(2017.11)

STRONG INVOLUTIONS IN FINITE SPECIAL LINEAR GROUPS OF ODD CHARACTERISTIC

JOHN D. DIXON, CHERYL E. PRAEGER, AND ÁKOS SERESS

ABSTRACT. Let t be an involution in $\mathrm{GL}(n,q)$ whose fixed point space E_+ has dimension k between $n/3$ and $2n/3$. For each $g \in \mathrm{GL}(n,q)$ such that tt^g has even order, $\langle tt^g \rangle$ contains a unique involution $z(g)$ which commutes with t. We prove that, with probability at least $c/\log n$ (for some $c > 0$), the restriction $z(g)_{|E_+}$ is an involution on E_+ with fixed point space of dimension between $k/3$ and $2k/3$. This result has implications in the analysis of the complexity of recognition algorithms for finite classical groups in odd characteristic. We discuss how similar results for involutions in other finite classical groups would solve a major open problem in our understanding of the complexity of constructing involution centralisers in those groups.

1. INTRODUCTION

The 2001 paper of Altseimer and Borovik [1] marked a break-through in computational group theory by using involution centralisers to distinguish between the simple Lie type groups $\mathrm{PSp}(2n,q)$ and $\Omega(2n+1,q)$, with q odd. These are groups which share many properties, such as having the same order, and they had proved difficult to distinguish computationally. The paper [1] inspired the work of Parker and Wilson [11] who demonstrated that involution-centraliser methods could be used for solving several problems previously believed to be computationally difficult, and gave complexity analyses for methods to construct involutions and their centralisers in quasisimple Lie type groups in odd characteristic. These methods were based on Bray's algorithm [2] for constructing involution centralisers in finite groups. Our aim is to improve the analysis given by Parker and Wilson of Bray's algorithm in the case of finite special linear groups in odd characteristic. This is

This work was partially supported by ARC Grant DP160102323. The work for this paper was begun by the second and third authors in 2008, and early written drafts of the analysis, by both of these authors, date back to then. The paper was completed by the first and second authors after the death of their colleague Ákos Seress in February 2013. **2010 Mathematics Subject Classification:** 20G40, 20F69, 20D60, 20P05, 68W20. **Key words:** Finite classical groups, involution centralisers, recognition algorithms.

part of a program to improve the complexity analyses of a number of algorithms for computing with Lie type groups. In particular, we focus on its application in the recognition algorithm for special linear groups of Leedham-Green and O'Brien in [7]. In the rest of this section we give a brief overview of these applications to set the scene for our main result Theorem 1.1, and to pose some open problems.

1.1. **Algorithmic backgrond.** Leedham-Green and O'Brien [7] describe and analyse an algorithm which constructs a 'standard generating set' for a finite classical group $G = \mathrm{SX}(n, q)$ (q odd) in its natural representation. Here (abusing the notation in [7] slightly) SX is one of $\mathrm{SL}, \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^\varepsilon$, or Ω^ε, where $\varepsilon \in \{+, -, \circ\}$. In [7, Section 3] the authors define a standard generating set for SX (see especially [7, Table 1] for all groups except those of type Ω^ε, and [7, Lemmas 3.2-3.4] for those of type Ω^ε). The algorithm is recursive in the sense that it finds a certain direct decomposition $V_m \oplus V_{n-m}$ of the underlying n-dimensional vector space, where $\dim(V_m) = m$, $\frac{n}{3} \leq m \leq \frac{2n}{3}$ and the decomposition is orthogonal if $\mathrm{SX} \neq \mathrm{SL}$. It then constructs classical groups acting on each of V_m and V_{n-m} and finds standard generators for them recursively. The algorithm concludes by 'patching together' these standard generating sets for the subgroups to obtain standard generators for G.

The key challenge is to obtain an appropriate direct decomposition $V_m \oplus V_{n-m}$ and construct the classical subgroups acting on each direct summand. This is done in [7] by finding an involution $t \in G$ with ± 1-eigenspaces of suitable dimensions $m, n - m$, then constructing (the second derived subgroup of) its centraliser $C_G(t)$, and extracting the central 'factors' of $C_G(t)$ induced on the eigenspaces of t.

The analysis given in [7] is based on the construction of $O(n)$ random elements at several stages in the algorithm (see [7, bottom of page 835]). O'Brien mentioned in private communication to the second and third authors, probably in 2008, that the practical performance of the algorithm was much faster than the analysis in [7] suggested. He wondered whether the number of random elements required may be much smaller than a multiple of n.

We briefly discuss the steps in the algorithm in [7] where it was estimated, in [7], that $O(n)$ random elements might be needed. We highlight where subsequent improvements on these estimates are available, and where more work is still needed. Our comments, in particular, refer to improvements on the complexity analysis in [11] for finding involution centralisers in finite classical groups in odd characteristic.

Step 1. Finding the involution t. An involution $t \in G$ with ± 1-eigenspaces having dimensions in the interval $[\frac{n}{3}, \frac{2n}{3}]$ is said to be a *strong involution*. Involutions are constructed in [7] by finding an element $g \in G$ of even order, by random selection, and computing the involution $g^{|g|/2}$. For any $g \in G$, let us write $\mathrm{inv}(g)$ for the involution obtained from g in this way (and set $\mathrm{inv}(g) = I$ if g has odd order). By [7, Theorem 8.12], examination of a constant multiple of n random elements suffices to find, with high probability, an even ordered element g such that $\mathrm{inv}(g)$ is a strong involution. This estimate was improved by Lübeck, Niemeyer and the second author in [8, Theorem 1.1] to show that only $O(\log n)$ random elements were needed for this step.

Step 2. Finding $C_G(t)$: Bray's algorithm. This is the critical step and uses ideas of John Bray ([2, Section 2], see also [11, Theorem 10]). Let $g \in G$, and note that $D := \langle t, t^g \rangle$ is a dihedral group. Bray observed that, if the product tt^g has odd order $2s+1$, then $g(tt^g)^s$ commutes with t; while if tt^g has even order, then both $\mathrm{inv}(tt^g)$ and $\mathrm{inv}(tt^{g^{-1}})$ commute with t, as they are the central involutions in the dihedral groups $D, D^{g^{-1}}$, respectively. Moreover, if g is (nearly) uniformly distributed among the elements of G for which tt^g has odd order (the 'odd case'), then Richard Parker showed that $g(tt^g)^s$ is (nearly) uniformly distributed among the elements of $C_G(t)$ (see [2, Theorem 3.1] or [11, Theorem 11]). On the other hand, if g is uniformly distributed among the elements of G for which tt^g has even order (the 'even case'), then each of $\mathrm{inv}(tt^g)$ and $\mathrm{inv}(tt^{g^{-1}})$ is uniformly distributed among the elements of the $C_G(t)$-conjugacy class containing it. (Note that if $x = \mathrm{inv}(tt^g)$ is obtained precisely for the elements $g \in \{g_1, \ldots, g_N\}$ then, for $y \in C_G(t)$, $x^y = \mathrm{inv}(tt^g)$ precisely for $g \in \{g_1^y, \ldots, g_N^y\}$.)

Although involutions in $C_G(t)$ obtained from the even case are 'gratefully accepted' and used in implementations of Bray's algorithm, complexity analyses up to the present have been unable to take them into account because of their relatively poor randomisation properties (see for example [6, Section 3], [7, Theorem 12.3], or [11, Theorem 2]). Indeed, Parker and Wilson [11, Theorem 2] prove that, for a uniformly distributed random element $g \in G$, the product tt^g has odd order (that is, the 'odd case' occurs) with probability at least c/n for some constant c. Hence $O(n)$ random elements suffice to obtain, with high probability, a random element of $C_G(t)$. This result underpins the analyses in [6, 7] which use the estimate of $O(n)$ random elements for this step of their algorithms.

A series of computer experiments conducted by the third author indicated that the even case does indeed occur much more frequently

than the odd case. Moreover when t is a strong involution, then fairly often an element $z = \mathrm{inv}(tt^g)$ obtained in $C_G(t)$ in the even case induces a balanced involution on each eigenspace of t, that is to say, there are constants α, β satisfying $0 < \alpha < \beta < 1$ such that, if the ± 1-eigenspace $E_\pm(t)$ of t has dimension k, then the involution induced by z on $E_\pm(t)$ has fixed-point space of dimension in the range $[\alpha k, \beta k]$. Such an involution in a k-dimensional classical group is said to be (α, β)-*balanced*. The major result Theorem 1.1 of [12] is critical for the analysis of Bray's algorithm for balanced involution centralisers: namely, consider $H = \mathrm{SY}(k, q)$ (q odd) in its natural representation, where SY is one of $\mathrm{SL}, \mathrm{SU}, \mathrm{Sp}$ or SO^ε. Then, for given α, β such that $0 < \alpha < \frac{1}{2} < \beta < 1$, there is an explicitly computable constant $c = c(\alpha, \beta)$ such that, with probability at least $1 - q^{-k}$, H will be generated by a sequence $(x_1, \ldots, x_c)$ of (α, β)-balanced involutions of H such that each x_i is random and uniformly distributed in its H-conjugacy class.

Since elements $z \in C_G(t)$ constructed from the even case of Bray's algorithm possess this randomisation property, it follows that, with high probability, a constant number of such elements z, which are in addition (α, β)-balanced on the t-eigenspaces, will generate (the second derived subgroup of) $C_G(t)$. Given this result, the missing link in the program to improve the analysis of Bray's algorithm for strong involutions is therefore *a more realistic estimate for the number of random elements needed to produce an element z in the 'even case' such that, in addition, z induces an (α, β)-balanced involution on a t-eigenspace*. Our main result Theorem 1.1 addresses this problem in the case $(\alpha, \beta) = (\frac{1}{3}, \frac{2}{3})$ for special linear groups. Theorem 1.1 implies that, for a strong involution t in $G = \mathrm{SL}(n, q)$, only $O(\log n)$ random elements are required to obtain a strong involution in the induced action on a t-eigenspace, and hence on average only $O(\log n)$ elements are required in Bray's algorithm to construct the second derived subgroup of $C_G(t)$.

Theorem 1.1. [Main Theorem] *There exist positive constants κ and n_0 such that the following is true. Suppose that $n \geq n_0$, that t is a strong involution in $\mathrm{GL}(n, q)$, and that g is a uniformly distributed random element of $\mathrm{GL}(n, q)$. Let $z(g) := \mathrm{inv}(tt^g)$ (recalling that $\mathrm{inv}(tt^g) := I$ if $|tt^g|$ is odd), and let $z(g)_\varepsilon$ be the restriction of $z(g)$ to the eigenspace $E_\varepsilon(t)$ ($\varepsilon = +$ or $-$). Then*

(i) $z(g)_+$ is a strong involution with probability at least $\kappa/\log n$; and
(ii) $z(g)_-$ is a strong involution with probability at least $\kappa/\log n$.

Remark 1.2. (a) The proof shows that we can take $n_0 = 700$ and $\kappa = 0.0002$ but we believe that these constants are far from best possible.

(b) We comment on the reason for considering elements t, g in $\mathrm{GL}(n,q)$ rather than $\mathrm{SL}(n,q)$. Our aim is to construct the centraliser of an involution t. In the discussion above we consider products tt^g (where g is random in $\mathrm{GL}(n,q)$). Such products always have determinant 1 (since t and t^g have the same determinant ± 1) and so these products lie in $\mathrm{SL}(n,q)$, and hence the involutions we construct $z = \mathrm{inv}(tt^g)$ also lie $\mathrm{SL}(n,q)$. However, the restrictions z_+ and z_- may or may not lie in the special linear groups on the eigenspaces $E_+(t)$ and $E_-(t)$ respectively, and the groups induced by the centraliser of t on these spaces are general linear groups. Thus recursively we must consider elements t, g in general linear groups.

To complete a similar improvement of this step of Bray's algorithm for the other classical groups we need an analogue of Theorem 1.1 for them.

Problem 1.3. *Prove an analogue of Theorem* 1.1 *with a similar bound for the other classical groups.*

Step 3. Extracting the 'factors' of $C_G(t)$. This step is discussed and analysed in [7, Section 11]. A linear transformation x on a space V over $\mathbb{F}_q$ is called a *ppd-element* if there is an x-invariant subspace U of V such that: (i) x is irreducible on U; (ii) $e := \dim U > \frac{1}{2}\dim V$; and (iii) the order of x is divisible by a primitive prime divisor (ppd) of $q^e - 1$ (that is, a prime divisor r of $q^e - 1$ such that $r \nmid q^i - 1$ for all $i < e$). The basic idea in Step 3 is to find elements $x \in C_G(t)$ such that the induced action of some power x^s on one of the eigenspaces, $E_+(t)$ or $E_-(t)$, is a ppd-element, and such that x^s fixes the other eigenspace pointwise.

The analysis is based on the theory of ppd-elements developed in [5, 9, 10], and shows that $O(\log\log n)$ random elements from $C_G(t)$ are sufficient to find, with high probability, suitable ppd-elements to construct the factors (see [7, Theorem 11.10] and other results in [7, Sections 13 and 14] for small dimensions).

Thus application of Theorem 1.1 reduces, for $\mathrm{SL}(n,q)$, estimates of the number of random elements required for the algorithms in [6, 7, 11] from $O(n)$ to $O(\log n)$. A solution to Problem 1.3 would yield the same improvement for the other classical groups.

The rest of the paper is devoted to proving Theorem 1.1. We discuss aspects of dihedral subgroups of $\mathrm{GL}(n,q)$ in Section 2, some preliminary inequalities in Section 3, estimates related to coefficients in various power series in Section 4, and we complete the proof of Theorem 1.1 in Section 5.

1.2. **Outline of the proof of the Main Theorem.** The remainder of the paper consists of the proof of Theorem 1.1. As an aid to the reader we outline the steps involved.

Throughout the paper q denotes a power of an odd prime.

The proof begins with an analysis of dihedral subgroups $\langle t, y\rangle$ of $\mathrm{GL}(n, q)$, where $t^2 = I$ and $t^{-1}yt = y^{-1}$ (Section 2). We are particularly concerned with the case where y has even order, and we use $\mathrm{inv}(y)$ to denote the involution in $\langle y\rangle$. It turns out (Remark 2.6) that the analysis is significantly easier in the case where the characteristic polynomial $c_y(X)$ of y lies in the set $\Pi(n, q)$, namely, when $c_y(X)$ has no repeated roots and neither 1 nor -1 is a root of $c_y(X)$ (Definition 2.4). In particular, polynomials $c_y(X)$ with this property are separable, and admit a factorisation (1) as a product of pairwise distinct $*$-irreducible polynomials (a monic polynomial is $*$-irreducible if it is either a self-conjugate irreducible polynomial or a product of two distinct conjugate irreducible polynomials). The set of pairs (t, y) with $c_y(X) \in \Pi(n, q)$ is denoted by $\Delta(n, q)$; note that $\Pi(n, q)$ and $\Delta(n, q)$ are non-empty only when n is even (Definition 2.5). When $c_y(X) \in \Pi(n, q)$, the separability of $c_y(X)$ implies that the elements of $\mathrm{GL}(n, q)$ with characteristic polynomial $c_y(X)$ lie in a single conjugacy class. Both the size of the class, and the type of the involution $\mathrm{inv}(y)$ associated with $(t, y) \in \Delta(n, q)$, are determined by $c_y(X)$ (Lemma 2.8 and Corollary 2.15).

