Kripke-Style Logical Relations for Normalization*

Robert Harper

April 12, 2021

1 Introduction

In Harper (2020) Tait's computability method is developed to prove *termination* of closed terms of the typed λ-calculus with respect to weak head reduction. The proof lays bare the skeleton of Tait's method through a graduated series of failed attempts leading to the discovery. But in doing so it also evades crucial aspects of Tait's original proof of *normalization* of the typed λ-calculus.[1] Whereas weak head reduction corresponds to the (lazy) execution of closed functional programs, normalization corresponds to simplifications of algebraic formulas with free variables, reducing, for example, $(x+1)\,(x-1)$ to x^2-1 using the laws of arithmetic.

Termination states that every well-typed λ-term may be brought into *fully evaluated* form, normalization states that every well-typed λ-term may be brought into *fully simplified* form. The unicity of the fully evaluated form is obvious, because weak head reduction is *deterministic* in that at most one head reduction applies to any given term. The unicity of the fully simplified form is far from obvious, and must be proved separately, again making use of Tait's method! The critical difference is that simplification applies to open, as well as closed, terms, and may be performed within the body of a λ-abstraction. For example the term $\lambda_A(x\,.\,\mathsf{ap}(\lambda_A(y\,.\,y), x))$ may be simplified to $\lambda_A(x\,.\,x)$ using a reduction analogous to one step of execution.

To account for free variables the normalization theorem makes use of a generalization of Tait's method, called *Kripke logical relations*. In Kripke's terminology the computability predicates are indexed not only by a type, but also by a *possible world* that determines the free variables that may occur in the terms to which the predicate applies. Possible worlds are pre-ordered by *extension*, adding fresh variables to world to obtain another. The extending world is said to be a *future world* of the extended world. Crucially, the computability predicates must be *monotone* with respect to this pre-order: if a term is computable in a world, then it remains computable in all future worlds.

Using possible worlds it is possible to prove that every substitution instance of a well-typed open term by well-typed open terms is, in a sense to be made precise, hereditarily normalizing. What is not obvious, however, is that well-typed open terms are normalizable (in contrast to hereditary termination, which immediately implies termination.) To obtain the desired result requires an additional maneuver, Tait's *pas-de-deux* relating normalized terms to a class of *hereditarily neutral* terms that include the variables of the world. From this the desired normalization property follows directly.

[1] As mentioned in Harper (2020) Tait considers a stronger property called, oddly enough, *strong normalization*, whose purpose is of no concern here.

β-$\to$

$$\frac{}{\mathsf{ap}(\lambda_A(x\,.\,M), M_2) \to_\beta [M_2/x]M}$$

β-$\times$-LFT

$$\frac{}{\langle M_1\,,\,M_2\rangle \cdot 1 \to_\beta M_1}$$

β-$\times$-RHT

$$\frac{}{\langle M_1\,,\,M_2\rangle \cdot 2 \to_\beta M_2}$$

LFT

$$\frac{M \to_\beta M'}{M \cdot 1 \to_\beta M' \cdot 1}$$

RHT

$$\frac{M \to_\beta M'}{M \cdot 2 \to_\beta M' \cdot 2}$$

APP-FUN

$$\frac{M_1 \to_\beta M_1'}{\mathsf{ap}(M_1, M_2) \to_\beta \mathsf{ap}(M_1', M_2)}$$

APP-ARG*

$$\frac{M_2 \to_\beta M_2'}{\mathsf{ap}(M_1, M_2) \to_\beta \mathsf{ap}(M_1, M_2')}$$

LAM*

$$\frac{M \to_\beta M'}{\lambda_A(x\,.\,M) \to_\beta \lambda_A(x\,.\,M')}$$

PAIR-LFT*

$$\frac{M_1 \to_\beta M_1'}{\langle M_1\,,\,M_2\rangle \to_\beta \langle M_1'\,,\,M_2\rangle}$$

PAIR-RHT*

$$\frac{M_2 \to_\beta M_2'}{\langle M_1\,,\,M_2\rangle \to_\beta \langle M_1\,,\,M_2'\rangle}$$

Figure 1: β-Reduction $M \to_\beta M'$

2 Reduction and Normalization

Let the syntax and statics of the type λ-calculus be defined as in Harper (2020). The *β-reduction* relation, $M \to_\beta M'$, on open terms M and M' is inductively defined by the rules in Figure 1. Multistep reduction, $M \to_\beta^* M'$, is the reflexive and transitive closure of β-reduction, and $M \to_\beta^+ M'$ is its transitive closure. Weak head β-reduction, $M \mapsto_\beta M'$ is defined on open terms similarly to β-reduction by omitting the "starred" rules in Figure 1.

