Church's Semigroup Is Sq-Universal

Rick Statman ✉
Carnegie Mellon University, Pittsburgh, PA, USA

Abstract

We prove Church's lambda calculus semigroup is sq-universal.

2012 ACM Subject Classification Theory of computation → Lambda calculus

Keywords and phrases lambda calculus, Church's semigroup, sq-universal

Digital Object Identifier 10.4230/LIPIcs.FSCD.2021.6

1 Introduction

In 1937 ([2]) Church formulated lambda calculus as a semigroup. His ideas were pursued by Curry and Feys ([3]), and later by Bohm (Barendregt [1, 532]) and Dezani ([4]). If lambda terms in some way represent functions, then such a presentation based on composition is a quite natural complement to the presentation based on application. Of course, it is widely held that lambda calculus, therefore this semigroup, is an important part of the foundation of functional programming.

In 1968 Peter Neumann [6] introduced the notion of an sq-universal group. Many results in classical group theory can be interperted as saying that a particular group (or class of groups) is sq-universal. The notion of sq-universal makes perfectly good sense for semigroups as well as groups. A countable semigroup O is sq-universal if every countable semigroup is a subsemigroup of a homomorphic image (quotient) of O ("sq" stands for "sub ... of quotient ...").

We shall show that Church's semigroup is sq-universal. We shall also characterize lambda theories as special kinds of quotients of the semigroup (there are quotients which do not correspond to lambda theories) at least when $I = 1$ (eta).

2 Church's semigroup

Some notation will be useful. We adopt for the most part the notation and terminology of [1].

$$\begin{aligned} I &:= \lambda x.\, x \\ 1 &:= \lambda xy.\, xy \\ B &:= \lambda xyz.\, x(yz) \\ K &:= \lambda xy.\, x \\ C &:= \lambda xyz.\, xzy. \\ \sim &:= \text{ beta conversion} \\ \to &:= \text{ beta reduction} \\ \twoheadrightarrow &:= \text{ beta reduction multistep.} \end{aligned}$$

Both Church and Curry observed that the combinators form a semigroup under multiplication B and beta conversion. The same is true for addition $\lambda xyuv.\, xu(yuv)$ and beta conversion. Since these satisfy the right distributive law

$$(\lambda xyz.\, x(yz))((\lambda xyuv.\, xu(yuv))ab)c \sim (\lambda xyuv.\, xu(yuv))((\lambda xyz.\, x(yz))ac)(((\lambda xyz.\, x(yz))bc)$$

they form a near semiring.

6th International Conference on Formal Structures for Computation and Deduction (FSCD 2021).
Editor: Naoki Kobayashi; Article No. 6; pp. 6:1–6:6
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Many years ago I noticed a generalization of this near semiring structure to a hierarchy of semigroups. Define

$$A_n := \lambda xyu_1 \cdots u_n v.\, xu_1 \cdots u_n(yu_1 \cdots u_n v)$$

so $A_0 := B$ and A_1 is Church's addition. Then combinators form a semigroup with multiplication A_n with beta conversion. Again the right distributive law holds. More precisely we have

$$\begin{array}{lll} \text{(associativity)} & A_m(A_n xy) \sim A_0(A_n x)(A_n y) & \text{if } m = n, \\ \text{(distributivity)} & A_m(A_n xy) \sim A_{n+1}(A_m x)(A_m y) & \text{if } m < n. \end{array}$$

and in addition,

(i) $A_m x \sim A_{m+1}(Kx)I$
(ii) $K(A_m xy) \sim A_{m+1}(Kx)(Ky)$.

Let O_n be the semigroup of all combinators with multiplication A_n. Let $J = \lambda x.\, xI$ (J is usually written $C{*}{*}$). Now we adopt the infix notation $*$ for the prefixing of B.

(iii) $J * K \sim I$
(iv) $J(A_{m+1}xy) \sim A_m(Jx)(Jy)$.

3 Homomorphisms

A homomorphism h of O_n induces a congruence relation H defined by $M \mathrel{\mathrm{H}} N$ iff $h(M) = h(N)$. Here we identify h with the map that takes M to its congruence class $\{N \mid M \mathrel{\mathrm{H}} N\}$, so h is a set valued map.

▶ **Example 1.** $h(M) := BM$ defines a homomorphism of O_0.

