COMBINATORS HEREDITARILY OF ORDER ONE

by

Rick Statman
Department of Mathematics
Carnegie Mellon University
Pittsburgh, PA 15213

Research Report No. 88-32 2

July 1988

Combinators Hereditarily of

Order One

by

Rick Statman

July 1988

Introduction

In this note we shall introduce a fragment of the un(i)typed λ calculus which is suitable for computing on finite structures. This fragment is generated by taking arbitrary applicative combinations of combinators which are hereditarily of order one (HOO). Members of HOO are a generalization of the proper combinators of order one. HOO combinations enjoy many properties familiar from the untyped λ calculus. There are pairing and fixed point constructions as well as a nice set of integers. Nevertheless, our first main result is that *the word problem for HOO combinations is (log space complete for) polynomial time*. In contrast, our second main result is that *Hilbert's 10^{th} problem can be encoded into the unification problem for HOO combinations*. In other words, all effective computing can be done by equation solving in HOO combinations.

(0) HOO

For the present we shall think of members of HOO as atoms with associated reduction rules. These reduction rules generate a notion of reducibility which we shall refer to as $\twoheadrightarrow$. HOO and $\twoheadrightarrow$ are defined simultaneously by induction as follows.

If $\mathfrak{X}$ is a combination of x's then X defined by the reduction rule

$$Xx \to \mathfrak{X}$$

belongs to HOO. If $\mathfrak{X}$ is a $\twoheadrightarrow$ normal combination of members of HOO and x's then X defined by the reduction rule

$$Xx \to \mathfrak{X}$$

belongs to HOO. In each case we write $X \equiv \lambda x\ \mathfrak{X}$. Examples:

$$I \equiv \lambda x\ x$$

$$\omega \equiv \lambda x\ xx$$

$$K_{*} \equiv \lambda x\ I$$

$$C_{**} \equiv \lambda x\ xI$$

(1) Encloding Data Types in HOO

Booleans:

$$T \equiv I$$

$$F \equiv K_{*}$$

$$\supset \equiv I$$

If ____ then ____ else ____ (and pairing):

$$[X,Y] \equiv \lambda x\ x(\lambda y X)Y$$

Fixed Points:

If $X \equiv \lambda x\ \mathcal{X}$ set $\mathcal{Y} \equiv [yy/x]\mathcal{X}$, $Y \equiv \lambda y\ \mathcal{Y}$ and $Fix(X) \equiv YY$. Then $X\ Fix(X) = Fix(X)$

Finite Sets with Discriminators:

Given $\{a_0, \ldots a_n\}$ set $\underline{a_i} \equiv \lambda x_1 \ldots x_i\ I$, and $E_i \equiv \lambda x\ x\underbrace{I \ldots I}_{i}\ \underline{a_n}\ \underline{a_n}\ \underline{a_{n-1}}\ \underline{a_{n-2}} \ldots \underline{a_1}$. Note that

$$E_i\ \underline{a_j} = \begin{cases} T & \text{if} \quad j \leq i \\ F & \text{if} \quad i < j \end{cases}$$

Integers:

$\underline{0} \equiv I$, $1 \equiv \lambda x\ xx \equiv \omega$, $\underline{2} \equiv \lambda x (xx)(xx)$,

$\underline{3} \equiv \lambda x\ ((xx)(xx))((xx)(xx)), \ldots.$

Set $\infty \equiv \underline{2}\,\underline{2} \equiv Fix(\underline{1})$, and $\hat{n} \equiv \lambda x\ \underbrace{x(\ldots (x}_{n+1}\omega) \ldots)$. We have $\hat{n}1 = \underline{n}\ \Omega$ and more generally

$$\hat{n}\ \underline{m} = \underline{(n+1)m - 1}\ \Omega.$$

More about this later.

(2) Circuit Value Problems

A circuit value problem is a list of Boolean equations in the variables $x_1 \ldots x_n$ of the form

$$x_i = T$$
$$x_i = F$$
$$x_i = x_j \vee x_k \qquad j,k < i$$
$$x_i = x_j \wedge x_k \qquad j,k < i$$

where each x_i appears on the ℓ.h.s. exactly once. For each x_i we define $X_i \in$ HOO as follows

$$X_i x \to xT \quad \text{if} \quad x_i = T$$
$$X_i x \to xF \quad \text{if} \quad x_i = F$$
$$X_i x \to xX_j I(\lambda y X_k)(\lambda z\ F)I \quad \text{if} \quad x_i = x_j \vee x_k$$
$$X_i x \to xX_j I(\lambda y\ T)X_k\ I \quad \text{if} \quad x_i = x_j \wedge x_k.$$

Observe that the X_i can be computed from the circuit value problem in ℓog space and

$$X_i I = T \Leftrightarrow x_i = T$$
$$X_i I = F \Leftrightarrow x_i = F$$

for $i = 1 \ldots n$.

