Bull. Austral. Math. Soc. 20m20, 20m99
Vol. 57 (1998) [59–71]

PRODUCTS OF TWO IDEMPOTENT TRANSFORMATIONS OVER ARBITRARY SETS AND VECTOR SPACES

Rachel Thomas

In this paper we consider the characterisation of those elements of a transformation semigroup S which are a product of two proper idempotents. We give a characterisation where S is the endomorphism monoid of a strong independence algebra A, and apply this to the cases where A is an arbitrary set and where A is an arbitrary vector space. The results emphasise the analogy between the idempotent generated subsemigroups of the full transformation semigroup of a set and of the semigroup of linear transformations from a vector space to itself.

1. Introduction

The full transformation semigroup $T(X)$ of a set X consists of all transformations from X to itself under composition of transformations. In 1966 Howie described the subsemigroup $E(X)$ of $T(X)$ generated by the proper idempotents (that is, those not the identity) of $T(X)$ for an arbitrary set X.

Several results analogous to those involving the products of idempotents in $T(X)$ have been discovered for $L(V)$, the semigroup of all linear transformations from a vector space V to itself, under composition of transformations. The subsemigroup $E(V)$ of $L(V)$ generated by the proper idempotent linear transformations of $L(V)$ was described by Erdos (in [**2**]) for a finite dimensional vector space, and by Reynolds and Sullivan (in [**11**]) for an infinite dimensional space. These descriptions are similar to Howie's results for the set case.

These semigroups, $T(X)$ and $L(V)$, are in fact examples of *independence algebras*. The descriptions of the idempotent generated subsemigroup of *End*(A), the semigroup of endomorphisms of an independence algebra A, by Fountain and Lewin in [**3**] and [**4**] are generalisations of the corresponding results for $T(X)$ and $L(V)$ and begin to explain the links between these structures.

Received 7th April, 1997
This paper was written while the author was a research student under the supervision of Dr R.P. Sullivan, whose support and advice the author acknowledges. The author also acknowledges the assistance of Mr B. Murphy with the typesetting of this paper. Finally, the author acknowledges the support of an Australian Postgraduate Award.

This paper further explores the comparable nature of these idempotent generated semigroups by characterising the products of two proper idempotents in each case. We present the most general result in Section 2. The result is a description of those elements that are the products of two proper idempotents in $End(A)$ for an arbitrary independence algebra A. The applications of this result to $T(X)$ for an arbitrary set X and $L(V)$ for an arbitrary vector space V are presented, with further implications, in sections 3 and 4.

2. Products of 2 idempotents in strong independence algebras

The following is taken from [**3**] and [**4**].

If A is an algebra, the subalgebra generated by a subset X of A is denoted $\langle X \rangle$. The unique minimum subalgebra of A is denoted $\langle \emptyset \rangle$. It is the subalgebra generated by the constants of A if A contains constants, and is the empty set otherwise.

A subset X of A is said to be *independent* if $X = \emptyset$ or $x \notin \langle X \setminus \{x\} \rangle$ for every element $x \in X$. When the algebra A is a set, every subset of A is independent, and when A is a vector space every linearly independent subset of A is independent.

An algebra with the following equivalent properties [**3**, Proposition 1.1] is said to have the *exchange property* ([EP]).

Proposition 1. *For an algebra A, the following conditions are equivalent.*

1. *For every subset X of A and all elements u, v of A, if $u \in \langle X \cup \{v\} \rangle$ and $u \notin \langle X \rangle$, then $v \in \langle X \cup \{u\} \rangle$.*
2. *For every subset X of A and every element u of A, if X is independent and $u \notin \langle X \rangle$, then $X \cup \{u\}$ is independent.*
3. *For every subset X of A, if Y is a maximal independent subset of X, then $\langle X \rangle = \langle Y \rangle$.*
4. *For subsets X, Y of A with $Y \subseteq X$, if Y is independent, then there is an independent set Z with $Y \subseteq Z \subseteq X$ and $\langle Z \rangle = \langle X \rangle$.*

A *basis* for an algebra A is an independent subset which generates A. If an algebra has the exchange property, then it has a basis which can be equivalently defined as a minimal generating set or maximal independent subset of A. Also if an algebra A has the exchange property then any independent subset can be extended to a basis for A (see [**3**] for further discussion).

An *independence algebra* A is one which has the exchange property and also satisfies the following condition.

[F] *For any basis X of A and any function $\alpha : X \to A$, there is an endomorphism $\overline{\alpha}$ of A such that $\overline{\alpha}|_X = \alpha$.*

A homomorphism α on an independence algebra A can be uniquely defined by specifying its action on the elements of a basis of A, similar to the way in which linear maps on vector spaces can be defined. Also the following is true (this is an extension of [**3**, Lemma 1.5]). Note we follow [**11**] by denoting the set $\{e_i : i \in I\}$ by $\{e_i\}$ when the index set is unambiguous.

LEMMA 1. *Let α be an endomorphism of an independence algebra A. If $\{x_i\}$ is an independent subset of* $\operatorname{Im}\alpha$ *and if for every i, $y_i \in A$ is chosen such that $y_i\alpha = x_i$, then $\{y_i\}$ is independent.*

In an independence algebra A, we define a *complement* of a subalgebra V in A to be a subalgebra U such that if $\{u_i\}$ is a basis for U and $\{v_j\}$ is a basis for V then $\{u_i\} \cup \{v_j\}$ is a basis for A. When this definition is applied to the particular examples of A being a set or vector space, it is the usual definition of complements in these cases.

