An Elementary Proof That Every Singular Matrix Is a Product of Idempotent Matrices

J. Araújo and J. D. Mitchell

In this note we give an elementary proof of a theorem first proved by J. A. Erdos [3]. This theorem, which is the main result of [3], states that every noninvertible $n \times n$ matrix is a finite product of matrices M with the property that $M^2 = M$. (These are known as *idempotent matrices*. Noninvertible matrices are also called *singular matrices*.) An alternative formulation of this result reads: every noninvertible linear mapping of a finite dimensional vector space is a finite product of idempotent linear mappings α, linear mappings that satisfy $\alpha^2 = \alpha$. This result was motivated by a result of J. M. Howie asserting that each self-mapping α of a nonempty finite set X with image size at most $|X| - 1$ (which occurs precisely when α is noninvertible) is a product of idempotent mappings. We shall see that Erdos's theorem is a consequence of Howie's result.

Together the papers [3] and [4] are cited in over one hundred articles, dealing with subjects including universal algebra, ring theory, topology, and combinatorics. Since its publication, various proofs of the result in [3] have appeared. For example, a semigroup theoretic proof appears in [1, pp. 121-131] and linear operator theory is used to prove the theorem in [2]. Here we give a new proof using a basic combinatorial argument. Unlike the previous proofs our argument involves only elementary results from linear algebra and one basic result concerning permutations. On the way to proving the main result of this note we provide a short proof of Howie's result.

Throughout this paper X signifies an arbitrary nonempty finite set. If $\alpha : A \to X$, where A is a subset of X, then A is the *domain of* α; we denote this set by $\mathrm{dom}(\alpha)$. Naturally, the set $\alpha(A)$ is called the *image of* α and is denoted by $\mathrm{im}(\alpha)$. Recall that a mapping α is *injective* (or *one-to-one*) if $\alpha(x) \neq \alpha(y)$ for all x and y in $\mathrm{dom}(\alpha)$ with $x \neq y$. Let $\mathcal{T}_X$ denote the set of all mappings from X to X with domain X. We note that this set is closed under composition of mappings and that this composition is associative. We now define one of the most important notions we require in the proofs in this note. For a mapping $\alpha : \mathrm{dom}(\alpha) \to X$ we say that α is a *restriction* of an element β of $\mathcal{T}_X$ if β and α agree on the domain of α. In other words, $\beta(x) = \alpha(x)$ for all x in $\mathrm{dom}(\alpha)$. For x and y in X we denote the transposition that fixes every point of X other than x or y and that maps x to y, and vice versa, by $(x\ y)$.

1 HOWIE'S THEOREM.

We begin by reproving Theorem I in [4]:

Theorem 1.1 (Howie). *Every noninvertible mapping in $\mathcal{T}_X$ is a finite product of idempotent mappings in $\mathcal{T}_X$.*

We prove this result by showing that every noninvertible mapping is the product of an idempotent and an injective mapping (not in $\mathcal{T}_X$) with image size strictly less than $|X|$. We will find it useful to write mappings in a particular form. For example, if $X = \{1, 2, 3, 4\}$, then the mapping

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 2 & 1 \end{pmatrix},$$

can be written as

$$\begin{pmatrix} \{1,3\} & \{2\} & \{4\} \\ 2 & 4 & 1 \end{pmatrix}.$$

For an arbitrary finite set X, let α in $\mathcal{T}_X$ be an arbitrary noninvertible mapping. If the image of α is $\{x_1, x_2, \ldots, x_n\}$, then for each i we denote by A_i the largest subset of X satisfying $\alpha(A_i) = x_i$. As in the preceding example, we can write

$$\alpha = \begin{pmatrix} A_1 & A_2 & \cdots & A_n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}.$$

Choose for each i an arbitrary but fixed element a_i of A_i, and define a mapping ϵ with domain $\{x_1, x_2, \ldots, x_n\}$ that takes x_i to a_i for each i. It is obvious that $\epsilon\alpha$ is an idempotent. Let ϵ^{-1} denote the mapping that takes a_i to x_i for each i. Since α is noninvertible we have $n < |X|$, and therefore we can express α as the product $\epsilon^{-1}(\epsilon\alpha)$ of the injective mapping ϵ^{-1}, with $|\operatorname{im}(\epsilon^{-1})| < |X|$, and the idempotent $\epsilon\alpha$. It remains to prove that any injective mapping with image size strictly less than $|X|$ is a restriction of a product of idempotents. We establish this in the next two lemmas.

