Available online at www.sciencedirect.com
ScienceDirect
Journal of Combinatorial Theory, Series A 115 (2008) 442–465
Journal of Combinatorial Theory
Series A
www.elsevier.com/locate/jcta

Sets of elements that pairwise generate a linear group ☆

J.R. Britnell [a,1], A. Evseev [b,2], R.M. Guralnick [c,3], P.E. Holmes [d,4], A. Maróti [c,3,5]

[a] *Pembroke College, Cambridge, CB2 1RF, UK*
[b] *Mathematical Institute, University of Oxford, Oxford, OX2 3LB, UK*
[c] *Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA*
[d] *DPMMS, Centre for Mathematical Sciences, University of Cambridge, Cambridge CB3 0BW, UK*

Received 25 September 2006

Available online 10 September 2007

Communicated by William M. Kantor

Abstract

Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. Define a (simple) graph $\Gamma = \Gamma(G)$ on the set of elements of G by connecting two vertices by an edge if and only if they generate G. Suppose that n is at least 12. Then the maximum size of a complete subgraph in Γ is equal to the chromatic number of Γ if $n \not\equiv 2 \pmod 4$, or if $n \equiv 2 \pmod 4$, q is odd and $G = (P)SL(n,q)$. This work was motivated by a question of Blackburn.

Keywords: General linear group; Covering; Pairwise generating set

☆ Some of this work was carried out during the Asymptotic Group Theory Conference at the Institute for Advanced Studies in Jerusalem. The second, third, and fifth authors thank the organizers for financial support.

E-mail addresses: j.r.britnell@ncl.ac.uk (J.R. Britnell), evseev@maths.ox.ac.uk (A. Evseev), guralnic@usc.edu (R.M. Guralnick), P.E.Holmes@dpmms.cam.ac.uk (P.E. Holmes), maroti@usc.edu (A. Maróti).

[1] Present address: School of Mathematics & Statistics, Newcastle University, Newcastle upon Tyne, NE1 7RU, UK.

[2] Research of the second author was supported by a Scatcherd European Scholarship.

[3] Research of the third and fifth authors was supported by NSF Grant DMS 0140578.

[4] The fourth author was supported by a Royal Society Dorothy Hodgkin fellowship and the EPSRC grant EP/C523229/1(P).

[5] Research of the fifth author was partially supported by OTKA T049841.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2007.07.002

1. Introduction

Let G be a finite group that can be generated by two elements. We define $\mu(G)$ to be the largest positive integer m so that there exists a subset X in G of order m with the property that any distinct pair of elements of X generates G. Let n be a positive integer, q a prime power, and V the n-dimensional vector space over the field of q elements. Let $[x]$ denote the integer part of the real number x. We have

Theorem 1.1. *Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. Let b be the smallest prime factor of n, and let $N(b)$ be the number of proper subspaces of V of dimensions not divisible by b. If $n \geqslant 12$, then*

$$\mu(G) = \frac{1}{b}\prod_{\substack{i=1\\ b\nmid i}}^{n-1}\left(q^n - q^i\right) + \left[N(b)/2\right].$$

Let G be a non-cyclic finite group. Cohn [9] defined the function $\sigma(G)$ to be the least integer k such that G is the union of k of its proper subgroups. Much is known about $\sigma(G)$ for various groups G. For example, for a finite solvable group G, Tomkinson [30] showed that $\sigma(G) = q+1$ where q is the size of the smallest chief factor group of G that has more than one complement. There are many papers on covering non-solvable groups by proper subgroups. See Lucido [23], Bryce, Fedri, Serena [8], Maróti [25], and Holmes [17]. For an interesting survey of the subject see Serena [28]. If G is a non-cyclic finite group that can be generated by two elements, then $\mu(G) \leqslant \sigma(G)$.

Let S_n be the symmetric group on n letters. Maróti [25] proved that the set of prime numbers n for which $\mu(S_n) = \sigma(S_n) = 2^{n-1}$ has density 1 in the set of all primes. In a beautiful paper, this result was considerably extended by Blackburn [3] who showed that if n is a sufficiently large odd integer, then $\mu(S_n) = \sigma(S_n) = 2^{n-1}$, and that if n is a sufficiently large integer congruent to 2 modulo 4, then $\mu(A_n) = \sigma(A_n) = 2^{n-2}$ for the alternating group A_n. In the same paper Blackburn asked what the relationship between the numbers $\sigma(G)$ and $\mu(G)$ is when G is a finite simple group. For example, is it true that $\sigma(G)/\mu(G) \to 1$ as $|G| \to \infty$? An affirmative answer to this question in the special case when G is a projective special linear group is given in Section 6. In many cases we can say more.

Theorem 1.2. *Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. Let b be the smallest prime factor of n, let $\begin{bmatrix} n \\ k \end{bmatrix}_q$ be the number of k-dimensional subspaces of the n-dimensional vector space V, and let $N(b)$ be the number of proper subspaces of V of dimensions not divisible by b. Suppose that $n \geqslant 12$. Then if $n \not\equiv 2 \pmod 4$, or if $n \equiv 2 \pmod 4$, q odd and $G = (P)SL(n,q)$, then*

$$\sigma(G) = \mu(G) = \frac{1}{b}\prod_{\substack{i=1\\ b\nmid i}}^{n-1}\left(q^n - q^i\right) + \left[N(b)/2\right].$$

Otherwise $\sigma(G) \neq \mu(G)$ and

$$\sigma(G) = \frac{1}{2}\prod_{\substack{i=1\\ 2\nmid i}}^{n-1}\left(q^n - q^i\right) + \sum_{\substack{k=1\\ 2\nmid k}}^{(n/2)-1}\begin{bmatrix} n \\ k \end{bmatrix}_q + \frac{q^{n/2}}{q^{n/2}+1}\begin{bmatrix} n \\ n/2 \end{bmatrix}_q + \epsilon$$

where $\epsilon = 0$ if q is even and $\epsilon = 1$ if q is odd.

Theorem 1.2 extends earlier results of Bryce, Fedri, Serena [8]. Also, the formulae for $\sigma(G)$ for the groups $(P)GL(3,q)$, $(P)SL(3,q)$ was kindly communicated to one of us by Serena [29].

Define a (simple) graph $\Gamma = \Gamma(G)$ on the set of elements of the non-cyclic finite group G by connecting two distinct vertices by an edge if and only if they generate G. Let $\chi(\Gamma)$ be the chromatic number of Γ, that is, the least number of colors needed to color the vertices of Γ in such a way that adjacent vertices receive different colors. In other words, $\chi(\Gamma)$ is the minimum number k such that $V(\Gamma)$ can be partitioned into k stable sets. We clearly have $\mu(G) \leqslant \chi(\Gamma) \leqslant \sigma(G)$. Theorems 1.1 and 1.2 imply the following.

Corollary 1.1. *Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$, and let $\Gamma = \Gamma(G)$ be as above. Let $n \geqslant 12$. Then the maximum size of a complete subgraph in Γ is equal to the chromatic number of Γ if $n \not\equiv 2 \pmod 4$, or if $n \equiv 2 \pmod 4$, q is odd and $G = (P)SL(n,q)$.*

A couple of remarks need to be made.

A quick corollary to the solution of Dixon's conjecture, stated by Liebeck and Shalev in [21] (see Corollary 1.7), is that there exists a universal constant c so that $\mu(G) \geqslant c \cdot n$ for any finite simple group G where n denotes the minimal index of a proper subgroup in G.

A group is said to have spread at least k if, for any non-identity $x_1, \ldots, x_k \in G$, there is some $y \in G$ such that $G = \langle x_i, y\rangle$ whenever $1 \leqslant i \leqslant k$. The number $s(G)$ denotes the largest integer k so that G has spread at least k. There are many papers on spread, see, for example, Breuer, Guralnick, Kantor [4]. It is easy to see that for any non-cyclic finite group G that can be generated by two elements, the inequality $s(G) < \mu(G)$ holds.

We also note that similar work on the commuting graph of a finite group was carried out by Pyber [27] and Brown [6,7].

2. Covering linear groups

The purpose of this section is to give two upper bounds for $\sigma(G)$. In later sections we will show that, in many cases, these bounds are exact.

Let G be a finite non-cyclic group. Here and throughout this paper, a set $\mathcal{H}$ of (mostly maximal) proper subgroups of G is said to be a covering for G if the set-theoretic union of all members of $\mathcal{H}$ is G. A covering $\mathcal{H}$ is minimal if $|\mathcal{H}| = \sigma(G)$. Let V be the n-dimensional vector space over the field of q elements. Let us denote the number of k-dimensional subspaces of V by $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Lemma 2.1. *Let b be the smallest prime divisor of the integer n. Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. Then we have*

$$\sigma(G) \leqslant \frac{|GL(n,q)|}{|GL(n/b, q^b).b|} + \sum_{\substack{k=1 \\ b\nmid k}}^{[n/2]} \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

Proof. We claim that the set $\mathcal{H}$ consisting of all conjugates of the extension field subgroup $GL(n/b, q^b).b$ and all stabilizers of all subspaces of V having dimensions at most $[n/2]$ and not a multiple of b is a covering for $GL(n,q)$. This would prove the lemma for $G = GL(n,q)$. This claim would also imply the lemma for $G = SL(n,q)$ since no member of $\mathcal{H}$ contains $SL(n,q)$. All members of $\mathcal{H}$ contain the center of $GL(n,q)$, and it is easy to see that $\sigma(PGL(n,q)) \leqslant |\mathcal{H}|$.

Similarly, our claim would also give $\sigma(PSL(n,q)) \leqslant |\mathcal{H}|$. In the remaining part of the proof we will verify our claim.

Let x be an element of $GL(n,q)$, and let f be its characteristic polynomial. If f is irreducible, then, by Schur's lemma and Wedderburn's theorem, x is contained in some conjugate of $GL(n/b,q^b).b$. So we may (and do) assume that f is not an irreducible polynomial.

If f has an irreducible factor of degree k, then, by the theorem on rational canonical forms, x must leave a k-dimensional subspace invariant. So if k is not divisible by b, then x is an element of some member of the above set. Hence we may (and do) assume that the degree of each irreducible factor of f is divisible by b.

Put $f = f_1^{m_1} \dots f_\ell^{m_\ell}$ where each f_i is an irreducible polynomial of degree $r_i b$ for some positive integer r_i. Then, by the theorem on rational canonical forms, $V = \bigoplus_{i=1}^{\ell} V_i$ viewed as an $\langle x\rangle$-module where for each i the linear transformation x has characteristic polynomial ${f_i}^{m_i}$ on the module V_i. Now each module V_i contains an irreducible submodule of dimension $r_i b$, and so by Schur's lemma and Wedderburn's theorem, the centralizer of x contains a field of order $q^{r_i b}$, and hence a field of order q^b. This means that we may view x as a linear transformation on V viewed as an n/b-dimensional space over a field of q^b elements, and so x is an element of a conjugate of $GL(n/b,q^b).b$.

This completes the proof of the lemma. □

Lemma 2.2. *Let n be a positive integer congruent to* 2 mod 4. *If q is even, then let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. If q is odd, then let G be any of the groups $(P)GL(n,q)$. Then we have*

$$\sigma(G) \leqslant \frac{|GL(n,q)|}{|GL(n/2,q^2).2|} + \sum_{\substack{k=1\\ 2\nmid k}}^{(n/2)-1} \begin{bmatrix} n \\ k \end{bmatrix}_q + \frac{q^{n/2}}{q^{n/2}+1} \begin{bmatrix} n \\ n/2 \end{bmatrix}_q + \epsilon$$

where $\epsilon = 0$ if q is even and $\epsilon = 1$ if q is odd.

