Proportion of cyclic matrices in maximal reducible matrix algebras

Scott Brown [a,1], Michael Giudici [a], S.P. Glasby [b,*,2], Cheryl E. Praeger [a,3]

[a] *Centre for Mathematics of Symmetry and Computation, School of Mathematics and Statistics, University of Western Australia, 35 Stirling Highway, Crawley 6009, Australia*
[b] *Department of Mathematics, Central Washington University, WA 98926, USA*

ABSTRACT

Let $M(V) = M(n, \mathbb{F}_q)$ denote the algebra of $n \times n$ matrices over $\mathbb{F}_q$, and let $M(V)_U$ denote the (maximal reducible) subalgebra that normalizes a given r-dimensional subspace U of $V = \mathbb{F}_q^n$ where $0 < r < n$. We prove that the density of non-cyclic matrices in $M(V)_U$ is at least $q^{-2}(1 + c_1 q^{-1})$, and at most $q^{-2}(1 + c_2 q^{-1})$, where c_1 and c_2 are constants independent of n, r, and q. The constants $c_1 = -\frac{4}{3}$ and $c_2 = \frac{35}{3}$ suffice.

© 2012 Elsevier Inc. All rights reserved.

* Corresponding author.
   E-mail addresses: scott.brown@graduate.uwa.edu.au (S. Brown), Michael.Giudici@uwa.edu.au (M. Giudici), GlasbyS@gmail.com (S.P. Glasby), Cheryl.Praeger@uwa.edu.au (C.E. Praeger).
   URLs: http://www.maths.uwa.edu.au/~giudici/ (M. Giudici), http://www.cwu.edu/~glasbys/ (S.P. Glasby), http://www.maths.uwa.edu.au/~praeger/ (C.E. Praeger).
[1] Current address: TSG Consulting, Perth 6000, Australia.
[2] Also affiliated with The Faculty of Information Sciences and Engineering, University of Canberra, ACT 2601, Australia.
[3] Also affiliated with King Abdulaziz University, Jeddah, Saudi Arabia.

1. The main result

The MEAT-AXE is an algorithm often used to test whether a given group or algebra of matrices over a finite field acts irreducibly on the underlying vector space, see [P,HR,NP2]. It uses random selection to find a 'good' matrix, and if successful is able to determine whether the action is reducible or irreducible. One definition of a 'good' matrix in this context is a *cyclic* matrix. (A matrix is cyclic if its characteristic and minimal polynomials are equal.) The density of cyclic matrices in absolutely irreducible groups and algebras is constrained by the following result of Neumann and the fourth author [NP1, Theorem 4.1]. The probability $P_{d,q} := \mathrm{Prob}(X \in \mathrm{M}(d, \mathbb{F}_q)$ is non-cyclic) satisfies

$$\frac{q^{-3}}{1 + q^{-1}} < P_{d,q} < \frac{q^{-3}}{(1 - q^{-1})(1 - q^{-2})} \quad \text{for all } d \geqslant 2 \text{ and } q \geqslant 2. \tag{1}$$

Thus $\frac{2q^{-3}}{3} \leqslant P_{d,q} \leqslant \frac{8q^{-3}}{3}$, so $P_{d,q} = \Omega(q^{-3})$ for $d \geqslant 2$. If $d = 1$, then $P_{1,q} = 0$ because each 1×1 matrix is cyclic. Bounds on the proportion of non-cyclic matrices in irreducible-but-not-absolutely-irreducible matrix algebras are also available in [NP1].

This note shows that cyclic matrices are less dense in maximal *reducible* matrix algebras than full matrix algebras, with density $1 - c(q)q^{-2}$ rather than $1 - c'(q)q^{-3}$ where $c(q), c'(q)$ are bounded functions. We do not know how to estimate the density δ of cyclic matrices in arbitrary non-maximal reducible algebras. Since $0 \leqslant \delta \leqslant 1$, our lower bound $q^{-2}(1 + c_1 q^{-1}) < \delta$ is unhelpful if $c_1 < -q$ for some choice of q. Similarly, our upper bound $\delta < q^{-2}(1 + c_2 q^{-1})$ is unhelpful if $c_2 > q(q^2 - 1)$. We go to some effort to find helpful bounds for all values of q. While motivated by a complexity analysis of the MEAT-AXE algorithm, we feel that this problem has broader interest.

A modification of Norton's Irreducibility Test, called the Cyclic Irreducibility Test, was presented in [NP2]. It was shown to be a Monte Carlo algorithm that proved irreducibility of a finite irreducible matrix algebra $\mathcal{A}$ provided a *cyclic pair* was found, that is a pair (v, X) where X is a cyclic matrix in $\mathcal{A}$, and v is a cyclic vector for X. It was hoped that cyclic pairs in reducible matrix algebras, if such exist, could be used to construct a proper $\mathcal{A}$-invariant subspace. However, it was not known which reducible algebras $\mathcal{A}$ might contain a sufficiently high proportion of cyclic matrices to make this approach worth exploring. In this paper we prove that finite maximal reducible matrix algebras do indeed have a plentiful supply of cyclic elements, with the proportion slightly less than that for the full matrix algebra. A variant of the Cyclic Irreducibility Test is given in [B, p. 141].

Notation A. The following notation will be used throughout the paper.

