On Cartesian Monoids[*]

Rick Statman[†]
Department of Mathematical Sciences
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

A Cartesian monoid is a structure $(M, *, I, L, R, (<>))$ where $(M, *, I)$ is a monoid with L and R members of M and $\langle\rangle : M^2 \to M$ s.t.

$$L * \langle x, y\rangle = x$$

$$R * \langle x, y\rangle = x$$

$$\langle x, y\rangle * z = \langle x * z, y * z\rangle$$

$$\langle L, R\rangle = I.$$

Cartesian monoids are easy to come by. Any surjective pairing function lifts pointwise to a $\langle\rangle$ on the monoid M of all functions under composition with L and R the lifted projections. Cartesian monoids were first introduced by Dana Scott in [5] and independently by Lambek in [3]. We first learned about them from Dana and Peter Freyd. There are many connections to the lambda calculus. First, the connection to simply typed lambda calculus with surjective pairing is transparent and forms the basis for [7]. Second, such monoids always contain a copy of the Freyd-Heller group (see below) thus there is a further connection to lambda calculus ([6], [10]). Finally, such monoids come up in the study of type algebras especially in connection to Curry's subject reduction theorem ([8], [9]).

It is the purpose of this paper to collect in one place our observations on Cartesian monoids, especially the free Cartesian monoid, which are useful for applications to lambda calculus. In particular, we shall derive the undecidability of the matching and unification problems for F (in a very strong form). Our approach is to treat the free Cartesian monoid as an algebraic structure of the sort that we learned about in school. This is not to say that we have any argument with the category theoretic approach; it is only to say that we are not competent to carry out that approach. We shall now summarize our principal results.

In 2, we show that the free Cartesian monoid F is simple and has no non-trivial homomorphisms (it follows from this that the simply typed lambda calculus with surjective pairing is complete ([7])). Also in 2, we show that F is finitely generated (this is a key fact in the results that follow on unification). In 3, we consider the group G of F and the submonoid H of right invertible elements. We give simple syntactic characterizations

[*] Supported in part by the National Science Foundation, CCR-9201893

[†] The author would like to thank the referee for numerous helpful suggestions, several illuminating comments, and a few critical demands which significantly improved the paper.

of membership in G and H, and in addition, useful generators for G. In the process we locate the Freyd-Heller group as (anti isomorphic to) a subgroup of G. Also in 3, we observe that the wreath product of the number theoretic functions of finite support with F is embeddable in F. This construction is the basis for all of the recursion theoretic results proved below. In 4, we give a simple representation theorem for F in the spirit of the one for the Freyd-Heller group in [1]. The members of F are represented faithfully as the piecewise shift operators on Cantor space (again the representation is an anti isomorphism). The Freyd-Heller group turns up as the subgroup of order-preserving homeomorphisms. These observations are not used elsewhere but we think that they are of independent interest. In 5, we generalize many of the above results to the polynomial monoid $F[x]$. In particular, we show that it is separable. Moving to $F[x]$ permits the generalization of the results for F to all higher types in the lambda calculus (via the theory of reducibility; see [7]). In 6, we embed the non-negative integers into F and conclude the undecidability of the matching problem for F. In particular, it is proved that every RE subset of H is the projection of the set of solutions to a matching problem in F. In 7, we show that every finitely generated submonoid of F is the projection of the set of solutions to a unification problem in F. Finally in 7, we conclude that every RE subset of F is the projection of the set of solutions to a unification problem in F. This is done by Gödel numbering using 6 and 7.

1 Cartesian Monoids

A Cartesian monoid is a structure $C = (M, *, I, L, R, \langle\rangle)$ where $(M, *, I)$ is a monoid, that is

$$(x^* (y^* z)) = ((x^* y)^* z)$$

and

$$x^* I = I^* x = x$$

where, since * is associative, we omit parentheses when it causes no confusion and with

$$L \in M \text{ and } R \in M \qquad \langle\rangle : M^2 \rightarrow M, \text{ and}$$

$$L * \langle x, y\rangle = x$$

$$R * \langle x, y\rangle = y$$

$$\langle x, y\rangle * z = \langle x * z, y * z\rangle$$

$$\langle L, R\rangle = I.$$

These axioms insure that a Cartesian monoid is a monoid with a surjective pairing function $\langle , \rangle : M^2 \rightarrow M$. The last axiom insures surjectivity since $x = I^* x = \langle L, R\rangle^* x = \langle L^* x, R^* x\rangle$ and conversely if $\langle , \rangle$ is surjective then, for any x, $I^* x = x = \langle L, R\rangle^* x$ and in particular for $x = I$ we have $I = \langle L, R\rangle$.

The next to the last axiom expresses that we expect the pairing to be lifted pointwise to the monoid of functions from a pairing function on a set; viz, lifted to satisfy $\langle f,g\rangle = \lambda x.\langle f(x),g(x)\rangle$.

Cartesian monoids were first introduced by Dana Scott in [6], and independently by J. Lambek in [4].