▶ **Definition 2.** *h is said to be "entire" if*
(a) $h(KM) = K(h(M))$
(b) $h(JM)$ *contains* $J(h(M))$
(c) $h(1M) = h(M)$

▶ **Example 3.** $h(M) :=$ the beta-eta congruence class of M is entire. For, if KM beta-eta converts to N there exists P s.t. N beta converts to KP. This follows from Church-Rosser and eta postponement.

Now if h is an entire homomorphism for O_n then h is a homomorphism for every O_m with $m < n$, for we have

$$\begin{aligned} &K(h(A_{n-1}xy)) \sim \\ &h(K(A_{n-1}xy)) \sim \\ &h(A_n(Kx)(Ky)) \sim \\ &A_n(h(Kx))(h(Ky)) \sim \\ &A_n(K(h(x)))(K(h(y))) \sim \\ &K(A_{n-1}(h(x))(h(y))) \end{aligned}$$

so by (iii) $h(A_{n-1}xy) \sim A_{n-1}(h(x))(h(y))$.

Lambda theories are defined as in [1] 4.1.1. Each lambda theory T over beta conversion induces a homomorphism for each O_n where H is defined by $M \text{ H } N$ iff $T \vdash M = N$. Each lambda theory T over beta- eta conversion induces an entire homomorphism for each O_n where H is defined by $M \text{ H } N$ iff $T \vdash M = N$. Now there are O_0 homomorphisms which are not induced by theories. For example, the Rees factor monoid induced by the ideal $\{KM \mid \text{all } M\}$. However we shall show that this is essentially the only example.

▶ **Theorem 4.** *Let h be an entire homomorphism for O_1. Then $T = \{M = N \mid M \text{ H } N\}$ is closed under logical consequence over beta conversion.*

Proof. We suppose that $T \vdash M = N$ over beta conversion. For what follows we will use a theorem of Jacopini [5] in the form exposited and marginally improved in [8].

By Jacopini's theorem, there exist $M_i = N_i$ in T for $i = 1, \dots, n$ and closed terms $P_1, \dots, P_n$ such that

$$\begin{aligned} M &\sim P_1 M_1 N_1 \\ P_1 N_1 M_1 &\sim P_2 M_2 N_2 \\ P_2 N_2 M_2 &\sim P_3 M_3 N_3 \\ &\vdots \\ P_n N_n M_n &\sim N. \end{aligned}$$

Thus by Church's theorem ([1, 531]), which uses eta in one spot,

$$\begin{aligned} &M \text{ H } CIN_1 * CIM_1 * CIP_1 * B * B * CI \\ &CIM_1 * CIN_1 * CIP_1 * B * B * CI \text{ H } CIN_2 * CIM_2 * CIP_2 * B * B * CI \\ &CIM_2 * CIN_2 * CIP_2 * B * B * CI \text{ H } CIN_3 * CIM_3 * CIP_3 * B * B * CI \\ &\vdots \\ &CIM_n * CIN_n * CIP_n * B * B * CI \text{ H } N. \end{aligned}$$

Now let us write $\#$ for A_1 infixed. We have

$$\begin{aligned} &KM \text{ H } K(CIN_1) \# K(CIM_1) \# K(CIP_1) \# KB \# KB \# K(CI) \\ &K(CIM_1) \# K(CIN_1) \# K(CIP_1) \# KB \# KB \# K(CI) \text{ H} \\ &\qquad K(CIN_2) \# K(CIM_2) \# K(CIP_2) \# KB \# KB \# K(CI) \\ &K(CIM_2) \# K(CIN_2) \# K(CIP_2) \# KB \# KB \# K(CI) \text{ H} \\ &\qquad K(CIN_3) \# K(CIM_3) \# K(CIP_3) \# KB \# KB \# K(CI) \\ &\vdots \\ &K(CIM_n) \# K(CIN_n) \# K(CIP_n) \# KB \# KB \# K(CI) \text{ H } KN \end{aligned}$$

by (ii). Now $K(CIx) \sim CI * Kx$ so since h is entire

$$h(K(CIM_i)) = h(K(CIN_i)) \quad \text{for } i = 1, \dots, n.$$

Thus, since h is a $\#$ homomorphism, $h(KM) = h(KN)$. But h is entire so $h(M) = h(N)$. ◀

▶ **Corollary 5.** *Let h be an entire homomorphism for O_1. Then $T = \{M = N \mid M \text{ H } N\}$ is closed under logical consequence over beta-eta conversion.*

▶ **Corollary 6.** *If h is an entire homomorphism for O_1 then it is an entire homomorphism for all O_n.*

4 SQ universality

▶ **Definition 7.** *A set \$ of order zero lambda-I terms is said to be independent if for every member M of \$ no beta reduct of M contains a beta reduct of any member of \$ as a proper subterm.*

▶ **Example 8.** The set of terms $(\lambda x.\, xx)(\lambda x.\, xx)N$, where N is a non-zero Church numeral is independent.

