Elements in finite classical groups whose powers have large 1-Eigenspaces

Alice Niemeyer, Cheryl Praeger

Discrete Mathematics and Theoretical Computer Science DMTCS vol. **16:1**, 2014, 303–312

Elements in finite classical groups whose powers have large 1-Eigenspaces

Alice C. Niemeyer[1,2] Cheryl E. Praeger[1,3]

[1] *Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics M019, The University of Western Australia, Crawley, Australia*
[2] *Lehrstuhl D für Mathematik, RWTH Aachen University, Aachen, Germany*
[3] *King Abdulazziz University, Jeddah, Saudi Arabia*

received 16th Dec. 2011, accepted 11th Apr. 2014.

We estimate the proportion of several classes of elements in finite classical groups which are readily recognised algorithmically, and for which some power has a large fixed point subspace and acts irreducibly on a complement of it. The estimates are used in complexity analyses of new recognition algorithms for finite classical groups in arbitrary characteristic.

Keywords: proportion of elements, finite classical groups, 1-eigenspaces

1 Introduction

A crucial task in designing algorithms to compute with matrix groups defined over finite fields is to recognise whether a given matrix group H is isomorphic to a finite classical group and, if so, to find an isomorphism with the natural representation of H. The isomorphism is defined by identifying appropriate elements of H with the standard generators of the natural representation. Algorithms which accomplish this task are generally referred to as constructive recognition algorithms by Kantor and Seress (2001). In this paper, we concentrate on the important special case when H is already given in its natural representation, by a set of $d \times d$ matrices over a finite field $\mathbb{F}_q$ (but we have not yet found appropriate elements of H that can serve as standard generators). In this special case, for odd q, a highly efficient and practical algorithm has been designed by Leedham-Green and O'Brien (2009). Recently, Dietrich et al. (2013) designed recognition algorithms for even q and Neunhöffer and Seress (see also Neunhöffer and Seress (2012)) designed algorithms for arbitrary q. In both new algorithms, a pivotal step is to find an element x which acts irreducibly on a subspace of dimension m, that is it does not leave invariant a subspace of the m-dimensional space, with m small relative to d, and fixes a complementary subspace pointwise. Dietrich et al. (2013) seek such elements elements for which the dimension m is at least a constant fraction of d (see Section 5, especially Lemma 5.5 of their paper), whereas Neunhöffer and Seress use such elements with $m = O(\log(d))$ (see our Corollary 3.5). Using results of Praeger et al. (to appear), Neunhöffer and

H	d	α	δ	ϵ
$\mathrm{SL}_n(q)$	n	1	1	1
$\mathrm{SU}_n(q)$	n	1	2	-1
$\mathrm{Sp}_{2n}(q)$	$2n$	2	1	1
$\mathrm{SO}_{2n+1}(q)$	$2n+1$	2	1	1
$\mathrm{SO}^{\pm}_{2n}(q)$	$2n$	2	1	1

Tab. 1: Groups and constants in Theorems 1.1 and 3.3

Seress prove that, if x satisfies an additional condition on its order (divisible by a primitive prime divisor, see Section 3) then, with high probability, x and a random conjugate of x in H generate a classical group of dimension $2m$. This smaller classical group is then processed in a recursive procedure. As elements with large 1-eigenspaces are rare, the algorithms seek such elements as appropriate powers of nearly uniformly distributed random elements of H. In this paper, we show that a significant proportion of elements of H have a power with the desired properties.

For an integer k we introduce in Definition 3.1 three subsets of H, called Q_k, Q_k^{ppd} and Q_k^{full}, for which $Q_k^{\mathrm{full}} \subseteq Q_k^{\mathrm{ppd}} \subseteq Q_k$ and if $k \geq 3$, then $Q_k^{\mathrm{full}} \neq \emptyset$. (Here H is one of the classical groups in Table 1, and the defining condition for the sets depends on the integer α given in Table 1.) Elements in Q_k power to elements leaving invariant an αk-dimensional subspace without a 1-eigenvalue and having a $(d-\alpha k)$-dimensional 1-eigenspace and in addition elements in Q_k^{ppd} power to elements acting irreducibly on the αk-dimensional subspace. Membership in these sets can readily be determined algorithmically: for example, in the case of Q_k, by examining the degrees of the irreducible factors of the characteristic polynomial. Properties of these subsets are discussed in more detail in Section 3. We state here our main result on the properties and proportions of elements in these subsets. We note that the proportion of elements of H that lie in Q_k^{ppd} for $\alpha k > d/2$ differs only by a constant from the proportion of so-called ppd-elements determined in (Niemeyer and Praeger, 1998, Theorem 5.7) (see also its generalisation in (Niemeyer and Praeger, 2010, Theorem 1.9)). Throughout the paper $\log$ denotes the natural logarithm to base e.