A typical example is the monoid of all number theoretic functions $f:\mathbf{N}\to\mathbf{N}$ equipped as follows. Consider the (modified) Cantor diagonal pairing function $[,]:\mathbf{N}^2\to\mathbf{N}$ defined by $[x,y] = ((x+y+1)(x+y+2)/2)+(y+1)$ which traverses the lattice points of the first quadrant by traversing the lines $y=-x+b$ for $b=0,1,2\ldots$ from $x=b$ to $x=0$. The function $[,]$ is clearly a surjective pairing of natural numbers and thus has inverses $l:\mathbf{N}\to\mathbf{N}$ and $r:\mathbf{N}\to\mathbf{N}$. Now we define the Cartesian structure on the monoid of functions by

$$\langle f,g\rangle = \lambda x.[f(x),g(x)]$$

$$L = l$$

and

$$R = r.$$

Another example is the free Cartesian moind F defined as follows. The objects of the monoid F are the congruence classes of the closed (variable free) monoid expressions determined by the congruence generated by the axioms above. That is two expressions are congruent if and only if they are equal in all Cartesian monoids (equivalently, are provably equal from the axioms above). This congruence will be analyzed below in Section 2. The operations on the monoid are defined pointwise as follows: where, for expressions e, the congruence class of e is denoted e/F.

$$I = I/F$$

$$f/F^{*}g/F = (f^{*}g)/F$$

$$L = L/F$$

$$R = R/F$$

and

$$\langle f/F, g/F\rangle = \langle f,g\rangle/F.$$

It is a well known exercise of universal algebra to show that these definitions have all the desired properties (see below).

The Cartesian monoid polynomials are the Cartesian monoid expressions possibly containing free variables. We write $f = f(x1,\ldots,xn)$ if the polynomial f contains at most the variables (indeterminates) $x1,\ldots,xn$. Here we define the matching and unification problems.

The Unification Problem:

Given polynomials $f(x1,\ldots,xn)$ and $g(x1,\ldots,xn)$ decide if there are closed $h1,\ldots,hn$ such that in all Cartesian monoids (equivalently in F)

$$f\,(h1,\ldots,hn) = g\,(h1,\ldots,hn)\,.$$

The Matching Problem:

Given a polynomial $f\,(x1,\ldots,xn)$ and a closed expression g decide if there are closed $h1,\ldots,hn$ such that in all Cartesian monoids (equivalently in F)

$$f\,(h1,\ldots,hn) = g.$$

Below we shall use the word *expression* to mean *closed expression* except when we explicitly say otherwise (as in Section 5).

The reader should consult [8] for a detailed explanation of the connection to the simply typed lambda calculus.

2 Normal Forms

Each expression can be rewritten uniquely in a normal form consisting of a binary tree whose nodes correspond to applications of $\langle\rangle$, with strings of L's and R's joined by $*$, at its leaves (here I counts as the empty string) and with no subexpression of the form $\langle L*x, R*x\rangle$. This is accomplished by considering the equivalent rewrite system

$$\begin{gathered} L*\langle x,y\rangle \longrightarrow x \\ R*\langle x,y\rangle \longrightarrow y \\ \langle x,y\rangle * z \longrightarrow \langle x*z, y*z\rangle \\ \langle L*x, R*x\rangle \longrightarrow x \\ \langle L,R\rangle \longrightarrow I \\ I*x \longrightarrow x \\ x*I \longrightarrow x \end{gathered}$$

modulo the associativity axioms. This rewrite system is equivalent to the axioms in the sense that the smallest associative congruence containing the rules as identities is the congruence generated by the axioms. Note that the rewrite system is not left linear; however, it is strongly normalizing and Church-Rosser. This rewrite system is strongly normalizing because we can interpret it in the integers with rewrites decreasing as follows

$$L = R = I = 2$$

$$\begin{gathered} x*y = x \text{ multiplied by } y \\ \langle x,y\rangle = x+y+1. \end{gathered}$$

The rewrite system is obviously weakly Church-Rosser therefore, by König's lemma, it is Church-Rosser. The binary tree of a given expression is called its diagram. Diagrams D have the above described shape. Almost every thing that follows depends on this. We shall make two immediate applications. The first concerns homomorphisms.