Curiously, independent sets must exist for recursion theoretic reasons.

▶ **Lemma 9.** *There must be an infinite independent set.*

Proof. We construct an increasing sequence of finite independent sets by induction.

Basis: $\{(\lambda x.\, xx)(\lambda x.\, xx)\}$ is independent.

Induction step; we suppose that \$ is a finite independent set. Now the following sets of lambda-I terms are RE and closed under beta reduction

- **(i)** the set of combinators with positive order
- **(ii)** the set of combinators M s.t. there is a beta reduct of a member of $\$ \cup \{M\}$ which is a proper subterm of a beta reduct of M.

In addition, both of these sets have non-empty complements. Thus by Visser's theorem (as modified in [7] and adapted to lambda-I) the intersection of the complements of these two sets is infinite (modulo beta-conversion). Thus one element can be added to \$. ◀

▶ **Definition 10.** *The B polynomials over \$ are defined as follows. Any variable or member of \$ is a B polynomial. If F and G are B polynomials then so is $F * G$.*

▶ **Lemma 11.** *Let \$ be an independent set. Let $P, P_1, \ldots, P_k$ be products of the members of \$. Then if $P \sim MP_1 \cdots P_k$ there exists a B polynomial $F(x_1, \ldots, x_k)$ over \$ s.t. $Mx_1 \cdots x_k \sim F(x_1, \ldots, x_k)$.*

Proof. Wlog we can assume that $P = \lambda x.\, J_1(\cdots(J_l x)\cdots)$ for the J_i members of \$ where if $l = 1$ then $P = J_1$. When $l = 1$ consider a standard reduction of $MP_1 \cdots P_k$ to P. Now if one of the P_j comes to the head of the head reduction part of the standard reduction we have

$$P_j \twoheadrightarrow J_1$$

and $Mx_1 \cdots x_k \twoheadrightarrow x_j$. Otherwise since the members of \$ are independent $Mx_1 \cdots x_k \twoheadrightarrow J_1$. Let $l > 1$, and let

$$MP_1 \cdots P_k \twoheadrightarrow \lambda x.\, J_1(\cdots(J_l x)\cdots)$$

by a standard beta reduction. Now if one of the P_j comes to the head of the head reduction part let @ be the substitution $[P_1/x_1, \ldots, P_k/x_k]$. We have for some X, $P_j = \lambda x.\, J_1(\cdots(J_m x)\cdots)$ or J_1

$$\begin{aligned} \lambda x.\, P_j(@\, X) &\twoheadrightarrow P \\ (\lambda x_1 \cdots x_k x.\, X)P_1 \cdots P_k &\twoheadrightarrow \lambda x.\, J_{m+1}(\cdots(J_l x)\cdots). \end{aligned}$$

In this case the proposition follows by induction on l. If no P_j comes to the head then at the end of the head reduction we have a term

$$\lambda x.\ @((\lambda y.\, Y)Y_1 \cdots Y_m)$$

which reduces to P by internal reductions. Thus $m = 2$ and $@((\lambda y. Y)Y_1) \twoheadrightarrow J_1$ by internal reductions, and

$$(\lambda x_1 \cdots x_k x. Y_2)P_1 \cdots P_k \twoheadrightarrow \lambda x. J_2(\cdots(J_l x)\cdots).$$

Since the J_i are independent $(\lambda y. Y)Y_1 \twoheadrightarrow J_1$ and the case follows by induction. ◀

Now if T is any set of equations between products of members of the independent set \$ then the lambda theory generated by T is certainly consistent since all these terms are unsolvables. Now these equations can be thought of as the presentation of a semigroup on the alphabet \$. If $P = Q$ is an equation between products of members of \$ then we may have $T \vdash P = Q$ where T is a lambda calculus theory, or $T \vdash P = Q$ where T is thought of as the presentation of a semigroup. It will be convenient to use the terminology $T \vDash P = Q$ for the semigroup case. Clearly if $T \vDash P = Q$ then $T \vdash P = Q$.

