LMS J. Comput. Math. 18 (1) (2015) 404–418
doi:10.1112/S146115701500008X

Nilpotent-independent sets and estimation in matrix algebras

Brian P. Corr, Tomasz Popiel and Cheryl E. Praeger

Abstract

Efficient methods for computing with matrices over finite fields often involve *randomised* algorithms, where matrices with a certain property are sought via repeated random selection. Complexity analyses for such algorithms require knowledge of the proportion of relevant matrices in the ambient group or algebra. We introduce a method for estimating proportions of families N of elements in the algebra of all $d \times d$ matrices over a field of order q, where membership of a matrix in N depends only on its 'invertible part'. The method is based on the availability of estimates for proportions of certain non-singular matrices depending on N, so that existing estimation techniques for non-singular matrices can be used to deal with families containing singular matrices. As an application, we investigate primary cyclic matrices, which are used in the Holt–Rees `MEATAXE` algorithm for testing irreducibility of matrix algebras.

1. *Introduction*

Randomised algorithms for groups and algebras of matrices typically rely on a randomised search for certain 'desirable' matrices: the correctness of the algorithm is justified by a theoretical result which says that if a certain kind of matrix can be found, then the question being considered can be resolved. Complexity analyses of such algorithms therefore depend on estimating the number of desirable elements in the given group or algebra.

The 'quokka theory' of Niemeyer and Praeger [**23**] is a method for estimating the cardinality of subsets Q of finite simple groups of Lie type such that Q is a union of conjugacy classes and membership of Q depends only on the semisimple part of the Jordan decomposition of an element. This technique was first used by Lehrer [**12**, **13**] to study representations of finite Lie-type groups and has recently proven useful for several estimation problems [**14**, **20**, **21**]. In this paper, we extend the quokka theory in a certain sense to the full matrix algebra $M = \mathrm{M}(d, q)$. By analogy, we deal with subsets N of M for which inclusion depends only on the *invertible part* of the matrix, and not on the *nilpotent part*, as defined in § 1.1. We call such sets *nilpotent-independent*. The technique itself involves estimating the cardinality of certain subsets N_i of $\mathrm{GL}(i, q)$, $1 \leqslant i \leqslant d$, related to N, and therefore allows one to utilise existing methods (such as quokka theory) that apply only to non-singular matrices in order to treat families containing singular matrices. This research forms part of the first author's PhD thesis [**2**, Chapter 6].

Our formula for estimating the size of a nilpotent-independent set is given in § 1.1 (Theorem 1.3). We also give an application to primary cyclic matrices (Theorem 1.4), the significance of which is discussed in § 1.2. Further examples of nilpotent-independent sets are discussed in § 1.3. The proofs of Theorems 1.3 and 1.4 are given in §§ 2 and 3, respectively.

Received 7 May 2014; revised 4 February 2015.

2010 Mathematics Subject Classification 20P05 (primary).

This paper forms part of the first author's PhD thesis. The first author was supported by an Australian Postgraduate Award, a UWA Top-Up Scholarship and, during the writing of the paper, an Australian Mathematical Society Lift-Off Fellowship. The research forms part of Australian Research Council Discovery Project DP140100416.

1.1. *Definitions and main results*

Let $V = \mathbb{F}_q^d$ be the d-dimensional space of row vectors over the field $\mathbb{F}_q$, and let $\mathrm{M}(V) = \mathrm{M}(d, q)$ be the algebra of linear transformations of V. Our main theorem relates the size of a subset N of $\mathrm{M}(V)$ satisfying certain properties to the sizes of certain subsets N_i of $\mathrm{GL}(i, q)$, $1 \leqslant i \leqslant d$, that are determined by N together with a fixed maximal flag of V (see Definition 1.2). Each $X \in \mathrm{M}(V)$ determines a unique decomposition

$$V = V_{\mathrm{inv}}(X) \oplus V_{\mathrm{nil}}(X)$$

such that $X_{\mathrm{inv}} := X|_{V_{\mathrm{inv}}(X)}$ is invertible and $X_{\mathrm{nil}} := X|_{V_{\mathrm{nil}}(X)}$ is nilpotent. We call X_{inv} the *invertible part* and X_{nil} the *nilpotent part* of X and, by abuse of notation, we write $X = X_{\mathrm{inv}} \oplus X_{\mathrm{nil}}$. In the language of primary decompositions [9], $V_{\mathrm{nil}}(X)$ is precisely the t-primary component of V and $V_{\mathrm{inv}}(X)$ is the direct sum of all the other primary components; that is, $V_{\mathrm{inv}}(X) = \bigoplus_{f \in \mathrm{Irr}(q), f \neq t} V_f(X)$, where $\mathrm{Irr}(q)$ is the set of monic irreducible polynomials in $\mathbb{F}_q[t]$.

Definition 1.1. A subset N of $\mathrm{M}(V)$ is called a *nilpotent-independent* (NI) subset if the following conditions hold:

(i) N is closed under conjugation by elements of $\mathrm{GL}(V)$; and
(ii) for $X \in \mathrm{M}(V)$, we have $X \in N$ if and only if $X_{\mathrm{inv}} \oplus 0_{V_{\mathrm{nil}}(X)} \in N$, where $0_{V_{\mathrm{nil}}(X)}$ is the zero transformation on $V_{\mathrm{nil}}(X)$.

Thus, membership of an NI subset depends only on the invertible part of $X \in \mathrm{M}(V)$ and is independent of the nilpotent part. In particular, unions of conjugacy classes of $\mathrm{GL}(V)$ are NI subsets: for a non-singular matrix X, $X_{\mathrm{nil}} = 0$ and hence condition (ii) above holds vacuously for all families of non-singular matrices. Hence, in particular, all quokka subsets of $\mathrm{GL}(V)$ are NI subsets (see § 3.2).

Definition 1.2. A *maximal flag* of V is a family of subspaces $V_1, \ldots, V_d$ such that $\{0\} = V_0 \subset V_1 \subset \ldots \subset V_d = V$. Note that $\dim V_i = i$ for $0 \leqslant i \leqslant d$. Given a maximal flag $\{V_i\}$ and an NI subset N, we write, for each i,

$$N(i) = \{X \in N \mid \dim(V_{\mathrm{inv}}(X)) = i\},$$
$$N_i = \{Y \in \mathrm{GL}(V_i) \mid Y = X_{\mathrm{inv}} \text{ for some } X \in N \text{ such that } V_{\mathrm{inv}}(X) = V_i\}.$$

The set $\{N_i \mid 0 \leqslant i \leqslant d\}$ is called the *invertible family corresponding to* N *and* $\{V_i\}$.

Note that, since N is closed under conjugation, the $N(i)$ do not depend on the maximal flag $\{V_i\}$ (but the N_i do depend on $\{V_i\}$).

We are interested in NI subsets that contain non-invertible elements. Each such set determines (up to conjugacy in $\mathrm{GL}(V)$) a collection of sets of invertible elements in smaller dimensions, namely the N_i above. In § 1.1, we derive the following precise relationship between the size of N and the sizes of the N_i, thus reducing the enumeration problem in $\mathrm{M}(d, q)$ to a set of enumeration problems in $\mathrm{GL}(i, q)$ for $0 \leqslant i \leqslant d$.