For any two members of F, f and g, define $f^g : M \longrightarrow M$ by $f^g(x) = f * x * g$ (i.e., conjugation). Given any two distinct normal forms $h1$ and $h2$ there exist f and g such that $f^g(h1) = L$ and $f^g(h2) = R$. This can be seen as follows. We can first assume that $h1$ and $h2$ have the same D by expansions of the form $x \longleftarrow \langle L * x, R * x\rangle$ or $I \longleftarrow \langle L, R\rangle$. Indeed in this way normal expressions can be transformed into various shapes such as one where the binary tree is complete of all strings have the same length. Thus, there is an f such that $f * hl = / = f * h2$, and both of these reeduce to $\langle\rangle$-free $h3$ and $h4$ and integers k and l such that

$$f * h1 * \langle I, I\rangle^k * \langle R, L\rangle^l = h3 * L \text{ and}$$

$$f * h2 * \langle I, I\rangle^k * \langle R, L\rangle^l = h4 * R \text{ and}$$

there exist integers n and m such that

$$h3 * L * \langle \langle I, I\rangle^n * L, \langle I, I\rangle^m * R\rangle = L \text{ and}$$

$$h4 * R * \langle \langle I, I\rangle^n * L, \langle I, I\rangle^m * R\rangle = R.$$

Thus we can set

$$g = \langle I, I\rangle^k * \langle R, L\rangle^l * \langle \langle I, I\rangle^n * L, \langle I, I\rangle^m * R\rangle.$$

We conclude that there are no non-trivial homomorphisms of F. Since F is the free Cartesian monoid it follows that every Cartesian monoid contains a natural copy of F. In particular, this implies the completeness of the simply typed calculus with surjective pairing (see [8]). The next application concerns the finite generation of F.

The monoid F is finitely generated. We see this as follows. Let

$$S = \{\langle X * L, \langle Y * L * R, Z * R * R\rangle\rangle : X, Y, Z \in \{L, R, I\}\} \; U \{\langle I, \langle I, I\rangle\rangle\}.$$

Now for any f, g, h $\langle\rangle$-free strings of L's and R's the element $\langle f \langle g, h\rangle\rangle$ can be generated from S by a simple recursive procedure. Now say that f is a derivation if it has the form $\langle\langle \ldots \langle f1, f2\rangle \ldots\rangle, fn\rangle$ for $n > 2$ such that

$$f1 = L$$

$$f2 = R$$

$$f3 = I \text{ and for } j > 3$$

$$\begin{aligned} fj &= \langle fk, fl\rangle && \text{for some } k, l < j \text{ or} \\ &= L * fk && \text{for some } k < j \text{ or} \\ &= R * fk && \text{for some } k < j. \end{aligned}$$

It is easy to see that every derivation can be generated from S using the previous observation. It follows that all of F is generated from S. Any Cartesian monoid which if finitely generated by $f1, \ldots, fn$ is generated by two elements $e0 = \langle R, \langle f1, \langle \ldots \langle fn, R \rangle \ldots \rangle \rangle \rangle$ and $e1 = L$. For F we denote $e0$ by E.

3 The Group

Let H be the submonoid of right invertible elements. That is f belongs to H if and only if there exists a g such that $f^*g = I$. Let G be the group of (doubly) invertible elements of F. That is f belongs to G if and only if there exist $g1$ and $g2$ such that $f^*g1 = g2^*1 = I$.

Evidently if $g1$ and $g2$ exist then they are equal.

Our goal is to prove several useful lemmas about H and G such as the following. f belongs to H if and only if, some $g, \langle f, g \rangle$ belongs to G. Clearly L and R belong to H. If we begin with f in normal form then it is easy to see that $f \in H$ $\langle = \rangle$ f can be expanded so that all of its strings at the leaves have the same length and none occurs more than once. f has left inverse $\langle = \rangle$ f can be expanded so that all of its strings have the same length n and each of 2^n strings of this length occurs at least once. The reader should compare this to the beta-eta group presented in [1] page 530.

It follows that $H = L * G = R * G$. Let

$$Bn = \langle L, \langle \ldots \langle L * R^{n-1}, \langle L * L * R^n, \langle R * L * R^n, R^{n+1} \rangle \rangle \rangle \ldots \rangle \rangle$$

$$C0 = \langle R, L \rangle$$

$$Cn + 1 = \langle L, \langle \ldots \langle L * R^{n-1} \langle L * R^{n+1} \langle L * R^n, R^{n+2} \rangle \rangle \rangle \ldots \rangle \rangle .$$

Clearly, both Bn and Cn are invertible and the set of all of them generate G. Indeed observe that if $n < m$ then

$$Bn * Bm = Bm + 1 * Bn.$$

The group generated by the Bn alone is (anti)isomorphic to the Freyd-Heller group [2]. It is generated by $B0$ and $B1$ as a group. Thus, it is easy to see that G is generated by $B0, B1, C0$, and $C1$ as a group.

Let J be the monoid of all number theoretic functions of finite support so that $s : N \longrightarrow N$ belongs to J if there exists n such that for $m > n$ $s(m) = m$. Suppose that $t : N \longrightarrow F$ so that for $m > k$, $t(m) = I$ and s and n are as above; let $l = \max \{n, k\}$, then the pair (t, s) can be represented by

$$\left\langle t(0) * L * R^{s(0)}, \left\langle \ldots \left\langle t(l) * L * R^{s(l)}, R^{l+1} \right\rangle \ldots \right\rangle \right\rangle .$$

This representation gives an embedding of the wreath product of F with J into F (this should be compared to [2]T6).