Proof. Let q be even. In this case it is sufficient to show that a proportion of the subspace stabilizers of $n/2$-dimensional subspaces can be removed from the covering established in the proof of Lemma 2.1, and that this proportion is $1/(q^{n/2}+1)$. This is exactly the proportion of $n/2$-dimensional subspaces of V which contain a given non-zero vector v. A transformation x which preserves such a subspace either preserves another subspace of dimension at most $n/2$, and not containing v, or else is indecomposable. In the indecomposable case, its minimum polynomial is f^2 for some irreducible polynomial f of degree $n/2$. But then x^2 can easily be seen to lie inside a copy of $GL(1,q^n)$. We shall show that x itself lies inside some copy of $GL(1,q^n).2$, and hence of $GL(n/2,q^2).2$. This will establish the lemma.

Let y be an element of a Singer cycle whose minimum polynomial is f, and let τ be the involutory automorphism in $GL(1,q^n).n$. Then τ centralizes y, and hence $y\tau$ has order $2(q^{n/2}-1)$. It cannot lie inside a Singer cycle of $GL(n,q)$, since its order does not divide q^n-1, and hence its minimum polynomial is reducible. But since $(y\tau)^2 = y^2$, the eigenvalues of $y\tau$ are the same as those of y (since q is even). It follows that $y\tau$ has minimum polynomial f^2, and hence that it is conjugate to x, which completes the proof.

Now let q be odd. Then there is a subgroup N in G of index 2 consisting of all elements of G with determinants equal to the even powers of a generator of the cyclic group $GF(q)^*$. Note that N contains the center of G. Let $\mathcal{H}$ be the set of all conjugates of the extension field subgroup $GL(n/2,q^2).2$, all stabilizers of all subspaces of V having odd dimensions at most $(n/2)-1$,

and all stabilizers of all $n/2$-dimensional subspaces of V which do not contain a prescribed non-zero vector v. By the above it follows that any element $x \in G$ is contained in some member of $\mathcal{H}$ unless x has minimal polynomial f^2 for some irreducible polynomial f of degree $n/2$. Since such an exceptional element lies in N, we see that $\mathcal{H} \cup \{N\}$ is a covering for G. □

3. Pairing off subspaces

Write V as the direct sum of complementary subspaces U and W. In the next section we will define certain linear transformations which act irreducibly on both U and W. We want many such elements in the special and general linear groups, and for this reason, we wish to find as many distinct pairs of complementary subspaces (U, W) as possible so that every subspace appears at most once as the entry of some pair. Let the dimensions of U and W be k and $n-k$ respectively, and let $\mathcal{S}_r$ be the set of r-dimensional subspaces of V.

If $1 \leqslant k < n/2$, then there exists a bijection φ_k between the sets $\mathcal{S}_k$ and $\mathcal{S}_{n-k}$ with the property that $V = U \oplus U\varphi_k$ whenever $U \in \mathcal{H}_k$. Such a bijection exists by the following reason. Define a bipartite graph with vertex set $\mathcal{S}_k \cup \mathcal{S}_{n-k}$ so that there is an edge between $U \in \mathcal{S}_k$ and $W \in \mathcal{S}_{n-k}$ if and only if $V = U \oplus W$. Since this graph is regular and $|\mathcal{S}_k| = |\mathcal{S}_{n-k}|$, there exists a matching from $\mathcal{S}_k$ to $\mathcal{S}_{n-k}$ and hence one from $\mathcal{S}_{n-k}$ to $\mathcal{S}_k$ by Hall's (or König's) theorem.

From now on assume n is even and put $k = n/2$. Put $N = |\mathcal{S}_{n/2}| = \begin{bmatrix} n \\ n/2 \end{bmatrix}_q$. The following lemma shows that N is odd if q is even, and N is even if q is odd.

Lemma 3.1. *N is even if and only if q is odd.*

Proof.

$$N = \frac{\prod_{i=1}^{k}(q^{k+i}-1)}{\prod_{i=1}^{k}(q^i-1)}.$$

This number is clearly odd if q is even. Suppose q is odd. It is well known that the Grassmannian space of all k-dimensional subspaces of V can be represented as a disjoint union of $\binom{2k}{k}$ affine spaces over the ground field $\mathbb{F}_q$. The number of elements in each of those affine spaces is a power of q, so is odd. Since $\binom{2k}{k}$ is always even, N is even. □

We hope to find a matching of maximal cardinality on the set $\mathcal{S}_{n/2}$ with the property that only complementary subspaces are to be paired together. If ψ is such a matching, then we will use the equivalent notations $U\psi = W$ and $W\psi = U$ to mean that the complementary subspaces U and W are paired together in the matching ψ. We will show that the number of pairs in such a maximal matching is $[N/2]$.

For an arbitrary (undirected) graph Δ with N vertices, let $\nu(\Delta)$ be its matching number, that is the greatest number l such that there exist distinct vertices $a_1, \ldots, a_l, b_1, \ldots, b_l$ of Δ such that a_i is connected to b_i by an edge whenever $1 \leqslant i \leqslant n$. Define

$$\operatorname{def}(\Delta) = N - 2\nu(\Delta)$$

to be the *deficiency* of Δ.

Let $\Gamma = (\mathcal{V}, \mathcal{E})$ be the undirected graph whose set of vertices $\mathcal{V}$ is the set of all k-dimensional subspaces of V, and whose set of edges is

$$\mathcal{E} = \big\{(A, B) \in \mathcal{V} \times \mathcal{V}\colon\ A \cap B = \{0\}\big\}.$$

Our aim is to prove the following result.

Theorem 3.1. *If q is odd, then* $\operatorname{def}(\Gamma) = 0$. *If q is even, then* $\operatorname{def}(\Gamma) = 1$ *unless* $q = 2$ *and* $n = 4$.

We note that the statement of the above theorem is true even if $(n, q) = (4, 2)$, but here we will not give an explicit matching for that special case.

If S is a subset of the set of vertices of a graph Δ, then let $\Delta - S$ be the graph obtained from Δ by throwing away all the vertices in S and all the edges incident to at least one of those vertices. Let $c_o(\Delta)$ denote the number of connected components of Δ with an odd number of vertices. The following matching theorem, known as Berge formula, will be our main tool.

Theorem 3.2. *(See [22, 3.1.14].) For any graph Δ,*

$$\operatorname{def}(\Delta) = \max\bigl\{c_o(\Delta - S) - |S|\colon\ S \subseteq V(\Delta)\bigr\}.$$

In order to apply this result to Γ, we shall estimate the number of edges in Γ. Since $GL(V)$ acts transitively on the vertices of Γ and each element of $GL(V)$ induces an automorphism of Γ, the graph Γ is regular. Let $N = |V(\Gamma)|$. Let d be the degree of each vertex A of Γ, i.e. the number of edges incident to A.

Lemma 3.2. *If $q > 2$, then $d \geqslant N/2$. If $q = 2$, then $d \geqslant 2N/7$.*

Proof. We adopt a probabilistic approach. We will write $\mathbb{P}(J)$ for the probability of the event J and $\mathbb{P}(J|K)$ for the probability of the event J subject to the event K.

Let A be a vertex of Γ. Choose a basis $\{e_1, \dots, e_n\}$ of V so that A is spanned by $\{e_1, \dots, e_k\}$. Suppose k vectors $v_1, \dots, v_k$ are chosen at random from V. (Here and in what follows we use the uniform distribution.) Let Ω be the set of all such choices, so $\mathbb{P}(\Omega) = 1$. Let I be the event that $v_1, \dots, v_k$ are linearly independent. Write $v_i = v_{1i}e_1 + \cdots + v_{ni}e_n$ (where $v_{ji} \in \mathbb{F}_q$), and let M be the matrix

$$\begin{pmatrix} v_{k+1,1} & v_{k+1,2} & \dots & v_{k+1,k} \\ v_{k+2,1} & v_{k+2,2} & \dots & v_{k+2,k} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \dots & v_{nk} \end{pmatrix}.$$

Let B be the subspace $\langle v_1, \dots, v_k\rangle$. If the event I occurs, then B is a k-dimensional subspace, and subject to I the distribution of B among the vertices of Γ is uniform. Let E be the event that M is non-singular. Observe that, if I happens, then $A \cap B = \{0\}$ if and only if E occurs. So

$$\mathbb{P}\bigl(A \cap B = \{0\}|I\bigr) = \mathbb{P}(E|I).$$

If I does not occur, then the matrix M is singular. So $\mathbb{P}(E|I) \geqslant \mathbb{P}(E)$. Hence, it suffices to show that $\mathbb{P}(E) \geqslant 1/2$ ($\mathbb{P}(E) \geqslant 2/7$ if $q = 2$). Let $w_1, \dots, w_k$ be the rows of M. Observe that these are independent and uniformly distributed among the vectors in $\mathbb{F}_q^k$. For $1 \leqslant i \leqslant k$, let F_i be the event that w_i is a linear combination of $w_1, \dots, w_{i-1}$. Then $E = \Omega \setminus (F_1 \cup F_2 \cup \cdots \cup F_k)$. Since the subspace $\langle w_1, \dots, w_{i-1}\rangle$ contains at most q^{i-1} elements, $\mathbb{P}(F_i) \leqslant q^{i-1-k}$. Hence, if $q > 2$,

$$\mathbb{P}(E) \geqslant 1 - \sum_{i=1}^{k}\bigl(\mathbb{P}(F_i)\bigr) \geqslant 1 - \sum_{j=1}^{k} q^{-j} \geqslant 1 - \frac{1}{q-1} \geqslant \frac{1}{2}.$$

(Here the second inequality is obtained by substituting $j = k - i + 1$.) Assume now that $q = 2$. Then

$$\mathbb{P}(E) = \prod_{i=1}^{k} \mathbb{P}(\text{not } F_i | \text{not } F_1,\ \text{not } F_2, \ldots, \text{not } F_{i-1}) = \prod_{i=1}^{k} \bigl(1 - 2^{i-k-1}\bigr) \geqslant \alpha$$

where $\alpha = \prod_{j=1}^{\infty}(1 - 2^{-j})$. We can estimate α by expanding $\log(\alpha)$ using Taylor series:

$$-\log(\alpha) = -\sum_{j=1}^{\infty} \log\bigl(1 - 2^{-j}\bigr) = \sum_{j=1}^{\infty}\sum_{l=1}^{\infty} \frac{2^{-jl}}{l} = \sum_{l=1}^{\infty} \frac{1}{l(2^l - 1)} \leqslant \sum_{l=1}^{10} \frac{1}{l(2^l - 1)} + 2^{-10}.$$

A computer-assisted calculation shows that the exponent of the last constant is smaller than 3.466, so $\alpha > \frac{2}{7}$. □

Lemma 3.3. *Suppose $q = 2$. Let A and B be vertices of Γ. Then A and B have at least $2d/7$ and, if $A \neq B$, at most $d/2$ common neighbours in Γ.*

Proof. We use a probabilistic approach again. Let $r = \dim(A \cap B)$. Choose a basis $e_1, \ldots, e_n$ of V so that

$$A = \langle e_1, \ldots, e_k \rangle \quad \text{and}$$
$$B = \langle e_1, \ldots, e_r, e_{k+1}, e_{k+2}, \ldots, e_{n-r} \rangle.$$