It is true that if X and Y are independent subsets of an independence algebra such that $X \cup Y$ is independent then $\langle X\rangle \cap \langle Y\rangle = \langle\emptyset\rangle$. If an independence algebra A also satisfies the converse of this statement, that is

[S] *If X and Y are two independent subsets of A such that $\langle X\rangle \cap \langle Y\rangle = \langle\emptyset\rangle$, then $X \cup Y$ is independent also,*

then it is a *strong* independence algebra. Vector spaces and sets are both examples of strong independence algebras.

The following lemma is from [**7**].

LEMMA 2. *Let S be a regular semigroup. If a=ex, where $a, e \in S$ and e^2 =e, then there exists f in S such that $a = fx$, $f\mathcal{R}\ a$ and $f^2 = f$.*

It is noted in [**4**] that $End(A)$ is a regular semigroup for an independence algebra A. Therefore Lemma 2 (and its dual) can be applied by taking $S = End(A)$. Let $\alpha \in End(A)$ such that $\alpha = \delta_1 \dots \delta_k$ for some proper idempotents δ_i. Then there exist two proper idempotents η_1 and η_k such that $\alpha = \eta_1\delta_2 \dots \delta_{k-1}\eta_k$ and $\alpha\mathcal{R}\eta_1$ and $\alpha\mathcal{L}\eta_k$ (where $\mathcal{R}, \mathcal{L}$ are two of Green's relations). The following proposition is part of [**3**, Proposition 1.3]. Note that $\ker\alpha = \{(a, b) \in A \times A : a\alpha = b\alpha\}$.

PROPOSITION 2. *Let A be an independence algebra. Then for $\alpha, \beta \in End(A)$,*

1. *$\alpha\mathcal{L}\beta$ if and only if* $\operatorname{Im}\alpha = \operatorname{Im}\beta$,
2. *$\alpha\mathcal{R}\beta$ if and only if* $\ker\alpha = \ker\beta$.

Hence by this proposition and Lemma 2, if A is an independence algebra and $\alpha \in End(A)$ is a product of k proper idempotents, $\alpha = \delta_1 \dots \delta_k$, then without loss of generality we can assume $\ker\alpha = \ker\delta_1$ and $\operatorname{Im}\alpha = \operatorname{Im}\delta_k$.

We now characterise those endomorphisms of a strong independence algebra A that are products of two proper idempotents. Note that id_A refers to the identity relation on the algebra A.

THEOREM 1. *Let A be a strong independence algebra and let $\alpha \in End(A)$. Then α is a product of two proper idempotents in End(A) if and only if* $\ker\alpha \neq \mathrm{id}_A$ *and there exists a complement U of* $\operatorname{Im}\alpha$ *in A such that for any complement W of* $\operatorname{Fix}\alpha$ *and for any element $v \in \operatorname{Im}\alpha \cap W$ there is an element $u \in U$ such that $u\alpha = v$.*

https://doi.org/10.1017/S0004972700031427 Published online by Cambridge University Press

PROOF: Let $\alpha \in End(A)$ such that $\ker\alpha \neq \mathrm{id}_A$ and let $\{e_j\}$ be a basis for $\mathrm{Fix}\,\alpha$. As $\ker\alpha \neq \mathrm{id}_A$, $\mathrm{Fix}\,\alpha \neq A$ and hence the subalgebra $\mathrm{Fix}\,\alpha$ has a nontrivial complement in A. If W is any such complement of $\mathrm{Fix}\,\alpha$ in A, let $\{e_k\alpha, e_r\}$ be a basis for W where $\{e_k\alpha\}$ is a basis for $W \cap \mathrm{Im}\,\alpha$. Then by the definition of a complement of a subalgebra, $\{e_j, e_k\alpha, e_r\}$ is a basis for A. So $\{e_j, e_k\alpha\}$ is an independent subset of $\mathrm{Im}\,\alpha$ which can be expanded (by the [EP]) to a basis $\{e_j, e_k\alpha, e_m\}$ for $\mathrm{Im}\,\alpha$.

Suppose there is an element $x \in \langle e_r\rangle$, $x \notin \langle\emptyset\rangle$ such that $x \in \mathrm{Im}\,\alpha$. Then $x \in \langle e_k\alpha\rangle$ as $\langle e_r\rangle \subseteq W$, and thus $\langle e_k\alpha\rangle \cap \langle e_r\rangle \neq \langle\emptyset\rangle$. However this contradicts the independence of $\{e_k\alpha, e_r\}$ and so $\langle e_r\rangle \cap \mathrm{Im}\,\alpha = \langle\emptyset\rangle$. That is, $\langle e_r\rangle \cap \langle e_j, e_k\alpha, e_m\rangle = \langle\emptyset\rangle$, and as A is a strong independence algebra, it must be that $\{e_r, e_j, e_k\alpha, e_m\}$ is independent. But this contradicts the basis $\{e_j, e_k\alpha, e_r\}$ being a maximal independent set in A. Hence $\{e_m\} = \emptyset$ and $\{e_j, e_k\alpha\}$ is a basis for $\mathrm{Im}\,\alpha$.

Then $\{e_j, e_k\}$ is independent by Lemma 1 and we can extend this to a basis $\{e_j, e_k, e_q\}$ for A. So we can describe α by its action on this basis:

$$\alpha = \begin{pmatrix} e_j & e_k & e_q \\ e_j & e_k\alpha & e_q\alpha \end{pmatrix}.$$

Now suppose that $\alpha = \delta_1\delta_2$ for two proper idempotents in $End(A)$. Then by Proposition 2, we can assume without loss of generality that $\ker\alpha = \ker\delta_1$ and $\mathrm{Im}\,\alpha = \mathrm{Im}\,\delta_2$. Therefore as δ_1 is a proper idempotent, $\ker\alpha \neq \mathrm{id}_A$.