4 Representation

In [2] the authors give a faithful representation of the Freyd-Heller group in the continuous order preserving permutations of the real numbers. Here we will generalize a modified such representation to F. Let CS be Cantor space, here construed as the product of $\{0,1\}$, endowed with the discrete topology, along N. The properties of CS are very well known; in particular, CS is a totally disconnected compact Hausdorf space. Among the continuous open mappings $A : CS \rightarrow CS$ are the shift operators Z and O defined by

$$Z(f)(0) = 0 \qquad O(f)(0) = 1$$

$$Z(f)(n+1) = f(n) \qquad O(f)(n+1) = f(n)$$

We simply write $0f$ for $Z(f)$ and $1f$ for $O(f)$. If C is a collection of mappings $A : CS \rightarrow CS$ we let piecewise C be the closure of C under the following kind of definition of A by cases from A' and A''

$$\begin{aligned} A(0f) &= A'(f) \\ A(1f) &= A''(f). \end{aligned}$$

Indeed, if all C mappings are continuous and open then so are all piecewise C mappings. The piecewise shift operators A can be explicitly characterized by the following condition:

Whenever $A(f) = g$ there exists basic open neighborhoods $(f(0), \ldots, f(r))$ and $(g(0), \ldots, g(s))$ containing resp f and g such that for any $t > s$ $g(t) = f(t - s + r)$.

We define a Cartesian monoid structure on the piecewise shift operators as follows:

$$I = I$$

$$L = Z$$

$$R = O$$

$$x * y = \text{the composition } z \mapsto y(x(z))$$

$$\langle x, y\rangle (f) = \begin{cases} x(f) & \text{if } f(0) = 0 \\ y(f) & \text{if } f(0) = 1. \end{cases}$$

It is not difficult to see that this Cartesian monoid is isomorphic to F. Now let us order the members of CS lexicographically and let $G+$ be the order preserving members of G (under this isomorphism). Then $G+$ is precisely the Freyd-Heller group. For, if A is a member of $G+$ then by 5 above; A can be given by an expression all of whose strings have the same length n such that all 2^n strings of this length occur exactly once. Since A is order preserving these strings must occur in lexicographic order when viewed from left to right. Thus, the expression for A can be generated by the Bn and their inverses alone.

The converse is obvious.

5 The Polynomial Monoid $F[x]$

All of the principal results mentioned above for F hold as well for $F[x]$. More generally, if $f(x)$ and $g(x)$ are distinct normal expressions then there exists an $h \in F$ such that $f(h) = / = g(h)$. Indeed, if $f(x1, \ldots, xn)$ and $g(x1, \ldots, xn)$ are distinct normal expressions in $F[x1, \ldots, xn]$ then we shall find $h1, \ldots, hn$ such that $f(h1, \ldots, hn) = / = g(h1, \ldots, hn)$. The construction takes two steps. In the first step n may be increased. We remove subexpressions of the form $L{*}xi{*}h$ and $R{*}xi{*}h$ (for h possibly empty) by making substitutions $xi \leftarrow \langle y, z\rangle$ and re-normalizing. It is easy to see that this process terminates and that the original f and g are recoverable by the substitutions $y \leftarrow L * xi$ and $z \leftarrow R * xi$. Thus, we can assume that the first step is completed and f and g are normal, distinct, and have no subexpressions of the above forms. Indeed, expressions like this can be recursively generated as a string of xi's followed by a string of L's and R's or a string of xi's followed by a single $\langle\rangle$ of expressions of the same form. Given such an expression e, if we evaluate each xi, L, and R as $1, \langle\rangle$ as max, and $*$ as $+$, then the result is a positive integer $\#e$ (the "length of the longest path in e"). Let $m = \max\{\#f, \#g\} + 1$, and $k = m(m + n + 1)$. For each positive integer i set

$$hi \;=\; \left\langle \left\langle \underbrace{R^k, \langle \ldots \langle R^k}_{m+i}, I\rangle \ldots \rangle \right\rangle, R^k \right\rangle .$$

We shall show that both $f(x1, \ldots, xn)$ and $g(x1, \ldots, xn)$ are reconstructible from the normal forms of $f(h1, \ldots, hn)$ and $g(h1, \ldots, hn)$ respectively and thus, $f(h1, \ldots, hn) = / = g(h1, \ldots, hn)$. Toward this end note that if t is a normal expression for a member of F and $\#t < k$ then $hi * t = e = df$

$$\left\langle \left\langle \underbrace{t', \langle \ldots \langle t'}_{m+i}, t\rangle \ldots t' \right\rangle \right\rangle$$

where t' is $\langle\rangle$-free and $\#e < \#t{+}m{+}n{+}2$. Now consider either $f(h1, \ldots, hn)$ or $g(h1, \ldots, hn)$. The normal form of this expression can be computed recursively bottom-up as in the computation of e from $hi * t$ above. Observe that no subexpression of the form $\langle L * h, R * h\rangle$ or $\langle L, R\rangle$ is introduced since each t' begins with R. In order to reconstruct, say, $f(x1, \ldots, xn)$ proceed top-down to find subterms e as above with t' $\langle\rangle$-free. By choice of m such a subterm is not the "trace" ([3] pg. 18) of a subterm of $f(h1, \ldots, hn)$ disjoint from the hi. Such subterms cannot overlap because their left components have $\langle\rangle$. Finally, consider any of the pairs $\langle\rangle$ in e. Such a pair cannot be the trace of a pair in $f(h1, \ldots, hn)$ disjoint from the hi since the left component of hi contains $\langle\rangle$. Thus, $e = hi * t$ as above.