As in the previous lemma, let $v_1, \ldots, v_k$ be vectors chosen randomly from a uniform distribution on V. Let Ω be the set of all such choices. Write $v_i = v_{1i}e_1 + \cdots + v_{ni}e_n$. Let $C = \langle v_1, \ldots, v_k \rangle$. For $j = 1, \ldots, n$, let $w_j = (v_{j1}, v_{j2}, \ldots, v_{jk}) \in \mathbb{F}_q^k$. These are independent and uniformly distributed among the elements of $\mathbb{F}_q^k$. Let J_A be the event that $w_{k+1}, \ldots, w_n$ are linearly independent, and let J_B be the event that $w_{r+1}, \ldots, w_k, w_{n-r+1}, w_{n-r+2}, \ldots, w_n$ are linearly independent. If J_A (or J_B) occurs, then $\dim(C) = k$. Assuming $\dim(C) = k$, $A \cap C = \{0\}$ (respectively, $B \cap C = \{0\}$) if and only if J_A (respectively, J_B) occurs. Hence, assuming $A \neq B$, the present lemma is equivalent to the inequality

$$\frac{2}{7} \leqslant \mathbb{P}(J_B | J_A) \leqslant \frac{1}{2}.$$

(The case $A = B$ is trivial.) For $i = 1, \ldots, k - r$, let F_i be the event that w_{r+i} is a linear combination of $w_{r+i+1}, w_{r+i+2}, \ldots, w_k, w_{n-r+1}, \ldots, w_n$. Then

$$J_A \cap J_B = J_A \setminus (F_1 \cup \cdots \cup F_{k-r}).$$

It follows that

$$\begin{aligned}\mathbb{P}(J_B | J_A) &\leqslant \mathbb{P}(\Omega \setminus F_1 | w_{r+2}, \ldots, w_k, w_{n-r+1}, \ldots, w_n \text{ are linearly independent, and } J_A) \\ &\leqslant \frac{1}{2}.\end{aligned}$$

On the other hand,

$$\mathbb{P}(J_B | J_A) = \mathbb{P}(J_B | w_{n-r+1}, \ldots, w_n \text{ are linearly independent}) \geqslant \mathbb{P}(J_B).$$

This last probability is the same as the probability that a randomly chosen $(k \times k)$-matrix over $\mathbb{F}_q$ is non-singular, which was shown to be at least $2/7$ in the proof of Lemma 3.2. □

We now prove Theorem 3.1. If $q > 2$, then $d \geqslant N/2$, hence by Theorem 3 of [12], the graph Γ contains a Hamiltonian cycle. Using the edges in this cycle, one obtains the required matching. (Alternatively, one can derive the result from Theorem 3.2.)

Assume $q = 2$ and $n \geqslant 6$ (the case $n = 2$ is trivial). Suppose for contradiction that $\mathrm{def}(\Gamma) > 1$, so $\mathrm{def}(\Gamma) \geqslant 3$ because of parity considerations. Then by Theorem 3.2, there is a set S of vertices of Γ such that $c_o(\Gamma - S) \geqslant |S| + 3$. Let N_i be the number of connected components of $\Gamma - S$ that consist of i vertices. Write $m = c_o(\Gamma - S)$. Then $m = \sum_{i=0}^{\infty} N_{2i+1}$ and

$$m \geqslant |S| + 3. \tag{1}$$

By counting the number of vertices in odd components, we obtain

$$|S| + \sum_{i=0}^{\infty} (2i+1) N_{2i+1} \leqslant N. \tag{2}$$

Claim 3.1. $N_1 > 0$.

Let l be the smallest integer such that $N_{2l+1} > 0$. Then (2) implies that

$$|S| + (2l+1)m \leqslant N.$$

Using (1), we derive

$$(2l+2)|S| \leqslant N. \tag{3}$$

However, by Lemmata 3.2 and 3.3, any two vertices in Γ have at least $4N/49$ common neighbours. Since $\Gamma - S$ is not connected, $|S| \geqslant 4N/49$. We conclude that $2l + 2 \leqslant 12$, i.e. $l \leqslant 5$. So there exists a connected component Λ of $\Gamma - S$ of size at most 11. Any vertex of Λ is connected to at least $d - 10$ vertices of Γ outside Λ, so $|S| \geqslant d - 10$. If $l \geqslant 1$, the inequality (3) gives

$$4d - 40 \leqslant N.$$

However, $d \geqslant 2N/7$ by Lemma 3.2, so $N \leqslant 280$. This is not the case if $n \geqslant 6$, so $l = 0$.

Claim 3.2. $N_1 \leqslant 5|S|/7$ *and* $|S| \geqslant d$.

Let X be the set of all vertices in $\Gamma - S$ that are only connected by edges to vertices in S. By Claim 3.1, X is non-empty, hence $|S| \geqslant d$. Also, the number r of edges between vertices in X and those in S is equal to $d|X| = dN_1$. On the other hand, let A be a vertex in S. Suppose $(A, B) \in \mathcal{E}$, where $B \in X$. By Lemma 3.3, A and B have at least $2d/7$ common neighbours, all of which must lie in S. Therefore every vertex in S is connected to at most $5d/7$ vertices in X, so $m \leqslant 5d|S|/7$. We have

$$dN_1 = r \leqslant \frac{5}{7} d|S|,$$

and the claim follows.

Claim 3.3. $N_3 > 0$ *or* $N_5 > 0$.

Suppose $N_3 = N_5 = 0$. Let $t = \sum_{i=3}^{\infty} N_{2i+1}$. By (2),

$$|S| + N_1 + 7t \leqslant N.$$

Combining this with (1) and using $m = N_1 + t$, we get

$$2|S| + 6t \leqslant N.$$

Since $N_1 \leqslant 5|S|/7$, the inequality (1) gives $t \geqslant 2|S|/7$. Hence

$$\frac{26}{7}|S| \leqslant N.$$

However, $|S| \geqslant d \geqslant 2N/7 > 7N/26$, a contradiction.

We are now in a position to finish the proof. By Claim 3.3, there is a component Λ of $\Gamma - S$ that consists of 3 or 5 vertices. Let A_1, A_2 and A_3 be three of those vertices. Each A_j is connected to at least $d - 4$ vertices in S, and any two vertices A_j, A_l $(j \neq l)$ have at most $d/2$ common neighbours in Γ. Hence by the inclusion–exclusion formula,

$$|S| \geqslant 3(d-4) - \frac{3}{2}d = \frac{3}{2}d - 12. \tag{4}$$

Let $t = \sum_{i=1}^{k} N_{2i+1}$. Similarly to the proof of Claim 3.3, we have

$$|S| + N_1 + 3t \leqslant N, \quad \text{hence}$$
$$2|S| + 2t \leqslant N;$$

also, $t \geqslant 2|S|/7$. Thus

$$\frac{18}{7}|S| \leqslant N.$$

On the other hand, using (4) and the inequality $d \geqslant 2N/7$, we get

$$|S| \geqslant \frac{3}{7}N - 12 > \frac{7}{18}N$$

because $N > 303$ (here we use the condition that $n \geqslant 6$ again). This contradiction proves the theorem.

4. Overgroups of special elements

We now define certain elements of $GL(n,q)$ and $SL(n,q)$. A generator of a Singer cycle in $GL(n,q)$ will be called an element of type GL0. For every positive integer k so that $1 \leqslant k < n/2$ establish a bijection φ_k from the set $\mathcal{S}_k$ of all k-dimensional subspaces of V to the set $\mathcal{S}_{n-k}$ of all $(n-k)$-dimensional subspaces of V in such a way that for every k-dimensional subspace U we have $V = U \oplus U\varphi_k$. For an arbitrary positive integer k such that $1 \leqslant k < n/2$, $b \nmid k$, and for an arbitrary vector space $U \in \mathcal{S}_k$ an element of the form

$$\begin{pmatrix} {S_U}^{(q-1)} & 0 \\ 0 & S_{U\varphi_k} \end{pmatrix}$$

is called an element of type GLk where S_U is a generator of a Singer cycle on U and $S_{U\varphi_k}$ is a generator of a Singer cycle on $U\varphi_k$. The $q-1$ power of an element of type GL0, GLk is called an element of type SL0, SLk respectively.

Let q be odd and let n be a positive integer congruent to 2 modulo 4. An element g of $GL(n,q)$ is said to be of type GLOdd* if there exist complementary subspaces U and U' of dimensions $n/2$ such that g has the form

$$\begin{pmatrix} S_{U'} & I \\ 0 & S_U \end{pmatrix}$$

where I is the $n/2$-by-$n/2$ identity matrix and $S_{U'}$, S_U are $GL(n/2,q)$-conjugate elements acting as a generator of a Singer cycle on the vector space U', U, respectively. The $q-1$ power of an element of type GLOdd* is called an element of type SLOdd.

Let q be odd, and let n be a positive integer congruent to 2 modulo 4. Let φ be a matching on the set of all $n/2$-dimensional subspaces $\mathcal{S}_{n/2}$ of V so that for any $n/2$-dimensional subspace U we have $V = U \oplus U\varphi$. Such a matching exists by Theorem 3.1. An element g in $GL(n,q)$ is said to be of type GLOdd if g has the form

$$\begin{pmatrix} S_U & 0 \\ 0 & S_{U\varphi}^2 \end{pmatrix}$$

where S_U, $S_{U\varphi}^2$ denotes a generator and the square of a generator of a Singer cycle on U and $U\varphi$, respectively.

Let q be even, and let n be a positive integer congruent to 2 modulo 4. Fix an $n/2$-dimensional subspace W in V. Let φ_W be a matching on $\mathcal{S}_{n/2}$ so that for any $n/2$-dimensional subspace U different from W we have $V = U \oplus U\varphi_W$ and $W\varphi_W = W$. Such a matching exists by Theorem 3.1. An element g in $GL(n,q)$ is said to be of type GLE if there exists some $n/2$-dimensional subspace $U \neq W$ so that g has the form

$$\begin{pmatrix} S_U & 0 \\ 0 & S_{U\varphi_W}^2 \end{pmatrix}$$

where S_U, $S_{U\varphi_W}^2$ denotes a generator and the square of a generator of a Singer cycle on U and $U\varphi_W$, respectively. Finally, an element of $SL(n,q)$ is said to be of type SLE if it is the $q-1$ power of an element of type GLE.

We use the lists of the Guralnick, Penttila, Praeger, Saxl [14] paper and the Phd thesis of Joseph DiMuro [11], the Kantor [19] and the Bereczky [2] results to obtain all maximal overgroups of elements of types GL0, GLk, SL0, SLk, GLOdd*, SLOdd, GLE, SLE, GLOdd for $n \geqslant 5$.

