

Traces of powers of matrices over finite fields

Ofir Gorodetsky, Brad Rodgers

Abstract

Let M be a random matrix chosen according to Haar measure from the unitary group $U(n, \mathbb{C})$. Diaconis and Shahshahani proved that the traces of M, M^2, \dots, M^k converge in distribution to independent normal variables as $n \rightarrow \infty$, and Johansson proved that the rate of convergence is superexponential in n .

We prove a finite field analogue of these results. Fixing a prime power $q = p^r$, we choose a matrix M uniformly from the finite unitary group $U(n, q) \subseteq GL(n, q^2)$ and show that the traces of $\{M^i\}_{1 \leq i \leq k, p \nmid i}$ converge to independent uniform variables in \mathbb{F}_{q^2} as $n \rightarrow \infty$. Moreover we show the rate of convergence is exponential in n^2 . We also consider the closely related problem of the rate at which characteristic polynomial of M equidistributes in ‘short intervals’ of $\mathbb{F}_{q^2}[T]$. Analogous results are also proved for the general linear, special linear, symplectic and orthogonal groups over a finite field. In the two latter families we restrict to odd characteristic.

The proofs depend upon applying techniques from analytic number theory over function fields to formulas due to Fulman and others for the probability that the characteristic polynomial of a random matrix equals a given polynomial.

1 Introduction

1.1 A motivation from classical random matrix theory

The unitary group $U(n, \mathbb{C}) \subseteq GL(n, \mathbb{C})$ consists of the matrices

$$U(n, \mathbb{C}) = \{g \in GL(n, \mathbb{C}) : g\bar{g}^t = I_n\},$$

where \bar{g} is the matrix obtained by complex conjugating the entries of g . Let M be a random matrix chosen from Haar measure (of total mass 1) on $U(n, \mathbb{C})$. Fix a positive integer k and let $\{Z_j = X_j + iY_j\}_{j=1}^k$ be a sequence of independent complex normal variables with X_j, Y_j real-valued independent, mean 0 and variance $\frac{1}{2}$ normal variables. Diaconis and Shahshahani [DS94, Thm. 1] proved that as $n \rightarrow \infty$,

$$(\text{Tr}(M), \text{Tr}(M^2), \dots, \text{Tr}(M^k)) \longrightarrow (\sqrt{1}Z_1, \sqrt{2}Z_2, \dots, \sqrt{k}Z_k), \quad (1.1)$$

where the arrow indicates convergence in distribution. In their proof, Diaconis and Shahshahani used the method of moments and the representation theory of $U(n, \mathbb{C})$. They also proved similar results for the orthogonal and compact symplectic groups.

This work formed the basis for a number of works in random matrix theory, see e.g. [Rai97, Wie02, BD02, BG06].

Building further upon (1.1) and confirming a conjecture of Diaconis, Johansson [Joh97] showed that the rate of convergence is superexponential, in particular

$$\mathbb{P}(\text{Re Tr } M^k \leq x, \text{Im Tr } M^k \leq y) - \mathbb{P}(\text{Re } \sqrt{k}Z_k \leq x, \text{Im } \sqrt{k}Z_k \leq y) = O_k(e^{-c_k n \log n}),$$

where c_k is a constant that depends on k only. Again, related results are proved for the orthogonal and compact symplectic groups, with a slightly slower rate of convergence. Further work of Duits and Johansson [DJ10] and subsequently Johansson and Lambert [JL20] investigates the extent to which the convergence of $\text{Tr } M^k / \sqrt{k}$ to Z_k is uniform in k .

1.2 Equidistribution of traces

In this note we prove a finite field analogue of these results. We first define some classical groups over finite fields; see the books Artin [Art88], Dieudonné [Die71], Dickson [Dic58] and Taylor [Tay92] for a more complete introduction. Fix a prime power $q = p^r$ and let \mathbb{F}_q denote the finite field with q elements.

Let $\mathrm{GL}(n, q) := \{M \in \mathrm{Mat}(n, \mathbb{F}_q) : \det(M) \neq 0\}$ be the general linear group over \mathbb{F}_q . The finite unitary group $\mathrm{U}(n, q) \subseteq \mathrm{GL}(n, q^2)$ consists of the matrices

$$\mathrm{U}(n, q) = \{M \in \mathrm{GL}(n, q^2) : M\bar{M}^t = I_n\},$$

where \bar{M} is the matrix obtained by replacing the entries of g by their q -th powers. In positive characteristic the following phenomena occurs. If A is a square matrix over \mathbb{F}_q , then

$$\mathrm{Tr}(A^p) = \mathrm{Tr}(A)^p.$$

Thus, in our setting, if M is a random matrix chosen uniformly from a subgroup of $\mathrm{GL}(n, q)$, then $(\mathrm{Tr}(M), \mathrm{Tr}(M^2), \dots, \mathrm{Tr}(M^k))$ does not converge in distribution to a sequence of *independent* random variables once $k \geq p$. Instead, we have the following results.

Theorem 1.1. *Let $M \in \mathrm{GL}(n, q)$ be a random matrix chosen according to Haar measure. Fix a strictly increasing sequence b_1, \dots, b_k of positive integers coprime to p . Then for any sequence a_1, \dots, a_k of elements of \mathbb{F}_q , we have*

$$\left| \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\forall 1 \leq i \leq k : \mathrm{Tr}(M^{b_i}) = a_i) - q^{-k} \right| \leq q^{-\frac{n^2}{2b_k}} \left(1 + \frac{1}{q-1}\right)^n \binom{n-1+b_k}{n}. \quad (1.2)$$

Remark 1. The upper bound in (1.2) implies the more succinct upper bound of e.g. $q^{-\frac{n^2}{2b_k} + 3n}$, using $\binom{a}{b} \leq 2^a$ for $b_k \leq n$, and $q^{-\frac{n^2}{2b_k} + 3n} \geq 1$ for $b_k > n$. For small b_k this result is optimal up to constants in the exponent, as $|\mathrm{GL}(n, q)|$ grows exponentially in n^2 .