6 Integers in F

Let $Int = \{R^n : n = 0, 1, \ldots\}$ with $n = R^n$.

1. $f \in Int \ \langle = \rangle\ f * R = R * f$.

   Indeed, if $f * R = R * f$ then, taking f in normal form, f cannot have a nontrivial D. Thus, f is a string of L's and R's.

2. $f \in F * L \ \langle = \rangle\ f * \langle L, L \rangle = f$

   $f \in F * R \ \langle = \rangle\ f * \langle R, R \rangle = f$

   These can be proved by induction on normal forms.

3. We say that f is an n-sequence if f has the form $\langle f0 * L, \langle f1 * L, \langle \ldots \langle fn - 1 * L, R \rangle \ldots \rangle \rangle \rangle$. For $f \in H$ we have f is an n-sequence $\langle = \rangle\ R^n * f = R$. This can be easily seen from paragraph (5).

4. Define

   $\text{Copy}(f, n) = \left\langle f * L, \left\langle f * R * L, \left\langle \ldots \left\langle f * R^{n-1} * L, R \right\rangle \ldots \right\rangle \right\rangle \right\rangle.$

   $\text{Iterate}(f, n) = \left\langle f^n * L, \left\langle f^{n-1} * L * R, \left\langle \ldots \left\langle f * L * R^{n-1}, R^n \right\rangle \ldots \right\rangle \right\rangle \right\rangle.$

   These are related in the following way:

   $g = \text{Copy}(f, n)\ \langle = \rangle\ g$ is an n-sequence and
   $g = R * g * \left\langle \langle L, L \rangle, < f * R^{n-1} * L, R \right\rangle$

   $g = \text{Iterate}(f, n)\ \langle = \rangle\ g = \text{Copy}(f * L) * \langle I, R^n \rangle * R * g * \left\langle I, \left\langle f * L * R^{n-1}, R^n \right\rangle \right\rangle.$

   Moreover, if $f \in H$ then $\text{Copy}(f * L, n) \in H$ and $\text{Iterate}(f, n) \in H$. Finally,

   $$g = f^n \ \langle = \rangle\ g = L * \text{Iterate}\,(f, n) * \langle I, I \rangle.$$

   Now it follows from paragraph (5) and (i), (ii), and (iii) above that for any Diophantine set S of integers there exists an F polynomial $f\,(x, y)$ and $g \in F$ such that $n \in S\ \langle = \rangle$ there exists h, t such that

   $$\langle f, h \rangle * t = I \text{ and } t * \langle f, h \rangle = I$$

   and

   $$\langle g, h \rangle * t = I \text{ and } t * \langle g, h \rangle = I.$$

   Thus, by the famous theorem of Matiyasevich ([5]), the matching problem for F is unsolvable. With a bit more work it can be shown that every *RE* subset of H is the set of projections of such a matching problem. We do not believe that this extends to the whold of F. In particular, we conjecture that the set of simplicies $\{\langle I, I \rangle^n \mid n \text{ a natural no.}\}$ is not the projection of a matching problem. Indeed, it can be shown that if the set of simplicies is the projection of a matching problem then every *RE* subset of F is the set of projections of a matching problem.

7 Finitely Generated Submonoids

We shall next show that any finitely generated submonoid of F is the set of projections of an F unification problem. This requires some definitions.

First, we want to characterize n-sequences for f not in H. Let $\mathrm{Copy}(n) = \mathrm{Copy}(L, n)$, then

$$f = \mathrm{Copy}\,(n) \; \langle = \rangle \; R^n * f = R \text{ and } f = R * f * \left\langle \langle L, L\rangle, \left\langle L * R^{n-1} * L, R \right\rangle \right\rangle$$

and f is an n-sequence $\langle = \rangle$ $R^n * f = R$ and

$$\mathrm{Copy}\,(n) * \left\langle I, L * R^{n-1} * f \right\rangle = \mathrm{Copy}\,(n) * \left\langle I, L * R^{n-1} \right\rangle * f * \langle L, L\rangle .$$

