MANY ZEROS OF MANY CHARACTERS OF GL(n, q)

PATRICK X. GALLAGHER*, MICHAEL J. LARSEN, AND ALEXANDER R. MILLER

Abstract. For $G = \mathrm{GL}(n, q)$, the proportion $P_{n,q}$ of pairs (χ, g) in $\mathrm{Irr}(G) \times G$ with $\chi(g) \neq 0$ satisfies $P_{n,q} \to 0$ as $n \to \infty$.

1. Introduction

A few years ago, it was shown [5] that for $G = S_n$ the proportion P_n of pairs (χ, g) in $\mathrm{Irr}(G) \times G$ with $\chi(g) \neq 0$ satisfies

$$P_n \to 0 \text{ as } n \to \infty. \tag{1}$$

Here we prove the analogous statement for $\mathrm{GL}(n, q)$:

Theorem 1. *The proportion $P_{n,q}$, in $\mathrm{Irr}(\mathrm{GL}(n, q)) \times \mathrm{GL}(n, q)$, of pairs (χ, g) with $\chi(g) \neq 0$ satisfies*

$$\sup_q P_{n,q} \to 0 \text{ as } n \to \infty. \tag{2}$$

To prove (2) for $\mathrm{GL}(n, q)$, we compare conjugacy class sizes s_g and character degrees d_χ. In Section 3, we prove the general inequality (3). In Section 7, using technical information from Sections 4–6, we prove that for most pairs (χ, g) consisting of an irreducible character of G and an element of G, the greatest common divisor (d_χ, s_g) is much smaller than d_χ. In Section 2, we prove that these two facts imply the theorem. The precise statements are as follows.

Lemma A. *For each finite group G and $\varepsilon > 0$, the proportion P, in $\mathrm{Irr}(G) \times G$, of pairs (χ, g) with $\chi(g) \neq 0$ satisfies*

$$P \leq Q(\varepsilon) + \varepsilon^2, \tag{3}$$

with $Q(\varepsilon)$ the proportion, in $\mathrm{Irr}(G) \times G$, of pairs (χ, g) with $(d_\chi, s_g)/d_\chi \geq \varepsilon$.

Lemma B. *For all $\delta, \varepsilon > 0$, there exists N such that if $n \geq N$, q is a prime power, and $G = \mathrm{GL}(n, q)$, then for (χ, g) in $\mathrm{Irr}(G) \times G$,*

$$\frac{(d_\chi, s_g)}{d_\chi} < \varepsilon, \tag{4}$$

except for (χ, g) in a subset $\mathcal{R} \subset \mathrm{Irr}(G) \times G$ such that

$$|\mathcal{R}| \leq \delta |\mathrm{Irr}(G) \times G|. \tag{5}$$

We are grateful to the referees for several suggestions which improved the exposition.

---

*Paper finished posthumously.

ML was partially supported by the NSF grant DMS-1702152. AM was partially supported by the Austrian Science Foundation.

2. Proof of Theorem 1 using Lemmas A and B

For $G = \mathrm{GL}(n, q)$ and $\varepsilon > 0$, Lemma A gives

$$P_{n,q} \leq Q_{n,q} + \varepsilon^2,$$

with $P_{n,q}$ the proportion of pairs (χ, g) with $\chi(g) \neq 0$ and $Q_{n,q}$ the proportion of pairs with $(d_\chi, s_g)/d_\chi \geq \varepsilon$. Lemma B gives $Q_{n,q} \leq \delta$ for $n \geq N$. Thus for n sufficiently large,

$$P_{n,q} \leq \delta + \varepsilon^2,$$

from which Theorem 1 follows. □

3. Proof of Lemma A by a device of Burnside

We follow [2]. For $\chi \in \mathrm{Irr}(G)$ and $g \in G$, it is well-known that $\chi(g)$ ([6, Prop. 15]) and $s_g\chi(g)/d_\chi$ ([6, Ex. 6.9]) are algebraic integers, and, of course, both lie in the cyclotomic field $\mathbb{Q}(\zeta_{|G|})$ with $\zeta_{|G|} = e^{2\pi i/|G|}$. Thus, for all $a, b \in \mathbb{Z}$,

