SIMPLY TYPED λ CALCULUS
WITH
SURJECTIVE PAIRING

by

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

April 1992

Abstract

There are two significant differences between the simply typed λ claculus and the simply typed λ calculus with surjective pairing. These differences are summarized by our two principal results

Theorem 1. If $\mathscr{A}$ is any non trivial model of $\beta\,\eta$ S P

then

$$\mathscr{A} \models M = N \Leftrightarrow M \underset{\beta\eta SP}{=} N$$

Theorem 2. The collection of all sets of projections of $\beta\,\eta$ S P unification problems is precisely the collection of all recursively enumeable sets of terms of the same type closed under $\beta\,\eta$ S P conversion.

In this note we consider the simply typed λ–calculus over a single ground type 0 ([1] pg. 561) together with surjective pairing ([1] pg. 403) at type 0. More precisely, we add to the simply typed λ calculus Λ new constants $\delta \in 0 \longrightarrow (0 \longrightarrow 0)$, $\delta_1 \in 0 \longrightarrow 0$, and $\delta_2 \in 0 \longrightarrow 0$ and new reduction rules

$$SP \begin{cases} (\delta_i) & \delta_i(\delta\ X_1\ X_2) \longrightarrow X_i \quad i \in \{1, 2\} \\ (\delta) & \delta\,(\delta_1\ X)\ (\delta_2\,X) \longrightarrow X \end{cases}$$

for $X \in \Lambda\ \delta\ \delta_1\ \delta_2$. In [6] it is shown that $\beta\,\eta$ S P is Church – Rosser and strongly normalizable.

Let α be a closed term of type $0 \longrightarrow 0$ in long ([9] pg. 533) $\beta\,\eta$ S P normal form. Then α has one of the forms $\lambda a.\ a$, $\lambda a.\ \delta t_1 t_2$, $\lambda a.\ \delta_i t$ for first order terms t. We consider the Böhm tree of α less the prefix $\lambda a.$ It consists of a full binary tree whose nodes are labelled δ, called the Δ of α, followed by paths whose nodes are labelled δ_i except for the leaves labelled a. This variable a will remain fixed throughout. It is useful to note here that δ expansions of α have a similar shape.

For each type σ we define $\delta_i \in 0 \longrightarrow 0$ and $\delta \in \sigma \longrightarrow (\sigma \longrightarrow \sigma)$ recursively by

$$\delta_i \equiv \lambda xz \;\; \delta_i(xz) \qquad\qquad i \in \{1, 2\}$$

$$\delta \equiv \lambda xyz \;\; \delta(xz)\,(yz).$$

We have

$$\delta_i\,(\delta\, X_1\, X_2) \xrightarrow[\beta\eta SP]{} X_i$$

$$\delta\,(\delta_1\, X)\,(\delta_2\, X) \xrightarrow[\beta\eta SP]{} X$$

When $\sigma = 0 \longrightarrow 0$ we shall write $<x, y>$ for $\delta\, x\, y$. Let $\alpha \in \Lambda\; \delta\; \delta_1 \delta_2$ be a closed long $\beta\,\eta$ S P normal form $\in 0 \longrightarrow 0$; as above α has one of 3 forms. We can write $\alpha \equiv I$, $\alpha \underset{\beta\eta SP}{=} < \lambda a.\, t_1 , \lambda a.\, t_2 >$, or $\alpha \underset{\beta\eta SP}{=} \delta_i \circ \lambda a.t.$

Thus each such α can, modulo $\beta\,\eta$ S P conversion, be built up from I, δ_1 , δ_2 by $\circ$ and $< \;\; >$. A Cartesian monoid $(M, \circ, I, L, R, < \;\; >)$ is a structure s.t. $(M, \circ, I)$ is a monoid, with $L, R \in M$ and $< \;\; > : M^2 \longrightarrow M$ satisfying

$$L \circ < x, y > = x\,,$$

$$R \circ < x, y > = y\,,$$

$$\langle x, y \rangle \circ z = \langle x \circ z, y \circ z \rangle, \text{ and}$$
$$\langle L, R \rangle = I.$$

([4] pg. 389). The free Cartesian monoid generated by L and R (and I) is denoted '$\mathcal{M}$'. We have seen that there is an obvious homomorphism from $\mathcal{M}$ onto the closed terms of type $0 \to 0$.

Now the embedding of $\mathcal{M}$ into $M \to M$ by left multiplications $\alpha \longmapsto \hat{\alpha} = \lambda x.\ \alpha \circ x$ extends to the Cartesian structure of $\mathcal{M}$. In particular, $\langle \hat{\alpha}_1, \hat{\alpha}_2 \rangle = \lambda x \langle \hat{\alpha}_1(x), \hat{\alpha}_2(x) \rangle$. Thus by the Church – Rosser theorem the above homomorphism is an isomorphism. In summary,

<u>Proposition 1.</u> $\mathcal{M}$ is isomorphic to

$$\left[\overline{\Lambda\ \delta}\ \delta_1\ \delta_2{}^{0 \to 0} \big/ =_{\beta\eta SP},\ B, I, \delta_1, \delta_2, \lambda(x, y)\ \delta xy\right]$$

