Semantic Equality for Typed λ-Calculus[*]

Robert Harper

Summer 2022

1 Introduction

The unary logical relations developed in Harper (2022) may be extended from unary predicates to binary relations. In binary form these relations define *exact equality* at each type. Unlike axiomatic accounts (those given by rules) exact equality defines when two terms of a type are *semantically equal*. For example, the "add-to-self" and "doubling" functions on the natural numbers are exactly equal, because they have the same I/O behavior. This formulation—the standard one for equality of functions—is called *extensional equality*.

This note defines exact equality for terms of each type, and establishes some basic properties of it, in particular that it is an equivalence relation that is compatible with the term-forming operations, and that it respects—and thus contains—evaluation.

2 Exact Equality

The definition of exact equality is very similar to the definition of hereditary termination given in Harper (2022).

$$M \doteq M' \in \mathsf{ans} \text{ iff } M, M' \longmapsto^* \mathsf{yes} \text{ or } M, M' \longmapsto^* \mathsf{no}$$

$$M \doteq M' \in \mathsf{1} \text{ iff } M, M' \longmapsto^* \langle\rangle$$

$$\begin{aligned} M \doteq M' \in A_1 \times A_2 \text{ iff } & M \longmapsto^* \langle M_1\,,M_2\rangle, M' \longmapsto^* \langle M_1'\,,M_2'\rangle, \text{ and} \\ & M_1 \doteq M_1' \in A_1 \text{ and } M_2 \doteq M_2' \in A_2 \\ M \doteq M' \in A_1 \to A_2 \text{ iff } & M \longmapsto^* \lambda x.N, M' \longmapsto^* \lambda x.N', \text{ and} \\ & \text{if } M_1 \doteq M_1' \in A_1 \text{ then } [M_1/x]N \doteq [M_1'/x]N' \in A_2 \end{aligned}$$

Exercise 1. *Give the definitions of exact equality for the empty type, sum types, and the type of natural numbers.*

Exercise 2. *Prove that* $\lambda x.x + x \doteq \lambda x.2 \times x \in \mathsf{Nat} \to \mathsf{Nat}$*, for suitable definitions of the two functions in terms of iteration on the natural numbers.*

If exact equality is to be so-called, it ought to be symmetric and transitive.

[*]

Lemma 1. *1. If $M \doteq M' \in A$ then $M' \doteq M \in A$.*

2. If $M \doteq M' \in A$ and $M' \doteq M'' \in A$, then $M \doteq M'' \in A$.

Proof. By induction on A. Consider the case $A = A_1 \to A_2$.

1. Suppose that $M \doteq M' \in A$ with the goal to show that $M' \doteq M \in A$. By assumption $M \longmapsto^* \lambda x.N$ and $M' \longmapsto^* \lambda x.N'$. Assume that $M_1' \doteq M_1 \in A_1$, with the intent to show that $[M_1'/x]N' \doteq [M_1/x]N \in A_2$. A direct application of the outer assumption yields $[M_1/x]N' \doteq [M_1'/x]N \in A_2$, which is not what is required. However, exact equality at both A_1 and A_2 is symmetric. First, appealing to symmetry at A_1, from the assumption $M_1' \doteq M_1 \in A_1$ it follows that $M_1 \doteq M_1' \in A_1$, and hence by the outer assumption $[M_1/x]N \doteq [M_1'/x]N' \in A_2$. Then, applying symmetry at A_2, the desired result follows.

2. Suppose that $M \doteq M' \in A$ and $M' \doteq M'' \in A$ with the goal to show that $M \doteq M'' \in A$. By the definition of exact equality at function type, the two assumptions imply that $M \longmapsto^* \lambda x.N$, $M' \longmapsto^* \lambda x.N'$, and $M'' \longmapsto^* \lambda x.N''$. Now suppose that $M_1 \doteq M_1'' \in A_1$ with the intent to show that $[M_1/x]N \doteq [M_1''/x]N'' \in A_2$. Here again a direct application of the outer assumptions does not seem to help, obtaining

   (a) $[M_1/x]N \doteq [M_1''/x]N' \in A_2$, and

   (b) $[M_1/x]N' \doteq [M_1''/x]N'' \in A_2$.

