

# On embedding countable sets of endomorphisms

J. ARAÚJO, J.D. MITCHELL AND N. SILVA

ABSTRACT. Sierpiński proved that every countable set of mappings on an infinite set  $X$  is contained in a 2-generated subsemigroup of the semigroup of all mappings on  $X$ . In this paper we prove that every countable set of endomorphisms of an algebra  $\mathcal{A}$  which has an infinite basis (independent generating set) is contained in a 2-generated subsemigroup of the semigroup of all endomorphisms of  $\mathcal{A}$ .

## 1. Introduction

Let  $X$  be an infinite set. In [20] Sierpiński proved the following result:

**Proposition 1.1.** *Any countable subset of the semigroup  $\mathcal{T}_X$  of all transformations on  $X$  is contained in a 2-generated subsemigroup of  $\mathcal{T}_X$ .*

A short proof of this result was immediately given by Banach in [3] (see also [13]). In [13] it was shown that the method of Banach can be modified slightly to prove analogous results for countable subsets of the semigroup of all partial bijections and the semigroup of partial mappings on an infinite set  $X$ . As may be expected the situation is more complicated for bijections of an infinite set  $X$ . However, in [9, Theorem 3.3] it was proven that every countable set of permutations of  $X$  is contained in a two-generated subgroup of the symmetric group  $\mathcal{S}_X$ .

There are several important corollaries of these results, including the result that every countable semigroup can be embedded in a two-generated semigroup. This result was proven, independently of Sierpiński's result, by Evans in [6]. Several other proofs of this result appeared, including [19] and [22].

The full transformation semigroup can be considered as the semigroup of endomorphisms of the (unstructured) set  $X$ . It is natural to ask if a result, analogous to Proposition 1.1, holds when  $X$  is endowed with some structure. It was shown in [15] that every countable set of endomorphisms of an infinite dimensional vector space  $\mathcal{V}$ , over an arbitrary field, is contained in a two-generated subsemigroup of the semigroup of all endomorphisms of  $\mathcal{V}$ . This result was motivated by results in [21] relating to the semigroup of continuous self-maps  $S(X)$  of a topological space  $X$ . In [21] it was shown that any countable subset of  $S(X)$  is contained in a two-generated subsemigroup of  $S(X)$  when  $X$  is the rationals, the irrationals, the countable discrete space, an  $m$ -dimensional closed unit cube, or the Cantor set.

---

1991 *Mathematics Subject Classification*: 20M20, 20M10, 08A35.

*Key words and phrases*: Endomorphisms, universal algebras, independence, semigroups.

The main aim of this paper is to prove that a result analogous to Proposition 1.1 holds for the endomorphism semigroups of a large class of algebras.

For the remainder of this section we introduce the main notions and terminology we shall use in this paper. Let  $A$  be a non-empty set. For  $n \in \mathbb{N}$ , an  $n$ -ary operation on  $A$  is a mapping  $\alpha : A^n \rightarrow A$ , where  $A^n$  denotes the Cartesian product  $A \times A \times \cdots \times A$  with  $n$  terms. As usual a nullary operation on  $A$  is a mapping  $a : \emptyset \rightarrow A$ . These operations may be referred to as *finitary operations*. A mapping from  $A^I$  to  $A$ , where  $I$  is an infinite set, is called an *infinitary operation*. Throughout this paper we shall follow the convention of writing operations on the left and mappings on the right. A (universal) *algebra* with universe  $A$  is a pair  $\mathcal{A} = (A, \Omega)$  where  $\Omega$  is a set of (finitary or infinitary) operations on  $A$ . For a subset  $B \subseteq A$  we shall denote by  $\langle B \rangle$  the subalgebra generated by  $B$ .

Let  $\mathcal{A}$  and  $\mathcal{B}$  be algebras. Then a *morphism* from  $\mathcal{A}$  to  $\mathcal{B}$  is any mapping  $\alpha$  from  $A$  to  $B$  that preserves the operations of  $\mathcal{A}$ . Note that such a mapping can only reasonably exist if  $\mathcal{A}$  and  $\mathcal{B}$  have the ‘same’ operations, in some sense. However, in this paper we shall only consider morphisms from an algebra to itself and so this concern does not affect us. A morphism which is injective and surjective is called an *isomorphism*. An *endomorphism of  $\mathcal{A}$*  is a morphism from  $\mathcal{A}$  to  $\mathcal{A}$ . Since composition of endomorphisms is associative the set of all endomorphisms of  $\mathcal{A}$  is a semigroup, which we denote by  $\text{End}(\mathcal{A})$ .