Remark 2. Theorem 1.1 shows that $\mathrm{Tr} M^b$ equidistributes as $n \rightarrow \infty$ as long as $b \leq C_q n$, where C_q is a constant which becomes larger as q increases.

Theorem 1.2. *Let $M \in \mathrm{U}(n, q)$ be a random matrix chosen according to Haar measure. Fix a strictly increasing sequence b_1, \dots, b_k of positive integers coprime to p . Then for any sequence a_1, \dots, a_k of elements from \mathbb{F}_{q^2} , we have*

$$\left| \mathbb{P}_{M \in \mathrm{U}(n, q)}(\forall 1 \leq i \leq k : \mathrm{Tr}(M^{b_i}) = a_i) - (q^2)^{-k} \right| \leq q^{-\frac{n^2}{4b_k}} q^{\frac{n}{2}} \left(1 + \frac{1}{q-1}\right)^n \binom{n-1+2b_k}{n}$$

Remark 3. More succinctly one can replace the upper bound by e.g. $q^{-\frac{n^2}{4b_k} + \frac{9}{2}n}$, analogous to Remark 1.

In Theorems 4.6, 6.22, 7.10 we prove analogous results for the traces of matrices drawn from the other finite classical groups $\mathrm{SL}(n, q)$, $\mathrm{Sp}(2n, q)$, $\mathrm{O}^+(n, q)$, $\mathrm{O}^-(n, q)$. In the symplectic and orthogonal case we restrict to odd characteristic. The more complicated even q can possibly be dealt with by methods developed by Fulman and Guranick [FG04] and Fulman, Saxl and Tiep [FST12], but we do not pursue it in the current work.

1.3 Equidistribution of characteristic polynomials

The methods we apply to prove Theorems 1.1 and 1.2 also allow us to prove a closely related result regarding the distribution of the characteristic polynomial of a random matrix within ‘short intervals’ of $\mathbb{F}_q[T]$.

Let $\mathcal{M}_q \subset \mathbb{F}_q[T]$ be the collection of monic polynomials with coefficients from \mathbb{F}_q and $\mathcal{M}_{n, q} \subset \mathcal{M}_q$ be the collection of monic polynomials of degree n . For $M \in \mathrm{GL}(n, q)$, define

$$\mathrm{CharPoly}(M) = \det(T - M),$$

so $\mathrm{CharPoly}(M) \in \mathcal{M}_{n, q}$.

For $f \in \mathcal{M}_{n, q}$ and $0 \leq h \leq n-1$ define a ‘short interval’ by

$$I(f; h) = \{g \in \mathcal{M}_q : |f - g| \leq q^h\} = \{g \in \mathcal{M}_q : \deg(f - g) \leq h\},$$

where $\deg(\cdot)$ is the degree of a polynomial, and $|\cdot| = q^{\deg(\cdot)}$ (where we set $\deg(0) = -\infty, |0| = 0$). Such a notion of a short interval is common in function field arithmetic (see e.g. [KR14, BBSR15]).

Theorem 1.3. *Let $M \in \mathrm{GL}(n, q)$ be a random matrix chosen according to Haar measure. Then for $0 \leq h < n - 1$ and for $f \in \mathcal{M}_{n, q}$,*

$$\left| \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) \in I(f; h)) - \frac{q^{h+1}}{q^n} \right| \leq q^{-\frac{n^2}{2(n-h-1)}} \left(1 + \frac{1}{q-1}\right)^n \binom{2n-h-2}{n}. \quad (1.3)$$

Remark 4. $|\mathcal{M}_{n, q}| = q^n$ and for $\deg(f) = n > h$, $|I(f; h)| = q^{h+1}$ so $|I(f; h)|/|\mathcal{M}_{n, q}| = q^{h+1}/q^n$. That is to say, Theorem 1.3 is a discrepancy bound for the equidistribution of $\mathrm{CharPoly}(M)$ in its possible range.

In Theorems 4.5, 6.21, 7.9 we prove analogous theorems for the characteristic polynomials of matrices drawn from other finite classical groups $\mathrm{SL}(n, q)$, $\mathrm{Sp}(2n, q)$, $\mathrm{O}^+(n, q)$, $\mathrm{O}^-(n, q)$.

Note that Theorem 1.3 implies a fast rate of equidistribution when h is of order n . But it does not necessarily say anything non-trivial for small h . In fact, it may be seen using a different method that equidistribution persists for short intervals of a much smaller size, though at a slower rate.

Theorem 1.4. *Let $M \in \mathrm{GL}(n, q)$ be a random matrix chosen according to Haar measure. Then for $0 \leq h < n - 1$ and $f \in \mathcal{M}_{n, q}$,*

$$\left| \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) \in I(f; h)) - \frac{q^{h+1}}{q^n} \right| \leq \frac{n-h}{q^n}. \quad (1.4)$$

Remark 5. Hence the characteristic polynomial equidistributes as long as $h/\log_q(n) \rightarrow \infty$, since in this case $(n-h)/q^n = o(q^{h+1}/q^n)$. It may be possible to show that equidistribution does not occur at some smaller scales of h , but we have not pursued this.

In Theorems 4.8, 6.24, 7.12 we prove analogous theorems for the characteristic polynomials of matrices drawn from other finite classical groups $\mathrm{SL}(n, q)$, $\mathrm{Sp}(2n, q)$, $\mathrm{O}^+(n, q)$, $\mathrm{O}^-(n, q)$. In summary we show that in ‘large’ short intervals the characteristic polynomial equidistributes superexponentially and for smaller short intervals the characteristic polynomial equidistributes as well, unless prevented from doing so for reasons related to relatively obvious symmetries.

From Theorem 1.4 we may deduce immediately, using Lemma 2.1 below, an analogous result for traces.

Theorem 1.5. *Let $M \in \mathrm{GL}(n, q)$ be a random matrix chosen according to Haar measure. Then for $1 \leq k \leq n$ and for $\{a_i\}_{1 \leq i \leq k, p \nmid i} \subseteq \mathbb{F}_q$, we have*

$$\left| \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\forall 1 \leq i \leq k, p \nmid i : \mathrm{Tr}(M^i) = a_i) - \frac{1}{q^{k - \lfloor \frac{k}{p} \rfloor}} \right| \leq \frac{(k+1)q^{\lfloor \frac{k}{p} \rfloor}}{q^n}.$$

Here the non-trivial range is $(n-k)/\log_q(n) \rightarrow \infty$. Theorems 4.9, 5.22, 6.30, 7.17 are analogous results for the other classical compact groups.

