*Bull. Aust. Math. Soc.* **98** (2018), 402–413
doi:10.1017/S000497271800076X

# ON MINIMAL SETS OF (0, 1)-MATRICES WHOSE PAIRWISE PRODUCTS FORM A BASIS FOR $M_n(\mathbb{F})$

**W. E. LONGSTAFF**

(Received 25 February 2018; accepted 13 June 2018; first published online 28 August 2018)

Dedicated to Peter Rosenthal

**Abstract**

Three families of examples are given of sets of (0, 1)-matrices whose pairwise products form a basis for the underlying full matrix algebra. In the first two families, the elements have rank at most two and some of the products can have multiple entries. In the third example, the matrices have equal rank $\sqrt{n}$ and all of the pairwise products are single-entried (0, 1)-matrices.

2010 *Mathematics subject classification*: primary 15A30.

*Keywords and phrases*: matrix algebra, elementary matrices, basis.

## 1. Introduction

Let $\mathbb{F}$ be a field with identity denoted by 1 and let $M_n(\mathbb{F})$ denote the algebra of $n \times n$ matrices with entries in $\mathbb{F}$. We call a matrix having only one of its entries nonzero and its nonzero entry equal to 1 an *elementary matrix*. If this 1 is in the position $(i, j)$ we denote the matrix by $E_{i,j}$. If $\{A_i\}_\Gamma$ is a set of $n \times n$ matrices whose pairwise products, that is, the set of matrices $\{A_iA_j : i, j \in \Gamma\}$, form a basis for $M_n(\mathbb{F})$ then, obviously, the cardinality of $\Gamma$ is at least $n$. In [1] an example is given to show that this lower bound is attained whatever the value of $n$. In this example most, but not all, of the products are elementary matrices and the following question is raised.

QUESTION 1.1. *Is it possible to find n matrices in $M_n(\mathbb{F})$ whose set of pairwise products is the basis of $M_n(\mathbf{F})$ consisting of elementary matrices?*

We show (Theorem 3.5) that it is possible if $n$ is the square of an integer. If $n$ is not a square and $\mathbb{F}$ is the real or complex field, no set of (0, 1)-matrices with $n$ elements can have this property (Theorem 3.1).

## 2. Matrices of rank at most two

EXAMPLE 2.1. Let $\mathbb{F}$ be a field with identity denoted by 1. Let $n \in \mathbb{Z}^+$. For $1 \le i \le n$ define the $n \times n$ matrix $A_i \in M_n(\mathbb{F})$ by $A_i = E_{i,1} + E_{1,i}$. We show that the pairwise products of $\{A_1, A_2, \ldots, A_n\}$, that is, the set of matrices $\{A_iA_j : 1 \le i, j \le n\}$, is a basis for $M_n(\mathbb{F})$. Since this set has $n^2$ elements, we need only show that it spans $M_n(\mathbb{F})$, and to show this it is enough, in turn, to show that every elementary matrix $E_{i,j}$ belongs to the span. For the proof note that

(i) $E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$;
(ii) $E_{i,j} = A_iA_j$, if $i \ne 1,\ j \ne 1,\ i \ne j$;
(iii) $E_{1,1} = \frac{1}{4}A_1^2\ (= \frac{1}{2}A_1)$;
(iv) $E_{i,i} = A_i^2 - \frac{1}{4}A_1^2,\ 2 \le i \le n$;
(v) $E_{i,1} = \frac{1}{2}A_iA_1,\ 2 \le i \le n$;
(vi) $E_{1,j} = \frac{1}{2}A_1A_j,\ 2 \le j \le n$.

More generally, we have the following theorem. We introduce some notation to make computations with elementary matrices somewhat easier. In most of what follows we will denote the elementary matrix $E_{i,j}$ simply by $(i; j)$. From (i) above, we can write $(i; j)(k; l) = \delta_{j,k}(i; l)$.

THEOREM 2.2. *Let $\mathbb{F}$ be a field, $n \in \mathbb{Z}^+$ and $p \in \{1, 2, \ldots, n\}$ and let $\mu$ and $\sigma$ be permutations of $\{1, 2, \ldots, n\}$. Define $A_i \in M_n(\mathbb{F})$ by $A_i = (\mu(i); p) + (p; \sigma(i))$ for $1 \le i \le n$. The pairwise products of $\{A_1, A_2, \ldots, A_n\}$ form a basis for $M_n(\mathbb{F})$.*

PROOF. Since $A_{\mu^{-1}(i)} = (i; p) + (p; \sigma \cdot \mu^{-1}(i))$ we can suppose that $\mu = \iota$, the identity permutation. We will show that each of the $n^2$ elementary matrices $(i; j)$ belongs to $\mathcal{P} = \text{span}\{A_iA_j : 1 \le i, j \le n\}$.

For $1 \le i, j \le n$ and $i \ne \sigma^{-1}(p)$, $j \ne \sigma(p)$ and $j \ne \sigma^2(i)$,

$$A_iA_{\sigma^{-1}(j)} = ((i; p) + (p; \sigma(i)))((\sigma^{-1}(j); p) + (p; j)) = (i; j).$$

So $(i; j) \in \mathcal{P}$ if $i \ne \sigma^{-1}(p)$, $j \ne \sigma(p)$ and $j \ne \sigma^2(i)$. It remains to show that $(i; j) \in \mathcal{P}$ if $i = \sigma^{-1}(p)$ or $j = \sigma(p)$ or $j = \sigma^2(i)$.

*Case I*: $p = \sigma(p)$. Then $A_p = 2(p; p)$ and so $A_p^2 = 4(p; p)$. Hence $(p; p) = \frac{1}{4}A_p^2 \in \mathcal{P}$.

*Subcase I(a)*: $i = \sigma^{-1}(p)$. In this case, $i = p$ and we need to show that $(p; j) \in \mathcal{P}$, for $1 \le j \le n,\ j \ne p$. If $j \ne p$,

$$A_pA_{\sigma^{-1}(j)} = 2(p; p)((\sigma^{-1}(j); p) + (p; j)) = 2(p; j).$$

Hence $(p; j) = \frac{1}{2}A_pA_{\sigma^{-1}(j)} \in \mathcal{P}$, if $j \ne p$.

*Subcase I(b)*: $j = \sigma(p)$. In this case, $j = p$ and we need to show that $(i, p) \in \mathcal{P}$, for $1 \le i \le n, i \ne p$. If $i \ne p$,

$$A_iA_p = 2((i; p) + (p; \sigma(i)))(p; p) = 2(i; p).$$

Hence $(i; p) = \frac{1}{2}A_iA_p \in \mathcal{P}$, if $i \ne p$.

