JOURNAL OF ALGEBRA **199,** 124–141 (1998)
ARTICLE NO. JA977167

A Theorem on Random Matrices and Some Applications

Aner Shalev

Institute of Mathematics, The Hebrew University, Jerusalem, 91904, Israel

Received October 1, 1996

1. INTRODUCTION

A conjecture of Cameron [C] (see also [CK]) states that the proportion of permutations of S_n which belong to a transitive subgroup other than S_n or A_n tends to 0 as $n \to \infty$. This conjecture has recently been proven by Łuczak and Pyber in [LP], where several applications are included (see [MP], [Sh2] for additional applications). In [LP] it is suggested that the analogous phenomenon might hold for matrices. More specifically, the following is posed:

Problem. Suppose that p is a fixed prime and n tends to infinity. Is it true that almost all matrices in $GL(n, p)$ do not belong to an irreducible subgroup not containing $SL(n, p)$?

The purpose of this paper is to provide an affirmative answer to this question. In fact, our result is somewhat more general, in that we also deal with prime powers q, which need not be fixed (they may well depend on n). For brevity, let us say that a subgroup H of $GL(n, q)$ is *proper* if H does not contain $SL(n, q)$, and that H is *maximal* if it is maximal with respect to being proper.

THEOREM. *There exists a series of real numbers* $\{\delta_n\}$ *tending to* 0 *such that*, *for every prime power* q, *the probability that a randomly chosen matrix in* $GL(n, q)$ *belongs to a proper irreducible subgroup is at most* δ_n.

We note that, by Neumann and Praeger [NP, Lemma 2.3], the probability that a matrix $A \in GL(n, q)$ is irreducible is at least $1/(n + 1)$. In

0021-8693/98 $25.00

particular, the probability that a matrix in $GL(n, q)$ belongs to a proper irreducible subgroup is bounded away from zero if n is bounded, so in this sense our theorem is best possible.

Our proof shows that we can take $\delta_n = o(1/\log\log\log n)$, but in fact better bounds can be obtained with some more care. The main tools in the proof are recent results of Schmutz [S] on random matrices, as well as well known results of Aschbacher [A] and Liebeck [L] on maximal subgroups of classical groups. It is easy to see that our main result still holds if we replace $GL(n, q)$ by any almost simple group with socle $PSL(n, q)$. It is likely that analogues for other classical groups also exist; this may require extending the statistical theory of $GL(n, q)$ (see [S] and the references therein) to symplectic, orthogonal, and unitary groups.

The main result of this paper seems to be useful in several contexts. Applying it we show that, if x is any non-trivial element of $PSL(n, q)$, then the probability that x and a randomly chosen element y generate $PSL(n, q)$ tends to 1 as $q \to \infty$ (regardless of n). This extends a result of Guralnick, Kantor, and Saxl from [GKS]. We also show that, for large n, $GL(n, q)$ is generated invariably by two elements, which can be found rather easily. See Section 4 for terminology and more details. Additional applications of the main result will be included in [Sh1, LSSh].

I thank Laci Pyber, Martin Liebeck, and Jan Saxl for stimulating discussions, and All Souls College, Oxford, for its hospitality while this work was carried out.

2. PRELIMINARIES

Throughout this paper n denotes a large integer (sufficiently large to satisfy all required inequalities below).

Let P denote the uniform distribution on $GL(n, q)$. For a matrix $A \in GL(n, q)$, let $f_A \in F_q[x]$ denote its characteristic polynomial. Let M_n denote that set of all monic polynomials of degree n in $F_q[x]$. Then the correspondence $A \mapsto f_A$ defines a function $\psi : GL(n, q) \to M_n$ (whose image is the set of polynomials in M_n with non-zero constant term). Let P' denote the uniform distribution on M_n. We shall often use a different probability measure on M_n, induced from P, which (by abuse of notation) is also denoted by P. More specifically, for a subset $E \subseteq M_n$, define

$$P(E) := P\big(\psi^{-1}(E)\big).$$

The measure P will be used whenever we talk about probability without specifying the probability measure.

The order of a matrix $A \in GL(n,q)$ is denoted by $o(A)$. For $f \in M_n$ with $f(0) \neq 0$ we define the order (or the exponent) of f by

$$o(f) = \min\{k > 0 : f \mid (x^k - 1)\}.$$

Let C_f denote the companion matrix of f, namely the matrix corresponding to multiplication by t in $F_q[x]/(f)$ with respect to the basis consisting of the images of $1, x, \ldots, x^{n-1}$ (see for instance [J, p. 191]). It is then clear that $o(f) = o(C_f) < q^n$ (where the last inequality follows from the fact that the group of units of $F_q[x]/(f)$ has order $< q^n$).

Now, let $A \in GL(n,q)$ and let $f = f_A$ be its characteristic polynomial. Then A can be brought to a rational canonical form $\operatorname{diag}(C_{f_1}, \ldots, C_{f_k})$, where f_i are polynomials in $F_q[x]$ satisfying $f = f_1 \cdots f_k$. Setting $m = o(f)$ we see that for $i = 1, \ldots, k$, $o(C_{f_i}) = o(f_i)$ divides m, and this implies that $o(A)$ divides m as well. In particular it follows that for a matrix $A \in GL(n,q)$ we have $o(A) \leq o(f_A)$ (equality need not hold).

