Computational Higher Type Theory (CHTT)

Robert Harper

Lecture Notes of Week 3 by Michael Coblenz and Ryan Kavanagh

1 Setting the Scene

Last week, we discovered the need for Kripke logical relations, which are related to the notion of pre-sheaves from category theory. The problem, we discovered, is that we need to allocate fresh variables, but when we add them to the context, we have to worry about whether all the things we proved in the previous context still hold with the addition a new variable. We will establish an ordering on worlds Δ and show that properties that hold one world hold in future worlds too.

When we write $\mathsf{HN}_A^\Delta(M)$:

- Δ is the "world" of indeterminates, that is, variables and their types;
- A is the type at which to consider M.

We define hereditary normalization as follows:

$$\mathsf{HN}_b^\Delta(M) \triangleq M \text{ norm}_\beta$$
$$\mathsf{HN}_{A_1 \to A_2}^\Delta(M) \triangleq \forall \Delta' \geq \Delta. \text{ if } \mathsf{HN}_{A_1}^{\Delta'}(M_1) \text{ then } \mathsf{HN}_{A_2}^{\Delta'}(M M_1)$$

That is, a function is hereditarily normalizing if, when applied to a hereditarily normalizing argument, the application is hereditarily normalizing.

Review from last time:

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

Lemma 2 (Workhorse)**.**

1. *If* $\mathsf{HN}_A^\Delta(M)$ *then* M *norm*$_\beta$.
2. *If* $\mathcal{E}$ *norm*$_\beta$ *then* $\mathsf{HN}_A^\Delta(\mathcal{E}\{x\})$ *where* $\Delta \vdash x : C$ *and* $\Delta \vdash \mathcal{E} : C \rightsquigarrow A$.

Theorem 3 (Fundamental theorem of logical relations (FTLR))**.** *If* $\Gamma \vdash M : A$ *and* $\gamma : \Delta \to \Gamma$*, then* $\mathsf{HN}_\Delta^\Gamma(\gamma)$ *implies* $\mathsf{HN}_A^\Delta(\hat{\gamma}(M))$.

Corollary 4. *If* $\Gamma \vdash M : A$ *then* M *norm*$_\beta$*. i.e. well-typed terms are normalizing.*

It is important to note that these considerations are *behavioral*, that is, they pertain to the behavior of terms. This is much deeper than structural considerations. However, the important thing about the setup here is that the structure of a term results in specific behavior. The point is that we can know that a term normalizes (a behavioral question) by knowing only that it has a type (a structural question).

In order to prove theorem 3, we need to show: if $\Delta \vdash x : A$, then $\mathsf{HN}_A^\Delta(x)$.

Informally, we need to show that xM is hereditarily normalizing whenever M is hereditarily normalizing. We also need to show that $\mathsf{HN}_{A_1 \to A_2}^\Delta(M)$ implies M norm$_\beta$ (Lemma 9 from last week). These two proofs rely on each other via mutual induction.

The problem is that in the function case, we need an argument for M, which we don't have, because in our negative formulation we can only reason about M by applying it something. The question is, what do we apply it to? Our idea is to allocate a fresh variable. We have to do so at type smaller than $A_1 \to A_2$ so that the induction hypothesis will hold, and conveniently, A_1, the argument type of M, is such a type. Consider Mx, which is of type A_2, and note that the induction hypothesis applies! Then we can conclude that Mx norm_β, so therefore M norm_β by head expansion.

In order to allocate a variable, we need to move from Δ (which does not include the fresh variable) to $\Delta' = \Delta, x : A_1$ (which does). But now we have a problem, *stability*: Do facts from the old world Δ still hold in the new world Δ'? What we need is to know that for a given proposition P, $\mathsf{HN}_A^\Delta(P)$ implies $\mathsf{HN}_A^{\Delta'}(P)$ for all $\Delta' \geq \Delta$

These worlds are ordered by a relation $\geq$. We also need $\geq$ to be transitive so that once a fact is established in a given world, it is also established in *all* future worlds. Furthermore, if $\Delta' \geq \Delta$, then $\mathsf{HN}_A^\Delta(M)$ implies $\mathsf{HN}_A^{\Delta'}(M)$; this property is called "functoriality" or "monotonicity". In our context, this is going to mean that we can allocate a fresh variable without altering the behavior of a given program.

Exercise 5 (Adding products)**.** Add "negative" products to the language and prove termination and normalization. The products look like this:

$\langle M_1, M_2 \rangle$	value
$M \cdot 1$, $M \cdot 2$	projections
$\langle M_1, M_2 \rangle.1 \mapsto M_1$	
$\langle M_1, M_2 \rangle.1 \mapsto M_1$	
$\langle M_1, M_2 \rangle.2 \mapsto M_2$	

Define:

1. $\mathsf{HT}_{A_1 \times A_2}(M)$, and reprove termination.
2. $\mathsf{HN}^\Delta_{A_1 \times A_2}(M)$, and reprove termination.

Consider this for negative and positive types. The negative formulation takes the approach that if one projects from it, it is well-behaved; that is, one uses a negative pair by projecting from it. The positive formulation would be defined in terms of pattern matching:

- let $\langle\rangle$ be M in N
- let $\langle x, y \rangle$ be M in $N_{x,y}$

2 Booleans

This brings us to showing hereditary termination and hereditary normalization for the booleans. We can think of booleans as the prime example of positive types.