Corollary 2.12 explains how the 2-part of the multiplicative order of the roots of a $*$-irreducible polynomial is related to the 2-part of the degree of the polynomial, and this provides an important way to estimate the number of pairs $(t, y) \in \Delta(n, q)$ for which the involution $\mathrm{inv}(y)$ has a particular type.

Most of the paper is an analysis of pairs $(t, y) \in \Delta(n, q)$. Only in the final Section 5 do we relax this condition and consider a more general situation (Definition 5.2).

Controlling the proportion of eigenvalues of y whose orders have maximal 2-part enables us to control the dimensions of the eigenspaces of $\mathrm{inv}(y)$. We estimate the probability of finding suitable involutions $\mathrm{inv}(y)$ through a careful analysis of various generating functions. First we consider a generating function related to the sets $\Delta(n, q)$, namely $R(q, u) := \sum_{n=0}^{\infty} r(2n, q)u^n$, where $r(2n, q) := \frac{|\Delta(2n,q)|}{|\mathrm{GL}(2n,q|}$ (recall $\Delta(n, q) = \emptyset$ when n is odd). It is known ([13, Section 5]) that

$$R(q, u) = \frac{1}{1 + u/(q-1)} \prod_{n=1}^{\infty} \left(1 + \frac{u^n}{q^n - 1}\right)^{N(q,n)}$$

where $N(q,n)$ denotes the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$. For each n, there is a factor $1+u^n/(q^n-1)$ corresponding to each of these $N(q,n)$ polynomials (in the case of $n=1$ one of these factors is cancelled by the initial factor $(1+u/(q-1))^{-1}$). In order to estimate the distribution of the type of $\mathrm{inv}(y)$, as (t,y) runs over $\Delta(2n,q)$, we use the related quantities

$$R_b(q,u)=\frac{1}{1+u/(q-1)}\prod_{2^{b+1}\nmid n}\left(1+\frac{u^n}{q^n-1}\right)^{N(q,n)}$$

for $b=1,2,\ldots$. These are the corresponding generating functions for the numbers $r_b(2n,q):=\frac{|\Delta_b(2n,q)|}{|\mathrm{GL}(2n,q)|}$ (see (5)). In the infinite product for $R_b(q,u)$, the monic irreducible polynomials which correspond to the factors are limited to those of degree not divisible by 2^{b+1}. We also need to consider a certain subset of monic irreducble polynomials for which the degree is divisible by 2^{b+1} but not by 2^{b+2}. We do this via the additional function

$$G_b^0(q,u):=\prod_{m\ odd}\left(1+\frac{u^{2^bm}}{q^{2^bm}-1}\right)^{N^0(q,2^{b+1}m)}$$

where $N^0(q,2^{b+1}m)$ is defined just before Corollary 2.12; in particular $N^0(q,2^{b+1}m)\leq N(q,2^{b+1}m)$. Then, as discussed in Remark 2.16, $|\mathrm{GL}(2k,q)|$ times the coefficient of u^kz^ℓ in $R_b(q,u)G_b^0(q,uz)$ provides a lower bound for the number of pairs $(t,y)\in\Delta(2k,q)$ such that $\mathrm{inv}(y)$ is of type $(2k-2\ell,2\ell)$. This bound is simplified by introducing a further generating function $F_b(q,u)$ in (7).

In Section 4, we compute bounds on the coefficients $r(2n,q)$ and $r_b(2n,q)$, and on the coefficients of $F_b(q,u)$ (Lemma 4.1, Lemma 4.5 and Lemma 4.6). These estimates are used in Section 5.

In the final Section 5 we complete the proof of Theorem 1.1. We begin by estimating the number $|J(2m,q;\alpha,\beta)|$ of pairs $(t,y)\in\Delta(2m,q)$ such that $\mathrm{inv}(y)$ is (α,β)-balanced (Lemma 5.1). However, this is not enough since Theorem 1.1 refers to the restrictions of $\mathrm{inv}(y)$ to the eigenspaces $E_+(t)$ and $E_-(t)$ of t. To analyse these restrictions we must consider a more general situation where the underlying space V is a direct sum $V_1\oplus V_2$ of $\langle t,y\rangle$-invariant subspaces such that $t_{|V_1}=y_{|V_1}=I$ and $(t_{|V_2},y_{|V_2})\in\Delta(2k,q)$ for some $k\leq m$ (see Definition 5.2). The final arguments show that there are sufficiently many pairs (t,t^g) with $g\in\mathrm{GL}(2n,q)$ and $y=tt^g$ in this more general situation such that conclusions (i) and (ii) of Theorem 1.1 are satisfied.

Acknowledgement 1.4. The authors wish to thank Stephen Glasby, Eamonn O'Brien, and two anonymous referees, for suggestions which improved the exposition of this paper. In particular we thank Eamonn for encouraging us to simplify the title. The paper under a longer title was referred to in the list of references for [12] (reference [17] in that paper).

2. Dihedral subgroups of $\mathrm{GL}(n,q)$

We only consider fields of odd characteristic, and in the rest of this paper q will denote a power of an odd prime.

An involution in $\mathrm{GL}(n,q)$ is an element t such that $t^2 = 1$. We consider the identity map I as the 'trivial' involution, and if the order $|t| = 2$, we call t 'proper'. For an involution $t \in \mathrm{GL}(n,q)$, the underlying vector space $V := \mathbb{F}_q^n$ is a direct sum of the eigenspaces of t, namely $V = E_+(t) \oplus E_-(t)$, where t acts as the identity I on $E_+(t)$ and as $-I$ on $E_-(t)$. If the dimensions of these eigenspaces are n_+ and n_-, respectively, then we say that t is of *type* (n_+, n_-). Two involutions are of the same type if and only if they are conjugate in $\mathrm{GL}(n,q)$ so, apart from the trivial involution which has type $(n,0)$, there are n conjugacy classes of (proper) involutions.

Given $0 \le \alpha < \beta \le 1$ we say, as in Section 1, that an involution of type (n_+, n_-) in $\mathrm{GL}(n,q)$ is (α,β)-*balanced* if $\alpha \le n_+/n \le \beta$, and we say that a $(\frac{1}{3},\frac{2}{3})$-balanced involution is *strong*.

An element $y \in \mathrm{GL}(n,q)$ is called *self-conjugate* if y and y^{-1} are conjugate in $\mathrm{GL}(n,q)$. For any polynomial $f(X) \in \mathbb{F}_q[X]$ with no roots equal to 0, we define the *conjugate* (monic) polynomial $f^*(X) := f(0)^{-1} X^{\deg f} f(X^{-1})$, where $\deg f$ is the degree of $f(X)$, and we call $f(X)$ *self-conjugate* if $f(X) = f^*(X)$ (this can only happen if $f(X)$ is monic). We define the characteristic polynomial of an element $y \in \mathrm{GL}(n,q)$ as $c(X) := \det(XI - y)$, so $c(X)$ is always monic. Note that y is self-conjugate if and only if its characteristic polynomial $c(X)$ is self-conjugate. The self-conjugate polynomials of degree 1 are $X+1$ and $X-1$. Since a finite field is perfect, each irreducible polynomial over $\mathbb{F}_q$ is *separable*, that is to say, it has no repeated roots in its splitting field. In particular, it is clear that the roots of an irreducible self-conjugate polynomial of degree greater than 1 come in pairs α, α^{-1}, and so irreducible self-conjugate polynomials of degree greater than 1 have even degree (see, for example [4, Lemma 1.3.15 (c)]).

A dihedral subgroup D of $\mathrm{GL}(n,q)$ is a subgroup generated by two elements t, y such that $t^2 = I$ and $t^{-1}yt = tyt = y^{-1}$. Note that also $(ty)^2 = I$. Conversely, if t and t' are involutions and we define $y := tt'$,

then $t^{-1}yt = y^{-1}$ and $\langle t, t' \rangle = \langle t, y \rangle$ is a dihedral group. We allow the trivial case where $t = I$. In the nontrivial case where t is a proper involution, $|D| = 2m$ where m is the order of the normal subgroup $\langle y \rangle$.

Lemma 2.1. *Let $D = \langle t, y \rangle$ be an irreducible dihedral subgroup of $\mathrm{GL}(n, q)$ with $t^2 = I$ and $t^{-1}yt = y^{-1}$, and let $c(X)$ be the characteristic polynomial of y.*

1. *If $n = 1$, then D is cyclic and the only possibilities are: $(t, y) = (I, I)$, $(I, -I)$, $(-I, I)$ or $(-I, -I)$.*
2. *If $n > 1$, then n is even, and one of the following holds:*
   - (a) *$\langle y \rangle$ is an irreducible subgroup of $\mathrm{GL}(n, q)$ and $c(X)$ is an irreducible self-conjugate polynomial of degree n;*
   - (b) *$\langle y \rangle$ is a reducible subgroup and the underlying vector space is a direct sum of two $\langle y \rangle$-irreducible subspaces; $c(X)$ is a product $c_1(X)c_1^*(X)$ where $c_1(X)$ and $c_1^*(X)$ are monic irreducible polynomials of degree $n/2$.*

Proof. Note that y is self-conjugate, since y is conjugate to y^{-1}. The case $n = 1$ is clear since $\mathrm{GL}(1, q) \cong Z_{q-1}$, so all dihedral subgroups are cyclic and have orders at most 2. Suppose now that $n > 1$.

Let V be the underlying vector space. Since q is odd and D is irreducible on V, the normal subgroup $H := \langle y \rangle$ is completely reducible by Clifford's theorem. Let W be an irreducible H-subspace. Then Wt is also an irreducible H-subspace because $Wty = Wy^{-1}t = Wt$. Since $W + Wt$ is invariant under both y and t, and V is irreducible under D, we have $V = W + Wt$. On the other hand W is an irreducible H-subspace, so the H-subspace $W \cap Wt = W$ or $\{0\}$. Thus either $V = W$ or $V = W \oplus Wt$. The characteristic polynomial $c(X)$ is self-conjugate since y is.

If $V = W$ then V is H-irreducible and so $c(X)$ is irreducible. This proves part 2(a).

If $V = W \oplus Wt$ then let $c_1(X)$ (respectively, $c_2(X)$) be the characteristic polynomial of y restricted to W (respectively, Wt). These polynomials are irreducible of degree $n/2$ because W and Wt are irreducible H-subspaces of dimension $n/2$. Since $c_2(X)$ is irreducible, it is the minimal polynomial of y acting on Wt. However, $Wtc_1(y^{-1})y^{n/2} = Wc_1(y)ty^{n/2} = 0$ and so $c_2(X)$ divides $c_1(0)^{-1}X^{n/2}c_1(X^{-1}) = c_1^*(X)$. Since $c_1^*(X)$ and $c_2(X)$ are both monic of degree $n/2$, we conclude that $c_2(X) = c_1^*(X)$. This proves part 2(b). □

We can say more. Summarizing [13, Lemmas 2.2 and 2.4] we have the following information, which we state without proof.

Lemma 2.2. *Suppose that y is a self-conjugate element of order m in $\mathrm{GL}(n,q)$, where n is even, and let $c(X)$ be its characteristic polynomial.*

(i) *If $c(X)$ is irreducible then $m \mid (q^{n/2}+1)$ and y is inverted by precisely $q^{n/2}+1$ involutions in $\mathrm{GL}(n,q)$.*

(ii) *If $c(X) = c_1(X)c_1^*(X)$, for a monic irreducible polynomial $c_1(X)$ such that $c_1(X) \neq c_1^*(X)$, then $m \mid (q^{n/2}-1)$ and y is inverted by precisely $q^{n/2}-1$ involutions in $\mathrm{GL}(n,q)$.*

Moreover, in both cases each involution inverting y is of type $(\frac{n}{2},\frac{n}{2})$.

Remark 2.3. The claim in Lemma 2.2 (ii) that $m \mid (q^{n/2}-1)$ follows from the fact that the roots of the irreducible polynomials $c_1(X)$ and $c_1^*(X)$ lie in the group $\mathbb{F}^*_{q^{n/2}}$. These roots are the eigenvalues of y and so have order m.

Recall that a polynomial is separable if it has no multiple roots in its splitting field. We will study the following set of separable polynomials.

Definition 2.4. Let $\Pi(n,q)$ be the set of all separable self-conjugate (monic) polynomials $f(X) \in \mathbb{F}_q[X]$ with no root equal to $0, 1$ or -1. Note that each $f(X) \in \Pi(n,q)$ can be factorised uniquely into pairwise distinct factors over $\mathbb{F}_q$

$$f(X) = f_1(X)\dots f_k(X) \tag{1}$$

where each $f_i(X)$ is a monic self-conjugate polynomial which is either (i) irreducible, or (ii) a product $g_i(X)g_i^*(X)$ of monic irreducible polynomials over $\mathbb{F}_q$ with $g_i(X) \neq g_i^*(X)$. We call (1) the *$*$-factorization* of $f(X)$ and we say that the $f_i(X)$ are *$*$-irreducibles*. In particular, since $X-1$ and $X+1$ do not divide $f(X)$, each $f_i(X)$ has even degree. Thus $\Pi(n,q)$ is nonempty only for even n.

An element $y \in \mathrm{GL}(n,q)$ is called *separable* if its characteristic polynomial is separable; in [13] such elements are called regular semisimple.

Definition 2.5. Define $\Delta(n,q)$ to be the set of pairs (t,y), with $t \in \mathrm{GL}(n,q)$ and $y \in \mathrm{SL}(n,q)$, such that $t^2 = 1$, $t^{-1}yt = y^{-1}$, and the characteristic polynomial of y lies in $\Pi(n,q)$. Equivalently these are the pairs (t,y) which generate a dihedral group for which y is separable and self-conjugate, and no eigenvalue of y equals 1 or -1.

If $c(X)$ is the characteristic polynomial for y and its $*$-factorization is $c(X) = c_1(X)\dots c_k(X)$, as in (1), then the underlying space for $\mathrm{GL}(n,q)$ has a unique decomposition $V = \bigoplus_i V_i$ into irreducible $\langle t,y\rangle$-invariant subspaces such that the restriction $y_{|V_i}$ has characteristic polynomial $c_i(X)$, for each i. Again $\Delta(n,q)$ is nonempty only for even n

and the involution t must be of type $(n/2, n/2)$ (apply Lemma 2.2 to each of the restrictions $t_{|V_i}$).