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

*Subcase I(c)*: $j = \sigma^2(i)$. We need to show that $(i;\sigma^2(i)) \in \mathcal{P}$, for $1 \le i \le n$, $i \ne p$. If $i \ne p$,

$$A_iA_{\sigma(i)} = ((i;p) + (p;\sigma(i)))((\sigma(i);p) + (p;\sigma^2(i))) = (i;\sigma^2(i)) + (p;p).$$

Hence $(i;\sigma^2(i)) = A_iA_{\sigma(i)} - \frac{1}{4}A_p^2 \in \mathcal{P}$, if $i \ne p$.

*Case II*: $p \ne \sigma(p)$. If $j \ne \sigma(p)$ and $j \ne \sigma^2(p)$,

$$A_{\sigma^{-1}(p)}A_{\sigma^{-1}(j)} = (\sigma^{-1}(p);j) + (p;j) \quad \text{and} \quad A_pA_{\sigma^{-1}(j)} = (p;j).$$

Hence,

$$(\sigma^{-1}(p);j) = A_{\sigma^{-1}(p)}A_{\sigma^{-1}(j)} - A_pA_{\sigma^{-1}(j)} \in \mathcal{P} \quad \text{whenever } j \ne \sigma(p), \sigma^2(p). \tag{2.1}$$

Also, if $i \ne \sigma^{-1}(p)$ and $i \ne \sigma^{-2}(p)$,

$$A_iA_p = (i;p) + (i;\sigma(p)) \quad \text{and} \quad A_iA_{\sigma^{-1}(p)} = (i;p).$$

Hence

$$(i;\sigma(p)) = A_iA_p - A_iA_{\sigma^{-1}(p)} \in \mathcal{P} \quad \text{whenever } i \ne \sigma^{-1}(p), \sigma^{-2}(p). \tag{2.2}$$

Now, if $i \ne \sigma^{-1}(p)$,

$$A_iA_{\sigma(i)} = (i;\sigma^2(i)) + (p;p).$$

Since $A_pA_{\sigma^{-1}(p)} = \delta(p;p)$ where $\delta = 1$ if $p \ne \sigma^2(p)$ and $\delta = 2$ if $p = \sigma^2(p)$,

$$(i;\sigma^2(i)) = A_iA_{\sigma^2(i)} - \frac{1}{\delta}A_pA_{\sigma^{-1}(p)} \in \mathcal{P} \quad \text{whenever } i \ne \sigma^{-1}(p). \tag{2.3}$$

Taking (2.1), (2.2) and (2.3) into consideration, to complete the proof it only remains to show that each of (i) $(\sigma^{-1}(p);\sigma(p))$, (ii) $(\sigma^{-1}(p);\sigma^2(p))$ and (iii) $(\sigma^{-2}(p);\sigma(p))$ belongs to $\mathcal{P}$ (still with $p \ne \sigma(p)$).

*Case (i)*: $(\sigma^{-1}(p);\sigma(p))$. If $p \ne \sigma^2(p)$,

$$(\sigma^{-1}(p);\sigma(p)) = A_{\sigma^{-1}(p)}A_p - A_p^2 - A_{\sigma^{-1}(p)}^2 + A_pA_{\sigma^{-1}(p)} \in \mathcal{P}.$$

If $p = \sigma^2(p)$,

$$(\sigma^{-1}(p);\sigma(p)) = (\sigma(p);\sigma(p)) = A_{\sigma(p)}A_p + \tfrac{1}{2}A_pA_{\sigma(p)} - A_p^2 - A_{\sigma(p)}^2 \in \mathcal{P}.$$

*Case (ii)*: $(\sigma^{-1}(p);\sigma^2(p))$. If $p \ne \sigma^2(p)$,

$$(\sigma^{-1}(p);\sigma^2(p)) = A_{\sigma^{-1}(p)}A_{\sigma(p)} - A_pA_{\sigma(p)} + A_pA_{\sigma^{-1}(p)} \in \mathcal{P}.$$

If $p = \sigma^2(p)$,

$$(\sigma^{-1}(p);\sigma^2(p)) = (\sigma(p);p) = A_{\sigma(p)}^2 - \tfrac{1}{2}A_pA_{\sigma(p)} \in \mathcal{P}.$$

*Case (iii)*: $(\sigma^{-2}(p);\sigma(p))$. Notice that

$$(\sigma^{-2}(p);\sigma(p)) = A_{\sigma^{-2}(p)}A_p - A_{\sigma^{-2}(p)}A_{\sigma^{-1}(p)} + \frac{1}{\delta}A_pA_{\sigma^{-1}(p)} \in \mathcal{P},$$

where, as before, $\delta = 1$ if $p \ne \sigma^2(p)$ and $\delta = 2$ if $p = \sigma^2(p)$.

This completes the proof. □

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

REMARK 2.3. The example given in [1] is of a type covered by the preceding theorem.

The next example shows that, with the $A_i$ defined as in the preceding theorem (with $\mu = \iota$), $\sigma$ need not be a permutation if the pairwise products span $M_n(\mathbf{F})$.

EXAMPLE 2.4. Define the mapping $\sigma : \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$ by $\sigma(1) = \sigma(3) = 2$ and $\sigma(2) = 3$. Define matrices $A, B, C \in M_3(\mathbf{F})$ by $A = (1; 1) + (1; 2)$, $B = (2; 1) + (1; 3)$ and $C = (3; 1) + (1; 2)$. We have the multiplication table:

| | $A$ | $B$ | $C$ |
|---|---|---|---|
| $A$ | $(1; 1) + (1; 2)$ | $(1; 3) + (1; 1)$ | $(1; 2)$ |
| $B$ | $(2; 1) + (2; 2)$ | $(2; 3)$ | $(2; 2) + (1; 1)$ |
| $C$ | $(3; 1) + (3; 2)$ | $(3; 3) + (1; 1)$ | $(3; 2)$ |

It is easily seen that the set of products in this table span, and so form a basis for, $M_3(\mathbb{F})$. This example is a simple case of the following general result.