Consider the set $\{e_k\delta_1\}$. Let $w \in \langle e_k\delta_1\rangle$, $w \notin \langle\emptyset\rangle$ and suppose $w \in \mathrm{Im}\,\alpha = \mathrm{Im}\,\delta_2$. Then $w\delta_1 = w$ as $w \in \mathrm{Im}\,\delta_1$ and $w\delta_2 = w$ as $w \in \mathrm{Im}\,\delta_2$. That is, $w\alpha = w$ and thus $w \in \langle e_j\rangle$. Also as $w = w\delta_2 \in \langle e_k\delta_1\rangle\delta_2 = \langle e_k\alpha\rangle$, we have $\langle e_j\rangle \cap \langle e_k\alpha\rangle \neq \langle\emptyset\rangle$. However as this contradicts the independence of $\{e_j, e_k\alpha\}$, $w \notin \mathrm{Im}\,\alpha$ and $\langle e_k\delta_1\rangle \cap \langle e_j, e_k\alpha\rangle = \langle\emptyset\rangle$. Therefore $\{e_j, e_k\alpha, e_k\delta_1\}$ is independent and can be extended to a basis $\{e_j, e_k\alpha, e_k\delta_1, e_i\}$ for A. If $U = \langle e_k\delta_1, e_i\rangle$ then U is a complement of $\mathrm{Im}\,\alpha$. Moreover if v is any element of $\mathrm{Im}\,\alpha \cap W$ where W is an arbitrary complement of $\mathrm{Fix}\,\alpha$, then $v \in \langle e_k\alpha\rangle = \langle e_k\delta_1\rangle\alpha$. That is, there is an element $u \in \langle e_k\delta_1\rangle \subseteq U$ such that $u\alpha = v$. Hence if an endomorphism α is a product of two proper idempotents, the condition in the statement of the theorem is satisfied.

Conversely, suppose $\alpha \in End(A)$, $\ker\alpha \neq \mathrm{id}_A$ and there is a complement U of $\mathrm{Im}\,\alpha$ such that for every complement W of $\mathrm{Fix}\,\alpha$ and for all $v \in \mathrm{Im}\,\alpha \cap W$ there is an element $u \in U$ such that $u\alpha = v$. Using our earlier notation, let $W = \langle e_k\alpha, e_r\rangle$ be the complement of $\mathrm{Fix}\,\alpha$ described above, where $\langle e_k\alpha\rangle = W \cap \mathrm{Im}\,\alpha$. Then for each $k \in K$, there is an element $u_k \in U$ such that $u_k\alpha = e_k\alpha$. By Lemma 1 $\{u_k\}$ is independent and we extend this to a basis $\{u_k, e_i\}$ for the complement U of $\mathrm{Im}\,\alpha$. So we have two bases for A, $\{e_j, e_k, e_q\}$ and $\{e_j, e_k\alpha, u_k, e_i\}$ and we now use these to define several endomorphisms over A.

To define the first, we note that for each $q \in Q$ as $e_q\alpha \in \langle e_j, e_k\alpha\rangle = \langle e_j, e_k\rangle\alpha$, there is some element $w_q \in \langle e_j, e_k\rangle$ such that $w_q\alpha = e_q\alpha$. We then define an endomorphism δ_1

by

$$\begin{aligned} e_j\delta_1 &= e_j, \\ e_k\delta_1 &= u_k, \\ e_q\delta_1 &= w_q\delta_1. \end{aligned}$$

We define a second endomorphism δ_2 by

$$\begin{aligned} e_j\delta_2 &= e_j, \\ e_k\alpha\delta_2 &= e_k\alpha, \\ u_k\delta_2 &= e_k\alpha, \\ e_i\delta_2 &= e_i. \end{aligned}$$

Then $e_j\delta_1\delta_2 = e_j$ and $e_k\delta_1\delta_2 = e_k\alpha$ and $\delta_1\delta_2$ equals α on the independent set $\{e_j, e_k\}$. Moreover as $w_q \in \langle e_j, e_k\rangle$, $e_q\delta_1\delta_2 = w_q\delta_1\delta_2 = w_q\alpha = e_q\alpha$. Therefore $\delta_1\delta_2$ equals α on a basis of A, and hence $\delta_1\delta_2 = \alpha$.

Consider the endomorphism γ defined by

$$\begin{aligned} e_j\gamma &= e_j, \\ e_k\alpha\gamma &= u_k, \\ e_m\gamma &= e_m, \end{aligned}$$

where $\{e_j, e_k\alpha, e_m\}$ is a basis for A. Then $e_j\alpha\gamma = e_j$ and $e_k\alpha\gamma = u_k$ and so $\alpha\gamma|_{\langle e_j,e_k\rangle} = \delta_1|_{\langle e_j,e_k\rangle}$. Then again as $w_q \in \langle e_j,\, e_k\rangle$, $e_q\delta_1 = w_q\delta_1 = w_q\alpha\gamma = e_q\alpha\gamma$, and we have $\alpha\gamma = \delta_1$. In fact, as $\alpha = \delta_1\delta_2$ also, $\alpha\mathcal{R}\delta_1$. Hence by Proposition 2 , $\ker\alpha = \ker\delta_1$.

