrow \mathsf{z}$: By definition we know that $M' \doteq M \in \mathsf{nat}$.
    - Subcase $M \Downarrow \mathsf{s}(N), M' \Downarrow \mathsf{s}(N'), N \doteq N' \in \mathsf{nat}$: By induction hypothesis on $N \doteq N' \in \mathsf{nat}$ we know that $N' \doteq N \in \mathsf{nat}$. Thus by definition we know that $M' \doteq M \in \mathsf{nat}$.
  - Transitivity: By inversion on $M \doteq M' \in \mathsf{nat}$ and then a case analysis:
    - Subcase $M \Downarrow \mathsf{z}, M' \Downarrow \mathsf{z}$: By the determinism of evaluation and inversion on $M' \doteq M'' \in \mathsf{nat}$, we know that M'' also evaluates to z. By definition we have $M \doteq M'' \in \mathsf{nat}$.
    - Subcase $M \Downarrow \mathsf{s}(N), M' \Downarrow \mathsf{s}(N'), N \doteq N' \in \mathsf{nat}$: By the determinism of evaluation and inversion on $M' \doteq M'' \in \mathsf{nat}$, we know that M'' evaluates to $\mathsf{s}(N'')$ for some N'' and $N' \doteq N'' \in \mathsf{nat}$. Then by induction hypothesis we know that $N \doteq N'' \in \mathsf{nat}$. By definition we have $M \doteq M'' \in \mathsf{nat}$.
- Case $A = A_1 \to A_2$:
  - Symmetry: By inversion we know that $M \Downarrow \lambda x : A_1.M_1$, $M' \Downarrow \lambda x : A_1.M_1'$ and for all N, N' such that $N \doteq N' \in A_1$, $[N/x]M_1 \doteq [N'/x]M_1' \in A_2$. We are supposed to show that for all N', N such that $N' \doteq N \in A_1$, $[N'/x]M_1' \doteq [N/x]M_1 \in A_2$. By induction hypothesis, we have $N \doteq N' \in A_1$, and it suffices to show that $[N/x]M_1 \doteq [N'/x]M_1' \in A_2$. It follows directly from assumptions.
  - Transitivity: By inversion on $M \doteq M' \in A_1 \to A_2$, $M' \doteq M'' \in A_1 \to A_2$, and determinism of evaluation, we know that $M \Downarrow \lambda x : A_1.M_1$, $M' \Downarrow \lambda x : A_1.M_1'$, $M'' \Downarrow \lambda x : A_1.M_1''$, for all N, N' such that $N \doteq N' \in A_1$, $[N/x]M_1 \doteq [N'/x]M_1' \in A_2$, and for all N', N'' such that $N' \doteq N'' \in A_1$, $[N'/x]M_1' \doteq [N''/x]M_1'' \in A_2$. We are suppose to show that for all N, N'' such that $N \doteq N'' \in A_1$, $[N/x]M_1 \doteq [N''/x]M_1'' \in A_2$. By assumption, we know that $[N/x]M_1 \doteq [N''/x]M_1' \in A_2$. Then it suffices to show that $[N''/x]M_1' \doteq [N''/x]M_1'' \in A_2$. It turns out that we need to prove $N'' \doteq N'' \in A_1$. By induction hypothesis on $N \doteq N'' \in A_1$ for symmetry, we know that $N'' \doteq N \in A_1$. Then by induction hypothesis for transitivity, we have $N'' \doteq N'' \in A_1$. Thus we conclude the proof.

□

The symmetry and transitivity can also be proved for open behavioral equality.

Lemma 4. *For any typing context* Γ *and type* A*,*

- $\Gamma \gg M \doteq M' \in A$ *implies* $\Gamma \gg M' \doteq M \in A$.
- $\Gamma \gg M \doteq M' \in A$ *and* $\Gamma \gg M' \doteq M'' \in A$ *imply* $\Gamma \gg M \doteq M'' \in A$.

Proof.