▶ **Lemma 12.** *If $T \vdash P = Q$ then $T \vDash P = Q$.*

Proof. Suppose that $T \vdash P = Q$. By Jacopini's theorem ([5]) there exist $M_1, \ldots, M_m$, and $P_1 = Q_1, \ldots, P_m = Q_m$ in T s.t.

$$\begin{aligned} P &\sim M_1P_1Q_1 \\ M_1Q_1P_1 &\sim M_2P_2Q_2 \\ M_2Q_2P_2 &\sim M_3P_3Q_3 \\ &\vdots \\ M_mQ_mP_m &\sim Q, \end{aligned}$$

The proof is by induction on m. Wlog we can assume that $P = \lambda x. J_1(\cdots(J_l x)\cdots)$. By lemma 11 there exists a B polynomial $F(x_1, x_2)$ over \$ s.t.

$$M_1x_1x_2 \sim F(x_1, x_2)$$

so

$$\begin{aligned} P &\sim F(P_1, Q_1) \\ T &\vDash P = F(P_1, Q_1) \\ T &\vDash P = F(Q_1, P_1) \\ F(Q_1, P_1) &\sim M_2P_2Q_2 \end{aligned}$$

and we can apply the induction hypothesis to

$$\begin{aligned} F(Q_1, P_1) &\sim M_2P_2Q_2 \\ M_2Q_2P_2 &\sim M_3P_3Q_3 \\ &\vdots \\ M_mQ_mP_m &\sim Q. \end{aligned}$$ ◀

▶ **Theorem 13.** *O_0 is sq-universal.*

Proof. Suppose that the countable semigroup S is given. We take a set of generators and a presentation of S on these generators. Using lemma 9, we construct an independent set, which we identify with these generators, and we construct a lambda theory T, which encodes the presentation of S. By lemma 12 $T \vdash P = Q$ if and only if $P = Q$ is true in S. But by section 2 there is a homomorphism h of O_0 s.t. $T \vdash P = Q$ if and only if $h(P) = h(Q)$. ◀

References

1 Hendrik Pieter Barendregt. *The Lambda Calculus – Its Syntax and Semantics*, volume 103 of *Studies in logic and the foundations of mathematics*. North-Holland, 1985.

2 Alonzo Church. *The Calculi of Lambda Conversion*. Princeton University Press, 1941.

3 Haskell B. Curry and Robert Feys. *Combinatory Logic*, volume 1. North Holland, 1958.

4 Mariangiola Dezani-Ciancaglini. Characterization of Normal Forms Possessing Inverse in the *lambda-beta-eta*-Calculus. *Theor. Comput. Sci.*, 2(3):323–337, 1976. doi:10.1016/0304-3975(76)90085-2.

5 Giuseppe Jacopini. A condition for identifying two elements of whatever model of combinatory logic. In Corrado Böhm, editor, *Lambda-Calculus and Computer Science Theory, Proceedings of the Symposium Held in Rome, Italy, March 25-27, 1975*, volume 37 of *Lecture Notes in Computer Science*, pages 213–219. Springer, 1975. doi:10.1007/BFb0029527.

6 P. Neumann. The SQ-universality of some finitely presented groups. *J. Austral. Math. Soc.*, 16:1–6, 1973.

7 Richard Statman. Morphisms and Partitions of V-Sets. In Georg Gottlob, Etienne Grandjean, and Katrin Seyr, editors, *Computer Science Logic, 12th International Workshop, CSL '98, Annual Conference of the EACSL, Brno, Czech Republic, August 24-28, 1998, Proceedings*, volume 1584 of *Lecture Notes in Computer Science*, pages 313–322. Springer, 1998. doi:10.1007/10703163_21.

8 Richard Statman. Consequences of Jacopini's Theorem: Consistent Equalities and Equations. In Jean-Yves Girard, editor, *Typed Lambda Calculi and Applications, 4th International Conference, TLCA'99, L'Aquila, Italy, April 7-9, 1999, Proceedings*, volume 1581 of *Lecture Notes in Computer Science*, pages 355–364. Springer, 1999. doi:10.1007/3-540-48959-2_25.