Furthermore, as $u_k\alpha = e_k\alpha$, $u_k\delta_1 = e_k\delta_1 = u_k$. Also as $w_q\delta_1 \in \langle e_j,\, u_k\rangle$, $\operatorname{Im}\delta_1 = \langle e_j, e_k, e_q\rangle\delta_1 = \langle e_j, u_k, w_q\delta_1\rangle = \langle e_j, u_k\rangle$. Thus, δ_1 fixes its image and is an idempotent. It is a proper idempotent as $\ker\delta_1 = \ker\alpha \neq \mathrm{id}_A$.

It is clear from its definition that δ_2 is an idempotent. If $|K| = 0$ then $\operatorname{Im}\alpha = \operatorname{Fix}\alpha$ and α is itself a proper idempotent. In which case $\alpha = \alpha^2$, a product of two proper idempotents. Else if $|K| > 0$, then δ_2 is a proper idempotent and $\alpha = \delta_1\delta_2$, a product of two proper idempotents.

Thus the sufficiency of the condition is proved. $\square$

3. Products of two idempotents in $T(X)$

The following theorem is the application of Theorem 1 to the case of A being an arbitrary set X. This result extends the characterisation found in [**8**] to encompass X being an infinite set.

Theorem 2. *If X is an arbitrary set and $\alpha \in T(X)$ then α is a product of two proper idempotents if and only if $\ker\alpha \neq \mathrm{id}_X$ and for every $y \in X\alpha$ such that $y\alpha \neq y$ there exists an element $x \in X \setminus X\alpha$ such that $x\alpha = y$.*

https://doi.org/10.1017/S0004972700031427 Published online by Cambridge University Press

We now examine several idempotent generated subsemigroups of $T(X)$ when X is an infinite set.

In his description of $E(X)$ for an infinite set X [6], Howie used the following cardinals:

$$\begin{aligned} d(\alpha) &= |X \setminus X\alpha| && \text{the } \textit{defect} \text{ of } \alpha, \\ s(\alpha) &= \left|\{s \in X : x\alpha \neq x\}\right| && \text{the } \textit{shift} \text{ of } \alpha, \\ c(\alpha) &= \left|\bigcup\{y\alpha^{-1} : |y\alpha^{-1}| \geqslant 2\}\right| && \text{the } \textit{collapse} \text{ of } \alpha. \end{aligned}$$

The description is, if $|X| \geqslant \aleph_0$, then $E(X) = F \cup I$ where

$$F = \left\{\alpha \in T(X) : 0 < d(\alpha) \leqslant s(\alpha) < \aleph_0\right\}$$

and

$$I = \left\{\alpha \in T(X) : d(\alpha) = s(\alpha) = c(\alpha) \geqslant \aleph_0\right\}.$$

For some cardinal m, let

$$Q_m = \left\{\alpha \in T(X) : d(\alpha) = s(\alpha) = c(\alpha) = m \geqslant \aleph_0\right\}.$$

Then the set I can be thought of as

$$I = \bigcup_{m=\aleph_0}^{m=|X|} Q_m.$$

It was shown in [7] that F and all the sets Q_m, $\aleph_0 \leqslant m \leqslant |X|$, are regular, idempotent generated subsemigroups of $T(X)$ (that is, if $\alpha \in S$ where S is F or one of the Q_m, then α is a product of idempotents in S). Also proved was that if ε was an idempotent in $T(X)$ and the defect, shift or collapse of ε was equal to m, where $\aleph_0 \leqslant m \leqslant |X|$, then $\varepsilon \in Q_m$ [**7**, Lemma 2.8]. Marques in [**9**] examined the Rees quotient semigroup $P_m = Q_m/I_m$ where $I_m = \{\alpha \in Q_m : |X\alpha| < m\}$ is an ideal of Q_m. She also showed that P_m is idempotent generated and can be viewed as $P_m = J_m \cup 0$ where $J_m = \{\alpha \in Q_m : r(\alpha) = m\}$ and $\alpha\beta = 0$ for some $\alpha, \beta \in J_m$ if $r(\alpha\beta) < m$.

The following corollary examines the products of two proper idempotents in P_m and Q_m.

COROLLARY 1. *Let S denote P_m or Q_m and suppose $\alpha \in S$ ($\alpha \neq 0$). Then α is a product of two proper idempotents in S if and only if* $\ker\alpha \neq \mathrm{id}_X$ *and for every $y \in X\alpha$ such that $y\alpha \neq y$ there exists an element $x \in X \setminus X\alpha$ such that $x\alpha = y$.*

PROOF: Suppose $\alpha = \lambda\mu$ for some proper idempotents $\lambda, \mu \in S$. Then α is a product of two proper idempotents in $T(X)$ and so, by Theorem 2, the condition as stated in the corollary must hold. Conversely, suppose $\alpha \in S$, $\ker\alpha \neq \mathrm{id}_X$ and for every $y \in X\alpha$ such that $y\alpha \neq y$ there exists an $x \in X \setminus X\alpha$ such that $x\alpha = y$. Then, by Theorem 2, $\alpha = \lambda\mu$ for some proper idempotents $\lambda, \mu \in T(X)$ and by Lemma 2 we can assume that

$\ker\alpha = \ker\lambda$ and $\operatorname{Im}\alpha = \operatorname{Im}\mu$. Therefore, $c(\alpha) = c(\lambda)$ and $d(\alpha) = d(\mu)$. Hence, by [7, Lemma 2.8], if $\alpha \in Q_m$ then $\lambda, \mu \in Q_m$ also. Moreover, if either λ or μ have rank strictly less than m the the same is true of α. That is, if $\alpha \in P_m$ then $\lambda, \mu \in P_m$ also. ∎

The following semigroups K_m and L_m are regular subsemigroups of P_m when m is regular or singular respectively.

$$K_m = \left\{\alpha \in P_m : \left|y\alpha^{-1}\right| = m \text{ for some } y \in X\right\} \cup 0$$

and

$$L_m = \left\{\alpha \in P_m : \text{for all } p < m\ \exists y \in X \text{ such that } \left|y\alpha^{-1}\right| > p\right\} \cup 0.$$

Note that $K_m \subseteq L_m$ for any set X.