Theorem 1.1 *Let H be a d-dimensional classical group defined over a finite field with q elements, as in one of the rows of Table 1. Let n, α be as in Table 1, and let k be an integer such that $\max\{3, \log(n)\} \leq k \leq n/2$ and k odd if $H = SU_n(q)$. Let Q denote one of the sets Q_k, Q_k^{ppd} or Q_k^{full}. Then each element of Q powers up to an element which has a $(d-\alpha k)$-dimensional 1-eigenspace and acts irreducibly on a complementary invariant subspace of dimension αk. Moreover for $Q = Q_k$ or $Q = Q_k^{\mathrm{ppd}}$*

$$\frac{2}{9e\alpha k} \leq \frac{|Q|}{|H|} \leq \frac{5}{3\alpha k} \quad \textit{while} \quad \frac{2}{10e\alpha k^2 \log(q+1)} \leq \frac{|Q_k^{\mathrm{full}}|}{|H|} \leq \frac{5}{3\alpha k}.$$

Every element g in a finite classical group admits a multiplicative Jordan decomposition as $g = us$, where s is semisimple and u is unipotent. As s is diagonalisable over the algebraic closure $\overline{\mathbb{F}}_q$ of the field $\mathbb{F}_q$ with q elements, the eigenvalues of g over $\overline{\mathbb{F}}_q$ are those of s and the characteristic polynomial of g equals that of s. The characteristic polynomial of s yields information about the eigenvalues of s (and g): for each irreducible factor of degree k, there are k eigenvalues over $\overline{\mathbb{F}}_q$ which lie in $\mathbb{F}_{q^k}$ and no smaller field.

Our aim is to group the eigenvalues of g into two disjoint sets in such a way that we can find an integer B such that the B-th power of each eigenvalue in the first set is equal to 1, while the B-th power of each eigenvalue in the second set is distinct from 1. We identify elements g in classical groups for which we can read off from the characteristic polynomial whether or not they have such eigenvalues. Moreover the integer B can then also be determined from the characteristic polynomial, see Remark 3.2.

In order to give a precise description of the elements we seek, we use detailed information about the eigenvalues of elements in finite classical groups. Such information was obtained in (Lübeck et al., 2009, Sections 3,5) and we present a summary of the information relevant to this paper in Section 2. In Section 3 we are then able to define the elements we seek precisely. We state in Theorem 3.3 a complete and detailed version of Theorem 1.1 giving upper and lower bounds on the proportions for the three classes of elements separately. In Section 4 we outline the strategy of our proof and prove Theorem 3.3 in Subsection 4.4. Theorem 1.1 then follows.

2 Eigenvalues of elements in maximal tori

The theory of algebraic groups necessary to understand the results in this paper can be found in Carter (1993). Here we just mention that for a finite classical group H and for W the corresponding Weyl group, the H-conjugacy classes of F-stable maximal tori are in one-to-one correspondence with the F-conjugacy classes of the Weyl group W of H. When H is a finite classical group the Weyl group W of H is isomorphic to a full symmetric group S_n (lines 1-2 of Table 1), or a wreath product $S_2 \wr S_n$ (lines 3-4 of Table 1), or the index 2 subgroup of $S_2 \wr S_n$ consisting of even permutations (line 5 of Table 1). Thus the F-conjugacy classes of the Weyl group are parametrised by partitions or pairs of partitions of n. In this section we describe the eigenvalues over $\overline{\mathbb{F}}_q$ and the characteristic polynomials of the semi-simple elements in the maximal tori T_C corresponding to the F-conjugacy class C of W. The information needed for this description is extracted from (Lübeck et al., 2009, Sections 3,5). Let H, n and ε be as in one of the lines of Table 1.

2.1 Characteristic polynomials in corresponding tori in $\mathrm{SL}_n(q)$ and $\mathrm{SU}_n(q)$

Here H is the set of elements of the algebraic group $G = \mathrm{GL}_n(\overline{\mathbb{F}}_q)$ fixed by the Frobenius morphism $F : (a_{ij}) \to (a_{ij}^{\epsilon q})$, where $\epsilon = 1$ or -1, according as $H = \mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$, respectively. An F-conjugacy class C of W is uniquely determined by a partition of n. For each part λ of this partition the elements of T_C have λ corresponding eigenvalues in $\overline{\mathbb{F}}_q$ which lie in $\mathbb{F}_{q^\lambda}$ and these are permuted by the map $\tau : a \mapsto a^{\epsilon q}$. If one of these λ eigenvalues lies in a smaller field, say $\mathbb{F}_{q^{\lambda'}}$, for λ' a proper divisor of λ, then so do all of its Galois conjugates. Therefore, for each part λ of the partition of n and for all divisors λ' of λ, the torus T_C contains elements whose characteristic polynomials have λ/λ' factors of degree λ' which are irreducible over $\mathbb{F}_q$.