$F = \mathbb{F}_q$ a finite field with q elements;
$V = F^n$ the F-space of $1 \times n$ row vectors;
U a fixed r-dimensional subspace of V where $0 < r < n$;
$\mathrm{M}(V) = \mathrm{M}(n, F) = F^{n \times n}$ the F-algebra of all $n \times n$ matrices over F;
$\mathrm{GL}(V)$ the group of units of $\mathrm{M}(V)$: isomorphic to the general linear group $\mathrm{GL}(n, q)$;
$\mathrm{M}(V)_U$ the stabilizer in $\mathrm{M}(V)$ of U: isomorphic to the algebra of matrices $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$ with $A \in F^{r \times r}$, $B \in F^{(n-r) \times (n-r)}$, and $C \in F^{(n-r) \times r}$;
$\mathrm{GL}(V)_U$ the group of units of $\mathrm{M}(V)_U$ comprising all X with $\det(X) = \det(A)\det(B) \neq 0$.

Theorem 1. *Suppose that $0 < r < n$ and U is an r-dimensional subspace of $V := \mathbb{F}_q^n$. Then there exist constants c_1, c_2, independent of n, r, q, such that the probability that a uniformly distributed random matrix $X \in \mathrm{M}(V)_U$ is non-cyclic satisfies*

$$q^{-2}(1 + c_1 q^{-1}) \leqslant \mathrm{Prob}(X \in \mathrm{M}(V)_U \text{ is non-cyclic}) \leqslant q^{-2}(1 + c_2 q^{-1}).$$

The constants $c_1 = -\frac{4}{3}$ and $c_2 = \frac{35}{3}$ suffice.

Table 1

Proportions of cyclic matrices in $M(V)_U$ as $\dim(V) \to \infty$.

$\dim U$	Proportion of cyclic matrices in $M(V)_U$ as $\dim(V) \to \infty$
1	$1 - q^{-2} - 2q^{-3} - q^{-4} \phantom{+ 4q^{-5}} + 2q^{-6} + 3q^{-7} +$ lower terms
2	$1 - q^{-2} - 4q^{-3} - q^{-4} + 4q^{-5} + 5q^{-6} + 4q^{-7} +$ lower terms
3	$1 - q^{-2} - 4q^{-3} - 3q^{-4} + 4q^{-5} + 11q^{-6} + 8q^{-7} +$ lower terms
4	$1 - q^{-2} - 4q^{-3} - 3q^{-4} + 2q^{-5} + 11q^{-6} + 14q^{-7} +$ lower terms
5	$1 - q^{-2} - 4q^{-3} - 3q^{-4} + 2q^{-5} + 9q^{-6} + 14q^{-7} +$ lower terms
6	$1 - q^{-2} - 4q^{-3} - 3q^{-4} + 2q^{-5} + 9q^{-6} + 12q^{-7} +$ lower terms
7	$1 - q^{-2} - 4q^{-3} - 3q^{-4} + 2q^{-5} + 9q^{-6} + 12q^{-7} +$ lower terms

Table 2

Proportions of cyclic matrices in $GL(V)_U$ as $\dim(V) \to \infty$.

$\dim U$	Proportion of cyclic matrices in $GL(V)_U$ as $\dim(V) \to \infty$
1	$1 - q^{-2} - 2q^{-3} \phantom{+ 3q^{-4}} + q^{-5} + 3q^{-6} + q^{-7} +$ lower terms
2	$1 - q^{-2} - 3q^{-3} + q^{-4} + 3q^{-5} + 4q^{-6} - 2q^{-7} +$ lower terms
3	$1 - q^{-2} - 3q^{-3} + q^{-4} + 4q^{-5} + 4q^{-6} - 5q^{-7} +$ lower terms
4	$1 - q^{-2} - 3q^{-3} + q^{-4} + 4q^{-5} + 4q^{-6} - 6q^{-7} +$ lower terms
5	$1 - q^{-2} - 3q^{-3} + q^{-4} + 4q^{-5} + 4q^{-6} - 6q^{-7} +$ lower terms
6	$1 - q^{-2} - 3q^{-3} + q^{-4} + 4q^{-5} + 4q^{-6} - 6q^{-7} +$ lower terms
7	$1 - q^{-2} - 3q^{-3} + q^{-4} + 4q^{-5} + 4q^{-6} - 6q^{-7} +$ lower terms

Remark 2. (a) The lower bound in Theorem 1 is positive for all $q \geqslant 2$, and the upper bound is less than 1 for all $q > 2$. With more care we may increase c_1 and decrease c_2. However, a new argument is needed to give an upper bound less than 1 when $q = 2$ because the first term in (3) below is $\frac{q^{-2}}{(1-q^{-1})^2} = 1$ when $q = 2$.