Lemma 1.2. *Let $\alpha : \operatorname{dom}(\alpha) \to X$ be an injective mapping with $|\operatorname{im}(\alpha)| < |X|$ and with the property that $\alpha(x)$ belongs to $\operatorname{dom}(\alpha)$ for all x in $\operatorname{dom}(\alpha)$. Then there exists a finite product of idempotents π from $\mathcal{T}_X$ such that α is a restriction of π.*

Proof. Let u in $X \setminus \operatorname{dom}(\alpha)$, and let x and y in $\operatorname{dom}(\alpha)$ $(x \neq y)$ be arbitrary. Define mappings $\beta_{x,u}$, $\beta_{y,x}$, and $\beta_{u,y}$ in $\mathcal{T}_X$ that map x to u, y to x, and u to y, respectively, and that fix all other elements of X. It is easy to verify that these mappings are idempotents. The product $\beta_{u,y}\beta_{y,x}\beta_{x,u}$ maps x to y and y to x, and fixes all other elements of $\operatorname{dom}(\alpha)$. Therefore $\beta_{u,y}\beta_{y,x}\beta_{x,u}$, although defined on the whole of X, may be thought of as the transposition $(x\ y)$ of $\operatorname{dom}(\alpha)$. It is well known that every permutation of a finite set can be written as a product of transpositions of that set. Since α is a permutation of its domain the result follows. ■

We now apply Lemma 1.2 to prove that every injective mapping $\alpha : \mathrm{dom}(\alpha) \to X$ with image size strictly less than $|X|$ is the restriction of some product of idempotents from $\mathcal{T}_X$.

Lemma 1.3. *If $\alpha : \mathrm{dom}(\alpha) \to X$ is an injective mapping with $|\,\mathrm{im}(\alpha)| < |X|$, then there exists a finite product ρ of idempotent mappings from $\mathcal{T}_X$ such that α is a restriction of ρ.*

Proof. Partition $\mathrm{dom}(\alpha)$ into the sets $A = \{\, x \in \mathrm{dom}(\alpha) \,:\, \alpha(x) \in \mathrm{dom}(\alpha) \,\}$ and $B = \{\, x \in \mathrm{dom}(\alpha) \,:\, \alpha(x) \notin \mathrm{dom}(\alpha) \,\}$. Let σ be any permutation of $\mathrm{dom}(\alpha)$ such that $\sigma(a) = \alpha(a)$ for each a in A and is arbitrary elsewhere in $\mathrm{dom}(\alpha)$. By Lemma 1.2 we can find a product of idempotents π such that $\pi(x) = \sigma(x)$ for each x in $\mathrm{dom}(\alpha)$ (if $A = \emptyset$ then we assume that π is the mapping that fixes all the elements of $\mathrm{dom}(\alpha)$). For each element b of B define a mapping ϵ_b that maps $\pi(b)$ to $\alpha(b)$ and fixes the remaining elements of X. Each of these mappings is an idempotent. Let ϵ denote the product of all the mappings ϵ_b. It follows that $\alpha(x) = \epsilon\pi(x)$ for every x in $\mathrm{dom}(\alpha)$. Since both π and ϵ are products of idempotents, the conclusion follows. ■

Returning to the argument prior to Lemma 1.2, we observe that ϵ^{-1} is an injective mapping with $|\,\mathrm{im}(\epsilon^{-1})| < |X|$, so by Lemma 1.3 there exists a product of idempotents ρ such that ϵ^{-1} and ρ agree on the domain of ϵ^{-1}. It follows that $\alpha = \epsilon^{-1}(\epsilon\alpha) = \rho(\epsilon\alpha)$, which completes the proof of Theorem 1.1.