Let ϕ denote the Euler function (so that $\phi(d)$ is the number of positive integers $k < d$ which are prime to d), and let $\Phi_d(x)$ denote the dth cyclotonic polynomial. We now define some parameters which will be used throughout the paper, as

$$\epsilon_n = (\log\log\log n)^{-1},$$

$$d_n = (\log\log\log n)^2,$$

$$b_n = (\log n)^{1-\epsilon_n}.$$

The main result of [S] shows that, if n is large, then

$$P\left(q^{n-(\log n)^{2+\epsilon_n}} < o(A) < q^{n-(\log n)^{2-\epsilon_n}}\right) \geq 1 - o(\epsilon_n). \tag{1}$$

For $d \geq 1$ let $\alpha_d = \alpha_d(f)$ be the number of irreducible factors of degree d of f, counted with multiplicity. Let $\omega_d = \omega_d(f)$ be the number of distinct irreducible divisors of f whose degree is divisible by d (thus ω_1 is the number of distinct irreducible factors of f). Let $\Omega_d = \Omega_d(f)$ denote the number of irreducible factors of f whose degree is divisible by d, counted with multiplicity (thus $\Omega_d \geq \omega_d$). Set

$$w_d = w_d(f) = \max\{0, \Omega_d(f) - 1\}.$$

It is shown in [S, Lemma 6] that, with probability $1 - o(\epsilon_n)$ we have

$$\alpha_d(f) \leq d_n \text{ for all } d, \qquad \text{and} \qquad \alpha_d(f) \leq 1 \text{ for all } d > d_n. \tag{2}$$

Note that, if f satisfies (2), then the number of irreducible factors of f of degree $\leq d_n$ is at most $\sum_{d \leq d_n} \alpha_d(f) \leq d_n^2$.

Let

$$\mu_d = \mu_{d,n} = \frac{1}{d} \log(n/d).$$

Then it follows from [S, Theorem 5] that the condition

$$|\omega_d(f) - \mu_d| \leq \frac{1}{4}\mu_d \qquad \text{for all } d \leq b_n \tag{3}$$

holds with probability $1 - o(\epsilon_n)$. Define

$$M_n' = \{f \in M_n : f \text{ satisfies conditions (2) and (3) above}\}.$$

Then $P(M_n') \geq 1 - o(\epsilon_n)$.

For a group H, let $m(H)$ denote the maximal order of an element of H. Then we have $m(H) \leq m(H/K)m(K)$ for $K \lhd H$. It is also clear that, if G is a central product of H and K, then $m(G) = \max\{m(H), m(K)\}$. It is well known that

$$m(GL(n,q)) = q^n - 1. \tag{4}$$

It is also known that

$$m(S_k) \leq c^{\sqrt{k \log k}}, \tag{5}$$

where c is some absolute constant.

We need the following observation on the maximal order of cyclic subgroups of finite simple groups in general. By a simple group we shall always mean a nonabelian finite simple group. Recall that an almost simple group is a group lying between a simple group and its automorphism group.

LEMMA 2.1. *Let T be a finite almost simple group. Then*

$$m(T) \leq |T|^{1/3 + o(1)}.$$

Proof. Let T be almost simple with socle T_0. Then

$$m(T) \leq m(T_0)m(T/T_0) \leq m(T_0)|T/T_0| \leq m(T_0)\mathrm{Out}(T_0).$$

It is well known that $|\mathrm{Out}(T_0)| \leq |T_0|^{o(1)}$ (see [At]). This shows that $m(T) \leq m(T_0)|T|^{o(1)}$, so the result for T would follow from the result for T_0. We may therefore assume that T is simple.

Sporadic groups can obviously be ignored, and so it suffices to deal with alternating groups and with simple groups of Lie type. If T is alternating, then (5) shows that $m(T) \leq |T|^{o(1)}$ and we are done. So suppose T is a simple group of Lie type. Denote the (twisted) Lie rank of T by l, and let q denote the size of the underlying field.

There are absolute positive constants c_1, δ with the property that $|T| \geq q^{\delta l^2}$ and $T \leq PGL(n, q)$ for some $n \leq c_1 l$. Hence $m(T) \leq m(PGL(n, q)) \leq q^n \leq q^{c_1 l}$. It follows that $m(T) \leq |T|^{o(1)}$ provided $l \to \infty$. So it remains to deal with groups of bounded rank.

Let $m_s(T)$ ($m_u(T)$) denote the maximal order of a semisimple (unipotent) element of T. Then the Jordan decomposition in T shows that

$$m(T) \leq m_s(T) m_u(T).$$

Clearly, $m_u(T)$ is equal to the exponent of a Sylow p-subgroup P of T (recall that q is a pth power). Now, P is embedded in a Sylow p-subgroup Q of $PGL(n, q)$, where $n \leq c_1 l$ is bounded, say, by c_2. Hence

$$m_u(T) \leq \exp Q \leq pn \leq c_2 p \leq c_2 q.$$

By the structure of maximal tori in T we also have

$$m_s(T) \leq c_3 q^l.$$

It follows that $m(T) \leq c_4 q^{l+1}$ in general, and that $m(T) \leq c_5 q^l$ if p is bounded.