Theorem 1.3. *Let* $\{V_i \mid 0 \leqslant i \leqslant d\}$ *be a maximal flag of* $V = \mathbb{F}_q^d$ *and let* N *be an NI subset of* $\mathrm{M}(V)$. *Then each* N_i *as in Definition* 1.2 *is a union of conjugacy classes of* $\mathrm{GL}(V_i)$, *the family* $\{N_i \mid 0 \leqslant i \leqslant d\}$ *is unique and*

$$\frac{|N|}{|\mathrm{M}(V)|} = \omega(d, q) \sum_{i=0}^{d} \frac{q^{-(d-i)}}{\omega(d-i, q)} \frac{|N_i|}{|\mathrm{GL}(V_i)|}, \tag{1}$$

where $\omega(0, q) = 1$ *and* $\omega(j, q) = \prod_{k=1}^{j}(1 - q^{-k}) = |\mathrm{GL}(j, q)|/|\mathrm{M}(j, q)|$, $j \geqslant 1$.

https://doi.org/10.1112/S1461157015000008X Published online by Cambridge University Press

The following formula is equivalent to (1):

$$\frac{|N|}{|\mathrm{GL}(V)|} = \sum_{i=0}^{d} \frac{q^{-(d-i)}}{\omega(d-i,q)} \frac{|N_i|}{|\mathrm{GL}(V_i)|}. \tag{2}$$

A matrix in $\mathrm{M}(d,q)$ is *primary cyclic* if there exists a monic irreducible polynomial $f \in \mathbb{F}_q[t]$ such that the multiplicities of f in the characteristic and minimal polynomials of X are equal (and at least 1). In § 3, we apply Theorem 1.3 to obtain a lower bound on the proportion of matrices in $\mathrm{M}(V) = \mathrm{M}(c, q^b)$ that are primary cyclic when viewed as elements of a larger, ambient matrix algebra $\mathrm{M}(bc, q)$ which contains $\mathrm{M}(c, q^b)$ as an irreducible (but not absolutely irreducible) subalgebra. Specifically, we prove the following result.

THEOREM 1.4. *Let $b, c \geqslant 2$ be integers and let $N = N(c, q, b)$ be the set of matrices X in $\mathrm{M}(c, q^b) \subseteq \mathrm{M}(bc, q)$ that are primary cyclic with respect to some irreducible polynomial $f(t) \neq t$ of degree greater than $\dim(V_{\mathrm{inv}}(X))/2$. Then*

$$\frac{|N|}{|\mathrm{M}(c, q^b)|} > \log 2 - \frac{\log 2 + 3}{c} - \frac{2(1 - 1/c)}{q^{b/2}}.$$

REMARK 1.5. The set N in Theorem 1.4 contains the set P of so-called *primitive prime divisor* elements of $\mathrm{GL}(c, q^b)$, namely non-singular matrices X with order divisible by a prime that divides $q^{bi} - 1$ for some $i > c/2$ but does not divide $q^j - 1$ for any $j < bi$. The proportion $|P|/|\mathrm{GL}(c, q^b)|$ is approximately $\log 2$ [**22**, Theorem 6.1], and it seems reasonable that $|N|/|\mathrm{M}(c, q^b)|$ should also be roughly $\log 2$. Theorem 1.4 shows that this is the case for even modest values of b, q.

1.2. *Irreducibility testing and the* `MEATAXE`

Primary cyclic matrices are used in the Holt–Rees `MEATAXE` algorithm [**10**] for testing irreducibility of matrix algebras. The original ideas behind this test are due to Simon Norton, and the basic Norton irreducibility test was first presented in Richard Parker's paper [**25**] without an analysis of its complexity or effectiveness. This version of the algorithm seeks by random selection from an algebra M a special type of primary cyclic matrix, namely one whose characteristic polynomial has a multiplicity-1 linear factor. If such a matrix is found, then the algorithm is guaranteed either to determine that M is irreducible or to return a proper non-trivial invariant subspace in the natural or dual module for M.

Holt and Rees [**10**] generalised this algorithm, and gave an analysis of the `MEATAXE`. For the Holt–Rees `MEATAXE`, arbitrary primary cyclic matrices are used for the Norton irreducibility test. However, in their analysis in [**10**, p. 7], Holt and Rees used only a constant lower bound for the density of a certain subfamily of primary cyclic matrices in a full matrix algebra, namely the subfamily used by Parker [**25**]. Ivanyos and Lux [**11**, Lemma 2.2] extended the analysis of Holt and Rees to obtain the same result for all irreducible matrix algebras and showed that, for a reducible matrix algebra M, again a constant fraction of the elements can be used to prove that M is reducible.

For the case where M is a full matrix algebra $\mathrm{M}(V)$, the constant lower bound given by Holt and Rees [**10**] was improved upon by Glasby and Praeger [**8**]. For the case where M is a proper irreducible subalgebra of $\mathrm{M}(V)$, namely the case considered in this paper, Theorem 1.4 gives an explicit lower bound for the proportion of matrices that are primary cyclic with respect to a polynomial of 'large' degree. By contrast, the first and third authors [**3**] have previously determined a lower bound on the proportion of matrices that are primary cyclic with respect to an irreducible polynomial of smallest possible degree.

https://doi.org/10.1112/S146115701500008X Published online by Cambridge University Press

Neumann and Praeger [16, § 5] proposed a modification of the Norton irreducibility test, called the cyclic irreducibility test, in which the elements sought by random selection are cyclic matrices. The proportion of cyclic matrices in $\mathrm{M}(d,q)$ is at least $1-1/((q^2-1)(q-1))$ [15, Theorem 4.1] (see also [26]), and their proportion in a proper irreducible matrix algebra $\mathrm{M}(c,q^b)$ (where $d=bc$, $b>1$) is at least $1-q^{-1}$ if $b\geqslant 3$, and at least $1-q^{-1}-2q^{-2}$ if $b=2$ [15, Theorem 5.5]. These lower bounds are, in particular, lower bounds for the proportion of primary cyclic matrices in such algebras, since cyclic matrices are primary cyclic relative to any of their primary components. Glasby and Praeger [8, Theorem 1] proved that there is a constant a such that the proportion of primary cyclic matrices in $\mathrm{M}(d,q)$ is greater than $1-a^{-d}$. That is to say, the proportion approaches 1 exponentially quickly as $d\to\infty$. Thus, there are considerably more primary cyclic matrices than cyclic matrices in $\mathrm{M}(d,q)$. However, it is not known whether the same is true in a proper irreducible subalgebra $\mathrm{M}(c,q^b)$.

In § 2, we use our theory of NI sets to obtain an estimate for the proportion of a certain subfamily of primary cyclic matrices in $\mathrm{M}(c,q^b)$ (and, as mentioned above, in [11] and [3] bounds are obtained for different subfamilies of such matrices). It would be interesting to know, for example, whether the proportion of primary cyclic matrices in $\mathrm{M}(c,q^b)$ is indeed asymptotically larger than the bounds obtained by Neumann and Praeger. In particular, does the proportion of primary cyclic matrices approach 1 as $c\to\infty$?

For further discussion of primary cyclic matrices and their significance to the Holt–Rees `MEATAXE` algorithm, we refer the reader to Glasby [7] and Corr and Praeger [3].

1.3. *Further examples of NI sets*

Here we briefly discuss some other examples of useful and interesting sets of matrices that are nilpotent-independent. We describe three broad classes, and give examples that are well studied and practically useful.

The first class consists of subsets of matrices in $\mathrm{M}(d,q)$ determined by properties of their characteristic polynomials. There are well-known examples, such as unipotent matrices (that is, matrices with characteristic polynomial $c(t)=(t-1)^d$, see [5]) or separable matrices ($c(t)$ multiplicity free). There are also less well-known examples. Niemeyer *et al.* [19] studied matrices that induce an irreducible action on a subspace of dimension greater than $d/2$, while Niemeyer and the third author [24, § 3] introduced the family where $c(t)$ has an irreducible degree-k factor and no other factor of $c(t)$ has degree divisible by k. Matrices in the latter family play a role in new recognition algorithms for classical groups in arbitrary characteristic, since they power up to matrices acting irreducibly on a k-space and fixing a complementary $(d-k)$-space pointwise (see [4, 17, 18]). The family of matrices considered in Theorem 1.4 generalises that studied in [19]. Note that the dimension of our $V_{\mathrm{nil}}(X)$ is the multiplicity of t dividing $c_X(t)$. We study the family of matrices X in a proper irreducible subalgebra $\mathrm{M}(c,q^b)$ of $\mathrm{M}(d,q)$ for which some irreducible factor f of $c_X(t)$ (over $\mathbb{F}_q$) has degree greater than $(d-\dim V_{\mathrm{nil}}(X))/2$.