(b) The bounds in Theorem 1 in the cases $r = 1$ and $r = n - 1$ can be deduced from results in Jason Fulman's paper [F] since in these cases $GL(V)_U$ is an affine group. The first asymptotic estimate for the probability in Theorem 1, for general values of r, was given as the main result in the PhD thesis of the first author [B] where a probabilistic generating function was found for the proportion of cyclic matrices in $GL(V)_U$ for a subspace U of fixed dimension r. The limiting proportions of cyclic matrices in both $GL(V)_U$ and $M(V)_U$, as $\dim(V) \to \infty$, were proved to be power series in q^{-1} of the form $1 - q^{-2} + \sum_{i \geqslant 3} \gamma_i q^{-i}$. (In Tables 1 and 2 the 'lower terms' residual was not bounded by a function of r and q in [B]. By contrast, bounding constants independent of r, n, q are explicit in the statement, and proof, of Theorem 1.) Exact values for these limiting proportions can be determined from the generating function for small values of r, and some sample results are given in Tables 1 and 2. These results show that the γ_i depend mildly on the dimension r when $i \geqslant 3$. The expressions for $r = 1, 2$ were deduced analytically, and those for $3 \leqslant r \leqslant 7$ were obtained using MATHEMATICA [W].

(c) Truncating the power series in Table 1 suggests (heuristically) that the probability in Theorem 1 'ought' to have the form $q^{-2}(1 + 4q^{-1})$. This is consistent with the constants given in Theorem 1 as $-\frac{4}{3} = c_1 \leqslant 4 \leqslant c_2 = \frac{35}{3}$.

(d) The PhD thesis of the first author contains analogous results for the limiting proportions (as $\dim(V) \to \infty$) of cyclic matrices in maximal completely reducible matrix algebras [B, Theorems 5.2.8 and 5.3.5], see also the unpublished paper [BGP]. The limiting proportions of separable matrices in maximal reducible matrix algebras are described in [B, Theorem 6.4.6].

Proof Strategy for Theorem 1. Since $GL(V)$ acts transitively on the set of r-dimensional subspaces of V, the stabilizers of r-dimensional subspaces, being conjugate, all have the same cardinality. Thus it suffices to consider the stabilizer $M(V)_U$ of the r-dimensional subspace $U := \langle e_1, \ldots, e_r \rangle$ where e_i denotes the ith row of the $n \times n$ identity matrix I_n. Suppose that $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in M(V)_U$ is non-cyclic.

Exactly one of the following holds:

  (i) A is non-cyclic, or
 (ii) A is cyclic, and B is non-cyclic, or
(iii) $A \in \mathrm{M}(U)$ and $B \in \mathrm{M}(V/U)$ are cyclic, and $X \in \mathrm{M}(V)_U$ is non-cyclic.

Denote by n_1, n_2, n_3 the number of *non-cyclic* $X \in \mathrm{M}(V)_U$ satisfying the pairwise mutually exclusive cases (i), (ii), and (iii), respectively. The desired probability is $\pi = \pi_1 + \pi_2 + \pi_3$ where $\pi_i := \frac{n_i}{|\mathrm{M}(V)_U|}$, and $|\mathrm{M}(V)_U| = q^{n^2 - nr + r^2}$.

    The cases when $r = 1$ or $n - 1$ can be handled separately. Suppose $1 < r < n - 1$. The probability π_1 that A is non-cyclic is $\Omega(q^{-3})$ by (1). Since the events 'A is cyclic' and 'B is non-cyclic' are independent, the probability π_2 is $(1 - \pi_1)\,\mathrm{Prob}(B \text{ non-cyclic}) = \Omega(q^{-3})$. Explicit upper and lower bounds may be determined by applying (1). The proof is complete once we prove that $\pi_3 = q^{-2}(1 + \Omega(q^{-1}))$. This is achieved by constructing an upper bound for n_3 in Section 2, and a lower bound for n_3 in Section 4. $\quad\square$

    Bounds for the density of non-cyclic matrices in the group $\mathrm{GL}(V)_U$ can be deduced from those for the density in the algebra $\mathrm{M}(V)_U$. Dividing by $|\mathrm{GL}(V)_U|$ instead of $|\mathrm{M}(V)_U|$ is not problematic since $|\mathrm{GL}(V)_U| = |\mathrm{M}(V)_U|(1 + \Omega(q^{-1}))$. An upper bound for non-cyclic matrices in $\mathrm{M}(V)_U$ is also an upper bound for non-cyclic matrices in $\mathrm{GL}(V)_U$ as $\mathrm{GL}(V)_U \subseteq \mathrm{M}(V)_U$. A lower bound for non-cyclic matrices in $\mathrm{GL}(V)_U$ needs to be altered to ensure that only *invertible* non-cyclic matrices are counted. This requires only minor modifications to Section 4. Since the Meat-axe is more commonly concerned with algebras and not groups, we leave this modification to an interested reader.

2. The upper bound

    Let U be an r-dimensional subspace of the vector space $V = F^n$ where $0 < r < n$ and $F = \mathbb{F}_q$ is the field with q elements. Let $\mathrm{M}(V)_U = \{X \in \mathrm{M}(V) \mid UX \subseteq U\}$ be the algebra of $q^{r^2 - rn + n^2}$ matrices that normalize U. The goal of this section is to compute an upper bound for the number, n_3, of matrices $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in \mathrm{M}(V)_U$ for which U is a cyclic $F[A]$-module, V/U is a cyclic $F[B]$-module, and V is a *non-cyclic* $F[X]$-module.

Notation B. As well as Notation A, the following notation will be used in the paper.