The paper is structured so that each group is treated in a mostly independent section. A reader looking to become quickly acquainted with the main ideas is advised to focus on §3; the other groups considered have proofs that are more technical but rely on related ideas.

1.4 Related works

1.4.1 Fixed n , large q

In the ‘large finite field’ limit, namely the limit where one takes n fixed and lets q tend to infinity, one can easily obtain equidistribution of traces and characteristic polynomials as follows. By a result of Reiner and of Gerstenhaber, discussed in Theorem 3.3 below, we have

$$\mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) = f_0) = q^{-n} \left(1 + O_n\left(\frac{1}{q}\right)\right) \quad (1.5)$$

uniformly for any monic f_0 of degree n with $f_0(0) \neq 0$. In particular, by summing over f_0 in a short interval, this implies that

$$\mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) \in I(f; h)) = \frac{q^{h+1}}{q^n} \left(1 + O_n\left(\frac{1}{q}\right)\right)$$

for any monic f of degree n and any $0 \leq h < n$. Using Lemma 2.1 an analogous result holds for traces. A similar argument works for other classical groups.

1.4.2 Pointwise bounds

An explicit form of (1.5) is provided by Chavdarov [Cha97, §3], who by a completely different method proved that for $f_0(0) \neq 0$,

$$\frac{(q-3)^{n^2-n}}{|\mathrm{GL}(n, q)|} \leq \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) = f_0) \leq \frac{(q+3)^{n^2-n}}{|\mathrm{GL}(n, q)|}$$

for $q > 4$. A similar result is proved for the symplectic group. Chavdarov was after a large- q result. However, for fixed q and growing n one can do better. Examining Theorem 3.3, one sees that if f_0 factorizes as $\prod_{i=1}^r P_i^{e_i}$ then

$$q^n \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) = f_0) = \prod_{i=1}^r \prod_{j=1}^{e_i} (1 - q^{-m_i j})^{-1}.$$

An immediate consequence is a lower bound $q^n \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) = f_0) \geq 1$. This is in fact tight, as may be seen by taking f_0 to be a prime polynomial of growing degree. As for an upper bound, our proof of Theorem 1.4 in fact works as is for $h = -1$, in which case $I(f_0; h) = \{f_0\}$ is a singleton and one obtains

$$q^n \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) = f_0) \leq n + 2$$

whenever $f_0(0) \neq 0$. With more work one should be able to show that the correct upper bound is logarithmic in n , though we do not prove this here. This is obtained for instance by taking $f_0 = \prod_{\deg P \leq m} P^{\lfloor m/\deg(P) \rfloor}$, where the product is over prime polynomials of degree up to m .

1.4.3 Exponential sums over matrices

Let χ be a (possibly trivial) multiplicative character of \mathbb{F}_q^\times and ψ a non-trivial additive character of \mathbb{F}_q . Eichler [Eic38] and later Lamprecht [Lam57] evaluated the generalized Gauss sum

$$\sum_{g \in G} \chi(\det(g)) \psi(\mathrm{Tr}(g)) \quad (1.6)$$

for $G = \mathrm{GL}(n, q)$, in terms of the ordinary Gauss sum. In a series of works, Kim [Kim97a, Kim97b, Kim97c, Kim98a, Kim98b, Kim98c], Kim and Lee [KL96] and Kim and Park [KP97] studied (1.6) for other classical groups G , and in the case of $G = \mathrm{GL}(n, q)$ also evaluated the generalized Kloosterman sum [Kim98b, Thm. C]

$$\sum_{g \in G} \psi(\mathrm{Tr}(ag + bg^{-1})), \quad (a, b \in \mathbb{F}_q^\times). \quad (1.7)$$

Their methods relied on a variant of Bruhat decomposition. In [CK03] and [CK08] Chae and Kim used ℓ -adic cohomology and Deligne-Lusztig theory, respectively, to obtain new proofs for these formulas.

In the course of proving our superexponential results, we end up evaluating exponential sums over the various classical groups which are more general than (1.6) and (1.7), see e.g. Theorems 3.6 and 5.15 below. Our evaluation is in terms of zeros of certain L -functions associated with each classical group. Additionally we provide bounds on these sums. These results may be of independent interest, in view of recent applications of the works of Kim et al. [CFHS12, CDSS17, PG18, PG19]. Our proofs differ substantially from those just mentioned, and in particular do not involve the theory of reductive groups.

1.4.4 Cohen-Lenstra heuristics

In our approach we will study $P_{GL}(f) = \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) = f)$ as an arithmetic function over $\mathbb{F}_q[T]$ (see Definition 3.2 below). As it ends up the Dirichlet series for $P_{GL}(f)$ bear a certain formal resemblance to Dirichlet series which have previously been investigated by Cohen and Lenstra.

Indeed, let A be the ring of integers of a number field, e.g. $A = \mathbb{Z}$. The norm of an ideal $\mathfrak{a} \subseteq A$ is defined as $\mathrm{Nm}(\mathfrak{a}) = |A/\mathfrak{a}|$. If G is a finite A -module, let $w_A(G) = |\mathrm{Aut}(G)|^{-1}$, where $\mathrm{Aut}(G)$ is the group of A -homomorphisms of G . With any such G , we associate an ideal of A by the following process: G is necessarily isomorphic to a direct sum $\oplus_i A/\mathfrak{a}_i$ of cyclic submodules, and we set $I(G) := \prod_i \mathfrak{a}_i$; this ideal does not depend on the specific decomposition into cyclic submodules. With this notion in hand, we extend w_A to ideals of A as follows:

$$w_A(\mathfrak{a}) = \sum_{\substack{G \text{ up to } A\text{-isomorphism} \\ I(G) = \mathfrak{a}}} w_A(G).$$

Cohen and Lenstra define the Dirichlet series $\zeta_{\infty,A}(s) = \sum_{\mathfrak{a}} w_A(\mathfrak{a}) \text{Nm}(\mathfrak{a})^{-s}$, converging for $\text{Re } s > 0$, where the sum is over non-zero ideals of A . They prove that

$$\zeta_{\infty,A}(s) = \prod_{j \geq 1} \zeta_A(s+j),$$

where ζ_A is the Dedekind zeta function of A [CL84, Cor. 3.7] and study the analytic properties of $\zeta_{\infty,A}$ in [CL84, §7].