A second class of NI sets are subsets of matrices in $\mathrm{M}(d,q)$ determined by properties of their actions on the space $V(d,q)$. Often this is described by some property of the minimal polynomial, or combined properties of the characteristic and minimal polynomials. Examples include cyclic matrices, regular matrices and semisimple matrices (estimates for which are found for classical groups in [5, 15, 26]), primary cyclic matrices, nilpotent matrices and p-abundant matrices in classical groups [21]. Note that some of these example classes are contained in $\mathrm{GL}(d,q)$.

A third class of NI sets are those determined by the order of the invertible part X_{inv} of their members. Examples include primitive prime divisor elements (see Remark 1.5) and Singer cycles, involutions or sets which induce such elements on V_{inv}. This class also contains the set of matrices for which V_{inv} is the identity (that is, for which all vectors in v are either fixed or 'eventually killed' by X).

https://doi.org/10.1112/S146115701500008X Published online by Cambridge University Press

2. *Nilpotent-independent subsets*

In this section, we prove Theorem 1.3 and deduce some corollaries that give bounds on the cardinality of N under certain generic assumptions.

2.1. *Proof of Theorem 1.3*

We begin with a lemma about the structural relationship between the sets $N(i)$ and N_i in Definition 1.2. As before, let $V = \mathbb{F}_q^d$.

LEMMA 2.1. *Let N be an NI subset of $\mathrm{M}(V)$, let $\{V_i \mid 0 \leqslant i \leqslant d\}$ be a maximal flag of V and, for $0 \leqslant i \leqslant d$, define $N_i, N(i)$ as in Definition 1.2. Then the following hold.*

(i) *For each i, N_i is closed under $\mathrm{GL}(V_i)$-conjugacy.*
(ii) *The set $N_0 \subseteq \mathrm{GL}(V_0)$ is empty if N contains no nilpotent elements, and has size 1 otherwise.*
(iii) *For a maximal flag $\{V_i' \mid 0 \leqslant i \leqslant d\}$ with corresponding invertible family $\{N_i' \mid 0 \leqslant i \leqslant d\}$, there exists $g \in \mathrm{GL}(V)$ such that, for each i, $V_i^g = V_i'$ and $N_i^g = N_i'$.*
(iv) *For each i, $|N(i)| = \begin{bmatrix} d \\ i \end{bmatrix}_q q^{(d-i)(d-1)}|N_i|$, where*

$$\begin{bmatrix} d \\ i \end{bmatrix}_q = \frac{|\mathrm{GL}(d,q)|}{|\mathrm{GL}(i,q)||\mathrm{GL}(d-i,q)|} q^{-i(d-i)}$$

is the q-binomial coefficient, namely the number of i-dimensional subspaces of V.

Proof. (i) If N_i is empty, then there is nothing to prove, so suppose that N_i is non-empty and let $X_i \in N_i$. Then there exists $X \in N$ with $V_{\mathrm{inv}}(X) = V_i$, $X_{\mathrm{inv}} = X_i$ and $X_{\mathrm{nil}} = 0_{V_{\mathrm{nil}}(X)}$. Now let $x \in \mathrm{GL}(V_i)$. Then $x' = x \oplus I_{V_{\mathrm{nil}}(X)} \in \mathrm{GL}(V)$, where $I_{V_{\mathrm{nil}}(X)}$ is the identity map on $V_{\mathrm{nil}}(X)$. Since N is closed under conjugacy, $X^{x'} = X_i^x \oplus 0_{V_{\mathrm{nil}}(X)} \in N$. Hence, $(X^{x'})_{\mathrm{inv}} = X_i^x$ is the invertible part of the element $X^{x'}$ of N and it lies in $\mathrm{GL}(V_i)$, so $X_i^x \in N_i$. Thus, N_i is closed under conjugacy.

(ii) If N contains no nilpotent elements, then there is no $X \in N$ with $\dim V_{\mathrm{inv}}(X) = 0$ and hence N_0 is empty. If N contains a nilpotent element X, then $V_{\mathrm{inv}}(X) = \{0\} = V_0$ and X_{inv}, the identity map on V_0, lies in N_0.

(iii) Let $\{v_i \mid 1 \leqslant i \leqslant d\}, \{v_i' \mid 1 \leqslant i \leqslant d\}$ be bases for V such that, for $1 \leqslant i \leqslant d$, the sets $\{v_j \mid 1 \leqslant j \leqslant i\}, \{v_j' \mid 1 \leqslant j \leqslant i\}$ are bases for V_i, V_i', respectively. Then the transformation $g \in \mathrm{GL}(V)$ defined by $v_i^g = v_i'$, $1 \leqslant i \leqslant d$, and extended by linearity to V has the desired properties.

(iv) Write $N(V_i) = \{X \in N \mid V_{\mathrm{inv}}(X) = V_i\}$. Let $X_i \in N_i$. Then, for every complement U of V_i in V, and for every nilpotent $n \in \mathrm{M}(U)$, we have $X_i \oplus n \in N(V_i)$. Moreover, each different choice of U, n yields a different element of $N(V_i)$, and all of $N(V_i)$ arises in this way. Thus, the size of $N(V_i)$ is precisely $|N_i|$ times the number $q^{i(d-i)}$ of complements U, times the number $q^{(d-i)(d-i-1)}$ of nilpotent elements in $\mathrm{M}(U)$ [6]. The set $N(i)$ is the disjoint union of $N(V_i')$ over all i-dimensional subspaces V_i' of V. By (ii) and (iii), all of the $N(V_i')$ have the same size $|N(V_i)|$ and so $|N(i)|$ is equal to $|N(V_i)|$ times the number of i-dimensional subspaces of V. The result follows. □

Let us now prove Theorem 1.3. Recall that we want to show that (1) holds, namely that

$$\frac{|N|}{|\mathrm{M}(V)|} = \omega(d,q) \sum_{i=0}^{d} \frac{q^{-(d-i)}}{\omega(d-i,q)} \frac{|N_i|}{|\mathrm{GL}(V_i)|}.$$

https://doi.org/10.1112/S1461157015000008X Published online by Cambridge University Press

Proof of Theorem 1.3. The first assertions of the theorem are proved in Lemma 2.1. It remains to prove (1). Note that $|\mathrm{GL}(d-i,q)| = q^{(d-i)^2}\omega(d-i,q)$ for all i. Lemma 2.1 gives

$$\begin{aligned}\frac{|N(i)|}{|\mathrm{M}(d,q)|} &= \frac{1}{|\mathrm{M}(d,q)|}\begin{bmatrix} d \\ i \end{bmatrix}_q q^{(d-i)(d-1)}|N_i| \\ &= \frac{1}{|\mathrm{M}(d,q)|}\left(\frac{|\mathrm{GL}(d,q)|}{|\mathrm{GL}(i,q)||\mathrm{GL}(d-i,q)|}q^{-i(d-i)}\right)q^{(d-i)(d-1)}|N_i| \\ &= \frac{|\mathrm{GL}(d,q)|}{|\mathrm{M}(d,q)|}.\frac{q^{(d-i)(d-i-1)}}{|\mathrm{GL}(d-i,q)|}.\frac{|N_i|}{|\mathrm{GL}(i,q)|} \\ &= \omega(d,q).\frac{q^{-(d-i)}}{\omega(d-i,q)}.\frac{|N_i|}{|\mathrm{GL}(i,q)|}.\end{aligned}$$

Since the $N(i)$ partition N, $|N| = \sum_{1\leqslant i\leqslant d}|N(i)|$ and the result follows. □

It is unusual when enumerating sets in $\mathrm{GL}(V)$ to consider 0-dimensional cases, but the 0th term of the sum in (1) is well behaved, as follows.