    $F[t]$ denotes the ring of polynomials with coefficients in F;
    $X \in \mathrm{M}(V)$ denotes a matrix, and $v \in V$ denotes a (row) vector;
    $F[X]$ is the subalgebra of $\mathrm{M}(V)$ comprising all polynomials in X with coefficients in F;
    $vF[X] = \langle v, vX, vX^2, \ldots \rangle$ is the *cyclic $F[X]$-submodule* of V generated by v;
    $f \in \mathrm{Irr}(d, F)$ denotes a monic polynomial of degree d which is irreducible in $F[t]$;
    c_X denotes the characteristic polynomial $c_X(t) = \det(tI_n - X)$ of $X \in \mathrm{M}(n, F)$;
    m_X denotes the minimal polynomial of $X \in \mathrm{M}(n, F)$;
    $V(f) = \{v \in V \mid vf(X) = 0\} = \ker f(X)$;
    $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in \mathrm{M}(V)_U$ denotes a block matrix with $A \in \mathrm{M}(r, F)$ and $B \in \mathrm{M}(n - r, F)$ cyclic, $C \in F^{(n-r) \times r}$, and X non-cyclic;
    $\omega(n, q) = \prod_{i=1}^{n}(1 - q^{-i})$; note that $|\mathrm{GL}(n, q)| = q^{n^2}\omega(n, q)$;
    $C(a)$ the (row) companion matrix of a polynomial $a(t) = t^r + \sum_{i=0}^{r-1} a_i t^i$, see (5).

    There exists a monic irreducible polynomial $f \in \mathrm{Irr}(d, q)$ with $1 \leqslant d \leqslant \min(r, n - r)$ for which $V_0 := \ker f(X)$ is a non-cyclic $F[X]$-module. The restriction, X_0, of X to V_0 has minimal polynomial f. Since $U_0 := V_0 \cap U$ and $(V_0 + U)/U \cong V_0/U_0$ are cyclic $F[X]$-modules, it follows that X_0 is conjugate to the block diagonal matrix $\mathrm{diag}(C(f), C(f))$. The number of d-dimensional subspaces U_0 of the r-dimensional space U is given by the q-binomial coefficient

$$\begin{bmatrix} r \\ d \end{bmatrix} := \prod_{i=0}^{d-1} \frac{q^r - q^i}{q^d - q^i} = q^{d(r-d)} \prod_{i=0}^{d-1} \frac{1 - q^{-(r-i)}}{1 - q^{-(d-i)}} = \frac{q^{d(r-d)}\omega(r,q)}{\omega(d,q)\omega(r-d,q)}. \tag{2}$$

It is well known that $\begin{bmatrix} r \\ d \end{bmatrix} \in \mathbb{Z}[q]$ is a polynomial in q over $\mathbb{N}$, and $\deg(\begin{bmatrix} r \\ d \end{bmatrix}) = d(r-d)$.

First, choose d in the range $1 \leqslant d \leqslant \min(r, n-r)$, next choose a monic $f \in \mathrm{Irr}(d, q)$, then a $2d$-dimensional subspace V_0 for which $\dim(V_0 \cap U) = \dim((V_0 + U)/U) = d$, then choose a linear transformation X_0 on V_0 with minimal polynomial $m_{X_0} = f$ satisfying $U_0 X_0 \subseteq U_0$, and finally choose an extension X of X_0 to V. The number of 4-tuples (f, V_0, X_0, X) overcounts the number n_3 since different f may give the same X. Moreover we shall overcount the number of 4-tuples.

In this paragraph the value of d satisfying $1 \leqslant d \leqslant \min(r, n-r)$ is fixed. There are at most $\frac{q^d - q}{d}$ choices for f if $d \geqslant 2$, and q choices if $d = 1$. How many choices are there for V_0? First, choose U_0 in $\begin{bmatrix} r \\ d \end{bmatrix}$ ways, then choose $U + V_0$, or equivalently choose the d-dimensional subspace $(U + V_0)/U$ of the $(n-r)$-dimensional space V/U in $\begin{bmatrix} n-r \\ d \end{bmatrix}$ ways. Finally, choose a d-dimensional complement V_0/U_0 to the $(r-d)$-dimensional subspace U/U_0 in $(U + V_0)/U$ in $q^{d(r-d)}$ ways. Multiplying shows that there are exactly $\begin{bmatrix} r \\ d \end{bmatrix}\begin{bmatrix} n-r \\ d \end{bmatrix}q^{d(r-d)}$ choices for V_0. Since $U_0 X_0 \subseteq U_0$ and X_0 has minimal polynomial $m_{X_0} = f$, it is conjugate in $\mathrm{GL}(V_0)_{U_0}$ to the 2×2 block diagonal matrix $\mathrm{diag}(C(f), C(f))$. The centralizer in $\mathrm{GL}(V_0)_{U_0}$ of X_0 has order $(q^d - 1)^2 q^d = q^{3d}(1 - q^{-d})^2$, and the conjugacy class $X_0^{\mathrm{GL}(V_0)_{U_0}}$ has cardinality

$$\left|X_0^{\mathrm{GL}(V_0)_{U_0}}\right| = \frac{|\mathrm{GL}(V_0)_{U_0}|}{|C_{\mathrm{GL}(V_0)_{U_0}}(X_0)|} = \frac{q^{3d^2}\omega(d,q)^2}{q^{3d}(1 - q^{-d})^2} = \frac{q^{3(d^2-d)}\omega(d,q)^2}{(1 - q^{-d})^2}.$$