THEOREM 2.5. *Let $n, p \in \mathbb{Z}^+$ with $n \geq 3$ and $1 \leq p \leq n$. If the map $\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ satisfies*

(i) $\sigma(\{1, 2, \ldots, n\}\backslash\{p\}) = \{1, 2, \ldots, n\}\backslash\{p\} = \text{range}(\sigma)$,
(ii) $\sigma(p) \neq \sigma^2(p)$,

*then the $n \times n$ matrices $A_i = (i; p) + (p; \sigma(i))$, for $1 \leq i \leq n$, have the property that the set of matrices $\{A_iA_j : 1 \leq i, j \leq n\}$ is a basis for $M_n(\mathbb{F})$.*

PROOF. Let $\mathcal{V}$ denote the span of $\{A_iA_j : 1 \leq i, j \leq n\}$. We show that $\mathcal{V} = M_n(\mathbb{F})$ by showing that $\mathcal{V}$ contains every elementary matrix $(i; j)$. Notice that $\sigma(p) = \sigma(q)$ for some $q \neq p$ and $q \neq \sigma(p)$ because $\sigma(p) \neq \sigma^2(p)$.

Let $1 \leq i \leq n$. Then

$$A_iA_q = ((i; p) + (p; \sigma(i)))((q; p) + (p; \sigma(p))) = (i; \sigma(p)) \in \mathcal{V}.$$

Since

$$A_iA_p = ((i; p) + (p; \sigma(i)))((p; p) + (p; \sigma(p))) = (i; p) + (i; \sigma(p),$$

it now follows that $(i; p) \in \mathcal{V}$. In particular, $(p; p) \in \mathcal{V}$. Then, from

$$A_iA_{\sigma(i)} = ((i; p) + (p; \sigma(i)))((\sigma(i); p) + (p; \sigma^2(i))) = (i; \sigma^2(i)) + (p; p),$$

it follows that $(i; \sigma^2(i)) \in \mathcal{V}$.

So far, we have shown that each of $(i; p), (i; \sigma(p))$ and $(i; \sigma^2(i))$ belongs to $\mathcal{V}$. For $1 \leq j \leq n$ and $j \notin \{p, \sigma(i)\}$,

$$A_iA_j = ((i; p) + (p; \sigma(i)))((j; p) + (p; \sigma(j))) = (i; \sigma(j)) \in \mathcal{V}.$$

Using property (i) in the statement of the theorem, it is easily shown that

$$\sigma(\{1, 2, \ldots, n\}\backslash\{p, \sigma(i)\}) = \{1, 2, \ldots, n\}\backslash\{p, \sigma^2(i)\},$$

and so we have proved that $(i; j) \in \mathcal{V}$ for $1 \leq i, j \leq n$. Thus $\mathcal{V} = M_n(\mathbf{F})$. □

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

Remark 2.6. Possibly the simplest example of a map $\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ satisfying the hypotheses of the preceding theorem is given by $\sigma(n) = 2, \sigma(i) = i + 1$ for $i \neq n$, and where we have taken $p = 1$.

Remark 2.7. Suppose the map $\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ satisfies $\sigma(p) = p$ and $\{A_iA_j : 1 \leq i, j \leq n\}$ is a basis for $M_n(\mathbb{F})$, where $A_i = (i; p) + (p; \sigma(i))$. Then $\sigma$ is a permutation of $\{1, 2, \ldots, n\}$. For, in this case, $A_p = 2(p; p)$. Let $\sigma(i) = \sigma(j)$. If neither $i$ nor $j$ is equal to $p$ then

$$A_pA_i = 2(p; p)((i; p) + (p; \sigma(i))) = 2(p; \sigma(i)) = 2(p; \sigma(j)) = A_pA_j$$

and so $i = j$ (since the set of products $\{A_rA_s : 1 \leq r, s \leq n\}$ is linearly independent). If $i = p$ and $j \neq p$ then $\sigma(i) = \sigma(j) = p$ and

$$A_jA_p = 2((j; p) + (p; p))(p; p) = 2((j; p) + (p; p)) = 2A_j^2,$$

and this is a contradiction.

## 3. Matrices of rank two or more

We turn our attention to generating sets of matrices with $n$ elements whose pairwise products are elementary matrices. In Theorem 2.5 above, each of the matrices $A_i$ is a $(0, 1)$-matrix with two nonzero entries. The same is true for the matrices in Theorem 2.2 if $\sigma(p) \neq p$ and $\mu = \iota$. We next show that, for real or complex matrices, if each generator $A_i$ is a $(0, 1)$-matrix with two nonzero entries, the pairwise products cannot all be elementary matrices unless $n = 4$.

Theorem 3.1. *Let $n \in \mathbb{Z}^+$ and let $\mathbb{F}$ be a field with characteristic zero in which $n$ has a square root. Let $\{A_i : 1 \leq i \leq n\} \subseteq M_n(\mathbb{F})$ be a set of $(0, 1)$-matrices such that:*

(i) *$A_i$ has $m_i$ nonzero entries for $1 \leq i \leq n$;*
(ii) *$A_iA_j$ is an elementary matrix for $1 \leq i, j \leq n$;*
(iii) *$\{A_iA_j : 1 \leq i, j \leq n\}$ is a basis for $M_n(\mathbb{F})$.*

*Then $A_i$ has rank equal to $m_i$ for $1 \leq i \leq n$ and $n = m^2$ for some positive integer $m$ satisfying $\sum_{i=1}^{n} m_i = nm$.*

Proof. Suppose that such a set $\{A_i : 1 \leq i \leq n\}$ of matrices exists. Let $1 \leq i \leq n$ and suppose that $(r; s)$ is a summand of $A_i$ . If no $A_p$ had a summand of the form $(s; t)$, for some $t$, then the $s$th row of each elementary matrix $A_xA_y$ would be zero. Since this is a contradiction, there exists $A_p$ having a summand $(s; t)$, for some $t$. Similarly, considering columns, there exists $A_q$ having a summand of the form $(u; r)$, for some $u$. Thus if $(r; s)$ is also a summand of $A_j$ then $A_iA_p = A_jA_p = (r; t)$, so $i = j$. This shows that the sets of summands of the $A_i$ are pairwise disjoint. Also, if $(r_1; s_1)$ and $(r_2; s_2)$ are distinct summands of $A_i$ then $r_1 \neq r_2$, since otherwise $A_qA_i$ is not an elementary matrix for some $A_q$ (of the form $(u_1; r_1)$, for some $u_1$). Similarly, $s_1 \neq s_2$. Thus the number of nonzero entries of $A_i$ is the rank of $A_i$, that is, $m_i$.