Theorem 4.1. *Let V be the n-dimensional vector space over the field of q elements. Let k be a positive integer so that $1 \leqslant k < n/2$ and that k is not divisible by the smallest prime divisor of n. Let g be an element of type GL0, SL0, GLk, SLk, GLE, SLE, GL0dd*, GLOdd, or SL0dd. If g is of type GL0, GLk, GLE, GLOdd*, or GL0dd, then put $G = GL(n,q)$. Otherwise let $G = SL(n,q)$. Let M be a maximal subgroup of G containing g.*

(1) *If g is of type GL0 or SL0 and $n \geqslant 4$, then M is an extension field subgroup $(GL(n/a,q^a).a) \cap G$ for some prime a. No other G-conjugate of M contains g.*
(2) *If g is of type GLk or SLk and $n \geqslant 4$, $(n,q) \neq (4,2)$, $(11,2)$, then M is one of a conjugate copies of the extension field subgroup $(GL(n/a,q^a).a) \cap G$ for some prime a dividing k, or is a maximal reducible subgroup of G leaving the same k-dimensional or $(n-k)$-dimensional subspace invariant that g does.*
(3) *If g is of type GLE, SLE, GL0dd*, GLOdd or SL0dd, and $n \geqslant 14$ is congruent to 2 modulo 4, then M is one of $2a$ conjugate copies of the extension field subgroup $(GL(n/a,q^a).a) \cap G$ for some prime a different from 2, is a maximal reducible subgroup of G leaving the same k-dimensional or $(n-k)$-dimensional subspace invariant that g does, is an imprimitive linear group conjugate to $(GL(n/2,q) \wr S_2) \cap G$, or it is the stabilizer of a tensor product decomposition of V conjugate to one of the $q^{n/2}-1$ conjugate copies of the group $(GL(2,q) \otimes GL(n/2,q)) \cap G$.*

An element of type GL0 is a generator of a Singer cycle (or a Singer subgroup) in $GL(n,q)$. A Singer cycle can be written in the form $GL(1,q^n)$. If H is a Singer cycle, then a generator of the group $H \cap SL(n,q)$ is an element of type SL0. Part (1) of Theorem 4.1 follows from the two theorems and the two lemmas given below.

Much of our basic observations on Singer cycles are found on pp. 187–189 in Huppert [18].

Theorem 4.2. *(See Kantor [19].) Each overgroup of a Singer subgroup $GL(1,q^n)$ is an extension field type subgroup, that is, a subgroup lying between a copy of $GL(n/a,q^a)$ and its normalizer $GL(n/a,q^a).a$ where a is a divisor of n.*

Theorem 4.3. *(See Bereczky [2].) Let $n \geqslant 2$ and $(n,q) \neq (2,2),\ (2,5),\ (2,7),\ (2,9),\ (3,4)$. Let H be a Singer subgroup in $GL(n,q)$. Then each overgroup of $H \cap SL(n,q)$ in $SL(n,q)$ is an extension field type subgroup, that is, a subgroup lying between a copy of $GL(n/a,q^a) \cap SL(n,q)$ and its normalizer $GL(n/a,q^a).a \cap SL(n,q)$ where a is a divisor of n.*

Lemma 4.1. *Let q be a prime power, and let a and n be positive integers so that $a \mid n$. Then there is a chain of subgroups of the form*

$$GL\big(1,q^n\big).n \leqslant GL\big(n/a,q^a\big).a \leqslant GL(n,q).$$

Moreover, no element of type GL0 is contained in two distinct conjugates of the group $GL(n/a,q^a).a$.

Proof. Let V be an n-dimensional vector space over the field F of q elements. Let a be a positive divisor of n. Then V can be considered to be an A-module and also a K-module where $A : F$ and $K : A$ are field extensions of degrees a and n/a respectively. Let the multiplicative group of K be $GL(1,q^n)$, the group of A-linear transformations of V be $GL(n/a,q^a)$, and the group of F-linear transformations of V be $GL(n,q)$. The normalizer of $GL(1,q^n)$ in $GL(n,q)$ is $GL(1,q^n).\langle\sigma\rangle$ where σ is a generator of the Galois group of the extension $K : F$. In particular, there are precisely $|GL(n,q)|/|GL(1,q^n).n|$ Singer subgroups in $GL(n,q)$. The group $GL(n/a,q^a)$ contains the group $GL(1,q^n).\langle\sigma^a\rangle$, and hence

$$GL\big(n/a,q^a\big).\big(\langle\sigma\rangle/\big\langle\sigma^a\big\rangle\big) \cong GL\big(n/a,q^a\big).a$$

contains

$$GL\big(1,q^n\big).\big\langle\sigma^a\big\rangle.\big(\langle\sigma\rangle/\big\langle\sigma^a\big\rangle\big) \cong GL\big(1,q^n\big).n.$$

This proves the first part of the lemma.

The group $GL(n/a,q^a).a$ is its own normalizer in $GL(n,q)$, so each of the $|GL(n,q)|/|GL(n/a,q^a).a|$ conjugates of $GL(n/a,q^a).a$ contains a $GL(n/a,q^a).a$-conjugacy class of $|GL(n/a,q^a).a|/|GL(1,q^n).n|$ Singer subgroups.

We claim that all Singer subgroups inside $GL(n/a,q^a).a$ are $GL(n/a,q^a).a$-conjugate. Suppose that $\langle x\rangle$ and $\langle y\rangle$ are two Singer subgroups in $GL(n/a,q^a).a$. Notice that $\langle x^a\rangle$ and $\langle y^a\rangle$ are $GF(q^a)$-irreducible subgroups of the same order in $GL(n/a,q^a)$, so they are $GL(n/a,q^a)$-conjugate. Let S_x and S_y be the unique Singer subgroups in $GL(n/a,q^a)$ that contain $\langle x^a\rangle$ and $\langle y^a\rangle$ respectively. We must show that $\langle x\rangle = S_x$ and $\langle y\rangle = S_y$. It is sufficient to see that $\langle x\rangle = S_x$. Let C be the normalizer of $\langle x^a\rangle$ in $GL(n/a,q^a).a$. Since C contains a Singer subgroup and is contained in $GL(n/a,q^a).a$, by Kantor's theorem, it is isomorphic to a group of the form H where

$$GL\big(n/ar,q^{ar}\big) \leqslant H \leqslant GL\big(n/ar,q^{ar}\big).ar.$$

Hence $\langle x^a \rangle$ is contained in the group of scalars of $GL(n/ar, q^{ar})$. But $\langle x^a \rangle$ is $GF(q^a)$-irreducible, so ar must be n. This proves that $\langle x \rangle = S_x$.

The proof of the lemma is complete. □

Lemma 4.2. *Let H be a Singer subgroup in $GL(n, q)$. Then the order of the group $H \cap SL(n, q)$ is $(q^n - 1)/(q - 1)$, and its normalizer in $SL(n, q)$ is*

$$\big((q^n - 1)/(q - 1)\big).n \cong \big(GL\big(1, q^n\big).n\big) \cap SL(n, q).$$

Now let $n \geqslant 3$ and $(n, q) \neq (3, 4)$. If a is a prime dividing n, then

$$SL\big(n/a, q^a\big).\big((q^a - 1)/(q - 1)\big).a \cong \big(GL\big(n/a, q^a\big).a\big) \cap SL(n, q)$$

is a maximal subgroup of $SL(n, q)$ containing $((q^n - 1)/(q - 1)).n$. Moreover, no generator of $H \cap SL(n, q)$ is contained in two distinct conjugates of the group $(GL(n/a, q^a).a) \cap SL(n, q)$.

Proof. The first three statements of the lemma follow from [2], so we only give the proof of a fundamental claim. We claim that if x is a Singer cycle in $GL(n, q)$, then x has determinant a generator of the multiplicative group $GF(q)^*$. The Jordan form of x consists of one block. Let the characteristic polynomial of x be $p(t)$. (The coefficients of $p(t)$ lie in $GF(q)$.) By the Cayley–Hamilton theorem, we have $p(x) = 0$. Now view x as an element of $GF(q^n)$ considered as an extension field of $GF(q)$. All conjugates of x (under the Galois group C_n) are roots of $p(t)$. Since $p(t)$ has degree n, we conclude that $p(t)$ decomposes into linear factors over $GF(q^n)$. The determinant of x is then the product of all conjugates of x which is

$$x^{1+q+q^2+\cdots+q^{n-1}} = x^{(q^n-1)/(q-1)},$$

a generator of the multiplicative group of $GF(q)$.

We now turn to the proof of the last statement of the lemma. Let a be a positive integer dividing n. All copies of the group $GL(n/a, q^a).a$ are $GL(n, q)$-conjugate. Hence all copies of the group $(GL(n/a, q^a).a) \cap SL(n, q)$ are $GL(n, q)$-conjugate. Similarly, all copies of H are $GL(n, q)$-conjugate and hence all copies of $H \cap SL(n, q)$ are $GL(n, q)$-conjugate. The number of $GL(n, q)$-conjugates of $H \cap SL(n, q)$ in $(GL(n/a, q^a).a) \cap SL(n, q)$ is $|GL(n/a, q^a).a|/|GL(1, q^n).n|$, the number of $GL(n, q)$-conjugates of $GL(n/a, q^a).a \cap SL(n, q)$ in $SL(n, q)$ is $|GL(n, q)|/|GL(n/a, q^a).a|$, and the number of $GL(n, q)$-conjugates of $H \cap SL(n, q)$ in $SL(n, q)$ is $|GL(n, q)|/|GL(1, q^n).n|$. This proves the last statement of the lemma. □

We now turn to the proof of parts (2) and (3) of Theorem 4.1.

It was proved by Zsigmondy [33] in 1892 that, if a and k are integers, $a \geqslant 2$, $k \geqslant 3$ and the pair (a, k) is not $(2, 6)$, then $a^k - 1$ has a primitive prime divisor. Primitive prime divisors also exist when $k = 2$, unless $a + 1$ is a power of 2.

If g is an element of type GLk, SLk, GLOdd*, SLOdd, GLE, SLE, or GLOdd, then the order of g is divisible by $(q^{n-k} - 1)/(q - 1)$ where we put $k = n/2$ in case n is congruent to 2 modulo 4, and $n - k \geqslant n/2$. Hence, if $n \geqslant 4$, then the order of g is divisible by a prime divisor of $q^{n-k} - 1$. (Notice that $k \neq 2$ if $n = 4$.) This means that a maximal overgroup M of g in G is conjugate to one of the groups listed in [14] (if g is of type GLk or SLk) or is conjugate to one of the groups listed in [11] (if g is of type GLOdd*, SLOdd, GLE, SLE, or GLOdd).

Let us first go through the list of [14]. Let g be an element of type GLk or SLk. Let $n \geqslant 4$, and let Z be the center of $GL(n, q)$.

The argument used in Proposition 5.23 of [4] may be used to show that M cannot be of Example 2.1. This could also be shown by consideration of the rational canonical form of g. Criteria, in terms of rational canonical form, for membership of the groups of Example 2.1, are given in Britnell [5], following Wall [32]. However, we omit details here.

If M is a group of Example 2.2, then M is the stabilizer of the k or the $(n-k)$-dimensional subspace left invariant by g. No other conjugate of M contains g.

If M is of Example 2.4, then M is conjugate to a copy of $(GL(n/a, q^a).a) \cap G$ where a is a prime number dividing both n and k. Conversely, for any prime number a dividing both n and k exactly a conjugates of $(GL(n/a, q^a).a) \cap G$ contain g.

The group M cannot be of Example 2.5, since k and n cannot be both even.

The group M cannot be of Example 2.7, a group such that $S \leqslant M/(M \cap Z) \leqslant \mathrm{Aut}(S)$ where S is a sporadic simple group, since, by [10], such a group cannot contain an element of order at least $(q^{n-k}-1)/(q-1)$.

Before we consider groups of Examples 2.3 and 2.6 of [14], we need a little preparation. Let $r(m)$ denote the maximal order of an element in the symmetric group S_m. In 1903 Landau [20] gave an asymptotic formula for this function $r(m)$ as m tends to infinity. For our purposes it is sufficient to have only an explicit upper bound.

Lemma 4.3. *(See Massias [24].) For any positive integer m the maximal order of an element in the symmetric group S_m is at most $e^{a\sqrt{m \ln m}}$ where $a = 1.05314$.*

The following is a technical lemma.