- true, false are the values, otherwise known as the introduction or canonical forms.
- $\mathrm{if}(M; P; Q)$ is the elimination form.
- We extend the evaluation contexts: $\mathcal{E} ::= \ldots \mid \mathrm{if}(\mathcal{E}; P; Q)$
- Dynamic semantics:
  - $\mathrm{if}(\mathsf{true}; P; Q) \mapsto P$
  - $\mathrm{if}(\mathsf{false}; P; Q) \mapsto Q$

$$\frac{}{\Gamma \vdash \mathsf{true} : \text{bool}} \qquad\qquad \frac{}{\Gamma \vdash \mathsf{false} : \text{bool}}$$

$$\frac{\Gamma \vdash M : \text{bool} \qquad \Gamma \vdash P : A \qquad \Gamma \vdash Q : A}{\Gamma \vdash \text{if}_A(M; P; Q) : A}$$

The subscript A in if is a bit of syntax for the formalism, but upon type erasure, it would go away.

Note that if is a *recursor*: it witnesses the fact that bool is inductively defined by true and false. Importantly, if has nothing to do with logical implication! It merely witnesses that these are the two booleans. Perhaps a better name for if would have been boolcase because it is the thing that case-analyzes on the two booleans, but that is not the case for historical reasons.

2.1 Termination for closed interpretations

In this section, we prove termination for closed interpretations in the presence of booleans. The key idea here is our definition of hereditary termination:

$$\mathsf{HT}_{\text{bool}}(M) \triangleq \; M \mapsto^* \mathsf{true} \text{ or } M \mapsto^* \mathsf{false}$$

This is a *positive* interpretation because if is itself positive. We have not formulated if in a style of “if you were to do something with an if, this is how it would behave…”.

By our updated definition of hereditary termination, if $\mathsf{HT}_{\text{bool}}(M)$ then M term_β (since bool is a base type). Head expansion is also straightforward because of the way we defined the dynamic semantics; one can always back evaluation up a step.

The proof of the fundamental theorem of linear relations needs to be updated for bool, but this is easy. We need to show that if $\Gamma \vdash M : A$ and $\mathsf{HT}_\Gamma(\gamma)$ then $\mathsf{HT}_A(\hat{\gamma}(M))$. Specifically:

$$\text{if } \Gamma \vdash M : \text{bool and } \mathsf{HT}_\Gamma(\gamma) \text{ then } \mathsf{HT}_{\text{bool}}(\hat{\gamma}(M)).$$

By case analysis on the typing judgement, we see that either $M = \mathsf{true}$ or $M = \mathsf{false}$. In either case, M contains no variables, so $\hat{\gamma}(M)) = M$. By definition of the dynamic semantics, M is a value.

A corollary: if $M : A$ then M term_β.

Exercise 6. *Show hereditary termination for positive products.*

$$\mathsf{HT}_1(M) \triangleq M \mapsto^* \langle\rangle$$
$$\mathsf{HT}_{A_1 \times A_1}(M) \triangleq M \mapsto^* \langle M_1, M_2\rangle \textit{ such that } \mathsf{HT}_{A_1}(M_1) \textit{and } \mathsf{HT}_{A_2}(M_2)$$

As an aside, is it possible to give a *negative* formulation of bool? It would look like this:

$\mathsf{HT}_{\text{bool}}(M) \triangleq$ if

1. A type
2. $\mathsf{HT}_A(P)$
3. $\mathsf{HT}_A(Q)$

But now we would be in trouble in the proof: A is not smaller than bool, so the proof doesn't go through!

Now, observe regarding the negative formulation of booleans:

$$\text{bool} = \forall A. A \to A \to A$$

These are also called Church booleans! This is exactly how one encodes the booleans in lambda calculus. Presumably Church observed this correspondence directly when inventing this representation of the booleans.

2.2 Open terms

We need to show normalization for open terms in the presence of booleans. The fundamental theorem of logical relations says:

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

Now we need to define $\mathsf{HN}^{\text{bool}}_{\Delta}(M)$ so that we are able to prove the above. How should we do it?

A first attempt:

$$\mathsf{HN}^{\Delta}_{\text{bool}}(M) \triangleq M \mapsto^{*} \mathsf{true} \text{ or } M \mapsto^{*} \mathsf{false}$$

But this makes no sense because M is open. M may well be (for example) x, or xN, or even $\text{if}(xN; P; Q)$.

This shows a constraint regarding our definition. We must validate:

Lemma 7 (HN for booleans)**.**

1. *$\mathsf{HN}^{\Delta}_{bool}(\mathsf{true})$ and $\mathsf{HN}^{\Delta}_{bool}(\mathsf{false})$*
2. *If $\mathsf{HN}^{\Delta}_{bool}(\hat{M})$ and $\mathsf{HN}^{\Delta}_{A}(\hat{P})$ and $\mathsf{HN}^{\Delta}_{A}(\hat{Q})$, then $\mathsf{HN}^{\Delta}_{A}(\text{if}(\hat{M}; \hat{P}; \hat{Q}))$.*

If we choose a definition of hereditary termination that meets these criteria, we will be done. But what definition should that be? Let us discover it.

By the hypothesis to Lemma 7.2 and the workhorse lemma, we know that $\hat{M}$ norm$_\beta$. The key fact is that for any M such that M norm$_\beta$, you have that $M \mapsto^{*} N$ for some N that is head irreducible, that is, some N that is in head normal form. In our proof of the work-horse lemma, we will want proceed by case analysis on the head normal form of $\hat{M}$, and so it is sufficient for us to require that $\mathsf{HN}^{\Delta}_{\mathsf{bool}}(M)$ if and only if M norm$_\beta$.