Similarly, the "polynomial" Cartesian monoids $\mathcal{M}[x_1, \dots, x_n]$ are isomorphic to the structures

$$\left[\overline{\Lambda\ \delta}\ \delta_1\ \delta_2{}^{\overbrace{(0 \to 0) \to (\dots((0 \to 0)}^{n} \to (0 \to 0))\dots)} \big/ =_{\beta\eta SP},\ B_n,\ I_n,\ \delta_{1,n}, \delta_{2,n}, \lambda(x, y)\ \delta_{,n} xy\right]$$

where

$B_n \equiv \lambda uv\ \lambda x_1 \dots x_n . \lambda a.\ u x_1 \dots x_n (v x_1 \dots x_n\ a)$ and $I_n \equiv \lambda x_1 \dots x_n . \lambda a.\ a$ ([10] pg. 186), $\delta_{i,n} \equiv \lambda x_1 \dots x_n\ \delta_i$, and $\delta_{,n} \equiv \lambda x_1 \dots x_n\ \delta$.

For many purposes all of $\overline{\Lambda\ \delta\ \delta_1}\ \delta_2$ can be reduced to $(0 \longrightarrow 0) \longrightarrow (0 \longrightarrow 0)$ and therefore $\mathcal{M}$ [x]

<u>Proposition 2.</u> For each type σ there exists $M \in \overline{\Lambda\ \delta\ \delta_1}\ \delta_2{}^{\sigma \to ((0 \to 0) \to (0 \to 0))}$ such that for all $N_i \in \overline{\Lambda\ \delta}\ \delta_1\ \delta_2{}^{\sigma}$, $i \in \{1, 2\}$

$$N_1 \underset{\beta\eta SP}{=} N_2 \Leftrightarrow MN_1 \underset{\beta\eta SP}{=} MN_2$$

<u>Proof.</u> We can copy the proof of [9] pg. 517 propositon 1 to reduce each type σ to $(0 \to (0 \to 0)) \longrightarrow (0 \to 0)$. This type in turn is reducible to $(0 \to 0) \longrightarrow (0 \to 0)$ by

$$\lambda u\ \lambda x\ \lambda a.\ u(\lambda z_1 z_2\ x\ (\delta\ (xz_1)\ (xz_2)))a$$

<u>Proposition 3.</u> Suppose M and N are closed terms $\in (0 \to 0) \longrightarrow (0 \to 0)$ and $M \underset{\beta\eta SP}{\neq} N$, then there exist a closed $\theta \in 0 \to 0$ s.t.

$$M\theta \underset{\beta\eta SP}{\neq} N\theta$$

<u>Proof.</u> More generally suppose $\vec{x} = x_1, \ldots, x_n$, $\alpha(\vec{x})$ and $\beta(\vec{x}) \in \mathcal{M}\ [\vec{x}]$ and $\alpha(\vec{x}) \neq \beta(\vec{x})$. We shall find $\vec{\theta} = \theta_1, \ldots, \theta_n$ s.t. $\alpha(\vec{\theta}) \neq \beta(\vec{\theta})$. The proof consists of 2 parts. In the first part n may be increased. W.l.o.g. we can assume that $\alpha(\vec{x})$ and $\beta(\vec{x})$ are in long $\beta\eta$SP normal form. The 1st part of the construction removes subexpressions $L(x_i\ t)$ and $R(x_i\ t)$ by making substitutions $[< y, z > \mid x_i]$ and renormalizing. It is easily seen that this process teminates $\alpha(\vec{x})$ and $\beta(\vec{x})$ can be recovered by making substitutions $[L \circ x \mid y\ , R \circ x \mid z]$. Thus we can assume that $\alpha(\vec{x})$ and $\beta(\vec{x})$ are normal, distinct and without such subexpressions.

Now let m exceed the length of the longest path in the Böhm tree of $\alpha(\vec{x})$ or $\beta(\vec{x})$. We shall set $\theta_i =$

$$< < \underbrace{w, < . . . < w,}_{m\ +\ i} I > \ldots > > , w >$$

where $w = R^k$ for sufficiently large k. Note that if t is normal, contains only the variable a, and k exceeds the length of the longest path in the Δ of t then $\theta_i t =$

(*) $$< < t^1, < \ldots < t^1 , t > \ldots > > , t^1 >$$

where t^1 is $< \ >$ free, and the longest path in the Δ increases by at most $m + i + 1 \leq m + n + 1$.

Put $k = m\ (m + n + 1)$. We shall show that $\alpha(\vec{x})$ and $\beta(\vec{x})$ are reconstructible from the normal forms of $\alpha(\vec{\theta})$ and $\beta(\vec{\theta})$ and thus $\alpha(\vec{\theta}) \neq \beta(\vec{\theta})$. These normal forms can be computed recursively bottom – up as above in (*). Observe that no δ redex is introduced since each t^1 begins with R. In order to reconstruct $\alpha(\vec{x})$ and $\beta(\vec{x})$ proceed top – down on the results. Find subterms (*) as above with $t^1 < \ >$ free. By choice of m such a subterm is not the trace ([2] pg. 18) of a subterm in $\alpha(\vec{\theta})$ or $\beta(\vec{\theta})$ disjoint from $\vec{\theta}$. Such subterms cannot overlap since their left components have $< \ >$. Now consider any of the pairs $< \ >$ in (*). Such a pair cannot be the trace of a pair $< \ >$ in $\alpha(\vec{\theta})$ or $\beta(\vec{\theta})$ disjoint from $\vec{\theta}$ since the left component of θ_i contains $< \ >$. Thus $(*) = \theta_i t$ as above.