- Suppose $\gamma \doteq \gamma' \in \Gamma$. It suffices to show $\widehat{\gamma}(M') \doteq \widehat{\gamma'}(M) \in A$. By symmetry we know that $\gamma' \doteq \gamma \in \Gamma$. By assumption we know that $\widehat{\gamma'}(M) \doteq \widehat{\gamma}(M') \in A$. By symmetry again we conclude that $\widehat{\gamma}(M') \doteq \widehat{\gamma'}(M) \in A$.
- Suppose $\gamma \doteq \gamma'' \in \Gamma$. It suffices to show $\widehat{\gamma}(M) \doteq \widehat{\gamma''}(M'') \in A$. By symmetry we know that $\gamma'' \doteq \gamma \in \Gamma$. By transitivity we know that $\gamma \doteq \gamma \in \Gamma$. By assumption we know that $\widehat{\gamma}(M) \doteq \widehat{\gamma}(M') \in A$. By assumption we know that $\widehat{\gamma}(M') \doteq \widehat{\gamma''}(M'') \in A$. By transitivity we conclude that $\widehat{\gamma}(M) \doteq \widehat{\gamma''}(M'') \in A$.

□

Because behavioral equality reasons about behavioral equivalence of programs, and the evaluation of the STLC is deterministic, the equality relation should also be closed under reverse execution.

Lemma 5 (Head expansion)**.** *If $M \doteq M' \in A$, $N \mapsto^* M$, and $N' \mapsto^* M'$, then $N \doteq N' \in A$.*

Proof. By induction on the structure of A:

- Case $A = \mathsf{ans}$: By inversion we know that either $M \Downarrow \uparrow$, $M' \Downarrow \uparrow$, or $M \Downarrow \downarrow$, $M' \Downarrow \downarrow$. If M, M' evaluates to $\uparrow$, then $N \mapsto^* M$ and $N' \mapsto^* M'$ imply that $N \Downarrow \uparrow$ and $N' \Downarrow \uparrow$, thus $N \doteq N' \in \mathsf{ans}$. It is similar to prove for the case where M, M' evaluates to $\downarrow$.
- Case $A = \mathsf{nat}$: By inversion and a then a case analysis:
  - Subcase $M \Downarrow \mathsf{z}, M' \Downarrow \mathsf{z}$: $N \mapsto^* M$ and $N' \mapsto^* M'$ imply that $N \Downarrow \mathsf{z}$ and $N' \Downarrow \mathsf{z}$, thus $N \doteq N' \in \mathsf{nat}$.
  - Subcase $M \Downarrow \mathsf{s}(M_1), M' \Downarrow \mathsf{s}(M_1'), M_1 \doteq M_1' \in \mathsf{nat}$: $N \mapsto^* M$ and $N' \mapsto^* M'$ imply that $N \Downarrow \mathsf{s}(M_1)$ and $N' \Downarrow \mathsf{s}(M_1')$, thus by definition we have $N \doteq N' \in \mathsf{nat}$.
- Case $A = A_1 \to A_2$: By inversion we know that $M \Downarrow \lambda x : A_1.M_1$, $M' \Downarrow \lambda x : A_1.M_1'$, and for all M_2, M_2' such that $M_2 \doteq M_2' \in A_1$, $[M_2/x]M_1 \doteq [M_2'/x]M_1' \in A_2$. $N \mapsto^* M$ and $N' \mapsto^* M'$ imply that $N \Downarrow \lambda x : A_1.M_1$ and $N' \Downarrow \lambda x : A_1.M_1'$. By definition we know that $N \doteq N' \in A_1 \to A_2$.

□

Now we turn to prove the fundamental theorem to show that structural equality suffices for behavioral equality. We start with a lemma which justifies the positive definition of behavioral equality for function types.

Lemma 6. *$M \doteq M' \in A_1 \to A_2$ and $N \doteq N' \in A_1$ imply $M\ N \doteq M'\ N' \in A_2$.*

Proof. By inversion on $M \doteq M' \in A_1 \to A_2$ we know that $M \Downarrow \lambda x : A_1.M_1$, $M' \Downarrow \lambda x : A_1.M_1'$, and for all N, N' such that $N \doteq N' \in A_1$, $[N/x]M_1 \doteq [N'/x]M_1' \in A_2$. Thus we know that $[N/x]M_1 \doteq [N'/x]M_1' \in A_2$. Observe that $M\ N \mapsto^* (\lambda x : A_1.M_1)\ N \mapsto [N/x]M_1$, and $M'\ N' \mapsto^* (\lambda x : A_1.M_1')\ N' \mapsto [N'/x]M_1'$. Thus by head expansion we conclude that $M\ N \doteq M'\ N' \in A_2$. □

We show that well-typed terms are behaviorally equal to itself for its type.

