Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 325 (2016) 299–304

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

On the Representation of Semigroups and Other Congruences in the Lambda Calculus

Rick Statman[1]

Mathematical Sciences
Carnegie Mellon University
Pittsburgh, PA
USA

Abstract

We show that every semigroup with an RE word problem can be pointwise represented in the lambda calculus. In addition, we show that the free monoid generated by an arbitrary RE subset of combinators can be represented as the monoid of all terms which fix a finite set of points.

Keywords: lambda calculus, semigroups, representation

1 Introduction

Combinators being both functions and arguments can act on one another by application and composition. More generally, if $' and $" are sets of combinators closed under beta conversion, the A action of $' on $" is the set $\{AMN|M$: $' and N:$"} closed under beta conversion. First we recall the definitions of some familiar combinators:

$$\begin{aligned} B &:= \lambda abc.a(bc) & S &:= \lambda abc.ac(bc) \\ B' &:= \lambda abc.b(ac) & O &:= (\lambda x.xx)(\lambda x.xx) \\ C^* &:= \lambda ab.ba & 0 &:= \lambda yz.z \\ K &:= \lambda ab.a & s &:= \lambda xyz.y(xyz) \\ I &:= \lambda a.a & Y &:= (\lambda xz.z(xxz))(\lambda xyz.z(xxz)) \end{aligned}$$

Example 1.1 $A := K$: this is the trivial action.

Example 1.2 $A := I$: this is the applicative action.

[1] Email: statman@cs.cmu.edu

http://dx.doi.org/10.1016/j.entcs.2016.09.044
1571-0661/© 2016 The Author(s). Published by Elsevier B.V.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Example 1.3 $A := B$: this is the semigroup action.

Example 1.4 $A := S$: the pointwise applicative action.

Of course, this definition extends to multiple arguments by Currying. We write

$$M = N \text{ mod beta}$$

if M beta converts to N.

It is trivial that general A can be reduced to I, and that multiple arguments can be reduced to a single argument by pairing. In addition, applicative action can be reduced to the semigroup action since $K(xy) = Bx(Ky)$ mod beta. However, there is another reduction which is lambda I.

Let

$$D := Y(\lambda fxyz.\ fx(zy))$$

where Y is Turing's fixed point combinator as above.

Lemma 1.5 *For any* U, V *if* $B(C^*U)D = B(C^*V)D$ mod beta *then*

$$U = V \text{ mod beta.}$$

Proof. Straightforward. □

Now given $\$'$ and $\$''$, since

$$\begin{aligned} C^*(AM) &= B(B(C^*M)(C^*A))B \text{ mod beta} \\ C^*(AMN) &= B(B(B(C^*M)(C^*A))B)(B(C^*N)D) \text{ mod beta, and} \\ &= B(C^*M)(B(C^*A)(BB(B(C^*N)D))) \text{ mod beta} \end{aligned}$$

the A action of $\$'$ on $\$''$ is equivalent to the semigroup action of $\{C^*M \mid M : \$'\}$ on $\{(B(C^*A)(BB(B(C^*N)D))) \mid N : \$''\}$. We next consider an example of the action of I in representing semi-groups.

Definition 1.6 Let $\$'$ be an RE set of combinators closed under beta conversion. An equivalence relation $\sim$ on $\$'$ is said to be pointwise representable on $\$''$ if for every $M, N : \$'$ we have

$$MP : \$'' \text{ for all } P : \$''$$

$$M \sim N \text{ iff for all } P : \$''$$
$$MP = NP \text{ mod beta}$$

Example 1.7 (Kleene):

$\$'$ = any RE set of definitions of total recursive functions

$\$''$ = the Church numerals and $\sim =$ extensional equality

Non-example (Plotkin):

$\$' =$ all combinators

$\$'' =$ all combinators and $\sim =$ beta conversion.