As it turns out, the arithmetic function $P_{GL}(f)$ and analogous functions for other classical groups resemble function-field analogues of $w_A(\mathfrak{a})$. In particular, for any Dirichlet character $\chi: \mathbb{F}_q[T] \rightarrow \mathbb{C}$, the Dirichlet series $\sum_{f \in \mathbb{F}_q[T], \text{monic}} P_{GL}(f) \chi(f) |f|^{-s}$ behaves similarly to $\zeta_{\infty,A}(s)$ in that we have the factorization

$$\sum_f \frac{P_{GL}(f) \chi(f)}{|f|^s} = \prod_{j \geq 1} L_{GL}(q^{-s-j}, \chi)$$

where $L_{GL}(u, \chi)$ is related to the L -function of χ , see Theorem 3.5 below. Although Cohen-Lenstra heuristics in the context of matrices over rings were studied extensively in the literature, see e.g. [FW89, CH18, Woo19], the formal connection which we note here seems to be new and we do not know if there is a deeper reason for it.

1.4.5 Trace as a fixed-point count

There is another perspective which leads to a different finite field analogue for results about the traces of random matrices. Given a permutation π on n elements, we may consider its permutation matrix P_π . The trace of P_π counts the fixed points of π . Sampling π uniformly from the symmetric groups S_n and letting n tend to infinity, $\text{Tr}(P_\pi)$ is known to tend to a Poisson distribution with parameter 1, see e.g. the discussion in [DS94, §5]. One can similarly study the number of vectors fixed by a random matrix from $\text{GL}(n, q)$ as n tends to infinity. This was studied for $\text{GL}(n, q)$ and the various finite classical groups by Rudvalis and Shinoda [RS88], who obtained formulas for the probability that the fixed space of a random matrix has a given dimension. Recently, Fulman and Stanton [FS16] computed the limit of the moments of the number of fixed vectors as n tends to infinity, as well as simplified and unified the results of Rudvalis and Shinoda.

Acknowledgments

For discussions related to this paper we thank Gilyoung Cheong, Jason Fulman, Valeriya Kovaleva and Will Sawin. We thank the anonymous referee for their suggestions and corrections. The first author was supported by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreements n° 320755 and 786758. The second author was partly supported by the US NSF grant DMS-1701577 and an NSERC grant. Work for this paper was done during visits to the University of Michigan, Tel Aviv University, and the Centre de Recherches Mathématiques and we thank these institutions for their hospitality.

2 Preliminary background

2.1 Hayes characters

Here we review a generalization of Dirichlet characters which were introduced by Hayes [Hay65]. Other papers with a review similar to what we give below include [Gor20, GS20].

2.1.1 Equivalence relation

Let ℓ be a non-negative integer and H be a non-zero polynomial in $\mathbb{F}_q[T]$. We define an equivalence relation $R_{\ell,H,q}$ on \mathcal{M}_q by saying that $A \equiv B \pmod{R_{\ell,H,q}}$ if and only if A and B have the same first ℓ next-to-leading coefficients and $A \equiv B \pmod{H}$. (We do not require that A and B have the same degree. For instance $T^3 + T + 1 \equiv T^5 + T^3 + T^2 + 1 \pmod{R_{2,T,q}}$ for any q .) We adopt the following convention throughout: the j -th next-to-leading coefficient of a polynomial $f(T) \in \mathcal{M}_q$ with $j > \deg(f)$ is considered to be 0. It may be verified that there is a well-defined quotient monoid $\mathcal{M}_q / R_{\ell,H,q}$, where multiplication is the usual polynomial multiplication. An element of \mathcal{M}_q is invertible modulo $R_{\ell,H,q}$ if and only if it is

coprime to H . The units of $\mathcal{M}_q/R_{\ell,H,q}$ form an abelian group, having as identity element the equivalence class of the polynomial 1. We denote this unit group by $(\mathcal{M}_q/R_{\ell,H,q})^\times$. It may be verified that

$$|(\mathcal{M}_q/R_{\ell,H,q})^\times| = q^\ell \phi(H),$$

where $\phi(H)$ is Euler's totient function.

2.1.2 Characters

For every character χ of the finite abelian group $(\mathcal{M}_q/R_{\ell,H,q})^\times$, we define χ^\dagger with domain \mathcal{M}_q as follows. If A is invertible modulo $R_{\ell,H,q}$ and if \mathfrak{c} is the equivalence class of A , then $\chi^\dagger(A) = \chi(\mathfrak{c})$. If A is not invertible, then $\chi^\dagger(A) = 0$.

The set of functions χ^\dagger defined in this way are called the characters of the relation $R_{\ell,H,q}$, or sometimes "characters modulo $R_{\ell,H,q}$ ". We abuse language somewhat and write χ instead of χ^\dagger to indicate a character of the relation $R_{\ell,H,q}$ derived from the character χ of the group $(\mathcal{M}_q/R_{\ell,H,q})^\times$. Thus we write χ_0 for the character of $R_{\ell,H,q}$ which has the value 1 when A is invertible and the value 0 otherwise. We denote by $G(R_{\ell,H,q})$ the set $\{\chi^\dagger : \chi \text{ a character of } (\mathcal{M}_q/R_{\ell,H,q})^\times\}$.