Lemma 4.4. *Let q be a prime power, n a positive integer at least 4, let $r(n)$ be as above, and let $\lceil m \rceil$ denote the upper integer part of a positive integer m. Then $q^{\lceil (n+1)/2 \rceil} - 1 > (q-1)^2 \cdot r(n)$. If $n \geqslant 8$, then $q^{\lceil (n+1)/2 \rceil} - 1 > (q-1)^2 \cdot r(n+2)$. If $n \equiv 2 \pmod 4$ and $n \geqslant 14$, then we also have $q^{n/2} - 1 > (q-1)^2 \cdot r(n+2)$.*

Proof. This follows from Lemma 4.3 for $n \geqslant 32$. For $n \leqslant 31$ we use the known list of integers $\{r(m)\}_{m=4}^{m=33}$. □

Since g has order at least $(q^{\lceil (n+1)/2 \rceil} - 1)/(q-1)$ and every element of any group of Example 2.3 has order at most $(q-1) \cdot r(n)$, Lemma 4.4 shows that M cannot be of Example 2.3 of [14]. Similarly, by Lemma 4.4, the group M cannot be of Example 2.6(a) for $n \geqslant 8$. More careful considerations are used to show that no group of Example 2.6(a) can contain the element g for $4 \leqslant n \leqslant 7$.

The group M cannot be of Example 2.6(b) or (c) unless $(n, q) = (4, 2)$ or $(4, 4)$. This can be seen by using the condition that $n \geqslant 4$, the fact that the smallest prime divisor of n does not divide k, and by using a little group element order consideration in the case $n = 4$.

Since the smallest prime factor of n does not divide k, the group M cannot be of Table 6 of Example 2.8 unless it is of lines 6, 7, or 9, and M cannot be of Table 7 of Example 2.9 unless it is of lines 6, 10, or 12. A group of line 7 of Table 6 has elements of orders at most $2(q-1)q^3 \log_3(q)$ which is less than $(q^6-1)/(q-1)$ for q a power of 3. A group of line 6 of Table 7 has elements of orders at most 30 which is strictly less than $(q^4-1)/(q-1)$ for $q \geqslant 3$. Line 10 of Table 7 will be dealt with later when working through line 3 of Table 8. A group of line 12 of Table 7 has elements of orders less than $(q^3-1)/(q-1)$ for $q \geqslant 27$ and not divisible

by 91 (here we consider the case $q = 9$). Finally, a group of line 6 or 9 of Table 6 cannot contain an element of order divisible by $(q^6 - 1)/(q - 1)$.

We need another technical lemma which is well known, but we could not find an explicit reference for it.

Lemma 4.5. *The order of any linear transformation in $GL(n, q)$ is less than q^n.*

Proof. A Singer element has order exactly $q^n - 1$, so the upper bound given is best possible. It will be enough to prove the lemma for indecomposable transformations. Suppose X is indecomposable, and has minimal polynomial f^a, where f has degree d. Let b be the least integer such that $q^b \geqslant a$. It is clear that $b \leqslant a - 1$. Since $f(x)$ is a factor of $x^{q^d-1} - 1$, it is clear that $X^{(q^d-1)q^b} = I$, and hence X has order less than $q^{d(a-1)}$. Since $n = da$, this proves the lemma. □

Now let us consider Table 8 of Example 2.9. Here S is a simple group of Lie type with characteristic different from p where p is the prime divisor of q. We suppose that the overgroup M of g satisfies $S \leqslant M/(M \cap Z) \leqslant \mathrm{Aut}(S)$.

Let $S = PSL(t, s)$ where $t \geqslant 3$ is prime. By Lemma 4.5, the order of an arbitrary element in M is at most $(q - 1) \cdot s^t \cdot |\mathrm{Out}(S)| \leqslant (q - 1) \cdot s^{t+2}$. The order of g is at least $(q^{n-1} - 1)/(q - 1) > (q^{s^{t-1}} - 1)/(q - 1)$ which is larger than $(q - 1) \cdot s^{t+2}$ when $s^{t-1} \geqslant 32$. So suppose that $s^{t-1} \leqslant 31$. Then $t = 3$ or $t = 5$. If $t = 5$, then $s = 2$, and it is easy to see that such a subgroup cannot contain an element of order $o(g)$. If $t = 3$, then $s = 2$, 3, or 5. If $s = 3$, or 5, then such a subgroup cannot contain an element of order $o(g)$. If $s = 2$, then $q \geqslant 3$, and again, such a subgroup cannot contain g. This is a contradiction: M cannot be of this type.

Now let $S = PSU(t, s)$ where $t \geqslant 3$ is prime. Let f be the positive integer such that $s = r^f$ where r is prime. Let d denote the largest common divisor of t and $s + 1$. By Lemma 4.5, we see that an element of a subgroup of line 2 of Table 8 has order at most $2(q - 1) \cdot f \cdot d \cdot s^t$ which is strictly less than $(q^{(s^t+1)/(s+1)-1} - 1)/(q - 1)$ unless $(t, s) = (3, 2)$ when $n = 3$ holds. This is a contradiction.

Let $S = PSp(2t, s)$ where s is odd, f is as above, t is a power of 2, and $\frac{1}{2}(s^t + 1)$ is prime. By Lemma 4.5, we see that an element of a subgroup of line 3 of Table 8 has order at most $4(q - 1) \cdot f \cdot s^{2t}$ which is strictly less than $(q^{\frac{1}{2}(s^t-1)} - 1)/(q - 1)$ unless $(t, s) = (2, 3)$ when $n = 5$ holds. If $(t, s) = (2, 3)$, then the order of an element of the subgroup of line 3 of Table 8 is at most $24(q - 1)$ which is strictly less than $(q^4 - 1)/(q - 1)$ if $q > 3$. This also settles the case of line 10 of Table 7. Finally, for $q = 2$ and $q = 3$, there is no element in $PSp(4, 3)$ of order divisible by 15 or 40. A contradiction.

Let $S = PSp(2t, 3)$ where t is an odd prime and $\frac{1}{2}(3^t - 1)$ is prime. We have $4(q - 1) \cdot 3^{2t} < (q^{\frac{1}{2}(3^t-3)} - 1)/(q - 1)$. A contradiction.

Let $S = PSL(2, s)$ where $s \geqslant 7$. An element of a subgroup of line 5 in Table 8 has order at most $(q - 1)(s + 1) \cdot d \cdot f$ (by Dickson's list) where d is the largest common divisor of 2 and $s - 1$, and f is as above. This is strictly less than $(q^{\frac{1}{2}(s-1)-1} - 1)/(q - 1)$ unless $s \leqslant 11$. If $s = 7$, then such a group cannot contain g unless $n = 3$ or $(n, q) = (4, 2)$. (This can be seen by a more careful consideration of element orders.) If $s = 8$, then the maximal order of an element of such a group is at most $9(q - 1)$ which is less than $(q^6 - 1)/(q - 1)$. If $s = 9$, then an element of a subgroup of line 5 in Table 8 has order at most $10(q - 1)$ and this is less than $(q^4 - 1)/(q - 1)$ and less than $(q^3 - 1)/(q - 1)$ for $q \geqslant 8$. If $s = 9$ and $q \leqslant 7$, then such a group cannot contain an element

of order divisible by 7, 13, 21, 31, or 57. If $s = 11$, then an element of a subgroup of line 5 in Table 8 has order at most $12(q-1)$ and this is less than $(q^4-1)/(q-1)$. A contradiction.

This proves part (2) of Theorem 4.1.

Now let g be of type GLE, SLE, GLOdd*, GLOdd, or SLOdd, and let $n \geqslant 14$ be congruent to 2 modulo 4. If M is a maximal subgroup of G listed in part (3) of Theorem 4.1, then it is possible to show that M contains a conjugate of g.

Let M be a maximal subgroup of $GL(n,q)$ not G-conjugate to any of the groups listed in part (3) of Theorem 4.1. Suppose that M contains g. Then $(q^{n/2}-1)/(q-1)$ divides $|M|$. In particular, a primitive prime divisor of $q^{n/2}-1$ divides $|M|$. This means that M is conjugate to a subgroup in the list of Joseph DiMuro [11]. The different possibilities for M (which may contain the element g) are the following.

(1) One of the classical groups $SL(n,q)$, $Sp(n,q)$, $SU(n,q^{1/2})$, or $\Omega^{\epsilon}(n,q)$ (for $\epsilon = \pm$ or $\circ$) is normal in M. Since g cannot be realized over a subfield of $GF(q)$, $SU(n,q^{1/2})$ cannot be normal in M. By considering the determinant of g, we see that case $SL(n,q)$ cannot occur when $G = GL(n,q)$. The other classical groups can be eliminated by considering the rational canonical form of g. Rational canonical forms for elements of conformal groups are discussed in Britnell [5].
(2) M is a subgroup of $GL(1,q) \wr S_n$. By the last statement of Lemma 4.4, one sees that this possibility cannot occur.
(3) M is an almost simple group with socle A_d, an alternating group for $d \geqslant 5$ and M is a fully deleted permutation module (as in Example 2.6(a) of [14]). Again, by the last statement of Lemma 4.4, one sees that this possibility cannot occur.
(4) M is an almost simple group with a sporadic simple socle. In this case $n = 18$ and $M' \cong J_3$, or $3 \cdot J_3$, or $n = 22$ and $M' \cong M_{23}$, M_{24}, Co_2, or Co_3. Using [10] one can show that none of these possibilities actually occur.
(5) M is an almost simple group, and its socle S is a group of Lie type in characteristic other than p. In this case one of the following holds.
   (a) $S = PSL(t,s)$, $t \geqslant 3$, $n = \frac{s^t-1}{s-1} - 1$, t prime;
   (b) $S = PSU(t,s)$, $t \geqslant 3$, $n = \frac{s^t+1}{s+1} - 1$, t prime;
   (c) $S = PSp(2t,s)$, $n = \frac{1}{2}(s^t-1)$, $n+1$ prime, s odd, $t = 2^c \geqslant 2$;
   (d) $S = PSL(2,s)$, $s \geqslant 7$, $s \neq 9$. There are five subcases.
      (i) $n = s$, $n+1$ is prime, $s = 2^{2^c}$;
      (ii) $n = s-1$, s is prime;
      (iii) $n = \frac{1}{2}(s-1)$, s is prime, $s \equiv 1 \pmod 4$;
      (iv) $n = \frac{1}{2}(s-1)$, $\frac{1}{2}(s+1)$ is prime, s is odd;
      (v) $n = s-1$, $\frac{1}{2}(s+1)$ is prime, s is odd.

Let $S = PSL(t,s)$ where $t \geqslant 3$ is prime. By Lemma 4.5 and the above, the order of an arbitrary element in M is at most $(q-1)\cdot s^{t+2}$. The order of g is at least $(q^{n/2}-1)/(q-1) > (q^{s^{t-1}/2}-1)/(q-1)$ which is larger than $(q-1)s^{t+2}$ unless $t = 3$ and $s = 2$, 3, 4, or $t = 5$ and $s = 2$. Only $t = 5$ and $s = 2$ can occur from these exceptional cases as $n \geqslant 14$ and n is congruent to 2 modulo 4. But even then, $(q^{n/2}-1)/(q-1) > (q-1)s^{t+2}$.

Let $S = PSU(t,s)$ where $t \geqslant 3$ is prime. As above, we know that an element of M has order at most $2(q-1)\cdot f \cdot d \cdot s^t$ where f is the positive integer such that $s = r^f$ where r is prime and d is the largest common divisor of t and $s+1$. This is strictly less than $(q^{(s^t+1)/2(s+1)}-1)/(q-1)$

unless $t = 3$ or $t = 5$ and $s \leqslant 4$. Since $n \geqslant 14$ and n is congruent to 2 modulo 4, none of the exceptional cases can occur.

