Computational Higher Type Theory (CHTT)

Robert Harper

Lecture Notes of Week 2 by Stephanie Balzer and Yue Niu

1 Notation & Historical Notes

The following proof method is attributed to William Tait, who first proved normalization for the STLC. Below are some notations you might find in the literature:

1. hereditarily ...
2. logical relations (Statman)
3. Tait's Method (W. Tait)
4. Girard's Method (J-Y Girard)
5. Computability (Tait's Method)
6. Reducibility Method (Girard)

2 Fundamental Theorem Cont'd

2.0.1 Head expansion

To complete the proof from last time (that well-typed terms are hereditarily terminating under substitution by hereditarily terminating maps), we need to prove a lemma known as "head expansion" or "reverse execution":

Lemma 1 (Head expansion)**.** *If* $\mathsf{HT}_A(M')$ *and* $M \mapsto M'$ *then* $\mathsf{HT}_A(M)$*.*

Proof. Induction on A.

- $A = b$
  Suppose $\mathsf{HT}_b(M')$ and $M \mapsto M'$. We need to show $\mathsf{HT}_b(M)$. By definition, it suffices to show that $M \Downarrow$. This is clear since $M' \Downarrow$ and $M \mapsto M'$.
- $A = A_1 \to A_2$
  Suppose $\mathsf{HT}_{A_1 \to A_2}(M')$ and $M \mapsto M'$. We need to show $\mathsf{HT}_{A_1 \to A_2}(M)$. Now suppose $\mathsf{HT}_{A_1}(N)$, and we need to show $\mathsf{HT}_{A_2}(M\ N)$. By the definition of HT and our assumption, we have $\mathsf{HT}_{A_2}(M'\ N)$. Note that $M\ N \mapsto M'\ N$ by our assumption and the compuation rule. Now applying the IH, we have $\mathsf{HT}_{A_2}(M\ N)$. [1] □

2.0.2 Termination of STLC

Now we need to show that hereditary termination implies termination of terms in the STLC:

Theorem 2. *If* $\mathsf{HT}_A(M)$ *then* $M\ \mathsf{term}_\beta$*.*

Proof. Induction on A.

- $A = b$
  Suppose $\mathsf{HT}_b(M)$. Done by definition of hereditary termination.

[1] Terms in the hereditary termination predicate get bigger, but types get smaller. Since the induction is on A, we are okay.

- $A = A_1 \to A_2$
  Suppose $\mathsf{HT}_{A_1 \to A_2}(M)$. We need to show M term_β. We are stuck here; and there are a couple of options to consider.

□

1. Weaken the theorem so that we can only conclude termination for observables (terms in the base type).
2. Add M term_β to the definition of $\mathsf{HT}_A(M)$; while this comes off as a hack, everything so far will still work out.

2.1 Another Hereditary Termination (Positive Formulation)

Notice in the definition of hereditary termination above, we take a "negative" approach with respect to the function type, in that we consider everything that can happen in the elimination form for functions. Dually, we can also formulate hereditary termination "positively".

$$\mathsf{HT}^+_b(M) \triangleq M \mapsto^* c$$
$$\mathsf{HT}^+_{A \to B}(M) \triangleq M \mapsto^* \lambda x{:}A.\, M_2 \text{ and } \forall M_1.\ \mathsf{HT}^+_A(M_1) \implies \mathsf{HT}^+_{A_2}([M_1/x]M_2)$$

This is also known as the "method of canonical forms", and we can define hereditary termination in terms of "hereditary values", whose definition will depend on whether we are working "call by value" or "call by name".

2.2 C.B.V vs. C.B.N

In both C.B.V and C.B.N, a hereditary value at base type is simply a value. At the function type for C.B.N, we have

$$\mathsf{HT}^{\mathsf{cbn}}_{A_1 \to A_2}(V) \triangleq V = \lambda x{:}A.\, M_2 \text{ and } \forall M_1.\mathsf{HT}_{A_1}(M_1) \implies \mathsf{HT}_{A_2}([M_1/x]M_2)$$

For C.B.V:

$$\mathsf{HT}^{\mathsf{cbv}}_{A_1 \to A_2}(V) \triangleq V = \lambda x{:}A.\, M_2 \text{ and } \forall V_1.\mathsf{HT}^{\mathsf{cbv}}_{A_1}(V_1) \implies \mathsf{HT}_{A_2}([V_1/x]M_2)$$

TODO: fill in explanation for distinction.