$$\frac{(ad_\chi + bs_g)\chi(g)}{d_\chi}$$

is an algebraic integer. Choosing a and b so that $ad_\chi + bs_g$ is the greatest common divisor (d_χ, s_g) of d_χ and s_g, this gives

$$\chi(g) = \frac{d_\chi}{(d_\chi, s_g)}\alpha_{\chi,g}, \tag{6}$$

with $\alpha_{\chi,g}$ an algebraic integer in $\mathbb{Q}(\zeta_{|G|})$.

From (6), for each χ,

$$\sum_{g\in G}\Big(\frac{d_\chi}{(d_\chi, s_g)}\Big)^2|\alpha_{\chi,g}|^2 = |G|. \tag{7}$$

To (7), apply elements σ of the Galois group $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_{|G|})/\mathbb{Q})$, average over Γ, and use the fact, due to Burnside, that the average over Γ of $|\sigma(\alpha)|^2$ is ≥ 1 for each non-zero algebraic integer $\alpha \in \mathbb{Q}(\zeta_{|G|})$, [2, p. 459]. This gives, for each χ,

$$\sum_{g\in G}{}'\Big(\frac{d_\chi}{(d_\chi, s_g)}\Big)^2 \leq |G|, \tag{8}$$

the dash meaning that the sum is over those g with $\chi(g) \neq 0$, [2, p. 460]. From (8),

$$\sum_{\chi\in\mathrm{Irr}(G)}\sum_{g\in G}{}'\Big(\frac{d_\chi}{(d_\chi, s_g)}\Big)^2 \leq |\mathrm{Irr}(G)||G|. \tag{9}$$

From (9), the proportion, in $\mathrm{Irr}(G) \times G$, of pairs (χ, g) with both $\chi(g) \neq 0$ and $(d_\chi, s_g)/d_\chi \leq \varepsilon$ is at most ε^2, from which (3) follows. □

4. Number theoretic lemmas: partitions

We denote by $p(n)$ the number of partitions of a non-negative integer n.

Lemma 1. *For each positive integer n, $p(n) \leq 2^{n-1}$.*

Proof. The base case $n = 1$ is trivial. For $n > 1$, the number of partitions with smallest part m is at most $p(n-m)$, so

$$p(n) \leq 1 + p(1) + p(2) + \cdots + p(n-1) \leq 1 + 1 + 2 + \cdots + 2^{n-2} = 2^{n-1},$$

and the lemma follows by induction. □

Lemma 2. *Let $\phi := \frac{1+\sqrt{5}}{2}$. Then $p(n) \leq \phi^n$ for all non-negative integers n.*

Proof. The partition function is non-decreasing since the number of partitions of $n+1$ with a part of size 1 is $p(n)$. The lemma holds for $n \in \{0, 1\}$. For $n \geq 2$, the pentagonal number theorem implies

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + \cdots, \tag{10}$$

with sign pattern $++--++--++--\cdots$ and where the sum on the right-hand side terminates at the last term $\pm p(n-m)$, where m is the largest generalized pentagonal number for which $n \geq m$. By monotonicity, the right-hand side of (10) is at most $p(n-1) + p(n-2)$, so the lemma follows by induction on n. □

Lemma 3. *There exists $\gamma < 1$ such that if $q \geq 2$ and a and b are positive integers such that $a(b-1) \geq N \geq 0$, then*

$$\frac{p(b)}{q^{a(b-1)}} < 2\gamma^N.$$

Proof. It suffices to prove the lemma for $q = 2$. For $a = 1$, we have $b - 1 \geq N$, so Lemma 2 implies

$$\frac{p(b)}{2^{a(b-1)}} = \frac{p(b)}{2^{b-1}} < 2(\phi/2)^N.$$

For $a \geq 2$, $a(b-1) \leq 2(a-1)(b-1)$, so by Lemma 1,

$$\frac{p(b)}{2^{a(b-1)}} \leq 2^{-(a-1)(b-1)} \leq (1/\sqrt{2})^N < 2(1/\sqrt{2})^N.$$