An open term M is in *β-normal form* iff it is β-irreducible, $M \not\to_\beta$, meaning that there is no M' such that $M \to_\beta M'$. An open term M is *normalizable*, written $\mathsf{norm}_\beta(M)$, iff there exists a β-normal form, N, such that $M \to_\beta^* N$.

Theorem 1 (Normalization)**.** *If $\Gamma \vdash M : A$, then $\mathsf{norm}_\beta(M)$.*

For an incremental development of the proof, see Angiuli (2015). The main idea is to introduce a generalization of the hereditary termination condition obtained in Harper (2020) that accounts for free variables. Let Δ range over variable contexts pre-ordered by (reversed) containment: $\Delta' \leq \Delta$ iff every variable declaration in Δ is also in Δ'. The family $\mathsf{HN}_A^\Delta(M)$ of predicates indexed by contexts, Δ, as possible worlds, and types, A, on well-formed terms $\Delta \vdash M : A$, is defined in Figure 2.

Besides being applicable to open terms, the definition differs from hereditary termination in several notable ways:

1. The conditions for unit and answer types require only normalizability.
2. The conditions for product and function types are given in terms of their elimination forms, respectively projection and application. The term M cannot be expected to have canonical form; it might, for example, be a variable declared in Δ.

$$\mathsf{HN}^{\Delta}_{\mathbf{1}}(M) \text{ iff } \mathsf{norm}_{\beta}(M)$$
$$\mathsf{HN}^{\Delta}_{\mathbf{2}}(M) \text{ iff } \mathsf{norm}_{\beta}(M)$$
$$\mathsf{HN}^{\Delta}_{A_1 \times A_2}(M) \text{ iff } \mathsf{HN}^{\Delta}_{A_1}(M \cdot 1) \text{ and } \mathsf{HN}^{\Delta}_{A_2}(M \cdot 2)$$
$$\mathsf{HN}^{\Delta}_{A_1 \to A_2}(M) \text{ iff for all } \Delta' \leq \Delta, \text{ if } \mathsf{HN}^{\Delta'}_{A_1}(M_1) \text{ then } \mathsf{HN}^{\Delta'}_{A_2}(\mathsf{ap}(M, M_1))$$

$$\mathsf{HN}^{\Delta}_{\Gamma}(\gamma) \text{ iff } \mathsf{HN}^{\Delta}_{A}(\gamma(x)) \text{ for all } x : A \in \Gamma$$

Figure 2: Hereditary Normalization, $\mathsf{HN}^{\Delta}_{A}(M)$

3. Hereditary normalization at function types quantifies over all "future" worlds, which is to say all extensions of Δ. Intuitively, by weakening a term of a type in Δ is also a term of a type in Δ'. Thus, a function in Δ must be applicable in any enlarged context in which it may be used.

Lemma 2 (Anti-Monotonicity)**.** *If* $\mathsf{HN}^{\Delta}_{A}(M)$ *and* $\Delta' \leq \Delta$*, then* $\mathsf{HN}^{\Delta'}_{A}(M)$*.*

Proof. The proof proceeds by induction on the structure of A. Note that if $\Delta \vdash M : A$, and $\Delta' \leq \Delta$, then $\Delta' \vdash M : A$—typing is closed under weakening. The cases for unit and answer type are immediate; the case for product types is proved by appeal to induction on the component types. For function types, suppose that $A = A_1 \to A_2$, and that $\mathsf{HN}^{\Delta}_{A}(M)$, with the goal to show that $\mathsf{HN}^{\Delta'}_{A}(M)$. To this end suppose that $\Delta'' \leq \Delta'$ and $\mathsf{HN}^{\Delta''}_{A_1}(M_1)$. By transitivity $\Delta'' \leq \Delta$, so by assumption $\mathsf{HN}^{\Delta''}_{A_2}(\mathsf{ap}(M, M_1))$, as required. □

Lemma 3 (Head Expansion)**.** *If* $M' \mapsto_{\beta} M$ *and* $\mathsf{HN}^{\Delta}_{A}(M)$*, then* $\mathsf{HN}^{\Delta}_{A}(M')$*.*

Proof. Exercise. □

Observe that the definition of head reduction is chosen so that the preceding lemma holds; in particular, head reduction must descend through projection and (the function position) of application.

The fundamental theorem quantifies over all *open* instances of a term, and also accounts for weakening to an extended context.