We now introduce the notion that is central to the results contained in this paper. Let  $\mathcal{A}$  be an algebra with universe  $A$  and let  $X \subseteq A$ .

**Definition 1.2.** We say that  $X$  is *independent* if every mapping  $\alpha : X \rightarrow \mathcal{A}$  can be extended to a morphism  $\epsilon_\alpha : \langle X \rangle \rightarrow \mathcal{A}$  such that the restriction of  $\epsilon_\alpha$  to  $X$  equals  $\alpha$

$$\epsilon_\alpha|_X = \alpha.$$

For an arbitrary mapping  $\alpha$  from an independent set  $I$  to  $\mathcal{A}$  we shall denote by  $\epsilon_\alpha$  the extension of  $\alpha$  to an endomorphism from  $\langle I \rangle$  to  $\mathcal{A}$ .

There are many definitions of independence in different mathematical structures. Here we follow the definition of Marczewski in [16] and [17]. We say that  $B$  is a *basis* for  $\mathcal{A}$  if  $B$  is an independent generating set for  $\mathcal{A}$ . For  $\alpha, \beta \in \text{End}(\mathcal{A})$  it is clear that

$$\alpha = \beta \text{ if and only if } \alpha|_B = \beta|_B.$$

There are many well-known algebraic structures, such as vector spaces, which have bases. There are also many algebraic structures without bases. We give an example of such a structure. Let  $p$  be a prime and let  $\mathbb{Z}_p$  denote the cyclic group of order  $p$ . Inductively, let  $\mathbb{Z}_{p^i}$  be the cyclic group of order  $p^i$ , where  $\mathbb{Z}_{p^{i-1}}$  is a subgroup of  $\mathbb{Z}_{p^i}$ . We denote the countable union of this ascending chain of subgroups  $\bigcup_{i=1}^{\infty} \mathbb{Z}_{p^i}$  by  $\mathbb{Z}_{p^\infty}$ . This group can also be described as the set of all the  $p^{\text{th}}$  roots of unity with the usual complex multiplication. It is easy to verify that this group is not finitely generated and that the maximum size of an independent set is one.

For more information about semigroups or algebras see [4], [5], [12] or [14].

## 2. The main result

Throughout this section let  $\mathcal{A}$  denote an algebra with infinite basis  $B$ . In order to prove our main result we partition  $B$  into countably many disjoint sets  $B_0, B_1, B_2, \dots$  so that each  $B_i$  has cardinality equal to that of  $B$ . Similarly, we partition  $B_0$  into countably many disjoint sets  $B_{0,1}, B_{0,2}, B_{0,3}, \dots$  so that each  $B_{0,i}$  has cardinality equal to that of  $B$ .

**Remark 2.1.** Let  $\alpha \in \text{End}(\mathcal{A})$  be an arbitrary endomorphism, let  $i \in \mathbb{N}$  and let  $\beta$  be any bijection from  $B$  into  $B_{0,i}$ . Then the mapping  $\delta_i$  from  $B_{0,i}$  to  $\mathcal{A}$  defined by

$$b\delta_i = b\beta^{-1}\alpha|_B \quad (b \in B_{0,i})$$

satisfies  $\beta\delta_i = \alpha|_B$ , and hence  $\epsilon_\beta\epsilon_{\delta_i} = \alpha$ .

We now prove our main result.

**Theorem 2.2.** *Let  $\mathcal{A}$  be an algebra which has an infinite basis. Then any countable subset of  $\text{End}(\mathcal{A})$  is contained in a 2-generated subsemigroup of  $\text{End}(\mathcal{A})$ .*

*Proof.* Let  $\{\alpha_1, \alpha_2, \alpha_3, \dots\}$  be our countable subset of elements of  $\text{End}(\mathcal{A})$ . We find two elements of  $\text{End}(\mathcal{A})$  which generate a semigroup that contains this set.

Let  $\beta$  be any mapping from  $B$  to  $B \setminus B_0$  which maps  $B_i$  to  $B_{i+1}$  bijectively for each  $i \in \{0, 1, 2, \dots\}$ . Since  $B$  is independent  $\beta$  can be extended to an endomorphism  $\epsilon_\beta$  of  $\mathcal{A}$ .