Consider the first biconditional. The direction $\Leftarrow$ can be seen as follows. If $R^n * f = R$ we can write $f = \langle f1, \langle f2, \langle \ldots \langle fn, R\rangle \ldots \rangle\rangle\rangle$, and we can compute

$$R * f * \left\langle \langle L, L\rangle, \left\langle L * R^{n-1} * L, R \right\rangle \right\rangle = \left\{ f2 * \left\langle \langle L, L\rangle, \left\langle L * R^{n-1} * L, R \right\rangle \right\rangle , \right.$$

$$\left. \left\langle \ldots \left\langle fn * \left\langle \langle L, L\rangle, \left\langle L * R^{n-1} * L, R \right\rangle \right\rangle, \left\langle L * R^{n-1} * L, R \right\rangle \right\rangle \ldots \right\rangle \right\} .$$

If this $= f$ then for $i = 1, \ldots, n-1$ $fi = fi+1 * \left\langle \langle L, L\rangle, \left\langle L * R^{n-1} * L, R \right\rangle \right\rangle$ and $fn = L * R^{n-1} * L$. Thus, $fi = L * R^{i-1} * L$ and $f = \mathrm{Copy}(n)$. The direction $\Rightarrow$ is obvious. The second biconditional is proved similarly. As above

$$g = f^n \, \langle = \rangle \, g = L * \text{ Iterate}\,(f, n) * \langle I, I\rangle .$$

If $s : N \rightarrow N$ let

$$\mathrm{Copy}\,(f, s, n) = \left\langle f * R^{s(0)} * L, \left\langle \ldots \left\langle f * R^{s(n-1)} * L, R \right\rangle \ldots \right\rangle \right\rangle$$

so $\mathrm{Copy}(f, n) = \mathrm{Copy}(f,$ identity, $n)$. In addition, let

$$\mathrm{Comp}\,(f, s, n) = \left\langle L * f * R^{s(0)} * L, \left\langle \ldots \left\langle L * R^{n-1} * f * R^{s(n-1)} * L, R \right\rangle \ldots \right\rangle \right\rangle .$$

The point of these definitions is that Comp can be expressed in terms of Copy and Comp effects multi-ary compositions. Indeed for $f = \langle f0, \langle \ldots \langle fn-1, R\rangle \ldots \rangle\rangle$ and $g = \langle g0, \langle \ldots \langle gn-1, R\rangle \ldots \rangle\rangle$ define $f \# g = \langle f0 * g0, \langle \ldots \langle fn-1 * gn-1, R\rangle \ldots \rangle\rangle$. Then $f \# g = \mathrm{Comp}(f * L,$ identity, $n) * \langle I, R^n\rangle * g$.

1. There exists s such that $g = \mathrm{Copy}\;(I, s, n)$ if and only if g is an n-sequence

   and $g * \langle R, R\rangle = \mathrm{Copy}(R * L,$ identity, $n) * \langle I, R^n\rangle * g$.

   For $\Leftarrow$, if $g = \langle g0 * L, \langle \ldots \langle gn-1 * L, R\rangle \ldots \rangle\rangle$ we compute $\mathrm{Copy}(R * L,$ identity, $n) * \langle I, R^n g\rangle = \langle R * g0, \langle \ldots \langle R * gn-1, R\rangle \ldots \rangle\rangle$, $g * \langle R, R\rangle = \langle g0 * R, \langle \ldots \langle gn-1 * R, R\rangle \ldots \rangle\rangle$, and if these are equal we have for each $i = 0, \ldots, n-1$, $R * gi = gi * R$. Thus, by paragraph 8 (i) there is an s such that $gi = R^{s(i)}$.

2. $g =$ Comp$(f,$ identity, $n)$ iff and only if there exist $h1, h2, h3$ such that

   a) $h1$ is an n-sequence.

   b) $h2$ is an n^2-sequence.

   c) there exists an s such that $h3 =$ Copy(I, s, n).

   d) $f = h1 * \langle I, R^n * f\rangle$.

   e) $h2 = R^n * h2 * \left\langle \langle L, L\rangle, h1 * \left\langle R^{n-1} * L, R\right\rangle\right\rangle$.

   f) $h3 = R * h3 * \left\langle \langle I, I\rangle^{n+1} * L, \left\langle R^{(n^2-1)} * L, R\right\rangle\right\rangle$.

   g) $g =$ Copy$(L * L,$ identity, $n) * \langle L, R^n\rangle * h3 * \langle h2, R\rangle$.