If λ' is odd, then each of these irreducible factors of degree λ' is also irreducible over $\mathbb{F}_{q^2}$, whereas if λ' is even then each irreducible factor of degree λ' is a product of a pair of τ-conjugate factors of degree $\lambda'/2$ which are irreducible over $\mathbb{F}_{q^2}$.

2.2 Characteristic polynomials in corresponding tori in $\mathrm{Sp}_{2n}(q)$ and $\mathrm{SO}_{2n+1}(q)$

Here H is the set of elements of the algebraic group $G = \mathrm{Sp}_m(\overline{\mathbb{F}}_q)$ or $\mathrm{SO}_m(\overline{\mathbb{F}}_q)$ (subgroups of $\mathrm{GL}_m(\overline{\mathbb{F}}_q)$) fixed by the Frobenius morphism $F : (a_{ij}) \to (a_{ij}^q)$, where $m = 2n$ if $H = \mathrm{Sp}_m(q)$ and $m = 2n + 1$

if $H = \mathrm{SO}_m(q)$. An F-conjugacy class C of W is determined by a partition of n, where each part is marked either positive or negative.

For any positive part λ, the elements of T_C have λ eigenvalues in $\overline{\mathbb{F}}_q$, and they, together with their λ inverses, lie in $\mathbb{F}_{q^\lambda}$ and are permuted by the map $a \mapsto a^q$ in two cycles of length λ. If one of these 2λ eigenvalues lies in a smaller field, say $\mathbb{F}_{q^{\lambda'}}$, for λ' a proper divisor of λ, then so do all of its Galois conjugates and all of their inverses. Therefore, for each positive part λ of the partition of n and for all divisors λ' of λ the torus T_C contains elements whose characteristic polynomials have λ/λ' corresponding pairs of factors, each of degree λ' and irreducible over $\mathbb{F}_q$ and if $\xi \in \overline{\mathbb{F}}_q$ is a root of one of these factors, then ξ^{-1} is a root of its paired factor.

For any negative part μ, the elements of T_C have μ eigenvalues in $\overline{\mathbb{F}}_q$, and they together with their μ inverses lie in $\mathbb{F}_{q^{2\mu}}$, and are permuted by the map $a \mapsto a^q$ in a cycle of length 2μ. Therefore, for each negative part μ of the partition of n and for all divisors μ' of μ the torus T_C contains elements whose characteristic polynomials have μ/μ' corresponding factors of degree $2\mu'$ which are irreducible over $\mathbb{F}_q$. Moreover, if $\xi \in \overline{\mathbb{F}}_q$ is a root of one of these factors, then so is ξ^{-1}.

2.3 Characteristic polynomials in corresponding tori for $\mathrm{SO}^{\pm}_{2n}(q)$

Finally, we treat this case similarly to the previous case by considering $\mathrm{SO}^{\pm}_{2n}(q)$ as a natural subgroup of $\mathrm{SO}_{2n+1}(q)$. Then the maximal tori of $\mathrm{SO}^{\pm}_{2n}(q)$ are those tori of $\mathrm{SO}_{2n+1}(q)$ that correspond to pairs (β^+, β^-) of partitions of n with $|\beta^+| + |\beta^-| = n$ such that β^- has an even number of parts for $\mathrm{SO}^+_{2n}(q)$, whereas β^- has an odd number of parts for $\mathrm{SO}^-_{2n}(q)$. The Weyl group W has index 2 in the Weyl group W_B of $\mathrm{SO}_{2n+1}(\overline{\mathbb{F}}_q)$. For each F-conjugacy class C in W which does not correspond to a single part of length n, the characteristic polynomials that arise are the same as in the case $\mathrm{SO}_{2n+1}(q)$ (and all the classes C we consider are of this type).

3 The elements we seek

Having obtained a description of the eigenvalues and characteristic polynomials of semisimple elements, we are now in a position to define the elements we seek. Let $H, d, n, \alpha, \delta, \varepsilon$ be as in one of the rows of Table 1. As mentioned in the introduction, we aim to find elements whose eigenvalues belong to one of two distinct sets. For a fixed integer k, we would like to find elements with αk eigenvalues that lie in $\mathbb{F}_{q^{\delta\alpha k}}$ and no proper subfield, such that the remaining eigenvalues all have order dividing an integer B which is divisible by no primitive prime divisor of $q^{\delta\alpha k} - 1$. (A primitive prime divisor of $q^m - 1$ is a prime r dividing $q^m - 1$ but not dividing $q^i - 1$ for integers i with $1 \le i < m$.)

We say that two polynomials $f_1(x)$ and $f_2(x)$ defined over a finite field $\mathbb{F}_q$ with q elements are *conjugate* if for any root a of $f_1(x)$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, the element a^{-1} is a root of $f_2(x)$. A polynomial $f(x)$ is *self-conjugate* if $f(x)$ is conjugate to itself. For an integer k, we can now define the set Q_k and its two subsets Q_k^{ppd} and Q_k^{full}.