2.3 Summary

We we have shown so far can be summarized as a relationship between syntax and semantics: well-typed terms terminate according to the semantics (the computation rules). We can make this more apparent by introducing some new notation:

$$\Gamma \gg A\ \mathsf{type} \tag{1}$$
$$M \in A \qquad \mathsf{HT}_A(M) \tag{2}$$
$$\Gamma \gg M \in A \qquad \gamma \in \Gamma \implies \hat{\gamma}(M) \in A \tag{3}$$
$$\tag{4}$$

Notice that the "membership" relation has a computation flavor; it is a behavorial condition on M: which says that M satisfy the specification A.

Now, we can state our theorem as follows:

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

This is in some sense a soundness theorem (in the language of formal logics), which means that the formally derivable terms are actually true (according to the computational specification). Therefore, we can think of formal systems as a way of *accessing* the *truth*. Note that we make no claims that $\Gamma \gg M \in A$ be decidable, as it is fruitless to expect the truth to be decidable in general. [2]

3 Normalization

We can also interpret variables in a different sense, where they stand for open terms - they are indeterminates. Then the judgment $\Gamma \vdash M : A$ could be interpreted as a mapping M from open terms to the type A.

Recall the beta-contraction relation, $P \ \mathrm{contr}_\beta \ P'$:

$$(\lambda x{:}A.\, M)\ N \ \mathrm{contr}_\beta \ [N/x]M$$

With this, we formulate beta-reduction:

$$\frac{M \ \mathrm{contr}_\beta \ N}{M \mapsto_\beta N} \qquad \frac{M \mapsto_\beta M'}{M\ N \mapsto_\beta M'\ N} \qquad \frac{N \mapsto_\beta N'}{M\ N \mapsto_\beta M\ N'} \qquad \frac{M \mapsto_\beta M'}{\lambda x{:}A.\, M \mapsto_\beta \lambda x{:}A.\, M'}$$

Further, we define beta-normal form, $N \ \mathrm{nf}_\beta$:

$$N \ \mathrm{nf}_\beta \triangleq N \not\mapsto_\beta$$

Where $N \not\mapsto_\beta$ means that no beta-reduction rule applies to N. This informal notation can be formalized.

Finally, we can define when a term is beta-normalizing, $M \ \mathrm{norm}_\beta$:

$$M \ \mathrm{norm}_\beta \triangleq \exists N. M \mapsto_\beta^* N \text{ and } N \ \mathrm{nf}_\beta$$

Now we can state the fundamental theorem for normalization:

Theorem 4. *If $\Gamma \vdash M : A$ then M norm$_\beta$.*

Following the proof for termination, we introduce a stronger notion for normalization, *hereditary normalization*:

$$\begin{aligned} \mathsf{HN}^\Delta_b(M) &\triangleq M \ \mathrm{norm}_\beta \\ \mathsf{HN}^\Delta_{A\to B}(M) &\triangleq \forall N.\ \mathsf{HN}^\Delta_A(N) \implies \mathsf{HN}^\Delta_B(M\ N) \end{aligned}$$

As before, we define $\mathsf{HN}^\Delta_\Gamma(\gamma)$ to be $\forall x : A \in \Gamma.\ \mathsf{HN}^\Delta_A(\gamma(x))$

Some notes about this definition:

- This predicate is defined on terms M s.t. $\Delta \vdash M : A$. The extra argument to the hereditary normalization (compared to termination) Δ reflects this fact, since normalization is defined on open terms.

- We formulate hereditary normalization in the negative way; turns out this is the only way

- What can we say about positive types (sums)?

The proof can be divided into three lemmas:

Lemma 5. *If $\Gamma \vdash M : A$ and $\mathsf{HN}^\Delta_\Gamma(\gamma)$, then $\mathsf{HN}^\Delta_A(\hat\gamma(M))$.*

Lemma 6. *If $\mathsf{HN}^\Delta_A(M)$ then M norm$_\beta$.*

Lemma 7. $\mathsf{HN}^\Gamma_\Gamma(\mathsf{id}(\Gamma))$.