Specifying X_0, can be viewed (after a change of basis) as specifying d of the top r rows, and d of the bottom $n - r$ rows of $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix}$. The remaining rows can be completed in at most $|\mathrm{M}(V)_U| q^{-(r+n)d}$ ways. This shows

$$n_3 \leqslant \sum_{d=1}^{\min(r,n-r)} |\mathrm{Irr}(d,q)| \cdot \begin{bmatrix} r \\ d \end{bmatrix}\begin{bmatrix} n-r \\ d \end{bmatrix} \frac{q^{d(r-d)}}{1} \cdot \frac{q^{3(d^2-d)}\omega(d,q)^2}{(1 - q^{-d})^2} \cdot \frac{|\mathrm{M}(V)_U| q^{-(r+n)d}}{1}.$$

Eq. (2) yields $\begin{bmatrix} r \\ d \end{bmatrix} \leqslant \frac{q^{d(r-d)}}{\omega(d,q)}$ and $\begin{bmatrix} n-r \\ d \end{bmatrix} \leqslant \frac{q^{d(n-r-d)}}{\omega(d,q)}$. This, in turn, shows

$$n_3 \leqslant \sum_{d=1}^{\min(r,n-r)} |\mathrm{Irr}(d,q)| \cdot \frac{q^{d(r-d)+d(n-r-d)+d(r-d)}}{\omega(d,q)^2} \cdot \frac{q^{3(d^2-d)}\omega(d,q)^2}{(1 - q^{-d})^2} \cdot \frac{|\mathrm{M}(V)_U| q^{-(r+n)d}}{1}.$$

Collecting powers of q gives q^{-3d}. Cancelling $\omega(d,q)^2$, dividing by $|\mathrm{M}(V)_U|$, and using the inequality $|\mathrm{Irr}(d,q)| \leqslant \frac{q^d - q}{d}$ for $d \geqslant 2$ gives

$$\frac{n_3}{|\mathrm{M}(V)_U|} \leqslant \frac{q^{-2}}{(1 - q^{-1})^2} + \sum_{d=2}^{\min(r,n-r)} \frac{q^d - q}{d} \cdot \frac{q^{-3d}}{(1 - q^{-d})^2}$$

$$< \frac{q^{-2}}{(1 - q^{-1})^2} + \sum_{d=2}^{\infty} \frac{q^{-2d}}{d(1 - q^{-d})}. \tag{3}$$

The first term is $\frac{q^{-2}}{(1-q^{-1})^2} \leqslant q^{-2}(1+6q^{-1})$, and the infinite sum is less than $\frac{8q^{-4}}{9}$ because $\frac{1}{d(1-q^{-d})} \leqslant \frac{1}{2(1-2^{-2})} \leqslant \frac{2}{3}$ for $d \geqslant 2$, and $\sum_{d=2}^{\infty} q^{-2d} = \frac{q^{-4}}{1-q^{-2}} \leqslant \frac{4q^{-4}}{3}$. Hence

$$\frac{n_3}{|M(V)_U|} < q^{-2}\left(1+6q^{-1}\right) + \frac{4q^{-3}}{9} \leqslant q^{-2}\left(1 + \frac{58q^{-1}}{9}\right).$$

3. Counting polynomials

The goal of this section is to prove a simple combinatorial result for polynomials over $\mathbb{F}_q$. This result will be used in Section 4 to prove a lower bound for n_3. Morrison [M] proves that the density of coprime pairs of polynomials of degree *at most* r over $\mathbb{F}_q$ is $1 - q^{-1} + q^{-2r-1} - q^{-2r-2}$. A simpler answer exists if the degrees are *precisely* r.

Lemma 3. *Let $\mathcal{M}_r$ denote the set of q^r monic polynomials in $\mathbb{F}_q[t]$ of degree r.*

(a) *The number of coprime ordered pairs (a, b) in $\mathcal{M}_r \times \mathcal{M}_s$ is $q^{r+s}(1 - q^{-1})$ when $rs > 0$, and q^{r+s} when $rs = 0$.*
(b) *Fix $f \in \mathrm{Irr}(d, q)$ and suppose $1 \leqslant d \leqslant \min(r, s)$. Then the number of coprime pairs (a, b) in $\mathcal{M}_r \times \mathcal{M}_s$ satisfying $\gcd(f, ab) = 1$ is at least $q^{r+s}(1 - q^{-1} - 2q^{-d} + 2q^{-2d})$.*

Proof. (a) Let $c(r, s)$ denote the number of coprime ordered pairs $(a, b) \in \mathcal{M}_r \times \mathcal{M}_s$. The cardinality of $\mathcal{M}_r \times \mathcal{M}_s$, viz. $|\mathcal{M}_r||\mathcal{M}_s| = q^{r+s}$, can be determined in a different way.