Definition 3.1 *Let k be an integer such that $1 \le k \le d$.*

(i) *Let Q_k denote the set of all elements $g \in H$ with characteristic polynomial $c_g(x)$ for which one of the following conditions holds:*

  (a) *$H = \mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$ and $c_g(x)$ has an irreducible factor of degree k over $\mathbb{F}_q$, where k is odd in case $\mathrm{GU}_n(q)$, and no other irreducible factors of degree divisible by k,*

(*b*) $H = \mathrm{Sp}_{2n}(q)$, $\mathrm{SO}^{\pm}_{2n}(q)$ *or* $\mathrm{SO}_{2n+1}(q)$ *and* $c_g(x)$ *has a self-conjugate irreducible factor of degree* $2k$*, no other self-conjugate irreducible factors of degree divisible by* $2k$ *and no non-self-conjugate irreducible factors of degree divisible by* k*.*

(*ii*) *Let* Q_k^{ppd} *denote the subset of* Q_k *consisting of those elements* g *for which, in addition, there is a primitive prime divisor* r *of* $q^{\delta\alpha k}-1$ *which divides* $|g|$*.*

(*iii*) *Let* Q_k^{full} *denote the subset of* Q_k^{ppd} *of elements* g *such that, for every primitive prime divisor* r *of* $q^{\delta\alpha k}-1$ *which divides* $|H|$*, the order* $|g|$ *is divisible by the* r*-part of* $q^{\delta\alpha k}-1$ *(that is, by the highest power of* r *dividing* $q^{\delta\alpha k}-1$*).*

Then for an element $g \in Q_k$ we can find an integer B as described in the following remark such that g^B has a $(d-\alpha k)$-dimensional 1-eigenspace and a k-dimensional invariant subspace on which g acts irreducibly.

Remark 3.2 Let $g \in Q_k$. We define a positive integer B as follows (see also (Leedham-Green and O'Brien, 2009, Section 2.2)). Let $c_g(x)$ denote the characteristic polynomial of g and suppose that $c_g(x)$ factors into irreducibles as $c_g(x) = \prod_{i=1}^{s} f_i(x)^{n_i}$, where the degree of $f_i(x)$ is k_i, $k_1 = \alpha k$, and $n_1 = 1$ (and f_1 is self-conjugate in the symplectic and orthogonal cases). Let $B = p^\beta \prod_{i=2}^{s}(q^{\delta k_i}-1)$, where p is the characteristic of $\mathbb{F}_q$ and $\beta = \lceil \log_p(\max(n_i)) \rceil$. All eigenvalues of g over $\overline{\mathbb{F}}_q$ corresponding to an irreducible factor $f_i(x)$ of degree k_i, for $i > 1$, lie in $\mathbb{F}_{q^{k_i}}$ and hence are powered to 1 by B. For $i > 1$ we have $\gcd(q^{\delta\alpha k}-1, q^{\delta k_i}-1) = q^{\delta \gcd(\alpha k, k_i)}-1$ and since $\gcd(\alpha k, k_i) \neq \alpha k$, it follows that $\gcd(q^{\alpha k}-1, B)$ divides $\mathrm{lcm}\{q^\ell - 1 \mid \ell \text{ a proper divisor of } \alpha k\}$. Therefore the eigenvalues of g lying in $\mathbb{F}_{q^{\alpha k}}$, but in no proper subfield, are not powered to 1 by B. Thus g^B has a $(d-\alpha k)$-dimensional 1-eigenspace and leaves invariant a subspace U of the underlying vector space of dimension αk on which g^B acts without a 1-eigenvector. Note that $g^B|_U$ may not be irreducible: for example, if $q = \alpha = 2, k = 3$, then there is an f_1 such that $g^B|_U$ has order 9; under our assumptions it is possible to have $k_2 = 4$ and hence for B to be divisible by 3 so that g^B has order 3 and acts reducibly on the 6-dimensional subspace U.

Even though g is irreducible on U, the element g^B may not be. For example, if $H = \mathrm{SL}_{11}(2)$, there exists $g \in Q_6$ with $c_g(t)$ a product of irreducibles of degrees 2,3 and 6 and inducing a Singer cycle on a 6-dimensional space U, while $B = 21$ and g^B leaves invariant several 2-dimensional subspaces of U. For some applications we require g^B to be irreducible on U, and this is the reason for defining the subsets Q_k^{ppd} and Q_k^{full} of Q_k. Indeed, if $g \in Q_k^{\mathrm{ppd}}$ then $|g|$ is divisible by some primitive prime divisor r of $q^{\delta\alpha k}-1$, and r does not divide $q^{\delta k_i}-1$ for $i = 2, \ldots, s$ as $k_i \not\equiv 0 \pmod{\alpha k}$. Thus r divides the order $|g^B|$ and hence $g|_U$ is irreducible. Moreover, if $g \in Q_k^{\mathrm{full}}$, and r^a divides $q^{\delta\alpha k}-1$, then r^a also divides $|g^B|$, for the same reason.