Remark 2.2. By definition, an NI subset N of $\mathrm{M}(V)$ must contain either all nilpotent elements of $\mathrm{M}(V)$, or none. In the former case, the 0th term of the sum in (1) is

$$\frac{q^{-d}}{\omega(d,q)} = q^{-d}\frac{|\mathrm{M}(V)|}{|\mathrm{GL}(V)|}.$$

In the latter case, the 0th term is 0.

2.2. *Some generic lower bounds for* $|N|$

If we can estimate each proportion $|N_i|/|\mathrm{GL}(i,q)|$ in terms of i and q, then we can use (1) to estimate the proportion $|N|/|\mathrm{M}(d,q)|$. In this way, estimation techniques that are normally effective only in $\mathrm{GL}(d,q)$ (for example, quokka theory) can be used to deal with subsets of $\mathrm{M}(d,q)$. If we can find bounds on the $|N_i|/|\mathrm{GL}(i,q)|$ that behave 'uniformly' in some sense, for example as in Proposition 2.4 or Proposition 2.6, then (1) can be applied without much additional effort. We first prove a useful formula by considering the case $N = \mathrm{M}(d,q)$.

Corollary 2.3. *For any prime power q and any positive integer d,*

$$\sum_{i=0}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)} = \sum_{i=0}^{d}\frac{q^{-i}}{\omega(i,q)} = \frac{1}{\omega(d,q)}. \tag{3}$$

Equivalently,

$$\sum_{i=1}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)} = \sum_{i=0}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)} - \frac{q^{-d}}{\omega(d,q)} = \frac{1-q^{-d}}{\omega(d,q)}. \tag{4}$$

Proof. The first equality in (3) is just a change of variable. Now consider $N = \mathrm{M}(d,q)$. Then N is an NI subset and, for every i, $N_i = \mathrm{GL}(i,q)$. By (2),

$$\frac{|N|}{|\mathrm{GL}(d,q)|} = \sum_{i=0}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)}\cdot 1$$

and so the left-hand side of (3) is equal to $|\mathrm{M}(d,q)|/|\mathrm{GL}(d,q)|$, which is $1/\omega(d,q)$. □

https://doi.org/10.1112/S146115701500008X Published online by Cambridge University Press

PROPOSITION 2.4. *Let d be a positive integer, N an NI subset of $\mathrm{M}(V)$ and $\{N_i\}$ a corresponding invertible family. Suppose that there exist constants $a, k > 0$ such that $|N_i|/|\mathrm{GL}(i,q)| \geqslant a - kq^{-i}$ for $1 \leqslant i \leqslant d$. Then*

$$\frac{|N|}{|\mathrm{M}(d,q)|} \geqslant a - (a+k)dq^{-d} \geqslant a - (a+k)\left(\frac{2q}{3}\right)^{-d}.$$

Proof. Applying (2) and (4),

$$\begin{aligned}\frac{|N|}{|\mathrm{M}(d,q)|} &= \omega(d,q)\frac{|N|}{|\mathrm{GL}(d,q)|} = \omega(d,q)\left(\sum_{i=0}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)}.\frac{|N_i|}{|\mathrm{GL}(V_i)|}\right)\\ &\geqslant \omega(d,q)\left(0 + \sum_{i=1}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)}.(a - kq^{-i})\right)\\ &= a\omega(d,q)\sum_{i=1}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)} - k\omega(d,q)q^{-d}\sum_{i=1}^{d}\frac{1}{\omega(d-i,q)}\end{aligned}$$

and, using (4), this is equal to $a(1-q^{-d}) - k\omega(d,q)q^{-d}\sum_{i=1}^{d} 1/\omega(d-i,q)$. Noting that $\omega(d-i,q) \geqslant \omega(d-1,q) = \omega(d,q)/(1-q^{-d})$ for $1 \leqslant i \leqslant d$, this is at least $a(1-q^{-d}) - k(1-q^{-d})dq^{-d} \geqslant a - (k+a)dq^{-d}$. Since $d < (3/2)^d$ for all integer values of d,

$$(a+k)dq^{-d} < (a+k)\left(\frac{3}{2}\right)^{d}q^{-d} = (a+k)\left(\frac{2q}{3}\right)^{-d},$$

and the second asserted inequality follows. □

A similar result holds when we have slower convergence to the limiting proportion. We need the following lemma, which is easily verified.

LEMMA 2.5. *For all $d \geqslant 1$ and $q \geqslant 2$,*

$$d\sum_{i=1}^{d}\frac{q^i}{i} < 3q^d.$$

PROPOSITION 2.6. *Let d be a positive integer, N an NI subset of $\mathrm{M}(V)$ and $\{N_i\}$ a corresponding invertible family. Suppose that $|N_i|/|\mathrm{GL}(i,q)| \geqslant a - k/i$ for $1 \leqslant i \leqslant d$ for some $a, k > 0$. Then*

$$\frac{|N|}{|\mathrm{M}(d,q)|} \geqslant \left(a - \frac{3k}{d}\right)(1-q^{-d}) > a - \frac{a+3k}{d}.$$

Proof. Applying (2) and using the assumed bounds and the fact that $|N_0| \geqslant 0$,

$$\begin{aligned}\frac{|N|}{|\mathrm{M}(d,q)|} &\geqslant \omega(d,q)\sum_{i=1}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)}\left(a - \frac{k}{i}\right)\\ &= a\omega(d,q)\sum_{i=1}^{d}\frac{q^{-(d-i)}}{\omega(d-i,q)} - k\omega(d,q)\sum_{i=1}^{d}\frac{q^{-(d-i)}}{i\omega(d-i,q)}\\ &= a(1-q^{-d}) - k\omega(d,q)q^{-d}\sum_{i=1}^{d}\frac{q^i}{i\omega(d-i,q)},\end{aligned}$$

https://doi.org/10.1112/S1461157015000008X Published online by Cambridge University Press

where we use (4) for the last equality. As $\omega(d-i,q) \geqslant \omega(d-1,q)$ for every i considered,

$$\frac{|N|}{|\mathrm{M}(d,q)|} \geqslant a(1-q^{-d}) - k(1-q^{-d})q^{-d}\sum_{i=1}^{d}\frac{q^i}{i},$$

which, by Lemma 2.5, is greater than $a(1-q^{-d}) - k(1-q^{-d})q^{-d}\cdot 3q^d/d = (a-3k/d)(1-q^{-d})$. The result follows, since $d < q^d$ for all $d \geqslant 1$, giving

$$\left(a-\frac{3k}{d}\right)(1-q^{-d}) > a - \frac{3k}{d} - \frac{a}{q^d} > a - \frac{3k}{d} - \frac{a}{d}. \qquad \square$$

3. *An application to primary cyclic matrices*

Recall again that a matrix $X \in \mathrm{M}(n,q)$ is said to be *primary cyclic* if there exists a monic irreducible polynomial $f \in \mathbb{F}_q[t]$ such that the multiplicities of f in the characteristic polynomial $c_{X,V(n,q)}(t)$ and the minimal polynomial $m_{X,V(n,q)}(t)$ are equal and at least 1. Here we use the notation $c_{X,V(n,q)}(t), m_{X,V(n,q)}(t)$ to denote the characteristic and minimal polynomials of X *in its action on* $V(n,q)$: this is necessitated by our consideration of actions over different fields. This is equivalent to the requirement that the action of X on its f-primary component is cyclic.

In this section, we use quokka theory to determine lower bounds on the proportion of primary cyclic matrices in a subgroup $\mathrm{GL}(c,q^b)$ of $\mathrm{GL}(bc,q)$, and apply our theory of NI subsets to obtain a lower bound on the proportion of primary cyclic matrices in an irreducible subalgebra $\mathrm{M}(c,q^b)$ of $\mathrm{M}(bc,q)$.