Theorem 4 (Fundamental Theorem)**.** *If* $\Gamma \vdash M : A$*, then for all* Δ*, if* $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$*, then* $\mathsf{HN}^{\Delta}_{A}(\hat{\gamma}(M))$*.*

Proof. By induction on typing. For concision, write $\hat{M}$ for $\hat{\gamma}(M)$ when γ is clear from context.

VAR We have $\Gamma = \Gamma', x : A$, and $M = x$. By assumption $\mathsf{HN}^{\Delta}_{A}(\gamma(x))$, and, noting that $\hat{\gamma}(x) = \gamma(x)$ by definition, the result follows immediately.

APP Fix Δ and γ such that $\mathsf{HN}^{\Delta}_{\gamma}(\Gamma)$; we are to show $\mathsf{HN}^{\Delta}_{A_2}(\mathsf{ap}(\hat{M}, \hat{M_1}))$. By induction $\mathsf{HN}^{\Delta}_{A_1 \to A_2}(\hat{M})$ and $\mathsf{HN}^{\Delta}_{A_1}(\hat{M_1})$, using reflexivity of the ordering on worlds.

LAM Fix Δ and $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$; we are to show $\mathsf{HN}^{\Delta}_{A_1 \to A_2}(\lambda_{A_1}(x\ .\ \hat{M_2}))$. Suppose that $\Delta' \leq \Delta$, and suppose that $\mathsf{HN}^{\Delta'}_{A_1}(M_1')$. Then, by anti-monotonicity, $\mathsf{HN}^{\Delta'}_{\Gamma}(\gamma)$. Therefore, for some $x \notin \Gamma$, $\mathsf{HN}^{\Delta'}_{\Gamma, x:A_1}(\gamma[x \mapsto M_1'])$. Therefore, by induction, and by the definition of substitution, $\mathsf{HN}^{\Delta'}_{A_2}([M_1/x]\hat{M_2})$. The result follows by head expansion.

$$
\begin{aligned}
&\mathsf{NN}_{A}^{\Delta,x:A}(x)\\
&\mathsf{NN}_{A_1}^{\Delta}(U \cdot 1) \textit{ if } \mathsf{NN}_{A_1 \times A_2}^{\Delta}(U)\\
&\mathsf{NN}_{A_2}^{\Delta}(U \cdot 2) \textit{ if } \mathsf{NN}_{A_1 \times A_2}^{\Delta}(U)\\
&\mathsf{NN}_{A_2}^{\Delta}(\mathsf{ap}(U, M_1)) \textit{ if } \mathsf{NN}_{A_1 \to A_2}^{\Delta}(U) \text{ and } \mathsf{norm}_{\beta}(M_1)
\end{aligned}
$$

Figure 3: Normalizable Neutrality, $\mathsf{NN}_{A}^{\Delta}(M)$.

□

Exercise 1. *Complete the proof of Theorem 4 for the product and answer types. Extend it to account for finite sums.*

In the proof of termination given in Harper (2020) it is immediate that hereditary termination implies termination, at all types. Thus, the termination theorem, which is analogous to the fundamental theorem here, directly implies the desired termination property. Moreover, it is sensible to ask only for termination of closed terms of answer type, and, correspondingly, to give a purely "negative" formulation of hereditary termination that does not demand evaluation to a value at compound types.

In contrast normalization is, by its nature, a property of all terms, of any type, not just answer type. Because it is defined for open terms a negative formulation of hereditary normalization is required. Consequently, it is not immediate that a hereditary normalizing term is normalizing, except at answer type. The proof of normalization proceeds as follows:

1. Instantiate the fundamental theorem at the identity substitution sending each variable in Γ to itself, and conclude that $\mathsf{HN}_{A}^{\Gamma}(M)$ whenever $\Gamma \vdash M : A$. To use the identity substitution requires that the variables in a world be hereditarily normalizable at their declared type. This is immediate for atomic types, but requires proof at compound types.

2. Show that hereditary normalization implies normalization at all types. This is immediate for the atomic types, but requires proof at compound types. The proof requires that variables of any type be hereditarily normalizable.

As will become clear shortly, both properties must be proved simultaneously, proceeding by induction on the structure of types. Moreover, it is not sufficient to consider not only variables, but a larger class of *neutral* terms, U, given by the following grammar:

$$U ::= x \mid U \cdot 1 \mid U \cdot 2 \mid \mathsf{ap}(U, M).$$

Figure 3 defines the class of *normalizable neutral* terms of a type, written $\mathsf{NN}_{A}^{\Delta}(U)$, by induction on the structure of U.