If $(t, y) \in \Delta(n, q)$, then ty is also an involution and $(ty, y) \in \Delta(n, q)$. Thus t and ty are both involutions of type $(n/2, n/2)$ and so are conjugate in $\mathrm{GL}(n, q)$. Hence $y = t(ty) = tt^g$ for some $g \in \mathrm{GL}(n, q)$. In particular $y \in \mathrm{SL}(n, q)$ because $\det t = \det t^g = (-1)^{n/2}$.

Remark 2.6. In the rest of this paper we concentrate on dihedral groups generated by pairs from $\Delta(n, q)$ (as in Definition 2.5) and closely related dihedral groups. This restriction means that our lower bounds in the Main Theorem will be weaker than they otherwise would be, but the separability of y significantly simplifies the analysis. The restriction that y is separable is only expected to have a modest effect on our estimates since the proportion of elements in $\mathrm{GL}(n, q)$ which are separable is asymptotic to $1 - 1/q$ as $n \to \infty$ (proved independently in [3, 14], see also [4, page 2]).

Definition 2.7. Let $y \in \mathrm{GL}(n, q)$ have order m. If m is even then $\mathrm{inv}(y) := y^{m/2}$ denotes the unique nontrivial involution in $\langle y \rangle$; and if m is odd we define $\mathrm{inv}(y) := I$, the trivial involution. Note that if $(t, y) \in \Delta(2n, q)$ then $m > 2$ and $\mathrm{inv}(y)$ generates the centre of the dihedral group $\langle t, y \rangle$.

The following result is a key observation on how to recognize the type of $\mathrm{inv}(y)$ from the $*$-factorization of the characteristic polynomial of y.

Lemma 2.8. *Let $(t, y) \in \Delta(2n, q)$ and suppose that y has even order $2^k h$ ($k \geq 1$ and h odd) and $\mathrm{inv}(y)$ has type (n_+, n_-). Let $c(X)$ be the characteristic polynomial for y, let Γ be the set of eigenvalues of y whose multiplicative order is divisible by 2^k, and let $c^0(X) := \prod_{\xi \in \Gamma}(X - \xi)$. Then $n_- = \deg c^0 = |\Gamma|$, and $c^0(X)$ is the product of all $*$-irreducible factors of $c(X)$ whose roots lie in Γ.*

Proof. Let Λ be the set of all eigenvalues of y over a splitting field for y (recall that y is separable by the definition of $\Delta(2n, q)$). Now $\mathrm{inv}(y) = y^{2^{k-1}h}$ so the eigenvalues of $\mathrm{inv}(y)$ are precisely the elements $\xi^{2^{k-1}h}$ ($\xi \in \Lambda$). The latter eigenvalues are all equal to ± 1, and the result follows since $\xi \in \Gamma$ if and only if $\xi^{2^{k-1}h} = -1$. □

2.1. **Monic irreducible polynomials.** By elementary Galois theory the Galois group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is cyclic of order n and is generated by the Frobenius automorphism $\psi : \xi \longmapsto \xi^q$. Any orbit under the action of $\langle \psi \rangle$ on $\mathbb{F}_{q^n}^*$ consists of the roots of a monic irreducible polynomial

of degree d, say, where $d \mid n$. Conversely if $d \mid n$ then any monic irreducible polynomial of degree d over $\mathbb{F}_q$ splits into d distinct linear factors over $\mathbb{F}_{q^n}$. For each $d \mid n$, this gives a bijection between the set of orbits of length d for $\langle\psi\rangle$ and the set of all monic irreducible polynomials over $\mathbb{F}_q$ with d distinct nonzero roots. Hence if $N(q,d)$ denotes the number of monic irreducible polynomials of degree d over $\mathbb{F}_q$, and with nonzero roots, then

$$q^n - 1 = \sum_{d|n} d\, N(q,d).$$

Thus by the Möbius inversion formula we have the well known formula

$$N(q,n) = \frac{1}{n}\sum_{d|n} \mu(d)(q^{n/d} - 1) \tag{2}$$

where μ is the Möbius function (see [4, p. 22]). For $n > 1$ the right hand sum is also equal to $\sum_{d|n} \mu(d) q^{n/d}$ since $\sum_{d|n} \mu(d) = 0$ when $n > 1$. See, for example [4, Lemma 1.3.10].

Lemma 2.9. *Let q be an odd prime power. Then*

(i) $N(q,n) = \frac{1}{n}\left\{(q^n - 1) - \theta_2(q^{n/2} - 1) - \eta(q,n)\right\}$ *where θ_2 is 1 if n is even and 0 if n is odd, and $0 \le \eta(q,n) \le \frac{5}{4}(q^{n/3} - 1)$;*

(ii) $\left(q^n - 2q^{n/2}\right)/n < N(q,n) \le (q^n - 1)/n$ *for all $n \ge 1$, and $N(q,n) > 0.956(q^n - 1)/n$ for $n \ge 5$;*

(iii) $N(q,n+1) > N(q,n)$ *for all $n \ge 1$;*

(iv) $N(q,n)/(q^n - 1) \ge N(3,n)/(3^n - 1)$ *for all $n \ge 1$.*

Proof. (i) By (2), $nN(q,n) = \sum_{d|n} \mu(d)(q^{n/d} - 1)$ where the Möbius function μ takes values ± 1 and 0. Since $N(q,1) = q - 1$, part (i) holds for $n = 1$ with $\eta(q,n) = 0$. If $n = p^s > 1$ is a power of a prime p, then $nN(q,n) = (q^n - 1) - (q^{n/p} - 1)$, and since $\mu(p) = -1$, the assertion holds with $\eta(q,n) = 0$ when $p = 2$, and $\eta(q,n) = q^{n/p} - 1$ when p is odd.

Thus suppose that n is not a power of a prime and let p be the least odd prime dividing n. Put $m := n/p$. Since n is not a prime power we have $m \ge 2$ and

$$nN(q,n) = (q^n - 1) - \theta_2(q^{n/2} - 1) - (q^m - 1) + \delta$$

where

$$\delta := \sum_{d|n,\ d>p} \mu(d)(q^{n/d} - 1).$$

We claim that $|\delta| \le (q^m - 1)/4$. Since $m \le n/3$ this will complete the proof of part (i).

The values of n/d in the sum for δ are distinct integers in the range $[1, m-1]$. Suppose first that there is no divisor d such that $n/d = m-1$. Then

$$|\delta| \leq \sum_{k=2}^{m-1}(q^{m-k}-1) < (q^m-1)\sum_{k=2}^{\infty} q^{-k} = \frac{q^m-1}{q(q-1)}.$$

Since $1/q(q-1) < 1/4$ for $q \geq 3$ the claim is proved in this case.

On the other hand, suppose that there exists a divisor d of n such that $n/d = m-1$. Then $pm = n = d(m-1)$ and $\gcd(m, m-1) = 1$, so $(m-1) \mid p$. This shows that $m = 2$ or $p+1$ and so $n = 2p$ or $p(p+1)$. By hypothesis p is the smallest odd prime dividing n, so in the latter case $p+1$ must be a power of 2. Thus in either case $n = 2^s p$ for some $s \geq 1$. Therefore $nN(q,n) = (q^n-1)-(q^{n/2}-1)-(q^m-1)+(q^{m/2}-1)$ and so $\delta = q^{m/2}-1 = (q^m-1)/(q^{m/2}+1)$. Since $m \geq 2$ and $q \geq 3$ we conclude that $|\delta| \leq (q^m-1)/4$. This completes the proof of part (i).

(ii) Now $\eta(q,n) \leq q^{n/2}$ for $n \geq 1$ by part (i) (see the first paragraph of the proof of part (i) for n a prime power), so that $(q^n - 2q^{n/2})/n < N(q,n) \leq (q^n-1)/n$. On the other hand, since $q^n - 2q^{n/2} = q^n\left(1-2q^{-n/2}\right) > 0.956q^n$ for $q \geq 3$ and $n \geq 7$ the second inequality in (ii) now follows for all $n \geq 7$ and can be verified directly for $n = 5$ and 6 (it is false for $q = 3$ and $n = 2, 3, 4$).

(iii) This is easily verified for $n \leq 4$. For $n \geq 5$ it follows from (ii) because $0.956(q^{n+1}-1)/(n+1) > (q^n-1)/n$.

(iv) The result is trivially true if $n = 1$. If $n > 1$ and n is a power of a prime p, then $nN(q,n) = q^n - q^{n/p}$ and the inequality can be verified directly. So suppose that n is divisible by at least two primes, and let $p < p'$ be the two smallest primes dividing n. Then $nN(q,n) = q^n - q^{n/p} - \beta_n q^{n/p'}$ where $|1-\beta_n| < \sum_{k=1}^{\infty} q^{-k}$ since $|\mu(d)| \leq 1$ for each d. Now $\sum_{k=1}^{\infty} q^{-k} = 1/(q-1) \leq 1/2$ for all $q \geq 3$, and so $1/2 < \beta_n < 3/2$. Thus $nN(q,n)/(q^n-1) > (q^n-q^{n/p})/(q^n-1) - (3/2)q^{n/p'}/(q^n-1)$ for all $q \geq 3$ whenever n is not a prime power. Similarly $nN(3,n)/(3^n-1) < (3^n-3^{n/p})/(3^n-1) - (1/2)3^{n/p'}/(3^n-1)$ and so the required inequality is easily verified. □

2.2. **Powers of** 2. For pairs $(t,y) \in \Delta(n,q)$ (as in Definition 2.5), we are concerned with the powers of 2 which divide the order of $y \in \mathrm{SL}(n,q)$. Recall that q is odd and $\Delta(n,q)$ is nonempty only when n is even. We use the following notation.

Notation 2.10. For arbitrary n and odd q, let $2^{e_q(n)}$ denote the largest power of 2 which divides q^n-1, that is, the 2-part $(q^n-1)_2 = 2^{e_q(n)}$. The following are easily verified.

(1) If $n = 2^k h$ with $k \geq 0$ and h odd, then $e_q(n) = e_q(2^k)$ since $q^n - 1 = (q^{2^k} - 1)(q^{2^k(h-1)} + \cdots + 1)$, and q and h are odd.
(2) $e_q(2) > e_q(1) \geq 1$ and $e_q(2) \geq 3$ since $q^2 \equiv 1 \pmod 8$ for odd q.
(3) For $k > 1$ we have $e_q(2^k) = 1 + e_q(2^{k-1})$, since $q^{2^k} - 1 = (q^{2^{k-1}} - 1)(q^{2^{k-1}} + 1)$ and $q^{2^{k-1}} \equiv 1 \pmod 8$. Therefore $e_q(2^k) = k - 1 + e_q(2) \geq k + 2$ for $k \geq 1$.

Suppose that $f(X) \in \mathbb{F}_q[X]$ is non-constant and let K be its splitting field. We define

(1) $\omega(f)$ to be the order of the (cyclic) subgroup of K^* generated by the roots of $f(X)$, and
(2) $\omega_2(f)$ to be the largest power of 2 which divides $\omega(f)$.

If $f(X)$ is irreducible, then all its roots have the same multiplicative order which is equal to $\omega(f)$, and we note that $\omega(f) = \omega(f^*)$ since the roots of $f^*(X)$ are the inverses of roots of $f(X)$.

Lemma 2.11. *Let $\mathcal{P}_n$ be the set of monic irreducible polynomials $f(X)$ of degree n over $\mathbb{F}_q$ (q odd) with nonzero roots (so $|\mathcal{P}_n| = N(q,n)$). Then*

(i) *$\omega_2(f) \leq 2^{e_q(n)}$ for all $f(X) \in \mathcal{P}_n$, and*
(ii) *$\omega_2(f) = 2^{e_q(n)}$ for at least $\frac{1}{2}N(q,n)$ of the $f(X) \in \mathcal{P}_n$.*

In the special case where $n = 2^k$ we have $\omega_2(f) = 2^{e_q(n)}$ for exactly $\frac{q^n-1}{2n}$ of the $f(X) \in \mathcal{P}_n$.

Proof. Put $e := e_q(n)$ and write $q^n - 1 = 2^e \ell$ where ℓ is odd by definition. The multiplicative group $G := \mathbb{F}_{q^n}^*$ of the field $\mathbb{F}_{q^n}$ is cyclic of order $q^n - 1$ and so has even order. Let ξ be a generator of G. Then $\zeta := \xi^\ell$ is an element of order 2^e and $\langle\zeta\rangle$ is the set of all 2-elements of G. Let H be the unique subgroup of index 2 in G. Then H consists of all elements of the form ξ^m where m is even. Also $H\zeta$ consists of the elements of the form ξ^m where m is odd, and is the set of all elements of G with 2-part of order 2^e.

Let Ω be the set of elements of $\mathbb{F}_{q^n}$ of degree n over $\mathbb{F}_q$. These elements are the roots of the polynomials in $\mathcal{P}_n$, and so part (i) follows from the fact that $\Omega \subset G$. Also $nN(q,n) = |\Omega|$ since each irreducible polynomial of degree n has n roots in Ω. By definition, Ω consists of those elements of $\mathbb{F}_{q^n}$ which do not lie in any proper subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$.

We now claim that $\eta \in \Omega \cap H$ implies that $\eta\zeta \in \Omega \cap H\zeta$. Indeed $\eta \in \Omega \cap H$ implies that $\mathbb{F}_{q^n}$ is the smallest extension of $\mathbb{F}_q$ containing both the 2-part η_2 and the $2'$-part $\eta_{2'}$ of η. Since $\eta \in H$, $\langle\eta_2\rangle$ is a proper subgroup of $\langle\zeta\rangle$ and so $\langle\eta\zeta\rangle = \langle\eta_{2'}, \eta_2\zeta\rangle \geq \langle\eta_{2'}, \eta_2\rangle = \langle\eta\rangle$

and therefore $\mathbb{F}_{q^n}$ is the smallest extension of $\mathbb{F}_q$ containing $\eta\zeta$, so $\eta\zeta \in \Omega$. Thus $\eta\zeta \in \Omega \cap H\zeta$ as claimed. It follows from this claim that $|\Omega \cap H\zeta| \geq |\Omega \cap H|$, and therefore

$$2\,|\Omega \cap H\zeta| \geq |(\Omega \cap H) \cup (\Omega \cap H\zeta)| = |\Omega| = nN(q,n).$$

Since $\Omega \cap H\zeta$ is the set of elements of degree n over $\mathbb{F}_q$ whose orders are divisible by 2^e the assertion in (ii) follows.