Lemma 7. *$\Gamma \vdash M : A$ implies $\Gamma \gg M \doteq M \in A$.*

Proof. We are supposed to show for all γ, γ' such that $\gamma \doteq \gamma' \in \Gamma$, $\widehat{\gamma}(M) \doteq \widehat{\gamma'}(M) \in A$. The proof proceeds by induction on the derivation of $\Gamma \vdash M : A$. We consider several nontrivial cases.

- $$\frac{\Gamma, x : A_1 \vdash M : A_2}{\Gamma \vdash \lambda x : A_1.M : A_1 \to A_2}$$
  Observe that $\widehat{\gamma}(\lambda x : A_1.M) = \lambda x : A_1.\widehat{\gamma}(M)$. By definition we are supposed to show that for all N, N' such that $N \doteq N' \in A_1$, $[N/x]\widehat{\gamma}(M) \doteq [N'/x]\widehat{\gamma'}(M) \in A_2$. Let $\gamma_x = \gamma[x \mapsto N]$ and $\gamma_x' = \gamma'[x \mapsto N']$. By assumption we know that $\gamma_x \doteq \gamma_x' \in \Gamma, x : A_1$. Thus by induction hypothesis we know that $\widehat{\gamma_x}(M) \doteq \widehat{\gamma_x'}(M) \in A_2$. Observe that $\widehat{\gamma_x}(M) = [N/x]\widehat{\gamma}(M)$ and $\widehat{\gamma_x'}(M) = [N'/x]\widehat{\gamma'}(M)$. Thus we conclude this case.

- $\dfrac{\Gamma \vdash M_1 : A_1 \to A_2 \qquad \Gamma \vdash M_2 : A_1}{\Gamma \vdash M_1\ M_2 : A_2}$

  Observe that $\widehat{\gamma}(M_1\ M_2) = \widehat{\gamma}(M_1)\ \widehat{\gamma}(M_2)$. By induction hypothesis we know that $\widehat{\gamma}(M_1) \doteq \widehat{\gamma'}(M_1) \in A_1 \to A_2$ and $\widehat{\gamma}(M_2) \doteq \widehat{\gamma'}(M_2) \in A_1$. By Lemma 6 we conclude that $\widehat{\gamma}(M_1)\ \widehat{\gamma}(M_2) \doteq \widehat{\gamma'}(M_1')\ \widehat{\gamma'}(M_2') \in A_2$.

- $\dfrac{\Gamma \vdash M : \mathsf{nat} \qquad \Gamma \vdash M_z : A \qquad \Gamma, x : A \vdash M_s : A}{\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(M) : A}$

  We are supposed to show that

  $$\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M)) \doteq \mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(\widehat{\gamma'}(M)) \in A.$$

  By induction hypothesis on $\Gamma \vdash M : \mathsf{nat}$ we know that $\widehat{\gamma}(M) \doteq \widehat{\gamma'}(M) \in \mathsf{nat}$. By horizontal induction on natural numbers:

  - Subcase $\widehat{\gamma}(M) \Downarrow \mathsf{z}, \widehat{\gamma'}(M) \Downarrow \mathsf{z}$: Observe that

    $$\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M)) \quad \mapsto^* \quad \widehat{\gamma}(M_z)$$

    $$\mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(\widehat{\gamma'}(M)) \quad \mapsto^* \quad \widehat{\gamma'}(M_z).$$

    By induction hypothesis on $\Gamma \vdash M_z : A$ we know that $\widehat{\gamma}(M_z) \doteq \widehat{\gamma'}(M_z) \in A$. Thus by head expansion we conclude this subcase.
  - Subcase $\widehat{\gamma}(M) \Downarrow \mathsf{s}(N), \widehat{\gamma'}(M) \Downarrow \mathsf{s}(N'), N \doteq N' \in \mathsf{nat}$ assuming that

    $$\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N) \doteq \mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(N') \in A :$$