Now, the order of T is given by some polynomial in q (depending on the type of T; see [At]). Let d denote the degree of this polynomial. Then $|T| \geq c_6 q^d$. Inspection of [At] shows that $l/d \leq 1/3$ in all cases, and that $(l+1)/d \leq 1/3$ except when $T = PSL(2, q)$, $PSL(3, q)$, or the Suzuki group $Sz(q)$. In view of our bounds on $m(T)$, we see that $m(T) \leq |T|^{1/3 + o(1)}$ if p is bounded (which includes the case $T = Sz(q)$), or if $T \neq PSL(2, q)$, $PSL(3, q)$. The cases $T = PSL(2, q)$, $PSL(3, q)$ are easily settled using the well known subgroup structure of these groups.

The result follows. ∎

Remark. The example of $PSL(2, q)$ shows that the exponent $1/3$ in Lemma 2.1 is best possible. It is likely that $m(T) = m_s(T)$ for simple groups of Lie type, perhaps with a few exceptions.

Now, let U be the union of all irreducible maximal subgroups of $GL(n, q)$. To prove the main result, we need to show that

$$P(U) = o(\epsilon_n).$$

By a theorem of Aschbacher (see [KL, p. 3]), the irreducible maximal subgroups of $GL(n,q)$ are divided into 8 classes, denoted by $C_2 - C_8$ and $\mathscr{S}$. We can therefore write

$$U = \left(\bigcup_{i=2}^{8} U_i\right) \cup U_{\mathscr{S}},$$

where $U_i(U_{\mathscr{S}})$ is the union of the maximal subgroups in $C_i(\mathscr{S})$.

Let S denote the set of all matrices in $GL(n,q)$ whose order is at most $q^{0.9n}$. Then it follows from (1) that

$$P(S) = o(\epsilon_n).$$

The theorem is therefore a direct consequence of the three following results.

PROPOSITION A. *For large n we have*

$$U_2 \cup U_4 \cup U_5 \cup U_6 \cup U_7 \cup U_{\mathscr{S}} \subseteq S.$$

PROPOSITION B. $P(U_3) = o(\epsilon_n)$.

PROPOSITION C. $P(U_8) = o(\epsilon_n)$.

3. PROOFS

Proof of Proposition A. Let $M \in C_2$. Then there is a factorization $n = ab$ (where $b \geq 2$) such that $M \cong GL(a,q) \wr S_b$. Hence

$$m(M) \leq q^a \cdot c^{\sqrt{b \log b}} \leq q^{n/2} \cdot c^{\sqrt{n \log n}} \leq q^{0.9n},$$

assuming n is large. Hence $M \subseteq S$ in this case.

Let $M \in C_4$. Then there is a factorization $n = ab$ (where $a, b \geq 2$) such that M is a central product of $GL(a,q)$ with $GL(b,q)$. Therefore

$$m(M) \leq \max\{q^a, q^b\} \leq q^{n/2} < q^{0.9n},$$

as required.

Let $M \in C_5$. Then there is a prime power q_0 and a prime r such that $q = q_0^r$ and $M \cong GL(n, q_0)$. It follows that

$$m(M) \leq q_0^n = (q^n)^{1/r} \leq q^{n/2} \leq q^{0.9n}.$$

Let $M \in C_6$. Then there is a prime r and an integer a such that $n = r^a$ and $M \cong (C_{q-1} \circ r^{1+2a}).Sp(2a, r)$ (a normalizer of a symplectic type r-

group). In this case we have

$$m(M) \leq qr^2 \cdot m(Sp(2a, r)) \leq qr^2 \cdot r^{2a} \leq qn^4 \leq q^{0.9n}.$$

Let $M \in C_7$. Then there are integers $a, t \geq 2$ such that $n = a^t$ and M is a central product of t copies of $GL(a, q)$, extended by the symmetric group S_t. Hence

$$m(M) \leq m(GL(a, q))m(S_t) \leq q^a c^{\sqrt{t \log t}} \leq q^{\sqrt{n}} c^{\sqrt{\log n \log \log n}} < q^{0.9n}.$$

Finally, let $M \in \mathscr{S}$. Let Z denote the centre of $GL(n, q)$. Then $M \supset Z$ and $T = M/Z$ is almost simple. Note that M is not S_k or A_k in a representation of smallest degree over F_q, since the resulting subgroups are not maximal in $GL(n, q)$ (they are contained in an orthogonal subgroup). Therefore we have $|T| < q^{3n}$ by the main result of [L]. Furthermore, by Corollary 4.3 of [L] (and the fact that n is large), one of the following holds:

(1) $n = \binom{k}{2}$ and $\mathrm{Soc}(T) = PSL(k, q)$,

(2) $|T| < q^{2n+4}$.