3.1. *Primary cyclic matrices in* $\mathrm{M}(c,q^b)$

Note that $\mathbb{F}_{q^b}$ has the structure of an F-vector space $V(b,q)$ with basis $\{\lambda_1 = 1,\dots,\lambda_b\}$, say. If $\{v_1,\dots,v_c\}$ is a basis for the $\mathbb{F}_{q^b}$-vector space $V(c,q^b)$, then $\{\lambda_i v_i \mid i = 1,\dots,b, j = 1,\dots,c\}$ is a basis for V regarded as an $\mathbb{F}_q$-vector space. In this way, $\mathrm{M}(c,q^b) \subseteq \mathrm{M}(bc,q)$, and each $X \in \mathrm{M}(c,q^b)$ can be regarded both as a matrix over $K = \mathbb{F}_{q^b}$ and as a matrix over $F = \mathbb{F}_q$.

A key result is Proposition 3.1, proved in [**3**], which gives necessary and sufficient conditions for a matrix $X \in \mathrm{M}(c,q^b)$ to be primary cyclic when viewed as an element of the larger algebra $\mathrm{M}(bc,q)$ (that is, for $X_{bc,q}$ to be primary cyclic). This characterisation involves the Galois group $\mathrm{Gal}(K/F)$ of automorphisms of K fixing F pointwise. As before, $\mathrm{Irr}(q)$ denotes the set of monic irreducible polynomials in $F[t]$, and $\mathrm{Irr}_m(q)$ denotes the subset of degree-m polynomials in $\mathrm{Irr}(q)$.

PROPOSITION 3.1. *Let $f \in \mathrm{Irr}(q)$ and $X \in \mathrm{M}(c,q^b)$ be such that f divides $c_{X,V(bc,q)}(t)$. Then $X_{bc,q}$ is f-primary cyclic if and only if b divides $\deg(f)$ and the following hold for some divisor $g \in K[t]$ of f of degree $\deg(f)/b$:*

(1) *X_{c,q^b} is g-primary cyclic; and*
(2) *for every non-trivial $\tau \in \mathrm{Gal}(K/F)$, the image $g^\tau \neq g$ and g^τ does not divide $c_{X,V(c,q^b)}(t)$.*

The following lemma gives a relationship between elements of $\mathrm{Irr}_{br}(q)$ and $\mathrm{Irr}_r(q^b)$.

LEMMA 3.2. *Let $r > 1$. Then each $f \in \mathrm{Irr}_{br}(q)$ is a product $\prod_{\tau\in\mathrm{Gal}(K/F)} g^\tau$, where $g \in \mathrm{Irr}_r(q^b)$ is such that $g^\tau \neq g$ for all non-trivial $\tau \in \mathrm{Gal}(K/F)$. In particular, the number of $g \in \mathrm{Irr}_r(q^b)$ with this property is $r|\mathrm{Irr}_{br}(q)|$.*

https://doi.org/10.1112/S1461157015000008X Published online by Cambridge University Press

Proof. Write $L = \mathbb{F}_{q^{br}}$. Then each $f \in \mathrm{Irr}_{br}(q)$ is of the form

$$f(t) = \prod_{i=0}^{br-1} (t - \lambda^{q^i}) \quad \text{for some } \lambda \in L.$$

For each $j \in \{1, \dots, b\}$, define

$$g_j(t) = \prod_{i=0}^{r} (t - \lambda^{q^{(i-1)b+j}}).$$

Denote by σ the automorphism of L that raises elements to their qth power. Then, for $1 \leqslant j \leqslant b-1$, we have $g_j^\sigma = g_{j+1}$ and $g_b^\sigma = g_1$. It follows that, for each j, $g_j^{\sigma^b} = g_j$ and hence $g_j \in K[t]$. Moreover, for f to be irreducible we require both that the g_j should be irreducible and that they should be pairwise distinct. Note that $\mathrm{Gal}(K/F)$ consists of the restrictions $\sigma^i|_K$ for $0 \leqslant i < b$ (since $\sigma^b|_K = 1$). Thus, each $f \in \mathrm{Irr}_{br}(q)$ gives rise to exactly b monic irreducible divisors $g \in K[t]$ satisfying the condition that $g^\tau \neq g$ for $1 \neq \tau \in \mathrm{Gal}(K/F)$. Moreover, for any g satisfying this condition, we have $\prod_{\tau \in \mathrm{Gal}(K/F)} g^\tau \in \mathrm{Irr}_{br}(q)$ and so there is a bijection between $\mathrm{Gal}(K/F)$-orbits of length b of irreducible polynomials of degree r over K and irreducible polynomials f of degree br over F. □

The following sets will be useful in our application of the theory of NI sets to f-primary cyclic matrices.

Definition 3.3. For $r, b, c \in \mathbb{Z}^+$, q a prime power and $f \in \mathrm{Irr}(q)$, define

$$N(c, q, b; f) := \{X \in \mathrm{GL}(c, q^b) \mid X_{bc,q} \text{ is } f\text{-primary cyclic}\},$$
$$N(c, q, b, r) := \bigcup_{f \in \mathrm{Irr}_{br}(q)} N(c, q, b; f),$$
$$N := N(c, q, b) = \bigcup_{r > c/2} N(c, q, b, r).$$

Note that if $b = 1$, then $N(c, q, 1; f)$ is the set of f-primary cyclic matrices in $\mathrm{M}(c, q)$.

Suppose that $f \in \mathrm{Irr}_{br}(q)$ with $r > c/2$, and that f divides $c_{X,V(bc,q)}(t)$. Since $r > c/2$, f is the only degree-br divisor of $c_{X,V(bc,q)}(t)$. Suppose also that $g \in \mathrm{Irr}_r(q^b)$ divides f and $c_{X,V(c,q^b)}(t)$. Then, again since $r > c/2$, no $g^\tau \neq g$ (for $\tau \in \mathrm{Gal}(K/F)$) can divide $c_{X,V(c,q^b)}(t)$. Thus:

(a) X_{c,q^b} is g-primary cyclic if and only if $X_{bc,q}$ is f-primary cyclic; and
(b) the sets $N(c, q, b; f)$ are pairwise disjoint for $f \in \bigcup_{r > c/2} \mathrm{Irr}_{br}(q)$.

In particular, $N(c, q, b)$ is a subset of the set of primary cyclic matrices in $\mathrm{M}(bc, q)$ lying in $\mathrm{M}(c, q^b)$, and so a lower bound for $|N|$ gives a lower bound for the number of primary cyclic matrices $X_{bc,q}$ in $\mathrm{M}(c, q^b)$.

Our goal is to determine the size of $N(c, q, b, r)$ for fixed $r > c/2$, by first enumerating $N(c, q, b; f)$ for a fixed f satisfying certain conditions. We use the approach described in § 3.2 to estimate the cardinality of these sets.

3.2. *Quokka theory*

In order to derive upper and lower bounds for the size of $N(c, q, b; f) \subseteq \mathrm{GL}(c, q^b)$ as in Definition 3.3, we apply the theory of *quokka sets* of $G = \mathrm{GL}(n, q)$ [**14**, **23**] (the theory can be applied to all finite groups of Lie type, but here we need only the linear case). These are subsets whose proportion in G can be determined by considering certain proportions in

https://doi.org/10.1112/S1461157015000008X Published online by Cambridge University Press

maximal tori in G and certain proportions in the corresponding Weyl group. Recall that each element $g \in G$ has a unique Jordan decomposition $g = su$, where $s \in G$ is semisimple, $u \in G$ is unipotent and $su = us$ (with s called the *semisimple part* of g and u the *unipotent part*) [1, p. 11]. Note that the order $o(s)$ of s is coprime to the characteristic of G, and that $o(u)$ is a power of the characteristic.