Finally, suppose that n is a 2-power, say 2^k. We claim that all the elements in the coset $H\zeta$ are roots of irreducible polynomials of degree n over $\mathbb{F}_q$. Since $|H\zeta| = \frac{1}{2}(q^n-1)$ this will show that there are $\frac{1}{2}(q^n-1)/n$ polynomials $f(X) \in \mathcal{P}_n$ with $\omega_2(f) = 2^{e_q(n)}$. The claim is trivially true for $k = 0$ since $H\zeta$ is the set of roots of highest 2-part order for linear polynomials. For $k \geq 1$ the field $\mathbb{F}_{q^n}$ has a unique maximal subfield $\mathbb{F}_{q^{n/2}}$ containing $\mathbb{F}_q$. Thus if $\alpha \in \mathbb{F}_{q^n}$ then α has degree n over $\mathbb{F}_q$ if and only if $\alpha \notin \mathbb{F}_{q^{n/2}}$. Since $\left|\mathbb{F}^*_{q^n} : \mathbb{F}^*_{q^{n/2}}\right| = q^{n/2}+1$ is even, $H \geq \mathbb{F}^*_{q^{n/2}}$ and so the claim follows for $k \geq 1$ as well. □

We define $N^0(q,2n)$ to be the the number of monic $*$-irreducible self-conjugate polynomials of degree $2n$ whose roots have multiplicative orders divisible by $2^{e_q(n)}$ (with $e_q(n)$ as in Notation 2.10).

Corollary 2.12. *Suppose that n is even (and q is odd) and put $e := e_q(n)$. Let Γ_1 be the set of monic self-conjugate irreducible polynomials of degree $2n$ over $\mathbb{F}_q$, and let Γ_2 be the set of monic self-conjugate $*$-irreducible polynomials of the form $g(X)g^*(X)$ with $g(X)$ monic irreducible of degree n over $\mathbb{F}_q$ and $g(X) \neq g^*(X)$. Then*

(i) for each $f(X) \in \Gamma_1$, we have $\omega_2(f) < 2^e$;

(ii) for each $f(X) = g(X)g^*(X) \in \Gamma_2$, the 2-part order satisfies $\omega_2(f) = \omega_2(g) \leq 2^e$, and at least $\frac{1}{4}N(q,n)$ of the polynomials $f(X) \in \Gamma_2$ have $\omega_2(f) = 2^e$; moreover if n is a power of 2 then there are exactly $\frac{q^n-1}{4n}$ such polynomials with $\omega_2(f) = 2^e$.

(iii) For n even, $N^0(q,2n) \geq \frac{1}{4}N(q,n)$, and in the special case where n is a power of 2 we have $N^0(q,n) = \frac{q^n-1}{4n}$.

Remark 2.13. We shall only need the case where n is even, but we note that the result is more complicated when n is odd. For example, if n is odd and $q \equiv 3 \pmod 4$, then $e_q(n) = 1$. In this case $\omega_2(f) \leq 2^1$ for all $f(X) \in \Gamma_2$, but there are polynomials $f(X) \in \Gamma_1$ with $\omega_2(f) \geq 2^2$.

Proof. Since n is even, $e \geq e_q(2) > 1$. If $f(X) \in \Gamma_1$ then $\omega(f) \mid (q^n+1)$ by Lemma 2.2. Since n is even and q is odd, $q^n \equiv 1 \pmod 4$ and so $\omega_2(f) \leq (q^n+1)_2 = 2 < 2^e$. Hence part (i) is proved.

By Lemma 2.11, all monic irreducible polynomials $g(X)$ of degree n over $\mathbb{F}_q$ have $\omega_2(g) \leq 2^e$. Also, as observed in Notation 2.10, $\omega(g) = \omega(g^*)$, and hence if $f(X) = g(X)g^*(X)$ and $g(X) \neq g^*(X)$, then $\omega(f) = \omega(g)$ and $\omega_2(f) = \omega_2(g)$. This proves the first assertion of part (ii).

To prove the rest of part (ii), let $g(X)$ be monic and irreducible of degree n with $\omega_2(g) = 2^e$. If $g(X) = g^*(X)$ then, since n is even, it follows from Lemma 2.2 (i) that $\omega(g) \mid (q^{n/2}+1)$ and since $(q^n-1)/(q^{n/2}+1) = q^{n/2}-1$ is even, $\omega_2(g) < 2^e$, which is a contradiction. Thus all $g(X)$ with $\omega_2(g) = 2^e$ satisfy $g(X) \neq g^*(X)$. Moreover Lemma 2.11 implies that $\omega_2(g) = 2^e$ holds for at least $\frac{1}{2}N(q,n)$ of the monic irreducible degree n polynomials $g(X)$, and if n is a power of 2 then equality holds for exactly $\frac{q^n-1}{2n}$ of them. Since each polynomial $f(X) = g(X)g^*(X) \in \Gamma_2$ with $\omega_2(f) = 2^e$ corresponds to two such polynomials, $g(X)$ and $g^*(X)$, we obtain the rest of part (ii).

In particular we have shown that each monic $*$-irreducible self-conjugate polynomial $f(X)$ of degree $2n$ with $\omega_2(f) = 2^e$ is of the form $g(X)g^*(X)$ where $g(X) \neq g^*(X)$. Thus part (iii) follows from parts (i) and (ii). □

2.3. **Generating series.**

Notation 2.14. Let $\mathcal{P}$ be the set of all power series in z with real coefficients. If $f(z) := \sum_{n\geq 0} f_n z^n$ we write $[z^n]f(z)$ to denote the coefficient f_n of z^n. Moreover, if $g(z) := \sum_{n\geq 0} g_n z^n$, then

$$\text{we write} \quad f(z) \ll g(z) \quad \text{if} \quad f_n \leq g_n \text{ for all } n.$$

The relation $\ll$ is a partial ordering on $\mathcal{P}$ with the following properties.

(1) $f_1(z) \ll g_1(z)$ and $f_2(z) \ll g_2(z)$ imply that $f_1(z) + f_2(z) \ll g_1(z) + g_2(z)$. If we also have $0 \ll f_2(z)$ then $f_1(z)f_2(z) \ll g_1(z)f_2(z)$.

(2) Since the power series for the exponential function $\exp(z)$ has positive coefficients, it also follows that $0 \ll f_1(z) \ll g_1(z)$ and $f_1(0) = g_1(0) = 0$ together imply that $\exp(f_1(z)) \ll \exp(g_1(z))$.

(3) If $f(z) = \sum f_n z^n$ then we write $|f|(z) := \sum |f_n| z^n$. We have $|f+g|(z) \ll |f|(z) + |g|(z)$, and if $h(z) := f(z)g(z)$, then by the definition of the product, $|h|(z) \ll |f|(z)\,|g|(z)$.

(4) If we set $f^{(n)}(z) := (f(z))^n$ then by induction, using parts (1) and (3), $\left|f^{(n)}\right|(z) \ll (|f|(z))^n$, for each integer $n \geq 0$.

(5) If $g(z) = \exp(f(z))$ and $f(0) = 0$, then by part (4),

$$|g|(z) \ll \sum_{k\geq 0} (|f^{(k)}|(z)/k!) \ll \exp(|f|(z)).$$

Recall the sets $\Delta(2n,q)$ from Definition 2.5, and set

$$r(2n,q) := \frac{|\Delta(2n,q)|}{|\mathrm{GL}(2n,q)|}, \quad \text{for } n \geq 1, \text{ and } r(0,q) = 1.$$

In [13, Section 5], a product is computed which gives the generating function $R(q,u) := \sum_{n=0}^{\infty} r(2n,q)u^n$. We describe this as follows. Define the series

$$G_0(q,u) := \frac{1}{1+u/(q-1)} \prod_{m \ odd} \left(1 + \frac{u^m}{q^m-1}\right)^{N(q,m)} \tag{3}$$

and for a positive integer b, define

$$G_b(q,u) := \prod_{m \ odd} \left(1 + \frac{u^{2^b m}}{q^{2^b m}-1}\right)^{N(q,2^b m)}. \tag{4}$$

It is shown in [13, Section 5] that $R(q,u) = \prod_{b=0}^{\infty} G_b(q,u)$ (the extra factor for $G_0(q,u)$ arises from the equation in [13, Lemma 5.1]).

We write $G_b(q,u) = \sum_{n \geq 0} g_b(2n,q)u^n$, so that the coefficient $g_b(2n,q)$ is $[u^n]G_b(q,u)$. By [13, Section 5], the quantity $[u^n]G_b(q,u)\,|\mathrm{GL}(2n,q)|$, that is to say, $g_b(2n,q) \times |\mathrm{GL}(2n,q)|$, is equal to the number of pairs $(t,y) \in \Delta(2n,q)$ for which the degree of each factor in the $*$-factorization of the characteristic polynomial for y has the form $2^b h$ for some odd h.

We define $\Delta_b(2n,q)$ to be the set of pairs (t,y) in $\Delta(2n,q)$ such that every factor in the $*$-factorization of the characterisitic polynomial for y has degree not divisible by 2^{b+1} and put $r_b(2n,q) := \frac{|\Delta_b(2n,q)|}{|\mathrm{GL}(2n,q)|}$. It follows by arguments similar to those in [13, Section 5], that

$$R_b(q,u) := \prod_{k=0}^{b-1} G_k(q,u) \quad \text{is equal to } \sum_{n=0}^{\infty} r_b(2n,q)u^n. \tag{5}$$

Note that all the roots of a $*$-irreducible polynomial have the same order, and recall the definition of $e_q(n)$ in Notation 2.10, and of $N^0(q,2n)$ just before Corollary 2.12. The next result, Corollary 2.15, is stated without proof: the first assertion follows from [13, Lemma 5.1] (since we will have $n > 1$), while the other assertions follow from Corollary 2.12 (since the set $\mathcal{P}^*_{2n}$ defined there is the union $\Gamma_1 \cup \Gamma_2$ of the sets Γ_1, Γ_2 defined in Corollary 2.12).

Corollary 2.15. *Let $n = 2^b m$, where $b \geq 1$ and m is odd, and let $\mathcal{P}^*_{2n}$ be the set of all monic, self-conjugate $*$-irreducible polynomials of degree $2n$ over $\mathbb{F}_q$. Further let $\mathcal{P}^0_{2n} \subseteq \mathcal{P}^*_{2n}$ such that $\mathcal{P}^0_{2n}$ comprises those*

polynomials whose roots have multiplicative order with 2-part equal to $2^{e_q(n)} = 2^{e_q(2^b)}$. *Then*

(i) $|\mathcal{P}^*_{2n}| = N(q,n)$;
(ii) $N^0(q,2n) = |\mathcal{P}^0_{2n}| \geq \frac{1}{4}N(q,n)$ *(and* $N^0(q,2n) = \frac{1}{4n}(q^n-1)$ *if* n *is a power of* 2*); and*
(iii) *each root of a polynomial in* $\mathcal{P}^*_{2n} \setminus \mathcal{P}^0_{2n}$ *has order with 2-part less than* $2^{e_q(2^b)}$.

Remark 2.16. For $b \geq 1$, we 'truncate' the infinite product defined by (4) by removing some of the factors. We set

$$G^0_b(q,u) := \prod_{m \text{ odd}} \left(1 + \frac{u^{2^b m}}{q^{2^b m}-1}\right)^{N^0(q,2^{b+1}m)}. \tag{6}$$

Then $[u^k]G^0_b(q,u)\,|\mathrm{GL}(2k,q)|$ is equal to the number of pairs $(t,y) \in \Delta(2k,q)$ such that the $*$-irreducible factors of the characterisitic polynomial for y all lie in $\bigcup_{m \text{ odd}} \mathcal{P}^0_{2^{b+1}m}$ (compare the arguments in [13, Section 5]). Note in particular that, if $G^0_b(q,u) = \sum_{k\geq 0} g^0_b(2k,q)u^k$, then whenever $k > 0$ and $g^0_b(2k,q) \neq 0$, the integer k is divisible by 2^b.

Therefore $a_{k\ell} := [u^k][z^\ell]R_b(q,u)G^0_b(q,uz)\,|\mathrm{GL}(2k,q)|$ is equal to the number of pairs $(t,y) \in \Delta(2k,q)$ such that the characteristic polynomial $c_y(X)$ for y has the form $c_y(X) = b_1(X)b_2(X)$, where

(i) $b_1(X)$ is the product of the $*$-irreducible factors of $c_y(X)$ which lie in $\bigcup_{m \text{ odd}} \mathcal{P}^0_{2^{b+1}m}$ and $\deg b_1(X) = 2\ell$; and
(ii) each $*$-irreducible factor of $b_2(X)$ has degree not divisible by 2^{b+1}.

Applying Lemma 2.8, it follows from (i) and (ii) that

(iii) if $\ell > 0$ then $\mathrm{inv}(y)$ is of type $(2k-2\ell, 2\ell)$

We do not know the value of $N^0(q,2n)$ so rather than calculate $G^0_b(q,u)$ it is simpler to compute

$$F_b(q,u) := \left(1 + \frac{u^{2^b}}{q^{2^b}-1}\right)^{\frac{q^{2^b}-1}{2^{b+2}}} \prod_{m \text{ odd},\ m>1} \left(1 + \frac{u^{2^b m}}{q^{2^b m}-1}\right)^{\lceil \frac{1}{4}N(q,2^b m)\rceil}. \tag{7}$$

Since $N^0(q,2^{b+1}) = 2^{-b-2}(q^{2^b}-1)$ the exponents in (7) are all positive integers. Thus the coefficients of $F_b(q,u)$ are nonnegative and Corollary 2.12 (iii) (or Corollary 2.15 (ii)) shows that $0 \ll F_b(q,u) \ll G^0_b(q,u)$.

We emphasise that $[u^n]F_b(q,u)\,|\mathrm{GL}(2n,q)|$ *is at most the number of pairs* (t,y) *in* $\Delta(2n,q)$ *such that for each* $*$*-irreducible factor of* $c_y(X)$, *its roots have multiplicative order with 2-part at least* $2^{e_q(2^b)}$.

3. Inequalities

In what follows we shall use a number of simple inequalities which we collect here.