Consequently, the word problem for HOO combinations is ℓog space hard for polynomial time.

(3) Properties of $\rightarrow$

$\rightarrow$ is a regular left normal combinatory reduction system ([3]) so it satisfies the Church-Rosser and Standardization theorems. Clearly any normal HOO combination belongs to HOO. If M is a HOO combination with no normal form we write $M = \perp$. This makes sense since the corresponding λ term is an order 0 unsolvable. More generally, it is easy to see that conversion based on $\rightarrow$ coincides with β conversion of the corresponding λ terms.

We define the notion of $\perp$ normal form ($\perp$nf) as follows. M is in $\perp$nf if $M \equiv X$ or

$$M \equiv XYM_1 \ldots M_m \text{ where } XY = \perp \text{ and each } M_i \text{ is in } \perp\text{nf}.$$

It is easy to see that $\perp$nf's always exist. However, they are not unique. Example:

Let $\alpha \equiv \lambda x\, xI\omega x$. Observing that $\alpha I \twoheadrightarrow I$ we have $\alpha\alpha \twoheadrightarrow \omega\alpha \twoheadrightarrow \alpha\alpha$.

The following relation $\rightarrowtail$ is useful in computing $\perp$nfs (as usual we assume $X \equiv \lambda x\, \mathfrak{X}$)

$$XM \rightarrowtail [M/x]\mathfrak{X} \quad \text{if} \quad M = \bot$$

$$XY \rightarrowtail \begin{cases} Z & \text{if} \quad XY = Z \\ [Y/x]\mathfrak{X} & \text{if} \quad XY = \bot \end{cases}$$

$\rightarrowtail$ is actually decidable; more about this later. A simple induction shows

$$M = X \Rightarrow M \twoheadrightarrow X.$$

We need some notation. If we write $M \equiv M[M_1,\ldots,M_m]$ then the M_i are disjoint occurrences of the corresponding HOO combinations in M.

Lemma:

Suppose $M \equiv M[M_1,\ldots,M_m]$ with $M_i = X_i$ for $i = 1\ldots m$ and $M \rightarrow N$. Then we can write $N = N[N_1,\ldots,N_n]$ with $N_j = Y_j$ for $j = 1\ldots n$ so that $M[X_1,\ldots,X_m] \twoheadrightarrow N[Y_1,\ldots,Y_n]$.

Proof:

Suppose $M \underset{\Delta}{\rightarrow} N$ by contracting the redex $\Delta \equiv XP$. As usual we assume $X \equiv \lambda x\, \mathfrak{X}$.

Case 1.

Δ is disjoint from the M_i. Then $M = M[\Delta, M_1,\ldots M_m]$ and $N \equiv M\,[[P/x]\mathfrak{X}, M_1,\ldots,M_m]$. In case $P = \bot$ we are done if we write

$N \equiv N[M_1, \ldots, M_m]$. Otherwise let $P \equiv Y$. By the above remark $P \succ\!\!\succ Y$. If $XY \equiv Z$ write $N \equiv N[[P/x]\mathfrak{A}, M_1, \ldots, M_m]$. We have $M[X_1, \ldots, X_m] \succ\!\!\succ M[XY, X_1, \ldots, X_m] \succ\!\!\succ N[Z, X_1, \ldots, X_m]$. Finally, if $XY \equiv 1$ write $\mathfrak{A} \equiv \mathfrak{L}[x, \ldots, x]$ showing all occurrences of x. We have $N \equiv M[\mathfrak{L}[P, \ldots, P], M_1, \ldots, M_m]$.

Write $N \equiv N[P, \ldots, P, M_1, \ldots, M_m]$. We have $M[X_1, \ldots, X_m] \succ\!\!\succ M[XY, X_1, \ldots, X_m] \succ\!\!\succ M[\mathfrak{A}[Y, \ldots, Y], X_1, \ldots, X_m] \equiv N[Y, \ldots, Y, X_1, \ldots, X_m]$.