    Observe that

    $$\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M)) \quad \mapsto^* \quad [\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N)/x]\widehat{\gamma}(M_s)$$

    $$\mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(\widehat{\gamma'}(M)) \quad \mapsto^* \quad [\mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(N')/x]\widehat{\gamma'}(M_s).$$

    Let

    $$\gamma_x = \gamma[x \mapsto \mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N)],\ \textit{and}$$
    $$\gamma_x' = \gamma'[x \mapsto \mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(N')].$$

    By assumption we know that $\gamma_x \doteq \gamma_x' \in \Gamma, x : A$. Thus by induction hypothesis on $\Gamma, x : A \vdash M_s : A$ we know that $\widehat{\gamma_x}(M_s) \doteq \widehat{\gamma_x'}(M_s) \in A$.
    Observe that

    $$\widehat{\gamma_x}(M_s) = [\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N)/x]\widehat{\gamma}(M_s),\ \textit{and}$$

    $$\widehat{\gamma_x'}(M_s) = [\mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(N')/x]\widehat{\gamma'}(M_s).$$

    Hence by head expansion we conclude this subcase.

□

Now we proceed to prove the fundamental theorem.

Theorem 8 (FTLR)**.** *If* $\Gamma \vdash M \equiv M' : A$*, then* $\Gamma \gg M \doteq M' \in A$*.*

Proof. The proof proceeds by induction on the derivation of $\Gamma \vdash M \equiv M' : A$. We consider several nontrivial cases.