Let \$ be a semigroup on a countable number of generators. We assume that the generators are denoted by the positive integers. Elements of \$ are then denoted by words

$$w = w(1)\ldots w(l).$$

of variable length l, on the generators of \$. We write $u = v$ mod \$ if the words u and v are equal in \$. We represent the word w by the lambda term

$$\text{‘}w' := B'Ow(1)(B'Ow(2)(\ldots B'Ow(n-1)Ow(n)\ldots))$$

where integers are replaced by their Church numerals.

We define combinators P, Q, R as follows.

By Theorem 3 of [7] there exists a closed term P such that $PM = PN$ mod beta if and only if either $M = N$ mod beta or both $M = \text{‘}u'U$ mod beta, $N = \text{‘}v'V$ mod beta, and $u = v$ mod \$, where either U or V, or both, may not exist, but each must be of positive order if it exists. Now we set

$p :=$ predecessor for Church numerals, and
$A := Y(\lambda xy.\ y0(B(py)1)$ (An $= n^{\text{th}}$ eta expansion of I mod beta)
$Q := \lambda xy\ .Y(Ax(fsx)(Py))$
$R := Q0.$

For each word w we define a second representation by the lambda term

$$\text{“}w'' := B(C^*\ \text{‘}w')B.$$

Then $\text{“}w'' = \lambda ab.a(\text{‘}w'b)$ mod beta and for words, w, u

$B\text{“}w''\text{“}u'' = \text{“}wu''$ mod beta

and for any words $w_1, \ldots, w_n, u_1, \ldots, u_m$

$$\begin{aligned}&\text{“}w''(R\text{“}w''_1\ldots\text{“}w''_n)(R''u''_1\ldots\text{“}u''_m)\\ &\quad = Q(n+1)(P(\text{“}w''_1))\ldots(P(\text{“}w''_n))(P\text{“}w''((R\text{“}u''_1\ldots\text{“}u''_m)))\\ &\quad = Q(n+1)(P(\text{“}w''_1))\ldots(P(\text{“}w''_n))(P\text{“}w'')\text{ mod beta.}\end{aligned}$$

Now it is not difficult to prove that if

$$\begin{aligned}&Q(n+1)(P(\text{“}w''_1))\ldots(P(\text{“}w''_n))(P\text{“}w'')\\ &\qquad = Q(n+1)(P(\text{“}w''_1))\ldots(P(\text{“}w''_n))(P\text{“}u'')\text{ mod beta}\end{aligned}$$

then $w = u$ mod \$.

Now take for $\$'$ the set of all $\text{“}w''$ and for $\$''$ the set of all $R(\text{“}w''_1)\ldots(\text{“}w''_n)$. Thus we have proved the

Proposition 1.8 *Every RE semigroup is pointwise representable.*

For a general RE congruence $\sim$, we illustrate with the case of one binary function symbol f. We assume that we have Gödel numbering $`t', `r'$ of terms t, r with a recursive function $t, r \mapsto ftr$ represented by a lambda term F; that is $F`t'`r' = `ftr'$ mod beta. By Theorem 3 of [7] there exists a closed term $P$ such that $PM = PN$ mod beta if and only if either $M = N$ mod beta or both $M = `u'$ mod beta, $N = `v'$ mod beta and $u = v$ mod \$. Now define an app

$$A := \lambda abcde.\langle a, e\rangle$$

and define

$$"t" := \langle A,' t', P't'\rangle$$
$$"f" := \lambda xy.\langle A, F(xK)(yK), P(F(xK)(yK))\rangle.$$

The set $\$''$ can be taken to be the set of all terms $\langle A, P't'\rangle$. Thus,

Proposition 1.9 *Every RE congruence is pointwise representable.*

These representation results implicitly use the "regularity" of the representation. If the representing functions are essentially irregular and beta conversion on that set is decidable, such as the set of Church numerals, then co-RE congruences can be represented. Using Kleene brackets $\{e\}$ for the recursive function with Gödel number e, we have