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

Let $A = \sum_{i=1}^{n} A_i$. By hypothesis,

$$\Big(\sum_{i=1}^{n} A_i\Big)^2 = A^2 = \mathbb{E}_n,$$

where $\mathbb{E}_n$ is the $n \times n$ matrix having all of its entries equal to 1. Since $A^2 e = ne$, where $e = (1, 1, \ldots, 1)$, it follows that $Af = \sqrt{n} f$, where $f = Ae + \sqrt{n} e$. Clearly $f \neq 0$. Thus $A^2 f = nf = \mathbb{E}_n f$ and it follows that $f$ is a nonzero multiple of $e$. So $Ae = \sqrt{n} e$ and all of the rows of $A$ sum to $\sqrt{n}$. From this, $n = m^2$ for some positive integer $m$ and $A$ has $nm$ nonzero entries. But the number of nonzero entries of $A$ is $\sum_{i=1}^{n} m_i$ (since the nonzero entries of the $A_i$ are pairwise disjoint). Hence, $\sum_{i=1}^{n} m_i = nm$. □

Corollary 3.2. *If each of the matrices $A_i$ has the same number $m$ of nonzero entries, then $n = m^2$.*

We now show that such sets of (0, 1)-matrices exist.

Example 3.3. Define the $4 \times 4$ (0, 1)-matrices $A, B, C, D$, each of rank two, by

$$A = (1;1) + (2;4), \quad B = (1;3) + (2;2), \quad C = (4;1) + (3;4), \quad D = (4;3) + (3;2).$$

We have the multiplication table

| | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | (1; 1) | (1; 3) | (2; 1) | (2; 3) |
| $B$ | (2; 4) | (2; 2) | (1; 4) | (1; 2) |
| $C$ | (4; 1) | (4; 3) | (3; 1) | (3; 3) |
| $D$ | (3; 4) | (3; 2) | (4; 4) | (4; 2) |

Here the set of 16 pairwise products of $A, B, C, D$ is the set of all $4 \times 4$ elementary matrices in $M_4(\mathbb{F})$.

Example 3.4. Define the $9 \times 9$ (0, 1)-matrices $A_{i,j}$, $0 \leq i, j \leq 8$, each of rank three, by

$$\begin{aligned}
A_{(0,0)} &= (1;1) + (2;5) + (3;9),\\
A_{(0,1)} &= (1;4) + (2;8) + (3;3),\\
A_{(0,2)} &= (1;7) + (2;2) + (3;6),\\
A_{(1,0)} &= (5;1) + (6;5) + (4;9),\\
A_{(1;1)} &= (5;4) + (6;8) + (4;3),\\
A_{(1,2)} &= (5;7) + (6;2) + (4;6),\\
A_{(2,0)} &= (9;1) + (7;5) + (8;9),\\
A_{(2,1)} &= (9;4) + (7;8) + (8;3),\\
A_{(2,2)} &= (9;7) + (7;2) + (8;6).
\end{aligned}$$

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

We have the multiplication table

| | $A_{(0,0)}$ | $A_{(0,1)}$ | $A_{(0,2)}$ | $A_{(1,0)}$ | $A_{(1,1)}$ | $A_{(1,2)}$ | $A_{(2,0)}$ | $A_{(2,1)}$ | $A_{(2,2)}$ |
|---|---|---|---|---|---|---|---|---|---|
| $A_{(0,0)}$ | (1; 1) | (1; 4) | (1; 7) | (2; 1) | (2; 4) | (2; 7) | (3; 1) | (3; 4) | (3; 7) |
| $A_{(0,1)}$ | (3; 9) | (3; 3) | (3; 6) | (1; 9) | (1; 3) | (1; 6) | (2; 9) | (2; 3) | (2; 6) |
| $A_{(0,2)}$ | (2; 5) | (2; 8) | (2; 2) | (3; 5) | (3; 8) | (3; 2) | (1; 5) | (1; 8) | (1; 2) |
| $A_{(1,0)}$ | (5; 1) | (5; 4) | (5; 7) | (6; 1) | (6; 4) | (6; 7) | (4; 1) | (4; 4) | (4; 7) |
| $A_{(1,1)}$ | (4; 9) | (4; 3) | (4; 6) | (5; 9) | (5; 3) | (5; 6) | (6; 9) | (6; 3) | (6; 6) |
| $A_{(1,2)}$ | (6; 5) | (6; 8) | (6; 2) | (4; 5) | (4; 8) | (4; 2) | (5; 5) | (5; 8) | (5; 2) |
| $A_{(2,0)}$ | (9; 1) | (9; 4) | (9; 7) | (7; 1) | (7; 4) | (7; 7) | (8; 1) | (8; 4) | (8; 7) |
| $A_{(2,1)}$ | (8; 9) | (8; 3) | (8; 6) | (9; 9) | (9; 3) | (9; 6) | (7; 9) | (7; 3) | (7; 6) |
| $A_{(2,2)}$ | (7; 5) | (7; 8) | (7; 2) | (8; 5) | (8; 8) | (8; 2) | (9; 5) | (9; 8) | (9; 2) |

Here the set of 81 pairwise products of the $A_{(i,j)}$ is the set of all $9 \times 9$ elementary matrices in $M_9(\mathbb{F})$.

The preceding two examples are particular cases of the following result.

THEOREM 3.5. *Let $m \in \mathbb{Z}^+$ and let $n = m^2$. There exists a set of $n$ $(0,1)$-matrices $\{A_i : 1 \le i \le n\} \subseteq M_n(\mathbb{F})$ such that each $A_i$ has $m$ nonzero entries and*

(i) *$A_iA_j$ is an elementary matrix for $1 \le i, j \le n$;*
(ii) *$\{A_iA_j : 1 \le i, j \le n\}$ is a basis for $M_n(\mathbb{F})$.*

PROOF. By Example 3.3 above, we can suppose that $m \ge 3$. Define the matrices $A_{(i,j)}$, for $0 \le i, j \le m-1$, by

$$A_{(i,j)} = \sum_{r=1}^{m-j} (\sigma^i(r) + im; (r-1+j)(m+1) - j + 1) + \sum_{r=m-j+1}^{m} (\sigma^i(r) + im; (r-m+j)(m+1) - j),$$

where $\sigma : \{1, 2, \dots, m\} \longrightarrow \{1, 2, \dots, m\}$ is the cyclic permutation $(1, 2, \dots, m)$ (that is, $1 \mapsto 2 \mapsto 3 \mapsto \cdots \mapsto (m-1) \mapsto m \mapsto 1$). Call $H_r(A_{(i,j)})$ the $r$th *head* of $A_{(i,j)}$ and call $T_r(A_{(i,j)})$ the $r$th *tail* of $A_{(i,j)}$ where these are defined by

$$H_r(A_{(i,j)}) = \sigma^i(r) + im,$$

$$T_r(A_{(i,j)}) = \begin{cases} (r-1+j)(m+1) - j + 1 & \text{if } 1 \le r \le m-j, \\ (r-m+j)(m+1) - j & \text{if } m-j+1 \le r \le m. \end{cases}$$