Given $\mu, \nu \in 0 \to 0$ set $\mu^\nu \equiv \lambda x.\ \mu \circ x \circ \nu$.

Proposition 4. If $\alpha, \beta \in \overline{\Lambda\ \delta}\ \delta_1\ \delta_2^{\,0 \to 0}$ and $\alpha \neq_{\beta\eta SP} \beta$ then $\exists\, \mu, \nu\ \ \mu^\nu \alpha = \delta_1\ \ \mu^\nu \beta =_{\beta\eta SP} \delta_2$

Proof. Suppose α, β are normal and $\neq_{\beta\eta SP}$. Again it is convenient to speak as if we are in $\mathcal{M}$.

By δ expansions we can assume α and β have the same Δ. Thus $\exists\mu_1$ s.t., for $\alpha_1 = \mu_1 \circ \alpha$ and $\beta_1 = \mu_1 \circ \beta$, we have $\alpha_1 \neq \beta_1$ and α_1, β_1 are $< \ >$ free. We can also assume that there is no $< \ >$ free γ s.t. $\alpha_1 = \gamma \circ \beta_1$ or $\beta_1 = \gamma \circ \alpha_1$. For suppose $\alpha_1 = \gamma \circ \beta_1$ and $\gamma = \gamma_0 \circ \delta_i$. Then if μ_1 is replaced by $\delta_{3-i} \circ \mu_1$, α_1 is replaced by $\delta_{3-i} \circ \alpha_1$ and β_1 by $\delta_{3-i} \circ \beta_1$. Thus there are $< \ >$ free α_2, β_2 and k, $\ell \geq 0$ such that

$$\alpha_1 \circ < I, I >^k \circ < \delta_2, \delta_1 >^\ell = \alpha_2 \circ \delta_1$$

$$\beta_1 \circ < I, I >^k \circ < \delta_2, \delta_1 >^\ell = \beta_2 \circ \delta_2$$

and there exist n, m ≥ 0 such that

$$\alpha_2 \circ \delta_1 \circ << I, I >^n \circ \delta_1 , < I, I >^m \circ \delta_2 > = \delta_1$$

$$\beta_2 \circ \delta_2 \circ << I, I >^n \circ \delta_1, < I, I >^m \circ \delta_2 > = \delta_2$$

Propositions 2, 3 and 4 yield the following completeness result

<u>Theorem 1.</u> Let M, N $\in \overline{\Lambda \ \delta \ \delta_1 \ \delta_2}^\sigma$ and let $\mathcal{M}$ be any non–trivial model. Then

$$\mathcal{M} \models M = N \Leftrightarrow M \underset{\beta\eta SP}{=} N$$

Let $\Sigma_0 = \left\{< \alpha_1 \circ \delta_1 < \alpha_2 \circ \delta_1 \circ \delta_2 , \alpha_3 \circ \delta_2^2 > > : \alpha_i \in \left\{\delta_1, \delta_2, I\right\} i = 1, 2, 3\right\} \cup$

$\left\{< I, < I, I > >\right\}$

Lemma 1. For any $\alpha_1, \alpha_2, \alpha_3 < \ >$ free $< \alpha_1, < \alpha_2, \alpha_3 > >$ can be generated from Σ_0 by $\circ$.

Proof. First observe recursively that $< \alpha_1 \circ \delta_1, < \alpha_2 \circ \delta_2 \circ \delta_1, \alpha_3 \circ \delta_2^2 > >$ can be generated, for if $\beta_1, \beta_2, \beta_3 \in \{\delta_1, \delta_2, I\}$

$< \alpha_1 \circ \beta_1 \circ \delta_1, < \alpha_2 \circ \beta_2 \circ \delta_1 \circ \delta_2, \alpha_3 \circ \beta_0 \circ \delta_2^2 > > = < \alpha_1 \circ \delta_1, < \alpha_2 \circ \delta_1 \circ \delta_2, \alpha_3 \circ \delta_2^2 > > \ < \beta_1 \circ \delta_1, < \beta_2 \circ \delta_1 \circ \delta_2, \beta_3 \circ \delta_2^2 > >$. Then $< \alpha_1, < \alpha_2, \alpha_3 > > = < \alpha_1 \circ \delta_1, < \delta_2 \circ \delta_1 \circ \delta_2, \alpha_3 \circ \delta_2^2 > > \ \circ \ < I, < I, I > >$.