A set of polynomials in \mathcal{M}_q is called a representative set modulo $R_{\ell,H,q}$ if the set contains one and only one polynomial from each equivalence class of $R_{\ell,H,q}$. If $\chi_1, \chi_2 \in G(R_{\ell,H,q})$, then

$$\frac{1}{q^\ell \phi(H)} \sum_F \chi_1(F) \overline{\chi_2(F)} = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2, \\ 1 & \text{if } \chi_1 = \chi_2, \end{cases} \quad (2.1)$$

where in this sum F runs through a representative set modulo $R_{\ell,H,q}$. If $n \geq \ell + \deg(H)$, then $\mathcal{M}_{n,q}$ is a disjoint union of $q^{n-\ell-\deg(H)}$ representative sets, and a set of polynomials on which $\chi \in G(R_{\ell,H,q})$ vanishes. Thus, applying (2.1) with $\chi_2 = \chi_0$, we obtain that for all $n \geq \ell + \deg(H)$:

$$\frac{1}{q^{n-\deg(H)} \phi(H)} \sum_{F \in \mathcal{M}_{n,q}} \chi(F) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ 1 & \text{if } \chi = \chi_0. \end{cases} \quad (2.2)$$

We also have, if $A, B \in \mathcal{M}_q$ are coprime to H ,

$$\frac{1}{q^\ell \phi(H)} \sum_{\chi \in G(R_{\ell,H,q})} \chi(A) \overline{\chi(B)} = \begin{cases} 1 & \text{if } A \equiv B \pmod{R_{\ell,H,q}}, \\ 0 & \text{otherwise.} \end{cases} \quad (2.3)$$

If $\chi \in G(R_{\ell,1,q})$ we say that χ is a *short interval character of ℓ coefficients*, and if $\chi \in G(R_{0,H,q})$ we say that χ is a *Dirichlet character modulo H* . Every element of $G(R_{\ell,H,q})$ is a product of an element from $G(R_{\ell,1,q})$ with an element from $G(R_{0,H,q})$.

2.1.3 L-Functions

Let $\chi \in G(R_{\ell,H,q})$. The L -function of χ is the following series in u :

$$L(u, \chi) = \sum_{f \in \mathcal{M}_q} \chi(f) u^{\deg(f)},$$

which also admits the Euler product

$$L(u, \chi) = \prod_P (1 - \chi(P) u^{\deg(P)})^{-1} \quad (2.4)$$

where the product is over irreducibles in \mathcal{M}_q . If χ is the trivial character χ_0 of $G(R_{\ell,H,q})$, then

$$L(u, \chi) = \frac{\prod_{P|H} (1 - u^{\deg(P)})}{1 - qu}.$$

Otherwise, the orthogonality relation (2.2) implies that $L(u, \chi)$ is a polynomial in u of degree at most $\ell + \deg(H) - 1$.

The first one to realize that Weil's proof of the Riemann Hypothesis for Function Fields [Wei74, Thm. 6, p. 134] implies the Riemann Hypothesis for the L -functions of $\chi \in G(R_{\ell,H,q})$ was Rhin [Rhi72,

Thm. 3] in his thesis (cf. [EH91, Thm. 5.6] and the discussion following it). Hence we know that if we factorize $L(u, \chi)$ as

$$L(u, \chi) = \prod_{i=1}^{\deg(L(u, \chi))} (1 - \gamma_i(\chi)u),$$

then for any i ,

$$|\gamma_i(\chi)| \in \{1, \sqrt{q}\}. \quad (2.5)$$

Remark 6. Although we use below the Riemann Hypothesis for Function Fields (in the form (2.5)) whenever we can, the trivial bound $|\gamma_i(\chi)| \leq q$ leads to results only slightly weaker than we obtain.

2.2 Traces of powers, and symmetric functions

Lemma 2.1. *Fix $n \geq k \geq 1$. Let $\{a_i\}_{1 \leq i \leq k, p \nmid i}$ be a sequence of $k' = k - \lfloor \frac{k}{p} \rfloor$ elements from \mathbb{F}_q . There are polynomials $\{f_i\}_{1 \leq i \leq q^{\lfloor \frac{k}{p} \rfloor}} \subseteq \mathcal{M}_{n, q}$ such that for $M \in \text{Mat}(n, \mathbb{F}_q)$, the following two conditions are equivalent:*

1. *For all $1 \leq i \leq k$ with $p \nmid i$, we have $\text{Tr}(M^i) = a_i$.*
2. *For some $1 \leq j \leq q^{\lfloor \frac{k}{p} \rfloor}$ we have $\text{CharPoly}(M) \in I(f_j; n - k - 1)$.*

Moreover, the sets $\{I(f_j; n - k - 1)\}_{1 \leq j \leq q^{\lfloor \frac{k}{p} \rfloor}}$ are disjoint, so that

$$\mathbb{P}_{M \in S}(\forall 1 \leq i \leq k, p \nmid i : \text{Tr}(M^i) = a_i) = \sum_{j=1}^{q^{\lfloor \frac{k}{p} \rfloor}} \mathbb{P}_{M \in S}(\text{CharPoly}(M) \in I(f_j; n - k - 1))$$

for any non-empty subset $S \subseteq \text{GL}(n, q)$, endowed with a uniform probability measure.

Proof. For $M \in \text{Mat}(n, \mathbb{F}_q)$, write its characteristic polynomial as

$$\text{CharPoly}(M) = T^n + c_1(M)T^{n-1} + \dots + c_n(M).$$

As $\text{Tr}(M^i)$ are the power sum symmetric polynomials in the eigenvalues of M (working in the closure of \mathbb{F}_q), and $(-1)^i c_i(M)$ are the elementary symmetric functions in the eigenvalues of M , Newton's identities allow us to express $\text{Tr}(M^i)$ as

$$\text{Tr}(M^i) = -ic_i(M) + P_i(c_1(M), \dots, c_{i-1}(M)) \quad (2.6)$$

for some explicit $P_i(x_1, \dots, x_{i-1}) \in \mathbb{Z}[x_1, \dots, x_{i-1}]$.