Case 2:

$A \subseteq M_i$ for some i. W.l.o.g. assume $i = 1$. Write $M_1 \equiv \mathfrak{L}_1[A]$. Since $N \equiv M[\mathfrak{L}_1[[P/x]\mathfrak{A}], \ldots, M_m]$ and $M_1[[P/x]\mathfrak{A}] = X_1$ we can write $N \equiv N[M_1[[P/x]\mathfrak{A}], \ldots, M_m]$ and $M[X_1, \ldots, X_m] \equiv N[X_1, \ldots, X_m]$.

Case 3:

Some $M_i \subseteq A$. Wlog assume $M_1, \ldots, M_k \subseteq A$ but no others. Clearly we can assume that no M_i is X so $M_1, \ldots, M_k \subseteq P$. Write $P \equiv P[M_1, \ldots, M_k]$ and let $Q \equiv [P/x]\mathfrak{A}$.

Subcase 1;

$P = 1$. Write $Q \equiv Q[M_1, \ldots, M_k]$ indicating all the substituted occurrences of the M_j $(j \leq k)$ in Q. We have $N \equiv M[Q[M_1, \ldots, M_k], M_{k+1}, \ldots, M_m]$, so we can write $N \equiv N[M_1, \ldots, M_k, M_{k+1}, \ldots, M_m]$, and then $M[X_1, \ldots, X_m] \equiv M[XP[X_1, \ldots, X_k], X_{k+1}, \ldots, X_m] \succ\!\!\succ M[[P[X_1, \ldots, X_k]/x]\mathfrak{A}, X_{k+1}, \ldots, X_m] \equiv M[Q[\vec{X}_1, \ldots, \vec{X}_k], X_{k+1}, \ldots, X_m] \equiv N[\vec{X}_1, \ldots, \vec{X}_k, X_{k+1}, \ldots, X_m]$.

Subcase 2;

$P = Y$ and $XY = \bot$. Write $Q \equiv Q[\vec{P}]$ indicating the substituted occurrences of P in Q. We have $N \equiv M[Q[\vec{P}], M_{k+1}, \ldots, M_m]$, so we can write $N \equiv N[\vec{P}, M_{k+1}, \ldots, M_m]$, and then $M[X_1, \ldots, X_m] \equiv M[XP[X_1, \ldots, X_k], X_{k+1}, \ldots, X_m] \succ\!\!\twoheadrightarrow M[XY, X_{k+1}, \ldots, X_m] \succ\!\!\twoheadrightarrow M[[Y / x]\mathfrak{X}, X_{k+1}, \ldots, X_m]$ $\equiv M[Q[\vec{Y}], X_{k+1}, \ldots, X_m] \equiv N[\vec{Y}, X_{k+1}, \ldots, X_m]$.

Subcase 3;

$P = Y$ and $XY = Z$. Write $N \equiv N[Q, M_{k+1}, \ldots M_m]$. Then $M[X_1, \ldots, X_m]$ $\succ\!\!\twoheadrightarrow M[XY, X_{k+1}, \ldots, X_m] \succ\!\!\twoheadrightarrow M[Z, X_{k+1}, \ldots, X_m] \equiv N[Z, X_{k+1}, \ldots, X_m]$.

Proposition:

If $M \longrightarrow\!\!\!\!\!\twoheadrightarrow N$ and N is $\bot$ normal, then $M \succ\!\!\twoheadrightarrow N$.

Proof:

By the lemma we can write $N \equiv N[N_1, \ldots, N_n]$ with $N_i = Y_i$ so that $M \succ\!\!\twoheadrightarrow N[Y_1, \ldots, Y_n]$. Since N is in $\bot$nf for $i = 1 \ldots m$ $N_i \equiv Y_i$. Thus $M \succ\!\!\twoheadrightarrow N$.

(4) $\sqsubseteq$

$\sqsubseteq$ is the partial order on HOO generated from the following cover relations

$$Y \sqsubsetneq X \quad \text{if} \quad X \equiv \lambda x \;\; Y$$

$$\lambda x \; \mathfrak{X}_i \sqsubsetneq X \quad \text{if} \quad X \equiv \lambda x \;\; x\mathfrak{X}_1 \ldots \mathfrak{X}_n$$

$\mathbf{X} \equiv X_1, \ldots, X_n \subset \mathrm{HOO}$ is admissible if $\mathbf{X}$ is closed under $\subsetneq$ and $X_i \subsetneq X_j \Rightarrow i < j$. Note that if $\mathbf{X}$ is admissible and $X_i X_j = Y$ then $Y \in \mathbf{X}$.