Let $$\Sigma_1 = \left\{< \alpha_1, < \alpha_2, \alpha_3 > > : \alpha_i < \ > \text{ free } i = 1, 2, 3\right\}$$

Lemma 2. Every α can be generated from Σ_1 by $\circ$

Proof. A derivation is an $\alpha = < < \ldots. < \alpha_1, \alpha_2 > \ldots >, \alpha_n >$ such that $n \geq 3$

1. $\alpha_1 = \delta_1$
2. $\alpha_2 = \delta_2$
3. $\alpha_3 = I$

$$j. \ \exists k, \ell < j \ \ a_j = < a_k, a_\ell > > \wedge \exists k < j \exists \ell$$

$$a_j = \delta_\ell \circ a_k \quad \text{when } j > 3$$

Such an a is said to be a derivation of a_n. Obviously, every β has a derivation. Note that $< < \delta_1, \delta_2 > , I > = < I, I > = < I, < \delta_1, \delta_2 > > \in \Sigma$. Now suppose that a is as above and $\delta_1 \circ a$ can be generated from Σ_1 by $\circ$. Incase, $a_n = < a_k, a_\ell >$ for $k, \ell < n$ we have

$$\alpha = < I, < \delta_2 \circ \delta_1^{n-k}, \delta_2 \circ \delta_1^{n-\ell} > > \circ \delta_1 \circ \alpha$$

(with δ_2 replaced by δ_1 if the corresponding k or ℓ is 1). In case $\alpha_n = \delta_\ell \circ \alpha_k$ for $k < n$ we have

$$\alpha = < I, < \delta_1 \circ \delta_\ell \circ \delta_2 \circ \delta_1^{n-k}, \delta_2 \circ \delta_\ell \circ \delta_2 \circ \delta_1^{n-k} > > \circ \delta_1 \circ \alpha$$

(modified as above if $k = 1$). Thus by induction every derivation can be generated from Σ_1 by $\circ$. In addition $\delta_2 = < \delta_1 \circ \delta_2 < \delta_1 \circ \delta_2 \circ \delta_2, \delta_2^2 \circ \delta_2 > > \in \Sigma_1$. This completes the proof.

We have seen

<u>Proposition 5.</u> $\mathscr{M}$ is finitely generated by Σ_0.

<u>Corollary.</u> $\mathscr{M}$ [x] is finitely generated.

This can be generalized to higher types but we do not do it here.

We close this section with the remark that the wreath product of $\mathscr{M}$ ($\mathscr{M}$ [x]) with number theoretic functions of finite support can be embedded into $\mathscr{M}$ ($\mathscr{M}$ [x]). For suppose $i \longmapsto a_i$ s.t. $\forall n > k$ $a_n = I$ $i = 0, 1, 2, \ldots$ and $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ s.t. $\forall n > \ell\, f(n) = n$. Let $m = \max\{k, l\}$, then the pair $(f, \lambda i\, a_i)$ is represented by

$$< a_0 \circ L \circ R^{f(0)} < \quad < a_m \circ L \circ R^{f(m)}, R^{m+1} > \quad > >$$

A unification problem is an equation $Mx = Nx$ where $M, N \in \overline{\Lambda\ \delta}\ \delta_1\ \delta_2{}^{\sigma \to \tau}$ and $x \in \sigma$. $P \in \overline{\Lambda\ \delta}\ \delta_1\ \delta_2{}^{\sigma}$ is a solution to $Mx = Nx$ if $MP \underset{\beta\eta SP}{=} NP$. $\Sigma \subseteq \overline{\Lambda\ \delta}\ \delta_1\ \delta_2{}^{\sigma}$ is said to be projective if there exists a unification problem, as above, s.t.

$$Q \in \Sigma \Leftrightarrow \exists P \quad \delta PQ \text{ is a solution to}$$
$$Mx = Nx.$$

obviously every projective set is recursively enumerable. Below we shall prove the converse. The proof first consists of solving the Markov – Löb problem ([7] pg. 1) for $\mathscr{M}$ ($\mathscr{M}$ [x]) in the negative. Below we work for the most part in $\mathscr{M}$ ($\mathscr{M}$ [x]).

<u>Lemma 3.</u> $\exists n \ \alpha = R^n \Leftrightarrow R \circ \alpha \quad \alpha \circ R$

<u>Proof.</u> Suppose that $R \circ \alpha = \alpha \circ R$, and α is normal. If α has a non–empty Δ then the Δ of the normal form of $R \circ \alpha$ is smaller but the Δ of the normal form of $\alpha \circ R$ is the same. Thus α is $< \ >$ free and $\alpha = R^n$ for some $n \geq 0$.

Let $\Phi_n = < L \circ L, < L \circ R \circ L, < \ldots < L \circ R^{n-1} \circ L, R > \ldots > > >$.

<u>Lemma 4.</u> $\exists \beta \ \alpha = \beta \circ L \Leftrightarrow \alpha \circ < L, L > = \alpha$.

<u>Proof.</u> $\Longrightarrow$ is proved by induction on the normal form of α.