We define the second of our mappings  $\gamma$  from  $B$  to  $\mathcal{A}$  in two stages. First, we define  $\gamma$  on  $B \setminus B_0$  to be any mapping which takes  $B_i$  to  $B_{0,i}$  bijectively, for each  $i \in \{1, 2, 3, \dots\}$ . We observe that  $\phi_i = \beta\gamma\beta^i\gamma$  is a (well-defined) bijection from  $B$  to  $B_{0,i}$ .

By Remark 2.1 it follows that for each  $i \in \mathbb{N}$  there exists a mapping  $\delta_i$  such that  $\phi_i\delta_i = \alpha_i|_B$ . We now complete the definition of  $\gamma$  so that for  $b \in B_{0,i}$  we have  $b\gamma = b\delta_i$ . Hence for each  $i \in \mathbb{N}$  we have

$$\alpha_i|_B = \phi_i\delta_i = \phi_i\gamma = \beta\gamma\beta^i\gamma^2.$$

It follows that  $\alpha_i = \epsilon_\beta\epsilon_\gamma\epsilon_\beta^i\epsilon_\gamma^2$ , and so  $\{\alpha_1, \alpha_2, \alpha_3, \dots\} \subseteq \langle \epsilon_\beta, \epsilon_\gamma \rangle$ .  $\square$

For the remainder of this section we shall give examples of algebras which satisfy the condition of our theorem, i.e. algebras which have infinite bases.

Let  $\mathfrak{A}$  be a class of algebras. Then every free  $\mathfrak{A}$ -algebra  $\mathcal{A}$  on an infinite set  $X$  has an infinite basis, namely  $X$ . That  $X$  generates  $\mathcal{A}$  is evident and that  $X$  is independent follows immediately from the definition of a free algebra.

**Corollary 2.3.** *Let  $\mathcal{A}$  be a non-finitely generated free  $\mathfrak{A}$ -algebra. Then every countable subset of  $\text{End}(\mathcal{A})$  is contained in a 2-generated subsemigroup of  $\text{End}(\mathcal{A})$ .*

Examples of such algebras are the non-finitely generated free algebras of any variety.

Another example of a type of algebra which satisfies our condition is provided by a class of algebras which includes finite and infinite dimensional vector spaces as special cases. In order to define this class we require a slightly different definition of independence. Let  $\mathcal{A}$  be an algebra with universe  $A$  and let  $X \subseteq A$ . Then we

say  $X$  is  $T$ -independent if  $x \notin \langle X \setminus \{x\} \rangle$  for each  $x \in X$ . An algebra  $\mathcal{A}$  is called an *independence algebra* if it satisfies the following properties:

- (i) for every subset  $X$  of  $A$  and every element  $u$  of  $A$ , if  $X$  is  $T$ -independent and  $u \notin \langle X \rangle$ , then  $X \cup \{u\}$  is  $T$ -independent;
- (ii) for any basis  $X$  of  $\mathcal{A}$  and any function  $\alpha$  from  $X$  to  $\mathcal{A}$ , there is an endomorphism  $\epsilon_\alpha$  of  $\mathcal{A}$  such that  $\epsilon_\alpha|_X = \alpha$ .

The notions of  $T$ -independence and independence are not equivalent in general, but in the case of independence algebras they coincide. Independence algebras were first introduced in [18] and the basic structure of their endomorphism semigroups was described in [11]. This study, for both finite and infinite independence algebras, was continued in [1], [2], [7], [8] and [10]. Examples of independence algebras are (unstructured) sets, vector spaces and for any group  $G$ , free  $G$ -sets. It is clear that any independence algebra  $\mathcal{A}$  has a basis, the cardinality of which is called the *dimension of  $\mathcal{A}$* .

**Corollary 2.4.** *Let  $\mathcal{A}$  be an infinite dimensional independence algebra. Then any countable subset of  $\text{End}(\mathcal{A})$  is contained in a 2-generated subsemigroup of  $\text{End}(\mathcal{A})$ .*

Since every vector space is an independence algebra this corollary provides a shorter proof of Theorem 3.1 in [15].

### 3. Concluding remarks

We conclude the paper by giving an example of a finitely generated free algebra  $\mathcal{A}$  for which it is not true that every countable subset of  $\text{End}(\mathcal{A})$  is contained in a two-generated subsemigroup of  $\text{End}(\mathcal{A})$ , thereby demonstrating that we cannot omit the condition that  $\mathcal{A}$  is non-finitely generated from Corollary 2.3.