Let S denote K_m or L_m. In [**10**, Proposition 3.3], the authors aimed to characterise when a nilpotent with index two in S is a product of two idempotents in S. However, suppose X is a union of disjoint sets U and R, where $|U| = |R| = m \geqslant \aleph_0$ and ϕ is a bijection from R to U. Consider the transformation α defined by

$$U\alpha = u_0,$$

where u_0 is some element of U, and

$$r\alpha = r\phi$$

for every $r \in R$. Then α is a product of two idempotents as it satisfies the condition in Theorem 2. However $|C(\alpha) \setminus X\alpha| = 0$ (where $C(\alpha) = \bigcup\{y\alpha^{-1} : |y\alpha^{-1}| \geqslant 2\}$) and hence α is a counter-example to the proposition in [**10**].

Note that this transformation α is also a counter-example to [**10**, Proposition 3.1]. This proposition will be corrected and generalised in a forthcoming paper.

We now correct and generalise [**10**, Proposition 3.3].

Corollary 2. *Let S denote K_m or L_m and suppose $\alpha \in S$ ($\alpha \neq 0$). Then α is a product of two proper idempotents in S if and only if $\ker\alpha \neq \mathrm{id}_X$ and for every $y \in X\alpha$ such that $y\alpha \neq y$ there exists an element $x \in X \setminus X\alpha$ such that $x\alpha = y$.*

Proof: As before, if α is a product of two proper idempotents in S then it is a product of two proper idempotents in $T(X)$ and so, by Theorem 2, $\ker\alpha \neq \mathrm{id}_X$ and for every $y \in X\alpha$ not fixed by α, there is an element $x \in X \setminus X\alpha$ such that $x\alpha = y$. Conversely, suppose $\alpha \in S$ and this condition holds. Then by Theorem 2, $\alpha = \lambda\mu$ for some proper idempotents $\lambda, \mu \in T(X)$ and as before we can assume $\lambda, \mu \in P_m$ and $\ker\alpha = \ker\lambda$. Hence, from the definitions of K_m and L_m, we deduce that $\lambda \in S$. In addition, since $d(\lambda) = m$ (as $\lambda \in Q_m$) we can choose an element $a \notin X\alpha$ and replace μ by μ' defined by:

$$\begin{aligned} x\mu' &= x\mu \quad \text{if } x \in X\lambda, \text{ and} \\ x\mu' &= a \quad\ \ \text{if } x \notin X\lambda. \end{aligned}$$

https://doi.org/10.1017/S0004972700031427 Published online by Cambridge University Press

Then μ' is a proper idempotent in P_m. In fact, as $|a(\mu')^{-1}| = |X \setminus X\lambda| = m$, $\mu' \in K_m$ and consequently $\mu' \in L_m$ as $K_m \subseteq L_m$. Hence α is a product of two proper idempotents λ and μ' in S. $\square$

4. Products of two idempotents in $L(V)$

In this section we apply Theorem 1 to the case when $A = L(V)$, the semigroup of all linear transformations on an arbitrary vector space V. We then give an alternative characterisation of the products of two proper idempotents in $L(V)$ when V is a finite dimensional vector space.

We now present the notation that will be used in the vector space setting.

If $\{\mathbf{e}_i : i \in I\}$ (bold text is used only for vectors) is a basis for a vector space V, we can define an element $\alpha \in L(V)$ by defining the action of α on the basis, and extending the action of α linearly to the whole of V. For example we write

$$\alpha = \begin{pmatrix} \mathbf{e}_i \\ \mathbf{a}_i \end{pmatrix}$$

where $\mathbf{a}_i = \mathbf{e}_i\alpha$ for all $i \in I$.

For an element $\alpha \in L(V)$, the *rank* of α is the dimension $r(\alpha)$ of $\operatorname{Im}\alpha$ and $n(\alpha)$, the *nullity* of α, is the dimension of the nullspace. The nullspace of α is referred to as $\ker\alpha$, the *kernel* of α, and the subspace $\{\mathbf{x} \in V : \mathbf{x}\alpha = \mathbf{x}\}$ is referred to as $\operatorname{Fix}\alpha$.

Lemma 2 can be interpreted in a vector space setting. Namely, if S is the regular subsemigroup $E(V)$ of $L(V)$ (for proof of regularity for arbitrary vector spaces see [**11**]) and $\alpha = \delta_1 \dots \delta_k$, a product of proper idempotents δ_i in $L(V)$, the lemma implies that there exist two proper idempotents η_1 and η_k in $E(V)$ such that $\alpha = \eta_1\delta_2 \dots \delta_{k-1}\eta_k$ and $\eta_1\mathcal{R}\alpha$ and $\eta_k\mathcal{L}\alpha$. By [**1**, Exercise 6, p.57] we have $\ker\alpha = \ker\eta_1$ and $\operatorname{Im}\alpha = \operatorname{Im}\eta_k$. This fact and Theorem 1 now establish the following result. Note that the equivalence relation $\ker\alpha$ is not equal to id_A if and only if $n(\alpha) \neq 0$ when A is a vector space.