Note that $Q_k^{\mathrm{full}} \neq \emptyset$ provided $q^{\delta\alpha k}-1$ has a primitive prime divisor dividing $|H|$, and this is almost always true if $3 \leq k \leq n/2$ (with a small number of exceptions such as $k = 6, H = \mathrm{SL}_{11}(2)$, see Zsigmondy (1892)), hence our need to assume the subsets are non-empty in Theorem 3.3. Our main theorem is as follows. Recall that we use natural logarithms.

Theorem 3.3 *Let* q *be a prime power and* $\mathbb{F}_q$ *a finite field with* q *elements. Let* H*,* d*,* α, δ *and* ϵ *be as in one of the lines of Table* 1*. Let* k *be a positive integer with* $\max\{3, \log(n)\} \leq k \leq n/2$ *and such that* k *is odd when* $H = \mathrm{SU}_n(q)$*. Let* Q *be one of* $Q_k, Q_k^{\mathrm{ppd}}, Q_k^{\mathrm{full}}$ *such that* $Q \neq \emptyset$*, and let* $\ell_{k,Q}$ *and* $m_{n,Q}$ *be as in Table* 2*. Then*

Q	Q_k	Q_k^{ppd}	Q_k^{full}
$\ell_{k,Q}$	$1-\frac{2}{q^{k/2}}$	$1-\frac{1}{\alpha k}$	$\frac{\log(2)}{k\log(q+1)}$
$m_{n,Q}$	$1-\frac{2}{q^{\log(n)/2}}$	$1-\frac{1}{\alpha\log(n)}$	$\frac{\log(2)}{2\log(n)\log(q+1)}$

Tab. 2: Definitions of $\ell_{k,Q}$ and $m_{n,Q}$ in Theorem 3.3

(a)

$$\frac{\ell_{k,Q}}{3e\alpha k} \leq \frac{|Q|}{|H|} \leq \frac{5}{3\alpha k}.$$

(b) *If, in addition,* $\log(n) < k \leq 2\log(n)$*, then*

$$\frac{m_{n,Q}}{6e\alpha\log(n)} \leq \frac{|Q|}{|H|} < \frac{5}{3\alpha\log(n)}.$$

Note that if k is odd and $k > 1$, then every self-conjugate polynomial has even degree. Hence when H is one of the groups $\mathrm{Sp}_{2n}(q)$, $\mathrm{SO}^{\pm}_{2n}(q)$ or $\mathrm{SO}_{2n+1}(q)$, the elements in Q_k have a characteristic polynomial which has one self-conjugate irreducible factor of degree $2k$, and no other irreducible factors of degree divisible by k. This follows from the fact that a self-conjugate factor of degree divisible by an odd k would have degree divisible by $2k$. Thus, when k is odd, for all the groups H, the conditions in Definition 3.1 on $c_g(x)$ for g to lie in Q_k are that there is an irreducible factor of degree αk and all other irreducible factors have degrees not divisible by k. For $n \geq 5$ and odd integers $k > \log(n)$ we have in particular that $k \geq 3$ and therefore, by the Theorem of Zsigmondy (1892), $q^k - 1$ has a primitive prime divisor. Moreover, for $n \geq 5$ there is at least one odd integer k such that $\log(n) < k \leq 2\log(n)$. For such k, Theorem 3.3 yields a lower bound for the proportion $|Q_k|/|H|$, namely $|Q_k^{\mathrm{ppd}}|/|H| \geq (1-\frac{1}{\alpha\log(n)})\frac{1}{6e\alpha\log(n)} > \frac{1}{16e\alpha\log(n)}$, since $(1-\frac{1}{\alpha\log(n)})/6 > (1-\frac{1}{\log(5)})/6 > 1/16$. Thus we have the following corollary.

Corollary 3.4 *Let q be a prime power and $\mathbb{F}_q$ a finite field with q elements. Let H, d, α, δ, ϵ be as in one of the lines of Table* 1*. If $n \geq 5$ then for each odd integer k such that $\log(n) < k \leq 2\log(n)$, the proportion of elements in H which have a characteristic polynomial with an irreducible factor of degree αk and all other irreducible factors of degree not divisible by k is at least $\frac{1}{16e\alpha\log(n)}$.*

Moreover, if $n \geq 5$ then, by (Niven et al., 1991, Theorem 8.7), there is an odd prime k satisfying $\log(n) < k < 2\log(n)$. For odd primes k, the divisibility condition 'not divisible by k' is equivalent to the condition 'coprime to k'. Thus an immediate consequence of Corollary 3.4 is the following result.