Let  $X$  be a non-empty set. Recall that an element  $\alpha$  of the semigroup  $\mathcal{T}_X$ , of all mappings from  $X$  to  $X$ , is called a *proper idempotent* if  $\alpha^2 = \alpha$  and  $\alpha \neq 1_X$ , the identity map on  $X$ . For a subsemigroup  $T$  of  $\mathcal{T}_X$  and a set  $Y \subseteq X$  we say that  $X$  is  $T$ -isomorphic to  $Y$  if there exist mappings  $\delta, \gamma \in T$  such that  $X\delta \subseteq Y$ ,  $Y\gamma \subseteq X$ ,  $\delta\gamma = 1_X$  and  $\gamma\delta|_Y = 1_Y$ , where  $1_X$  and  $1_Y$  denote the identity maps on  $X$  and  $Y$  respectively.

We require the following result:

**Lemma 3.1.** *Let  $X$  be an infinite set and let  $T$  be a subsemigroup of  $\mathcal{T}_X$  which satisfies the following:*

- (i) *the identity  $1_X$  is in  $T$ ;*
- (ii) *there exists  $\alpha \in T$  such that  $\alpha$  is not injective;*
- (iii) *there exists  $\beta \in T$  such that  $\beta$  is not surjective but is injective;*

*If every countable subset of  $T$  can be embedded in a 2-generated subsemigroup of  $T$  then  $X$  is  $T$ -isomorphic to the image of a proper idempotent in  $T$ .*

For a proof see [15, Theorem 2.4].

Let  $A = \{a, b\}$  be an arbitrary two element alphabet. Then we denote by  $A^+$  the free semigroup on  $A$ . That is all finite, non-empty words on  $A$  with the product of two words  $u$  and  $v$  being the juxtaposition  $uv$  of  $u$  and  $v$ .

**Proposition 3.2.** *It is not possible to embed every countable set of endomorphisms of  $A^+$  in a 2-generated subsemigroup of  $\text{End}(A^+)$ .*

*Proof.* It is obvious that  $\text{End}(A^+) \leq \mathcal{T}_{A^+}$ . We verify that  $\text{End}(A^+)$  satisfies the properties (i) to (iii) of Lemma 3.1. Clearly  $1_{A^+} \in \text{End}(A^+)$ . Let  $\alpha$  be any endomorphism satisfying  $a\alpha = b$  and  $b\alpha = b$ ; it is evident that  $\alpha$  is not injective. Let  $\beta$  be any endomorphism satisfying  $a\beta = ab$  and  $b\beta = ab^2$ ; it is clear that  $\beta$  is not surjective but is injective.

It is easy to verify that every proper idempotent endomorphism of  $A^+$  has image  $\{a\}^+$  or  $\{b\}^+$ . Suppose that every countable subset of  $\text{End}(A^+)$  can be embedded in a 2-generated subsemigroup of  $\text{End}(A^+)$ . Then, by Lemma 3.1, there exist  $\delta, \gamma \in \text{End}(A^+)$  such that  $A^+\delta \subseteq \{a\}^+$ ,  $\{a\}^+\gamma \subseteq A^+$ ,  $\delta\gamma = 1_{A^+}$  and  $\gamma\delta|_{\{a\}^+} = 1_{\{a\}^+}$ . But it is clear that no subset of  $\{a\}^+$  has  $A^+$  as a homomorphic image, and hence we have a contradiction.  $\square$

The analogue of Sierpiński's result for subsets of the symmetric group was shown to be true in [9]. As we went from mappings of unstructured sets to endomorphisms of algebras, we ask if we can move from permutations of sets to automorphisms of algebras.

**Open Problem 3.3.** *Find algebras  $\mathcal{A}$  for which every countable subset of the group of automorphisms  $\text{Aut}(\mathcal{A})$  of  $\mathcal{A}$  is contained in a 2-generated subgroup of  $\text{Aut}(\mathcal{A})$ .*

*Acknowledgements:* The first author would like to acknowledge the support of 'Financiamento Plurianual do CAUL' and Fundação para a Ciência e a Tecnologia (FCT) and Fundo Europeu de Desenvolvimento Regional (FEDER) project number POCTI/32440/MAT/2000. The second author would like to acknowledge the support of FCT and FEDER project 'Financiamento Programático de CAUL'. The third author would like to acknowledge the support of 'Financiamento Plurianual do CAUL', FEDER and FCT grant number SFRH/BD/6081/2001.