$\chi_{\mathbf{X}}$ is the $n \times n$ matrix with entries in $\{1, \ldots, n, \perp\}$ defined by

$$\chi_{\mathbf{X}}(i,j) = \begin{cases} k & \text{if } X_i X_j = X_k \\ \perp & \text{otherwise} \end{cases}$$

The proceedure $(\ )^{\perp}$ is computed on $\mathbf{X}$ combinations as follows: $X_i^{\perp} \equiv X_i$ and

$$\begin{aligned}
(X_i M_1 \ldots M_m)^{\perp} = (X_j M_2 \ldots M_m)^{\perp} \quad & \text{if} \quad X_i \equiv \lambda x\, X_j \\
& \text{or} \quad M_1^{\perp} \equiv X_k \\
& \text{and} \quad X_i X_k = X_j \\
X_i X_j M_2^{\perp} \cdots M_m^{\perp} \quad & \text{if} \quad M_1^{\perp} \equiv X_j \\
& \text{and} \quad X_i X_j = \perp \\
[M_1^{\perp}/x]\mathcal{X} M_2^{\perp} \cdots M_m^{\perp} \quad & \text{if} \quad M_1 = \perp \\
& \text{and} \quad x \in \mathcal{X}
\end{aligned}$$

Although the output of $(\ )^{\perp}$ can be exponentially long in the input this is only because of repeated subterms. The proceedure will run in time polynomial in the input and $\chi_{\mathbf{X}}$ if the output is coded by a system of assignment statements. For example, if $X_i M_1 \ldots M_m$ is M, the last alternative in the definition of $(M)^{\perp}$ adds the assignment

$$x_M = [x_{M_1}/x]\mathfrak{X}\, x_{M_2} \ldots x_{M_m}$$

to those for $M_1, \ldots, M_m$. This coding is precisely what is needed for the application below.

Obviously, $M^{\perp}$ is in $\perp$nf.

(5) The Relation $\mapsto$

The relation $\mapsto$ is defined by

$$XY \mapsto ([Y/x]\mathfrak{X})^{\perp}.$$

Observe that the conversion relation generated by $\mapsto$ restricted to admissible **X** can be presented as a finitely presented algebra ([2]). $\mapsto$ is particularly useful in conversion between $\perp$nfs.

Fact:

If $M = \perp$, then $(MN)^{\perp} \equiv M^{\perp}N^{\perp}$

Proof:

By induction on the definition of $(\ )^{\perp}$

Fact:

If $X \equiv \lambda x\, \mathfrak{X}$ and $M = \perp$, then

$$(XM)^{\perp} \equiv ([M/x]\mathfrak{X})^{\perp}$$

Proof:

By induction on $\sqsubseteq$.

Lemma:

If $M \succ\!\!\longrightarrow N$ then $M^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N^{\perp}$.

Proof:

By induction on M. When M is an atom, there is nothing to prove.

Induction Step:

$M \equiv XM_1 \ldots M_m$. We suppose that $M \underset{\Delta}{\succ\!\!\longrightarrow} N$ by contracting the $\succ\!\!\longrightarrow$ redex Δ.

Case 1;

$\Delta \subseteq M_i$ for some i.

Subcase 1:

$X \equiv \lambda x\ Y$ or $M_1^{\perp} \equiv Z$ and $XZ = Y$. In case $i = 1$ we have $M^{\perp} \equiv (YM_2 \ldots M_m)^{\perp} \equiv N^{\perp}$. In case $i > 1$ we have $M^{\perp} \equiv (YM_2 \ldots M_m)^{\perp}$, $N^{\perp} \equiv (YN_2 \ldots N_m)^{\perp}$ and $YM_2 \ldots M_m \succ\!\!\longrightarrow YN_2 \ldots N_m$. Thus by induction hypothesis $M^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N^{\perp}$.

Subcase 2:

$M_1^{\perp} \equiv Y$ and $XY = \perp$. In case $i = 1$ we have $M^{\perp} \equiv XYM_2^{\perp} \ldots M_m^{\perp} \equiv N^{\perp}$. In case $i > 1$ we have $M^{\perp} \equiv XYM_2^{\perp} \ldots M_m^{\perp}$ and $N^{\perp} \equiv XYN_2^{\perp} \cdots N_m^{\perp}$ where for

$j = 2 \ldots m$ either $N_j \equiv M_j$ or $M_j \succ\!\!\to N_j$. Thus by induction hypothesis $M_j^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N_j^{\perp}$ and $M^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N^{\perp}$.