An ordered pair $(a, b) \in \mathcal{M}_r \times \mathcal{M}_s$ has $\gcd(a, b) = d$ if and only if $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. If $\deg(d) = k$, then there are q^k choices for d, and $c(r - k, s - k)$ pairs $(\frac{a}{d}, \frac{b}{d})$. Thus

$$|\mathcal{M}_r \times \mathcal{M}_s| = \sum_{k=0}^{\min(r,s)} |\mathcal{M}_k| c(r - k, s - k), \quad \text{or} \quad q^{r+s} = \sum_{k=0}^{\min(r,s)} q^k c(r - k, s - k).$$

Rearranging gives a recurrence relation $c(r, s) = q^{r+s} - \sum_{k=1}^{\min(r,s)} q^k c(r - k, s - k)$ with initial conditions $c(r, 0) = q^r$, $c(0, s) = q^s$. Induction may be used to prove $c(r, s) = q^{r+s}(1 - q^{-1})$ holds when $rs > 0$. (The sum in the recurrence telescopes to q^{r+s-1}.) It is noteworthy that the probability $c(r, s)/q^{r+s} = 1 - q^{-1}$ is independent of both r and s.

(b) Assume $f \in \mathrm{Irr}(d, q)$ and $1 \leqslant d \leqslant \min(r, s)$. We shall underestimate the number of coprime ordered pairs $(a, b) \in \mathcal{M}_r \times \mathcal{M}_s$ for which $\gcd(ab, f) = 1$. By part (a) there are $q^{r+s}(1 - q^{-1})$ coprime pairs $(a, b) \in \mathcal{M}_r \times \mathcal{M}_s$. The number of $a \in \mathcal{M}_r$ divisible by f is q^{r-d}, and the number of $(a, b) \in \mathcal{M}_r \times \mathcal{M}_s$ with $f \mid a$ and $f \mid b$ is q^{r+s-2d}. Hence $q^{r+s-d} - q^{r+s-2d}$ ordered pairs (a, b) have $f \mid a$ and $f \nmid b$. The same count holds for ordered pairs (a, b) with $f \nmid a$ and $f \mid b$. However, some of these ordered pairs may not be coprime, and therefore $q^{r+s}(1 - q^{-1}) - 2(q^{r+s-d} - q^{r+s-2d})$ underestimates the number of coprime (a, b) with $\gcd(f, ab) = 1$. Rearranging proves the result. $\square$

A heuristic argument suggests that the matrices $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in M(V)_U$ for which c_A and c_B are not coprime, has density roughly q^{-1}. An extra factor of q^{-1} arises when we insist that X is non-cyclic. This is basically because there are q non-cyclic matrices in $M(V)_U$ when $\dim(V) = 2$ and $\dim(U) = 1$, as C must be 0. A rigorous argument is given below.

4. The lower bound

Fix $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in M(V)_U$. Then V becomes an $F[t]$-module with $v * f(t) = vf(X)$ where the juxtaposition $vf(X)$ denotes vector-times-matrix multiplication. We also say that V is an $F[X]$-module,

where $F[X]$ is the subalgebra of $M(V)_U$ comprising all polynomials in X over F. In this section we give a lower bound for n_3 by underestimating the number of matrices $X \in M(V)_U$ which have a *unique* non-cyclic primary submodule. For these matrices, U is a cyclic $F[A]$-module, V/U is a cyclic $F[B]$-module, and V is a *non-cyclic* $F[X]$-module. That is, we are counting certain $X = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \in M(V)_U$ for which $c_A = m_A$, $c_B = m_B$, and $c_X = c_A c_B \ne m_X$.

Since U and V/U are cyclic, there exist vectors $u \in U$ and $v + U \in V/U$, generating the respective $F[t]$-modules. Consider the basis

$$u, uX, \ldots, uX^{r-1}, v, vX, \ldots, vX^{n-r-1} \tag{4}$$

for V. Then X is conjugate in $GL(V)_U$ to a matrix of the form $\begin{pmatrix} A' & 0 \\ C' & B' \end{pmatrix} \in M(V)_U$ where

$$A' = \begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \\ -a_0 & -a_1 & \cdots & -a_{r-1} \end{pmatrix}, \qquad B' = \begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \\ -b_0 & -b_1 & \cdots & -b_{n-r-1} \end{pmatrix},$$

$$C' = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ c_0 & c_1 & \cdots & c_{r-1} \end{pmatrix}. \tag{5}$$

Set $a := t^r + \sum_{i=0}^{r-1} a_i t^i = m_A$, $b := t^{n-r} + \sum_{i=0}^{n-r-1} b_i t^i = m_B$, and $c := \sum_{i=0}^{r-1} c_i t^i$. Then $ua(X) = 0$ and $vb(X) = uc(X)$ where $\deg(c) < \deg(a)$. The matrices A' and B' are called *companion matrices* of a and b and are abbreviated $C(a)$ and $C(b)$, respectively.