As per [23, Definition 1.1], a non-empty subset Q of G is called a *quokka set* if the following two conditions hold.

(i) If $g \in G$ has Jordan decomposition $g = su$ with semisimple part s and unipotent part u, then $g \in Q$ if and only if $s \in Q$.
(ii) Q is a union of G-conjugacy classes.

We note again the analogy with the definition of an NI subset of $\mathrm{M}(n, q)$. Indeed, the latter was formulated as a way to extend quokka theory to $\mathrm{M}(n, q)$.

Let $\bar{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$, with ϕ the Frobenius morphism (so that the fixed points of ϕ in $\bar{\mathbb{F}}_q$ are precisely the elements of $\mathbb{F}_q$). As outlined in [14, § 3], choose a maximal torus T_0 of $\mathrm{GL}(n, \bar{\mathbb{F}}_q)$ so that $W = N_{\hat{G}}(T_0)/T_0$ is the corresponding Weyl group, and note that for the linear case W is isomorphic to S_n. We summarise the results about quokka subsets of G that are used in the proof of Proposition 3.9. A subgroup H of the connected reductive algebraic group $\mathrm{GL}(n, \bar{\mathbb{F}}_q)$ is said to be *ϕ-stable* if $\phi(H) = H$ and, for each such subgroup H, we write $H^\phi = H \cap \mathrm{GL}(n, \mathbb{F}_q)$. Define an equivalence relation on W as follows: elements $w, w' \in W$ are *ϕ-conjugate* if there exists $x \in W$ such that $w' = x^{-1} w x^\phi$. The equivalence classes of this relation on W are called *ϕ-conjugacy classes* [1, p. 84]. The $\mathrm{GL}(n, \mathbb{F}_q)$-conjugacy classes of ϕ-stable maximal tori are in one-to-one correspondence with the ϕ-conjugacy classes of the Weyl group $W \cong S_n$. The explicit correspondence is given in [1, Proposition 3.3.3].

Let $\mathcal{C}$ be the set of ϕ-conjugacy classes in W and, for each $C \in \mathcal{C}$, let T_C be a representative element of the family of ϕ-stable maximal tori corresponding to C. The following theorem is a direct consequence of [23, Theorem 1.3].

THEOREM 3.4. *Suppose that $Q \subseteq G = \mathrm{GL}(n, q)$ is a quokka set. Then, with the above notation,*

$$\frac{|Q|}{|G|} = \sum_{C \in \mathcal{C}} \frac{|C|}{|W|} \frac{|T_C^\phi \cap Q|}{|T_C^\phi|}. \tag{5}$$

In order to apply Theorem 3.4, we check that the sets $N(c, q^b, 1; f)$ in Definition 3.3 are quokka sets. To do this, we prove a more general statement about sets defined by properties of the characteristic polynomial.

LEMMA 3.5. *Let $g \in \mathrm{GL}(V)$ and suppose that g has multiplicative Jordan decomposition $g = su = us$, where u is unipotent and s is semisimple. Then $c_g(t) = c_s(t)$.*

Proof. Let $f \in \mathrm{Irr}(q)$ divide $c_g(t)$ with multiplicity m, and let $V_f = \ker(f^m(g))$ be the f-primary component of g. Then both u and s fix V_f setwise, since they commute. Since $u|_{V_f} \in \mathrm{GL}(V_f)$ is unipotent, its fixed-point space $U = \mathrm{Fix}\, u|_{V_f}$ is non-trivial. Now, for any $v \in U$, we have $(v^s)^u = v^{us} = v^s$ and so s fixes U setwise. It follows that g fixes U setwise, and indeed $g|_U = u|_U s|_U = s_U$, that is, s and g agree on U. Hence, f^m divides the characteristic polynomial of s. Since this holds for all f, it follows that $c_g(t)$ divides $c_s(t)$ and, since these are both monic polynomials of the same degree, equality holds. □

REMARK 3.6. A consequence of Lemma 3.5 is that any subset of $\mathrm{GL}(V)$ defined by properties of its members' characteristic polynomials is a quokka set. Indeed, if membership of a subset depends only on the characteristic polynomial of $X \in \mathrm{GL}(V)$, then membership depends only

https://doi.org/10.1112/S146115701500008X Published online by Cambridge University Press

on a property of the semisimple part of X. Since the characteristic polynomial is invariant under $\mathrm{GL}(V)$-conjugacy, it follows that sets defined in this way are quokka sets.

LEMMA 3.7. *Let $c, b \in \mathbb{Z}^+$, let q be a prime power and write $K = \mathbb{F}_{q^b}$, $F = \mathbb{F}_q$ as before. Let $r > c/2$ and let $g \in \mathrm{Irr}_r(q)$ satisfy $g^\tau \neq g$ for all non-trivial $\tau \in \mathrm{Gal}(K/F)$. Then, for $f = \prod_{\tau \in \mathrm{Gal}(K/F)} g^\tau$, we have $f \in \mathrm{Irr}_{br}(q)$, and $N(c, q, b; f)$ is a quokka set. In particular, $X \in N(c, q, b; f)$ if and only if g^τ divides $c_{X,V(c,q^b)}(t)$ for exactly one $\tau \in \mathrm{Gal}(K/F)$.*

Proof. By hypothesis, all the g^τ, $\tau \in \mathrm{Gal}(K/F)$, are distinct and hence $f \in \mathrm{Irr}(q)$ with $\deg(f) = br$. Suppose that $X \in \mathrm{M}(c, q^b)$ is such that some g^τ divides $c_{X,V(c,q^b)}(t)$. Then, since $r > c/2$, it is not possible for $g^{\tau'}$ to divide $c_{X,V(c,q^b)}(t)$ for any $\tau' \neq \tau$, and also $(g^\tau)^2$ cannot divide $c_{X,V(c,q^b)}(t)$. Hence, $X_{c,q^b}(t)$ is g^τ-primary cyclic, and it follows from Proposition 3.1 that $X_{bc,q}$ is f-primary cyclic. So, $X \in N(c, q, b; f)$. Conversely, if $X \in N(c, q, b; f)$, then, by Proposition 3.1, X_{c,q^b} is g^τ-primary cyclic and hence g^τ divides $c_{X,V(c,q^b)}(t)$ for exactly one $\tau \in \mathrm{Gal}(K/F)$.

Since conjugate matrices have the same characteristic polynomial, condition (ii) for a quokka set holds. Condition (i) also holds. Indeed, suppose that $X \in N(c, q, b; f)$ with Jordan decomposition $X = US = SU$. We have just proved that g^τ divides $c_{X,V(c,q^b)}(t)$ for exactly one $\tau \in \mathrm{Gal}(K/F)$. Let W be its g^τ-primary component in $V(c, q^b)$. Then $X|_W$ is irreducible and, as U, S centralise X, they both leave W invariant and both $U|_W, S|_W$ centralise $X|_W$. Since $U|_W$ is unipotent, it follows that $U|_W = 1$ and hence $X|_W = S|_W$, which implies that g^τ divides $c_{S,V(c,q^b)}(t)$. Thus, arguing as above, τ is unique with this property and $S \in N(c, q, b; f)$. So, $N(c, q, b; f)$ is a quokka set. □