<u>Lemma 5.</u> $\alpha = \Phi_n \Leftrightarrow R^n \circ \alpha = R \quad \alpha = R \circ \alpha \circ$

$$< < L, L > , < L \circ R^{n-1} \circ L, R > >$$

<u>Proof.</u> $\Longleftarrow$ If $R^n \circ \alpha = R$ we can write $\alpha = < \alpha_1, < \ldots < \alpha_n, R > \ldots > >$ and $R \circ \alpha \circ < < L, L > , < L \circ R^{n-1} \circ L, R > > = < \alpha_2, < \ldots < \alpha_n, R > \ldots > > \circ < < L, L >,$ $< L \circ R^{n-1} \circ L, R > > = < \alpha_2 \circ < < L, L >, < L \circ R^{n-1} \circ L, R > > , < \ldots < \alpha_n \circ$ $< < L, L > , < L \circ R^{n-1} \circ L, R > >, < L \circ R^{n-1} \circ L, R > > \ldots > >$. If this $= \alpha$ then we have $\alpha_n = L \circ R^{n-1} \circ L$ and for $i = 1 \ldots n-1$ $\alpha_i = \alpha_{i+1} \circ < < L, L >, < L \circ R^{n-1} \circ$ $L, R > >$. Thus $\alpha_i = L \circ R^{i-1} \circ L$ and $\alpha = \Phi_n$.

Define $\alpha \in Seq_n \Leftrightarrow \alpha = < \alpha_0 \circ L, < \ldots < \alpha_{n-1} \circ L, R > \ldots > >$, $\Psi_n = \Phi_n \circ < < I, I >,$ $L \circ R^{n-1} >$

Lemma 6. $\alpha \in Seq_n \Leftrightarrow R^n \circ \alpha = R \wedge \Phi_n \circ \alpha = \Phi_n \circ \alpha \circ <L, L>$.

Proof. $\Leftarrow$ If $R^n \circ \alpha = R$ we can write $\alpha = <\beta_0, <\ldots <\beta_{n-1}, R> \ldots>>$ and $\Phi_n \circ \alpha = <\beta_0, <\ldots <\beta_{n-1}, \beta_{n-1}> \ldots>$ In addition, $\Phi_n \circ \alpha \circ <L, L> = <\beta_0 \circ <L, L>, <\ldots <\beta_{n-1} \circ <L, L>, \beta_{n-1} \circ <L, L>> \ldots >>$. If these are $=$ by Lemma 4 $\beta_i = \alpha_i \circ L$ for $i = 1 \ldots n-1$ and $\alpha \in Seq_n$.

Let $\Phi_n (\alpha, \delta) = <\alpha \circ R^{f(0)} \circ L, <\ldots <\alpha \circ R^{f(n-1)} \circ L, R> \ldots >>$ for $f: \mathbb{N} \longrightarrow \mathbb{N}$.

Note that $\Phi_n = \Phi_n (L, id)$. As in Lemma 5

Lemma 7. $\beta = \Phi_n (\alpha, id) \Leftrightarrow \beta \in Seq_n \wedge \beta = R \circ \beta \circ <<L, L>, <\alpha \circ R^{n-1} \circ L, R>>$

Lemma 8. $\exists f\ \alpha = \Phi_n (I, f) \Leftrightarrow \alpha \in Seq_n \wedge \alpha \circ <R, R> = \Phi_n (R \circ L, id) \circ <I, R^n> \circ \alpha$.

Proof. We have $\Phi_n (R \circ L, id) \circ <I, R^n> = <R \circ L, <\ldots <R \circ L \circ R^{n-1}, R^n> \ldots >>$. $\Leftarrow$. If $\alpha \in Seq_n$ we can write $\alpha = <\alpha_0 \circ L, <\ldots <\alpha_{n-1} \circ L, R> \quad >>$ so $\alpha \circ <R, R> = <\alpha_0 \circ R, <\ldots <\alpha_{n-1} \circ R, R> \ldots >>$. In addition $\Phi_n (R \circ L, id) \circ <I, R^{n-1}> \circ \alpha = <R \circ \alpha_0, <\ldots <R \circ \alpha_{n-1}, R> \ldots >>$. If these are $=$ we have for $i = 0, \ldots, n-1$, $R \circ \alpha_i = \alpha_i \circ R$ so, by Lemma 3, $\alpha_i = R^{f(i)}$.

Note here that as in Lemma 5 $\beta = \Phi_n (\alpha, \lambda x\, 0) \Leftrightarrow \beta \in Seq_n \wedge \beta = R \circ \beta \circ <L, <\alpha, R>>$.

Lemma 9. $\beta = \alpha^n \Leftrightarrow \exists \gamma \in Seq_n\ \gamma = R \circ \gamma \circ <\alpha \circ L, <\alpha \circ L, R>> \wedge L \circ \gamma = \beta$.

Proof. Similar to Lemma 5.

Let $X_n (\alpha, f) = <L \circ \alpha \circ R^{f(0)} \circ L, <\ldots <L \circ R^{n-1} \circ \alpha \circ R^{f(n-1)} \circ L, R> \ldots >>$.

Lemma 10. $\beta = X_n (\alpha, id) \Leftrightarrow \exists \gamma_1 \in Seq_n \exists \gamma_2 \in Seq_n 2 \exists \gamma_3$.