In the first case, inequality (4) yields

$$m(M) \leq q^k m(\mathrm{Out}(PSL(k, q))) \leq q^k 2k \log q < q^{0.9n}.$$

So suppose $|T| < q^{2n+4}$. Applying Lemma 2.1, we find that either $|T|$ is bounded, in which case the conclusion follows trivially, or

$$m(T) < |T|^{2/5}. \tag{6}$$

Using (6) it follows that

$$m(M) < q(q^{2n+4})^{2/5} = q^{0.8n+2.6} < q^{0.9n}.$$

Proposition A is proved.

Proof of Proposition B. Let $M \in C_3$. Then there is a factorization $n = ab$ (where b is prime and $a \geq 1$) such that $M \cong GL(a, q^b).C$, where C is the Galois group of F_{q^b} over F_q. Set $N = GL(a, q^b) \lhd M$.

Claim 1. $M \setminus N \subseteq S$.

To show this, let $A \in M \setminus N$. Then $A = B\sigma$ where $B \in N$ and $1 \neq \sigma \in C$. Note that

$$A^b = BB^{\sigma} \cdots B^{\sigma^{b-1}} \in N.$$

This implies that $(A^b)^\sigma = B^\sigma B^{\sigma^2} \cdots B$ is conjugate in N to A^b. Let $f \in F_{q^b}[x]$ be the characteristic polynomial of A^b, as a matrix in $GL(a, q^b)$. Then the characteristic polynomial of $(A^b)^\sigma$ is f^σ, and so it follows that $f = f^\sigma$. Hence $f \in F_q[x]$, since the fixed field of σ is F_q (recall that b is prime). However, the degree of f is a. It follows that $o(f) \leq q^a$. Since the order of a matrix in $GL(a, q^b)$ is at most the order of its characteristic polynomial, we conclude that

$$o(A^b) \leq q^a.$$

This implies

$$o(A) \leq bq^a \leq nq^{n/2} < q^{0.9n}.$$

The claim follows.

Next, we study matrices inside N. We need some more notation. Given a polynomial $f \in M_n$, we shall write

$$f = \prod_{i=1}^{k} f_i^{m_i},$$

where $f_i \in F_q[x]$ are distinct monic irreducible polynomials, and the multiplicities m_i are positive.

Claim 2. Suppose $A \in N$ and $f = f_A$. Then $b \mid m_i \deg(f_i)$ for all $i = 1, \ldots, k$.

Indeed, let g be the characteristic polynomial of A as an element of $GL(a, q^b)$. Then $f = \prod_{\sigma \in C} g^\sigma$. Now let $h \in F_{q^b}[x]$ be an irreducible factor of g. Then either $h \in F_q[x]$, and h contributes h^b to the factorization of f over F_q, or $h \notin F_q[x]$, in which case the contribution is $\prod_{\sigma \in C} g^\sigma$, which is irreducible (over F_q) of degree divisible by b. The claim follows.

For a prime b let Q_b denote the set of all polynomials $f \in M_n$ with factorization $\prod_i f_i^{m_i}$ satisfying $b \mid m_i \deg(f_i)$ for all i. Let $Q = \cup Q_b$ over all primes b. By Claim 2 we have

$$N \subseteq \psi^{-1}(Q).$$

We shall now show that $P(Q) = o(\epsilon_n)$, and this will complete the proof of the proposition.

Let

$$Q' = Q \cap M'_n, \qquad Q'_b = Q_b \cap M'_n.$$

Then the polynomials $f \in Q'$ satisfy conditions (2) and (3) (stated in Section 2). Since $P(M'_n) \geq 1 - o(\epsilon_n)$, we have

$$P(Q) \leq P(Q') + o(\epsilon_n).$$

It therefore suffices to show that $P(Q') = o(\epsilon_n)$.

Claim 3. $|\omega_1(f) - \omega_b(f)| \le d_n^2$ for all $f \in Q'_b$.

Indeed, let $f \in Q'_b$. Since f satisfies (2), all irreducible factors of f of degree exceeding d_n occur with multiplicity 1, and so the degrees of such factors are all divisible by b. It also follows from (2) that there are at most d_n^2 irreducible factors of degree $\le d_n$. The claim follows.

Claim 4. $Q'_b = \emptyset$ for all $b \le b_n$.

Suppose, by contradiction, that $b \le b_n$ and $f \in Q'_b$. Since f satisfies condition (3) we have

$$\omega_1(f) \ge \frac{3}{4}\mu_1 = \frac{3}{4}\log n.$$

We also have

$$\omega_b(f) \le \frac{5}{4}\mu_b = \frac{5}{4}\frac{1}{b}\log(n/b) \le \frac{5}{8}\log n.$$

By combining the above inequalities we obtain

$$\omega_1(f) - \omega_b(f) \ge \frac{1}{8}\log n.$$

In view of Claim 3 it follows that

$$\frac{1}{8}\log n \le d_n^2 = (\log\log\log n)^4.$$

For n large this yields a contradiction.