Then $A_{(i,j)} = \sum_{r=1}^{m} (H_r(A_{(i,j)}); T_r(A_{(i,j)}))$. Notice that, for $0 \le i, j \le m-1$,

$$|H_r(A_{(i,j)}) - H_s(A_{(i,j)})| \le m-1 \quad \text{for } 1 \le r, s \le m,$$
$$|T_r(A_{(i,j)}) - T_s(A_{(i,j)})| \ge m+1 \quad \text{for } 1 \le r, s \le m \text{ with } 0 < |r-s| \ne m-1,$$
$$|T_r(A_{(i,j)}) - T_s(A_{(i,j)})| = 1 \quad \text{if } |r-s| = m-1.$$

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

In particular, all of the tails of $A_{(i,j)}$ are distinct and all of the heads are distinct because $\sigma^i$ is a bijection on $\{1, 2, \ldots, m\}$.

We claim that

$$|\{T_r(A_{(i,j)}) : 1 \le r \le m\} \cap \{H_s(A_{(p,q)}) : 1 \le s \le m\}| \le 1 \quad \text{for } 0 \le i, j, p, q \le m-1.$$

Suppose $T_r(A_{(i,j)}) = H_s(A_{(p,q)})$ and $T_u(A_{(i,j)}) = H_v(A_{(p,q)})$, with $r \ne u$ and $s \ne v$. Then

$$|T_r(A_{(i,j)}) - T_u(A_{(i,j)})| = |H_s(A_{(p,q)}) - H_v(A_{(p,q)})| \le m-1,$$

so $|T_r(A_{(i,j)}) - T_u(A_{(i,j)})| = 1$, and we can take $r = 1, u = m$, so that $T_r(A_{(i,j)}) = jm + 1$ and $T_u(A_{(i,j)}) = jm$. Consequently, $H_s(A_{(p,q)}) = \sigma^p(s) + pm = jm + 1$ and $H_v(A_{(p,q)}) = \sigma^p(v) + pm = jm$, and so $\sigma^p(v) = (j-p)m$. It follows that $j - p = m$, so that $\sigma^p(v) = m$. Since $\sigma^p(s) = \sigma^p(v) + 1$, we have $\sigma^p(s) = m + 1$. This is a contradiction and establishes the claim.

Next we shall show that

$$|\{T_r(A_{(i,j)}) : 1 \le r \le m\} \cap \{H_s(A_{(p,q)}) : 1 \le s \le m\}| = 1 \quad \text{for } 0 \le i, j, p, q \le m-1.$$

We do this by showing that

$$\{T_r(A_{(i,j)}) : 1 \le r \le m\} \cap \{H_s(A_{(p,q)}) : 1 \le s \le m\} \ne \emptyset \quad \text{for } 0 \le i, j, p, q \le m-1.$$

In fact we will show that

$$\begin{aligned}
&\text{(1i)} \quad T_{p-j+1}(A_{(i,j)}) = H_{m-j+1}(A_{(p,q)}) \quad \text{if } 1 \le j \le p,\\
&\text{(1ii)} \quad T_{p+1}(A_{(i,0)}) = H_1(A_{(p,q)}),\\
&\text{(2)} \quad T_{m-j+p+1}(A_{(i,j)}) = H_{m-j+1}(A_{(p,q)}) \quad \text{if } j \ge p+1.
\end{aligned}$$

*Case (1i).* Let $r = p - j + 1$ and $s = m - j + 1$ with $1 \le j \le p$. Then $1 \le r \le m - j$, and so $T_r(A_{(i,j)}) = (r - 1 + j)(m + 1) - j + 1 = p(m + 1) - j + 1$. Also $m - p + 1 \le s \le m$, so $H_s(A_{(p,q)}) = \sigma^p(s) + pm = s + p - m + pm = p - j + 1 + pm = T_r(A_{(i,j)})$.

*Case (1ii).* It is easily verified that $T_{p+1}(A_{(i,0)}) = H_1(A_{(p,q)}) = pm + p + 1$.

*Case (2).* Let $r = m - j + p + 1$ and $s = m - j + 1$ with $j \ge p + 1$. Then $m - j + 1 \le r \le m$, and so $T_r(A_{(i,j)}) = (r - m + j)(m + 1) - j = (p + 1)(m + 1) - j$. Also $1 \le s \le m - p$, so $H_s(A_{(p,q)}) = \sigma^p(s) + pm = s + p + pm = m - j + 1 + p + pm = T_r(A_{(i,j)})$.

Hence, for every $i, j$ and $p, q$, the set of tails of $A_{(i,j)}$ and the set of heads of $A_{(p,q)}$ have precisely one element in common. It follows that the product $A_{(i,j)}A_{(p,q)}$ is an elementary matrix. Since we know, in each case, the tail of $A_{(i,j)}$ and the head of $A_{(p,q)}$ which coincide, we can write down these elementary matrices (the other products are zero).

For $1 \le j \le p$,

$$\begin{aligned}
A_{(i,j)}A_{(p,q)} &= (H_{p-j+1}(A_{(i,j)}); T_{p-j+1}(A_{(i,j,)}))(H_{m-j+1}(A_{(p,q)}); T_{m-j+1}(A_{(p,q)}))\\
&= (H_{p-j+1}(A_{(i,j)}); T_{m-j+1}(A_{(p,q)}))
\end{aligned}$$

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

and this is equal to

$$\begin{cases}(p-j+i(m+1)+1;(m+q-j)(m+1)-q+1) \text{ if } p-j+i+1\le m,\ j\ge q+1,\\ (p-j+i(m+1)+1;(1-j+q)(m+1)-q) \text{ if } p-j+i+1\le m,\ j\le q,\\ (p-j+i(m+1)+1-m;(m+q-j)(m+1)-q+1) \text{ if } p-j+i\ge m,\ j\ge q+1,\\ (p-j+i(m+1)+1-m;(1-j+q)(m+1)-q) \text{ if } p-j+i\ge m,\ j\le q.\end{cases}$$

