LEFT IDEALS IN MATRIX RINGS OVER FINITE FIELDS

R. A. FERRAZ, C. POLCINO MILIES, AND E. TAUFER

Abstract. It is well-known that each left ideals in a matrix rings over a finite field is generated by an idempotent matrix. In this work we compute the number of left ideals in these rings, the number of different idempotents generating each left ideal, and give explicitly a set of idempotent generators of all left ideals of a given rank.

1. Introduction

Let $\mathbb{F}_q$ be the field with $q$ elements and denote by $M_n(\mathbb{F}_q)$ full ring of $n \times n$ matrices over $\mathbb{F}_q$. Given $M \in M_n(\mathbb{F}_q)$, the subspace of $\mathbb{F}_q^n$ generated by the rows of $M$, whose dimension is precisely the rank of $M$, will be denoted by $W(M)$. Since $M_n(\mathbb{F}_q)$ is semi-simple, every left ideal is generated by just one element. In particular, every left ideal has a generator that is an idempotent.

The left ideal generated by a matrix $M$ will be denoted by $\langle M \rangle$. Notice that, since $\text{rank}(AM) \leq \text{rank}(M)$ for all $A \in M_n(\mathbb{F}_q)$ we have that

$$\text{rank}(M) = \sup\{\text{rank}(XM) \mid X \in M_n(\mathbb{F}_q)\}.$$  

Consequently, two generators of the same ideal are of the same rank. For an ideal $J = \langle M \rangle$ we define $\text{rank}(J) = \text{rank}(M)$.

Results obtained here refer to left ideals, but similar results hold for right ideals.

2. Ideals and Subspaces

We intend to count the number of left ideals in $M_n(\mathbb{F}_q)$. To do so, we will establish a correspondence of these ideals with subspaces of $\mathbb{F}_q^n$. We begin with the following.

Lemma 2.1. Given $M_1, M_2 \in M_n(\mathbb{F}_q)$, then $\langle M_1 \rangle \subset \langle M_2 \rangle$ if, and only if, the rows of $M_1$ are linear combinations of the rows of $M_2$.

The second author was partially supported by CNPq., Proc. 300243/79-0(RN) and FAPESP, Proc 2015/09162-9.
Proof. Given $M_1 = (a_{ij}), M_2 = (b_{ij}) \in M_n(\mathbb{F}_q)$, note that $\langle M_1 \rangle \subset \langle M_2 \rangle$, and if only if, $M_1 \in \langle M_2 \rangle$, that is if there exists $(c_{ij}) \in M_n(\mathbb{F}_q)$, such that $M_1 = (c_{ij})M_2$.

Hence, $a_{ij} = \sum_{k=1}^{n} c_{ik}b_{kj}, \forall i, j$ and thus, the $l$-th row of $M_1$ is

$$(a_{l1}, a_{l2}, \ldots, a_{ln}) = \left( \sum_{k=1}^{n} c_{lk}b_{k1}, \sum_{k=1}^{n} c_{lk}b_{k2}, \ldots, \sum_{k=1}^{n} c_{lk}b_{kn} \right)$$

$$= \sum_{k=1}^{n} c_{lk}(b_{k1}, b_{k2}, \ldots, b_{kn})$$

The converse follows immediately. □

As an consequence, we have

Corollary 2.2.

$$\langle M_1 \rangle \subset \langle M_2 \rangle \iff W(M_1) \subset W(M_2)$$

$$\langle M_1 \rangle = \langle M_2 \rangle \iff W(M_1) = W(M_2).$$

Since every subspace of $\mathbb{F}_q^n$ is of the form $W(M)$, for some $M \in M_n(\mathbb{F}_q)$, we have the following.

Theorem 2.3. Given a positive integer $k$, $1 \leq k \leq n-1$, the map $W(N_i) \mapsto \langle N_i \rangle$ gives a bijection $\varphi$ between the set of subspaces of dimension $k$ of $\mathbb{F}_q^n$, and the set of left ideals of rank $k$ in $M_n(\mathbb{F}_q)$.