Theorem 3. *If V is an arbitrary vector space and $\alpha \in L(V)$ then α is the product of two proper idempotents in $L(V)$ if and only if $n(\alpha) \neq 0$ and there exists a complement U of $\operatorname{Im}\alpha$ such that for every complement W of $\operatorname{Fix}\alpha$ and for every $\mathbf{v} \in \operatorname{Im}\alpha \cap W$, there exists some $\mathbf{u} \in U$ such that $\mathbf{u}\alpha = \mathbf{v}$.*

Suppose that $\alpha \in L(V)$ is a product of two proper idempotents in $L(V)$ and that $\{\mathbf{e}_j\}$ is a basis for $\operatorname{Fix}\alpha$. Let W be any complement of $\operatorname{Fix}\alpha$ and let $\{\mathbf{e}_k\alpha\}$ be a basis for $\operatorname{Im}\alpha \cap W$. Consider the complement U of $\operatorname{Im}\alpha$ referred to in the proof of Theorem 1, where $\{\mathbf{u}_k, \mathbf{e}_i\}$ is a basis for the complement U such that each of the $\mathbf{u}_k$ is the pre-image of the corresponding basis element of $W \cap \operatorname{Im}\alpha$. It was seen in the proof of Theorem 1 that $\{\mathbf{e}_j, \mathbf{e}_k\alpha, \mathbf{u}_k, \mathbf{e}_i\}$ is a basis for V. Also, it can easily be shown that $\{\mathbf{e}_j, \mathbf{e}_k, \mathbf{e}_q\}$ is a basis for V where $\{\mathbf{e}_q\}$ is a basis for $\ker\alpha$.

Hence if V is finite dimensional and α is a product of two proper idempotents in $L(V)$ we must have

$$|Q| = |K| + |I|.$$

So

$$|Q| \geqslant |K|,$$

and hence

$$n(\alpha) \geqslant r(\alpha) - f(\alpha)$$

where $f(\alpha) = \dim(\operatorname{Fix}\alpha)$. In fact the converse is also true.

PROPOSITION 3. *Let $\alpha \in L(V)$ for a finite dimensional vector space V, with α not the identity transformation on V, and suppose*

$$n(\alpha) \geqslant r(\alpha) - f(\alpha).$$

Then α is a product of two proper idempotents.

PROOF: Suppose we have $\alpha \in L(V)$, α not the identity transformation, $\dim(V) = n$ and $n(\alpha) \geqslant r(\alpha) - f(\alpha)$ (note that this implies $n(\alpha) > 0$). Let $\{\mathbf{u}_1, \dots, \mathbf{u}_j\}$ be a basis for $\operatorname{Fix}\alpha$, and let W be any complement of $\operatorname{Fix}\alpha$. If $\{\mathbf{v}_1\alpha, \dots, \mathbf{v}_k\alpha\}$ is a basis for the subspace $W \cap \operatorname{Im}(\alpha)$ then it is straightforward to show that $\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1\alpha, \dots, \mathbf{v}_k\alpha\}$ is a basis for $\operatorname{Im}\alpha$ and

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{w}_1, \dots, \mathbf{w}_q\}$$

is a basis for V where $\{\mathbf{w}_1, \dots, \mathbf{w}_q\}$ is a basis for $\ker\alpha$. Therefore by our hypothesis we must have that $q \geqslant k$.

If $\mathbf{v}_i \in \operatorname{Im}\alpha$ for all $i = 1, \dots, k$, then $\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_k\}$ must be a basis for $\operatorname{Im}\alpha$. If this is the case, consider the set

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \dots, \mathbf{v}_1, \dots, \mathbf{v}_k, \dots, \mathbf{w}_1 + \mathbf{v}_1, \dots, \mathbf{w}_k + \mathbf{v}_k\}.$$

Then the equation

$$\sum_{i=1}^{j} a_i \mathbf{u}_i + \sum_{i=1}^{k} b_i \mathbf{v}_i + \sum_{i=1}^{k} c_i(\mathbf{w}_i + \mathbf{v}_i) = 0$$

is equivalent to

$$\sum_{i=1}^{j} a_i \mathbf{u}_i + \sum_{i=1}^{k} (b_i + c_i)\mathbf{v}_i + \sum_{i=1}^{k} c_i \mathbf{w}_i = 0$$

which has only the trivial solution as $\{\mathbf{u}_1, \dots, \mathbf{u}_j, \ \mathbf{v}_1, \dots, \mathbf{v}_k, \mathbf{w}_1, \dots \mathbf{w}_k\}$ is independent. Hence this set can be extended to a basis

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1 \dots, \mathbf{v}_k, \mathbf{w}_1 + \mathbf{v}_1, \dots, \mathbf{w}_k + \mathbf{v}_k, \mathbf{z}_1, \dots, \mathbf{z}_r\}$$

for V. If

$$U = \langle \mathbf{w}_1 + \mathbf{v}_1, \dots, \mathbf{w}_k + \mathbf{v}_k, \mathbf{z}_1, \dots, \mathbf{z}_r \rangle$$

then U is a complement of $\operatorname{Im}\alpha$ that satisfies the condition in Theorem 3. Hence α is a product of two proper idempotents in $L(V)$.