2 ERDOS'S THEOREM.

We now use Theorem 1.1 to reprove Erdos's result. In what follows we assume that $\mathcal{V}$ is a vector space of finite dimension over a field $\mathbb{F}$ and denote the zero vector of $\mathcal{V}$ by 0. We refer to a linear mapping $\alpha : \mathcal{V} \to \mathcal{V}$ as *nontrivial* if $\mathrm{im}(\alpha) \neq \langle\, 0 \,\rangle$. For a subset U of $\mathcal{V}$ we denote by $\langle\, U \,\rangle$ the subspace of $\mathcal{V}$ spanned by U.

We show that we can write a nontrivial noninvertible linear mapping α from $\mathcal{V}$ to $\mathcal{V}$ as the product of two linear mappings β and δ, where β maps some basis B (of $\mathcal{V}$) into B and δ maps $\beta(B)$ bijectively to $\alpha(B)$. To show that such a δ exists we must prove that for any basis B of $\mathcal{V}$ and any linearly independent set I in $\mathcal{V}$ there exists a linear mapping that takes some subset of B bijectively onto I. In general this is easy to accomplish, but we also require that δ be a product of idempotents. In this case, it is only possible to prove that such a linear mapping exists when the cardinality of the second independent set is strictly smaller than the dimension of $\mathcal{V}$. We take the initial step toward establishing the existence of δ with the following lemma.

Lemma 2.1. *For every nontrivial linear mapping $\alpha : \mathcal{V} \to \mathcal{V}$ there exists a basis B of $\mathcal{V}$ such that $\alpha(B)$ is a linearly independent set.*

Proof. Let I be a basis for the image of α, and let J be any set such that $\alpha(J) = I$ and $|J| = |I|$. Observe that, since I is a linearly independent set and $\alpha(J) = I$, J is also linearly independent. Let Z be a basis for the kernel of α (i.e., of the subspace $\ker(\alpha) = \{ v \in \mathcal{V} : \alpha(v) = 0 \}$). Note that Z may be empty. Since $\langle Z \rangle \cap \langle J \rangle = \langle 0 \rangle$, the union $Z \cup J$ is linearly independent. Moreover,

$$\dim(\mathcal{V}) = \dim(\ker(\alpha)) + \dim(\mathrm{im}(\alpha)) = |Z| + |J|,$$

so $Z \cup J$ is a basis for $\mathcal{V}$. Choose j in J. Then the set $B = J \cup (j + Z)$ is a basis for $\mathcal{V}$ and $\alpha(B) = I$, as required. ■

Next, we prove that the linear mapping δ in the foregoing discussion exists when our linearly independent sets differ by only a single element.

Lemma 2.2. *Let I be any linearly independent set in $\mathcal{V}$ for which there exists a j in $\mathcal{V}$ such that the set $I \cup \{j\}$ is linearly independent. Then for each i in I there exists an idempotent linear mapping $\delta : \mathcal{V} \to \mathcal{V}$ such that $\delta((I \setminus \{i\}) \cup \{j\}) = I$.*

Proof. Let B be any basis for $\mathcal{V}$ containing $I \cup \{j\}$. Define a mapping $\overline{\delta}$ that maps j to i and fixes all elements of $B \setminus \{j\}$. We extend this mapping in the usual way to a linear mapping δ from $\mathcal{V}$ to $\mathcal{V}$. It is clear that δ has the required property. ■

If our independent sets differ by more than one element, then we require the following lemma, which we prove by repeatedly applying Lemma 2.2.