- $\dfrac{\Gamma \vdash M : A}{\Gamma \vdash M \doteq M : A}$
  We conclude this case by Lemma 7.
- $\dfrac{\Gamma \vdash M' \equiv M : A}{\Gamma \vdash M \equiv M' : A}$
  We conclude this case by induction hypothesis and then Lemma 4.
- $\dfrac{\Gamma \vdash M \equiv M' : A \qquad \Gamma \vdash M' \equiv M'' : A}{\Gamma \vdash M \equiv M'' : A}$
  We conclude this case by induction hypothesis and then Lemma 4.
- $\dfrac{\Gamma, x : A_1 \vdash M : A_2 \qquad \Gamma \vdash N : A_1}{\Gamma \vdash (\lambda x : A_1.M)\ N \equiv [N/x]M : A_2}$
  Suppose $\gamma \doteq \gamma' \in \Gamma$. It suffices to show that $(\lambda x : A_1.\widehat{\gamma}(M))\ \widehat{\gamma}(N) \doteq [\widehat{\gamma'}(N)/x]\widehat{\gamma'}(M) \in A_2$. By Lemma 7 on $\Gamma \vdash N : A_1$ we know that $\widehat{\gamma}(N) \doteq \widehat{\gamma'}(N) \in A_1$. Let $\gamma_x = \gamma[x \mapsto \widehat{\gamma}(N)]$ and $\gamma'_x = \gamma'[x \mapsto \widehat{\gamma'}(N)]$. By assumption we know that $\gamma_x \doteq \gamma'_x \in \Gamma, x : A_1$. By Lemma 7 on $\Gamma, x : A_1 \vdash M : A_2$ we know that $\widehat{\gamma_x}(M) \doteq \widehat{\gamma'_x}(M) \in A_2$. Thus $[\widehat{\gamma}(N)/x]\widehat{\gamma}(M) \doteq [\widehat{\gamma'}(N)/x]\widehat{\gamma'}(M) \in A_2$. Observe that
  $$(\lambda x : A_1.\widehat{\gamma}(M))\ \widehat{\gamma}(N) \mapsto [\widehat{\gamma}(N)/x]\widehat{\gamma}(M).$$
  Thus by head expansion we conclude this case.
- $\dfrac{\Gamma \vdash M \equiv M' : A_1 \to A_2 \qquad \Gamma \vdash N \equiv N' : A_1}{\Gamma \vdash M\ N \equiv M'\ N' : A_2}$
  We conclude this case by induction hypothesis and then Lemma 6.
- $\dfrac{\Gamma, x : A_1 \vdash M \equiv M' : A_2}{\Gamma \vdash \lambda x : A_1.M \equiv \lambda x : A_1.M' : A_1 \to A_2}$
  Suppose $\gamma \doteq \gamma' \in \Gamma$. It suffices to show that $\lambda x : A_1.\widehat{\gamma}(M) \doteq \lambda x : A_1.\widehat{\gamma'}(M') \in A_1 \to A_2$. By definition we are supposed to show that for all N, N' such that $N \doteq N' \in A_1$, $[N/x]\widehat{\gamma}(M) \doteq [N'/x]\widehat{\gamma'}(M') \in A_2$. Let $\gamma_x = \gamma[x \mapsto N]$ and $\gamma'_x = \gamma'[x \mapsto N']$. By assumption we know that $\gamma_x \doteq \gamma'_x \in \Gamma, x : A_1$. Thus by induction hypothesis we know that $\widehat{\gamma_x}(M) \doteq \widehat{\gamma'_x}(M') \in A_2$. Observe that $\widehat{\gamma_x}(M) = [N/x]\widehat{\gamma}(M)$ and $\widehat{\gamma'_x}(M') = [N'/x]\widehat{\gamma'}(M')$. Hence we conclude this case.
- $\dfrac{\Gamma \vdash M \equiv M' : \mathsf{nat} \qquad \Gamma \vdash M_z \equiv M'_z : A \qquad \Gamma, x : A \vdash M_s \equiv M'_s : A}{\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(M) \equiv \mathsf{rec}_A\{M'_z; x.M'_s\}(M') : A}$
  Suppose $\gamma \doteq \gamma' \in \Gamma$. By induction hypothesis on $\Gamma \vdash M \equiv M' : \mathsf{nat}$ we know that $\widehat{\gamma}(M) \doteq \widehat{\gamma'}(M') \in \mathsf{nat}$. By horizontal induction on natural numbers:
  - Subcase $\widehat{\gamma}(M) \Downarrow \mathsf{z}, \widehat{\gamma'}(M') \Downarrow \mathsf{z}$: Observe that
    $$\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M)) \quad \mapsto^* \quad \widehat{\gamma}(M_z)$$
    $$\mathsf{rec}_A\{\widehat{\gamma'}(M'_z); x.\widehat{\gamma'}(M'_s)\}(\widehat{\gamma'}(M')) \quad \mapsto^* \quad \widehat{\gamma'}(M'_z).$$
    By induction hypothesis on $\Gamma \vdash M_z \equiv M'_z : A$ we know that $\widehat{\gamma}(M_z) \doteq \widehat{\gamma'}(M'_z) \in A$. Thus by head expansion we conclude this subcase.
  - Subcase $\widehat{\gamma}(M) \Downarrow \mathsf{s}(N), \widehat{\gamma'}(M') \Downarrow \mathsf{s}(N'), N \doteq N' \in \mathsf{nat}$ assuming that
    $$\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N) \doteq \mathsf{rec}_A\{\widehat{\gamma'}(M'_z); x.\widehat{\gamma'}(M'_s)\}(N') \in A :$$

Observe that

$$\begin{array}{rcl} \mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M)) & \mapsto^* & [\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N)/x]\widehat{\gamma}(M_s) \\ \mathsf{rec}_A\{\widehat{\gamma'}(M'_z); x.\widehat{\gamma'}(M'_s)\}(\widehat{\gamma'}(M')) & \mapsto^* & [\mathsf{rec}_A\{\widehat{\gamma'}(M'_z); x.\widehat{\gamma'}(M'_s)\}(N')/x]\widehat{\gamma'}(M'_s). \end{array}$$

Let

$$\gamma_x = \gamma[x \mapsto \mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N)], \text{ and}$$
$$\gamma'_x = \gamma'[x \mapsto \mathsf{rec}_A\{\widehat{\gamma'}(M'_z); x.\widehat{\gamma'}(M'_s)\}(N')].$$

By assumption we know that $\gamma_x \doteq \gamma'_x \in \Gamma, x : A$. Thus by induction hypothesis on $\Gamma, x : A \vdash M_s \equiv M'_s : A$ we know that $\widehat{\gamma_x}(M_s) \doteq \widehat{\gamma'_x}(M'_s) \in A$. Observe that $\widehat{\gamma_x}(M_s) = [\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(N)/x]\widehat{\gamma}(M_s)$ and $\widehat{\gamma'_x}(M'_s) = [\mathsf{rec}_A\{\widehat{\gamma'}(M'_z); x.\widehat{\gamma'}(M'_s)\}(N')/x]\widehat{\gamma'}(M'_s)$. Hence by head expansion we conclude this subcase.