Otherwise if $\mathbf{v}_i \notin \operatorname{Im}\alpha$ for some $i = 1, \dots, k$, assume that we have ordered $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ in such a way that $\mathbf{v}_i \in \operatorname{Im}\alpha$ for $i = 1, \dots, m$ $(m < k)$ and $\mathbf{v}_i \notin \operatorname{Im}\alpha$ for $i = m+1, \dots, k$. It follows that $\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m\}$ is a linearly independent set contained in $\operatorname{Im}\alpha$, so we can extend it to a basis $\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_p\}$ for $\operatorname{Im}\alpha$. Note that $p = k - m$ as $r(\alpha) = j + m + (k - m)$.

Now consider the subspace

$$M = \langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_k \rangle$$

which has dimension $j + m + (k - m) + r$ where $r \leqslant k - m$. If $k - m = r$ then the linearly independent set

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_k\}$$

is a basis for M. Otherwise, if this set is linearly dependent, the equation

$$\sum_{i=1}^{j} a_i \mathbf{u}_i + \sum_{i=1}^{m} b_i \mathbf{v}_i + \sum_{i=1}^{k-m} c_i \mathbf{x}_i + \sum_{i=m+1}^{k} d_i \mathbf{v}_i = \mathbf{0}$$

has a nontrivial solution for the scalars a_i, b_i, c_i and d_i. As

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}\}$$

is linearly independent, one of the d_i, say d_k is nonzero (there is no loss of generality as the set $\{\mathbf{v}_{m+1}, \dots, \mathbf{v}_k\}$ can be reordered if necessary). Then

$$\mathbf{v}_k \in \langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{k-1} \rangle,$$

that is,

$$M = \langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{k-1} \rangle.$$

If the set

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{k-1}\}$$

is still linearly dependent, we remove another of the $\mathbf{v}_i$, $(i = m+1, \dots, k-1)$, say $\mathbf{v}_{k-1}$, as above and continue in this way until we have a linearly independent set

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}\}$$

spanning M.

Now the subspace

$$\langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_k, \mathbf{w}_1, \dots, \mathbf{w}_q \rangle$$

contains a basis for V so it must have dimension n. As we have just seen

$$\{\mathbf{v}_{m+r+1}, \dots, \mathbf{v}_k\} \subseteq \langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r} \rangle.$$

so

$$V = \langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}, \mathbf{w}_1, \dots, \mathbf{w}_q \rangle.$$

Suppose the equation

$$\sum_{i=1}^{j} a_i \mathbf{u}_i + \sum_{i=1}^{m} b_i \mathbf{v}_i + \sum_{i=1}^{k-m} c_i \mathbf{x}_i + \sum_{i=m+1}^{k} d_i \mathbf{v}_i + \sum_{i=1}^{q} e_i \mathbf{w}_i = \mathbf{0}$$

has a nontrivial solution in the scalars a_i, b_i, c_i, d_i and e_i. As

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}\}$$

is linearly independent, $e_i \neq 0$ for some $i \in \{1, \dots, q\}$, say $e_q \neq 0$. Thus

$$V = \langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}, \mathbf{w}_1, \dots, \mathbf{w}_{q-1} \rangle.$$

As before for the basis of M, we continue removing elements of the set $\{\mathbf{w}_i : i = 1, \dots, q-1\}$ until we have a linearly independent set

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}, \mathbf{w}_1, \dots, \mathbf{w}_{q-r}\}$$

that spans V.

Then, as $q \geqslant k$ by our hypothesis, there are at least $k - r$ distinct vectors in $\{\mathbf{w}_1, \dots, \mathbf{w}_{q-r}\}$. So consider the set

$$\begin{aligned} B \;=\; \{&\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}, \\ &\mathbf{v}_1 + \mathbf{w}_1, \dots, \mathbf{v}_m + \mathbf{w}_m, \mathbf{v}_{m+r+1} + \mathbf{w}_{m+1}, \dots, \mathbf{v}_k + \mathbf{w}_{k-r}\}. \end{aligned}$$

We now show that this set is linearly independent. Suppose

$$\sum_{i=1}^{j} a_i \mathbf{u}_i + \sum_{i=1}^{m} b_i \mathbf{v}_i + \sum_{i=1}^{k-m} c_i \mathbf{x}_i + \sum_{i=m+1}^{m+r} d_i \mathbf{v}_i + \sum_{i=1}^{m} e_i (\mathbf{v}_i + \mathbf{w}_i) + \sum_{i=m+r+1}^{k} f_i (\mathbf{v}_i + \mathbf{w}_{i-r}) = 0$$

for some scalars a_i, b_i, c_i, d_i, e_i and f_i.

Now as

$$\mathbf{v}_i \in \langle \mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r} \rangle$$

https://doi.org/10.1017/S0004972700031427 Published online by Cambridge University Press

for all $i = 1, \dots, m$ and $i = m+r+1, \dots, k$ these $\mathbf{v}_i$ can be written as linear combinations of the vectors in the set