Corollary 3.5 *Let q be a prime power and $\mathbb{F}_q$ a finite field with q Let H, d, α, δ, ϵ be as in one of the lines of Table* 1*. If $n \geq 5$ then with probability at least $1/(16e\alpha\log(n))$, the characteristic polynomial of a random element of H has some irreducible factor, say of degree k, such that $\log(n) < k \leq 2\log(n)$ and the degrees of all other irreducible factors are coprime to k.*

4 The ingredients of the proofs

We quote a version of a theorem, originally employed in different contexts independently by Isaacs et al. (1995) and Lehrer (1992), which allows us to estimate the proportion of elements in any of the groups H

of Table 1 which lie in one of the sets Q_k, Q_k^{ppd} and Q_k^{full}. We use the notation introduced in Section 2 for F, W.

Theorem 4.1 *Let H be one of the groups in Table 1, let k be a positive integer with $k \geq \log(n)$, and let Q denote one of the sets Q_k, Q_k^{ppd} or Q_k^{full}. Then*

$$\frac{|Q|}{|H|} = \sum_C \frac{|C|}{|W|} \frac{|Q \cap T_C|}{|T_C|},$$

where the sum is over all F-conjugacy classes C of W and T_C is a representative of the H-conjugacy class of F-stable maximal tori corresponding to the F-conjugacy class C.

Proof: Clearly Q is closed under conjugation by elements in G. Moreover, for an element $g \in H$ having Jordan decomposition $g = us$ with u unipotent and s semisimple, we have $g \in Q$ if and only if $s \in Q$, as g and s have the same characteristic polynomial in their actions on the underlying vector space. The result follows as in the proof of (Isaacs et al., 1995, Theorem 6.2) or the proof of (Lübeck et al., 2009, Lemma 2.3) or from (Niemeyer and Praeger, 2010, Theorem 1.3). □

4.1 Relevant conjugacy classes

The proof of the main theorem will amount to identifying relevant conjugacy classes C in W and estimating the proportion of elements of Q that lie in the corresponding torus. The following lemma allows us to identify the relevant conjugacy classes when $Q = Q_k$ for some positive integer k. It follows directly from the discussion in Section 2.

Lemma 4.2 *Let H, n be as in one of the lines of Table 1, and let $2 \leq k < n$. Then a maximal F-stable torus T_C satisfies $T_C \cap Q_k \neq \varnothing$ if and only if the corresponding F-conjugacy class C contains elements w for which*

(a) *if $H = \mathrm{SL}_n(q)$, then w contains a k-cycle and all other cycle lengths are not divisible by k;*

(b) *if $H = \mathrm{SU}_n(q)$, then k is odd, w contains a k-cycle, and all other cycle lengths are not divisible by k;*

(c) *if $H = \mathrm{Sp}_{2n}(q), \mathrm{SO}_{2n+1}(q)$, or $\mathrm{SO}^{\pm}_{2n}(q)$, then w contains a unique negative cycle of length k (that is, its image in S_n has length k). Moreover, k does not divide the length of any other cycle, positive or negative.*

4.2 Proportions of elements in tori which lie in Q

Our aim in this subsection is to find good upper and lower bounds for $|T_C \cap Q_k|/|T_C|$ for a given F-conjugacy class C of W.

The following $O(1/\log(m))$ lower bound for $\varphi(m)/m$ is well known (see for example (Niemeyer and Praeger, 1998, Lemma 10.6)), where $\varphi(m)$ is the Euler phi-function, that is, the number of positive integers less than m and coprime to m.

Lemma 4.3 *For all integers m with $m \geq 3$ there is a constant a such that $\varphi(m)/m \geq a \log\log(m)/\log(m)$ and in particular $\varphi(m)/m \geq \frac{\log(2)}{\log(m)}$.*

Lemma 4.4 *Let C be an F-conjugacy class of W and T_C a representative of the corresponding class of F-stable maximal tori. Let k be an integer such that $k \geq \log(n)$ and $9 < q^k$. Then*

(a) If $T_C \cap Q_k \neq \emptyset$, then $1 - \frac{2}{q^{k/2}} \leq \frac{|T_C \cap Q_k|}{|T_C|} \leq 1$.

(b) If $T_C \cap Q_k^{\mathrm{ppd}} \neq \emptyset$, then $1 - \frac{1}{\alpha k} \leq \frac{|T_C \cap Q_k^{\mathrm{ppd}}|}{|T_C|} \leq 1$ with α as in Table 1.

(c) If $T_C \cap Q_k^{\mathrm{full}} \neq \emptyset$, then $\frac{\log(2)}{k \log(q+1)} \leq \frac{|T_C \cap Q_k^{\mathrm{full}}|}{|T_C|} \leq 1$.

Proof: Clearly the upper bound holds in all three cases. Statement (a) is proved in the proof of (Niemeyer et al., 2014, Lemma 4.3(a)).