## REFERENCES

- [1] ARAÚJO, J., *Generators for the semigroup of endomorphisms of an independence algebra*, Algebra Colloquium 9:4 (2002), 375-382.
- [2] ARAÚJO, J., *Normal semigroups of endomorphisms of proper independence algebras are idempotent generated*, Proc. Edinburgh Math. Soc. 45 (2002), 205-217.
- [3] BANACH, S., *Sur un théorème de M. Sierpiński*, Fund. Math. 25 (1935), 5-6.
- [4] BURRIS, S. and SANKAPPANAVAR, S.P., *A course in universal algebra*, Graduate Texts in Math. No. 78, Springer-Verlag, 1981.
- [5] COHN, P.M., *Universal algebra*, Mathematics and its applications, Vol. 6, D. Reidel Publishing Co., 1981.
- [6] EVANS, T., *Embedding theorems for multiplicative systems and projective geometries*, Proc. Amer. Math. Soc. 3 (1952), 614-620.
- [7] FOUNTAIN, J. and LEWIN, A., *Products of idempotent endomorphisms of an independence algebra of finite rank*, Proc. Edinburgh Math. Soc. 35 (1992), 493-500.
- [8] FOUNTAIN, J. and LEWIN, A., *Products of idempotent endomorphisms of an independence algebra of infinite rank*, Math. Proc. Cambridge Phil. Soc. 114 (1993), 303-319.
- [9] GALVIN, F., *Generating countable sets of permutations*, J. London Math. Soc. 51 (1995), 230-242.

- [10] GOMES, G.M.S. and HOWIE, J.M., *Idempotent endomorphisms of an independence algebra of finite rank*, Proc. Edinburgh Math. Soc. *38* (1995), 107-116.
- [11] GOULD, V., *Independence algebras*, Algebra Universalis *33* (1995), 294-318.
- [12] HIGGINS, P.M., *Techniques of semigroup theory*, Oxford Publications, The Clarendon Press, Oxford University Press, New York, 1992.
- [13] HIGGINS, P.M., HOWIE, J.M., MITCHELL, J.D. and RUŠKUC, N., *Countable versus uncountable ranks in full transformation semigroup*, submitted.
- [14] HOWIE, J.M., *Fundamentals of semigroup theory*, Oxford University Press, 1995.
- [15] MAGILL, K.D., *The countability index of the endomorphism semigroup of a vector space*, Linear and multilinear algebra *22* (1988), 349-360.
- [16] MARCZEWSKI, E., *A general scheme of the notions of independence in mathematics*, Bulletin de l'academie polonaise des sciences *VI* (1958), 731-736.
- [17] MARCZEWSKI, E., *Independence in algebras of sets and boolean algebras*, Fund. Math. *48* (1960), 137-145.
- [18] NARKIEWICZ, W., *Independence in a certain class of abstract algebras*, Fund. Math. *50* (1961/62), 333-340.
- [19] NEUMANN, B.H., *Embedding theorems for semigroups*, J. London Math. Soc. *35* (1960), 184-192.
- [20] SIERPIŃSKI, W., *Sur les suites infinies de fonctions définies dans les ensembles quelconques*, Fund. Math. *24* (1935), 209-212.
- [21] SUBBIAH, S., *Some finitely generated subsemigroups of  $S(X)$* , Fund. Math. *86* (1975), 221-231.
- [22] SUBBIAH, S., *Another proof of a theorem of Evans*, Semigroup Forum *6* (1973), 93-94.

J. ARAÚJO,  
 UNIVERSIDADE ABERTA,  
 R. ESCOLA POLITÉCNICA, 147  
 1269-001 LISBOA,  
 PORTUGAL  
 &  
 CENTRO DE ÁLGEBRA,  
 UNIVERSIDADE DE LISBOA,  
 1619-003 LISBOA,  
 PORTUGAL  
 MJOAO@LMC.FC.UL.PT

J.D. MITCHELL,  
 CENTRO DE ÁLGEBRA,  
 UNIVERSIDADE DE LISBOA,  
 1619-003 LISBOA,  
 PORTUGAL  
 MITCHELL@CIL.FC.UL.PT

N. SILVA,  
 MATHEMATICS INSTITUTE,  
 UNIVERSITY OF ST ANDREWS,  
 NORTH HAUGH,  
 ST ANDREWS,  
 FIFE,  
 KY16 9SS,  
 UK  
 &  
 CENTRO DE ÁLGEBRA,  
 UNIVERSIDADE DE LISBOA,  
 1619-003 LISBOA,  
 PORTUGAL  
 NELSON@MCS.ST-AND.AC.UK