Therefore, we may take $\gamma = \phi/2 > 1/\sqrt{2}$. □

5. Number theoretic lemmas: cyclotomic polynomials

For n a positive integer, let $\Phi_n(x)$ denote the minimal polynomial over $\mathbb{Q}$ of $e^{2\pi i/n}$. Thus

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \tag{11}$$

so by Möbius inversion,

$$\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}. \tag{12}$$

For any prime ℓ, let $\mathrm{ord}_\ell(x)$ denote the largest integer e such that ℓ^e divides x.

Lemma 4. *Let ℓ be a prime, e a positive integer, and n an integer such that $\mathrm{ord}_\ell(n-1) = e$.*

(i) *If k is a positive integer prime to ℓ, then $\mathrm{ord}_\ell(n^k - 1) = e$.*
(ii) *If ℓ is odd and $\mathrm{ord}_\ell(k) = 1$, then $\mathrm{ord}_\ell(n^k - 1) = e + 1$.*

Proof. Let $n = 1 + m\ell^e$, where $\ell \nmid m$. By the binomial theorem,

$$n^k \equiv 1 + km\ell^e \pmod{\ell^{2e}},$$

which implies claim (i). For claim (ii), using part (i), it suffices to treat the case $k = \ell$, for which we have

$$n^\ell \equiv 1 + m\ell^{e+1} + \frac{m^2(\ell-1)}{2}\ell^{2e+1} \pmod{\ell^{3e}}. \qquad \square$$

Lemma 5. *Suppose $n > 0$ and $a > 1$ are integers. We factor $\Phi_n(a)$ as $P_n(a)R_n(a)$, where $P_n(a)$ is relatively prime to n and $R_n(a)$ factors into prime divisors of n.*

(i) *Every prime divisor of $P_n(a)$ is $\equiv 1 \pmod n$.*
(ii) *If $n \geq 3$, $R_n(a)$ is a square-free divisor of n.*
(iii) *For $n \geq 3$, $P_n(a) > 2^{\sqrt{n/2} - \log_2 n - 2}$.*
(iv) *If $m\ell > n$ and ℓ is a prime divisor of $P_m(a)$, then*

$$\operatorname{ord}_\ell(a^n - 1) = \begin{cases} \operatorname{ord}_\ell P_m(a) & \text{if } m \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Fix any prime ℓ which divides $\Phi_n(a)$. As $\ell \mid a^n - 1$, a is not divisible by ℓ, so it represents a class in $\mathbb{F}_\ell^\times$. Let j be the order of this class. As $a^n \equiv 1 \pmod \ell$, $j \mid n$. Let s denote the largest square-free divisor of n/j. By (12),

$$\operatorname{ord}_\ell \Phi_n(a) = \operatorname{ord}_\ell \prod_{d \mid s} (a^{n/d} - 1)^{\mu(d)}.$$

Now, if s can be written ps' for some prime $p \neq \ell$,

$$\prod_{d \mid s} (a^{n/d} - 1)^{\mu(d)} = \prod_{d \mid s'} \Big(\frac{a^{n/d} - 1}{a^{n/pd} - 1} \Big)^{\mu(d)}. \tag{13}$$

Applying part (i) of Lemma 4 with $k = p$, the above formula implies $\operatorname{ord}_\ell \Phi_n(a) = 0$, contrary to assumption. Since s is square-free, it follows that it can only be 1 or ℓ.

If ℓ divides $P_n(a)$, then it does not divide n. That means $s = 1$, so the class of a has order n in a group of order $\ell - 1$. This implies part (i). Conversely, if ℓ does divide n, it cannot be 1 (mod n), so $s = \ell$.

If $s = \ell > 2$, then d square-free and $\operatorname{ord}_\ell(a^{n/d} - 1) > 0$ implies $d \in \{1, \ell\}$. Therefore, part (ii) of Lemma 4 implies that the left-hand side of (13) has ord_ℓ equal to 1. If $s = \ell = 2$, then $k = 1$, so we need only consider the case that n is a power of 2. For $t \geq 2$, $\Phi_{2^t}(x) = (x^{2^{t-2}})^2 + 1$, so plugging in a, the result has at most one factor of 2. This gives claim (ii).