We can now write

$$Q' = \cup_{b > b_n} Q'_b. \tag{7}$$

Choose a constant c_0 as in [S, Theorem 12].

Claim 5. With probability $1 - o(\epsilon_n)$,

$$\sum_{d > c_0 \log n} \phi(d) w_d(f) < (\log n)^{2+\epsilon_n}.$$

To show this, first note that, by [S, (14)], the inequality

$$\prod_{d \ge 1} \Phi_d(q)^{w_d(f)} < q^{(\log n)^{2+3\epsilon_n/4}}$$

holds with P'-probability $1 - o(\epsilon_n)$. We also have $\Phi_d(q) \geq q^{(1/2)\phi(d)}$ [S, Lemma 4], hence the inequality

$$\sum_{d \geq 1} \frac{1}{2} \phi(d) w_d(f) < (\log n)^{2+3\epsilon_n/4}$$

holds with P'-probability $1 - o(\epsilon_n)$. Assuming $(\log n)^{\epsilon_n/4} \geq 2$ as we may, we see that

$$\sum_{d \geq 1} \phi(d) w_d(f) < (\log n)^{2+\epsilon_n}$$

holds with P'-probability $1 - o(\epsilon_n)$. The same is true of course for the weaker inequality

$$\sum_{d > c_0 \log n} \phi(d) w_d(f) < (\log n)^{2+\epsilon_n}. \tag{8}$$

Since the above sum depends only on irreducible factors of f whose degree exceeds $c_0 \log n$, Theorem 12 of [S] implies that the P-probability of (8) and the P'-probability of (8) differ by at most $1/\log n$. Therefore inequality (8) occurs with P-probability at least $1 - o(\epsilon_n) - 1/\log n = 1 - o(\epsilon_n)$. The claim is proved.

Let Q'' (Q''_b) denote the set of all polynomials f in Q' (Q'_b) satisfying inequality (8). Then $P(Q') \leq P(Q'') + o(\epsilon_n)$, and so it suffices to show that $P(Q'') = o(\epsilon_n)$. In fact we show a bit more.

Claim 6. $Q'' = \emptyset$.

To show this first note that, by (7), we have

$$Q'' = \bigcup_{b > b_n} Q''_b.$$

Suppose, by contradiction, that $f \in Q''_b$ for some $b > b_n$. Let K denote the set of primes in the open interval $(c_0(\log n)^{\epsilon_n}, b_n)$, and fix $p \in K$. Assuming $c_0(\log n)^{\epsilon_n} > d_n$ as we may, we see that if g is an irreducible factor of f of degree divisible by p, then b divides $\deg(g)$ as well. This yields

$$\omega_p(f) = \omega_{pb}(f). \tag{9}$$

Since $p < b_n$ and $f \in Q'$, we have (for large n)

$$\omega_p(f) \geq \frac{3}{4} \mu_p = \frac{3}{4} \frac{1}{p} \log(n/p) \geq 1 + \frac{1}{2p} \log(n/p). \tag{10}$$

It follows from (9) and (10) that

$$w_{pb}(f) \geq \omega_{pb}(f) - 1 \geq \frac{1}{2p} \log(n/p). \tag{11}$$

Note that $pb > c_0 \log n$ for all $p \in K$. Since inequality (8) is satisfied in Q'', it follows that

$$\sum_{p \in K} \phi(pb) w_{pb}(f) < (\log n)^{2+\epsilon_n}. \tag{12}$$

However, using (11) we see that

$$\begin{aligned} \sum_{p \in K} \phi(pb) w_{pb}(f) &\geq (b-1) \sum_{p \in K} (p-1) \frac{1}{2p} \log(n/p) \\ &\geq \frac{b-1}{4} \sum_{p \in K} \log(n/p). \end{aligned} \tag{13}$$

Now,

$$\sum_{p \in K} \log(n/p) = |K| \log n - \sum_{p \in K} \log p. \tag{14}$$

By the Prime Number Theorem we have

$$|K| \sim \frac{b_n}{\log b_n} \qquad \text{and} \qquad \sum_{p \in K} \log p \sim b_n.$$

Substitution in (14) yields

$$\sum_{p \in K} \log(n/p) \sim \frac{b_n \log n}{\log b_n} - b_n \sim \frac{(\log n)^{2-\epsilon_n}}{\log \log n}.$$

Applying (13) we now obtain

$$\sum_{p \in K} \phi(pb) w_{pb}(f) \geq \frac{b-1}{4} \frac{(\log n)^{2-\epsilon_n}}{\log \log n} \geq \frac{(\log n)^{3-2\epsilon_n}}{4 \log \log n}. \tag{15}$$

This violates inequality (12) (for large n).

The claim follows.

The proof of Proposition B is complete.