Subcase 3:

$M_1 = \perp$ and $x \in \mathfrak{X}$. In case $i = 1$ we have $M^{\perp} \equiv [M_1^{\perp}x]\mathfrak{X}\, M_2^{\perp} \cdots M_m^{\perp}$ and $N^{\perp} \equiv [N_1^{\perp}/x]\mathfrak{X}M_2^{\perp} \cdots M_m^{\perp}$ where $M_1 \underset{\Delta}{\succ\!\!\longrightarrow} N_1$. By induction hypothesis $M_1^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N_1^{\perp}$ so $M^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N^{\perp}$. In case $i > 1$ we have $M_1^{\perp} \equiv [M_1^{\perp}/x]\mathfrak{X}M_2^{\perp} \cdots M_m^{\perp}$ and $N^{\perp} \equiv [M_1^{\perp}/x]\mathfrak{X}N_2^{\perp} \cdots N_m^{\perp}$ where for $j = 2 \ldots m$ either $N_j \equiv M_j$ or $M_j \underset{\Delta}{\succ\!\!\longrightarrow} N_j$. Thus by induction hypothesis $M_j^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N_j^{\perp}$ so $M^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N^{\perp}$.

Case 2;

$\Delta \equiv XM_1$.

Subcase 1:

$X \equiv \lambda x\ Y$ or $M_1^{\perp} \equiv Z$ and $XZ = Y$. In the first case $M^{\perp} \equiv (YM_2 \ldots M_m)^{\perp} \equiv N^{\perp}$. In the second case, since Δ is a $\succ\!\!\longrightarrow$ redex $M_1 \equiv Z$ and $M^{\perp} \equiv (YM_2 \ldots M_m)^{\perp} \equiv N^{\perp}$.

Subcase 2:

$M_1^{\perp} \equiv Y$ and $XY = \perp$. Since Δ is a $\succ\!\!\longrightarrow$ redex we have $M_1 \equiv Y$ and $N \equiv [Y/x]\mathfrak{X}\ \ M_2 \ldots M_m$. In addition $M^{\perp} \equiv XY\ M_2^{\perp} \cdots M_m^{\perp} \mapsto\!\!\!\!\twoheadrightarrow ([Y/x]\mathfrak{X})^{\perp}M_2^{\perp} \ldots M_M^{\perp})$ $\equiv ([Y/x]\mathfrak{X}M_2 \ldots M_m)^{\perp}$ since $[Y/x]\mathfrak{X} = \perp$. Thus $M^{\perp} \mapsto\!\!\!\!\twoheadrightarrow N^{\perp}$.

Subcase 3:

$M_1 = \bot$ and $x \in \mathfrak{X}$. We have $M^\bot \equiv [M_1^\bot/x]\mathfrak{X}M_2^\bot \cdots M_m^\bot \equiv ([M_1/x]\mathfrak{X})^\bot$ $M_2^\bot \cdots M_m^\bot \equiv ([M_1/x]\mathfrak{X}\ M_2\ \ldots\ M_m)^\bot$ since $M_1 = \bot = [M_1/x]\mathfrak{X}$. Thus $M^\bot \mapsto\!\!\!\twoheadrightarrow N^\bot$ in all the cases.

Proposition:

If M and N are $\bot$ normal and $M \twoheadrightarrow N$ then $M \mapsto\!\!\!\twoheadrightarrow N$.

Proof:

Suppose $M \twoheadrightarrow N$. By previous proposition $M \rightarrowtail\!\!\!\twoheadrightarrow N$. Thus by the lemma $M \equiv M^\bot \mapsto\!\!\!\twoheadrightarrow N^\bot \equiv N$.

Corollary.

If M and N are $\bot$nfs and $M = N$, then $\exists P$ P is a $\bot$nf and

$$M \mapsto\!\!\!\twoheadrightarrow P \twoheadleftarrow\!\!\!\dashv N.$$

Proof:

By the Church-Rosser theorem there is a Q s.t. $M \twoheadrightarrow Q \twoheadleftarrow N$. We can set $P \equiv Q^\bot$.

(6) Computation of $\chi_{\mathbf{X}}$

We suppose that $\chi_{\mathbf{X}}$ is given, and we wish to comput $\chi_{\mathbf{XX}_{n+1}}$. Toward this end we need a proceedure $(\ )^H$ which takes as an input an $\mathbf{XX}_{n+1}$ combination and depends on $\chi_{\mathbf{X}}$ and a parameter $\Gamma \subseteq \{1, \ldots, n+1\} \times \{n+1\}$

(Here we suppose $\chi_{\mathbf{X}}$ has been supplemented with values for pairs not in Γ.).