Proof. Given a $k$-dimensional subspace $W$ of $\mathbb{F}_q^n$, with basis $B = \{v_1, v_2, \ldots, v_k\}$, let us consider the matrix $M$ whose first $k$ rows are the vectors $v_1, v_2, \ldots, v_k$ and the others are linear combinations of these ones. Clearly $W$ is equal to $W(M)$. Also if $W(M_1) = W(M_2)$, then $\langle M_1 \rangle = \langle M_2 \rangle$, by Corollary 2.2. Therefore we conclude that $\varphi$ is well defined. Since, $\langle M_1 \rangle = \langle M_2 \rangle$ implies $W(M_1) = W(M_2)$, it follows that $\varphi$ is injective. As all the ideals of $M_n(\mathbb{F}_q)$ are principal, $\varphi$ is also surjective. □

Since [11, Chapter 24] gives the number of $k$-subspace of $\mathbb{F}_q^n$, with $0 < k \leq n$ we get the following.

Theorem 2.4. The number of left ideals of rank $k$ in $M_n(\mathbb{F}_q)$ is

$$\frac{(q^n - 1)(q^{n-1} - 1)(q^{n-2} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)(q^{k-2} - 1) \cdots (q - 1)}.$$

We now determine conditions on two idempotent matrices to generate the same left ideal.
Theorem 2.5. Given $R, S \in M_n(\mathbb{F}_q)$, the following assertions are equivalent:

(i) $R$ and $S$ are idempotents and $\langle S \rangle = \langle R \rangle$;

(ii) $RS = R$ and $SR = S$;

(iii) $R = S + (I - S)RS$ and $S$ is an idempotent, where $I$ denotes the identity matrix of $M_n(\mathbb{F}_q)$.

Proof. (i) $\Rightarrow$ (ii) If $R \in \langle S \rangle$ then, there exists $A \in M_n(\mathbb{F}_q)$, such that, $R = AS$.

Hence, $RS = AS, S = AS = R$, as $S$ is idempotent. Similarly, we conclude $SR = S$.

(ii) $\Rightarrow$ (i) Notice that (ii) implies that $R \in \langle S \rangle$ and $S \in \langle R \rangle$, thus $\langle S \rangle = \langle R \rangle$.

Also, $S^2 = (SR)S = S(RS) = SR = S$ and $R^2 = (RS)R = R(SR) = RS = R$.

(i) $\Rightarrow$ (iii) We compute, $S + (I - S)RS = S + (I - S)R = S + R - SR = R$.

Also $S^2 = (SR)S = S(RS) = SR = S$.

(iii) $\Rightarrow$ (ii) $SR = S (S + (I - S)RS) = S$, and $R = S + (I - S)RS = S + RS - SS = RS$.

□

Remark 2.7. Note that, if we denote by $[M]$ the right ideal generated by a matrix $M \in M_n(\mathbb{F}_q)$ and by $V(M)$ the subspace of $\mathbb{F}_q^n$ generated by the columns of $M$, then the following results, duals to those in this section, hold:
(a) \([M_1] = [M_2]\) if and only if \(V(M_1) = V(M_2)\).

(b) If \(R, S \in M_n(\mathbb{F}_q)\) are idempotents, then \([R] = [S]\) if and only if \(RS = S\) and \(SR = R\).

3. Idempotent generators of left ideals.

The purpose of this section is to exhibit idempotent generators of left ideals of a given rank \(k\) in \(M_n(\mathbb{F}_q)\) and to determine, for each ideal \(I\), the set of all idempotent generators of \(I\). We first study the idempotents of rank 1:

**Theorem 3.1.** The following matrices are idempotent generators of the different minimal left ideals of \(M_n(\mathbb{F}_q)\)

\[
\begin{bmatrix}
1 & a_1 & a_2 & \ldots & a_{n-1} \\
0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & 0 \\
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 0 & \ldots & 0 \\
0 & 1 & a_2 & \ldots & a_{n-1} \\
0 & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & 0 \\
\end{bmatrix},
\begin{bmatrix}
0 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 1 \\
\end{bmatrix}.
\]

Moreover, each minimal left ideal has \(q^{n-1}\) different idempotent generators.