If $c_p(M), c_{2p}(M), \dots, c_{p^{\lfloor \frac{k}{p} \rfloor}}(M)$ are fixed, then prescribing $\text{Tr}(M^i) = a_i$ for $1 \leq i \leq k$, $p \nmid i$, amounts to prescribing $c_i(M)$ for $1 \leq i \leq k$, $p \nmid i$. This is because for each such i we may iteratively use (2.6) to solve for $c_i(M)$ from $\text{Tr}(M^i)$ and the previous coefficients $c_j(M)$. This works in the other direction as well: we may use (2.6) to solve for $\text{Tr}(M^i)$ from $c_i(M)$ and the previous coefficients $c_j(M)$.

We wish to formulate this observation using short intervals. If $f \in \mathcal{M}_{n, q}$ and $h < n$, then $\text{CharPoly}(M) \in I(f; h)$ if and only if $c_1(M), \dots, c_{n-h-1}(M)$ coincide the first $n - h - 1$ next-to-leading coefficients of f . Thus, if $\{c_{pi}(M)\}_{1 \leq i \leq \lfloor k/p \rfloor}$ are fixed, then the set of matrices M in $\text{Mat}(n, \mathbb{F}_q)$ with $\text{Tr}(M^i) = a_i$ for $1 \leq i \leq k$, $p \nmid i$ is of the form $I(f; n - k - 1)$, where $f \in \mathcal{M}_{n, q}$ is determined by $\{c_{pi}(M)\}_{1 \leq i \leq \lfloor k/p \rfloor}$ and the values a_i . As we vary $\{c_{pi}(M)\}_{1 \leq i \leq \lfloor k/p \rfloor}$, this f necessarily changes as well.

All in all, we find that indeed the set of matrices M in $\text{Mat}(n, \mathbb{F}_q)$ with $\text{Tr}(M^i) = a_i$ for $1 \leq i \leq k$, $p \nmid i$ is a disjoint union of sets of the form $I(f; n - k - 1)$, for $q^{\lfloor \frac{k}{p} \rfloor}$ different polynomials f in $\mathcal{M}_{n, q}$. \square

Remark 7. Lemma 2.1 gives Theorem 1.5 from Theorem 1.4. The lemma can also be used to deduce a (weaker) version of Theorem 1.1 from Theorem 1.3. In fact for the purpose of Theorem 1.1, Lemma 2.2 gives a slightly better estimate.

Given $\lambda_1, \dots, \lambda_k \in \mathbb{F}_q$, define a function $\chi_\lambda: \mathcal{M}_q \rightarrow \mathbb{C}$ by

$$\chi_\lambda(f(T)) = e^{\frac{2\pi i}{p} \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\sum_{i=1}^k \lambda_i(\alpha_1^i + \dots + \alpha_d^i))},$$

where $f \in \mathcal{M}_q$ and $\{\alpha_i\}_{i=1}^d$ are the roots of f in $\overline{\mathbb{F}_q}$, listed with multiplicities.

Lemma 2.2. *Let k be a positive integer coprime to p . Let $\lambda_1, \dots, \lambda_k \in \mathbb{F}_q$ with $\lambda_k \neq 0$. The following hold.*

1. The function $\chi_{\bar{\lambda}}$ is completely multiplicative, that is, $\chi_{\bar{\lambda}}(fg) = \chi_{\bar{\lambda}}(f)\chi_{\bar{\lambda}}(g)$ for all $f, g \in \mathcal{M}_q$.
2. Given $M \in \text{GL}(n, q)$, we have $\chi_{\bar{\lambda}}(\text{CharPoly}(M)) = e^{\frac{2\pi i}{p} \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\sum_{i=1}^k \lambda_i \text{Tr}(M^i))}$.
3. The function $\chi_{\bar{\lambda}}$ is a short interval character of k coefficients.
4. The character $\chi_{\bar{\lambda}}$ is non-trivial.

Proof. The first part is trivial. The second part follows from the observation that $\text{Tr}(M^i)$ is the sum of the i -th powers of the eigenvalues of M , which are the roots of $\text{CharPoly}(M)$. For the third part, we need to show that $\alpha_1^i + \dots + \alpha_d^i$ is a function of the first i next-to-leading coefficients of f , for each i . This is a direct consequence of the fundamental theorem of symmetric polynomials, which in particular says that $\alpha_1^i + \dots + \alpha_d^i$ is a polynomial (with integer coefficients) in the first i elementary symmetric polynomials in α_i , which – up to sign – are the first i next-to-leading coefficients of $f(T)$. For the last part, we use Newton's identities which say in particular that

$$\sum_{i=1}^d \alpha_i^k = F(e_1(\alpha_i), e_2(\alpha_i), \dots, e_{k-1}(\alpha_i)) + (-1)^{k-1} k e_k(\alpha_i),$$

where e_i is the i -th elementary symmetric polynomial and F is some polynomial with integer coefficients, which assumes the value 0 at $\bar{0}$. As $k \neq 0$ in \mathbb{F}_q by assumption, this shows that $\chi_{\bar{\lambda}}(T^k + c)$ is not equal to 1 whenever $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c) \neq 0$. \square

2.3 A uniqueness theorem

We will make use of the following simple result.

Lemma 2.3. *Two functions $\alpha, \beta: \mathcal{M}_q \rightarrow \mathbb{C}$ are identical (that is $\alpha(g) = \beta(g)$ for all $g \in \mathcal{M}_q$) if and only if for all Hayes characters $\chi: \mathcal{M}_q \rightarrow \mathbb{C}$,*

$$\sum_{f \in \mathcal{M}_q} \alpha(f) \chi(f) u^{\deg(f)} = \sum_{f \in \mathcal{M}_q} \beta(f) \chi(f) u^{\deg(f)}, \quad (2.7)$$

with equality in the sense of formal power series in u .

Remark 8. The formal power series in (2.7) are well-defined; note that the sums $c_n(\alpha, \chi) = \sum_{f \in \mathcal{M}_{n,q}} \alpha(f) \chi(f)$ are finite for all n, q , and $\sum_{f \in \mathcal{M}_q} \alpha(f) \chi(f) u^{\deg(f)} = \sum_{n \geq 0} c_n(\alpha, \chi) u^n$.