$(\ )^H$

Input: M

If $M \equiv X_i$ then return i else

If $M \equiv X_i M_1 \ldots M_M$ then do

If $X_i \equiv \lambda x X_j$ then $(X_j M_2 \ldots M_M)^H$ else

h:= $(M_1)^H$

If h = (k,ℓ) then return (k,ℓ) else

If h = k then

cases: $(i,k) \in \Gamma$ return (i,k)

$i = n + 1$ and $k \leq n$ $h{:=}([X_k/x]\mathfrak{X}_{n+1})^H$

If h = p then

$(X_p M_2 \ldots M_m)^H$

else

return h

$(i,k) \notin \Gamma$. If $X_{\mathbf{X}}(i,k) = p$ then

$(X_p M_2 \ldots M_M)^H$

else

return (i,k)

Note that if the values $([X_k/x]\mathfrak{X}_{n+1})^H$ for $k = 1 \ldots n$ have been precomputed and stored for look up then the proceedure $(\ )^H$ runs in time polynomial in the input.

$(\ )^H$ computes a first approximation to the head of a $\perp$nf for the input. It is used as follows. For $i = 1, \ldots, n+1$ set $h_i = ([X_{n+1}/x]\mathcal{X}_i)^H$. Define a graph G_Γ as follows. The points of G_Γ are the values h_i and the pairs $(i, n+1) \in \Gamma$. The edges are the directed

$$(i, n+1) \longrightarrow h_i.$$

Given $(i, n+1) \in \Gamma$ $(i, n+1)$ begins a unique path which either cycles or terminates in a value outside of Γ. If this path cycles then $X_i X_{n+1} = \perp$ as we shall see below. The path terminates in a pair (j,k) only if $\chi_{\mathbf{X}}(j,k) = \perp$ so again $X_i X_{n+1} = \perp$.

Finally, if the path terminates in an integer k then for the last edge in the path

$$(j, n+1) \rightarrow k$$

we can conclude $X_j X_{n+1} = X_k$. Thus at least one new value can be added to $\chi_{\mathbf{X}}$ and Γ decreased by at least one.

Lemma:

If $[X_j/x]\mathcal{X}_i \twoheadrightarrow X_i X_j M_1 \ldots M_m$, then $X_i X_j = \perp$.

Proof:

If $[X_j/x]\mathcal{X}_i \twoheadrightarrow X_i X_j M_1 \ldots M_m$, then there is a standard reduction by the standardization theorem. This reduction has the form

$$[X_j/x]\mathfrak{X}_i \underset{\text{head}}{\twoheadrightarrow} X_i N_0 N_1 \ldots N_m \underset{\substack{\text{head} \\ \text{reduction of } N_0}}{\twoheadrightarrow}$$

$$X_i X_j N_1 \ldots N_m \underset{\text{internal}}{\twoheadrightarrow} X_i X_j M_1 \ldots M_m .$$

Now the reduction $X_i X_j \to [X_j/x]\mathfrak{X} \underset{\text{head}}{\twoheadrightarrow} X_i N_0 N_1 \ldots N_m$

$\underset{\substack{\text{head} \\ \text{reduction of } N_0}}{\twoheadrightarrow} X_i X_j N_1 \ldots N_m \to [X_j/x]\mathfrak{X}\ N_1 \ldots N_m \twoheadrightarrow \cdots$ is a quasi left most reduction of $X_i X_j$. Thus $X_i X_j$ has no normal form (see [1] pgs. 327-329).

Given admissible **X**, $\chi_{\mathbf{X}}$ can be computed recursively from the initial segments of **X** in time polynomial in **X**.

(7) A Polynomial Algorithm for the Word Problem

Suppose that we are given two HOO combinations M and N together with the reduction rules for their atoms. Construct an admissible **X** containing these rules. This can be done in time polynomial in the input. Next compute $\chi_{\mathbf{X}}$ as above. Using $\chi_{\mathbf{X}}$ compute $M^{\perp}$ and $N^{\perp}$ as systems of assignment statements. Finally add to these systems the equations $X_i X_j = ([X_j/x]\mathfrak{X}_i)^{\perp}$ for each pair $X_i, X_j \in \mathbf{X}$ (or rather the corresponding systems of assignment statements) and, using the algorithm for the word problem for finitely presented algebras [2], test whether $x_M = x_N$ is a consequence of these statements. (2)-(7) can be summarized as follows.

Theorem

The word problem for HOO combinations is log space complete for polynomial time.