   For $\Rightarrow$ suppose that $f = \langle f0, \langle \ldots \langle fn-1, fn\rangle \ldots\rangle\rangle$. Let

$$h1 = \langle f0 * L, \langle \ldots \langle fn - 1 * L, R\rangle \ldots\rangle\rangle$$

   so a) and d) are satisfied. Let

$$h2 = \left\langle f0 * L, \left\langle \ldots \left\langle fn - 1 * L, \left\langle f0 * R * L, \left\langle \ldots \left\langle f^{n-1} * R * L, \right.\right.\right.\right.\right.\right.$$

$$\left\langle \ldots \left\langle f0 * R^{n-1} * L, \left\langle \ldots \left\langle fn - 1 * R^{n-1} * L, R\right\rangle \ldots\right\rangle\right\rangle \ldots\right\rangle\right\rangle \ldots\right\rangle\right\rangle\right\rangle \ldots\right\rangle\right\rangle$$

   so b) and e) are satisfied. Finally, we put

$$h3 = \left\langle L, \left\langle R^{n+1} * L, \left\langle R^{2n+2} * L, \left\langle \ldots \left\langle R^{n^2-1} * L, R\right\rangle \ldots\right\rangle\right\rangle\right\rangle\right\rangle$$

   so c) is satisfied by the function s defined by $s(i) = i(n+1)$, and f) and g) are satisfied as well. For $\Leftarrow$ it is easy to argue that $h1, h2$ and $h3$ satisfying a) – g) must be as above in $\Rightarrow$.

3. There exists an s such that $g =$ Comp$(f,$ identity, $n) * \langle$Copy$(I, s, n), R\rangle$. Now suppose that $f1, \ldots, fk$ are given. We will express membership in the submonoid generated by $f1, \ldots, fk$. Let $Fit(n) =$ $\{f : f = \langle fs(1) * L, \langle \ldots \langle fs(n) * L, R\rangle \ldots\rangle\rangle$ for some $s : [1, n] \rightarrow [1, k]\}$. We say that f is an n-permutation if $f =$ Copy(L, s, n) for some permutation $s : [0, n-1] \rightarrow [0, n-1]$. It should be clear that

4. f is an n-permutation if and only if there exists s and m such that $f =$Copy(L, s, n) and $(f * \langle R^n\rangle)^m = I$.

$f \in$Fit(n) $\langle=\rangle$ there exist integers $m(1), \ldots, m(k)$ such that $m(1) + \ldots + m(k) = n$ and there exists g such that g is an n-permutation and

$$f = g * \langle I, R^n\rangle * \text{ Copy}(f1, \text{ zero}, m(1)) * \ldots *$$

$$\text{Copy}(fk, \text{ zero, m}(k))^{\cdot}.$$

Finally, we conclude that f belongs to the submonoid generated by $f1, \ldots, fk$ if and only if there is an n such that there exists an $n+1$-sequence h and g $\in$Fit(n) with $f = L * h * \langle I, R\rangle$ and $h = (g * \langle I, R\rangle \# (R * h)) * \langle L, \langle I * L, R\rangle\rangle$. In particular, the members of the submonoid generated by $f1, \ldots, fk$

are the projections of solutions to the above unification problem. When $f1 = L$ and $f2 = R$ we write Bit(n) for Fit(n), and "n-string" for "$a\,\langle\rangle$-free string of L's and R's of length n."

We define Binary(f, g) $\langle=\rangle$ for some $m, f = R^m$ and g is a $\langle\rangle$-free string of L's and R's such that if $b\,(i)$ is defined by

$$b\,(i) = \begin{cases} 1 \text{ if the } i^{\text{th}} \text{ element of } g \text{ is } L \\ \\ 0 \text{ if the } i^{\text{th}} \text{ element of } g \text{ is } R \end{cases}$$

when g is read from right to left and $i = 0, 1, \ldots, n-1$ then

$$m = (b\,(n-1))\,2^{n-1} + \ldots + (b\,(1))\,2 + b\,(0)\,.$$

We assign to each member of F a non-unique Gödel number as follows. Let $f = e\,(ik) * \ldots * e\,(i1)$ as in the last sentence of paragraph 2 and let m be as above (in binary) such that $b\,(j) = 0 \Leftrightarrow ij = 0$ and b$(j) = 1 \Leftrightarrow ij = 1$; then m is a Gödel number of f provided $b\,(n-1) = 1$. We can do the same with $F\,[x]$. Every member of $F\,(F\,[x])$ has a Gödel number since $L * \langle I, I\rangle = I$. The following are the key facts.

1. Binary$(f, g) \Leftrightarrow$ there are integers m and n and $h1, h2, h3, h4, h5$ such that

   i. $h1$ $\in$Bit(n)
   ii. $h2$ is an $n+1$-sequence
   iii. $h3$ is an n-sequence
   iv. $h4$ is an n-sequence
   v. $h5$ is an $n+1$-sequence
   vi. $g = L * h2 * \langle I, R\rangle$
   vii. $h2 = ((h1 * \langle I, R\rangle) \# (R * h2)) * \langle L, \langle I * L, R\rangle\rangle$
   viii. $L * R^{n-1} * h3 = R * L$
   ix. $h3 = ((R * h3 * \langle I, R\rangle) \# h3) * \langle L, \langle R * L, R\rangle\rangle$
   x. $h3 =$ Copy$(L * L,$ identity, $n) * \langle I, R^n\rangle * h4$
   xi. Copy$(I,$ zero, n$) =$ Copy$(R * L,$ identity, $n) * \langle I, R^n\rangle * h4$
   xii. $h5 = ((((h3 * \langle I, R\rangle) \# h4) * \langle I, R\rangle) \# (R * h5)) * \langle L, \langle I * L, R\rangle\rangle$
   xiii. $f = L * h5 * \langle I, I\rangle$