By workhorse lemma, we conclude $\hat{P}$ norm$_\beta$ and $\hat{Q}$ norm$_\beta$ (since we assumed that $\mathsf{HN}^{\Delta}_{A}(\hat{P})$ and $\mathsf{HN}^{\Delta}_{A}(\hat{Q})$. As a reminder, the workhorse lemma is:

Lemma (Workhorse lemma, duplicated for reference)**.**

1. *If $\mathsf{HN}^{\Delta}_{A}(M)$ then M norm$_\beta$.*
2. *If $\mathcal{E}$ norm$_\beta$ then $\mathsf{HN}^{\Delta}_{A}(\mathcal{E}\{x\})$ where $\Delta \vdash x : C$ and $\Delta \vdash \mathcal{E} : C \rightsquigarrow A$.*

Proof. We consider the cases for N. It will be easy to satisfy part 1 of theorem 7, but we must choose carefully so that we can show part 2: $\mathsf{HN}^{\Delta}_{A}(\text{if}(\hat{M}; \hat{P}; \hat{Q}))$.

case: $N = \mathsf{true}$. We will need to choose $\mathsf{HN}^{\Delta}_{A}(\cdot)$ so that we can show $\mathsf{HN}^{\Delta}_{A}(\text{if}(\hat{M}; \hat{P}; \hat{Q}))$. Since $\hat{M} \mapsto^{*} \mathsf{true}$, we know that the whole if expression reduces to $\hat{P}$, where $\mathsf{HN}^{\Delta}_{A}(\hat{P})$ (by assumption). Therefore, we have $\mathsf{HN}^{\Delta}_{A}(\text{if}(\hat{M}; \hat{P}; \hat{Q}))$ by head expansion.

case: $N = \mathsf{false}$. This case is similar to the case for $N = \mathsf{true}$ but with $\hat{Q}$ instead of $\hat{P}$.

case: otherwise: what do we know about N? N does not reduce, yet $N \neq \mathsf{true}$ and $N \neq \mathsf{false}$. How can this be, given that $\Delta \vdash N : \mathrm{bool}$? One possibility is that $N = x$. This is possible if $\Delta \vdash x : \mathrm{bool}$. Another case is $N = xR$; this is possible if $\Delta \vdash x : A \to \mathrm{bool}$ and $\Delta \vdash R : A$. In general, N can be any evaluation context that starts with a variable (otherwise it would have been head-reducible)! So $N = \mathcal{E}\{x\}$. **We will need to require that $\mathcal{E}$ norm$_\beta$.**

By part 2 of the workhorse lemma, since $\mathcal{E}$ norm$_\beta$, we conclude:

$$\mathsf{HN}_A^\Delta(\mathcal{E}\{x\})$$

What we are really interested in is showing:

$$\mathsf{HN}_A^\Delta(\mathrm{if}(\mathcal{E}\{x\}; \hat{P}; \hat{Q}))$$

But $\mathrm{if}(\mathcal{E}\{x\}; \hat{P}; \hat{Q}) \mapsto \mathcal{E}\{x\}$, so we have the result we need by applying the head expansion lemma.

We conclude that the following definition of hereditary normalization is the right one:

$$\mathsf{HN}_{\mathrm{bool}}^\Delta(M) \triangleq M \ \mathrm{norm}_\beta \ . \qquad \square$$

3 Adding Sum Types

Having wet our feet with booleans, we extend our development to handle more interesting sum types. We begin by extending our grammar of types to include the nullary sum—void—and binary sums:

$$A, B ::= \cdots \mid \mathsf{void} \mid A + B.$$

In the formal setting, these come with a collection of typing rules. The introduction rules are:

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash 1 \cdot M : A + B} \ (\textsc{Sum-L-I}) \qquad \frac{\Gamma \vdash M : B}{\Gamma \vdash 2 \cdot M : A + B} \ (\textsc{Sum-R-I})$$

Note that there is no introduction rule for void. The elimination rules are:

$$\frac{\Gamma \vdash M : \mathsf{void}}{\Gamma \vdash \mathsf{case}_A\, M\,\{\,\} : A} \ (\mathsf{void}\text{-E})$$

and

$$\frac{\Gamma \vdash M : A + B \quad \Gamma, x : A \vdash P : C \quad \Gamma, x : B \vdash Q : C}{\Gamma \vdash \mathsf{case}_C\, M\,\{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\} : C} \ (\textsc{Sum-E})$$

Strictly speaking, $1 \cdot M$ should be thought of as short hand for something like $\mathsf{in}[1]\{A, B\}(M)$, but we will dispense with such pedantry. We equip the corresponding terms with the following dynamics:

$$\frac{M \mapsto M'}{\mathsf{case}_C\, M\,\{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\} \mapsto \mathsf{case}_C\, M'\,\{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\}} \ (\textsc{Case-S})$$

$$\frac{}{\mathsf{case}_C\, 1 \cdot M\,\{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\} \mapsto [M/x]P} \ (\textsc{Case-L})$$

$$\frac{}{\mathsf{case}_C\, 2 \cdot M\,\{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\} \mapsto [M/x]Q} \ (\textsc{Case-R})$$

3.1 In a closed setting

The closed setting is again relatively straightforward. We define the corresponding hereditary termination predicates:

$$\begin{aligned}\mathsf{HT}_{\mathsf{void}}(M) &\triangleq \text{(never)},\\ \mathsf{HT}_{A+B}(M) &\triangleq \begin{cases}\text{either } M \mapsto^* 1\cdot N \text{ and } \mathsf{HT}_A(N),\\ \quad\text{or } M \mapsto^* 2\cdot N \text{ and } \mathsf{HT}_B(N).\end{cases}\end{aligned}$$