To prove part (b) let $m = \alpha k$, with α as in Table 1. Since $T_C \cap Q_k^{\mathrm{ppd}} \neq \emptyset$ the abelian group T_C contains elements of order divisible by a primitive prime divisor r of $q^{\delta m} - 1$. All elements of T_C lying outside a subgroup of index r have order divisible by r, and hence the proportion of such elements in T_C is at least $1 - \frac{1}{r} > 1 - \frac{1}{m}$, as $r \geq m + 1$. Thus the result follows.

For part (c), note that the F-stable maximal torus T_C contains a direct factor Z of order $\ell := q^k - 1$ or $q^k + 1$. If $t \in T_C$ is such that its projection $\pi(t)$ onto Z generates Z, then t lies in Q_k^{full} since the r-part r^a of $q^k - 1$ or $q^{2k} - 1$, respectively, divides ℓ, and hence divides $|\pi(t)|$. The number of generators of $\pi(T_C)$ is at least $\varphi(q^k - 1)$ or $\varphi(q^k + 1)$, respectively. Hence a lower bound for $|T_C \cap Q_k^{\mathrm{full}}|/|T_C|$ is $\varphi(\ell)/\ell$. By Lemma 4.3, $\varphi(\ell)/\ell \geq \log(2)/\log(\ell)$ which is at least $\log(2)/k \log(q + 1)$ since $\log(\ell) \leq \log(q^k + 1) \leq \log((q + 1)^k)$. □

4.3 Proportions of elements in symmetric groups

Let n, m be positive integers with $m < n$, and let $b_m(n)$ denote the proportion of elements in the symmetric group S_n with exactly one cycle of length m and all other cycle lengths not divisible by m.

Lemma 4.5 *If $m \geq 3$ and $\log(n) \leq m \leq n - m$, then $\frac{1}{3em} \leq b_m(n) \leq \frac{5}{3m}$.*

Proof: Let $p_{\neg m}(n - m)$ denote the proportion of elements in S_{n-m} which contain no cycle of length divisible by m. Observe first that $b_m(n) = \frac{1}{m} p_{\neg m}(n - m)$. Putting $c(j) = \frac{1}{\Gamma(1-1/j)}$ and applying the inequality derived from (Beals et al., 2002, Theorem 2.3(b)) in the proof of (Lübeck et al., 2009, Lemma 4.2) we have

$$\frac{m^{1/m} c(m)}{m(n-m)^{1/m}} \left(1 - \frac{1}{n-m}\right) \leq b_m(n) \leq \frac{m^{1/m} c(m)}{m(n-m)^{1/m}} \left(1 + \frac{2}{n-m}\right).$$

By our hypothesis $n - m \geq 3$, and also $1/2 \leq c(m) \leq 1$. Hence

$$\frac{1}{3} \frac{m^{1/m}}{m(n-m)^{1/m}} \leq b_m(n) \leq \frac{5}{3} \frac{m^{1/m}}{m(n-m)^{1/m}}.$$

Now $\left(\frac{m}{n-m}\right)^{1/m} \leq 1$ since $m \leq n - m$. This gives the required upper bound. We claim that $\left(\frac{m}{n-m}\right)^{1/m} \geq \frac{1}{e}$, or equivalently, $e^m \geq (n - m)/m$. To see that this is true, observe that, since $m \geq \log(n)$, we have $e^m \geq e^{\log(n)} = n > (n - m)/m$. This proves the claim and yields the required lower bound. □

4.4 Proof of Theorem 3.3

Let Q denote one of the sets Q_k, Q_k^{ppd} or Q_k^{full}, where $k \geq \log(n)$. By Theorem 4.1,

$$\frac{|Q|}{|H|} = \sum_C \frac{|C|}{|W|} \frac{|Q \cap T_C|}{|T_C|},$$

where the sum is over all F-conjugacy classes C of W, and T_C is a representative of the H-conjugacy class of F-stable maximal tori corresponding to C such that $T_C \cap Q \neq \emptyset$. By Lemma 4.4, we see that $\ell_{k,Q}$, as defined in Table 2, is a uniform lower bound for each non-zero $|T_C \cap Q|/|T_C|$ and we use 1 as a uniform upper bound for this quantity.

In lines 1 and 2 of Table 1, the proportion $\sum_C |C|/|W|$ is equal to $b_k(n)$, as defined in Section 4.3. In lines 3–5 of Table 1, the F-conjugacy classes C which correspond to tori containing elements of Q_k are those with one negative cycle of length k and no other cycles of length divisible by k. By (Lübeck et al., 2009, Lemma 4.2(c,d)) it follows that $\sum_C |C|/|W| = b_k(n)/2$. Thus in all cases $\sum_C |C|/|W| = b_k(n)/\alpha$, with α as in Table 1. The upper and lower bounds for part (a) now follow, since by Lemma 4.5 $1/(3e\alpha k) \leq b_n(k) < 5/(3\alpha k)$.