For $j=0$,

$$\begin{aligned}A_{(i,0)}A_{(p,q)} &= (H_{p+1}(A_{(i,0)});T_{p+1}(A_{(i,0)}))(H_1(A_{(p,q)});T_1(A_{(p,q)}))\\ &= (H_{p+1}(A_{(i,0)});T_1(A_{(p,q)}))\\ &= \begin{cases}(p+i(m+1)+1;qm+1) & \text{if } p+i+1\le m,\\ (p+i(m+1)+1-m;qm+1) & \text{if } p+i+1\ge m+1.\end{cases}\end{aligned}$$

For $j\ge p+1$,

$$\begin{aligned}A_{(i,j)}A_{(p,q)} &= (H_{p-j+m+1}(A_{(i,j)});T_{p-j+m+1}(A_{(i,j,)}))(H_{m-j+1}(A_{(p,q)});T_{m-j+1}(A_{(p,q)}))\\ &= (H_{p-j+m+1}(A_{(i,j)});T_{m-j+1}(A_{(p,q)}))\end{aligned}$$

and this is equal to

$$\begin{cases}(p-j+(i+1)(m+1);(m+q-j)(m+1)-q+1)\\ \quad \text{if } j\ge p+1+i \text{ and } j\ge q+1,\\ (p-j+(i+1)(m+1);(1-j+q)(m+1)-q)\\ \quad \text{if } j\ge p+1+i \text{ and } j\le q,\\ (p-j+(i+1)(m+1)-m;(m+q-j)(m+1)-q+1)\\ \quad \text{if } j\le p+i \text{ and } j\ge q+1,\\ (p-j+(i+1)(m+1)-m;(1-j+q)(m+1)-q)\\ \quad \text{if } j\le p+i \text{ and } j\le q.\end{cases}$$

There are $m^2=n$ matrices $A_{(i,j)}$, so there are $n^2$ such products. The proof will be complete if we show these products give rise to different elementary matrices, that is,

$$A_{(i_1,j_1)}A_{(p_1,q_1)}=A_{(i_2,j_2)}A_{(p_2,q_2)} \text{ implies that } (i_1,j_1)=(i_2,j_2) \text{ and } (p_1,q_1)=(p_2,q_2).$$

Let $A_{(i_1,j_1)}A_{(p_1,q_1)}=A_{(i_2,j_2)}A_{(p_2,q_2)}$ with $i_1,j_1,p_1,q_1,i_2,j_2,p_2,q_2\in\{0,1,2,\dots,m-1\}$. In the remainder of the proof, for an elementary matrix $(i;j)$, we will call $i$ the *head* of $(i;j)$ and $j$ the *tail* of $(i;j)$ and write $H((i;j))=i,\ T((i;j))=j$. Then

$$H(A_{(i_1,j_1)}A_{(p_1,q_1)})=H(A_{(i_2,j_2)}A_{(p_2,q_2)}) \quad \text{and} \quad T(A_{(i_1,j_1)}A_{(p_1,q_1)})=T(A_{(i_2,j_2)}A_{(p_2,q_2)}).$$

Now

$$H(A_{(i_1,j_1)}A_{(p_1,q_1)})=H_{p_1-j_1+1}(A_{(i_1,j_1)}) \text{ or } H_{p_1-j_1+m+1}(A_{(i_1,j_1)})$$

and

$$T(A_{(i_1,j_1)}A_{(p_1,q_1)})=T_{m-j_1+1}(A_{(p_1,q_1)}) \text{ or } T_1(A_{(p_1,q_1)}),$$

with similar expressions for $H(A_{(i_2,j_2)}A_{(p_2,q_2)})$ and $T(A_{(i_2,j_2)}A_{(p_2,q_2)})$.

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

*Case 1*: $j_1 = j_2 = 0$. Then $T(A_{(i_1,0)}A_{(p_1,q_1)}) = T(A_{(i_2,0)}A_{(p_2,q_2)})$, which gives

$$T_1(A_{(p_1,q_1)}) = T_1(A_{(p_2,q_2)}) = q_1m + 1 = q_2m + 1,$$

so that $q_1 = q_2$. Also, $H(A_{(i_1,0)}A_{(p_1,q_1)}) = H(A_{(i_2,0)}A_{(p_2,q_2)})$, which gives

$$H_{p_1+1}(A_{(i_1,0)}) = H_{p_2+1}(A_{(i_2,0)}) = \sigma^{i_1}(p_1 + 1) + i_1m = \sigma^{i_2}(p_2 + 1) + i_2m.$$

Thus $|\sigma^{i_1}(p_1 + 1) - \sigma^{i_2}(p_2 + 1)| = |i_2 - i_1|m \le m - 1$ and it follows that $i_1 = i_2$ and $\sigma^{i_1}(p_1 + 1) = \sigma^{i_2}(p_2 + 1)$, so $p_1 = p_2$. Thus $(i_1, j_1) = (i_2, j_2)$ and $(p_1, q_1) = (p_2, q_2)$.

*Case 2*: $j_1 \neq 0$, $j_2 \neq 0$. In this case

$$H(A_{(i_1,j_1)}A_{(p_1,q_1)}) = H_{r_1}(A_{(i_1,j_1)}) \quad \text{and} \quad H(A_{(i_2,j_2)}A_{(p_2,q_2)}) = H_{r_2}(A_{(i_2,j_2)}),$$

where $r_1 = p_1 - j_1 + 1$ or $p_1 - j_1 + 1 + m$ and $r_2 = p_2 - j_2 + 1$ or $p_2 - j_2 + 1 + m$. Thus $\sigma^{i_1}(r_1) + i_1m = \sigma^{i_2}(r_2) + i_2m$ and $|\sigma^{i_1}(r_1) - \sigma^{i_2}(r_2)| = |i_2 - i_1|m \le m - 1$. It follows that $i_1 = i_2$ and $r_1 = r_2$. Also

$$T(A_{(i_1,j_1)}A_{(p_1,q_1)}) = T_{m-j_1+1}(A_{(p_1,q_1)}) = T(A_{(i_2,j_2)}A_{(p_2,q_2)}) = T_{m-j_2+1}(A_{(p_2,q_2)}).$$