In particular, for any choice of M, $\mathsf{HT}_{void}(M)$ is a contradiction. We remark that this is a *positive* formulation. Suppose we were to attempt a negative formulation, perhaps something along the lines of:

$$\mathsf{HT}_{A+B}(M) \text{ if and only if, if } \begin{cases}\text{1. for all } N, \text{ if } \mathsf{HT}_A(N), \text{ then } \mathsf{HT}_C([N/x]P), \text{ and}\\ \text{2. for all } N, \text{ if } \mathsf{HT}_B(N), \text{ then } \mathsf{HT}_C([N/x]Q),\end{cases}$$
$$\text{then } \mathsf{HT}_C(\mathsf{case}_C\, M\,\{1\cdot x \hookrightarrow P \mid 2\cdot x \hookrightarrow Q\}).$$

The inductive character of our enterprise would then break down, and we would face the same problems as with a negative formulation of bool. We could, however, read off a Church encoding for sums:

$$\forall C.(A \to C) \to (B \to C) \to C.$$

We expand the proof of the head-expansion lemma (see theorem 2) to account for these new clauses:

Lemma 8 (Head expansion with sums)**.** *If* $\mathsf{HT}_T(M')$ *and* $M \mapsto M'$*, then* $\mathsf{HT}_T(M)$*.*

Proof. The proof was by induction on the type. We consider the following new cases for T:

- void. It is never the case that $\mathsf{HT}_{\mathsf{void}}(M')$, and so the result follows *ex falso.*
- $A+B$. Our positive formulation of $\mathsf{HT}_{A+B}(M')$ tells us that, without loss of generality, $M \mapsto^* 1\cdot N'$ for some N' such that $\mathsf{HT}_A(N')$. Because the reduction relation $\mapsto$ is deterministic, it follows that $M \mapsto^* 1\cdot N'$. From this, we conclude $\mathsf{HT}_{A+B}(M)$. □

We now prove the additional cases for the FTLR:

Theorem 9 (FTLR with sums)**.** *If* $\Gamma \vdash M : A$ *and the closing substitution* $\gamma : \cdot \to \Gamma$ *is such that* $\mathsf{HT}_\Gamma(\gamma)$*, then* $\mathsf{HT}_A(\hat{\gamma}(M))$*.*

Proof. The proof was by induction on the typing judgment. We consider the following new typing cases, remarking that there were no introduction rules for void.

- (Sum-L-I). By the induction hypothesis, we know that $\mathsf{HT}_A(\hat{\gamma}(M))$. We must show that $\mathsf{HT}_{A+B}(\hat{\gamma}(1\cdot M))$. But this is immediate from the fact that $\hat{\gamma}(1\cdot M) = 1\cdot\hat{\gamma}(M)$ and the fact that $1\cdot\hat{\gamma}(M) \mapsto^* 1\cdot\hat{\gamma}(M)$.
- (Sum-R-I). Follows by a symmetric argument to the previous case.
- (void-E). By the induction hypothesis, we know that $\mathsf{HT}_{\mathsf{void}}(\hat{\gamma}(M))$. But this is a contradiction, and so we are done.
- (Sum-E). We want to show that $\mathsf{HT}_C(\hat{\gamma}(\mathsf{case}_C\, M\,\{1\cdot x \hookrightarrow P \mid 2\cdot x \hookrightarrow Q\}))$, where $\hat{\gamma}(\mathsf{case}_C\, M\,\{1\cdot x \hookrightarrow P \mid 2\cdot x \hookrightarrow Q\}) = \mathsf{case}_C\, \hat{\gamma}(M)\,\{1\cdot x \hookrightarrow \hat{\gamma}(P) \mid 2\cdot x \hookrightarrow \hat{\gamma}(Q)\}$. By the induction hypothesis, we know the following:

– for any $\gamma : \cdot \to \Gamma$ satisfying $\mathsf{HT}_\Gamma(\gamma)$, that $\mathsf{HT}_{A+B}(\hat\gamma(M))$,
– for any $\gamma_A : \cdot \to \Gamma, x : A$ satisfying $\mathsf{HT}_{\Gamma,x:A}(\gamma_A)$, that $\mathsf{HT}_C(\hat\gamma_A(P))$, and
– for any $\gamma_B : \cdot \to \Gamma, x : B$ satisfying $\mathsf{HT}_{\Gamma,x:B}(\gamma_B)$, that $\mathsf{HT}_C(\hat\gamma_B(Q))$.

From $\mathsf{HT}_{A+B}(\hat\gamma(M))$, without loss of generality, we know that $\hat\gamma(M) \mapsto^* 1{\cdot}N$ for some N such that $\mathsf{HT}_A(N)$. Let $\gamma_A = \gamma[x \mapsto N]$. It follows that $\mathsf{HT}_{\Gamma,x:A}(\gamma_A)$, so $\mathsf{HT}_C(\hat\gamma_A(P))$. But $\hat\gamma_A(P) = [N/x]\hat\gamma(P)$ and $\hat\gamma(\mathsf{case}_C\, M\,\{1\cdot x \hookrightarrow P \mid 2\cdot x \hookrightarrow Q\}) \mapsto^* [N/x]\hat\gamma(P)$, so the result follows by head expansion (theorem 8). □

3.2 In an open setting

In the open setting, things are a bit trickier. We begin by extending the grammar of evaluation contexts and the associated judgments to cope with sums. First, we introduce the new evaluation context forms:

$$\mathcal{E} \triangleq \cdots \mid \mathsf{case}_C\, \mathcal{E}\,\{\,\} \mid \mathsf{case}_C\, \mathcal{E}\,\{1\cdot x \hookrightarrow P \mid 2\cdot x \hookrightarrow Q\}.$$