By (12),

$$\Phi_n(a) \geq a^{\deg \Phi_n} \prod_{i=1}^{\infty} (1 - a^{-i}) \geq a^{\phi(n)} \prod_{i=1}^{\infty} (1 - 2^{-i}) \geq \frac{2^{\phi(n)}}{4}. \tag{14}$$

As $\phi(p^e) \geq \sqrt{p^e}$ except when $p^e = 2$, the multiplicativity of ϕ implies $\phi(n) \geq \sqrt{n/2}$. By part (ii), $R_n(a) \leq n$, and claim (iii) follows.

If ℓ divides $P_m(a)$, then the image of a in $\mathbb{F}_\ell^\times$ is of order m, so ℓ divides $a^n - 1$ only if n is divisible by m. In that case, $P_m(a)$ divides $\Phi_m(a)$, which is a divisor of $a^m - 1$ and therefore $a^n - 1$. Moreover, ℓ does not divide m, so $\operatorname{ord}_\ell P_m(a) = \operatorname{ord}_\ell \Phi_m(a)$. To prove (iv), it remains to show that $a^n - 1$ has no additional factors of ℓ beyond those in $a^m - 1$. It suffices to prove that $\Phi_{n'}(a)$ is not divisible by ℓ if n' is a divisor

of n and m is a proper divisor of n'. Indeed, ℓ does not divide $P_{n'}(a)$ because a is not of order exactly m' (mod ℓ). If it divides $\Phi_{n'}(a)$, it must divide $R_{n'}(a)$, so it must divide n'. It does not divide m, so it must divide $n'/m \leq m$. This is ruled out by (i). □

6. Irreducible characters of GL(n,q)

In what follows, $G = \mathrm{GL}(n,q)$. By [1, Proposition 3.5],

$$\frac{q^n}{2} \leq |\mathrm{Irr}(G)| \leq q^n. \tag{15}$$

Denote by $\mathcal{P}$ the set of all partitions λ of integers $|\lambda| \geq 0$ (including the empty partition $\emptyset$) and by $\mathcal{F}$ the set of all non-constant monic irreducible polynomials $f(x) \in \mathbb{F}_q[x]$ with non-zero constant term. We define the *degree* of a map $\nu : \mathcal{F} \to \mathcal{P}$ as follows:

$$\deg(\nu) := \sum_{f \in \mathcal{F}} \deg(f)|\nu(f)|.$$

By Jordan decomposition, there is a natural bijection between conjugacy classes in G and maps $\nu : \mathcal{F} \to \mathcal{P}$ of degree n. Green [3] introduced the set $\mathcal{G}$ of *simplices* and proved (Theorem 12) that $\mathrm{Irr}(G)$ has a parametrization by maps $\nu : \mathcal{G} \to \mathcal{P}$ satisfying

$$\sum_{f \in \mathcal{G}} \deg(f)|\nu(f)| = n.$$

By fixing in a compatible way multiplicative generators of finite fields, he gave a degree-preserving bijection between $\mathcal{F}$ and $\mathcal{G}$. We will ignore the distinction between $\mathcal{F}$ and $\mathcal{G}$ henceforward. The same theorem of Green also gave a formula for the degree of the irreducible character χ associated to ν. It can be written

$$d_\chi = q^{N_\nu} \frac{\prod_{i=1}^{n}(q^i - 1)}{\prod_{f \in \mathcal{F}} \prod_{i=1}^{|\nu(f)|}(q^{h_{\nu(f),i} \deg(f)} - 1)}, \tag{16}$$

where N_ν is a certain non-negative integer, and the $h_{\lambda,i}$ are the hook lengths of the partition λ; in particular these are positive integers $\leq |\lambda|$.

By the *support of* ν, which we denote $\operatorname{supp}\nu$, we mean the set of $f \in \mathcal{F}$ such that $\nu(f) \neq \emptyset$.