Now $T_{m-j_1+1}(A_{(p_1,q_1)}) = (m + q_1 - j_1)(m + 1) - q_1 + 1$ or $(1 + q_1 - j_1)(m + 1) - q_1$ and $T_{m-j_2+1}(A_{(p_2,q_2)}) = (m + q_2 - j_2)(m + 1) - q_2 + 1$ or $(1 + q_2 - j_2)(m + 1) - q_2$. We cannot have $T_{m-j_1+1}(A_{(p_1,q_1)}) = (m + q_1 - j_1)(m + 1) - q_1 + 1$ and $T_{m-j_2+1}(A_{(p_2,q_2)}) = (1 + q_2 - j_2)(m + 1) - q_2$ since then

$$|m + q_1 - j_1 - 1 - q_2 + j_2|(m + 1) = |q_1 - q_2 - 1| \le m,$$

from which $q_1 - q_2 - 1 = 0$ and $j_1 - j_2 = m$, a contradiction. Similarly, we cannot have $T_{m-j_1+1}(A_{(p_1,q_1)}) = (1 + q_1 - j_1)(m + 1) - q_1$, $T_{m-j_2+1}(A_{(p_2,q_2)}) = (m + q_2 - j_2)(m + 1) - q_2 + 1$. So $T_{m-j_1+1}(A_{(p_1,q_1)}) = T_{m-j_2+1}(A_{(p_2,q_2)})$ must give

$$|(q_1 - j_1) - (q_2 - j_2)|(m + 1) = |q_2 - q_1| \le m,$$

from which we deduce that $q_1 = q_2$ and $j_1 = j_2$.

To show that $p_1 = p_2$ in this case, we should consider the fact that $r_1 = r_2$. We cannot have $r_1 = p_1 - j_1 + 1$ and $r_2 = p_2 - j_2 + 1 + m$, since then, using the fact that $j_1 = j_2$, we would have $m = p_1 - p_2$, which is a contradiction. Similarly, we cannot have $r_1 = p_1 - j_1 + 1 + m$ and $r_2 = p_2 - j_2 + 1$. Thus $H_{r_1}(A_{(i_1,j_1)}) = H_{r_2}(A_{(i_2,j_2)})$ must give $p_1 - j_1 = p_2 - j_2$, from which we deduce that $p_1 = p_2$, since $j_1 = j_2$. Thus $(i_1, j_1) = (i_2, j_2)$ and $(p_1, q_1) = (p_2, q_2)$.

Finally, we show we cannot have either $j_1 = 0$, $j_2 \neq 0$ or $j_1 \neq 0$, $j_2 = 0$. Suppose that $j_1 = 0$, $j_2 \neq 0$. Then $T(A_{(i_1,j_1)}A_{(p_1,q_1)}) = q_1m + 1$ and

$$T(A_{(i_2,j_2)}A_{(p_2,q_2)}) = (m + q_2 - j_2)(m + 1) - q_2 + 1 \text{ or } (1 + q_2 - j_2)(m + 1) - q_2.$$

If $T(A_{(i_2,j_2)}A_{(p_2,q_2)}) = (m + q_2 - j_2)(m + 1) - q_2 + 1$, then

$$q_1(m + 1) - q_1 + 1 = q_1m + 1 = (m + q_2 - j_2)(m + 1) - q_2 + 1,$$

so $|m + q_2 - j_2 - q_1|(m + 1) = |q_2 - q_1| \le m - 1$, which gives $q_2 = q_1$ and $j_2 = m$, a contradiction. If, on the other hand, $T(A_{(i_2,j_2)}A_{(p_2,q_2)}) = (1 + q_2 - j_2)(m + 1) - q_2$, then $q_1(m + 1) - q_1 + 1 = (1 + q_2 - j_2)(m + 1)$, so

$$|1 + q_2 - j_2 - q_1|(m + 1) = |q_2 - q_1 + 1| \le m,$$

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

and so $q_2 - q_1 + 1 = 0$ and $j_2 = 0$, a contradiction. Similarly, we cannot have $j_1 \neq 0$ and $j_2 = 0$. This completes the proof. □

REMARK 3.6. In the following remark, $e_k$ denotes the standard basis vector in $\mathbf{C}^n$ which has $k$th entry equal to one and all other entries zero. Also, $T^*$ denotes the adjoint of the matrix $T$. We use the well-known fact that for any rank-one complex square matrix $R$ and any complex matrices $X, Y$ of the same size as $R$, if $XRY = 0$ then either $XR = 0$ or $RY = 0$.

Question 1.1 from the introduction is answered in the affirmative by Theorem 3.5 for matrices of size $n$ where $n$ is a square. If $n$ is not square, the answer is still unknown, even for real or complex matrices, although Theorem 3.1 shows that, in this case, sets of $(0, 1)$-matrices will not provide an example. But suppose $n \geq 2$ and $\{A_i : 1 \leq i \leq n\}$ is a set of $n \times n$ real or complex matrices (not necessarily $(0, 1)$-matrices, and not necessarily of equal rank) such that $\{A_i A_j : 1 \leq i, j \leq n\} = \{E_{p,q} : 1 \leq p, q \leq n\}$.

(i) We cannot have $A_i A_j = E_{i,j}$, for $1 \leq i, j \leq n$. In fact, we will prove that if $i \neq j$, then $A_i^2 = E_{p,p}, A_j^2 = E_{q,q}$ and $A_i A_j = E_{u,v}$, with $u = p$ or $v = q$, leads to a contradiction. Suppose it were true. Then

$$0 = A_i^2 A_j^2 = A_i(A_i A_j)A_j = A_i E_{u,v} A_j,$$

so $A_i E_{u,v} = 0$ or $E_{u,v} A_j = 0$. If $u = p$, then $A_i E_{p,v} = 0$, so $A_i E_{p,p} = 0$ (since $A_i E_{p,p} E_{p,v} = 0$ and $E_{p,p} E_{p,v} \neq 0$). But this would mean $A_i^3 = 0$, which is a contradiction. On the other hand, if $v = q$, then $E_{u,q} A_j = 0$, so $E_{q,q} A_j = 0 = A_j^3$, which again is a contradiction.

(ii) Let $1 \leq i, j \leq n$. There exist $p, q$ such that $A_p A_q = E_{j,j}$. Then $\text{range}(A_i(A_p A_q)) = \text{span}\{A_i e_j\} = \text{range}((A_i A_p)A_q) \subseteq \text{range}(A_i A_p) = \text{span}\{e_k\}$, for some $k$. Thus each matrix $A_i$ has at most one nonzero entry in each column. Applying this result to the set of adjoints $\{A_i^* : 1 \leq i \leq n\}$ shows that each $A_i$ has at most one nonzero entry in each row. So the rank of any $A_i$ is the number of its nonzero entries.