1. $\gamma_1 \circ <I, R^n \circ \alpha> = \alpha$
2. $\gamma_2 = R^n \circ \gamma_2 \circ <<L, L>, <\gamma_1 \circ <R^{n-1} \circ L, R>>>$
3. $\exists f\ \gamma_3 = \Phi_n (I, f)$

4. $\gamma_3 = R \circ \gamma_3 \circ << I, I >^{n+1} \circ L, < R^{n^2-1} \circ L, R >>$

5. $\beta = \Phi_n (L^2, id) \circ <L, R^n> \circ \gamma_3 \circ < \gamma_2, R >$

Proof. Let $\alpha = < \alpha_0 < \dots < \alpha_{n-1}, \alpha_n > \dots >> \Longrightarrow$. Let $\gamma_1 = < \alpha_0 \circ L, < \dots < \alpha_{n-1} \circ L, R > \dots >>$ and $\gamma_2 = < \alpha_0 \circ L, < \dots < \alpha_{n-1} \circ L, < \alpha_0 \circ R \circ L, < \dots < \alpha_{n-1} \circ R \circ L, < \dots < \alpha_0 \circ R^{n-1} \circ L, < \dots < \alpha_{n-1} \circ R^{n-1} \circ L, R> \dots >> \dots >> \dots >>> \dots >>$. Then (1) and (2) are satisfied. Set $\gamma_3 = < L, < R^{n+1} \circ L, < \dots < R^{n-1} \circ L, R > \dots >>>$. Then γ_3 satisfies (3) and (4) for $f(0) = 0$ and $f(i + 1) = f(i) + n + 1$ $i = 0, \dots, n - 1$. Set $\gamma_4 = \Phi_n (L^2, id) \circ < L, R^n > \circ \gamma_3$. Then $\gamma_4 = < L^2 \circ L, < L^2 \circ R^{n+1} \circ L, < \dots < L^2 \circ R^{n-1} \circ L, R > \dots >>>$ and $\gamma_4 \circ < \gamma_2, R > = X_n (\alpha, id) \Longleftarrow$. It is easy to see that $\gamma_1, \gamma_2, \gamma_3$ must be as in $\Longrightarrow$.

Lemma 11. $\exists f\, \beta = X_n (\alpha, f) \Leftrightarrow \exists \gamma_1 \exists \gamma_2\, \gamma_1 = X_n (\alpha, id) \wedge \exists f\, \gamma_2 = \Phi_n (I, f) \wedge \beta = \gamma_1 \circ < \gamma_2, R >$.

Proof. Obvious

Given $\alpha = < \alpha_0 < \dots < \alpha_{n-1}, R > \dots >>$ and $\beta = < \beta_0, < \dots < \beta_{n-1}, R > \dots >>$ set $\alpha \otimes \beta = < \alpha_0 \circ \beta_0 < \dots < \alpha_{n-1} \circ \beta_{n-1}, R > \dots >$. We have $\alpha \otimes \beta = X_n (\alpha \circ L, id) \circ < I, R^n > \circ \beta$. In addition, note that $\Phi_n (\alpha, f) = X_n (\Phi_n (\alpha, \lambda x\, 0), f)$.

Let $\alpha \in Perm_n \Leftrightarrow \exists f\, \alpha = \Phi_n (L, f) \wedge f: [0, n - 1] \xrightarrow{\text{permutation}} [0, n - 1]$

Lemma 12. $\alpha \in Perm_n \Leftrightarrow \exists f\, \alpha = \Phi_n (L, f) \wedge \exists m\, (\alpha \circ < I, R^n >)^m = I$.

Proof. Clear

$$\alpha \in Bit_n \underset{df}{\Leftrightarrow} \alpha = < \alpha_0 \circ L, < \dots < \alpha_{n-1} \circ L, R > \dots >> \text{ where } \alpha_i \in \{L, R\}$$

$i = 0, 1, \dots, n - 1$.

Lemma 13. $\alpha \in Bit_n \Leftrightarrow \exists k \exists \ell\; k + \ell = n \wedge \exists \beta \in Perm_n\; \alpha = \beta \circ < I, R^n > \circ \Phi_k (L, \lambda x 0) \circ < I, \Phi_\ell (R, \lambda x\, 0) >$.

Proof. Obvious

Let $a \in String_n \Leftrightarrow a = a_0 \circ \quad \circ a_{n-1}$ where $a_i \in \{L, R\}$ $i = 0, 1, \ldots, n-1$

Lemma 14. $a \in String_n \Leftrightarrow \exists \beta \in Bit_n \; \exists \gamma \in Seq_{n+1} \; a = L \circ \gamma \circ < I, R > \wedge \gamma = (\beta \circ \; < I, R > \circledast R \circ \gamma) \circ < L, < I \circ L, R > >$.

Proof. $\Rightarrow$ Let $\beta = < a_0 \circ L, < \ldots < a_{n-1} \circ L, R > \ldots > >$ and $\gamma = < a_0 \circ \quad \circ a_{n-1} \circ L, < a_1 \circ \ldots \circ a_{n-1} \circ L < \ldots < a_{n-1} \circ L, < I \circ L, R > > \ldots > > >$. $\Leftarrow$. It is easy to see that β and γ must be as above.

If $a = R^m$ we write Binary (a, β) if β is a binary representation of a i.e. $\exists n \; \beta \in String_n$ so $\beta = \beta_{n-1} \circ \quad \circ \beta_o$ with $\beta_i \in \{L, R\}$ and if b_i is defined by

$$b_i = \begin{cases} 1 & \text{if} \quad \beta_i = L \\ 0 & \text{if} \quad \beta_i = R \end{cases}$$

$m = b_{n-1} \, 2^{n-1} + \quad + b_0 \, 2^0$

Lemma 15. Binary $(a, \beta) \Leftrightarrow \exists m \;\; a = R^m \wedge \exists n \;\; \beta \in String_n \;\; \wedge \;\exists \; \gamma_1 \, \gamma_2 \, \gamma_3 \, \gamma_4 \, \gamma_5$.