Lemma 6. *Let γ be defined as in Lemma 3, and let N be a positive integer. Then the number of degree n functions $\nu\colon \mathcal{F} \to \mathcal{P}$ satisfying $\deg(f)(|\nu(f)| - 1) \geq N$ for some f is less than $\frac{2N\gamma^N}{(1-\gamma)^2} q^n$.*

Proof. It suffices to prove that for each m, the number of choices of ν of degree n such that for some $f \in \mathcal{F}$, $\deg(f)(|\nu(f)| - 1) = m$ is less than $2m\gamma^m q^n$. Since there are at most m ways of expressing m as $a(b-1)$ for positive integers a and b, it suffices to prove that there are less than $2\gamma^m q^n$ such ν of degree n for which $|\nu(f)| = b$ for some $f \in \mathcal{F}$ of degree a. Since there are fewer than q^a elements of $\mathcal{F}$ of degree a, it suffices to prove that for given $f \in \mathcal{F}$ of degree a, there are at most $2\gamma^m q^{n-a}$ possibilities for ν with $|\nu(f)| = b$. For each partition λ of b, the functions ν of degree n with $\nu(f) = \lambda$ can be put into bijective correspondence with ν' of degree $n - ab$ with $\nu'(f) = \emptyset$. By (15), the number of possibilities for ν' and therefore for ν is at most $q^{n-ab} = q^{n-m-a}$. Summing over the possibilities for λ, which by Lemma 3 number less than $2\gamma^m q^m$, we obtain less than $2\gamma^m q^{n-a}$ possibilities for ν with $|\nu(f)| = b$, as claimed. □

We define the *deficiency* of a character of G or of the associated $\nu\colon \mathcal{F} \to \mathcal{P}$ to be the maximum of $\deg(f)(|\nu(f)|-1)$ over all $f \in \mathcal{F}$. Together, Lemma 6 and (15) imply that for all $\varepsilon > 0$ there exists an N such that for all n and q, the proportion of irreducible characters of $\mathrm{GL}(n,q)$ with deficiency $< N$ is at least $1-\varepsilon$.

Lemma 7. *Let m be a positive integer and ℓ a prime such that $\ell m > n$ and $\mathrm{ord}_\ell P_m(q) = e > 0$. Let χ be a character whose deficiency is less than $m/2$. Then*

$$\begin{aligned}\mathrm{ord}_\ell d_\chi &= e\lfloor n/m \rfloor - e|\{f \in \operatorname{supp}\nu \mid \deg(f) \in m\mathbb{Z}\}| \\ &= \mathrm{ord}_\ell |G| - e|\{f \in \operatorname{supp}\nu \mid \deg(f) \in m\mathbb{Z}\}|.\end{aligned}$$

Proof. If f is in the support of ν and $\deg(f)|\nu(f)| < m$, then by part (iv) of Lemma 5, f does not contribute any factor of ℓ to the denominator of (16). So we need only consider the case $\deg(f)|\nu(f)| \geq m$, in which case $\deg(f)(|\nu(f)|-1) \geq m/2$ if $|\nu(f)| \geq 2$. Since the deficiency of χ is less than $m/2$, this is impossible, which means that all f contributing factors of ℓ in (16) satisfy $\nu(f) = (1)$. Moreover, by Lemma 5, ℓ divides $q^k - 1$ if and only if m divides k, in which case $\mathrm{ord}_\ell(q^k-1) = e$. Thus, the factors in (16) contributing to ord_ℓ are $q^m - 1, q^{2m} - 1, \ldots, q^{\lfloor n/m \rfloor m} - 1$, each of which contributes e, and $q^{\deg(f)} - 1$ for each $f \in \operatorname{supp}\nu$ of degree divisible by m, again each contributing e. □

Lemma 8. *For any positive integer m, the number of $\nu\colon \mathcal{F} \to \mathcal{P}$ of degree n for which there exist $f \in \mathcal{F}$ of degree m with $\nu(f) = (1)$ is less than q^n/m.*