(iii) If $n$ is odd, there exists $i$ such that $A_i^2$ is diagonal. For an elementary matrix has nonzero trace if and only if it is diagonal. Since $\text{trace}(AB) = \text{trace}(BA)$, we see that $A_i A_j$ is a diagonal elementary matrix if and only if $A_j A_i$ is. If no $A_i^2$ is diagonal, the number of diagonal positions would be even, so $n$ would be even.

(iv) No $A_i$ can have rank one. For suppose that $A_i$ had rank one. Then $A_i = \lambda E_{p,q}$ for some nonzero scalar $\lambda$ and some $p, q$. Since $A_i^2$ is an elementary matrix, $\lambda^2 = 1$ and $p = q$, so $A_i = \pm E_{p,p}$. Now $\{A_i A_j : 1 \leq j \leq n\} = \{E_{p,r} : 1 \leq r \leq n\}$, $\{A_j A_i : 1 \leq j \leq n\} = \{E_{s,p} : 1 \leq s \leq n\}$. Let $r \neq p$. There exist $j, k$ such that $A_i A_j = E_{p,r}$ and $A_k A_i = E_{r,p}$. Then $(A_i A_j)(A_k A_i) = E_{p,p} = E_{p,p}(A_j A_k)E_{p,p}$. Since $A_j A_k$ is an elementary matrix, we must have $A_j A_k = E_{p,p} = A_i^2$ and so $j = k = i$, and $p = r$. This is a contradiction.

In particular, on a space of dimension two, no such set of matrices can exist, since otherwise, each $A_i$, being noninvertible and nonzero, would have rank one. (This was observed in [1].)

(v) No such family can exist on a space of dimension three. Suppose we had $3 \times 3$ matrices $A, B, C$ such that $\{A^2, AB, AC, BA, B^2, BC, CA, CB, C^2\}$ is the set of elementary

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press

matrices on $\mathbb{C}^3$. By what has been observed, each of $A, B, C$ has rank two, and one of them, which we can assume to be $A$, has a diagonal square. We can even suppose that $A^2 = E_{1,1}$. By the spectral mapping theorem, since $A^2 e_1 = e_1$, there exists a nonzero vector $f$ such that $Af = \mu f$, where $\mu = \pm 1$. Then $A^2 f = f$, so we can take $f = e_1$. Thus $e_1 \in \text{range}(A)$. Since the range of $A$ is spanned by elementary basis vectors (see (i) above), we can suppose that $\text{range}(A) = \text{span}\{e_1, e_2\}$. Then $\text{range}(A^2) = \text{span}\{e_1\} = \text{span}\{Ae_1, Ae_2\}$, so $Ae_2 = \gamma e_1$ for some scalar $\gamma$. Since $A^2 e_2 = 0 = \gamma A e_1 = \gamma\mu e_1$ we have $\gamma = 0$. Thus $Ae_2 = 0$ and since $A$ has rank two we must have $Ae_3 \neq 0$.

Suppose that $BC$ is diagonal. Then $CB$ is also diagonal (since it has nonzero trace), and we can suppose that $BC = E_{2,2}$ and then $CB = E_{3,3}$. Since $Ae_3 \neq 0$, we have $ACB \neq 0$. Now $e_3$ is orthogonal to the range of $A$, so it belongs to the kernel of $A^*$. Thus, since $A^*$ has rank two, $A^* e_2 \neq 0$, so $A^* E_{2,2} \neq 0$ and, taking adjoints, $E_{2,2}A = BCA \neq 0$.

We have shown that $ACB \neq 0$ and $BCA \neq 0$. Since $A^2 CB = A(AC)B = 0$ and $AC$ has rank one, and $ACB \neq 0$, we get $A^2 C = 0$ by using the fact mentioned at the beginning of this remark. Similarly, from $BCA^2 = B(CA)A = 0$, we get $CA^2 = 0$. Since $E_{1,1}C = CE_{1,1} = 0$, it follows that the matrix $C$ has the form $C = 0 \oplus D$, where $D$ is a $2 \times 2$ matrix. Since $C$ has rank two, $D$ is invertible. This contradicts the fact that $C^2 = 0 \oplus D^2$ has rank one.

We have just shown that $BC$ cannot be diagonal. Similarly $CB$ cannot be diagonal. Suppose that $AB$ was diagonal. Then $AB$ cannot equal $E_{3,3}$ since then we would have $BA = E_{2,2}$ so $BAe_2 = 0 = e_2$ (since $Ae_2 = 0$). Thus $AB = E_{2,2}$ and so $BA = E_{3,3}$. Then $BAe_1 = 0 = B(\mu e_1)$ so $Be_1 = 0$ and $BE_{1,1} = 0$. Now $A^3 = AE_{1,1} = \mu E_{1,1}$. Then $A^2 AB = 0 = A^3 B = \mu E_{1,1} B$, so $E_{1,1} B = 0$. As argued in the preceding paragraph, $E_{1,1}B = BE_{1,1} = 0$ contradicts the fact that $B^2$ has rank one. Thus we cannot have $AB$ diagonal. Similarly we cannot have $AC$ diagonal.

By what we have shown above, since there exist $X, Y \in \{A, B, C\}$ such that $XY = E_{2,2}$ and $YX = E_{3,3}$, we can suppose that $B^2 = E_{2,2}$ and $C^2 = E_{3,3}$. Then $A^2 C^2 = 0$ and $AC^2 \neq 0$ (since $Ae_3 \neq 0$) implies that $A^2 C = E_{1,1} C = 0$, which in turn implies that $B^2 C \neq 0$ (note that $C^* e_1 = 0$ implies that $C^* e_2 \neq 0$). Similarly, $B^2 A^2 = 0$ and $B^2 A \neq 0$ implies that $BA^2 = BE_{1,1} = 0$, which in turn implies that $BC^2 \neq 0$.

Thus $B^2 C \neq 0$ and $BC^2 \neq 0$. But this contradicts $B^2 C^2 = B(BC)C = 0$ (since $BC$ has rank one). So no such family can exist.

(vi) What about $5 \times 5$ real or complex matrices? Does such a family exist?

## Reference

[1] D. Rosenthal, 'Words containing a basis for the algebra of all matrices', *Linear Algebra Appl.* **436** (2012), 2615–2617.

W. E. LONGSTAFF,
11 Tussock Crescent, Elanora, Queensland 4221, Australia
e-mail: bill.longstaff@alumni.utoronto.ca

https://doi.org/10.1017/S000497271800076X Published online by Cambridge University Press