Next, we introduce the typing rules for the new evaluation contexts:

$$\frac{\mathcal{E} : (\Gamma \rhd D) \rightsquigarrow (\Gamma' \rhd \mathsf{void})}{\mathsf{case}_C\, \mathcal{E}\,\{\,\} : (\Gamma \rhd D) \rightsquigarrow (\Gamma' \rhd C)}\ (\mathcal{E}\text{-}\mathsf{void})$$

$$\frac{\mathcal{E} : (\Gamma \rhd D) \rightsquigarrow (\Gamma' \rhd A+B) \quad \Gamma', x : A \vdash P : C \quad \Gamma', x : B \vdash Q : C}{\mathsf{case}_C\, \mathcal{E}\,\{1\cdot x \hookrightarrow P \mid 2\cdot x \hookrightarrow Q\} : (\Gamma \rhd D) \rightsquigarrow (\Gamma' \rhd C)}\ (\mathcal{E}\text{-}\textsc{Sum})$$

Finally, we add a rule to specify when such contexts are normalizing:

$$\frac{\mathcal{E}\ \mathrm{norm}_\beta}{\mathsf{case}_C\, \mathcal{E}\,\{\,\}\ \mathrm{norm}_\beta}\ (\mathcal{E}\text{-}\mathsf{void}\text{-}\textsc{Norm})$$

$$\frac{\mathcal{E}\ \mathrm{norm}_\beta \quad P\ \mathrm{norm}_\beta \quad Q\ \mathrm{norm}_\beta}{\mathsf{case}_C\, \mathcal{E}\,\{1\cdot x \hookrightarrow P \mid 2\cdot x \hookrightarrow Q\}\ \mathrm{norm}_\beta}\ (\mathcal{E}\text{-}\textsc{Sum-Norm})$$

We must now turn our attention to what the definition of hereditary normalization for sums ought to be. Consider the rule (Sum-E) and the induction hypothesis it would give us when proving the FTLR:

1. $\mathsf{HN}^\Gamma_{A+B}(M)$, and
2. if $\mathsf{HN}^\Gamma_A(N)$, then $\mathsf{HN}^\Gamma_C([N/x]P)$, and
3. if $\mathsf{HN}^\Gamma_B(N)$, then $\mathsf{HN}^\Gamma_C([N/x]Q)$.

Further considering how the proof might go, we see that we would proceed by case analysis on the reduction $\hat\gamma(M) \mapsto^* N\ \mathrm{nf}_\beta$: either N is an injection, or it is in head normal form, that is, of the form $\mathcal{E}\{z\}$ for some variable z. We are then lead to the following definition:

$$\mathsf{HN}^\Gamma_{\mathsf{void}}(M) \triangleq M\ \mathrm{norm}_\beta,$$

$$\mathsf{HN}^\Gamma_{A+B}(M) \triangleq \begin{cases} 1.\ M\ \mathrm{norm}_\beta, \text{ and} \\ 2.\ \text{if } M \mapsto^* 1\cdot N, \text{ then } \mathsf{HN}^\Gamma_A(N), \text{ and} \\ 3.\ \text{if } M \mapsto^* 2\cdot N, \text{ then } \mathsf{HN}^\Gamma_B(N). \end{cases}$$

(Before proceeding, think about where the proof(s) will break down if, instead of requiring M norm$_\beta$, we had a definition analogous to $\mathsf{HT}_{\mathsf{void}}(M)$ and said that $\mathsf{HN}^\Gamma_{\mathsf{void}}(M)$ never held.)

We again begin by completing the proof of the head expansion lemma to deal with sums.

Lemma 10 (Head expansion with sums)**.** *If $\mathsf{HN}^\Gamma_T(M')$ and $M \mapsto M'$, then $\mathsf{HN}^\Gamma_T(M)$.*

Proof. The proof is by induction on the structure of T. We add the missing cases:

- void. By $\mathsf{HN}^\Gamma_{\mathsf{void}}(M')$, we have M' norm_β. Because $M \mapsto M'$, it then follows that M norm_β, and so we conclude $\mathsf{HN}^\Gamma_{\mathsf{void}}(M)$.
- $A + B$. By $\mathsf{HN}^\Gamma_{A+B}(M')$, we have M' norm_β. Because $M \mapsto M'$, it then follows that M norm_β. Assume, without loss of generality, that $M \mapsto^* 1 \cdot N$. Then because the $\mapsto$ relation is deterministic, it must be because $M \mapsto M' \mapsto^* 1 \cdot N$. By the hypothesis that $\mathsf{HN}^\Gamma_{A+B}(M')$, we know that $\mathsf{HN}^\Gamma_A(N)$. From this, we are justified in concluding that $\mathsf{HN}^\Gamma_{A+B}(M)$. □

We turn our attention to expanding the proof of the work-horse lemma (theorems 8 and 13).

Lemma 11 (Work-horse lemma)**.**

1. *If $\mathcal{E} : (\Gamma \rhd C) \rightsquigarrow (\Gamma \rhd D)$ is an evaluation context such that $\mathcal{E}$ norm_β and $\Gamma \vdash x : C$, then $\mathsf{HN}^\Gamma_D(\mathcal{E}\{x\})$.*
2. *If $\mathsf{HN}^\Gamma_A(M)$, then M norm_β.*

Proof. The proof is by induction on A. We add the missing cases:

- void. We show the two parts in turn.
  1. An induction on $\mathcal{E}$ gives us that $\mathcal{E}\{x\}$ norm_β, from which we conclude the result.
  2. Immediate by definition of $\mathsf{HN}^\Gamma_{\mathsf{void}}(M)$.
- $A + B$. We show the two parts in turn.
  1. We proceed by induction on the typing of $\mathcal{E}$.
     - If $\mathcal{E} = \cdot : (\Gamma \rhd A + B) \rightsquigarrow (\Gamma \rhd A + B)$, then the result is immediate from the fact that x nf_β and that neither $x \mapsto^* 1 \cdot N$ nor $x \mapsto^* 2 \cdot N$.
     - If $\mathcal{E} = \mathcal{E}'M : (\Gamma \rhd C) \rightsquigarrow (\Gamma \rhd A + B)$ because $\Gamma \vdash M : A_1$ and $\mathcal{E}' : (\Gamma \rhd C) \rightsquigarrow (\Gamma \rhd A_1 \to A + B)$, then we know by the induction hypothesis that $\mathsf{HN}^\Gamma_{A_1 \to A+B}(\mathcal{E}'\{x\})$. By applying the induction hypothesis to this, we know that $\mathcal{E}'\{x\}$ norm_β. Let N be the normal form of $\mathcal{E}'\{x\}$, that's to say, let N be such that $\mathcal{E}'\{x\} \mapsto^* N$ nf_β. We know that x must be in head position of N. By the hypothesis that $\mathcal{E}M$ norm_β, we know that M norm_β, and so let N' be its normal form. Because x is in head position of N, we know NN' nf_β and that NN' is not an injection. But $\mathcal{E}\{x\} \mapsto^* NN'$, so $\mathcal{E}\{x\}$ norm_β. From this, we conclude that $\mathsf{HN}^\Gamma_{A+B}(\mathcal{E}\{x\})$.
     - If $\mathcal{E} = \mathsf{case}_{A+B}\, \mathcal{E}'\, \{\,\} : (\Gamma \rhd C) \rightsquigarrow (\Gamma \rhd A + B)$ by ($\mathcal{E}$-void), then we know $\mathcal{E}' : (\Gamma \rhd C) \rightsquigarrow (\Gamma \rhd \mathsf{void})$, and by the induction hypothesis, that $\mathsf{HN}^\Gamma_{\mathsf{void}}(\mathcal{E}'x)$. By definition of $\mathsf{HN}^\Gamma_{\mathsf{void}}(\cdot)$, we know that $\mathcal{E}'\{x\}$ norm_β. Let N be its normal form, then $\mathcal{E}\{x\} \mapsto^* \mathsf{case}_{A+B}\, N\, \{\,\}$ nf_β. We remark that this normal form is not an injection and conclude $\mathsf{HN}^\Gamma_{A+B}(\mathcal{E}\{x\})$.
     - If $\mathcal{E} = \mathsf{case}_D\, \mathcal{E}'\, \{1 \cdot y \hookrightarrow P \mid 2 \cdot y \hookrightarrow Q\} : (\Gamma \rhd C) \rightsquigarrow (\Gamma \rhd A + B)$ by ($\mathcal{E}$-Sum), then for some F and G, we have $\mathcal{E}' : (\Gamma \rhd C) \rightsquigarrow (\Gamma \rhd F + G)$, $\Gamma, y : F \vdash P : A + B$, and $\Gamma, y : G \vdash Q : A + B$. By the induction hypothesis, we know that $\mathsf{HN}^\Gamma_{F+G}(\mathcal{E}'\{x\})$, and by definition of $\mathsf{HN}^\Gamma_{F+G}(\cdot)$, that $\mathcal{E}'\{x\}$ norm_β. Because the variable x occupies the head position of $\mathcal{E}'\{x\}$, we know that $\mathcal{E}'\{x\} \mapsto^* N$ nf_β and that N is not of the form $1 \cdot N'$

or $2 \cdot N'$. Observe that $\mathcal{E}\{x\} = \mathsf{case}_D\, \mathcal{E}'\{x\}\, \{1 \cdot y \hookrightarrow P \mid 2 \cdot y \hookrightarrow Q\}$, and so $\mathcal{E}\{x\} \mapsto^* \mathsf{case}_D\, N\, \{1 \cdot y \hookrightarrow P \mid 2 \cdot y \hookrightarrow Q\}$ nf_β. Thus, $\mathcal{E}\{x\}$ norm_β and $\mathcal{E}\{x\}$ does not normalize to an injection. From this, we conclude $\mathsf{HN}^{\Gamma}_{A+B}(\mathcal{E}\{x\})$.

2. Immediate by definition of $\mathsf{HN}^{\Gamma}_{A+B}(M)$. □

Finally, we ready to expand our proof of the fundamental theorem (theorem 7) to handle sums:

Theorem 12 (FTLR)**.** *If* $\Gamma \vdash M : A$ *and* $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$*, then* $\mathsf{HN}^{\Delta}_{A}(\hat{\gamma}(M))$.

Proof. The proof is by induction on derivation of $\Gamma \vdash M : A$. We add the missing cases:

- (Sum-L-I). We consider $\Gamma \vdash 1 \cdot M : A + B$. The injection $\hat{\gamma}(1 \cdot M) = 1 \cdot \hat{\gamma}(M)$ is a normal form, and so $1 \cdot \hat{\gamma}(M)$ norm_β. We have $\hat{\gamma}(1 \cdot M) \mapsto^* 1 \cdot \hat{\gamma}(M)$ reflexively, and we know $\mathsf{HN}^{\Delta}_{A}(\hat{\gamma}(M))$ by the induction hypothesis. From this, we conclude $\mathsf{HN}^{\Delta}_{A+B}(\hat{\gamma}(1 \cdot M))$.
- (Sum-R-I). Symmetric to the case (Sum-L-I).
- (void-E). We consider $\Gamma \vdash \mathsf{case}_A\, M\, \{\,\} : A$. By the induction hypothesis, we know $\mathsf{HN}^{\Delta}_{\mathsf{void}}(\hat{\gamma}(M))$. By definition of $\mathsf{HN}^{\Delta}_{\mathsf{void}}(\cdot)$, this implies that $\hat{\gamma}(M)$ norm_β. But the only normal forms of type void are of the form $\mathcal{E}'\{x\}$ for some $\mathcal{E}' : (\Delta \rhd C) \rightsquigarrow (\Delta \rhd \mathsf{void})$ and $\Delta \vdash x : C$. Let $\mathcal{E} = \mathsf{case}_A\, \mathcal{E}'\, \{\,\} : (\Delta \rhd C) \rightsquigarrow (\Delta \rhd A)$. Then $\mathsf{case}_A\, M\, \{\,\} \mapsto^* \mathcal{E}\{x\}$ nf_β. By the work-horse lemma (theorem 11), we know $\mathsf{HN}^{\Delta}_{A}(\mathcal{E}\{x\})$, and so we conclude the result by head expansion (theorem 10).
- (Sum-E). We now consider $\Gamma : \mathsf{case}_C\, M\, \{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\}$. By the induction hypothesis, we know:
  - for any $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$, that $\mathsf{HN}^{\Delta}_{A+B}(\hat{\gamma}(M))$,
  - for any $\mathsf{HN}^{\Delta,x:A}_{\Gamma,x:A}(\gamma)$, that $\mathsf{HN}^{\Delta,x:A}_{C}(\hat{\gamma}(P))$, and
  - for any $\mathsf{HN}^{\Delta,x:B}_{\Gamma,x:B}(\gamma)$, that $\mathsf{HN}^{\Delta,x:B}_{C}(\hat{\gamma}(Q))$.

  Let γ such that $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$ be arbitrary. Then we know by the work-horse lemma (theorem 11) that $\hat{\gamma}(M)$ norm_β, and so we fall into one of the following three subcases:

  1. $M \mapsto^* 1 \cdot N$. Because $\mathsf{HN}^{\Delta}_{A+B}(\hat{\gamma}(M))$, we know that $\mathsf{HN}^{\Delta}_{A}(N)$. It then follows that $\hat{\gamma}(\mathsf{case}_C\, M\, \{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\}) \mapsto^* [N/x]\hat{\gamma}(P)$. Because $\mathsf{HN}^{\Delta}_{A}(N)$ and $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$, we have $\mathsf{HN}^{\Delta,x:A}_{\Gamma,x:A}(\gamma')$, where $\gamma' = [\gamma \mid x \mapsto N]$. Then by the induction hypothesis, we get $\mathsf{HN}^{\Delta,x:A}_{C}(\hat{\gamma}'(P))$, and we conclude the result by head expansion (theorem 10).
  2. $M \mapsto^* 2 \cdot N$. This case is symmetric to the previous one.
  3. $M \mapsto^* \mathcal{E}'\{z\}$ for some evaluation context $\mathcal{E}'$ and variable $z : W \in \Gamma$. Let $\mathcal{E} = \mathsf{case}_C\, \mathcal{E}'\, \{1 \cdot x \hookrightarrow \hat{\gamma}(P) \mid 2 \cdot x \hookrightarrow \hat{\gamma}(Q)\}$. If we could show that $\mathcal{E}$ norm_β, then by the work-horse lemma (theorem 11), we would know that $\mathsf{HN}^{\Gamma}_{C}(\mathcal{E}\{z\})$. From this, we could use the fact that $\mathsf{case}_C\, M\, \{1 \cdot x \hookrightarrow P \mid 2 \cdot x \hookrightarrow Q\} \mapsto^* \mathcal{E}\{z\}$ and conclude the result by head expansion. To show that $\mathcal{E}$ norm_β, we it is sufficient to show that $\hat{\gamma}(P)$ norm_β and $\hat{\gamma}(Q)$ norm_β, because we already know that $\mathcal{E}'$ norm_β. Let $\gamma' = [\gamma \mid x \mapsto x]$, then $\gamma'(y) = \gamma(y)$ for all $y \in \mathrm{dom}(\gamma)$ and $\gamma'(x) = x$. We claim $\mathsf{HN}^{\Delta,x:A}_{\Gamma,x:A}(\gamma')$. Indeed, for all $y \in \mathrm{dom}(\gamma')$ such that $y \neq x$, we know that $\mathsf{HN}^{\Delta,x:A}_{A}(\gamma'(y))$ by functoriality of $\mathsf{HN}^{(-)}_{A}(y)$ and the hypothesis that $\mathsf{HN}^{\Delta}_{\Gamma}(\gamma)$. As for $\gamma'(x)$, we know that $\mathsf{HN}^{\Delta,x:A}_{A}(x)$ by the work-horse lemma (theorem 11) using the evaluation context $\cdot : (\Delta, x : A \rhd A) \rightsquigarrow (\Delta, x : A \rhd A)$. So applying the induction hypothesis on γ' and P, we get that $\mathsf{HN}^{\Delta,x:A}_{C}(\hat{\gamma}'(P))$.

By the work-horse lemma, we then get that $\hat{\gamma}'(P)$ norm$_\beta$. But $\hat{\gamma}'(P) = \hat{\gamma}(P)$, so $\hat{\gamma}(P)$ norm$_\beta$. An analogous argument gives us that $\hat{\gamma}(Q)$ norm$_\beta$. This gives us that $\mathcal{E}$ norm$_\beta$, so we are done. □

Remark 13. *We are now in a perfect position to show the above results for a positive formulation of products:*

$$\mathrm{let}\,\langle\,\rangle\,\mathrm{be}\,M\,\mathrm{in}\,N$$

$$\mathrm{let}\,\langle x, y\rangle\,\mathrm{be}\,M\,\mathrm{in}\,N_{x,y}$$

4 Natural numbers

We now consider a fragment of Gödel's System T; we refer the reader to [Harper, 2016, Chapter 9] for the full system. Gödel proved that normalization of system T is equivalent to the consistency of Peano Arithmetic. The types and terms are given by the following grammar:

$$\begin{aligned} A &::= \mathsf{nat} \mid A_1 \to A_2 \\ M &::= \mathsf{z} \mid \mathsf{s}(M) \mid \mathsf{rec}_A\{P; x.Q\}(M). \end{aligned}$$