   Note that a symmetric and transitive relation is reflexive on related elements: if $R(M, M')$ then $R(M', M)$, and so $R(M, M)$ and $R(M', M')$. By the inductive assumptions equality at type A_1 is symmetric and transitive, and so $M \doteq M \in A_1$ follows from the inner assumption. Then, by the first outer assumption, $[M/x]N \doteq [M/x]N' \in A_2$. Applying the second displayed equation above, and the transitivity of equality at A_2, the result follows.

□

Symmetric and transitive relations are called *partial equivalence relations*, or *pet's*. The remark in the proof about deriving reflexivity for related elements, called the "per trick," will be of further use below.

Exercise 3. *Check the remaining cases of symmetry and transitivity.*

The analogue of the fundamental theorem in Harper (2022) is the reflexivity of exact equality. Define $\gamma \doteq \gamma' \in \Gamma$ variable-by-variable and define $\Gamma \gg M \doteq M' \in A$ to mean if $\gamma \doteq \gamma' \in \Gamma$, then $\hat{\gamma}(M) \doteq \hat{\gamma'}(M') \in A$.

Lemma 2 (Reverse Evaluation)**.** *If $M \doteq M' \in A$ and $N \longmapsto M$, then $N \doteq M' \in A$.*

Exercise 4. *Prove Lemma 2.*

The analogous propery for the right-hand side of the equation follows from symmetry, or may be proved separately by an analogous argument.

Theorem 3 (Reflexivity)**.** *If $\Gamma \vdash M : A$, then $\Gamma \gg M \doteq M \in A$.*

Proof. By induction on typing derivations, proceeding analogously to the proof given in Harper (2022). □

Observe that the full meaning of reflexivity of open terms involves disparate substitution instances of them. This is necessitated by the definition of computability at function types.

The fundamental theorem tells us that well-typed terms are exactly equal to themselves. At first this may sound trivial, but because exact equality is a *behavioral* condition on evaluation, it requires proof, and can even fail when a type system is not properly designed. By Lemma 1 exact equality for *closed* terms is symmetric and transitive. However, this does not immediately imply that the same is true for *open* terms!

Lemma 4. *1. If $\Gamma \gg M \doteq M' \in A$, then $\Gamma \gg M' \doteq M \in A$.*

2. If $\Gamma \gg M \doteq M' \in A$ and $\Gamma \gg M' \doteq M'' \in A$, then $\Gamma \gg M \doteq M'' \in A$.

Proof. 1. Assume that $\Gamma \gg M \doteq M' \in A$, and suppose that $\gamma' \doteq \gamma \in \Gamma$, with the intent to show that $\widehat{\gamma'}(M') \doteq \hat{\gamma}(M) \in A$. Simply instantiating the assumption yields $\widehat{\gamma'}(M) \doteq \hat{\gamma}(M') \in A$, which is neither the intended result, nor its symmetric form. Instead, by the symmetry of closed exact equality, $\gamma \doteq \gamma' \in \Gamma$ holds as well, so that instantiating the assumption yields the desired result.

2. Assume the two premises, and suppose that $\gamma \doteq \gamma'' \in \Gamma$, with the intent to show $\hat{\gamma}(M) \doteq \widehat{\gamma''}(M'') \in A$. Instantiating the two premises directly yields

   (a) $\hat{\gamma}(M) \doteq \widehat{\gamma''}(M') \in A$, and

   (b) $\hat{\gamma}(M') \doteq \widehat{\gamma''}(M'') \in A$.

   These do not combine to yield the desired result. Instead, using again that the supposition governing the substitutions implies that $\gamma \doteq \gamma \in \Gamma$, we obtain $\hat{\gamma}(M) \doteq \hat{\gamma}(M') \in A$, which combines with the second equation above by transitivity to yield the desired conclusion.