Lemma 1.10 *Let $\sim$ be a co-RE equivalence relation on the set of natural numbers. Then there exists a recursive function f such that for any e, $\{f(e)\}$ is total recursive and $i \sim j$ iff $\{f(i)\} = \{f(j)\}$.*

Proof. We proceed recursively assuming that $f(i)$ is defined for $i = 0, \ldots, n$. To define $f(n+1)$ we compute successive values $\{f(n+1)\}(j)$ for $j = 0, \ldots, k$. Assume that these have been computed up to k. To compute the value for $k+1$ let @ be the subset of $\{0, 1, \ldots, n\}$ such that i : @ iff there is not $j < k+1$ with $\{f(i)\}(j) = / = \{f(n+1)\}(j)$. Now compute $\{f(i)\}(k+1)$ for each i : @. The values partition @; i and j belong to the same block iff $\{f(i)\}(k+1) = \{f(j)\}(k+1)$. Now the set of all i such that i is inequivalent to $n+1$ is uniformly RE in $n+1$. For any two distinct blocks in the partition of @, eventually every member of at least one of the blocks will appear in the enumeration. When there is only one block left in the partition we can set $\{f(n+1)\}(k+1) = \{f(i)\}(k+1)$ any i in that block provided after $k+1$ steps in the enumeration of the inequivalents to $n+1$ at least one member of that block has not been found. Otherwise, we set $\{f(n+1)\}(k+1) = 1 + \max[\{f(i)\}(k+1) | i : @]$. End of proof. □

The construction for Proposition 2 can now be modified to give

Proposition 1.11 *Every co-RE congruence is pointwise representable.*

Next we consider the case of a general RE set \$ closed under beta conversion. The members of \$ generate a free monoid under the map

$$M \mapsto C^* M.$$

Here we intend to include the Church numeral $1 = I$ mod eta as well as I. If $\$''$ is a set of terms closed under beta conversion we say that $\$'$ is fixed-pointwise representable on $\$''$ if the set $\{L \mid LX = X \text{ mod beta for all } X : \$''\}$ = the free monoid generated by

$$\{L \mid L = C^*M \text{ mod beta for some } M : \$'\}$$

Note here that we have specifically allowed $\$''$ to contain open terms. We recall some of the s of [5] with a few small changes. T is the fixed point combinator of Bohm ([1] 6.5.4) with a free variable b;

$$\begin{aligned}
E &:= \text{ the enumerator of } \{C^*N \mid M : \$\} \\
T &:= (\lambda xyz.\ z(xxyz))(\lambda xyz.\ z(xxyz))b \\
A' &:= \lambda fg.\ \lambda xyz.\ fx(a(Ex))(f(Sx)y(g(Sx))z) \\
A'' &:= \lambda fg.\ \lambda x.\ f(Sx)(a(E(Sx))(g(Sx))(gx) \\
G &:= T(\lambda u.\ A''(T(\lambda v.\ A'vu))u) \\
F &:= T(\lambda u.\ A'uG) \\
H &:= \lambda xa.\ F0(ax)(G0) \\
J &:= Y(\lambda f.\ \lambda xy.\ f(x(Hy)))(Y(\lambda g.g(H(E0))))
\end{aligned}$$

$$\begin{aligned}
L &:= Y(\lambda fxy.\ f(x(Jy)) \\
P &:= Y(\lambda f.\ fJ) \\
Q &:= LP \\
L' &:= Y(\lambda f.\ \lambda xy.\langle f, x\rangle) \\
L'' &:= Y(\lambda f.\ \lambda xyz.\langle f, x, z\rangle).
\end{aligned}$$

as in [3] have

Lemma 1.12 $JM = J$ mod beta *iff there exists an* m *such that* $Em = C^*M$ mod beta.

Now consider the following "points fixed" equations

(1) $x\langle L', 0\rangle = \langle L', 0\rangle$

(2) $x\langle L'', 0, 1\rangle = \langle L'', 0, 1\rangle$

(3) $xQ = Q$.