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}\}.$$

The coefficients of the vectors in this set can then be collected to give

$$\sum_{i=1}^{j} a_i' \mathbf{u}_i + \sum_{i=1}^{m} b_i' \mathbf{v}_i + \sum_{i=1}^{k-m} c_i' \mathbf{x}_i + \sum_{i=m+1}^{m+r} d_i' \mathbf{v}_i + \sum_{i=1}^{m} e_i \mathbf{w}_i + \sum_{i=m+r+1}^{k} f_i \mathbf{w}_{i-r} = 0$$

for some scalars $a_i', b_i', c_i', d_i', e_i$ and f_i. Thus $e_i = 0$ for all $i = 1, \dots, m$ and $f_i = 0$ for all $i = m + r + 1, \dots, k$ as

$$\{\mathbf{u}_1, \dots, \mathbf{u}_j, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_1, \dots, \mathbf{x}_{k-m}, \mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}, \mathbf{w}_1, \dots, \mathbf{w}_{q-r}\}$$

is linearly independent. This implies that the original coefficients a_i, b_i, c_i and d_i are also all zero. That is we have shown that the set B is linearly independent. As the set B contains a basis for $\operatorname{Im}\alpha$, the elements of B not contained in this basis, that is those in the set

$$\{\mathbf{v}_{m+1}, \dots, \mathbf{v}_{m+r}, \mathbf{v}_1 + \mathbf{w}_1, \dots, \mathbf{v}_m + \mathbf{w}_m, \mathbf{v}_{m+r+1} + \mathbf{w}_{m+1}, \dots, \mathbf{v}_k + \mathbf{w}_{k-r}\}$$

can be extended to a basis for a complement U of $\operatorname{Im}\alpha$. Then for every basis element $\mathbf{v}_i\alpha$, $i = 1, \dots, k$ of the intersection of W, the arbitrary complement of $\operatorname{Fix}\alpha$, and $\operatorname{Im}\alpha$, there is an element $\mathbf{z}_i$ in U such that $\mathbf{z}_i\alpha = \mathbf{v}_i\alpha$. Namely,

$$\begin{aligned}
\mathbf{v}_i\alpha &= (\mathbf{v}_i + \mathbf{w}_i)\alpha, \text{ for } i = 1, \dots, m \\
\mathbf{v}_i\alpha &= \mathbf{v}_i\alpha, \text{ for } i = m+1, \dots, m+r \\
\mathbf{v}_i\alpha &= (\mathbf{v}_i + \mathbf{w}_{i-r})\alpha, \text{ for } i = m+r+1, \dots, k.
\end{aligned}$$

Thus for every element $\mathbf{v} \in \operatorname{Im}\alpha \cap W$ for any complement W of $\operatorname{Fix}\alpha$ there is an element $\mathbf{u}$ in U such that $\mathbf{u}\alpha = \mathbf{v}$. Hence from the previous theorem, α is a product of two proper idempotents. $\square$

Hence, as a consequence of this proposition and the discussion preceding it, we have the following result concerning linear transformations over finite dimensional vector spaces.

THEOREM 4. *Let $\alpha \in L(V)$ for a finite dimensional vector space V, α not the identity transformation. Then α is a product of two proper idempotents in $L(V)$ if and only if*

$$n(\alpha) \geqslant r(\alpha) - f(\alpha).$$

In [5], a result of Laffey received in personal correspondance is mentioned. The result is that every $n \times n$ matrix of rank less than $n/2$ is a product of two idempotent matrices. If we consider a matrix of rank less than $n/2$, then the following set of inequalities hold:

$$\begin{aligned} n &\geqslant 2r(\alpha) \\ n - r(\alpha) = n(\alpha) &\geqslant r(\alpha) \\ n(\alpha) &\geqslant r(\alpha) - f(\alpha), \end{aligned}$$

and by the previous theorem we have that α is a product of two proper idempotents. Hence the previous theorem is a generalisation of the result of Laffey mentioned in [5].

References

[1] A.H. Clifford and G.B. Preston, *The algebraic theory of semigroups* (American Mathematical Society, Providence, R.I., 1961).

[2] J.A. Erdos, 'On products of idempotent matrices', *Glasgow Math. J.* **8** (1967), 118–122.

[3] J. Fountain and A. Lewin, 'Products of idempotent endomorphisms of an independence algebra of finite rank', *Proc. Edinburgh Math. Soc.* **35** (1992), 493–500.

[4] J. Fountain and A. Lewin, 'Products of idempotent endomorphisms of an independence algebra of infinite rank', *Math. Proc. Cambridge Philos. Soc.* **114** (1993), 303–319.

[5] E. Giraldes and J.M. Howie, 'Embedding finite semigroups in finite semibands of minimal depth', *Semigroup Forum* **28** (1984), 135–142.

[6] J.M. Howie, 'The subsemigroup generated by the idempotents of a full transformation semigroup', *J. London Math. Soc.* **41** (1966), 707–716.

[7] J.M. Howie, 'Some subsemigroups of infinite full transformation semigroups', *Proc. Roy Soc Edinburgh Sect. A* **88** (1981), 159–167.

[8] J.M. Howie, E.F. Robertson and B.M. Schein, 'A combinatorial property of finite full transformation semigroups', *Proc. Roy. Soc. Edinburgh Sect. A* **109** (1988), 319–328.

[9] M. Paula and O. Marques, 'A congruence-free semigroup associated with an infinite cardinal number', *Proc. Roy. Soc. Edinburgh Sect. A* **93** (1983), 245–257.

[10] M. Paula, O. Marques-Smith and R.P. Sullivan, 'Nilpotents and congruences on semigroups of transformations with fixed rank', *Proc. Roy. Soc. Edinburgh Sect. A* **125** (1995), 399–412.

[11] M.A. Reynolds and R.P. Sullivan, 'Products of idempotent linear transformations', *Proc. Roy. Soc. Edinburgh Sect. A* **100** (1985), 123–138.

Department of Mathematics
The University of Western Australia
Nedlands WA 6907
Australia