Proof. If α, β are identical then (2.7) is evident. On the other hand, suppose (2.7) holds for all Hayes characters χ . For any $n \geq 0$ and $g \in \mathcal{M}_{n,q}$, take $\ell > n$. Supposing (2.7) holds, one has for all $\chi \in G(R_{\ell,1,q})$ (that is, short interval characters of ℓ coefficients),

$$\sum_{f \in \mathcal{M}_{n,q}} \alpha(f) \chi(f) = \sum_{f \in \mathcal{M}_{n,q}} \beta(f) \chi(f).$$

Hence from (2.3)

$$\alpha(g) = \frac{1}{q^\ell} \sum_{\chi \in G(R_{\ell,1,q})} \chi(g) \sum_{f \in \mathcal{M}_{n,q}} \alpha(f) \bar{\chi}(f) = \frac{1}{q^\ell} \sum_{\chi \in G(R_{\ell,1,q})} \chi(g) \sum_{f \in \mathcal{M}_{n,q}} \beta(f) \bar{\chi}(f) = \beta(g).$$

Since g was arbitrary, this proves α and β are identical. \square

2.4 Some q -series identities

We make use of the following results from the theory of q -series, with the notation

$$(a; \nu)_n = (1-a)(1-a\nu) \cdots (1-a\nu^{n-1}),$$

and for $|\nu| < 1$,

$$(a; \nu)_\infty = \lim_{n \rightarrow \infty} (a; \nu)_n.$$

Theorem 2.4 (Euler). *[GR04, Eq. (18)] For $|x|, |\nu| < 1$,*

$$\frac{1}{(x; \nu)_\infty} = \sum_{j=0}^{\infty} \frac{x^j}{(\nu; \nu)_j}.$$

As a restatement, setting $\nu = 1/V$ and $x = y/V$, we have for $|y| < |V|$ and $|V| > 1$,

$$\prod_{i=1}^{\infty} \frac{1}{1 - y/V^i} = 1 + \sum_{j=1}^{\infty} \frac{V^{j(j-1)/2}}{(V^j - 1)(V^j - V) \cdots (V^j - V^{j-1})} y^j \quad (2.8)$$

$$= 1 + \sum_{j=1}^{\infty} \frac{V^{j(j-1)/2}}{(V^j - 1)(V^{j-1} - 1) \cdots (V - 1)} y^j. \quad (2.9)$$

Theorem 2.5 (Euler). [GR04, Eq. (19)] For $|x|, |\nu| < 1$,

$$\sum_{j=0}^{\infty} \frac{(-1)^j \nu^{j(j-1)/2} x^j}{(\nu; \nu)_j} = (x; \nu)_{\infty}.$$

As a restatement, setting $\nu = 1/V$ and $x = y/V$, we have for $|y| < |V|$ and $|V| > 1$,

$$1 + \sum_{j=1}^{\infty} \frac{(-1)^j}{(V^j - 1)(V^{j-1} - 1) \cdots (V - 1)} y^j = \prod_{i=1}^{\infty} (1 - y/V^i). \quad (2.10)$$

3 Results for $\text{GL}(n, q)$

3.1 $\text{GL}(n, q)$ and the space of characteristic polynomials

Recall that $\text{GL}(n, q) = \{M \in \text{Mat}(n, \mathbb{F}_q) : \det(M) \neq 0\}$.

Proposition 3.1. [Art88, Ch. IV.3] We have $|\text{GL}(n, q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.

We define $\mathcal{M}_{n,q}^{gl} = \{f \in \mathcal{M}_{n,q} : (f, T) = 1\}$. It is plain for $M \in \text{GL}(n, q)$ that $\text{CharPoly}(M) \in \mathcal{M}_{n,q}^{gl}$, and it follows by considering companion matrices that in fact $\mathcal{M}_{n,q}^{gl} = \{\text{CharPoly}(M) : M \in \text{GL}(n, q)\}$. The reader should take a moment to verify

$$|\mathcal{M}_{n,q}^{gl}| = q^n(1 - q^{-1}), \quad n \geq 1.$$

Let $\mathcal{M}_q^{gl} = \cup_{n \geq 0} \mathcal{M}_{n,q}^{gl}$. It is easy to see that \mathcal{M}_q^{gl} is a submonoid of \mathcal{M}_q with respect to multiplication (that is, if $f, g \in \mathcal{M}_q^{gl}$, then $fg \in \mathcal{M}_q^{gl}$). Furthermore, by unique factorization of polynomials with coefficients in \mathbb{F}_q , it follows that each $f \in \mathcal{M}_q^{gl}$ factorizes uniquely as $f = P_1^{e_1} \cdots P_r^{e_r}$ with each P_i an irreducible monic polynomial and $P_i \neq T$ for all i .

3.2 Expressions for $P_{GL}(f)$

Throughout this subsection we will take random $M \in \text{GL}(n, q)$ according to Haar measure (that is, uniform measure).

Definition 3.2. For $f \in \mathcal{M}_q$, we define the arithmetic function

$$P_{GL}(f) = \mathbb{P}_{M \in \text{GL}(n, q)}(\text{CharPoly}(M) = f) = \frac{|\{M \in \text{GL}(n, q) : \text{CharPoly}(M) = f\}|}{|\text{GL}(n, q)|},$$

where we take $n = \deg(f)$. For $f = 1$ we define $P_{GL}(1) = 1$.

Previous authors have considered the counts $|\{M \in \text{GL}(n, q) : \text{CharPoly}(M) = f\}|$. A closed formula for these is due independently to Reiner [Rei61, Thm. 2] and Gerstenhaber [Ger61, Sec. 2]. Another proof based on cycle types of matrices was later given in [Ful99, Thm. 17]. We have found it natural to phrase these formulas in the language of probability as above.

Theorem 3.3 (Reiner, Gerstenhaber). If $f \in \mathcal{M}_q^{gl}$ factorizes as $f = P_1^{e_1} \cdots P_r^{e_r}$ with each P_i an irreducible monic polynomial, set $m_i = \deg(P_i)$. Then

$$P_{GL}(f) = \prod_{i=1}^r \frac{q^{m_i e_i (e_i - 1)}}{|\text{GL}(e_i, q^{m_i})|}.$$

If f is a monic polynomial but $f \notin \mathcal{M}_q^{gl}$, then $P_{GL}(f) = 0$.