[2] see dreyer's Milner lectures for further discussion.

3.1 Lemma 5

Lemma. *If* $\Gamma \vdash M : A$ *and* $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$*, then* $\mathsf{HN}^{\Delta}_{A}(\hat{\gamma}(M))$.

Proof. Induction on typing.

- $\Gamma', x : A \vdash x : A$
  Suppose $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$. We need to show $\mathsf{HN}^{\Delta}_{A}(\hat{\gamma}(x))$, which follows directly by our assumption.

- $\Gamma \vdash c : b$
  Suppose $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$. We need to show that $\mathsf{HN}^{\Delta}_{b}(c)$, which is to show that c norm_{β}. Since c nf_{β}, we have c normalizing in 0 steps.

- $$\frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\ N : B}$$
  Applying the IH, we have $\mathsf{HN}^{\Delta}_{A \to B}(\hat{\gamma}(M))$ and $\mathsf{HN}^{\Delta}_{A}(\hat{\gamma}(N))$. By definition of hereditary normalization, we have $\mathsf{HN}^{\Delta}_{B}(\hat{\gamma}(M)\ \hat{\gamma}(N))$. Since $\hat{\gamma}(M\ N) = \hat{\gamma}(M)\ \hat{\gamma}(N)$, we have $\mathsf{HN}^{\Delta}_{B}(\hat{\gamma}(M\ N))$.

- $$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x{:}A.\, M : A \to B}$$
  Suppose $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$. We need to show that $\mathsf{HN}^{\Delta}_{A \to B}(\hat{\gamma}(\lambda x{:}A.\, M))$. Thus, suppose $\mathsf{HN}^{\Delta}_{A}(N)$. It suffices to show that $\mathsf{HN}^{\Delta}_{B}(\hat{\gamma}(\lambda x{:}A.\, M)\ N)$. Notice that with N, we can extend γ to be $\gamma' = \gamma[x \mapsto N]$, and since N is hereditarily normalizing in A, it follows that $\mathsf{HN}^{\Delta}_{\Gamma, x:A}(\gamma')$. Applying the IH, we have that $\mathsf{HN}^{\Delta}_{B}(\hat{\gamma'}(M))$. Since substitution is commutative, $\hat{\gamma'}(M) = [N/x]\hat{\gamma}(M)$, and $\hat{\gamma}(\lambda x{:}A.\, M)\ N = \lambda x{:}A.\, \hat{\gamma}(M)\ N$. Further, $\lambda x{:}A.\, \hat{\gamma}(M)\ N \mapsto [N/x]\hat{\gamma}(M)$ by the computation rule. The result then follows from head expansion. □

The proof for the next 2 lemmas will be mutual induction. However, this is not enough. We will need to further strengthen Lemma 7, but let's see where we fail.

3.2 Lemma 6

Lemma. *If* $\mathsf{HN}^{\Delta}_{A}(M)$ *then* M *norm*$_{\beta}$.

Proof Attempt. Induction on A.

- $A = b$
  Immediate from definition of hereditary normalization.

- $A = A_1 \to A_2$
  Suppose $\mathsf{HN}^{\Delta}_{A}(M)$. We need to show M norm_{β}. Now we are in a bind. If we can somehow use Lemma 7 to obtain a hereditarily normalizing input of type A_1, then we can proceed with induction to obtain the result. For now, we will assume (*) that gives us a Γ' such that $x : A_1 \in \Gamma'$. By Lemma (7) we have $\mathsf{HN}^{\Gamma'}_{\Gamma'}(\mathsf{id}(\Gamma'))$, in particular, $\mathsf{HN}^{\Gamma'}_{A_1}(x)$. By the definition of hereditary normalization, we further have that $\mathsf{HN}^{\Gamma'}_{A_2}(M\ x)$. Now applying the IH, we see that $M\ x$ norm_{β}, and by Lemma **??** we have M norm_{β}.

X

Postponing the issues with this proof, we will move on to proving Lemma 7, and resolve everything after presenting the two proofs.

3.3 Lemma 7

Lemma. $\mathsf{HN}^{\Gamma}_{\Gamma}(\mathsf{id}(\Gamma))$.