(8) Integers

X is said to be pure if it is a proper combinator of order one. Define Pure(M) $\Leftrightarrow$ MI = I and M∞ = ∞.

Fact:

Pure (M) $\Leftrightarrow \exists$Xpure M = X.

Proof:

$\Leftarrow$ is clear since $\infty\infty = \infty$. Suppose Pure(M). Since MI = I, M $\neq \perp$ so M = X for some X. As usual assume X $\equiv \lambda x\, \mathfrak{X}$. Since $\infty \to \infty\infty$, if Y is contained in $\mathfrak{X}$ then Y is contained in any reduct of X∞. Thus by Church-Rosser Y must be ∞. But this contradicts MI = I. Hence X is pure.

Define Int(M) $\Leftrightarrow$ Pure(M) and (MΩ)(MΩ) = M($\Omega\Omega$).

Fact:

Int(M)$\Leftrightarrow \exists$X integer M = X.

Proof:

$\Leftarrow$ is clear since if $\underline{n} \equiv \lambda x\, \mathfrak{X}$ then $\underline{n+1} \equiv \lambda x\, \mathfrak{X}\mathfrak{X} \equiv \lambda x[xx/x]\mathfrak{X}$. Suppose Int(M). Then for some pure X $\equiv \lambda x\, \mathfrak{X}$ M = X and $[\Omega/x]\mathfrak{X}[\Omega/x]\mathfrak{X} = [\Omega\Omega/x]\mathfrak{X}$. Since $\Omega \to \Omega$, by Church-Rosser, $\mathfrak{X}\mathfrak{X} \equiv [xx/x]\mathfrak{X}$. An easy induction shows that the tree $\mathfrak{X}$ is complete binary; thus X is an integer.

The notion of an ω-scheme is defined inductively as follows. I and $\lambda x\ \omega$ are ω-schemes. If $\lambda x\mathcal{X}_1, \ldots, \lambda x\mathcal{X}_n$ are ω-schemes then $\lambda x\ x\mathcal{X}_1 \ldots \mathcal{X}_n$ is an ω-scheme. For example, for each integer n $\hat{n}$ is an ω-scheme. Define Scheme(M) $\Leftrightarrow \exists N$ Pure(N) and $M\Omega = N\omega$ and $MI = \omega$. Note that for each integer n Scheme($\hat{n}$).

Fact:

Scheme(M) $\Rightarrow$ there exists an ω-scheme X s.t.

$$X = M$$

Proof:

Suppose Scheme(M) so $\exists N$ Pure(N), $M\Omega = N\omega$, and $MI = \omega$. Since Pure(N) there exist pure X s.t. $N = X$. Since $MI = \omega$, $M \neq \bot$ and there exists $Y \equiv \lambda y\ y$ s.t. $M = Y$. If $y \notin \mathcal{Y}$, since $MI = \omega$ we have $M = \lambda x\ \omega$. If $y \in \mathcal{Y}$, since $\Omega \rightarrow \Omega$, $\mathcal{Y}$ contains no atom other than ω. Thus Y is an ω-scheme.

Define Sum(M,N,P) $\Leftrightarrow P\Omega = M(N\Omega)$.

Fact:

Sum($\underline{n}, \underline{m}, \underline{p}$) $\Leftrightarrow p = n + m$.

Proof:

Obvious.

(9) Encoding Hilbert's 10^{th} Problem into HOO Unification

We have already seen how to represent the set of integers as the projection of the set of solutions to a HOO unification problem, and how to represent the sum of two integers. It remains to represent multiplication.

Lemma:

If X is an ω-scheme and there exist integers n, m s.t.. $X\underline{1} = \underline{n}\Omega$ and $X\underline{2} = \underline{m}\Omega$ then there exists a linear function $\ell_X : \mathbb{Z} \to \mathbb{Z}$ such that for all positive k

$$X\underline{k} = \underline{\ell_X(k)}\ \Omega$$

Proof:

By induction on $\mathfrak{X}$ (again we assume $X \equiv \lambda x\ \mathfrak{X}$).

Basis:

We shall check four cases. This will simplify the induction step.

Case 1;

$\mathfrak{X} \equiv x$. This is impossible since $\underline{2} \neq \underline{m}\Omega$

Case 2;

$\mathfrak{X} \equiv \omega$. This is impossible since $\underline{1} \neq \underline{m}\Omega$

Case 3;

$\mathfrak{X} \equiv xx$. This is impossible since $\infty \neq \underline{m}\Omega$.

Case 4;

$\mathfrak{X} \equiv x\omega$. Clearly $\ell_X(x) = x - 1$.