1. $\gamma_1 \in Bit_n$, $\gamma_2 \in Seq_{n+1}$, $\gamma_3 \in Seq_n$, $\gamma_4 \in Seq_n$, $\gamma_5 \in Seq_{n+1}$
2. $\beta = L \circ \gamma_2 \circ < I, R >$
3. $\gamma_2 = (\gamma \circ < I, R > \circledast R \circ \gamma_2) \circ < L, < I \circ L, R > >$
4. $L \circ R^{n-1} \circ \gamma_3 = R \circ L$
5. $\gamma_3 = (R \circ \gamma_3 \circ < I, R > \circledast \gamma_3) \circ < L, < R \circ L, R > >$
6. $\gamma_3 = \Phi_n \, (L^2, id) \circ < I, R^n > \circ \gamma_4$
7. $\Phi_n \, (I, \lambda x \, 0) = \Phi_n \, (R \circ L, id) \circ < I, R^n > \circ \gamma_4$
8. $\gamma_5 = (((\gamma_3 \circ < I, R > \circledast \gamma_4) \circ < I, R >) \circledast (R \circ \gamma_5)) \circ < L, < I \circ L, R > >$
9. $a = L \circ \gamma_5 \circ < I, I >$

Proof. We do $\Leftarrow$. From this $\Rightarrow$ will become clear. Suppose $\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5$ are given as above. As in the proof of Lemma 14, $\gamma_1 = < \mu_{n-1} \circ L, < \dots < \mu_o \circ L, R > \dots > >$ for $\mu_i \in$ $\{L, R\}$ and $\gamma_2 = < \mu_{n-1} \circ \dots \circ \mu_o\, L < \dots < \mu_o \circ L, < I \circ L, R > > \dots > >$, so $\beta = \mu_{n-1} \circ$ $\circ\, \mu_o$, by (1), (2), and (3). By (1) and (4) $\gamma_3 = < \nu_{n-1} \circ L < \quad < \nu_1 \circ L, < R \circ L, R > >$ $\dots > >$ and by (5) $\nu_{i+1} = \nu_i \circ \nu_i$ for $i = 0 \quad n-2$. Thus $\gamma_3 = < R^2 \circ L, < \dots < R^2 \circ L,$ $< R \circ L, R > > \dots > >$. By (1), (5), and (6) $\gamma_4 = < < R^{2^{n-1}}, I > \circ L, R < \dots < < R, I > \circ$ $L, R > \dots > >$. Thus $\gamma_3 \circ < I, R > \circledast \gamma_4 = < \xi_{n-1} \circ L, < \quad < \xi_o \circ L, R > \quad > >$

where

$$\xi_i = \begin{cases} R^{2^i} & \text{if } \mu_i = L \\ R^o & \text{if } \mu_i = R \end{cases}$$

By (1) and (8) $\gamma_5 = < \xi_{n-1} \circ \dots \circ \xi_o \circ L, < \dots < \xi_o \circ L, < I, R > > \dots > >$. Thus $\alpha = \xi_{n-1} \circ \dots \circ \xi_o =$

$$R^{b_{n-1}2^{n-1} + \quad + b_o 2^o}$$

where b_i is as above.

We shall now give a Gödel numbering of the members of $\mathcal{M}$ ($\mathcal{M}$ [x]) by positive integers. First note that any finitely generated Cartesian monoid can be generated by 2 elements L, θ where $\theta = < R, < \alpha_1, < \dots < \alpha_n, R > \dots > >$. for generators $\alpha_1, \dots, \alpha_n$. Let $m = b_{n-1}\, 2^{n-1} + \quad + b_o$, where $b_i \in \{0, 1\}$ $i = 0 \dots n-2$, and $b_{n-1} = 1$. Then m is the Gödel number of $\beta_{n-1} \circ \dots \circ \beta_o$ where

$$b_i = \begin{cases} L & \text{if } b_i = 1 \\ \theta & \text{if } b_i = 0 \end{cases}$$

Note that every element has at least one Gödel number since $L \circ <I, I> = I$. Write Num $(a, \beta) \Leftrightarrow a = R^m$ and m is a Gödel number of β.

Proposition 6: Num $(a, \beta) \Leftrightarrow \exists m \; a = R^m \wedge \exists n \; \exists \beta_1 \; \beta_1 \in String_n \wedge$ Binary $(a, \beta_1) \exists \gamma_1 \gamma_2$ $\gamma_1 \in Bit_n \wedge \gamma_2 \in String_{n+1} \wedge \beta_1 = L \circ \gamma_2 \circ <I, R> \wedge \gamma_2 = ((\gamma_1 \circ <I, R>) \circledast R \circ \gamma_2) \circ <L,$ $<I \circ L, R>> \exists \gamma_3 \; \gamma_3 = (\gamma_1 \circ <<L, \theta>, R> \circledast R \circ \gamma_3) \circ <L, <I \circ L, R>> \wedge \beta = L \circ \gamma_3$ $\circ <I, I>$

Proof. As in Lemmas 14 and 15.