2. f is the Gödel number of $g \Leftrightarrow$ there are integers n, m and elements $g1, h1, h2, h3$ such that

   i. $f = R^m$
   ii. $g1$ is an n-string
   iii. $h1$ $\in$Bit(n)

iv. $h2$ is an $n+1$-string

v. $g1 = L * h2 * \langle I, R\rangle$

vi. $h2 = ((h1 * \langle I, R\rangle) \# (R * h2)) * \langle L, \langle I * L, R\rangle\rangle$

vii. $h3 = ((h1 * \langle\langle L, E\rangle, R\rangle) \# (R * h3)) * \langle L, \langle I * L, R\rangle\rangle$

viii. $g = L * h3 * \langle I, I\rangle$

3. Let us prove fact (1) first. $\Leftarrow$. Suppose that $h1, h2, h3, h4$, and $h5$ are as in (i.) – (xiii). Then $h1 = \langle Xn-1 * L, \langle \ldots \langle X0 * L, R\rangle \ldots\rangle\rangle$ for $Xi \in \{L, R\}$, $i = 0 \ldots n-1$ by (i.) and $h2 = \langle Xn - 1 * \ldots * X * L, \langle \ldots \langle X0 * L, R\rangle \ldots\rangle\rangle$ by (ii.) and (vii.). Thus $g = Xn - 1 * \ldots * X0$ by (vi.). Now $h3 = \langle rn - 1 * L, \langle \ldots \langle r1 * L, \langle R * L, R\rangle\rangle \ldots\rangle\rangle$ by (iii.) and (viii.). By (ix.) $ri + 1 = ri * ri$ for $i = 0 \ldots n-2$. Thus $h3 = \left\langle R^{2^{n-1}} * L, \langle \ldots \langle R^2 * L, \langle R * L, R\rangle\rangle \ldots\rangle\right\rangle$. Hence by (iv.) and (x.) $h4 = \left\langle\left\langle R^{2^{n-1}}, I\right\rangle * L, \langle \ldots \langle\langle R, I\rangle * L, R\rangle \ldots\rangle\right\rangle$ so $(h3 * \langle I, R\rangle) \# h4 = \langle sn - 1 * L, \langle \ldots \langle s0 * L, R\rangle \ldots\rangle\rangle$ where

$$si = \begin{cases} R^{2^i} & \text{if } ri = L \\ \\ R^0 & \text{if } ri = R \end{cases} .$$

Now by (v.) and (xii.)

$$h5 = \langle sn - 1 * \ldots * s0 * L, \langle \ldots \langle s0 * L, R\rangle \ldots\rangle\rangle .$$

Thus by (xiii.) $f = sn-1*\ldots*s0 = R^{(bn-1)2^{(n-1)}+\ldots+(b1)2+b0}$ where the bi are as above. This completes the proof of $\Leftarrow$. For $\Rightarrow$ use the $h1, h2, h3, h4$ and $h5$ as in $\Leftarrow$. Finally (2) is proved like (1).

We conclude that the set of pairs (f, g) such that f is the Gödel number of g is the projection of the set of solutions to a (3 variable) unification problem. A similar result holds for $F[x]$. Combining this with paragraph 6 gives the following theorem:

Every *RE* subset of F is the projection of the set of solutions to a unification problem. A similar result holds for $F[x]$.

References

[1] Barendregt, "The Lambda Calculus", North Holland, 1981.

[2] Freyd & Heller, Splitting homotopy invariants (unpublished manuscript to appear in *Festschrift for Alex Heller*).

[3] Klop, Combinatory Reduction Systems, *Mathematical Centre Tracts*, **127,** Math Centrum Amsterdam, 1980.

[4] Lambek, From lambda calculus to Cartesian closed categories, Seldin & Hindley (eds.), *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, Academic Press, 1980 (Curry festschrift).

[5] Matiyasevich, Diophantine representation of recursively enumerable predicates in Fenstad ed., Proceedings of the Second Scandanavian Logic Symposium. North Holland, 1971.

[6] Scott, Relating theories of the lambda calculus, *Curry Festschrift.*

[7] Statman, Freyd's hierarchy of combinator monoids in Proceedings Symposium on Logic in Computer Science, *IEEE,* 1991.

[8] Statman, Simply typed Lambda Calculus with Surjective Pairing, CMU, Dept. of Mathematical Sciences, Report 92-146.

[9] Statman, Recursive types and the subject reduction theorem, CMU, Dept. of Mathematical Sciences, Report 94-164.

[10] Statman, A local translation of untyped lambda calculus into simply typed lambda calculus, CMU, Dept. of Mathematical Sciences, Report 91-134.

[11] Statman, Combinators and the theory of partitions, CMU, Dept. of Mathemtical Sciences, Report 88-31.