Proof Attempt. Let $x : A \in \Gamma$ be arbitrary. Proceed with induction on A.

- $A = b$
  We need to show $\mathsf{HN}^{\Gamma}_{b}(x)$, which holds since x nf_{β}.

- $A = A_1 \to A_2$
  We need to show $\mathsf{HN}^{\Gamma}_{A_1 \to A_2}(x)$. Suppose $\mathsf{HN}^{\Gamma}_{A_1}(M_1)$, and it suffices to show that $\mathsf{HN}^{\Gamma}_{A_2}(x\ M_1)$. Now it would be nice to apply the IH to complete the proof, but which is not strong enough.

X

Notice that for every variable of function type, we want them to be hereditarily normalizing when applied to beta-normal terms. We will add this to the lemma:

Lemma 8. *For all k, if $x : A_1 \to \cdots \to A_k \to A \in \Gamma$ and for each $i \leq k$, $\Gamma \vdash M_i : A_i$ and M_i norm_{β}, then $\mathsf{HN}^{\Gamma}_{A}(x\ M_1\ \ldots M_k)$.*

Note that we need each argument to be *normalizing* instead of merely *hereditarily normalizing*. Before proving 9, we shall see how to fix 6. The crucial fact is the (*) that gave us a context Γ' out of thin air, which allowed us to supply the argument to the function term. To do this, we will make a change to the definition of hereditary normalization, which will involve the notion of Kripke semantics.

3.4 Kripke semantics

Kripke semantics, or presheafs, are related to/gives the solution to the following:

- allocating a "fresh variable" in a context
- why should hereditary normalization be stable under context extensions? (In other words, why should context extensions be admissible for hereditary normalization?)

If we think of the typing context as a model of the "world", then Kripke semantics suggests that we can stipulate hereditary normalization to hold in all context extensions, or "future words". Viewed logically, this would be the admissibility of weakening with respect to hereditary normalization.

Thus for our definition, we change the higher order terms to expect "world extensions":

$$\mathsf{HN}^{\Delta}_{A_1 \to A_2}(M) \triangleq \text{ if } \Delta' \geq \Delta \text{ and } \mathsf{HN}^{\Delta'}_{A_1}(M_1) \text{ then } \mathsf{HN}^{\Delta'}_{A_2}(M\ M_1)$$

Note that $\geq$ is a pre-order on contexts Δ, and is reflexive and transitive. Now we can fix both lemmas.

3.5 Fix Lemmas

Lemma. *If $\mathsf{HN}^{\Delta}_{A}(M)$ then M norm_{β}.*

Proof. Induction on A.

- $A = b$
  Immediate from definition of hereditary normalization.

- $A = A_1 \to A_2$
  Suppose $\mathsf{HN}^{\Delta}_{A}(M)$. We need to show M norm_{β}. Let $\Delta' = \Delta, x : A_1$. By IH on Lemma 9 (with $k = 0$), we have $\mathsf{HN}^{\Delta'}_{A_1}(x)$. By the definition of hereditary termination, we have $\mathsf{HN}^{\Delta'}_{A_2}(M\ x)$. Applying the IH, we have $M\ x$ norm_{β}, and by Lemma **??** we have M norm_{β}. □

Lemma 9. *For all k, if $x : A_1 \to \cdots \to A_k \to A \in \Gamma$ and for each $i \leq k$, $\Gamma \vdash M_i : A_i$ and M_i norm_{β}, then $\mathsf{HN}^{\Gamma}_{A}(x\ M_1\ \ldots M_k)$.*

Proof. Proceed with induction on A.

- $A = b$
  We need to show $x\ M_1\ \ldots M_k$ norm_β, which holds since each M_i normalizing, and thus the term does not beta-reduce.

- $A = A_i \to A_j$
  We need to show $\mathsf{HN}^\Gamma_A(x\ M_1\ \ldots M_k)$. Let $\Gamma' \geq \Gamma$ and $\mathsf{HN}^{\Gamma'}_{A_i}(M_i)$. It suffices to show that $\mathsf{HN}^{\Gamma'}_{A_j}(x\ M_1\ \ldots M_k\ M_i)$. By IH on Lemma 6, we have that M_i norm_β, and we obtain the result by applying the IH with $k+1$.

□

4 Strong Normalization