Theorem 5 (Pas-de-deux)**.**

1. *If* $\mathsf{NN}_{A}^{\Delta}(U)$*, then* $\mathsf{HN}_{A}^{\Delta}(U)$*.*
2. *If* $\mathsf{HN}_{A}^{\Delta}(M)$*, then* $\mathsf{norm}_{\beta}(M)$*.*

Proof. Simultaneously, by induction on the structure of A.

1. $A = \mathbf{1}$ or $A = \mathbf{2}$:
   (a) Every normalizable neutral term of base type is self-evidently normalizable, and so hereditarily normalizable at that type.
   (b) Every hereditarily normalizable term at base type is, by definition, normalizable.
2. $A = A_1 \times A_2$:
   (a) If $\mathsf{NN}^{\Delta}_{A}(U)$, then, by definition, $\mathsf{NN}^{\Delta}_{A_1}(U \cdot 1)$ and $\mathsf{NN}^{\Delta}_{A_2}(U \cdot 2)$. By induction, $\mathsf{HN}^{\Delta}_{A_1}(U \cdot 1)$, and similarly $\mathsf{HN}^{\Delta}_{A_2}(U \cdot 2)$. But then $\mathsf{HN}^{\Delta}_{A}(U)$ by definition of hereditary normalizability.
   (b) If $\mathsf{HN}^{\Delta}_{A}(M)$, then $\mathsf{HN}^{\Delta}_{A_1}(M \cdot 1)$ and $\mathsf{HN}^{\Delta}_{A_2}(M \cdot 2)$, so by induction $\mathsf{norm}_{\beta}(M \cdot 1)$ and $\mathsf{norm}_{\beta}(M \cdot 2)$, and so $\mathsf{norm}_{\beta}(M)$, by a careful analysis of reductions from the projections.
3. $A = A_1 \to A_2$:
   (a) Suppose that $\mathsf{NN}^{\Delta}_{A}(U)$. To show $\mathsf{HN}^{\Delta}_{A}(U)$, let $\Delta' \leq \Delta$ and note that $\mathsf{NN}^{\Delta'}_{A}(U)$ as well. Suppose that $\mathsf{HN}^{\Delta'}_{A_1}(M_1)$. Then, by induction, $\mathsf{norm}_{\beta}(M_1)$, and so $\mathsf{NN}^{\Delta'}_{A_2}(\mathsf{ap}(U, M_1))$. But then, by induction, $\mathsf{HN}^{\Delta'}_{A_2}(\mathsf{ap}(U, M_1))$, as required.
   (b) Suppose $\mathsf{HN}^{\Delta}_{A}(M)$. Choosing $\Delta' = \Delta, x : A_1 \leq \Delta$, then $\mathsf{NN}^{\Delta'}_{A_1}(x)$ by definition, and so $\mathsf{HN}^{\Delta'}_{A_1}(x)$ by induction. But then $\mathsf{HN}^{\Delta'}_{A_2}(\mathsf{ap}(M, x))$ by definition, and, by induction $\mathsf{norm}_{\beta}(\mathsf{ap}(M, x))$. A careful analysis of reductions shows that $\mathsf{norm}_{\beta}(M)$.

□

Exercise 2. *Show that*

1. *If* $\mathsf{norm}_{\beta}(M \cdot 1)$ *and* $\mathsf{norm}_{\beta}(M \cdot 2)$*, then* $\mathsf{norm}_{\beta}(M)$*.*
2. *If* $\mathsf{norm}_{\beta}(\mathsf{ap}(M, x))$*, then* $\mathsf{norm}_{\beta}(M)$*.*

Exercise 3. *Prove that the identity substitution,* $\Gamma \vdash \iota : \Gamma$ *sending* x *to itself, is hereditarily normalizing, which is to say* $\mathsf{HN}^{\Gamma}_{\Gamma}(\iota)$*.*

Corollary 6 (Normalization)**.** *If* $\Gamma \vdash M : A$*, then* $\mathsf{norm}_{\beta}(M)$*.*

Proof. By the Fundamental Theorem and Exercise 3, $\mathsf{HN}^{\Gamma}_{A}(\hat{\imath}(M))$. But $\hat{\imath}(M) = M$, so, by the pas-de-deux, $\mathsf{norm}_{\beta}(M)$. □

References

Carlo Angiuli. How to prove that stlc is normalizing. Unpublished lecture note, May 2015. URL `https://www.cs.cmu.edu/~rwh/courses/chtt/pdfs/angiuli.pdf`.

Robert Harper. How to (re)invent Tait's method. Unpublished lecture note, Spring 2020. URL `https://www.cs.cmu.edu/~rwh/courses/chtt/pdfs/tait.pdf`.