Let $S = PSp(2t, s)$ and use the notations above. Under our conditions we have $4(q-1) \cdot f \cdot s^{2t} < (q^{(s^t-1)} - 1)/4(q-1)$. So this case cannot occur either.

Let $S = PSL(2, s)$ where $s \geqslant 7$. An element in M has order at most $(q-1)(s+1) \cdot d \cdot f$ (by Dickson's list) where d is the largest common divisor of 2 and $s-1$, and f is as above. This is strictly less than $(q^{\frac{1}{4}(s-1)} - 1)/(q-1)$ unless $s \leqslant 32$ and s is not a prime or $s \leqslant 23$ and s is a prime. Suppose that $s \leqslant 32$ and s is not a prime or $s \leqslant 23$ and s is a prime. Then one can see that subcases (iii) and (iv) cannot occur. It follows that $s - 1 \geqslant 14$ is congruent to 2 modulo 4, and so $s = 19, 23$, or 27. If $s = 19$ or $s = 23$, then $2(q-1)(s+1) \leqslant (q^{(s-1)/2} - 1)/(q-1)$. Finally, $s \neq 27$, since $\frac{1}{2}(s+1)$ is not prime in this case.

This proves part (3) of Theorem 4.1.

5. Proofs of Theorems 1.1 and 1.2

Next we proceed to show that for $n \geqslant 4$ the right-hand side of Lemma 2.1 is a lower bound for $\mu(G)(\leqslant \sigma(G))$ in case G is any of the groups $(P)GL(n, q)$, $(P)SL(n, q)$ and $n \not\equiv 2 \pmod 4$, or in case G is any of the groups $(P)SL(n, q)$, $n \equiv 2 \pmod 4$ and q is odd. It is clear that it is sufficient to see this only in the cases when G is $GL(n, q)$ or $SL(n, q)$. Let G be any of the groups $GL(n, q)$ or $SL(n, q)$.

Eventually, for the proof of Theorem 1.1, we will need the following result from [15]. See also [1,16,26].

Theorem 5.1. *(See Haxell, [15].) Let Γ be a (simple) graph so that every vertex of Γ has degree at most d for some positive integer d. Let $V(\Gamma) = V_0 \cup \cdots \cup V_t$ be a partition of the vertex set of Γ. Suppose that $2d \leqslant |V_i|$ for each i. Then Γ has an independent set $\{v_0, \ldots, v_t\}$ where $v_i \in V_i$ for each i.*

We define a graph Γ associated to $G = GL(n, q)$ or $SL(n, q)$ in the following way. If $n \equiv 2 \pmod 4$ and q is odd, then fix a matching φ (as above) on $\mathcal{S}_{n/2}$. If $n \equiv 2 \pmod 4$ and q is even, then fix an $n/2$-dimensional vector space W and an associated matching φ_W (as above) on the set $\mathcal{S}_{n/2}$. In case $G = GL(n, q)$ let the vertex set $V(\Gamma)$ of Γ be the set of all different cyclic subgroups of G generated by all elements of types GL0, GLk (for all k), and all elements of types GLOdd (if q is odd and $n \equiv 2 \pmod 4$), GLE (if q is even and $n \equiv 2 \pmod 4$) lying inside subgroups of the form $GL(U) \oplus GL(U\varphi)$ (if q is odd and $n \equiv 2 \pmod 4$) where $U \in \mathcal{S}$, or lying inside subgroups of the form $GL(U) \oplus GL(U\varphi_W)$ (if q is even and $n \equiv 2 \pmod 4$) where $U \in \mathcal{S}_{n/2}$ is different from W. In case $G = SL(n, q)$ let the vertex set $V(\Gamma)$ of Γ be the set of all different cyclic subgroups of G generated by all elements of types SL0, SLk (for all k), all elements of type SLOdd (this is defined only when $n \equiv 2 \pmod 4$ and q is odd), and all elements of type SLE (when $n \equiv 2 \pmod 4$ and q is even) lying inside subgroups of the form $GL(U) \oplus GL(U\varphi_W)$ where $U \in \mathcal{S}_{n/2}$ is different from W. Let b be the smallest prime divisor of $n \geqslant 2$, and let $\mathcal{H}_0$ be the set of all conjugates in G of the subgroup $(GL(n/b, q^b).b) \cap G$. For each positive integer k so that $1 \leqslant k < n/2$ and $b \nmid k$ let $\mathcal{H}_k$ be the set of all stabilizers of k-dimensional subspaces of V in G. If $n \not\equiv 2 \pmod 4$, then put $\mathcal{H}_{n/2} = \emptyset$. If $n \equiv 2 \pmod 4$, q is odd and $G = SL(n, q)$, then let $\mathcal{H}_{n/2}$ be the set of all stabilizers in G of $n/2$-dimensional subspaces of V. Otherwise, when $n \equiv 2 \pmod 4$ and either q is even or $G = GL(n, q)$, then let $\mathcal{H}_{n/2}$ be the set of all subgroups of the form $GL(U) \oplus GL(U\varphi)$ where $U \in \mathcal{S}_{n/2}$ when q is

odd, and the set of all subgroups of the form $GL(U) \oplus GL(U\varphi_W)$ where $U \in \mathcal{S}_{n/2}$ is different than W for some fixed $W \in \mathcal{S}_{n/2}$ when q is even. Let $\mathcal{H}$ be the union of $\mathcal{H}_0$, all the $\mathcal{H}_k$'s and $\mathcal{H}_{n/2}$. Put $t = |\mathcal{H}|$ for convenience, and let $\mathcal{H} = \{H_1, \ldots, H_t\}$. For each positive integer i so that $1 \leqslant i \leqslant t$ define V_i to be the subset of $V(\Gamma)$ consisting of all vertices contained (as subgroups) in H_i. Notice that the V_i's partition the vertex set $V(\Gamma)$ of Γ. For any two distinct vertices v, $w \in V(\Gamma)$ of Γ we draw an edge between them, if and only if, they lie in different V_i's and there exists a proper subgroup of G (not in $\mathcal{H}$) that contains both v and w.

By Theorem 4.1, an upper bound for $n \geqslant 4$ for the maximum degree of a vertex in Γ is $\frac{1}{2} \cdot (\sum |GL(n/a, q^a).a| + \epsilon \cdot |GL(n/2, q)||GL(2, q)|)$ where the sum is over all prime divisors a of n different from b and $\epsilon = 1$ if $n \equiv 2 \pmod 4$ and $\epsilon = 0$ otherwise. We will show (in most cases) that this upper bound is at most $\frac{1}{2} \cdot \min_{1 \leqslant i \leqslant t}\{|V_i|\}$. To do this we need a series of lemmas.

Lemma 5.1. *Let $n \geqslant 2$ be a positive integer and q a prime power. Put*

$$f(k) = \frac{|GL(k, q)|}{k(q^k - 1)} \cdot \frac{|GL(n-k, q)|}{(n-k)(q^{n-k} - 1)}$$

for positive integers $1 \leqslant k \leqslant n-1$. If n is even, then $f(n/2) \leqslant f(k)$ and if n is odd, then $f((n-1)/2) \leqslant f(k)$ for all positive integers $1 \leqslant k \leqslant n-1$.

Proof. It is easy to see that $f(k) = f(n-k)$ for all k and that the inequality $f(k) \geqslant f(k+1)$ is equivalent to the inequality

$$\frac{k}{k+1} q^k \left(q^k - 1\right) \leqslant \frac{n-k-1}{n-k} q^{n-k-1} \left(q^{n-k-1} - 1\right)$$

for all $1 \leqslant k \leqslant n-2$. Clearly, the function $\frac{x}{x+1} q^x (q^x - 1)$is increasing on the set of positive integers x, so we have $f(k) \geqslant f(k+1)$ if and only if $k \leqslant [(n-1)/2]$. This proves the lemma. □

Lemma 5.2. *Let b be the smallest prime divisor of the positive integer $n \geqslant 2$. If n is even, then we have*

$$\frac{|GL(n/2, q^2)|}{n^2(q^n - 1)} \leqslant \frac{4^{n/2-1} |GL(n/2, q)|^2}{n^2 (q^{n/2} - 1)^2}.$$

If n is odd, then we have

$$\frac{3 \cdot |GL(n/b, q^b).b|}{n^2(q^n - 1)} \leqslant \frac{4 \cdot |GL((n+1)/2, q)| \cdot |GL((n-1)/2, q)|}{(n^2 - 1)(q^{(n-1)/2} - 1)(q^{(n+1)/2} - 1)}.$$

Proof. First let n be even. Then the claim is true for $n = 2$. Suppose that $n \geqslant 4$. In this case we have to show that

$$\left(q^n - q^2\right) \cdot \cdots \cdot \left(q^n - q^{n-2}\right) \leqslant \left(2^{n/2-1} \left(q^{n/2} - q\right) \cdot \cdots \cdot \left(q^{n/2} - q^{n/2-1}\right)\right)^2.$$

In order to do so we will prove that $q^n - q^{2\ell} \leqslant 4(q^{n/2} - q^\ell)^2$ holds for all $1 \leqslant \ell \leqslant n/2 - 1$. One can check that this is true for $\ell = n/2 - 1$. So suppose that $n \geqslant 6$ and that $1 \leqslant \ell \leqslant n/2 - 2$. Then $q^n - q^{2\ell} < q^n$ is at most

$$4\left(q^n - q^{n-1}\right) < 4\left(q^n + q^{n-4} - 2q^{n-2}\right) = 4\left(q^{n/2} - q^{n/2-2}\right)^2 \leqslant 4\left(q^{n/2} - q^\ell\right)^2.$$

Let $n \geqslant 3$ be odd. In this case $b \geqslant 3$. The claim is true for $n = 9$ and for n a prime, so suppose that $n \geqslant 15$. It is sufficient to show that

$$3b \cdot q^{n^2/3} < \frac{|GL((n+1)/2, q)| \cdot |GL((n-1)/2, q)|}{(q^{(n-1)/2} - 1)(q^{(n+1)/2} - 1)}.$$

But this is true for $n \geqslant 15$ since the right-hand side of the previous inequality is greater than

$$\left(\frac{1}{2}q^{(n+1)/2}\right)^{(n+1)/2-1} \cdot \left(\frac{1}{2}q^{(n-1)/2}\right)^{(n-1)/2-1} > 2^{2-n}q^{(n^2+1)/2-n} > 3b \cdot q^{n^2/3}. \qquad \square$$

Lemma 5.3. *Let n be a positive integer different from 6 having at least two different prime divisors the smallest of which is b. Then we have*

$$\epsilon \cdot \big|GL(n/2, q)\big|\big|GL(2, q)\big| + \sum \big|GL\big(n/a, q^a\big).a\big| \leqslant \min\left\{\frac{|GL(n/b, q^b).b|}{n(q^n - 1)}, \min_{1 \leqslant i \leqslant n-1}\big\{f(k)\big\}\right\}$$

where $\epsilon = 1$ if n is congruent to 2 modulo 4 and is 0 otherwise, the sum is over all prime divisors a of n different from b, and the $f(k)$'s are defined in Lemma 5.1.