COROLLARY 3.8. *With notation as in Lemma 3.7,*

$$\frac{|N(c, q, b; f)|}{|\mathrm{GL}(c, q^b)|} = \frac{b}{q^{br} - 1}.$$

Proof. Since $Q := N(c, q, b; f)$ is a quokka set, the required proportion is given by (5). Now, $T_C \cap Q$ is non-empty if and only if T_C contains an element $X \in Q$ or, equivalently, by Lemma 3.7, g^τ divides $c_{X,V(c,q^b)}(t)$. This implies that all permutations in $C \subset W \cong S_c$ contain an r-cycle and, conversely, for all such C, $T_C \cap Q$ is non-empty. Each such torus T_C has the form

$$\mathbb{Z}_{q^{br}-1} \times S,$$

where S corresponds to parts outside the r-cycle. That is, one of the components of the torus T_C is the multiplicative group of a field extension $\mathbb{F}_{q^{br}}$: precisely r elements of this field are roots of g^τ and so precisely r elements of the corresponding torus factor $\mathbb{Z}_{q^{br}-1}$ have characteristic polynomial g^τ on the subspace K^r. This is true for each $\tau \in \mathrm{Gal}(K/F)$. Thus,

$$\frac{|N(c, q, b; f) \cap T_C|}{|T_C|} = \frac{br}{q^{br} - 1}.$$

Hence, if $\mathcal{C}'$ denotes the set of classes of S_c containing an r-cycle, then

$$\frac{|N(c, q, b; f)|}{|\mathrm{GL}(c, q^b)|} = \sum_{C \in \mathcal{C}'} \frac{|C|}{|S_c|} \frac{br}{q^{br} - 1} = \left(\sum_{C \in \mathcal{C}'} \frac{|C|}{|S_c|} \right) \frac{br}{q^{br} - 1} = \frac{1}{r} \frac{br}{q^{br} - 1},$$

since the proportion of permutations containing an r-cycle is $1/r$. □

https://doi.org/10.1112/S146115701500008X Published online by Cambridge University Press

PROPOSITION 3.9. *For $c, b, r \in \mathbb{Z}^+$ with $r > c/2$, and q a prime power,*

$$\frac{|N(c,q,b,r)|}{|\mathrm{GL}(c,q^b)|} = \frac{b|\mathrm{Irr}_{br}(q)|}{q^{br}-1}.$$

In particular,

$$\frac{1}{r}(1-2q^{-br/2}) < \frac{|N(c,q,b,r)|}{|\mathrm{GL}(c,q^b)|} \leqslant \frac{1}{r}.$$

Proof. Since $r > c/2$, $N(c,q,b,r)$ is the disjoint union of the sets $N(c,q,b;f)$ for $f \in \mathrm{Irr}_{br}(q)$. Thus, by Corollary 3.8, the first assertion holds. For the bounds, note that

$$\frac{1}{br}(q^{br}-2q^{br/2}) \leqslant |\mathrm{Irr}_{br}(q)| \leqslant \frac{q^{br}-1}{br}, \tag{6}$$

for, in the proof of Lemma 3.2, each $f \in \mathrm{Irr}_{br}(q)$ is a product $\prod_{i=0}^{br-1}(t-\lambda^{q^i})$ for some $\lambda \in \mathbb{F}_{q^{br}}$ lying in no proper subfield containing F and, by [**21**, Lemma 4.2], there are at least $q^{br}-2q^{br/2}$ such elements λ.

The first inequality in (6) gives

$$\begin{aligned}\frac{b|\mathrm{Irr}_{br}(q)|}{q^{br}-1} &\geqslant \frac{b}{q^{br}-1}\frac{1}{br}(q^{br}-2q^{br/2}) \\ &= \frac{q^{br}(1-2q^{-br/2})}{r(q^{br}-1)} > \frac{1-2q^{-br/2}}{r},\end{aligned}$$

since $1-2q^{-br/2} \geqslant 0$. □

As Proposition 3.9 demonstrates, the proportion $|N(c,q,b,r)|/|\mathrm{GL}(c,q^b)|$ is approximately $1/r$. We use this to derive estimates for $|\bigcup_{r>c/2} N(c,q,b,r)|$. The following lemma is easily verified and we omit the proof for brevity.

LEMMA 3.10. *Let $c \geqslant 2$. Then*

$$\log 2 - \frac{1}{c+1} \leqslant \sum_{r=\lfloor c/2+1 \rfloor}^{c} \frac{1}{r} \leqslant \log 2 + \frac{1}{c}.$$

PROPOSITION 3.11. *For $N(c,q,b)$ as in Definition 3.3,*

$$\log 2 - \frac{1}{c+1} - \frac{2}{q^{bc/4}} < \frac{|N(c,q,b)|}{|\mathrm{GL}(c,q^b)|} \leqslant \log 2 + \frac{1}{c}.$$

Proof. By definition, $N(c,q,b) = \bigcup_{r>c/2} N(c,q,b,r)$, and the $N(c,q,b,r)$ are pairwise disjoint, because no two polynomials of degree greater than $c/2$ can divide the characteristic polynomial of any one matrix. Thus,

$$\frac{|N(c,q,b)|}{|\mathrm{GL}(c,q^b)|} = \sum_{r>c/2} \frac{|N(c,q,b,r)|}{|\mathrm{GL}(c,q^b)|}$$

and so, by Proposition 3.9,

$$\sum_{r=\lfloor c/2 \rfloor+1}^{c} \frac{1}{r}(1-2q^{-br/2}) \leqslant \frac{|N(c,q,b)|}{|\mathrm{GL}(c,q^b)|} \leqslant \sum_{r=\lfloor c/2 \rfloor+1}^{c} \frac{1}{r}.$$

https://doi.org/10.1112/S1461157015000008X Published online by Cambridge University Press

The asserted upper bound for $|N(c,q,b)|/|\mathrm{GL}(c,q^b)|$ now follows from Lemma 3.10. For the lower bound, first apply Lemma 3.10 to get

$$\frac{|N(c,q,b)|}{|\mathrm{GL}(c,q^b)|} \geqslant \log 2 - \frac{1}{c+1} - \sum_{r=\lfloor c/2\rfloor+1}^{c} \frac{2}{rq^{-br/2}}.$$

To bound the remaining sum, observe that there are $\lceil c/2\rceil$ summands with

$$-\frac{2}{rq^{-br/2}} \geqslant -\frac{2}{r_0 q^{-br_0/2}}, \quad \text{where } r_0 := \lfloor c/2\rfloor + 1.$$

For c even, this yields

$$-\sum_{r=\lfloor c/2\rfloor+1}^{c} \frac{2}{rq^{-br/2}} \geqslant -\frac{2\cdot c/2}{(c/2+1)q^{bc/4}} > -\frac{2}{q^{bc/4}}$$

and, for c odd,

$$-\sum_{r=\lfloor c/2\rfloor+1}^{c} \frac{2}{rq^{-br/2}} \geqslant -\frac{2\cdot (c+1)/2}{(c+1)/2\cdot q^{bc/4}} = -\frac{2}{q^{bc/4}}. \qquad \square$$

Remark 3.12. The bounds in Proposition 3.11 are similar to the bounds obtained by Niemeyer and Praeger [**22**, Theorem 6.1] on the proportion P of elements $g \in \mathrm{GL}(c,q)$, $c \geqslant 3$, such that g is a so-called $\mathrm{ppd}(c,q;r)$-element for some $r > c/2$. This means that the order of g is divisible by a primitive prime divisor (ppd) of $q^r - 1$, namely a prime that divides $q^r - 1$ but does not divide $q^j - 1$ for any $j < r$ (as per Remark 1.5). The proportion P satisfies

$$\log 2 - \frac{1}{c+2} \leqslant P \leqslant \log 2 + \frac{1}{c-1}.$$

This kind of result, with linear convergence to the limit, seems to be the best that can be obtained by considering polynomials of large degree. We note that the set $N(c,q,b)$ is both more and less restrictive than the set of ppd elements. On the one hand, some matrices in $N(c,q,b)$ may have order not divisible by a ppd of $q^r - 1$; on the other hand, some ppd elements correspond to irreducible polynomials $g \in K[t]$ that do not have the property $g^\tau \neq g$ for non-trivial $\tau \in \mathrm{Gal}(K/F)$. Thus, the two sets are very similar but neither is contained in the other.