Proof of Proposition C. Let $M \in C_8$. Then $M = Sp_n(q)$ (n even), or $O_n^{\epsilon}(q)$ (q odd), or $GU_n(q^{1/2})$ (where q is a square), embedded naturally. Let t denote the transpose operation. If M is a unitary group, let σ be the generator of the Galois group $\mathrm{Gal}(F_q/F_{q^{1/2}})$, otherwise set $\sigma = 1$. Now, for a matrix $A \in GL(n, q)$, define

$$A^* = (A^t)^{\sigma}.$$

For a polynomial $f = \sum_{i=0}^{n} a_i x^i \in M_n$ with $a_0 \neq 0$, we define

$$\tilde{f} = (a_0^{\sigma})^{-1} \sum_{i=0}^{n} a_{n-i}^{\sigma} x^i.$$

Then $\tilde{f} \in M_n$. Note that $\tilde{f}$ is the monic scalar multiple of $t^n f^{\sigma}(t^{-1})$. Therefore, if $f = f_A$, then the characteristic polynomial of $(A^*)^{-1}$ is $\tilde{f}$.

Define

$$Q = \left\{ f \in M_n : f(0) \neq 0, f = \tilde{f} \right\}.$$

Claim 1. If $f = f_A$ for some $A \in M$, then $f \in Q$.

Indeed, if A lies in M (or in a conjugate of M), then A is conjugate in $GL(n, q)$ to $(A^*)^{-1}$ (see for instance Wall [W] for this and more detailed information). Thus A and $(A^*)^{-1}$ have the same characteristic polynomial, namely $f = \tilde{f}$.

In order to prove the proposition it suffices to show that

$$P(Q) = o(\epsilon_n).$$

Claim 2. Let $f \in Q$. Then for each irreducible factor g of f we have $g = \tilde{g}$ or $g\tilde{g} \mid f$. In particular, if $\alpha_d(f) = 1$ where $d = \deg(g)$, then $g = \tilde{g}$.

Indeed, this follows immediately from the equality $f = \tilde{f}$.

Define

$$Q' = Q \cap M_n'.$$

Then $P(Q) \leq P(Q') + o(\epsilon_n)$, and so it suffices to show that $P(Q') = o(\epsilon_n)$.

Let $f \in Q'$. Then $\alpha_d(f) \leq 1$ for all $d > d_n$. Therefore any irreducible factor g of f of degree exceeding d_n satisfies $g = \tilde{g}$.

For $d \geq 1$ let I_d denote the set of all monic irreducible polynomials of degree d (over F_q) and let

$$J_d = \{ g \in I_d : g = \tilde{g} \}.$$

It is known that

$$\frac{q^d}{d}(1 - q^{1-d/2}) \leq |I_d| \leq \frac{q^d}{d}.$$

In particular, $|I_d| \geq q^d/2d$ for $d > d_n$.

It is also clear that

$$|J_d| \le q^{d/2}.$$

Indeed, this is a bound on the number of *all* degree d monic polynomials g satisfying $g = \tilde{g}$. Let

$$J = \bigcup_{d > d_n} J_d.$$

Note that, if $f \in Q'$, then f has irreducible factors of degree exceeding d_n (indeed it has at least $\omega_1(f) - d_n^2 \ge (3/4)\log n - d_n^2$ such factors). We can therefore write

$$Q' = \bigcup_{g \in J} Q'(g),$$

where

$$Q'(g) = \{f \in Q' : g \mid f\}.$$

We also set

$$Q'_d = \bigcup_{g \in J_d} Q'(g).$$

Then

$$Q' = \bigcup_{d > d_n} Q'_d.$$

For g irreducible, define

$$M'_n(g) = \{f \in M'_n : f(0) \ne 0, g \mid f\}.$$

Claim 3. Suppose $d > d_n$ and $g \in I_d$. Then $P(M'_n(g)) \le 2dq^{-d}$.

It is known that, if $f \in M_n$ and $f(0) \ne 0$, then $P(\{f\})$ depends only on the degrees of the irreducible factors of f and their multiplicities (see [S, p. 353]). This implies that $P(M'_n(g)) = P(M'_n(h))$ for all $g, h \in I_d$. However, the events $M'_n(g)$ ($g \in I_d$) are pairwise disjoint (since $\alpha_d(f) \le 1$ for $f \in M'_n$). It follows that

$$|I_d| P\big(M'_n(g)\big) \le 1.$$

Since $|I_d| \ge q^d/2d$ the result follows.

Claim 4. For $d > d_n$, $P(Q'_d) \le 2dq^{-d/2}$.

Indeed, Q'_d is a union of $|J_d|$ subsets of the form $Q'(g)$. Since $Q'(g) \subseteq M'_n(g)$ we have $P(Q'(g)) \le 2dq^{-d}$ by Claim 3. It follows that

$$P(Q'_d) \le |J_d| 2dq^{-d} \le q^{d/2} 2dq^{-d} = 2dq^{-d/2}.$$

Claim 5. $P(Q') = o(\epsilon_n)$.

We have

$$P(Q') \le \sum_{d > d_n} P(Q'_d) \le \sum_{d > d_n} 2dq^{-d/2}.$$

For n large and $d > d_n$ we have $2d < q^{d/4}$. Thus

$$P(Q') \le \sum_{d > d_n} q^{-d/4} \le \frac{q^{-d_n/4}}{1 - q^{-1/4}} \le 10q^{-d_n/4}.$$

The term on the right hand side is clearly in $o(\epsilon_n)$. The claim follows.