Proof. Let c be the second smallest prime divisor of n. Then the left-hand side of the inequality of the lemma is at most

$$\epsilon \cdot q^{n^2/4+4} + \big(\omega(n) - 1\big) \cdot c \cdot q^{n^2/c}$$

where $\omega(n)$ denotes the number of distinct prime divisors of n. By Lemma 5.2 and by the fact that $q \geqslant 2$, the right-hand side of the inequality of the lemma is at least

$$\frac{b((3/4)q^n)^{(n/b)-1}}{2^{n-2}n^2}.$$

It is easy to check that

$$\epsilon \cdot q^{n^2/4+4} + \big(\omega(n) - 1\big) \cdot c \cdot q^{n^2/c} < \frac{b((3/4)q^n)^{(n/b)-1}}{2^{n-2}n^2}$$

holds for $n \geqslant 14$. If $n = 10$ or 12, then the inequality of the lemma can be checked by direct but tedious calculations. $\square$

We are now in the position to prove the following.

Theorem 5.2. *Let $n \geqslant 12$ be a positive integer with smallest prime divisor b. If n is not congruent to 2 modulo 4, then let G be any of the groups $(P)GL(n, q)$, $(P)SL(n, q)$. If n is congruent to 2 modulo 4, then let q be odd and put $G = (P)SL(n, q)$. Under these conditions we have*

$$\mu(G) = \sigma(G) = \frac{|GL(n, q)|}{|GL(n/b, q^b).b|} + \sum_{\substack{k=1 \\ b \nmid k}}^{[n/2]} \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

Proof. From the above it is sufficient to show that

$$\frac{|GL(n,q)|}{|GL(n/b,q^b).b|}+\sum_{\substack{k=1\\ b\nmid k}}^{[n/2]}\begin{bmatrix}n\\k\end{bmatrix}_q\leqslant\mu(G)$$

holds for $G=GL(n,q)$ or $SL(n,q)$. So let G be $GL(n,q)$ or $SL(n,q)$. Recall the graph Γ associated to the group G, and recall the set of subgroups $\mathcal{H}$. Notice that $t=|\mathcal{H}|$ is precisely the right-hand side of the equality of the theorem. Recall the subsets $V_1,\dots,V_t$ of $V(\Gamma)$ which partition the vertex set of Γ. By the above lemma, if $n\geqslant 12$, the maximum degree of a vertex in Γ is at most $\frac{1}{2}\min_{1\leqslant i\leqslant t}\{V_i\}$. By Haxell's theorem this implies that there is a set $\{v_1,\dots,v_t\}$ of independent vertices of Γ such that $v_i\in V_i$ for all i. These vertices correspond to distinct cyclic subgroups of G. Pick a generator from each of these cyclic subgroups. Let the set of these elements be $\Delta=\{g_1,\dots,g_t\}$. By Theorem 4.1 and our construction of Γ we see that Δ pairwise generates G if $n\geqslant 12$. This proves the theorem. □

This theorem can somewhat be extended. Let Γ be the graph defined after the statement of Haxell's theorem. (Note that this graph was defined for all n, q and for all groups $(P)GL(n,q)$, $(P)SL(n,q)$.) Recall the set of subgroups $\mathcal{H}$, the integer $t=|\mathcal{H}|$, and the partition $\{V_i\}_{1\leqslant i\leqslant t}$ of the vertex-set $V(\Gamma)$ of Γ. For an arbitrary subset Π of G define $\sigma(\Pi)$ to be the smallest integer r so that there exist r proper subgroups of G whose union contains Π, and define $\mu(\Pi)$ to be the largest integer m so that there exist a set of m distinct elements in Π that pairwise generates G. Put $\sigma(\emptyset)=\mu(\emptyset)=0$. The proof of the previous theorem easily yields the following.

Corollary 5.1. *Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$, and let $\mathcal{H}$, t be as above. Let Π be the union of all subgroups in $\mathcal{H}$. Then there exists a subset $X=\{g_1,\dots,g_t\}$ of Π that pairwise generates G with the property that for all $1\leqslant i\leqslant t$ the element g_i is a generator of some cyclic subgroup $v_i\in V_i$. In particular $t=\mu(X)\leqslant\mu(\Pi)\leqslant\mu(G)$.*

From now on let n be a positive integer congruent to 2 modulo 4. Let G be any of the groups $GL(n,q)$, $SL(n,q)$ if q is even, and let G be $GL(n,q)$ if q is odd. In the latter case (when q is odd and $G=GL(n,q)$) there exists a normal subgroup N in G of index 2 consisting of all matrices of G having determinants a square of an element of $GF(q)^*$. Notice that N contains the center of G.

Let Π_1 be the union of all members of $\mathcal{H}\setminus\mathcal{H}_{n/2}$. Let $t_0=|\mathcal{H}\setminus\mathcal{H}_{n/2}|$. Then, by Haxell's theorem, $\mu(\Pi_1)=\sigma(\Pi_1)=t_0$. Put $\Pi_2=(G\setminus\Pi_1)\cap N$ if N is defined and $\Pi_2=\emptyset$ otherwise. Clearly both $\sigma(\Pi_2)$ and $\mu(\Pi_2)$ is at most 1. Put $\Pi_3=G\setminus(\Pi_1\cup\Pi_2)$. Every element of Π_3 has the same minimal and characteristic polynomial $f\cdot g$ where f and g are (not necessarily distinct) irreducible polynomials of degrees $n/2$ over the field of q elements. Since the only proper subspaces of V left invariant by an element of Π_3 are $n/2$-dimensional and there are at least two of these, it is not difficult to see that $\mu(\Pi_3)\leqslant[N/2]$ where $N=|\mathcal{S}_{n/2}|$. By the above corollary we also have $[N/2]\leqslant\mu(\Pi_3)$. Hence $\mu(\Pi_3)=[N/2]=t-t_0$.

Since the group G is the disjoint union of Π_1, Π_2, Π_3, we have $\mu(G)\leqslant\mu(\Pi_1)+\mu(\Pi_2)+\mu(\Pi_3)$. If q is even, then this gives $\mu(G)\leqslant t_0+\mu(\Pi_3)=t$, and if q is odd, then we have $\mu(G)\leqslant t_0+1+\mu(\Pi_3)=t+1$. By the above corollary we conclude that $\mu(G)=t$ if q is even, and $\mu(G)=t$ or $t+1$ if q is odd.

We claim that $\mu(G)=t$ if q is odd. Suppose on the contrary that $\mu(G)=t+1$. Let X be a set that generates G pairwise so that $|X|=t+1$. Then $|X\cap\Pi_3|=[N/2]=N/2$ (the latter equality

following from the fact that N is even when q is odd). This can only be if for any $W \in \mathcal{S}_{n/2}$ there is an element $x \in X \cap \Pi_3$ that leaves W and a complementary subspace to W (in V) invariant. We must also have $|X \cap \Pi_2| = 1$. The element $y \in X \cap \Pi_2$ must leave an $n/2$-dimensional subspace invariant. But this is a contradiction since there is an element $x \in X \cap \Pi_3$ (different from y) leaving the same $n/2$-dimensional subspace invariant.

To finish the paper all remains to show is that the inequalities in the statements of Lemmas 2.1 and 2.2 are actually equalities for $n \geqslant 12$. So from now on assume that $n \geqslant 12$.

Let Π_2, Π_3 be as above, but set Π_1 to be the set of all elements of types GL0, GLk (for all k) in case $G = GL(n, q)$ and the set of all elements of types SL0, SLk (for all k) in case $G = SL(n, q)$. Put $\Pi = \Pi_1 \cup \Pi_2 \cup \Pi_3$. This time, as in the proof of Lemma 2.1, set $\mathcal{H}$ to be the set of all conjugates of the extension field subgroup $GL(n/2, q^2).2$, all stabilizers of all subspaces of V having odd dimensions at most $n/2 - 1$, all stabilizers of all $n/2$-dimensional subspaces of V which do not contain a prescribed non-zero vector v, and N (but only if q is odd). By Lemmas 2.1 and 2.2, we know that $\mathcal{H}$ is a covering for G. We must show that this is a minimal covering for G. It is sufficient to prove $\sigma(\Pi) = |\mathcal{H}|$.

Let M be a maximal subgroup in G different from any conjugate of any member in $\mathcal{H}$ and different from any conjugate of the group $GL(n/2, q) \wr S_2$. By Theorem 4.1 we see that

$$|\Pi \cap M| < \left| \Pi \cap \left(H' \setminus \bigcup_{H' \neq H \in \mathcal{H}} H \right) \right| \tag{5}$$

for any $H' \in \mathcal{H}$. A little more care is needed to see that (5) is true even if M is conjugate to a copy of the group $GL(n/2, q) \wr S_2$. All this implies that no copy of M can be involved in a minimal covering of the set Π (and of the group G). By Theorem 4.1 and by this observation, there is no element of a minimal covering of Π having a non-trivial intersection with both Π_1 and $\Pi_2 \cup \Pi_3$. Hence we have $\sigma(\Pi) = \sigma(\Pi_1) + \sigma(\Pi_2 \cup \Pi_3)$. By Theorem 4.1, Lemma 2.2 and the above inequality, it is not difficult to see that $\sigma(\Pi_1) = t_0$ where t_0 is as above. (Note that the set Π_1, which we defined a couple of paragraphs before when computing $\mu(G)$, is slightly different from this new set, Π_1.)

Let Σ be a minimal covering for Π_3. By the above, we know that Σ consists only of stabilizers of $n/2$-dimensional subspaces. We will need the following lemma.

Lemma 5.4. *Let Σ be as above. Then we have $|\Sigma| = (q^{n/2}/(q^{n/2} + 1))\begin{bmatrix} n \\ n/2 \end{bmatrix}_q$.*

For the proof of this lemma, we recall Theorem 1 of [13].

As usual, let V be an n-dimensional vector space over the field of q elements. A family F of subspaces of V is called t-intersecting if $\dim(W \cap W') \geqslant t$ whenever $W, W' \in F$. Theorem 1 of [13] is as follows.

Theorem 5.3. *(See Frankl and Wilson [13].) Suppose $n \geqslant 2k - t$, F is a t-intersecting family of k-dimensional subspaces of V. Then*

$$|F| \leqslant \max\left\{ \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q, \begin{bmatrix} 2k-t \\ k \end{bmatrix}_q \right\}.$$

It is fairly clear and is shown in [13] that equality can always be attained in the above theorem. We are now in the position to prove the lemma.

If Ω denotes the set of all $n/2$-dimensional subspaces of V, then $F = \Omega \setminus \Sigma$ is a 1-intersecting family of $n/2$-dimensional subspaces. By Theorem 5.3, $|F| \leqslant \begin{bmatrix} n-1 \\ n/2 \end{bmatrix}_q$, and hence

$$\begin{bmatrix} n \\ n/2 \end{bmatrix}_q - \begin{bmatrix} n-1 \\ n/2 \end{bmatrix}_q \leqslant |\Sigma|. \tag{6}$$

It is easy to check that the left-hand side of (6) is $(q^{n/2}/(q^{n/2}+1))\begin{bmatrix} n \\ n/2 \end{bmatrix}_q$. Since the set of all stabilizers of all $n/2$-dimensional subspaces of V which do not contain a prescribed non-zero vector v is a covering for Π_3, we also have $|\Sigma| \leqslant (q^{n/2}/(q^{n/2}+1))\begin{bmatrix} n \\ n/2 \end{bmatrix}_q$. This proves Lemma 5.4.

The above give

$$t_0 + \frac{q^{n/2}}{q^{n/2}+1}\begin{bmatrix} n \\ n/2 \end{bmatrix}_q = \sigma(\Pi) \leqslant \sigma(G)$$

if q is even. This is exactly what we wanted in this case.