Proof. Any degree m element of $\mathcal{F}$ splits completely in $\mathbb{F}_{q^m}$, so there are less than q^m/m such elements. For each f, there is a bijective correspondence between ν of degree n with $\nu(f) = (1)$ and ν' of degree $n-m$ with $\nu'(f) = \emptyset$. By (15), there are at most q^{n-m} such ν', so the total number of ν is less than q^n/m. □

Lemma 9. *For all $\varepsilon > 0$, if n is sufficiently large in terms of ε, m is a sufficiently large positive integer, ℓ is a prime divisor of $P_m(q)$, and $\ell m > n$, then the probability is at least*

$$1 - \frac{2 + 2\log n - 2\log m}{m} - \varepsilon$$

that a random element χ chosen uniformly from $\mathrm{Irr}(G)$ satisfies

$$\mathrm{ord}_\ell d_\chi = \mathrm{ord}_\ell |G|. \tag{17}$$

Proof. Choose N in Lemma 6 such that $N\gamma^N < (1-\gamma)^2\varepsilon/4$. By (15), the probability that χ has deficiency $\geq N$ is less than ε. We assume $m > 2N$, so with probability greater than $1-\varepsilon$, the deficiency of a random $\chi \in \mathrm{Irr}(G)$ is less than $m/2$. By Lemma 7, this implies (17) provided that no element in the support of ν has degree a multiple of m. If $f \in \operatorname{supp}\nu$ has degree km, then the deficiency condition on ν implies $\nu(f) = (1)$. By Lemma 8, the probability that there exists an element in the support of ν of degree km is less than $2/km$, so the probability that there is an element in the support of ν with degree in $m\mathbb{Z}$ is less than

$$\sum_{k=1}^{\lfloor n/m \rfloor} \frac{2}{km} < \frac{2 + 2\log n - 2\log m}{m}.$$

□

Lemma 10. *For all $\delta > 0$, if n is sufficiently large in terms of δ, $m \geq \sqrt{n}$, and ℓ is any prime divisor of $P_m(q)$, then the probability of (17) is greater than $1 - \delta/2$.*

Proof. By part (i) of Lemma 5, $\ell > m$, so $\ell m > n$. Applying Lemma 9 for $\varepsilon = \delta/4$, the claim holds if

$$\frac{2 + 2\log n - 2\log m}{m} < \frac{\delta}{4}.$$

For $n \geq 8$ and $m \geq \sqrt{n}$, the left-hand side is less than $2n^{-1/2}\log n$, which goes to zero as n goes to ∞. □

7. Proof of Lemma B

Let Fact f denote the total number of factors in the decomposition of $f(x) \in \mathbb{F}_q[x]$ into irreducibles. For each $g \in \mathrm{GL}(n,q)$, let $p_g(x)$ denote the characteristic polynomial of g.

Lemma 11. *There exist constants A and B such that for all m, n, and q, at most $An^B q^{-m}|\mathrm{GL}(n,q)|$ elements of $\mathrm{GL}(n,q)$ have a characteristic polynomial with a repeated irreducible factor of degree $\geq m$.*

Proof. By [4, Proposition 3.3], the number of elements of $\mathrm{GL}(n,q)$ with any given characteristic polynomial is at most $(A/8)n^B q^{n^2-n}$ for some absolute constants A and B. (Actually, the statement is proven only for "classical" groups, but the proof for $\mathrm{GL}(n,q)$ is identical.) For any given f of degree m, there are q^{n-2m} polynomials of degree $\leq n$ divisible by f^2, so there are less than q^{n-m} polynomials of degree n with a repeated irreducible factor of degree m and less than $q^{n-m} + q^{n-m-1} + \cdots < 2q^{n-m}$ polynomials with a repeated irreducible factor of degree $\geq m$. On the other hand, by the same argument as (14),

$$|\mathrm{GL}(n,q)| = \prod_{i=1}^{n}(q^n - q^i) > \frac{q^{n^2}}{4}.$$

The lemma follows. □

Proof of Lemma B. By [4, Proposition 3.4], for all $\delta > 0$ there exists k such that

$$\mathbf{P}[\mathrm{Fact}\, p_g > k\log n] < \frac{\delta}{4}, \tag{18}$$

where $\mathbf{P}$ denotes probability with respect to the uniform distribution on $G = \mathrm{GL}(n,q)$. (Actually, the cited reference proves the analogous claim for $\mathrm{SL}(n,q)$, but the proof goes through the $\mathrm{GL}(n,q)$ case.) Choose k so that this holds and assume that n is large enough that