**Proof.** We observe that, according to Theorem 2.3, each minimal left ideal \(I = \langle M \rangle \subset M_n(\mathbb{F}_q)\) is related with a 1-dimensional subspace \(W = W(M) \subset \mathbb{F}_q^n\). Let \(v = (a_1, a_2, \ldots, a_n)\) be a generator of \(W\). Then, the rows of any matrix in the ideal \(I\) are scalar multiples of \(v\).

Let \(i\) be the smallest index such that \(a_i \neq 0\), \(1 \leq i \leq n\) and set \(u = (1/a_i)v\). Then, \(u = (0, \ldots, 0, 1, b_{i+1}, \ldots, b_n)\), is also a generator of \(W\). Thus, we can assume that \(I\) is generated by a matrix whose \(i\)-th row is the vector \(u\) and the others are zero. Notice that the total number of matrices of this form is \(S_n = \sum_{i=1}^{n} q^{n-i} = \frac{q^{n-1}}{q-1}\).

To prove the second part of the statement, let \(E_{11}\) denote the matrix whose entry in position \((1, 1)\) is equal to 1 and all other entries are equal to 0. Then,

\[
\langle E_{11} \rangle = \left\{ \begin{bmatrix}
a_1 & 0 & \ldots & 0 \\
a_2 & 0 & \ldots & 0 \\
a_n & 0 & \ldots & 0 \\
\end{bmatrix} \middle| a_i \in \mathbb{F}_q, 1 \leq i \leq n \right\}.
\]

It is easy to see that a non-zero element in \(\langle E_{11} \rangle\) is idempotent if and only if \(a_1 = 1\), so the number of idempotents in \(\langle E_{11} \rangle\) is \(q^{n-1}\) and each of them is a generator of this ideal. Let \(J = \langle M \rangle\) be a minimal left ideal of \(M_n(\mathbb{F}_q)\). As \(\text{rank}(M) = 1\), there exist an invertible matrix \(U \in M_n(\mathbb{F}_q)\) such that \(U^{-1}MU = E_{11}\). Conjugation by \(U\) induces
an automorphism \( \psi_U : M_n(F_q) \rightarrow M_n(F_q) \) such that \( \psi_U(J) = \langle E_{11} \rangle \).

Consequently, \( J \) also has \( q^{n-1} \) generators which are idempotents.

We now extend this result to left ideals of a fixed rank \( k \), \( 1 \leq k \leq n \).

Let \( E(n,k) \) denote the set of all matrices \( A = (a_{ij}) \) such that there exist \( k \) rows, at positions denoted \( i_1, i_2, \ldots, i_k \) verifying:

(i) Every row of \( A \), except these, is a row of zeros.

(ii) \( a_{i_jj} = 1 \) and \( a_{i_jh} = 0 \) if \( h < i_j, 1 \leq j \leq k \).

(iii) \( a_{i_jh} = 0 \) for \( h = i_s, j + 1 \leq s \leq k \).

The set of numbers \( i_1, i_2, \ldots, i_k \) will be called the pivotal positions of \( A \).

For example, \( E(4,3) \) is the set of all matrices of the form:

\[
\begin{bmatrix}
1 & 0 & 0 & a_{14} \\
1 & 0 & a_{24} & 0 \\
1 & a_{34} & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}, \quad
\begin{bmatrix}
1 & 0 & a_{13} & 0 \\
1 & 0 & a_{23} & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0
\end{bmatrix}, \quad
\begin{bmatrix}
1 & a_{12} & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}, \quad
\begin{bmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0
\end{bmatrix}
\]

with each \( a_{ij} \in F_q \).

Clearly, every matrix in \( E(n,k) \) is an idempotent, of rank \( k \). We first claim that each matrix in \( E(n,k) \) generates a different left ideal of \( M_n(F_q) \).

In fact, notice that, given \( R,S \in E(n,k) \), if they differ in some pivotal position, then \( W(R) \neq W(S) \) so \( \langle R \rangle \neq \langle S \rangle \).

On the other hand, if \( R \) and \( S \) have the same pivotal positions, then it is easy to see that \([R] = [S]\) and part (b) of Remark 2.7 shows that \( RS = S \) and \( SR = R \). If \( \langle R \rangle = \langle S \rangle \), it follows from part (ii) of Theorem 2.5 that also \( RS = R \) and \( SR = S \), showing that \( R = S \).