In order to apply Theorem 1.3 to prove Theorem 1.4, we first note that Lemmas 2.4 and 2.6 rely on knowledge of the proportion $|N_i|/|\mathrm{GL}(i,q)|$ for *all* values of i. In defining the NI set that we wish to investigate, we must take care when considering matrices $X \in \mathrm{M}(d,q)$ with $\dim(V_{\mathrm{inv}}(X)) \leqslant 2$.

Proof of Theorem 1.4. Let $N \subset \mathrm{M}(c,q^b)$ be as in Theorem 1.4. Choose a maximal flag $\{0\} = V_0 \subset V_1 \subset \ldots \subset V_c = V(c,q^b)$ with $\dim V_i = i$ as an $\mathbb{F}_{q^b}$-space, and define $N(i)$ and N_i as in Definition 1.2, where we interpret $V_{\mathrm{inv}}(X)$ as an $\mathbb{F}_{q^b}$-space for $X \in N$. Then, by Theorem 1.3 applied to N as a subset of $\mathrm{M}(c,q^b)$,

$$\frac{|N|}{|\mathrm{M}(c,q^b)|} = \omega(c,q^b)\sum_{i=o}^{c} \frac{q^{-b(c-i)}}{\omega(c-i,q^b)}\frac{|N_i|}{|\mathrm{GL}(V_i)|}. \tag{7}$$

Note that N_0 is the empty set and that $N_1 = \mathrm{GL}(V_1)$. For $i \geqslant 2$, N_i is the subset $N(i,q,b)$ of Definition 3.3 (with the parameter c there replaced by i) and so, by Proposition 3.11,

$$\frac{|N_i|}{|\mathrm{GL}(i,q^b)|} \geqslant \log 2 - \frac{1}{i+1} - \frac{2}{q^{bi/4}} \geqslant \log 2 - \frac{1}{i+1} - \frac{2}{q^{b/2}}.$$

https://doi.org/10.1112/S1461157015000008X Published online by Cambridge University Press

This inequality also holds for $i = 1$ because $|N_1|/|\mathrm{GL}(1, q^b)| = 1$. Thus, by Proposition 2.6 with $a = \log 2 - 2/q^{b/2}$ and $k = 1$,

$$\frac{|N(c, q, b)|}{|\mathrm{M}(c, q^b)|} \geqslant \log 2 - \frac{2}{q^{b/2}} - \frac{\log 2 - 2q^{-b/2} + 3}{c}$$
$$= \log 2 - \frac{\log 2 + 3}{c} - \frac{2(1 - 1/c)}{q^{b/2}}. \qquad \square$$

Acknowledgements. We thank S. Glasby for several helpful discussions, and the referee for suggestions that improved the paper.

References

1. R. W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters* (John Wiley, Chichester, 1993).
2. B. P. Corr, 'Estimation and computation with matrices over finite fields', PhD Thesis, The University of Western Australia, 2014.
3. B. P. Corr and C. E. Praeger, 'Primary cyclic matrices in irreducible matrix subalgebras', Preprint, 2014, arXiv:1401.1598.
4. H. Dietrich, C. R. Leedham-Green and F. Lübeck, 'Constructive recognition of classical groups in even characteristic', *J. Algebra* 391 (2013) 227–255.
5. J. Fulman, P. M. Neumann and C. E. Praeger, 'A generating function approach to the enumeration of matrices in classical groups over finite fields', *Mem. Amer. Math. Soc.* 176 (2005) 1–90.
6. M. Gerstenhaber, 'On the number of nilpotent matrices with coefficients in a finite field', *Illinois J. Math.* 5 (1961) 330–333.
7. S. P. Glasby, 'The meat-axe and f-cyclic matrices', *J. Algebra* 300 (2006) 77–90.
8. S. P. Glasby and C. E. Praeger, 'Towards an efficient Meat-Axe algorithm using f-cyclic matrices: the density of uncyclic matrices in $M(n, q)$', *J. Algebra* 322 (2009) 766–790.
9. B. Hartley and T. O. Hawkes, *Rings, modules and linear algebra* (Chapman & Hall, London, 1980).
10. D. F. Holt and S. Rees, 'Testing modules for irreducibility', *J. Aust. Math. Soc. Ser. A* 57 (1994) 1–16.
11. G. Ivanyos and K. Lux, 'Treating the exceptional cases of the MeatAxe', *Exp. Math.* 9 (2000) 373–381.
12. G. I. Lehrer, 'Rational tori, semisimple orbits and the topology of hyperplane complements', *Comment. Math. Helv.* 67 (1992) 226–251.
13. G. I. Lehrer, 'The cohomology of the regular semisimple variety', *J. Algebra* 199 (1998) 666–689.
14. F. Lübeck, A. C. Niemeyer and C. E. Praeger, 'Finding involutions in finite Lie type groups of odd characteristic', *J. Algebra* 321 (2009) 3397–3417.
15. P. M. Neumann and C. E. Praeger, 'Cyclic matrices over finite fields', *J. Lond. Math. Soc.* (2) 52 (1995) 263–284.
16. P. M. Neumann and C. E. Praeger, 'Cyclic matrices and the meataxe', *Groups Comput.* 3 (2001) 291–300.
17. M. Neunhoeffer, Á. Seress, N. Ankaralioglu, P. Brooksbank, F. Celler, S. Howe, M. Law, S. Linton, G. Malle, A. C. Niemeyer, E. A. O'Brien and C. M. Roney-Dougal, 'recog. A collection of group recognition methods', ver. 1.2. http://gap-system.github.io/recog/.
18. M. Neunhöffer and Á. Seress, 'Constructive recognition of $\mathrm{SL}(n, q)$ in its natural representation', in preparation.
19. A. C. Niemeyer, S. B. Pannek and C. E. Praeger, 'Irreducible linear subgroups generated by pairs of matrices with large irreducible submodules', *Arch. Math.* 98 (2012) 105–114.
20. A. C. Niemeyer, T. Popiel and C. E. Praeger, 'On proportions of pre-involutions in finite classical groups', *J. Algebra* 324 (2010) 1016–1043.
21. A. C. Niemeyer, T. Popiel and C. E. Praeger, 'Abundant p-singular elements in finite classical groups', *J. Algebra* 408 (2014) 189–204.
22. A. C. Niemeyer and C. E. Praeger, 'A recognition algorithm for classical groups over finite fields', *Proc. Lond. Math. Soc.* (3) 77 (1998) 117–169.
23. A. C. Niemeyer and C. E. Praeger, 'Estimating proportions of elements in finite groups of Lie type', *J. Algebra* 324 (2010) 122–145.
24. A. C. Niemeyer and C. E. Praeger, 'Elements in finite classical groups whose powers have large 1-eigenspaces', *Discrete Math. Theor. Comput. Sci.* 16 (2014) 303–312.
25. R. A. Parker, 'The computer calculation of modular characters (the meat-axe)', *Computational group theory (Durham, 1982)* (Academic Press, London, 1984) 267–274.
26. G. E. Wall, 'On the conjugacy classes in the unitary, symplectic and orthogonal groups', *J. Aust. Math. Soc.* 3 (1963) 1–62.

Brian P. Corr
School of Mathematics and Statistics
The University of Western Australia
Australia

brian.p.corr@gmail.com

Current address: Departamento de Matemática
Instituto de Ciências Exatas
Universidade Federal de Minas Gerais
Av. Antônio Carlos, 6627
31270-901 Belo Horizonte, MG
Brazil

Cheryl E. Praeger
School of Mathematics and Statistics
The University of Western Australia
Australia

and
King Abdullaziz University, Jeddah
Saudi Arabia

cheryl.praeger@uwa.edu.au

Tomasz Popiel
School of Mathematics and Statistics
The University of Western Australia
Australia

tomasz.popiel@uwa.edu.au

https://doi.org/10.1112/S146115701500008X Published online by Cambridge University Press