This completes the proof of Proposition C, and of the main result.

4. APPLICATIONS

In this section we derive some new results concerning generating pairs for the general (and special) linear group.

For a group G and an element $x \in G$, let $P_x(G)$ denote the probability that x, y generate G, where y is a randomly chosen element of G. Set also

$$P^-(G) = \min\{P_x(G) : 1 \ne x \in G\}.$$

The probabilities $P_x(G)$, $P^-(G)$ were studied (in a slightly different notation) by Guralnick, Kantor, and Saxl [GKS] in the case where G is a finite simple classical group. Let G be such a group, let F_q be its underlying field, and let n denote the dimension of G. Then it is proved in [GKS] that

$$P^-(G) \le 1 - \frac{1}{2q^2 + 2},$$

so $P^-(G)$ is bounded away from 1 if q is bounded. It is also shown that

$$P^-(G) \to 1 \qquad \text{as } q \to \infty, \text{ provided } n \text{ is bounded.}$$

The case where both q and n tend to infinity remains unclear. For $PSL(n, q)$ this case can now be settled as follows.

THEOREM 4.1. *With the above notation,* $P^-(PSL(n,q)) \to 1$ *as* $q \to \infty$, *without restrictions on* n.

To prove the theorem we may assume $n \to \infty$. We need some notation. For a maximal subgroup M of G and an element $x \in G$, let $\mathrm{fix}(x, M)$ denote the number of fixed points of x in the permutation representation of G on the cosets of M, and let the fixity of G in this representation be defined by

$$\mathrm{fix}(G, M) = \max\{\mathrm{fix}(x, M) : 1 \neq x \in G\},$$

and the relative fixity (or the fixed-point ratio) by

$$\mathrm{rfix}(G, M) = \frac{\mathrm{fix}(G, M)}{|G : M|}.$$

Let $\mathscr{M}$ be a set of representatives for the conjugacy classes of maximal subgroups of G, and fix a non-identity element $x \in G$.

Now, if x, y do not generate G, then there is a maximal subgroup M of G containing x, such that $y \in M$. This yields the inequality

$$1 - P_x(G) \leq \sum_{x \in M \max G} |G : M|^{-1} = \sum_{M \in \mathscr{M}} \mathrm{rfix}(x, M), \tag{16}$$

which was obtained and used in [GKS].

Now, suppose $G = PSL(n, q)$, $n \to \infty$, and $y \in G$ is chosen at random. Then, by our main result, the probability that y lies in an irreducible maximal subgroup of G tends to 0, and is of the form $o(\epsilon_n)$. Therefore

$$1 - P_x(G) \leq o(\epsilon_n) + Q_x(G),$$

where $Q_x(G)$ is the probability that a random element $y \in G$ lies in some reducible maximal subgroup M of G containing x. Let $\mathscr{P}$ be a set of representatives for the conjugacy classes of the reducible maximal subgroups of G. As in (16), we have

$$Q_x(G) \leq \sum_{M \in \mathscr{P}} \mathrm{rfix}(x, M).$$

We therefore obtain

$$1 - P_x(G) \leq o(\epsilon_n) + \sum_{M \in \mathscr{P}} \mathrm{rfix}(x, M) \leq o(\epsilon_n) + \sum_{M \in \mathscr{P}} \mathrm{rfix}(G, M).$$

Maximizing the left hand side (over $1 \neq x \in G$) we obtain

$$1 - P^-(G) \leq o(\epsilon_n) + \sum_{M \in \mathscr{P}} \mathrm{rfix}(G, M).$$

To show that $P^-(G) \to 1$ it therefore suffices to show that

$$\sum_{M \in \mathscr{P}} \text{rfix}(G, M) \to 0 \text{ as } q \to \infty. \tag{17}$$

Write

$$\mathscr{P} = \{P_{k,n} : 1 \le k \le n-1\},$$

where $P_{k,n}$ is the stabilizer in G of some k-dimensional subspace. It follows from the results of Shih [Shi] that

$$\text{rfix}(G, P_{k,n}) \le \frac{c}{q^l},$$

where c is some absolute constant and $l = \min\{k, n-k\}$. This yields

$$\sum_{M \in \mathscr{P}} \text{rfix}(G, M) = \sum_{0<k<n} \text{rfix}(G, P_{k,n}) \le 2c \sum_{0<k\le n/2} q^{-k}$$

$$\le 2c \frac{q^{-1}}{1-q^{-1}} \le 4cq^{-1}.$$

This implies (17).

Theorem 4.1 is proved.

Note that our proof yields

$$P^-(PSL(n,q)) \ge 1 - O\left(\frac{1}{q}\right) - o\left(\frac{1}{\log\log\log n}\right).$$

Remark. Using somewhat similar ideas (and [LP] in particular), it can be shown that, for $x \in A_n$,

$$P_x(A_n) = \frac{\text{supp}(x)}{n} + o(1),$$

where $\text{supp}(x)$ denotes the number of points moved by x [Sh2]. It would be nice to obtain an analogous formula for $P_x(PSL(n,q))$, as a function of some relevant invariants of x.