Lemma 3.1. *Let M, N, a, b be positive real numbers such that $M \geq N$ and $a \leq b$, and suppose that $Ma \geq Nb$. Then*

(i) $[z^n](1+bz)^N \leq [z^n](1+az)^M \leq [z^n]\exp(aMz)$ *for all $n \leq N$; and*

(ii) *if M and N are integers, then as power series in z we have $(1+bz)^N \ll (1+az)^M \ll \exp(aMz)$.*

Proof. For $n \geq 0$ the coefficients of z^n in the three series in part (i) are

$$\frac{1}{n!}\prod_{i=0}^{n-1}(Nb-ib) \leq \frac{1}{n!}\prod_{i=0}^{n-1}(Ma-ia) \leq \frac{(Ma)^n}{n!}$$

for $n \leq N$. These inequalities hold for all $n \geq 0$ when M and N are integers. □

Corollary 3.2. *For each positive real number λ such that $\lambda N(3,m)$ and $\lambda N(q,m)$ are integers,*

$$(1+\frac{u^m}{3^m-1})^{\lambda N(3,m)} \ll (1+\frac{u^m}{q^m-1})^{\lambda N(q,m)} \ll \exp\left(\frac{\lambda N(q,m)}{q^m-1}u^m\right).$$

Proof. Follows from the previous lemma and Lemma 2.9 (iv). □

Lemma 3.3. *For positive a, n and M such that $n < M$,*

$$[z^n](1+az)^M \geq \frac{(aM)^n}{n!}\exp\left(-\frac{n^2}{2(M-n)}\right).$$

Hence

$$[z^m](1+az)^M \geq [z^m]\exp\left(-\frac{n^2}{2(M-n)}\right)\exp(aMz) \text{ for } m = 0, 1, \ldots, n.$$

Proof. The inequality is trivial if $n = 0$ or 1, so suppose that $1 < n < M$. Now $[z^n](1+az)^M = \frac{(aM)^n}{n!}\prod_{j=1}^{n-1}(1-j/M)$. On the other hand since $\log(1-\xi) \geq -\xi/(1-\xi)$ for $0 \leq \xi < 1$ we have

$$\log\prod_{j=1}^{n-1}(1-j/M) \geq -\sum_{j=1}^{n-1}\frac{j}{M-j} \geq \frac{-1}{M-n}\sum_{j=1}^{n-1}j > -\frac{n^2}{2(M-n)}$$

since $-1/(M-j) \geq -1/(M-n)$ for all $j < n$. The final inequality in the statement of the lemma follows because $-\frac{m^2}{2(M-m)}$ decreases as m increases. □

Lemma 3.4. *Let $f(z) = \sum f_n z^n$ be a power series such that $f_0 = 0$ and suppose that, for some positive constants α and β with $\frac{1}{2}\alpha+\beta \le 1$, we have $|f_n| \le \alpha\beta^{n-1}$ for all $n \ge 1$. Then, setting $g(z) := \exp f(z) = \sum g_n z^n$, we have $|g_n| \le \alpha(\frac{1}{2}\alpha+\beta)^{n-1}$ for all $n \ge 1$.*

Proof. Note that $\alpha z/(1-\beta z) = \sum_{n=1}^{\infty} \alpha\beta^{n-1}z^n$. Thus, by hypothesis, $\sum |f_n|\, z^n \ll \alpha z/(1-\beta z)$. Since $g(z) = \exp f(z)$ and $f(0) = 0$ we have, by Notation 2.14 (5), $\sum |g_n|\, z^n \ll \exp(\sum |f_n|\, z^n)$. Then for all $n \ge 1$,

$$\begin{aligned} |g_n| &\le [z^n] \exp\left(\frac{\alpha z}{1-\beta z}\right) \\ &= \sum_{k=1}^{n} \frac{\alpha^k}{k!} \left[z^{n-k}\right] (1-\beta z)^{-k}. \end{aligned}$$

Now $\binom{-k}{n-k} = (-1)^{n-k}\binom{n-1}{k-1}$ and $1/k! \le 1/2^{k-1}$, for all $k \ge 1$, so

$$\begin{aligned} |g_n| &\le \sum_{k=1}^{n} \frac{\alpha^k}{k!} \binom{-k}{n-k} (-\beta)^{n-k} = \sum_{k=1}^{n} \frac{\alpha^k}{k!} \binom{n-1}{k-1} \beta^{n-k} \\ &\le \alpha \sum_{k=1}^{n} \frac{\alpha^{k-1}}{2^{k-1}} \binom{n-1}{k-1} \beta^{n-k} = \alpha(\frac{1}{2}\alpha+\beta)^{n-1} \end{aligned}$$

as required. □

The following corollary to Lemma 3.4 will be useful.

Corollary 3.5.

$$1 + \frac{\alpha z}{1-\beta z} \ll \exp(\frac{\alpha z}{1-\beta z}) \ll 1 + \frac{\alpha z}{1-\left(\frac{1}{2}\alpha+\beta\right) z}$$

Proof. In Lemma 3.4 we may take $f(z) = \alpha z/(1-\beta z) = \sum_{n=1}^{\infty} \alpha\beta^{n-1}z^n$, and we see that $f(z) = |f|(z)$. If $g(z) = \exp f(z)$, then also $g(z) = |g|(z)$. Thus Lemma 3.4 implies that $g(z) \ll 1 + \frac{\alpha z}{1-\left(\frac{1}{2}\alpha+\beta\right)z}$. We also have $1 + f(z) \ll \exp f(z)$. □

Lemma 3.6. *Let $\alpha > 0$ and consider*

$$f(z) := \left(\frac{1+z}{1-z}\right)^{\alpha} = \sum_{n=0}^{\infty} f_n z^n, \text{ say.}$$

Then $f_n > 0$ for all n and $f_n \ge 2\alpha n^{-1}$ for all odd values of n.

Proof. Note that $f_0 = 1$. Since $\log f(z) = \alpha \log \frac{1+z}{1-z}$ we have $(1-z^2)f'(z) = 2\alpha f(z)$. Comparing coefficients of z^{n-1} in the last equality we get, since $f_0 = 1$,

$$f_1 = 2\alpha \text{ and } nf_n - (n-2)f_{n-2} = 2\alpha f_{n-1} \text{ for } n \ge 2.$$

Thus

$$f_n = \frac{2\alpha}{n} f_{n-1} + (1 - \frac{2}{n}) f_{n-2} \text{ for } n \geq 2.$$

It is now clear that: (i) $f_n > 0$ for all $n \geq 0$; and (ii) $f_n > (1 - \frac{2}{n}) f_{n-2}$ for all $n \geq 2$. Finally induction on n shows that $f_n \geq \frac{2\alpha}{n}$ for all odd n. □

Remark 3.7. For the function $f(z)$ in Lemma 3.6, $f_2 = 2\alpha^2$ and in general, for n even, f_n is a polynomial function in α which is divisible by α^2. As a consequence, when α is small, the coefficients of even powers of z in $f(z)$ are much smaller than neighbouring coefficients for the odd powers.

Lemma 3.8. *If $0 < a < c$ then*

$$\sum_{\substack{a \leq k \leq c \\ k \text{ odd}}} \frac{1}{k} \geq \frac{1}{2} \log(\frac{c}{a}) - \frac{1}{a}.$$

Proof. For each non-negative integer ℓ we have

$$1/(2\ell + 1) \geq \frac{1}{2} \int_{2\ell+1}^{2\ell+3} x^{-1} dx.$$

Set $\ell_0 := \lceil (a-1)/2 \rceil$ and $\ell_1 := \lfloor (c-1)/2 \rfloor$. Then (since $\ell_1 \geq (c-2)/2$) the sum in question is equal to

$$\sum_{\ell=\ell_0}^{\ell_1} \frac{1}{2\ell+1} \geq \frac{1}{2} \int_{2\ell_0+1}^{2\ell_1+3} x^{-1} dx \geq \frac{1}{2} \int_{2\ell_0+1}^{c} x^{-1} dx$$
$$= \frac{1}{2} \log(\frac{c}{a}) - \frac{1}{2} \log\left(\frac{2\ell_0+1}{a}\right).$$

Since $(2\ell_o + 1)/a = 1 + (2\ell_0 + 1 - a)/a < 1 + 2/a$ we have

$$\frac{1}{2} \log\left(\frac{2\ell_0+1}{a}\right) < \frac{1}{2} \log(1 + \frac{2}{a}) < \frac{1}{2} \cdot \frac{2}{a} = \frac{1}{a}$$

so the required inequality follows. □

4. Estimates of coefficients

4.1. **Coefficients of $R(q,u)$.** We write $R(q,u) = \sum_{n \geq 0} r(2n,q) u^n$ so that $r(2n,q) = [u^n] R(q,u)$. It is shown in [13, Lemma 5.2] that $r(2n,q)$ converges to $(1-q^{-1})^2$ as $n \to \infty$ at an exponential rate. Our objective here is to obtain an explicit lower bound for the size of $r(2n,q)$ which is valid for all n.

Recall that $R(q,u) = \prod_{b=0}^{\infty} G_b(q,u)$, as noted after (4). From this and Corollary 3.2, it follows that $R(3,u) \ll R(q,u)$ for every odd

prime power q. It is therefore sufficient to find a lower bound for the coefficients of $R(3,u)$. We use an alternative form for $R(q,u)$ derived in the proof of [13, Lemma 5.2], namely,

$$R(q,u) = \frac{(1-u/q)}{(1-u)(1+u/(q-1))} \prod_{n=1}^{\infty} \left(1 - \frac{u^n(u^n-1)}{q^n(q^n-1)}\right)^{N(q,n)}. \tag{8}$$

Direct computations show that the values of $r(2n,3) = [u^n]R(3,u)$, for $n = 0,\ldots,11$, (rounded to four decimal places) are given by

0	1	2	3	4	5
1.0000	0.5000	0.3750	0.4952	0.4257	0.4497
6	7	8	9	10	11
0.4440	0.4443	0.4446	0.4443	0.4445	0.4444

Lemma 4.1. *The coefficients of $R(3,q)$ satisfy $r(0,3) = 1$, $r(2,3) = 0.5000$, $r(4,3) = 0.3750$, $r(6,3) = 0.4952$, $r(8,3) = 0.4257$, and for $n > 4$, $0.4346 < r(2n,3) < 0.4543$.*

Proof. The values of $r(2n,3) = [u^n]R(3,u)$ for $0 \le n \le 4$, and the bounds on $r(2n,3)$ for $5 \le n \le 11$, follow from the table above. For clarity in our analysis to bound $r(2n,3)$ for $n \ge 12$, we start by looking more generally at $R(q,u)$ and specialize to $q = 3$ at the end. We can write $R(q,u)$ in the form

$$R(q,u) = A(q,u)B(q,u)$$

where

$$A(q,u) := \frac{(1-u/q)}{(1-u)(1+u/(q-1))} = \sum_{n\ge 0} a_n u^n, \text{ say}$$

and $B(q,u) = \sum_{n\ge 0} b_n u^n$ is the product of the remaining factors. We see that

$$A(q,u) = \left(1-\frac{1}{q}\right)^2 \frac{1}{1-u} + \frac{1}{q}\left(2-\frac{1}{q}\right)\frac{1}{1+(q-1)^{-1}u}$$

and so

$$a_n = \left(1-\frac{1}{q}\right)^2 + (-1)^n \frac{2q-1}{q^2(q-1)^n} \text{ for all } n. \tag{9}$$

On the other hand the absolute value of the coefficient of u^n in

$$\left(1 - \frac{u^m(u^m-1)}{q^m(q^m-1)}\right)^{N(q,m)}$$

is bounded above by the corresponding coefficient in

$$\left(1+\frac{u^m(u^m+1)}{q^m(q^m-1)}\right)^{N(q,m)} \ll \left(1+\frac{u^m(u^m+1)}{q^m(q^m-1)}\right)^{\left\lfloor\frac{q^m-1}{m}\right\rfloor} \ll \exp\left(\frac{u^m(u^m+1)}{mq^m}\right)$$

where the latter inequalities come from Lemma 2.9 and Lemma 3.1. Thus

$$|B|(q,u) \ll \prod_{m=1}^{\infty}\exp\left(\frac{u^m(u^m+1)}{mq^m}\right) = \exp\left(\sum_{m=1}^{\infty}\frac{u^m}{mq^m}\right)\exp\left(\sum_{m=1}^{\infty}\frac{u^{2m}}{mq^m}\right)$$

which equals $(1-\frac{u}{q})^{-1}(1-\frac{u^2}{q})^{-1}$ since $\log(1+x) = -\sum_{m\geq 1}(-x)^m/m$ for $|x|<1$. Since

$$\left(1-\frac{u}{q}\right)^{-1}\left(1-\frac{u^2}{q}\right)^{-1} = \frac{q}{q-1}\left\{\frac{1+q^{-1}u}{1-q^{-1}u^2}-\frac{q^{-1}}{1-q^{-1}u}\right\}$$

we see that

$$[u^n]\left(\left(1-\frac{u}{q}\right)^{-1}\left(1-\frac{u^2}{q}\right)^{-1}\right) = \begin{cases} \frac{q}{q-1}q^{-n/2}-\frac{1}{q-1}q^{-n} \text{ for } n \text{ even} \\ \frac{\sqrt{q}}{q-1}q^{-n/2}-\frac{1}{q-1}q^{-n} \text{ for } n \text{ odd} \end{cases}.$$

Thus we conclude that

$$|b_n| \leq \beta q^{-n/2} \text{ for all } n \text{ where } \beta := q/(q-1). \tag{10}$$

We now specialize to $q=3$. By (9) we can write $a_n = \alpha + c_n$ where $\alpha = \frac{4}{9}$ and $c_n = (-1)^n\frac{5}{9}2^{-n}$ for all n and by (10) we have $|b_n| \leq \beta\cdot 3^{-n/2} = \frac{3}{2}\cdot 3^{-n/2}$ for $n\geq 1$. Thus for all $n\geq 1$ we have, noting that $b_0=1$,

$$r(2n,3) = \sum_{k=0}^{n} a_{n-k}b_k = \alpha + v_n + w_n$$

where $\alpha = \alpha b_0$, $v_n := \alpha\sum_{k=1}^{n} b_k$ and $w_n := \sum_{k=0}^{n} c_{n-k}b_k$. Now the inequality (10) implies that $B(3,u)$ converges for all $|u|<3^{1/2}$, and since each of the factors for $B(3,u)$ takes the value 1 at $u=1$, we have, $1 = B(3,1) = \sum_{n=0}^{\infty} b_n$. Since $b_0=1$ we have $\sum_{k=1}^{n} b_k = -\sum_{k=n+1}^{\infty} b_k$ so

$$|v_n| = \left|\alpha\sum_{k=n+1}^{\infty} b_k\right| \leq \alpha\beta\sum_{k=n+1}^{\infty} 3^{-k/2} = \frac{\alpha\beta 3^{-(n+1)/2}}{1-3^{-1/2}} < 0.92\cdot 3^{-n/2}.$$

On the other hand

$$|w_n| \le \frac{5}{9}\beta \sum_{k=0}^{n} 2^{-n+k} \cdot 3^{-k/2} = \frac{5}{9}\beta \cdot 2^{-n} \sum_{k=0}^{n} (2/\sqrt{3})^k$$
$$< \frac{5}{9}\beta \cdot 2^{-n} \frac{(2/\sqrt{3})^{n+1}}{2/\sqrt{3}-1} \le 6.23 \cdot 3^{-n/2}.$$

Thus

$$|r(2n,3) - \alpha| < 7.15 \cdot 3^{-n/2} \text{ for all } n.$$

In particular this shows that $0.4346 < r(2n,3) < 0.4543$ for all $n \ge 12$, completing the proof of the lemma. □

The function $R(q,u)$ was shown in [13, Equation (9)] to be expressible as

$$R(q,u) = \frac{1}{1+u/(q-1)} \prod_{m\ge 1} \left(1 + \frac{u^m}{q^m-1}\right)^{N(q,m)}$$

and it follows from the definitions of $G_b(q,u)$ and $R_b(q,u)$ in (3), (4), and (5), that

$$R_b(q,u) = \frac{1}{1+u/(q-1)} \prod_{m_2 \le 2^{b-1}} \left(1 + \frac{u^m}{q^m-1}\right)^{N(q,m)}$$

where m_2 denotes the highest power of 2 dividing m. Thus, if we define, for a positive integer b,

$$T_b(q,u) := \prod_{m=1}^{\infty} \left(1 + \frac{u^{2^b m}}{q^{2^b m}-1}\right)^{N(q,2^b m)} , . \tag{11}$$

then $R_b(q,u) = R(q,u)T_b(q,u)^{-1}$.