Induction Step:

$\mathfrak{X} \equiv \mathfrak{X}_1\mathfrak{X}_2$. Set $M_1 \equiv [\underline{1}/x]\mathfrak{X}_1, N_1 \equiv [\underline{2}/x]\mathfrak{X}_1$, $M_2 \equiv [\underline{1}/x]\mathfrak{X}_2$, $N_2 \equiv [\underline{2}/x]\mathfrak{X}_2$.

Case 1;

$N_1 \neq \perp$. Since M_1 is an applicative combination of ω's, we have $M_1 \equiv \omega$ and $\mathfrak{X}_1 \equiv x$. If $M_2 \neq \perp$ similarly $M_2 \equiv \omega$, and since we are in the induction step and $\mathfrak{X}_2 \not\equiv x$, $\mathfrak{X}_2 \not\equiv \omega$ this is impossible. Thus $M_2 = \perp$. Similarly $N_2 = \perp$. Thus we have $\underline{n}\Omega = X\underline{1} = \omega\, M_2 = M_2M_2$ so $n > 0$ and $M_2 = \underline{n-1}\Omega$. In addition, $\underline{m}\Omega = X\underline{2} = \underline{2}N_2 = (N_2N_2)(N_2N_2)$ so $m > 1$ and $N_2 = \underline{m-2}\Omega$. Thus by induction hypothesis applied to $\lambda x\, \mathfrak{X}_2$, $\ell_{\lambda x\mathfrak{X}_2}$ exists. Thus by ℓ_X exists with

$$\ell_X(x) = \ell_{\lambda x\, \mathfrak{X}_2}(x) + x$$

Case 2;

$M_1 = \perp$. As above $N_1 = \perp$. Since $M_1M_2 = \underline{n}\Omega$ $n > 0$ and $M_2 = \underline{n-1}\Omega = M_2$. Similarly $m > 0$ and $N_1 = \underline{m-1}\Omega = N_2$. Thus by induction hypothesis applied to both $\lambda x\, \mathfrak{X}_1$ and $\lambda x\, \mathfrak{X}_2$, $\ell_{\lambda x\, \mathfrak{X}_1}$ and

$\ell_{\lambda x\,\mathcal{X}_2}$ exist. Since $\ell_{\lambda x\,\mathcal{X}_1}(1) = n - 1 = \ell_{\lambda x\,\mathcal{X}_2}$ and $\ell_{\lambda x\,\mathcal{X}_1}(2) = m - 1 = \ell_{\lambda x\,\mathcal{X}_2}(2)$, $\ell_{\lambda x\,\mathcal{X}_1} = \ell_{\lambda x\,\mathcal{X}_2}$. Thus ℓ_X exists and

$$\ell_X(x) = \ell_{\lambda x\,\mathcal{X}_1}(x) + 1.$$

Note that if the ω-scheme X satisfies $X\underline{1} = \underline{n}\Omega$ and $X\underline{2} = \underline{m}\Omega$, then $\ell_X(x) = (m - n)x + (2n - m)$.

Define It(M,N) $\Leftrightarrow \exists$ P,Q,R Scheme(M) and Int(P) and Int(Q) and Int(R) and Sum(P,$\underline{1}$,N) and Sum(N,N,Q) and Sum(R,$\underline{1}$,Q) and M$\underline{1}$ = PΩ and M$\underline{2}$ = RΩ.

Fact:

It($\hat{n}$,$\underline{n + 1}$).

Fact:

If It(M,$\underline{n}$) then there exists an ω scheme X s.t. M = X and for m > 0 X$\underline{m}$ = $\underline{n \cdot m - 1}$.

Finally we are ready to define multiplication.

Define Prod($M_1 N_1 P$) $\Leftrightarrow \exists$ LTQR It(L,T) and Int(T) and Int(Q) and Int(R) and Sum(M,$\underline{1}$,T) and Sum(Q,$\underline{1}$,LN) and Sum(R,N,Q) and R = P.

Fact:

$\text{Prod}(\underline{m},\underline{n},\underline{p}) \Leftrightarrow m \cdot n = p$.

(8)-(9) can be summarized as follows.

Theorem:

Every RE set of integers can be represented as the projection of the set of all solutions of a HOO unification problem.

(10) References

[1] Barendregt, *The Lambda Calculus*, North Holland, 1984.

[2] Kozen, The complexity of finitely presented algebras, *STOC*, 1977.

[3] Klop, *Combinatory Reduction Systems*, Math. Centrum, Amsterdam, 1980.