(a) $\sqrt{n} > k\log n$,
(b) $An^B 2^{-\sqrt{n}} < \frac{\delta}{4}$, where A and B are defined as in Lemma 11,
(c) $\sqrt{m/2} > \log_2 m + 2$ for all $m \geq \sqrt{n}$,
(d) $m > 1/\varepsilon$ for all $m \geq \sqrt{n}$.

Let $\mathcal{X}$ denote the set of elements g for which $p_g(x)$ has $\leq k\log n$ irreducible factors and no repeated factor of degree $\geq \sqrt{n}$. By condition (a) on n, every p_g with $g \in \mathcal{X}$ has a simple irreducible factor of degree $\geq \sqrt{n}$. By equation (18) and condition (b), $|G\setminus\mathcal{X}| < (\delta/2)|G|$. For each $g \in \mathcal{X}$, fix an irreducible factor of degree $m_g \geq \sqrt{n}$ of p_g. By condition (c) and part (iii) of Lemma 5, $P_{m_g}(q) > 1$, so for each g, we may fix a prime divisor ℓ_g of $P_{m_g}(q)$. We define $\mathcal{R}$ to consist of all pairs (χ, g) where $g \notin \mathcal{X}$ or where $g \in \mathcal{X}$ but

$$\mathrm{ord}_{\ell_g} d_\chi \neq \mathrm{ord}_{\ell_g}|G|.$$

By Lemma 10, for each $g \in \mathcal{X}$, there are at most $(\delta/2)|\mathrm{Irr}(G)|$ pairs $(\chi, g) \in \mathcal{R}$. Thus, $\mathcal{R}$ satisfies equation (5).

For pairs $(\chi, g) \notin \mathcal{R}$, we have $g \in \mathcal{X}$ and $\mathrm{ord}_{\ell_g} d_\chi = \mathrm{ord}_{\ell_g}|G|$. As $p_g(x)$ has an irreducible factor of degree m_g which occurs with multiplicity 1, the centralizer of g has order divisible by $q^{m_g} - 1$ and therefore by ℓ_g. Therefore, $\mathrm{ord}_{\ell_g} s_g < \mathrm{ord}_{\ell_g}|G|$. This implies that ℓ_g is a divisor of the denominator of $(d_\chi, s_g)/d_\chi$. As $\ell_g \equiv 1 \pmod{m_g}$, we have $\ell_g > m_g$. By condition (d) on n, $m_g \geq 1/\varepsilon$. Thus, equation (4) holds. □

References

1. J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364** (2012) 3023–3070.
2. P. X. Gallagher, Degrees, class sizes and divisors of character values. *J. Group Theory* **15** (2012) 455–467.
3. J. A. Green, The characters of the finite general linear groups. *Trans. Amer. Math. Soc.* **80** (1955) 402–447.
4. M. Larsen and A. Shalev, On the distribution of values of certain word maps. *Trans. Amer. Math. Soc.* **368** (2016) 1647–1661.
5. A. R. Miller, The probability that a character value is zero for the symmetric group. *Math. Z.* **277** (2014) 1011–1015.
6. J-P. Serre, Linear representations of finite groups. Translated from the second French edition by Leonard L. Scott. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977.

Department of Mathematics, Columbia University, New York, NY, USA
Email address: pxg@math.columbia.edu

Department of Mathematics, Indiana University, Bloomington, IN, USA
Email address: mjlarsen@indiana.edu

Fakultät für Mathematik, Universität Wien, Vienna, Austria
Email address: alexander.r.miller@univie.ac.at