4.2. **Coefficients of $T_b(q,u)^{-1}$.** Temporarily we fix a value of b and define $d := 2^b$, $U := u^d$ and $Q := q^d$. We are going to bound the coefficients $t_n := [U^n]T(U)$ of the power series $T(U)$ where

$$1 - T(U) := \prod_{m=1}^{\infty} \left(1 + \frac{U^m}{Q^m-1}\right)^{-N(q,dm)} = T_b(q,u)^{-1}. \tag{12}$$

Lemma 4.2. *Assume that $d \ge 8$ and define*

$$W(U) := -\log(1 - T(U)) + \frac{1}{d}\log(1-U).$$

Then, for $|u| < 1$, $W(U) = \sum_{n\ge 0} w_n U^n$, where $w_0 = 0$, and $|w_n| < 2.28 d^{-1} n^{-1} (Q-1)^{-n/2}$ for all $n \ge 1$.

Proof. Since $N(q,md) < q^{md}/md$, by Lemma 2.9 (ii), it follows from [4, Lemma 1.3.1] that $1 - T(U)$ converges absolutely and uniformly for $|u| < 1$. Thus $W(U)$ also converges absolutely and uniformly for $|U| < 1$, and since $\log(1-z) = -\sum_{k=1}^{\infty} z^k/k$ for $|z| < 1$ we have

$$\begin{aligned} W(U) &= \sum_{m=1}^{\infty} \left\{ N(q,md) \log\left(1 + \frac{U^m}{Q^m - 1}\right) - \frac{U^m}{md} \right\} \\ &= W_1(U) + W_2(U) \end{aligned}$$

where

$$W_1(U) := \sum_{m=1}^{\infty} \left\{ N(q,md) \frac{U^m}{Q^m - 1} - \frac{U^m}{md} \right\} = \sum_{n=1}^{\infty} w_{1,n} U^n, \text{ say}$$

and

$$W_2(U) := \sum_{m=1}^{\infty} \sum_{k=2}^{\infty} (-1)^{k+1} N(q,md) \frac{U^{mk}}{k(Q^m - 1)^k} = \sum_{n=2}^{\infty} w_{2,n} U^n, \text{ say.}$$

Since d is even and $Q = q^d$, Lemma 2.9 (i) shows that

$$N(q,md) \frac{U^m}{Q^m - 1} = \frac{U^m}{md} - \frac{U^m}{md(Q^{m/2} + 1)} - \eta(q,md) \frac{U^m}{md(Q^m - 1)}$$

where $0 \le \eta(q,md) \le \frac{5}{4}(Q^{m/3} - 1)$. Since $Q \ge 3^8$ we have, for all $n \ge 1$,

$$\begin{aligned} |w_{1,n}| &= \left| \frac{1}{nd(Q^{n/2} + 1)} + \frac{\eta(q,nd)}{nd(Q^n - 1)} \right| \\ &\le \frac{1}{nd(Q^{n/2} + 1)} \left\{ 1 + \frac{5}{4} \frac{Q^{n/3} - 1}{Q^{n/2} - 1} \right\} < \frac{1.277 Q^{-n/2}}{nd}. \end{aligned}$$

On the other hand, Lemma 2.9 shows that $N(q,md) \le (Q^m - 1)/md$ so

$$|w_{2,n}| \le \sum_{m|n,\ m<n} \frac{1}{nd(Q^m - 1)^{n/m - 1}} \le \sum_{1 \le m \le n/2} \frac{1}{nd(Q^m - 1)^{n/m - 1}}.$$

Since

$$\begin{aligned} \sum_{1 \le m \le n/2} (Q^m - 1)^{-n/m+1} &\le \sum_{1 \le m \le n/2} (Q-1)^{-n+m} \\ &= (Q-1)^{-\lceil n/2 \rceil} \sum_{0 \le k \le (n-2)/2} (Q-1)^{-k} \end{aligned}$$

we have

$$|w_{2,n}| < \frac{1}{nd} (Q-1)^{-n/2} \left(1 - (Q-1)^{-1}\right)^{-1} \le \frac{1.0002 (Q-1)^{-n/2}}{nd}.$$

Hence

$$|w_n| \le |w_{1n}| + |w_{2n}| < \frac{2.28(Q-1)^{-n/2}}{nd}$$

for all $n \ge 1$ as required. □

Corollary 4.3. *Under the assumptions of Lemma 4.2, the coefficients of* $E(U) := \exp(-W(U)) - 1 = \sum_{n=1}^{\infty} e_n U^n$ *satisfy* $|e_n| \le \frac{2.28}{1.14+d}\gamma^n$*, for all* $n \ge 1$*, where* $\gamma := (1 + 1.14d^{-1})(Q-1)^{-1/2}$*. In particular, for all* $d \ge 8$ *and* $q \ge 3$*, we have* $\gamma \le 0.0142$ *and* $d\,|e_1| < 0.03$*.*

Proof. Lemma 4.2 shows that $|w_n| \le 2.28d^{-1}(Q-1)^{-n/2}$ for all $n \ge 1$. Applying Lemma 3.4 to $-W(U)$, with $\beta = (Q-1)^{-1/2}$ and $\alpha = 2.28d^{-1}\beta$, proves the first assertion (noting that $\gamma = \frac{1}{2}\alpha + \beta < 1$). In particular, if $d \ge 8$ and $q \ge 3$, then $\gamma \le 0.0142$, and if $n = 1$, then $d\,|e_1| \le \frac{2.28d}{1.14+d}\gamma = 2.28(Q-1)^{-1/2} \le 2.28(3^8-1)^{-1/2}$ which is less than 0.03. □

Recall that $T_b(q,u)^{-1} = 1 - T(U)$ where $T(U) = \sum_{k=1}^{\infty} t_k U^k$, see (12). From the product formula for $T_b(q,u)$ in (11) we see that $t_1 = \frac{N(q,d)}{q^d-1}$. Let $h(U) = \sum_{k=1}^{\infty} h_k U^k$, say, be the series for $1 - (1-U)^{1/d}$. It follows from the definition of $W(U)$ in Lemma 4.2, and of $E(U)$ in Corollary 4.3, that

$$1 - T(U) = (1-U)^{1/d}(1 + E(U)) = (1 - h(U))\,(1 + E(U)). \tag{13}$$

Now for $k \ge 1$ we have

$$h_k := -\binom{1/d}{k}(-1)^k = \frac{1}{dk}\prod_{i=1}^{k-1}\left(1 - \frac{1}{di}\right).$$

In particular $dh_1 = 1$. For $k \ge 2$, since $1 - \xi > \exp\left(-\frac{\xi}{1-\xi}\right)$ for $0 \le \xi < 1$,

$$\begin{aligned} 1 \ge dkh_k &> \exp\left(-\sum_{i=1}^{k-1}\frac{1}{di-1}\right) \\ &> \exp\left(\frac{-1}{d-1}\sum_{i=1}^{k-1}\frac{1}{i}\right) > \exp\left(\frac{-(1+\log k)}{d-1}\right). \end{aligned} \tag{14}$$

We use this to estimate the values of the coefficients t_k.

Lemma 4.4. *Suppose that* $d \ge 8$*. Then* $0.58 < dkt_k < 1.02$ *for* $k \ge 1$*, whenever* $dk \le e^{d/2}$*.*

Proof. Suppose that $k \geq 1$ and $dk \leq e^{d/2}$. Then $d/2 \geq \log dk \geq \log k + \log 8 > \log k + 2$, so by (14), $\log(dkh_k) > -(d/2-1)/(d-1) \geq -0.5$. Thus $1 \geq dkh_k > 0.60$ for all $k \geq 1$.

On the other hand equation (13) shows that for all $k \geq 1$ we have $t_k = h_k - e_k + \sum_{i=1}^{k-1} e_{k-i}h_i$. Thus Corollary 4.3 gives

$$|t_k - h_k| \leq |e_k| + \sum_{i=1}^{k-1} \frac{|e_{k-i}|}{di} \leq \frac{2.28}{1.14+d}\left\{\gamma^k + \frac{1}{d}\sum_{i=1}^{k-1}\frac{1}{i}\gamma^{k-i}\right\} \text{ for } k \geq 1$$

where $\gamma := (1+1.14d^{-1})(1-q^{-d})^{-1/2}q^{-d/2} < 1.143q^{-d/2}$.

If $k = 1$ then, by equation (13), $t_1 = N(q,d)/(q^d-1) = (q^d - q^{d/2})/d(q^d-1)$ since d is a power of 2. Because $q^d \geq 3^8$, this implies that t_1 lies between d^{-1} and $0.9878d^{-1}$. Since $h_1 = \binom{1/d}{1} = d^{-1}$, this shows that $|t_1 - h_1| \leq 0.0122d^{-1}$. On the other hand, if $k \geq 2$, then $1/i \leq (k-i)/(k-1)$ for all i with $1 \leq i \leq k-1$ and so

$$\sum_{i=1}^{k-1}\frac{1}{i}\gamma^{k-i} \leq \frac{1}{k-1}\sum_{i=1}^{k-1}(k-i)\gamma^{k-i} < \frac{1}{k-1}\sum_{i=1}^{\infty} i\gamma^i = \frac{\gamma}{(k-1)(1-\gamma)^2}.$$

Since we are assuming that $dk \leq e^{d/2}$ and $d \geq 8$ we have $dk\gamma \leq 1.143(e/q)^{d/2} < 0.78$ and so for $k \geq 2$ we have

$$\begin{aligned}|t_k - h_k| &\leq \frac{2.28}{1.14+d}\left\{\gamma^k + \frac{\gamma}{d(k-1)(1-\gamma)^2}\right\} \\ &< \frac{2.28\gamma}{d^2k}\left\{kd\gamma + \frac{k}{(k-1)(1-\gamma)^2}\right\} < 6.5\gamma d^{-2}k^{-1}.\end{aligned}$$

Since $6.5\gamma d^{-1} < 6.5 \times 0.0142 \times 0.125 < 0.02$ we have $|t_k - h_k| < 0.02d^{-1}k^{-1}$ for all $k \geq 1$. We showed at the beginning of the proof that $0.60 < dkh_k \leq 1$ so we conclude that $0.58 < dkt_k < 1.02$ for all $k \geq 1$ as required. □

4.3. **Coefficients of $R_b(q,u)$.** We have $R_b(q,u) = R(q,u)T_b(q,u)^{-1}$ where $T_b(q,u)^{-1} = 1 - T(U) = 1 - \sum_{k=1}^{\infty} t_k u^{dk}$, see (5), (11), (12). By Lemma 4.4 we know that $0.58 < t_k dk < 1.02$ for all $k \geq 1$. Recall that $R_b(q,u) = \sum_{n=0}^{\infty} r_b(2n,q)u^n$ and $R(q,u) = \sum_{n=0}^{\infty} r(2n,q)u^n$, where $r(0,3) = 1 > r(2n,3)$ for all $n \geq 1$ and $0.4346 \leq r(2n,3) \leq 0.4543$, for all $n \geq 4$ (see Lemma 4.1).

Lemma 4.5. *Let $b \geq 3$ and $d = 2^b$. Then $r_b(2n,q) > 0.2029$ for all odd q and all $n \leq e^{d/2}$.*

Proof. First note that it follows from Corollary 3.2 that $R_b(3,u) \ll R_b(q,u)$ for all odd q. Therefore $r_b(2n,q) \geq r_b(2n,3)$ so it is enough to prove the lemma for $q = 3$. Thus from now on assume that $q = 3$.

Also note that $R_{b-1}(3,u) \ll R_b(3,u)$ since by (5) the latter is a product of the former with a power series with nonnegative coefficients and constant coefficient 1, so $r_{b-1}(2n,3) \le r_b(2n,3)$ for all n.

The values of $r_3(2n,3)$ for $n = 0, 1, ..., 23$ are given (reading left to right across row 1, then row 2, and so on) by

1.0000	0.5000	0.3750	0.4952	0.4257	0.4497
0.4440	0.4443	0.3211	0.3826	0.3982	0.3833
0.3919	0.3889	0.3896	0.3896	0.3347	0.3622
0.3690	0.3624	0.3662	0.3649	0.3652	0.3652

so $r_b(2n,3) \ge r_3(2n,3) > 0.2029$ for $b \ge 3$ and $n < 24$.

Claim: To prove that $r_b(2n,3) > 0.2029$ for all $b \ge 3$ and all $n \le e^{d/2}$ (noting that $d = 2^b$), it is enough to prove this inequality for n satisfying $3d \le n \le e^{d/2}$.

If $b = 3$ the claim holds since the cases $n < 3d$ are covered by the table above. Suppose now that $b > 3$ and that we have proved, for all integers $b' \in [3, b]$, that $r_{b'}(2n,3) > 0.2029$ for all n such that $3d' \le n \le e^{d'/2}$, where $d' = 2^{b'}$. Then by our observation above, $r_b(2n,3) \ge r_{b'}(2n,3) > 0.2029$, for all n in the interval $[3d', e^{d'/2}]$. Moreover, for each $b' \ge 4$, we have $3d' \le e^{d'/4}$, and so the interval $[3d', e^{d'/2}]$ contains the upper end-point $e^{d'/4}$ of the interval corresponding to $b'-1$, so that the union of all of these intervals, together with the interval $[0, 23]$ is equal to $[0, e^{d/2}]$. This proves the claim.