□

Proving Lemma 1 at the outset makes use of, and makes available, the "per trick" in the proof of Lemma 4. Another line of argumentation in the proof of Lemma 4 leads to an interesting variation on the foregoing development that will be essential in more general settings (see Harper (2020).) In this formulation reflexivity is taken as a *presupposition* of the exact equality judgment, which is to say that when speaking of $\Gamma \gg M \doteq M' \in A$, it is *pre-supposed* that $\Gamma \gg M \doteq M \in A$ and $\Gamma \gg M' \doteq M' \in A$.[1]

Let us then revisit the proof of Lemma 4 with this in mind. In both the symmetric and transitive cases the presuppositions are instantiated with the given substitutions, yielding the horizontal lines, oriented left-to-right, as depicted in Figure 2. The (solid) diagonal lines are provided by similarly instantiating the assumptions. The desired conclusions are then indicated by the dashed lines. In each case the diagonal is the *completion* of a *zig-zag* as depicted abstractly in Figure 1. Given Lemma 1 the desired completions may be obtained using symmetry to reverse the orientation of a line and transitivity to compose lines, and hence to complete these zig-zags, finishing the proofs.

[1] Becase the fundamental theorem ensures the reflexivity of equality of well-typed terms, the pre-supposition may instead be taken to be that the equated objects are well-typed.

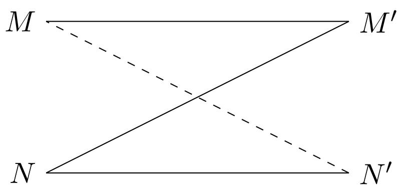

Figure 1: Zig-Zag Completeness

This suggests another perspective. A binary relation R is *zig-zag complete* iff $R \circ R^{\mathsf{op}} \circ R \subseteq R$; that is, if $R(M, M')$ and $R(N, M')$ and $R(N, N')$, then $R(M, N')$. A useful visualization is given in Figure 1 in which the premises are indicated by solid lines and the conclusion by the dashed line, bearing in mind that these lines are oriented from left to right. Noting that the only use of symmetry and transivity in the foregoing development is in the proof of Lemma 4, it is sufficient to prove that the relations are, instead, zig-zag complete, and then to appeal to this property directly to complete the (reformulated) proof of symmetry and transitivity for open terms.

Exercise 5. *Prove that closed exact equality is zig-zag complete.*

The importance of the zig-zag formulation becomes clear in Harper (2020), which is based on *heterogeneous* binary relations in which the left- and right-sides of the relation are of disparate types. For in that case symmetry of the relations does not even make type sense, and hence cannot be proved at the outset. Zig-zag completeness, on the other hand, is type-respecting, and suffices for the proof of the open, as well as closed, instances of symmetry and transitivity.

References

Robert Harper. Reynolds's parametricity theorem, directly. Unpublished lecture note, Spring 2020. URL `https://www.cs.cmu.edu/~rwh/courses/atpl/pdfs/reynolds.pdf`.

Robert Harper. How to (re)invent Tait's method. Unpublished lecture note, Spring 2022. URL `https://www.cs.cmu.edu/~rwh/courses/atpl/pdfs/tait.pdf`.

Neelakantan R Krishnaswami and Derek Dreyer. A relationally parametric model of the calculus of constructions. *Auxilliary materials at http://www. mpi-sws. org/˜ neelk/paradep-techreport. pdf*, 2012.

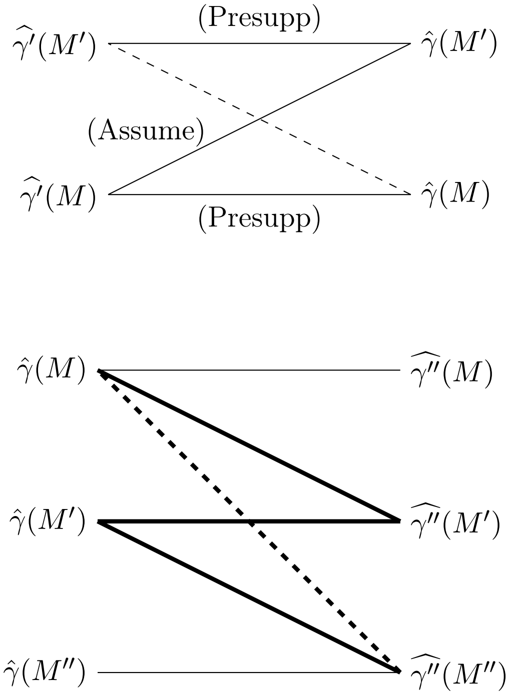

Figure 2: Symmetry and Transitivity via Zig-Zag Completeness