- $$\frac{\Gamma \vdash M : \mathsf{nat} \qquad \Gamma \vdash M_z : A \qquad \Gamma, x : A \vdash M_s : A}{\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(\mathsf{s}(M)) \equiv [\mathsf{rec}_A\{M_z; x.M_s\}(M)/x]M_s : A}$$

  Suppose $\gamma \doteq \gamma' \in \Gamma$. It suffices to show that $\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\mathsf{s}(\widehat{\gamma}(M)) \doteq [\mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(\widehat{\gamma'}(M))/x]\widehat{\gamma'}(M_s) \in A$. By assumption we can derive $\Gamma \vdash \mathsf{rec}_A\{M_z; x.M_s\}(M) : A$. Thus by Lemma 7 we know that $\Gamma \gg \mathsf{rec}_A\{M_z; x.M_s\}(M) \doteq \mathsf{rec}_A\{M_z; x.M_s\}(M) \in A$.
  Hence $\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M)) \doteq \mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(\widehat{\gamma'}(M)) \in A$. Let $\gamma_x = \gamma[x \mapsto \mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M))$ and $\gamma'_x = \gamma'[x \mapsto \mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(\widehat{\gamma'}(M))$. By assumption we know that $\gamma_x \doteq \gamma'_x \in \Gamma, x : A$. By Lemma 7 on $\Gamma, x : A \vdash M_s : A$ we know that $\widehat{\gamma_x}(M_s) \doteq \widehat{\gamma'_x}(M_s) \in A$. Thus

  $$[\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M))/x]\widehat{\gamma}(M_s) \doteq [\mathsf{rec}_A\{\widehat{\gamma'}(M_z); x.\widehat{\gamma'}(M_s)\}(\widehat{\gamma'}(M))/x]\widehat{\gamma'}(M_s) \in A.$$

  Observe that

  $$\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\mathsf{s}(\widehat{\gamma}(M)) \mapsto [\mathsf{rec}_A\{\widehat{\gamma}(M_z); x.\widehat{\gamma}(M_s)\}(\widehat{\gamma}(M))/x]\widehat{\gamma}(M_s).$$

  Hence by head expansion we conclude this subcase.

□

4 Discussion

Suppose we want to prove $x : \mathsf{nat} \gg M \doteq M' \in A$ in a proof assistant such as RedPRL. In other words, we want to show that if $N \doteq N \in \mathsf{nat}$, then $[N/x]M \doteq [N'/x]M' \in A$. By horizontal induction on natural numbers, it suffices to show

1. If $N \Downarrow \mathsf{z}, N' \Downarrow \mathsf{z}$, then $[N/x]M \doteq [N'/x]M' \in A$.
2. If $N \Downarrow \mathsf{s}(P), N' \Downarrow \mathsf{s}(P'), P \doteq P' \in \mathsf{nat}$, and $[P/x]M \doteq [P'/x]M' \in A$, then $[N/x]M \doteq [N'/x]M' \in A$.

Intuitively, the second condition can be expressed using the following "judgment":

$$[P/x]M \doteq [P'/x]M' \in A \models_{P \doteq P' \in \mathsf{nat}} [\mathsf{s}(P)/x]M \doteq [\mathsf{s}(P')/x]M' \in A$$

That is, we can derive a proof of equality from a proof of equality. We can even rewrite it as follows informally:

$$P \in \mathsf{nat}, P' \in \mathsf{nat}, y : \mathsf{Eq}_{\mathsf{nat}}(P, P'), z : \mathsf{Eq}_A([P/x]M, [P'/x]M') \gg \cdots \in \mathsf{Eq}_A([\mathsf{s}(P)/x]M, [\mathsf{s}(P')/x]M')$$

$\mathsf{Eq}_A(M, M')$ can be seen as an "equality type" whose inhabitants are proofs for equality of M and M' for type A. This fact motivates the "propositions-as-types" principle, which leads to the exploration of dependent type theory.