Thus we seek a proof that $r_b(2n,3) > 0.2029$ for $3d \le n < e^{d/2}$, where $d = 2^b$. Since $R_b(3,u) = R(3,u)(1 - T(U))$ where $U := u^d$ and $T(U) = \sum t_k U^k$ we have

$$r_b(2n,3) = r(2n,3) - \sum_{1 \le k \le k_0} r(2(n-kd),3)t_k$$

where $k_0 := \lfloor n/d \rfloor \ge 3$ since we are assuming that $n \ge 3d$. If $k < k_0$ then $n - kd \ge d \ge 8$, and so, by Lemma 4.1, $r(2n,3) \ge 0.4346$ for $n \ge d$; $r(2(n-k_0 d),3) \le 1$; and $r(2(n-kd),3) \le 0.4543$ for $k = 1, ..., k_0 - 1$. Since $kdt_k \le 1.02$ for all k by Lemma 4.4, and since $3d \le n \le e^{d/2}$ by hypothesis, we have

$$\begin{aligned} r_b(2n,3) &\ge 0.4346 - \frac{1.02}{d}\left\{\frac{1}{k_0} + 0.4543 \sum_{1 \le k \le k_0 - 1} \frac{1}{k}\right\} \\ &\ge 0.4346 - \frac{1.02}{d}\left\{\frac{1}{k_0} + 0.4543\,(\log k_0 + 1)\right\}. \end{aligned}$$

However $\log k_0 + 1 \le \log(n/d) + 1 \le \log n - \log d + 1 \le \log n - 1 \le d/2 - 1$, by the hypothesis on n, and $1/k_0 \le 1/3 < 0.4543$. Therefore $r_b(2n, 3) \ge 0.4346 - 1.02 \times 0.4543/2 > 0.2029$ as required. □

4.4. **Coefficients of $F_b(q, u)$.** We shall continue to assume that $b \ge 3$, $d := 2^b \ge 8$, $U = u^d$ and $Q = q^d$ with q odd. With this notation (7) becomes

$$F_b(q,u) = \left(1 + \frac{U}{Q-1}\right)^{\frac{1}{4}(Q-1)/d} \prod_{m \text{ odd},\, m>1} \left(1 + \frac{U^m}{Q^m - 1}\right)^{\lceil \frac{1}{4}N(q,md)\rceil}$$

$= F_b(U)$, say. If we write $F_b(q, u) = \sum_{n \ge 0} f_b(2n, q)u^n$, then $f_b(2n, q) \ne 0$ implies that $n = 2^b k$ for some integer k and $f_b(2n, q) = [U^k]F_b(U)$.

Recall that, since $0 \ll F_b(q, u) \ll G_b^0(q, u)$ (see equations (6) and (7)), the entry $[u^n]F_b(q, u)\,|\mathrm{GL}(2n, q)|$ is a lower bound on the number of pairs (t, y) in $\Delta(2n, q)$ such that the 2-part of the order of each eigenvalue of y is at least $2^{e_q(d)}$.

Lemma 4.6. *Assume $b \ge 3$, so $d = 2^b \ge 8$. Then $[U^k]F_b(U) \ge 0.2117 d^{-1}k^{-1}$ for all odd k with $kd \le e^{d/2}$.*

Proof. Fix an odd integer k such that $\log kd \le d/2$. To compute $[U^k]F_b(U)$ it is enough to know, for each m, and for all $\ell \le \frac{k}{m}$, the values of $[U^{m\ell}]\left(1 + \frac{U^m}{Q^m-1}\right)^{\lceil \frac{1}{4}N(q,md)\rceil}$. Now $k \le \frac{1}{d}e^{d/2} < \frac{1}{d}q^{d/2} < \frac{1}{4d}(q^d - 2q^{d/2})$ because $q^{d/2} - 2 > 4$, and so $k < \frac{1}{4}N(q, d) \le \frac{1}{4}N(q, md)$ for all $m \ge 1$, by Lemma 2.9 (ii). By Lemma 3.3 (applied with $z = U^m$, $a = \frac{1}{Q^m-1}$, $n = \ell$, and $M = \lceil \frac{1}{4}N(q, md)\rceil$),

$$\begin{aligned}
&[U^{m\ell}]\left(1 + \frac{U^m}{Q^m - 1}\right)^{\lceil \frac{1}{4}N(q,md)\rceil} \\
&\ge [U^{m\ell}] \exp\left(-\frac{2\ell^2}{N(q, md) - 4\ell}\right) \exp\left(\frac{N(q, md)}{4(Q^m - 1)}U^m\right)
\end{aligned}$$

for all $\ell \le k/m$. As ℓ increases in the range $0 \le \ell < \frac{1}{4}N(q, md)$, the value of $-2\ell^2/(N(q, md) - 4\ell)$ decreases. Also for the exceptional factor with $m = 1$ in the definition of $F_b(q, u)$ the exponent $\frac{Q-1}{4d} \ge \frac{N(q,d)}{4d}$, so the above lower bound holds in this case also. Thus $[U^k]F_b(U) \ge c_k[U^k]H(U)$ where

$$c_k := \prod_{m \text{ odd}} \exp\left(\frac{-2(k/m)^2}{N(q, md) - 4k/m}\right)$$

and

$$H(U) := \prod_{m \text{ odd}} \exp\left(\frac{N(q,md)U^m}{4(Q^m-1)}\right).$$

We first estimate c_k. By Lemma 2.9(ii), $N(q,md) - 4k/m \geq (Q^m - 2Q^{m/2} - 4kd)/md$. However $Q = q^d \geq 3^8$ and $4kdQ^{-1} \leq 4e^{d/2}q^{-d} \leq 0.0333$ so

$$Q^m - 2Q^{m/2} - 4kd \geq Q^m(1 - 2Q^{-1/2} - 4kdQ^{-1}) \geq 0.942Q^m.$$

This implies that

$$\begin{aligned} c_k &\geq \exp\left(-\sum_{m \text{ odd}} \frac{2(k/m)^2}{0.942Q^m/md}\right) \geq \exp\left(-\frac{2.124k^2d}{Q}\sum_{\ell=0}^{\infty} Q^{-2\ell}\right) \\ &\geq \exp(-2.13k^2dQ^{-1}) \end{aligned}$$

(the sum of powers of Q is very close to 1). Since $2.13k^2dQ^{-1} \leq 2.13d^{-1}e^dq^{-d} \leq 0.121$ we conclude that $c_k \geq 0.886$.

Next consider $H(U)$. Lemma 2.9(ii) shows that $mdN(q,md) \geq 0.956(Q^m - 1)$ and so

$$\frac{N(q,md)}{4(Q^m-1)} \geq \frac{0.239}{md} \text{ for } m \geq 1.$$

Set $2\alpha = 0.239d^{-1}$. Since $\exp\left(2\alpha \sum_{m \text{ odd}} U^m/m\right) = \left(\frac{1+U}{1-U}\right)^{\alpha}$ we have

$$H(U) \gg \left(\frac{1+U}{1-U}\right)^{\alpha}.$$

Finally using Lemma 3.6 we conclude that

$$\begin{aligned} [U^k]F_b(U) &\geq c_k[U^k]H(U) \geq c_k[U^k]\left(\frac{1+U}{1-U}\right)^{\alpha} \\ &\geq 0.886 \times \frac{2\alpha}{k} > 0.2117\frac{1}{dk} \end{aligned}$$

for all odd k with $kd \leq e^{d/2}$ as claimed. □

5. Proof of the Main Theorem

In this section we complete the proof of Theorem 1.1. We begin with some preliminary lemmas. Suppose that $0 \leq \alpha < \beta \leq 1$, and let $J(2m,q;\alpha,\beta)$ be the set of all $(t,y) \in \Delta(2m,q)$ for which $\mathrm{inv}(y)$ is (α,β)-balanced. Set

$$j(2m,q;\alpha,\beta) := |J(2m,q;\alpha,\beta)| \,/\, |\mathrm{GL}(2m,q)|\,. \tag{15}$$

If $c(X) \in \Pi(2m,q)$ is the characteristic polynomial for y and $c^0(X)$ is as in Lemma 2.8, then Lemma 2.8 shows that $\mathrm{inv}(y)$ is (α,β)-balanced

$\iff 2m(1-\beta) \leq \deg c^0(X) \leq 2m(1-\alpha)$. Our discussion following (6) shows that we may obtain a lower bound for $j(2m, q; \alpha, \beta)$ by summing, over $b \geq 1$, the coefficient of $u^m z^\ell$ in the power series $R_b(q,u)F_b(q,uz)$, provided that we only consider those terms corresponding to values of ℓ in the range $[m(1-\beta), m(1-\alpha)]$ (and we recall that non-zero summands in $F_b(q,uz) = \sum_{\ell \geq 0} f_b(2\ell, q)(uz)^\ell$ occur only if 2^b divides ℓ). Thus, for a fixed value of m, we have

$$j(2m, q; \alpha, \beta) \geq [u^m] \sum_{b=1}^{\infty} R_b(q,u) F_b(q, u; m(1-\beta), m(1-\alpha)) \tag{16}$$

where $F_b(q, u; m(1-\beta), m(1-\alpha))$ is the truncated power series obtained from $F_b(q,u) = \sum_{k=0}^{\infty} f_b(2^{b+1}k, q)u^{2^b k}$ by keeping only the terms $f_b(2^{b+1}k, q)u^{2^b k}$ for which $m(1-\beta) \leq 2^b k \leq m(1-\alpha)$.

Lemma 5.1. *Let $b \geq 3$ and $d := 2^b$. Then for all α and β with $0 \leq \alpha < \beta < 1$ and positive integers $m \leq e^{d/2}$, we have*

$$j(2m, q; \alpha, \beta) \geq \frac{0.02147}{d} \left(\log \left(\frac{1-\alpha}{1-\beta} \right) - \frac{2d}{m(1-\beta)} \right).$$

Proof. By Lemma 4.6, for all odd k such that $dk \leq e^{d/2}$, we have $f_b(2dk, q) \geq 0.2117/dk$, with $f_b(2dk, q)$ as above. Set $a := m(1-\alpha)$ and $c := m(1-\beta)$, and consider the sum s of the coefficients of terms of degree between c and a in $F_b(q,u)$:

$$\begin{aligned} s = \sum_{c/d \leq k \leq a/d} f_b(2dk, q) &\geq \sum_{\substack{c/d \leq k \leq a/d \\ k \text{ odd}}} \frac{0.2117}{dk} \\ &\geq \frac{0.2117}{2d} \left(\log \left(\frac{a}{c} \right) - \frac{2d}{c} \right) \end{aligned}$$

by Lemma 3.8. Since $[u^n]R_b(q,u) \geq 0.2029$ for all $n \leq e^{d/2}$, by Lemma 4.5, it follows from (16) that $j(2m, q; \alpha, \beta) \geq 0.2029\, s$, so the result follows. □

Let V be the underlying space for $\mathrm{GL}(n,q)$ and let K_s be the conjugacy class of involutions in $\mathrm{GL}(n,q)$ of type $(s, n-s)$. Assume that $s \geq n/2$ and set $h := 2s-n$. Let Ω be the set of all pairs (V_1, V_2) of subspaces of V such that $V = V_1 \oplus V_2$ with $\dim V_1 = h$ and $\dim V_2 = n-h$ $(= 2(n-s))$. Recall that for an involution t we write $E_+(t)$ and $E_-(t)$ to denote the eigenspaces for eigenvalues $+1$ and -1, respectively.

Definition 5.2. For $0 \leq \alpha < \beta < 1$, let $L(n, s, q; \alpha, \beta)$ be the set of pairs $(t, t') \in K_s \times K_s$ such that:

(i) $V_1 := E_+(t) \cap E_+(t')$ has dimension $h = 2s - n$.

(ii) There exists a $\langle t, t'\rangle$-invariant subspace V_2 of dimension $n-h$ such that $(t_{|V_2}, tt'_{|V_2}) \in \Delta(n-h, q)$ (see Definition 2.5).

(iii) $\mathrm{inv}(tt'_{|V_2})$ is (α, β)-balanced.

Note that for any $(t, t') \in L(n, s, q; \alpha, \beta)$ we have:

(iv) $t_{|V_1} = t'_{|V_1} = I$ by (i).

(v) Let Σ_1 be the class of all $\langle t, t'\rangle$-modules whose composition factors all have dimension 1, and let Σ_2 be the class of such modules, with all composition factors of dimension at least 2. It follows from Definition 2.5 that V_1 and V_2 are the maximal $\langle t, t'\rangle$-submodules of V lying in Σ_1 (respectively Σ_2). In particular V_1 and V_2 are uniquely determined and $V_1 \cap V_2 = 0$. The hypotheses on the dimensions show that $V = V_1 \oplus V_2$.

(vi) If W is a $\langle t, t'\rangle$-invariant subspace of V_2, then $\dim W$ is even, say $2k$, and the involutions $t_{|W}$ and $t'_{|W}$ are both of type (k, k), by Lemma 2.2 and the definition of $\Delta(n-h, q)$.

Define $\ell(n, s, q; \alpha, \beta) := |L(n, s, q; \alpha, \beta)| \,/\, |K_s|^2$ (the proportion of pairs in $K_s \times K_s$ which lie in $L(n, s, q; \alpha, \beta)$). Set

$$\varphi(k, q) := \prod_{i=1}^{k} (1 - q^{-i}) = q^{-k^2} \, |GL(k, q)|$$

for $k \geq 1$ and let $\varphi(0, q) = 1$.

Lemma 5.3. *If $h := 2s - n$ is nonnegative, then*

$$\ell(n, s, q; \alpha, \beta) = \theta(n, s, q) j(n-h, q; \alpha, \beta),$$

where $j(n-h, q; \alpha, \beta)$ is as in (15) *and*

$$\theta(n, s, q) = \frac{\varphi(n-s, q)^2 \varphi(s, q)^2}{\varphi(n, q)\varphi(h, q)}.$$

Proof. For each pair $(V_1, V_2) \in \Omega$, and each pair $(t_2, y_2) \in \Delta(n-h, q)$ acting on V_2 such that $\mathrm{inv}(y_2)$ is (α, β)-balanced, there is a unique pair (t, t') of involutions in $\mathrm{GL}(n, q)$ such that $t_{|V_2} = t_2$, $t'_{|V_2} = t_2 y_2$, and $t_{|V_1} = t'_{|V_1} = I$. Moreover, since each of t_2 and $t_2 y_2$ conjugates y_2 to its inverse, each is of type $(\frac{1}{2}(n-h), \frac{1}{2}(n-h))$ by Lemma 2.2. It follows from Definition 5.2 that $(t, t') \in L(n, s, q; \alpha, \beta)$.