The second application of our main theorem has to do with invariable generation of $GL(n,q)$.

We say that elements $x_1, \ldots, x_d$ of a group G generate G *invariably* if

$$x_1^{g_1}, \ldots, x_d^{g_d} \text{ generate } G \text{ for all } g_1, \ldots, g_d \in G.$$

This condition, which arises in the context of the inverse Galois problem and the computation of Galois groups (see [SM]), is obviously a very strong one; many groups do not have small sets of invariable generators. However, our main theorem can be used to prove that, for large n, $GL(n,q)$ is invariably generated by two elements. In fact we prove a little more.

THEOREM 4.2. *There exists $x \in GL(n,q)$ such that, if $y \in GL(n,q)$ is chosen at random, then the probability that x, y generate $GL(n,q)$ invariably is at least* $1 - o(\epsilon_n)$.

To prove the theorem, set $G = GL(n,q)$ and let $x \in G$ be a Singer cycle. Let U denote the set of elements $y \in G$ which do not belong to a proper irreducible subgroup. We shall prove

Claim. If $y \in U$ then x, y generate G invariably.

Indeed, suppose by contradiction that $y \in U$ and that x, y do not generate G invariably. Then there exist a conjugate x' of x and a conjugate y' of y such that

$$H := \langle x', y' \rangle \neq G.$$

Note that x' is also a Singer cycle, so in particular it is irreducible. This implies that the subgroup H is irreducible.

Now, since $y \in U$ we have $y' \in U$ (as U is closed under conjugacy). Since y' lies in the irreducible subgroup H it follows that H is not proper, namely $H \supseteq SL(n,q)$. We find that

$$H \supseteq \langle SL(n,q), x' \rangle = G$$

(where the last equality follows from the fact that the determinant of a Singer cycle generates the multiplicative group $F_q^{\star}$). This contradiction completes the proof of the claim.

Theorem 4.2 follows, since the probability that $y \in U$ is $1 - o(\epsilon_n)$.

Remark. It can be shown that a variant of Theorem 4.2 holds for S_n. More precisely, let x be the full cycle $(1, 2, \dots, n)$. Then, adopting the arguments of the proof of Theorem 4.2 and using [LP], one easily sees that the probability that x, y generate S_n invariably is $1 - o(n^{-0.05})$ if n is even, and $1/2 - o(n^{-0.05})$ if n is odd. In particular, if n is large, then S_n is invariably generated by two elements, which can in practice be found rather easily. This could be useful in deciding whether the Galois group of a given irreducible polynomial of degree n over the rationals is equal to the full symmetric group S_n (see [SM]).

REFERENCES

[A] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.

[At] J. H. Conway, S. P. Norton, R. A. Parker, and R. A. Wilson, "Atlas of Finite Groups," Oxford Univ. Press, Oxford, 1985.

[C] P. J. Cameron, Almost all quasigroups have rank 2, *Discrete Math.* **106 / 107** (1992), 111–115.

[CK] P. J. Cameron and W. M. Kantor, Random permutations: Some group-theoretic aspects, *Combinatorics Probab. Comput.* **2** (1993), 257–262.

[GKS] R. M. Guralnick, W. M. Kantor, and J. Saxl, The probability of generating a classical group, *Commun. Algebra* **22** (1994), 1395–1402.

[J] N. Jacobson, "Basic Algebra, I," Freeman, San Francisco, 1974.

[KL] P. B. Kleidman and M. W. Liebeck, "The Subgroup Structure of the Finite Classical Groups," London Math. Soc. Lecture Note Series, Vol. 129, Cambridge Univ. Press, Cambridge, United Kingdom, 1990.

[L] M. W. Liebeck, On the orders of maximal subgroups of the finite classical groups, *Proc. London Math. Soc. (3)* **50** (1985), 426–446.

[LSSh] M. W. Liebeck, J. Saxl, and A. Shalev, Fixed point free elements in simple transitive groups, in preparation.

[LP] T. Łuczak and L. Pyber, On random generation of the symmetric group, *Combinatorics Probab. Comput.* **2** (1993), 505–512.

[MP] T. Müller and L. Pyber, in preparation.

[NP] P. M. Neumann and C. E. Praeger, A recognition algorithm for special linear groups, *Proc. London Math. Soc (3)* **65** (1992), 555–603.

[S] E. Schmutz, The order of a typical matrix with entries in a finite field, *Israel J. Math.* **91** (1995), 349–371.

[SM] L. Soicher and J. McKay, Computing Galois groups over the rationals, *J. Number Theory* **20** (1985), 273–281.

[Sh1] A. Shalev, Random generation of simple groups by two conjugate elements, *Bull. London Math. Soc.*, **29** (1997), 571–576.

[Sh2] A. Shalev, Generation of symmetric groups, in preparation.

[Shi] T. Shih, "Bounds for Fixed Point Ratios of Permutation Representations of $GL_n(q)$ and Groups of Genus Zero," Ph.D. Thesis, Caltech, 1991.

[W] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* **3** (1963), 1–62.