We shall count non-cyclic matrices X for which $a = fg$, $b = fh$, $f \in \text{Irr}(d, q)$, and $\gcd(f, gh) = \gcd(g, h) = 1$. Note that $V = V(f) \oplus V(gh)$ where X is non-cyclic on $V(f) := \ker f(X)$, and cyclic on $V(gh) = V(g) \oplus V(h)$. Such matrices X are conjugate in $GL(V)_U$ to the block diagonal matrix $X_{f,g,h} := \text{diag}(C(g), C(f), C(f), C(h))$ for a uniquely determined triple (f, g, h). This fact is needed to establish a lower bound for n_3. (Different choices for f give different $X_{f,g,h}$ due to our assumption that $V(f)$ is the *unique* non-cyclic primary $F[X]$-submodule of V.) As X is conjugate in $GL(V)$ to $\text{diag}(C(f) \oplus C(f), C(gh))$, it follows that $|C_{GL(V)_U}(X)| \leqslant q^{3d}(1 - q^{-d})^2(q^{n-2d} - 1)$ because

$$C_{GL(V)_U}(X) \leqslant C_{GL(V)}(X) \cong C_{GL(V(f))}\big(C(f) \oplus C(f)\big) \times C_{GL(V(gh))}\big(C(gh)\big).$$

First, choose d in the range $1 \leqslant d \leqslant \min(r, n-r)$, next choose a monic $f \in \text{Irr}(d, q)$, then choose an ordered pair (g, h) satisfying $\gcd(f, gh) = \gcd(g, h) = 1$. By Lemma 3(b), there are at least

$$q^{(r-d)+(n-r-d)}\big(1 - q^{-1} - 2q^{-d} + 2q^{-2d}\big) = q^{n-2d}\big(1 - q^{-1} - 2q^{-d} + 2q^{-2d}\big)$$

ordered pairs (g, h). Summing over the relevant triples (f, g, h) gives

$$n_3 \geqslant \sum_{d=1}^{\min(r, n-r)} \sum_{f \in \text{Irr}(d,q)} \sum_{(g,h)} \frac{|GL(V)_U|}{|C_{GL(V)_U}(X_{f,g,h})|}.$$

But $|GL(V)_U| = |M(V)_U| \omega(r, q) \omega(n-r, q)$ and $|C_{GL(V)_U}(X)| \leqslant q^{3d}(1 - q^{-d})^2(q^{n-2d} - 1)$ so

$$\frac{n_3}{|M(V)_U|} \geqslant \sum_{d=1}^{\min(r, n-r)} \big|\text{Irr}(d, q)\big| \frac{\omega(r, q) \omega(n-r, q)}{q^{3d}(1 - q^{-d})^2(q^{n-2d} - 1)} \cdot q^{n-2d}\big(1 - q^{-1} - 2q^{-d} + 2q^{-2d}\big).$$

Euler's pentagonal number theorem shows that $\omega(\infty, q) > 1 - q^{-1} - q^{-2} + q^{-5}$. Therefore

$$\frac{n_3}{|M(V)_U|} \geqslant \sum_{d=1}^{\min(r, n-r)} |\mathrm{Irr}(d, q)| \frac{q^{-3d}(1 - q^{-1} - q^{-2} + q^{-5})^2}{(1 - q^{-d})^2(1 - q^{-(n-2d)})} \cdot (1 - q^{-1} - 2q^{-d} + 2q^{-2d}). \quad (6)$$

The number n_3 depends on r. To emphasize this dependence we write $n_3(r)$. The automorphism of $M(V)$ obtained by conjugating by $e_i \leftrightarrow e_{n-i}$ and then transposing, swaps the maximal reducible algebras $M(V)_{U(r)}$ and $M(V)_{U(n-r)}$. Hence $n_3(r) = n_3(n-r)$. By swapping r and $n-r$, if necessary, we shall assume that $\min(r, n-r) = r$. It is convenient to give a sharper lower bound than (6) in the case that $r = 1$. The calculation above has $a = t - \lambda = f$, $g = 1$, and $b = fh$ where $h(\lambda) \neq 0$. There are precisely $q^{n-2}(1 - q^{-1})$ choices for h. (This is a sharper estimate than given above.) Hence when $r = 1$, we have $d = 1$. Since $|\mathrm{Irr}(1, q)| = q$ and $1 - q^{-1} - q^{-2} + q^{-5} = (1 - q^{-1})(1 - q^{-2} - q^{-3} - q^{-4})$, a sharper bound than (6) for $n \geqslant 3$ is

$$\frac{n_3(1)}{|M(V)_U|} \geqslant \frac{q \cdot q^{-3}(1 - q^{-1} - q^{-2} + q^{-5})^2 q^{n-2}(1 - q^{-1})}{(1 - q^{-1})^2(q^{n-2} - 1)}$$

$$\geqslant q^{-2}(1 - q^{-2} - q^{-3} - q^{-4})^2(1 - q^{-1}). \quad (7)$$

This bound also holds when $n = 2$ and $r = 1$, as a direct calculation shows that $\frac{n_3(1)}{|M(V)_U|} = q^{-2}$ in this case.

Henceforth assume that $r \geqslant 2$, and hence that $n \geqslant 4$. The summand in (6) with $d = 1$ is greater than

$$q^{-2}(1 - q^{-2} - q^{-3} - q^{-4})^2(1 - 3q^{-1} + 2q^{-2}) \geqslant q^{-2}(1 - 3q^{-1} + 4q^{-3}). \quad (8)$$

It follows from (6) and (8) that

$$\frac{n_3(r)}{|M(V)_U|} \geqslant q^{-2}(1 - 3q^{-1} + 4q^{-3}) \geqslant q^{-2}(1 - 2q^{-1}) \quad (9)$$

holds for $r \geqslant 2$. However, the bound (9) when $r \geqslant 2$ is always smaller than the bound (7) when $r = 1$. Thus (9) gives a uniform lower bound for all r satisfying $0 < r < n$.