To see that part (b) holds, assume that $\log(n) < k \leq 2\log(n)$. The upper bound follows immediately from (a) since $k > \log(n)$. Similarly the lower bound follows using the bounds on k to obtain the lower bound $m_{n,Q}$ for $\ell_{k,Q}$ with k in the given range. □

4.5 Proof of Theorem 1.1

The upper bound follows immediately from Theorem 3.3. For the lower bound for Q_k and Q_k^{ppd} we may choose $Q = Q_k^{\mathrm{ppd}}$. Observe that the quantity $\ell_{k,Q}$ in Table 2 is at least $\ell_{k,Q} \geq 1 - 1/(\alpha k) \geq 2/3$ since $\alpha k \geq 3$. Then by Theorem 3.3, $|Q|/|H| \geq 2/(9e\alpha k)$. The lower bound for Q_k^{full} follows immediately from Theorem 3.3. □

Acknowledgements

The authors express their sadness at the recent passing of their colleague Ákos Seress, and wish to acknowledge his pivotal role in formulating the problem addressed in this paper, and indeed their appreciation of working with him over a number of years. The paper was originally submitted in December 2011 for the issue celebrating the sixtieth birthday of László Babai, and the authors extend very belated congratulations to Laci. The authors also thank Frank Lübeck for many valuable suggestions on the exposition. The research forms part of Australian Research Council Discovery Grants DP110101153 and DP140100416. The first author acknowledges a DFG grant in SPP1489. During the writing of this paper the second author was supported by Australian Research Council Federation Fellowship FF0776186.

References

R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, and Á. Seress. Permutations with restricted cycle structure and an algorithmic application. *Combin. Probab. Comput.*, 11(5):447–464, 2002. ISSN 0963-5483. doi: 10.1017/S0963548302005217. URL `http://dx.doi.org/10.1017/S0963548302005217`.

R. W. Carter. *Finite groups of Lie type*. Wiley Classics Library. John Wiley & Sons Ltd., Chichester, 1993. ISBN 0-471-94109-3. Conjugacy classes and complex characters, Reprint of the 1985 original, A Wiley-Interscience Publication.

H. Dietrich, C. Leedham-Green, F. Lübeck, and E. O'Brien. Constructive recognition of classical groups in even characteristic. *J. Algebra*, 391:227–255, 2013.

I. M. Isaacs, W. M. Kantor, and N. Spaltenstein. On the probability that a group element is p-singular. *J. Algebra*, 176(1):139–181, 1995. ISSN 0021-8693. doi: 10.1006/jabr.1995.1238. URL http://dx.doi.org/10.1006/jabr.1995.1238.

W. M. Kantor and Á. Seress. Black box classical groups. *Mem. Amer. Math. Soc.*, 149(708):viii+168, 2001. ISSN 0065-9266.

C. R. Leedham-Green and E. A. O'Brien. Constructive recognition of classical groups in odd characteristic. *J. Algebra*, 322(3):833–881, 2009. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2009.04.028. URL http://dx.doi.org/10.1016/j.jalgebra.2009.04.028.

G. I. Lehrer. Rational tori, semisimple orbits and the topology of hyperplane complements. *Comment. Math. Helv.*, 67(2):226–251, 1992. ISSN 0010-2571. doi: 10.1007/BF02566498. URL http://dx.doi.org/10.1007/BF02566498.

F. Lübeck, A. C. Niemeyer, and C. E. Praeger. Finding involutions in finite Lie type groups of odd characteristic. *J. Algebra*, 321(11):3397–3417, 2009. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2008.05.009. URL http://dx.doi.org/10.1016/j.jalgebra.2008.05.009.

M. Neunhöffer and Á. Seress. Constructive recognition of $\mathrm{SL}_n(q)$. in preparation.

M. Neunhöffer and Á. Seress. GAP package recog, version 1.2. Technical report, 2012. URL (http://www.gap-system.org/Packages/recog.html).

A. C. Niemeyer and C. E. Praeger. A recognition algorithm for classical groups over finite fields. *Proc. London Math. Soc. (3)*, 77(1):117–169, 1998. ISSN 0024-6115. doi: 10.1112/S0024611598000422. URL http://dx.doi.org/10.1112/S0024611598000422.

A. C. Niemeyer and C. E. Praeger. Estimating proportions of elements in finite groups of Lie type. *J. Algebra*, 324(1):122–145, 2010. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2010.03.018. URL http://dx.doi.org/10.1016/j.jalgebra.2010.03.018.

A. C. Niemeyer, T. Popiel, and C. E. Praeger. Abundant p-singular elements in finite classical groups. *J. Algebra*, 408:189–204, 2014.

I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons Inc., New York, fifth edition, 1991. ISBN 0-471-62546-9.

C. E. Praeger, Á. Seress, and Ş. Yalçınkaya. Generation of finite classical groups by pairs of elements with large fixed point spaces. *J. Algebra*, to appear.

K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892. ISSN 0026-9255. doi: 10.1007/BF01692444. URL http://dx.doi.org/10.1007/BF01692444.