The statics of this fragment are:

$$\frac{}{\Gamma, x : A \vdash x : A}\ (\textsc{Var}) \qquad \frac{}{\Gamma \vdash \mathsf{z} : \mathsf{nat}}\ (\mathsf{nat\text{-}z\text{-}I}) \qquad \frac{\Gamma \vdash M : \mathsf{nat}}{\Gamma \vdash \mathsf{s}(M) : \mathsf{nat}}\ (\mathsf{nat\text{-}s\text{-}I})$$

$$\frac{\Gamma \vdash M : \mathsf{nat} \quad \Gamma \vdash P : A \quad \Gamma, x : A \vdash Q : A}{\Gamma \vdash \mathsf{rec}_A\{P; x.Q\}(M) : A}\ (\mathsf{nat\text{-}E})$$

The dynamics of this fragment are:

$$\frac{}{\mathsf{z}\ \mathsf{value}}\ (\mathsf{z}\text{-}\textsc{Val}) \qquad \frac{M\ \mathsf{value}}{\mathsf{s}(M)\ \mathsf{value}}\ (\mathsf{s}\text{-}\textsc{Val}) \qquad \frac{M \mapsto M'}{\mathsf{s}(M) \mapsto \mathsf{s}(M')}\ (\mathsf{s}\text{-}\textsc{Step})$$

$$\frac{M \mapsto M'}{\mathsf{rec}_A\{P; x.Q\}(M) \mapsto \mathsf{rec}_A\{P; x.Q\}(M')}\ (\mathsf{rec}\text{-}\textsc{Step})$$

$$\frac{}{\mathsf{rec}_A\{P; x.Q\}(\mathsf{z}) \mapsto P}\ (\mathsf{rec\text{-}z}) \qquad \frac{\mathsf{s}(M)\ \mathsf{value}}{\mathsf{rec}_A\{P; x.Q\}(\mathsf{s}(M)) \mapsto [\mathsf{rec}_A\{P; x.Q\}(M)/x]Q}\ (\mathsf{rec\text{-}s})$$

As before, our goal is to show termination in the closed setting and normalization in the open setting. Explicitly, we want to show:

1. If $M : A$, then M term_β.
2. If $\Gamma \vdash M : A$, then M norm$_\beta$.

4.1 In a closed setting

We are going to show a stronger property than item 1 or hereditary termination. What we will show is that:

$$\text{If } \Gamma \vdash M : A \text{ and } \mathsf{HT}_\Gamma(\gamma), \text{ then } \mathsf{HT}_A(\hat{\gamma}(M)).$$

Our key desideratum is that $\mathsf{HT}_{\mathsf{nat}}(M)$ imply M term_β. Seeing that nat is a positive type, we do the obvious thing:

$$\mathsf{HT}_{\mathsf{nat}}(M) \triangleq \begin{cases} \text{either } M \mapsto^* \mathsf{z}, \\ \quad\ \text{or } M \mapsto^* \mathsf{s}(M') \text{ and } \mathsf{HT}_{\mathsf{nat}}(M'). \end{cases}$$

We should be sceptical of this definition! Indeed, this definition is circular, and not all circular definitions make sense, so we need to be careful.

A potentially useful way of thinking about the definition of $\mathsf{HT}_A(M)$ is that it is recursively defined along two axes. It has a "vertical" inductive structure on the type A, and when A is nat, it has a "horizontal" structure at that level.

We can formally define $\mathsf{HT}_{\mathsf{nat}}(\cdot)$ to be the *strongest* predicate P on terms such that:

1. if $M \mapsto^* \mathsf{z}$, then $P(M)$, and
2. if $M \mapsto^* \mathsf{s}(N)$ and $P(N)$, then $P(M)$.

Equivalently, one could define the corresponding functional F and define

$$\mathsf{HT}_{\mathsf{nat}} = \bigcup_{i \geq 0} F^{(i)}(\emptyset),$$

where $F^{(0)}$ never holds, and $F^{(k+1)}$ is defined in terms of $F^{(k)}$.

We remark that this definition is *not* mathematical induction! We are reasoning about a program's computation, not natural numbers.

In showing the result at the beginning of this subsection, you will need to curry-out the M in the rule (nat-E) to get:

$$\frac{\Gamma \vdash P : A \quad \Gamma, x : A \vdash Q : A}{\Gamma, z : \mathsf{nat} \vdash \mathsf{rec}_A\{P; x.Q\}(z) : A} \ (\mathsf{nat}\text{-E}')$$

This case will then be proven using the horizontal induction principle.

4.2 In an open setting

One follows the same development, using the definition

$$\mathsf{HN}^{\Gamma}_{\mathsf{nat}}(M) \triangleq \begin{cases} \text{1. } M \text{ norm}_\beta\text{, and} \\ \text{2. if } M \mapsto^* \mathsf{z}\text{, then (true), and} \\ \text{3. if } M \mapsto^* \mathsf{s}(N)\text{, then } \mathsf{HN}^{\Gamma}_{\mathsf{nat}}(N). \end{cases}$$

References

Kurt Gödel. Über eine bisher noch nicht benÜtzte erweiterung des finiten standpunktes. *Dialectica*, 12(3-4):280–287, 1958. ISSN 1746-8361. doi: 10.1111/j.1746-8361.1958.tb01464.x. URL http://dx.doi.org/10.1111/j.1746-8361.1958.tb01464.x.

Robert Harper. *Practical Foundations for Programming Languages.* Cambridge University Press, 2nd edition, 2016.