Conversely, for each $(t, t') \in L(n, s, q; \alpha, \beta)$, relative to V_1, V_2 as in Definition 5.2, the pair $(t_{|V_2}, tt'_{|V_2}) \in \Delta(n-h, q)$. Hence we have $|L(n, s, q; \alpha, \beta)| = |\Omega| \times |J(n-h, q; \alpha, \beta)|$. Since

$$j(n-h, q; \alpha, \beta) = |J(n-h, q; \alpha, \beta)| \,/\, |\mathrm{GL}(n-h, q)|$$

we conclude that $\ell(n,s,q;\alpha,\beta) = \theta(n,s,q)j(n-h,q;\alpha,\beta)$, where $\theta(n,s,q) = |\Omega|\,|\mathrm{GL}(n-h,q)|\,/\,|K_s|^2$. Finally

$$|\Omega| = \frac{|\mathrm{GL}(n,q)|}{|\mathrm{GL}(h,q)|\,|\mathrm{GL}(n-h,q)|} \text{ and } |K_s| = \frac{|\mathrm{GL}(n,q)|}{|\mathrm{GL}(s,q)|\,|\mathrm{GL}(n-s,q)|}$$

so we obtain the value of $\theta(n,s,q)$ given in the statement. □

Remark 5.4. We have $1 \geq \varphi(k,q) > \varphi(\infty,q) := \lim_{k\to\infty}\varphi(k,q)$ and it is easily seen that $\varphi(k,q) = \varphi(\infty,q) + O(q^{-k-1})$. For small odd values of $q \leq 9$, the values of $\varphi(\infty,q)$, correct to 5 decimal places, are given in the table below.

q	3	5	7	9
$\varphi(\infty,q)$	0.56013	0.76033	0.83680	0.87656

More precisely, by [12, Lemma 3.1] and its proof, $\varphi(n,q) \geq 1 - q^{-1} - q^{-2} + q^{-n-1}$, for all n and all q, so $\varphi(\infty,q) \geq 1 - q^{-1} - q^{-2}$ for all q. Since $\varphi(n-s,q) \geq \varphi(n,q)$ and $\varphi(h,q) \leq 1$ we have

$$\theta(n,s,q) \geq \varphi(n-s,q)\varphi(s,q)^2 > \varphi(\infty,q)^3 > 0.175.$$

Proof of the Main Theorem. Let t be a strong involution in $\mathrm{GL}(n,q)$. Then t is $(1/3,2/3)$-balanced and so is of type $(s,n-s)$ with $1/3 \leq s \leq 2/3$. We claim that it is enough to consider the case where $s \geq n/2$. Indeed, if $s < n/2$, then $-t$ is a strong involution of type $(n-s,s)$ with $n-s > n/2$ and since $(-t)(-t^g) = tt^g$ the value of $z(g) := \mathrm{inv}(tt^g)$ is unchanged. Thus by replacing t by $-t$ where necessary, we assume for the rest of this proof that $s \geq n/2$ and $0 \leq h := 2s - n \leq n/3$.

First consider the proof of (i). Let K_s be the conjugacy class of t in $\mathrm{GL}(n,q)$, that is, the set of involutions of type $(s,n-s)$, and let π_+ be the probability that, for a random $g \in \mathrm{GL}(n,q)$, the restriction of $\mathrm{inv}(tt^g)$ to $E_+(t)$ is $(1/3,2/3)$-balanced. Now π_+ is independent of the choice of t in K_s. A straightforward counting argument shows that π_+ is equal to the proportion of $(t,t') \in K_s \times K_s$ such that:

(*) the restriction of $\mathrm{inv}(tt')$ to $E_+(t)$ is $(1/3,2/3)$-balanced.

We shall prove via the following two steps that there exist positive absolute constants κ and n_0 such that $\pi_+ > \kappa/\log n$ for all $n \geq n_0$.

(a) First we find specific α,β (depending on n and s) such that (*) holds for (t,t') whenever $(t,t') \in L(n,s,q;\alpha,\beta)$. It will then follow that

$$\pi_+ \geq |L(n,s,q;\alpha,\beta)|\,/\,|K_s|^2 = \ell(n,s,q;\alpha,\beta).$$

(b) Secondly, for these specific α,β, we find absolute constants κ and n_0 such that $\ell(n,s,q;\alpha,\beta) \geq \kappa/\log n$ for all $n \geq n_0$.

We begin with the proof of (a). Let $0 \le \alpha < \beta < 1$ be constants which will be determined later and suppose that $(t, t') \in L(n, s, q; \alpha, \beta)$. Set $D := \langle t, t' \rangle$, $z := \mathrm{inv}(tt')$ and let (V_1, V_2) be the associated pair of subspaces as in Definition 5.2. The following table illustrates the relationships between the subspaces $E_+(t)$, $E_-(t)$ and the subspaces V_1, $V_{2+} := V_2 \cap E_+(z)$ and $V_{2-} := V_2 \cap E_-(z)$:

$$\begin{array}{cccc} & E_+(t) & E_-(t) & V \\ V_1 & h & 0 & h \\ V_{2+} & k & k & 2k \\ V_{2-} & \ell & \ell & 2\ell \\ V & \frac{1}{2}(n+h) & \frac{1}{2}(n-h) & \end{array}$$

where each integer entry is the dimension of the intersection of the subspaces at the heads of the row and column of the entry (k and ℓ are so far undetermined). Recall that $h = 2s - n$ so $s = \frac{1}{2}(n + h)$. Since V_{2+} and V_{2-} are D-invariant subspaces of V_2 it follows from condition (vi) (after Definition 5.2) that they have even dimensions, say $2k, 2\ell$, and that $\dim(E_+(t) \cap V_{2\varepsilon}) = \frac{1}{2}\dim(V_{2\varepsilon})$, for $\varepsilon = \pm$. Note that $E_+(t)$ and $E_-(t)$ are invariant under z since z is in the centre of the group D, but they are not invariant under tt' except in the trivial case where $s = h = n$. The dimensions k and ℓ depend on (t, t'). Since $(t, t') \in L(n, s, q; \alpha, \beta)$ the involution $z_{|V_2}$ is (α, β)-balanced by definition; that is to say, $E_+(z_{|V_2}) = E_+(z) \cap V_2 = V_{2+}$ satisfies

$$\alpha \le \frac{\dim(V_{2+})}{\dim(V_2)} = \frac{2k}{2(k+\ell)} = \frac{k}{k+\ell} \le \beta.$$

On the other hand for $z_{|E_+(t)}$ to be $(1/3, 2/3)$-balanced, we require $E_+(z_{|E_+(t)}) = E_+(z) \cap E_+(t) = V_1 \oplus (V_{2+} \cap E_+(t))$ to have dimension satisfying $1/3 \le \dim(E_+(z_{|E_+(t)}))/\dim(E_+(t)) \le 2/3$, that is to say, $1/3 \le (h + k)/(h + k + \ell) \le 2/3$.

Now define $\gamma := (n + h)/(n - h)$ and note that, since t is $(1/3, 2/3)$-balanced and we are assuming that $h \ge 0$, we have $0 \le h \le n/3$ and so $1 \le \gamma \le 2$.

$$\text{Set} \quad \alpha := \max\left\{0, 1 - \frac{2}{3}\gamma\right\} \text{ and } \beta := 1 - \frac{1}{3}\gamma$$

and note that $0 \le \alpha < \beta \le 2/3$ for all $\gamma \in [1, 2]$. We claim that, for these values of α and β, $z_{|E_+(t)}$ is $(1/3, 2/3)$-balanced whenever $z_{|V_2}$ is (α, β)-balanced.

Note that $h+k+\ell = s = \frac{1}{2}(n+h)$ and $k+\ell = \frac{1}{2}(n-h)$. Suppose that $z_{|V_2}$ is (α,β)-balanced. Then

$$\frac{1}{3}\gamma = 1-\beta \le 1 - \frac{k}{k+\ell} = \frac{\ell}{k+\ell} = \frac{2\ell}{n-h} = \frac{2\ell\gamma}{n+h} \le 1-\alpha \le \frac{2}{3}\gamma.$$

This implies that $\frac{1}{3} \le 2\ell/(n+h) \le \frac{2}{3}$. On the other hand this last inequality is equivalent to $\frac{1}{3} \le 1-2\ell/(n+h) = (h+k)/(h+k+\ell) \le \frac{2}{3}$ which shows that $z_{|E_+(t)}$ is $(1/3, 2/3)$-balanced. This proves step (a).

We now find κ and n_0 for which step (b) is true. Suppose that $n > e^4$, or equivalently, that $n > 54$. Then there exists a unique $b \ge 4$ such that $2^{b-2} < \log n \le 2^{b-1}$, or equivalently, setting $d := 2^b$, $e^{d/4} < n \le e^{d/2}$.

We start by proving Theorem 1.1 (i). Lemma 5.1 shows that

$$j(n-h,q;\alpha,\beta) \ge \frac{0.02147}{d}\left(\log\left(\frac{1-\alpha}{1-\beta}\right) - \frac{4d}{(n-h)(1-\beta)}\right).$$

Using the definitions of α, β and γ we have $(n-h)(1-\beta) = \frac{1}{3}\gamma(n-h) = \frac{1}{3}(n+h) \ge \frac{1}{3}n$ and

$$\frac{1-\alpha}{1-\beta} = \begin{cases} 2 & \text{if } 1 \le \gamma \le 3/2 \\ 3/\gamma & \text{if } 3/2 \le \gamma \le 2. \end{cases}$$

Since $\log\left((1-\alpha)/(1-\beta)\right) \ge \log 3/2 > 0.4054$ and $1/\{(n-h)(1-\beta)\} \ge 3/n$ we have

$$j(n-h,q;\alpha,\beta) \ge \frac{0.02147}{d}\left(0.4054 - \frac{12d}{n}\right) = \zeta_1(n,d), \text{ say.}$$

Elementary calculus shows that $\zeta_1(n,d)\log n$ increases with n, for $d > 0$ and $n \ge 3$. First consider the case where $b = 4$ and $d = 2^4$ (in this case $54 = \lfloor e^4 \rfloor < n \le 2980 = \lfloor e^8 \rfloor$). Since $\zeta_1(700,16)\log 700 = 0.001152\ldots$, we have $\zeta_1(n,16)\log n > 0.001152$ for all $n \ge 700$. On the other hand, when $b \ge 5$, $d := 2^b$ and $e^{d/4} < n \le e^{d/2}$, we have $d/n < e^{-d/4}d \le 32e^{-8} < 0.01074$ and $\log n > d/4$. Thus $\zeta_1(n,d)\log n > \frac{0.02147}{d}(0.4054 - 12\cdot 0.01074)\frac{d}{4} = 0.00148\ldots$ in this case. Hence $j(n-h,q;\alpha,\beta) > \frac{0.001152}{\log n}$ holds for all $n \ge 700$. Finally, we have, applying Lemma 5.3 and Remark 5.4,

$$\begin{aligned}\pi_+ &\ge \ell(n,s,q;\alpha,\beta) = \theta(n,s,q)j(n-h,q,\alpha,\beta) \\ &\ge \frac{0.175 \times 0.001152}{\log n} > \frac{0.0002}{\log n}\end{aligned}$$

for all $n \ge 700$. This proves (i).

The proof of Theorem 1.1 (ii) is similar. In this case we we can take $\alpha = 1/3$ and $\beta = 2/3$ since the table shows that $z_{|V_2}$ is an involution of type $(2k, 2\ell)$ and $z_{|E_-(t)}$ of type (k,ℓ) so the former is

$(1/3, 2/3)$-balanced exactly when the latter is. A similar estimate for $j(n-h, q; 1/3, 2/3)$ shows that, for all $n \geq n_0 = 700$, and d chosen as the power of 2 such that $e^{d/4} < n \leq e^{d/2}$, we have

$$j(n-h, q; 1/3, 2/3) \geq \frac{0.02147}{d}(\log 2 - \frac{18d}{n}) = \zeta_2(n, d), \text{ say.}$$

Again we find that $\zeta_2(700, 16) \log 700 = 0.00247\ldots$ and conclude that $\zeta_2(n, 16) \log n > 0.00247$ for $n \geq 700$. Furthermore an argument similar to the one above shows that when $b \geq 5$ and $e^{d/4} \leq n \leq e^{d/2}$ then $\zeta_2(n, d) \log n > \frac{0.02147}{d}(0.6931 - 18 \times 0.01074)\frac{d}{4} = 0.00268\ldots$. Hence for all $n \geq 700$ we have

$$j(n-h, q; 1/3, 2/3) > \frac{0.00247}{\log n}$$

and so

$$\pi_- \geq \ell(n, s, q; 1/3, 2/3) > \frac{0.175 \times 0.00247}{\log n} > \frac{0.0002}{\log n}.$$

This proves (ii) and completes the proof of Theorem 1.1 with $\kappa := 0.0002$ and $n_0 := 700$. □

References

[1] C. Altseimer and A. Borovik, Probabilistic recognition of orthogonal and symplectic groups. In: *Groups and Computation III.* Editors: W.M. Kantor and Á. Seress, de Gruyter, Berlin, New York (2001), pp. 1–20. With corrections in http://www.ma.umist.ac.uk/avb/pdf/alt-avb4.pdf.

[2] J. N. Bray, An improved method for generating the centralizer of an involution. *Arch. Math. (Basel)* **74** (2000), 241–245.

[3] Jason Fulman. Cycle indices for the finite classical groups. *J. Group Theory* **2** (1999), 251–289.

[4] Jason Fulman, Peter M. Neumann and Cheryl E. Praeger. A generating function approach to the enumeration of matrices in classical groups over finite fields. *Memoirs Amer. Math. Soc.* **176** (2005) No. 830.

[5] R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl, Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc.* **78** (1999), 167–214.

[6] P. E. Holmes, S. A. Linton, E. A. O'Brien, A. J. E. Ryba and R. A. Wilson. Constructive membership in black-box groups. *J. Group Theory* **11** (2008), 747–763.

[7] C.R. Leedham-Green and E.A. O'Brien, Constructive recognition of classical groups in odd characteristic. *J. Algebra* **322** (2009), 833–881.

[8] 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.

[9] Alice C. Niemeyer and Cheryl E. Praeger. A recognition algorithm for classical groups over finite fields. *Proc. Lond. Math. Soc.* **77** (1998), 117–169.

[10] Alice C. Niemeyer and Cheryl E. Praeger. A recognition algorithm for non-generic classical groups over finite fields. *J. Austral. Math. Soc. Ser. A* **67** (1999), 223–253.

[11] Christopher W. Parker and Robert A. Wilson, Recognising simplicity of black-box groups by constructing involutions and their centralisers. *J. Algebra* **324** (2010), 886–915.

[12] Cheryl E. Praeger and Ákos Seress. Probabilistic generation of finite classical groups in odd characteristic by involutions. *J. Group Theory* **14** (2011), 521–545.

[13] Cheryl E. Praeger and Ákos Seress. Regular semisimple elements and involutions in finite general linear groups of odd characterisitic. *Proc. Amer. Math. Soc.* **140** (2012), 3003–3015.

[14] G. E. Wall. Counting cyclic and separable matrices over a finite field. *Bull. Austral. Math. Soc.* **60** (1999), 253–284.

J. D. Dixon, School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada

E-mail address: jdixon@math.carleton.ca

C. E. Praeger, School of Physics, Mathematics and Computing, The University of Western Australia, Crawley, WA 6009, Australia

E-mail address: cheryl.praeger@uwa.edu.au