Lemma 2.3. *Let B be an arbitrary basis for $\mathcal{V}$, and let I be an arbitrary linearly independent set in $\mathcal{V}$ that is not a basis for $\mathcal{V}$. Then there is a finite product δ of idempotent linear mappings from $\mathcal{V}$ to $\mathcal{V}$ that maps some subset of B bijectively to I.*

Proof. Suppose that $n = |I| (< |B|)$ and that i_1 belongs to I. Now B is not contained in $\langle I \rangle$, so there exists b_1 in B such that $I \cup \{b_1\}$ is linearly independent. By Lemma 2.2 there exists an idempotent linear mapping $\delta_1 : \mathcal{V} \to \mathcal{V}$ that maps $I_1 = (I \setminus \{i_1\}) \cup \{b_1\}$ to I. Next let i_2 be a vector in $I \setminus \{i_1\}$. Then, as before, there exists b_2 in B such that $I_1 \cup \{b_2\}$ is linearly independent, and there exists an idempotent linear mapping δ_2 that maps $I_2 = (I_1 \setminus \{i_2\}) \cup \{b_2\}$ to I_1. Continuing in this way we produce a sequence of linearly independent sets (of equal cardinality) $I_0 = I, I_1, \ldots, I_n$ such that $I_n \subseteq B$ and such that for each k there is an idempotent linear mapping δ_k of $\mathcal{V}$ that maps I_k to I_{k-1}. The mapping $\delta = \delta_1 \delta_2 \cdots \delta_n$ maps the subset I_n of B bijectively to I, as required. ■

We now turn to the main result of this note:

Theorem 2.4 (Erdos). *Every noninvertible linear mapping of a finite dimensional vector space $\mathcal{V}$ is a finite product of idempotent linear mappings.*

Proof. Let α be a noninvertible linear mapping from $\mathcal{V}$ to $\mathcal{V}$. If α is trivial, then α is an idempotent and the result holds in this case. Otherwise α is nontrivial, and by Lemma 2.1 we can find a basis B for $\mathcal{V}$ such that $\alpha(B)$ is linearly independent. Let $\overline{\alpha}$ denote the mapping that is equal to α on the elements of B but is undefined elsewhere in $\mathcal{V}$. By Lemma 2.3 there exists a product β of idempotent linear mappings of $\mathcal{V}$ such that some subset of B is mapped bijectively to $\alpha(B)$. But then $\beta^{-1}\overline{\alpha}$ is a mapping in $\mathcal{T}_B$. Moreover, $\beta^{-1}\overline{\alpha}$ is noninvertible since α is noninvertible. Hence $\beta^{-1}\overline{\alpha}$ is a product of idempotent mappings in $\mathcal{T}_B$ by Theorem 1.1. Each of these idempotent mappings can be extended to an idempotent linear mapping from $\mathcal{V}$ to $\mathcal{V}$. Let δ denote the product of these linear mappings. It follows that $\alpha(B) = \beta(\beta^{-1}\overline{\alpha})(B) = \beta\delta(B)$, demonstrating that $\alpha = \beta\delta$. Because both δ and β are products of idempotents, so is α. ■

Corollary 2.5 (Erdos). *Every singular $n \times n$ matrix is a finite product of idempotent matrices.*

The industrious reader might want to check that the (stronger) result that every singular $n \times n$ matrix with rank $k(< n)$ is a product of idempotents of rank k follows from the arguments given in this note.

ACKNOWLEDGMENTS. 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."

References

[1] R. J. H. Dawlings, *The Semigroup of Singular Endomorphisms of a Finite-Dimensional Vector Space*, Academic Press, New York 1980.

[2] D. Ž. Djoković, Note on a theorem on singular matrices, *Canad. Math. Bull.* **11** (1968) 283-284.

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

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

J. Araújo, Universidade Aberta, R. Escola Politécnica, 147, 1269-001 Lisboa, Portugal
&
Centro de Álgebra, Universidade de Lisboa, 1649-003 Lisboa, Portugal
mjoao@lmc.fc.ul.pt

J.D. Mitchell, University of Louisville, 328 Natural Sciences Bldg., Louisville, KY 40292, USA
jd.mitchell@louisville.edu