We shall show that \( S(n,k) \), the number of elements in \( E(n,k) \) is equal to the number of left ideals of rank \( k \) in \( M_n(F_q) \).

**Lemma 3.2.** With the notations above, we have that

\[
S(n,k) = \frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)\cdots(q-1)}.
\]

**Proof.** We use induction on \( n \). If \( n = 1 \) the result is trivially true, so assume that the result holds for \( n - 1 \) and \( k \leq n - 1 \).

We compute separately the number of elements in \( E(n,k) \) that have the pivotal position \( i_k = n \) and those which do not. Clearly, there are \( S(n-1,k-1) \) idempotents that have an entry equal to 1 in position \( n,n \). Since each matrix having an entry equal to 0 in position \( n,n \) has
$k$ entries from $\mathbb{F}_q$ in the last column, there exist $S(n-1, k)q^k$ such matrices, so we have:

$$S(n, k) = S(n - 1, k - 1) + S(n - 1, k)q^k.$$ 

Using the induction hypothesis we get:

$$S(n, k) = (q^{n-1} - 1) \cdots (q^{n-k+1} - 1) \cdot \left( \frac{q^{n-k} - 1}{q^k - 1} + q^{n-k} \right) + \frac{(q^{n-1} - 1) \cdots (q^{n-k} - 1)}{(q^k - 1) \cdots (q - 1)} \cdot q^k = \frac{(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1) \cdots (q - 1)} \left[ \frac{q^{n-k} - 1}{q^k - 1} + q^{n-k} \right] + \frac{(q^{n-1} - 1) \cdots (q^{n-k} - 1)}{(q^k - 1) \cdots (q - 1)} \left[ 1 + \frac{(q^{n-k} - 1)q^k}{q^k - 1} \right].$$

Notice that the number of elements in $E(n, k)$ found above is equal to the number of left ideals of rank $k$ in $M_n(\mathbb{F}_q)$, as seen in Theorem 2.4.

So, we have shown the first part of the following.

**Theorem 3.3.** The elements of the set $S(n, k)$ are idempotent generators of the different left ideals of rank $k$ of $M_n(\mathbb{F}_q)$. Moreover, each left ideal of rank $k$ has $q^{(n-k)k}$ different idempotent generators.

**Proof.** We are left to prove only the last statement.

Set $F_{kk} = \text{diag}(1, \ldots, 1, 0, \ldots 0)$. Then, using Theorem 2.6, we have

$$M_0 = F_{kk} + (I - F_{kk})MF_{kk}, \text{ with } M \in M_n(\mathbb{F}_q).$$

So, $M_0 = \begin{bmatrix} I & 0 \\ B & 0 \end{bmatrix}$ with $I \in M_{k,k}(\mathbb{F}_q)$, $B \in M_{n-k,k}(\mathbb{F}_q)$.

Hence, this ideal has $q^{(n-k)k}$ generators.

Arguments similar to those in the proof of Theorem 3.1 show that all left ideals of rank $k$ have the same number of idempotent generators.

Notice that a matrix in $\langle F_{kk} \rangle$ is of rank $k$ if and only if the first $k$ rows are linearly independent. The total number of choices of $k$ elements of
which are linearly independent is
\[(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{k-1}).\]

All left ideals of rank \(k\) contain the same number of matrices of that rank, since they are isomorphic to \(\langle F_{kk} \rangle\). As every matrix of rank \(k\) belongs to one and only one such an ideal, using Theorem 3.3 above, we get the following.

**Theorem 3.4.** Let \(k\) be an integer, \(1 \leq k \leq n\). Then, the number of matrices of rank \(k\) in \(M_n(F_q)\) is
\[
\frac{(q^n - 1)(q^{n-1} - 1)(q^{n-2} - 1) \cdots (q^{n-k+1} - 1))^2}{(q^k - 1)(q^{k-1} - 1)(q^{k-2} - 1) \cdots (q - 1)}.
\]

**References**

[1] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge, Cambridge Univ. Press, 2001.