Let $\Sigma \subseteq \mathcal{M}$ ($\mathcal{M}$ [x]). Σ is said to be Diophantine if $\exists a(x), \beta(x) \in \mathcal{M}[x]$ s.t.

$$\theta \in \Sigma \Leftrightarrow \exists \gamma \in \mathcal{M}(\mathcal{M}[x]) \; a(<\gamma, \theta>) = \beta(<\gamma, \theta>).$$

Obviously, every Diophantine subset of $\mathcal{M}$ ($\mathcal{M}$ [x]) is recursively enumerable. Here we solve the Markov–Löb problem ([7] pg. 1) for $\mathcal{M}$ ($\mathcal{M}$ [x]).

Theorem 2. Every recursively enumerable subset of $\mathcal{M}$ ($\mathcal{M}$ [x]) is Diophantine.

Proof. First observe that there is no ambiguity in the statement of the theorem since the word problem for $\mathcal{M}$ ($\mathcal{M}$ [x]) is decidable (infact, polynomial time). We give the proof for $\mathcal{M}$.

First note that if $\mathcal{S} \subseteq \mathbb{N}$ is RE then $\mathcal{S}' = \{R^n ; n \in \mathcal{S}\}$ is Diophantine. For, by Lemmas 3 and 9, the sets and relations $\{R^n ; n \in \mathbb{N}\}$ $\{(R^n, R^m, R^{n+m}) : n, m \in \mathbb{N}\}$, $\{(R^n, R^m, R^{nm}) : n, m \in \mathbb{N}\}$ are Diophantine. Thus by Matiyasevich's solution to Hilbert's 10th problem ([5] pg [7]) every RE such $\mathcal{S}'$ is Diophantine.

Now if Σ is RE then the set of Gödel numbers of members of Σ is an RE subset of $\mathbb{N}$, say $\mathcal{S}$. Thus $\exists \alpha(x), \beta(x) \in \mathcal{M}[x]$ s.t..

$$\gamma_2 \in \mathcal{S}' \Leftrightarrow \exists \gamma_1 \in \mathcal{M} \; \alpha(<\gamma_1, \gamma_2>) = \beta(<\gamma_1, \gamma_2>)$$

Hence

$$\theta \in \Sigma \Leftrightarrow \exists\, \gamma \in \mathscr{M} \;\; \alpha(\gamma) = \beta(\gamma) \wedge$$
$$\text{Num}\ (\text{R} \circ \gamma,\ \theta).$$

Lemmas 3–15 and Proposition 6 show that the relation Num is Diophantine. Thus Σ is Diophantine.

<u>Corollary.</u> Suppose $\Sigma \subseteq \overline{\Lambda\ \delta}\ \delta_1\ \delta_2^{\ \sigma}$ is $\beta\eta$SP closed and recursively enumerable. Then Σ is projective.

<u>Proof.</u> Let M be as in Proposition 2. The set of $\beta\eta$SP normal forms of terms MNx for $\text{N} \in \Sigma$ generates an RE subset of $\mathscr{M}$ [x], say Σ', so by the theorem $\exists \alpha(\text{x}), \beta(\text{x})$ s.t. $\exists \gamma \in \mathscr{M}$ [x]

$$\alpha(<\gamma,\ \theta>) = \beta(<\gamma,\ \theta>) \;\Leftrightarrow\; \theta \in \Sigma'. \text{ Thus } \text{N} \in \Sigma \;\Leftrightarrow\; \exists \text{P} \in \overline{\Lambda\ \delta}\ \delta_1\ \delta_2^{(0 \to 0) \to (0 \to 0)}$$
$$\lambda \text{x}\ \alpha(<\text{Px},\ \text{MNx}>) = \lambda \text{x}\ \beta(<\text{Px},\ \text{MNx}>)$$

REFERENCES:

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

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

[3] Koymans, Models of the lambda calculus, Dissertation Univ. Utrecht Math. 1984.

[4] Lambek, From λ–calculus to Cartesian closed categories, Curry Festschrift, hindley & Seldin eds Academic Press 1980 pgs. 375–402.

[5] Matiyasevich, Diophantine representation of recursively enumerable predicates, 2nd Scandinavian Logic Symposium, Fenstad ed. North Holland 1971 pgs. 171–178.

[6] Pottinger, The Church–Rosser theorem for the typed λ calculus with extensional pairing, CMU Dept. of History & Philosophy Tech. Report 1979.

[7] Siekmann, Universal unification, 7th CAD, Shostak ed. LNICS 170 Springer–Verlag 1984 pgs. 1–42.

[8] Scott, Relating theories of the λ–claculus, Curry Festschrift, Hindley & Seldin eds. Academic Press 1980 pgs. 403–450.

[9] Statman, On the existence of closed terms in the typed λ calculus I, Curry Festschrift, Hindley & Seldin eds. Academic Press 1980 pgs. 511–534.

[10] Statman, Freyd's hierarchy of combinator monoids, 6th LICS IEEE 1991 pgs. 186–190.