Now let q be odd. Then $\Pi_2 \neq \emptyset$. A minimal covering (consisting only of maximal subgroups of G) for $\Pi_2 \cup \Pi_3$ can consist only of N and a number of stabilizers of $n/2$-dimensional vector spaces. By the above and by Lemma 2.2, we certainly have

$$\frac{q^{n/2}}{q^{n/2}+1}\begin{bmatrix} n \\ n/2 \end{bmatrix}_q = \sigma(\Pi_3) \leqslant \sigma(\Pi_2 \cup \Pi_3) \leqslant 1 + \frac{q^{n/2}}{q^{n/2}+1}\begin{bmatrix} n \\ n/2 \end{bmatrix}_q. \tag{7}$$

Now Σ cannot be a covering for $\Pi_2 \cup \Pi_3$, since $|\Sigma| < \begin{bmatrix} n \\ n/2 \end{bmatrix}_q$ and hence there exists at least one element in Π_2 which lies in exactly one stabilizer of an $n/2$-dimensional vector space different from any member of Σ. This proves that the lower bound in (7) cannot be exact. Hence the upper bound in (7) is exact. This proves that the upper bound for $\sigma(G)$ in Lemma 2.2 is exact even if q is odd.

6. The asymptotics

In this section we will answer the question of Blackburn [3] stated before Theorem 1.2 in the special case of a projective special linear group.

Following Blackburn [3], we say that a subset X of a finite group G pairwise generates G if any two distinct elements of X generates G. If g is a Singer element in $GL(n,q)$, then we say that g^{q-1} is a Singer element in $SL(n,q)$.

Let G be any of the groups $GL(n,q)$ and $SL(n,q)$. In case $G = SL(n,q)$, then assume that $n \geqslant 2$ and $(n,q) \neq (2,2)$, $(2,5)$, $(2,7)$, $(2,9)$, or $(3,4)$.

By Theorems 4.2 and 4.3, it is clear that a maximal overgroup of a Singer element in G is conjugate to a copy of $(GL(n/a, q^a).a) \cap G$ where a is a prime divisor of n. Let b denote the smallest prime divisor of n. If n is a power of b, then we may choose one Singer element from each conjugate of $(GL(n/b, q^b).b) \cap G$ to obtain a pairwise generating set of size $|GL(n,q)|/|GL(n/b, q^b).b|$. However, we are unable to obtain the same conclusion when b is not the unique prime divisor of n.

Our tool will be the following result from extremal graph theory.

Theorem 6.1. *(See Turán [31].) Let Γ be a graph on n vertices. If Γ does not have a complete subgraph of size r, then it has at most $((r-2)/(r-1)) \cdot n^2/2$ edges.*

We prove

Theorem 6.2. *Let G be as above. There is a set X consisting of at least $|GL(n,q)|/(\sum |GL(n/a,q^a).a|)$ Singer elements from G so that X pairwise generates G and the sum is over all prime divisors a of n. Moreover, if n is a prime power, then there is no such set of cardinality larger than $|GL(n,q)|/|GL(n/a,q^a).a|$ where a is the prime divisor of n.*

Proof. The second statement of the theorem is clear from the remark made before Theorem 6.1.

We will prove the first part of the theorem using Theorem 6.1. We will only deal with the case when $G = GL(n,q)$, since the proof for the other case is exactly the same. (If $G = SL(n,q)$, then the conditions of Theorem 4.3 are satisfied on n (see above), and we can use Lemma 4.2.)

Define a graph Γ on the set of Singer subgroups by connecting two vertices by an edge if and only if they generate a proper subgroup of $GL(n,q)$. By Theorem 4.2, if two vertices are connected by an edge, then they lie in the same maximal subgroup of the form $GL(n/a,q^a).a$ for some prime a dividing n. We must show that Γ contains an empty subgraph with r vertices where r is the smallest integer not smaller than $|GL(n,q)|/(\sum |GL(n/a,q^a).a|)$ where the sum is over all prime divisors a of n.

By Theorem 4.2 and Lemma 4.1, there are at most

$$\frac{1}{2}\sum\left(\frac{|GL(n,q)|}{|GL(n/a,q^a).a|}\cdot\left(\left(\frac{|GL(n/a,q^a).a|}{|GL(1,q^n).n|}\right)^2-\left(\frac{|GL(n/a,q^a).a|}{|GL(1,q^n).n|}\right)\right)\right)$$
$$=\frac{1}{2}\frac{|GL(n,q)|}{|GL(1,q^n).n|^2}\sum\left(\left|GL\left(n/a,q^a\right).a\right|-\left|GL\left(1,q^n\right).n\right|\right)$$

edges in Γ. Hence there are at least

$$\frac{1}{2}\frac{|GL(n,q)|}{|GL(1,q^n).n|^2}\left(\left|GL(n,q)\right|+\left(\omega(n)-1\right)\cdot\left|GL\left(1,q^n\right).n\right|-\sum\left|GL\left(n/a,q^a\right).a\right|\right)$$

edges in the dual graph of Γ where $\omega(n)$ denotes the number of prime divisors of n. By the definition of r, this latter expression is larger than

$$\frac{1}{2}\frac{|GL(n,q)|}{|GL(1,q^n).n|^2}\left(\left|GL(n,q)\right|+\left(\omega(n)-1\right)\cdot\left|GL\left(1,q^n\right).n\right|-\frac{1}{r-1}\left|GL(n,q)\right|\right).$$

From this we conclude that there are more than

$$\frac{1}{2}\frac{(r-2)}{(r-1)}\cdot\left(\frac{|GL(n,q)|}{|GL(1,q^n).n|}\right)^2$$

edges in the dual graph of Γ. By Theorem 6.1 we see that the dual graph of Γ must contain a complete subgraph on r vertices which means that Γ must have r independent points. This completes the proof of our theorem. □

An immediate consequence of this result is the following.

Corollary 6.1. *Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. In case $G = (P)SL(n,q)$ suppose that $n \geqslant 2$ and $(n,q) \neq (2,5)$, $(2,7)$, $(2,9)$, $(3,4)$. Then*

$$\left|GL(n,q)\right|\Big/\left(\sum\left|GL\left(n/a,q^a\right).a\right|\right)\leqslant\mu(G)\leqslant\sigma(G)\leqslant\frac{|GL(n,q)|}{|GL(n/b,q^b).b|}+\sum_{\substack{k=1\\ b\nmid k}}^{[n/2]}\begin{bmatrix}n\\k\end{bmatrix}_q,$$

where the first sum is over all prime divisors a of n and b is the smallest prime divisor of n.

Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. If $G = (P)SL(n,q)$, then assume that $n \geqslant 2$ and $(n,q) \neq (2,5), (2,7), (2,9), (3,4)$. Let b be the largest prime divisor of n.

By Corollary 6.1, we have

$$1 \leqslant \frac{\sigma(G)}{\mu(G)} \leqslant \frac{(1+o(1))\frac{|GL(n,q)|}{|GL(n/b,q^b.b)|}}{\frac{|GL(n,q)|}{(1+o(1))|GL(n/b,q^b.b)|}} = 1 + o(1)$$

as $|G| \to \infty$.

Acknowledgments

We thank László Lovász for an important e-mail and Joseph DiMuro for sharing an early version of his doctoral thesis with us. We also thank Christopher W. Parker and Penny E. Haxell for pointing out a reference.

References

[1] R. Aharoni, P.E. Haxell, Systems of disjoint representatives, unpublished.
[2] Á. Bereczky, Maximal overgroups of Singer elements in classical groups, J. Algebra 234 (1) (2000) 187–206.
[3] S. Blackburn, Sets of permutations that generate the symmetric group pairwise, J. Combin. Theory Ser. A 113 (7) (2006) 1572–1581.
[4] T. Breuer, R.M. Guralnick, W.M. Kantor, Probabilistic generation of finite simple groups, II, J. Algebra, in press.
[5] J.R. Britnell, Cyclic, separable and semisimple transformations in the finite conformal groups, J. Group Theory 9 (5) (2006) 571–601.
[6] R. Brown, Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements, J. Combin. Theory Ser. A 49 (2) (1988) 294–307.
[7] R. Brown, Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements. II, J. Combin. Theory Ser. A 56 (2) (1991) 285–289.
[8] R.A. Bryce, V. Fedri, L. Serena, Subgroup coverings of some linear groups, Bull. Austral Math. Soc. 60 (2) (1999) 227–238.
[9] J.H.E. Cohn, On n-sum groups, Math. Scand. 75 (1) (1994) 44–58.
[10] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups. Maximal Subgroups and Ordinary Characters for Simple Groups, Oxford University Press, Eynsham, 1985.
[11] J. DiMuro, On prime power elements of $GL_d(q)$ acting irreducibly on large subspaces, PhD thesis, University of Southern California, 2007.
[12] G.A. Dirac, Some theorems on abstract graphs, Proc. London Math. Soc. (3) 2 (1952) 69–81.
[13] P. Frankl, R.M. Wilson, The Erdős–Ko–Rado theorem for vector spaces, J. Combin. Theory Ser. A 43 (2) (1986) 228–236.
[14] R. Guralnick, T. Penttila, C.E. Praeger, J. Saxl, Linear groups with orders having certain large prime divisors, Proc. London Math. Soc. (3) 78 (1) (1999) 167–214.
[15] P.E. Haxell, A condition for matchability in hypergraphs, Graphs Combin. 11 (1995) 245–248.
[16] P.E. Haxell, A note on vertex list colouring, Combin. Probab. Comput. 10 (4) (2001) 345–347.
[17] P.E. Holmes, Subgroup coverings of some sporadic groups, J. Combin. Theory Ser. A 13 (6) (2006) 1204–1213.
[18] B. Huppert, Endliche Gruppen. I, Grundlehren Math. Wiss., Band 134, Springer-Verlag, Berlin, 1967.
[19] W.M. Kantor, Linear groups containing a Singer cycle, J. Algebra 62 (1) (1980) 232–234.
[20] E. Landau, Über die Maximalordnung der Permutationen gegebenen Grades, Archiv der Math. und Phys. (1903) 92–103.
[21] M.W. Liebeck, A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, J. Algebra 184 (1) (1996) 31–57.
[22] L. Lovász, M.D. Plummer, Matching Theory, North-Holland, 1986.
[23] M.S. Lucido, On the covers of finite groups, in: Groups St. Andrews 2001, vol. II, in: London Math. Soc. Lecture Note Ser., vol. 305, Cambridge Univ. Press, Cambridge, 2003, pp. 395–399.
[24] J.P. Massias, Majoration explicite de l'ordre maximum d'un élément du groupe symétrique, Ann. Fac. Sci. Toulouse Math. 6 (1984) 269–280.

[25] A. Maróti, Covering the symmetric groups with proper subgroups, J. Combin. Theory Ser. A 110 (1) (2005) 97–111.
[26] R. Meshulam, The clique complex and hypergraph matching, Combinatorica 21 (1) (2001) 89–94.
[27] L. Pyber, The number of pairwise noncommuting elements and the index of the centre in a finite group, J. London Math. Soc. (2) 35 (2) (1987) 287–295.
[28] L. Serena, On finite covers of groups by subgroups, in: Advances in Group Theory 2002, Aracne, Rome, 2003, pp. 173–190.
[29] L. Serena, Personal communication, 2000.
[30] M.J. Tomkinson, Groups as the union of proper subgroups, Math. Scand. 81 (1997) 191–198.
[31] P. Turán, An extremal problem in graph theory, Mat. Fiz. Lapok 48 (1941) 436–452.
[32] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Austral. Math. Soc. 3 (1963) 1–62.
[33] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. für Math. u. Phys. 3 (1892) 265–284.