Proof of Theorem 1. Recall the notation n_i and $\pi_i = \frac{n_i}{|M(V)_U|}$ used in the 'Proof Strategy' in Section 1. We shall prove $q^{-2}(1 + c_1 q^{-1}) \leqslant \pi \leqslant q^{-2}(1 + c_2 q^{-1})$, where $\pi = \pi_1 + \pi_2 + \pi_3$ equals $\mathrm{Prob}(X \in M(V)_U$ is non-cyclic), and $c_1 = -\frac{4}{3}$ and $c_2 = \frac{35}{3}$. As mentioned previously, we shall assume that $\min(r, n-r) = r$. If $n = 2$, then only the q scalar matrices of the q^3 elements of $M(V)_U$ are non-cyclic. Thus we have $\pi = \pi_3 = q^{-2}$ and the stated bounds $q^{-2}(1 - \frac{4q^{-1}}{3}) \leqslant q^{-2} \leqslant q^{-2}(1 + \frac{35q^{-1}}{3})$ clearly hold. Suppose now that $n \geqslant 3$. Consider the case when $r = 1$. Then the probability π_1 that A is non-cyclic is 0, and $\frac{2q^{-3}}{3} \leqslant \pi_2 \leqslant \frac{8q^{-3}}{3}$ by (1) because $n - r \geqslant 2$. We have shown in Section 2, and above, that

$$q^{-2}(1 - 2q^{-1}) \leqslant \pi_3 \leqslant q^{-2}\left(1 + \frac{58q^{-1}}{9}\right) \quad \text{for } n \geqslant 1. \quad (10)$$

Adding $\pi_1 = 0$ and $\frac{2q^{-3}}{3} \leqslant \pi_2 \leqslant \frac{8q^{-3}}{3}$ and $q^{-2} - 2q^{-3} \leqslant \pi_3 \leqslant q^{-2} + \frac{58q^{-3}}{9}$ gives $q^{-2}(1 - \frac{4q^{-1}}{3}) \leqslant \pi \leqslant q^{-2}(1 + \frac{82q^{-1}}{9})$ when $r = 1$.

Now consider the case when $2 \leqslant r \leqslant n - r$. Then $\frac{1}{12} \leqslant \frac{2q^{-3}}{3} \leqslant \pi_1 \leqslant \frac{8q^{-3}}{3} \leqslant \frac{1}{3}$ holds by (1). However, π_2 equals $1 - \pi_1$ times the probability that B is non-cyclic, and hence

$$\frac{4q^{-3}}{9} \leqslant (1 - \pi_1)\frac{2q^{-3}}{3} \leqslant \pi_2 \leqslant (1 - \pi_1)\frac{8q^{-3}}{3} \leqslant \frac{88q^{-3}}{36}.$$

Adding $\frac{2q^{-3}}{3} \leqslant \pi_1 \leqslant \frac{8q^{-3}}{3}$ and $\frac{4q^{-3}}{9} \leqslant \pi_2 \leqslant \frac{88q^{-3}}{36}$ to the bounds (10) for π_3 gives

$$q^{-2}\left(1 - \frac{8q^{-1}}{9}\right) \leqslant \pi_1 + \pi_2 + \pi_3 \leqslant q^{-2}\left(1 + \frac{104q^{-1}}{9}\right) \quad \text{for } r \geqslant 2.$$

The constants $c_1 = -\frac{4}{3}$ and $c_2 = \frac{35}{3}$ suffice as $-\frac{4}{3} < -\frac{8}{9}$ and $\frac{82}{9} < \frac{104}{9} < \frac{35}{3}$. $\quad \square$

Acknowledgments

References

[B]   S. Brown, Finite reducible matrix algebras, PhD Thesis, The University of Western Australia, Perth, Australia, 2006, available at: http://theses.library.uwa.edu.au/adt-WU2006.0079/.
[BGP] S. Brown, M. Giudici, C.E. Praeger, Proportions of cyclic matrices in maximal reducible matrix groups and algebras, unpublished manuscript, 2009, available at: arXiv:1105.4078v1.
[F]   J. Fulman, Finite affine groups: cycle indices, Hall–Littlewood polynomials, and probabilistic algorithms, J. Algebra 250 (2002) 731–756.
[HR]   D.F. Holt, S. Rees, Testing modules for irreducibility, J. Austral. Math. Soc. Ser. A 57 (1994) 1–16.
[M]   K.E. Morrison, Random polynomials over finite fields, preprint, http://www.calpoly.edu/~kmorriso/Research/RPFF.pdf, 1999.
[NP1] P.M. Neumann, C.E. Praeger, Cyclic matrices over finite fields, J. Lond. Math. Soc. 52 (1995) 263–264.
[NP2] P.M. Neumann, C.E. Praeger, Cyclic matrices and the Meataxe, in: Groups and Computation, III, Columbus, OH, 1999, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 291–300.
[P]   R.A. Parker, The computer calculation of modular characters (the meat axe), in: M.D. Atkinson (Ed.), Computational Group Theory, Proc. London Math. Soc. Symposium on Computational Group Theory, Durham, 1982, Academic Press, 1984, pp. 267–274.
[W]   Wolfram Research Inc., Mathematica, version 5.0, Champagne, Illinois, 2003.