Now if

$$M = \lambda a.\ a(C^*M_1)\dots(C^*M_m) \text{ for } M_i : \$$$

then

$$\begin{aligned}
M\langle L', 0\rangle &= L'M_1 0(C^*M_2)\dots(C^*M_m) \\
&= \langle L', 0\rangle(C^*M_2)\dots(C^*M_m) = \dots \\
&= \langle L', 0\rangle \text{ mod beta,}
\end{aligned}$$

and similarly

$$M\langle L'', 0, 1\rangle = \langle L'', 0, 1\rangle \text{ mod beta.}$$

In addition,

$$\begin{aligned}
MQ &= LP(C^*M_1)\dots(C^*M_m) = L(P(J(C^*M_1)))(C^*M_2)\dots(C^*M_m) \\
&= L(PJ)(C^*M_2)\dots(C^*M_m) = LP(C^*M_2)\dots(C^*M_m) = \dots \\
&= Q \text{ mod data}
\end{aligned}$$

Thus all the members of the free monoid generated by the C^*M with $M : \$$ satisfy (1), (2), and (3).

Proposition 1.13 *Suppose that N satisfies the equations (1), (2), and (3) mod beta, then N lies in the free monoid generated by the C^*M for M in $\$'$.*

Proof. Suppose that such an N is given. Since N satisfies (1) mod beta N has a head normal form. W.l.o.g. we may assume N is in head normal form. Since N satisfies equation (2) mod beta, and $\langle L', 0\rangle, \langle L'', 0, 1\rangle$ have head variables with a different number of arguments, the head variable of N is the first one bound in its lambda prefix. Since $\langle L', 0\rangle$ has order 1, the lambda prefix of N has length 1 or 2. First suppose that N has order 2: $N = \lambda xy.\ xX_1 \dots X_m$. Then setting $Z_i := [Q/x]X_i$

$NQ = \lambda y.\ QZ_1 \dots Z_m = \lambda y.\ L(P(JZ_1)) \dots (JZ_m))$ mod beta.

By an argument similar to the argument of [7] Theorem 3, this can only be the case if $Z_m = y$ mod beta and for $i < m$ we have $JZ_i = J$ mod beta. Since Q contains an unprojectible free variable in F and G it must be the case that each Z_i beta converts to a term without x, and for $i < m$ without y. In other words, x is head original and thus we assume that

$$N = \lambda xy.\ xN_1 \dots N_{m-1}y.$$

Hence, by Lemma 3 there exist $M_1, \dots, M_{m-1} : \$$ such that $N_i = C^*M_i$ mod beta for $i = 1, \dots, m-1$, and we have $N = B1(B(C^*M_1)(\dots(B(C^*M_{m-2})C^*M_{m-1} : \$))\dots)$ mod beta. The case for N of order 1 is similar with I replacing 1. □

Remark 1.14 If the members of $\$'$ all have normal forms then the members of $\$''$ can be taken to be closed terms.

References

[1] Barendregt, H., The Lambda Calculus, North Holland (1982)

[2] Church, A., A Note on the Entscheidungs Problem, *J. of Symbolic Logic*, **1** (1936).

[3] Curry, H. B., Feys, R., "Combinatory Logic Vol.I", North Holland, (1958).

[4] Statman, R., Combinators and the theory of partitions, CMU Research Report No. 88-31, (1988).

[5] Statman, R., Some Examples of Non-Existent combinators, *Theoretical Computer Science*, **121**, (1993).

[6] Statman, R., On Cartesian Monoids, CSL '97 LNCS 1258.

[7] Statman, R., Morphisms and Partitions of V-sets, *CSL*, (1998).

[8] Statman, R., Cartesian Monoids, MFPS 2010 ENTCS Vol 65, Sept. 6, 2010.

[9] Statman, R., Near semirings and lambda calculus, *TLCA* (2014).