We make the new observation that $P_{GL}(f)$ can also be written as an infinite Dirichlet convolution of simple arithmetic functions defined on \mathcal{M}_q .

Theorem 3.4. For $g \in \mathcal{M}_q$, define the arithmetic functions $\alpha_1^{GL}, \alpha_2^{GL}, \dots$ by

$$\alpha_i^{GL}(g) := \frac{1}{|g|^i} \mathbf{1}_{\mathcal{M}_q^{gl}}(g) = \begin{cases} 1/|g|^i & \text{for } g \in \mathcal{M}_{n,q}^{gl}, \\ 0 & \text{otherwise.} \end{cases}$$

Then for $f \in \mathcal{M}_q$,

$$P_{GL}(f) = \lim_{k \rightarrow \infty} (\alpha_1^{GL} * \alpha_2^{GL} * \dots * \alpha_k^{GL})(f).$$

The proof of Theorem 3.4 is given below. It is a corollary of the following theorem.

Theorem 3.5. For a Hayes character χ and $|u| < 1/q$, define

$$L_{GL}(u, \chi) = \sum_{f \in \mathcal{M}_q^{gl}} \chi(f) u^{\deg(f)}. \quad (3.1)$$

This sum converges absolutely for $|u| < 1/q$, and for $|u| < 1$ we have

$$\sum_{f \in \mathcal{M}_q} P_{GL}(f) \chi(f) u^{\deg(f)} = \prod_{i=1}^{\infty} L_{GL}\left(\frac{u}{q^i}, \chi\right), \quad (3.2)$$

with both the left hand sum and the right hand product converging absolutely.

Proof. We treat claims about convergence first. For (3.1), note that $\sum_{f \in \mathcal{M}_{n,q}^{gl}} |\chi(f)| \leq q^n$, which furthermore implies $|L(u, \chi)| \leq 1/(1 - q|u|)$. For the left hand side of (3.2), note that $\sum_{f \in \mathcal{M}_{n,q}} |P_{GL}(f)| \leq 1$, and for the right hand side note that $|L_{GL}(u/q^i, \chi)| \leq 1/(1 - |u|/q^{i-1})$.

We will make use of the Euler product:

$$\begin{aligned} L_{GL}(u, \chi) &= \sum_{f \in \mathcal{M}_q^{gl}} \chi(f) u^{\deg(f)} \\ &= \prod_{P \neq T} \frac{1}{1 - \chi(P) u^{\deg(P)}}, \end{aligned} \quad (3.3)$$

where the product is over all irreducible monic polynomials P in \mathcal{M}_q with $P \neq T$. As $|\{P \in \mathcal{M}_{n,q} : P \text{ irreducible}\}| \leq |\mathcal{M}_{n,q}| \leq q^n$, the reader may verify that the product in (3.3) converges for $|u| < 1/q$. As $|P| = q^{\deg(P)}$, we have

$$L_{GL}\left(\frac{u}{q^i}, \chi\right) = \prod_{P \neq T} \frac{1}{1 - \chi(P) u^{\deg(P)} / |P|^i}.$$

From Theorem 3.3, one sees that P_{GL} is a multiplicative arithmetic function on \mathcal{M}_q , with

$$P_{GL}(P^e) = \frac{|P|^{e(e-1)}}{(|P|^e - 1)(|P|^e - |P|) \dots (|P|^e - |P|^{e-1})},$$

for P an irreducible monic polynomial with $P \neq T$. Hence

$$\begin{aligned} \sum_{f \in \mathcal{M}_q} P_{GL}(f) \chi(f) u^{\deg(f)} &= \prod_{P \neq T} \left(1 + \sum_{e=1}^{\infty} \frac{|P|^{e(e-1)}}{(|P|^e - 1)(|P|^e - |P|) \dots (|P|^e - |P|^{e-1})} (\chi(P) u^{\deg(P)})^e \right) \\ &= \prod_{P \neq T} \prod_{i=1}^{\infty} \frac{1}{1 - \chi(P) u^{\deg(P)} / |P|^i} = \prod_{i=1}^{\infty} L_{GL}\left(\frac{u}{q^i}, \chi\right), \end{aligned}$$

using (2.8) to pass to the second line. The order of products in the final line may be swapped owing to absolute convergence (justified using the same facts as for the absolute convergence of (3.3)). \square

Proof of Theorem 3.4. Theorem 3.5 implies for $|u| < 1$,

$$\begin{aligned} \sum_{f \in \mathcal{M}_q} P_{GL}(f) \chi(f) u^{\deg(f)} &= \lim_{k \rightarrow \infty} \prod_{i=1}^k \sum_{g \in \mathcal{M}_q} \alpha_i^{GL}(g) \chi(g) u^{\deg(g)} \\ &= \lim_{k \rightarrow \infty} \sum_{f \in \mathcal{M}_q} (\alpha_1^{GL} * \dots * \alpha_k^{GL})(f) \chi(f) u^{\deg(f)}. \end{aligned} \quad (3.4)$$

We claim the limit and sum can be swapped in the last line. If $|(\alpha_1^{GL} * \dots * \alpha_k^{GL})(f)| \leq 1$ for all $f \in \mathcal{M}_q$, then this follows via dominated convergence. But indeed we do have $|(\alpha_1^{GL} * \dots * \alpha_k^{GL})(f)| \leq 1$. For, set $\chi = 1$; the left hand side of (3.4) is $\sum_{n \geq 0} u^n$, while for each $f \in \mathcal{M}_q$, the quantity $(\alpha_1^{GL} * \dots * \alpha_k^{GL})(f)$ is non-decreasing in k , so comparing coefficients we have $\sum_{f \in \mathcal{M}_{n,q}} (\alpha_1^{GL} * \dots * \alpha_k^{GL})(f) \leq 1$. Since all terms in this sum are non-negative this verifies the stated bound. (Note that this also implies $\lim_{k \rightarrow \infty} (\alpha_1^{GL} * \dots * \alpha_k^{GL})(f)$ exists, for all $f \in \mathcal{M}_q$.)

Hence for all Hayes characters χ ,

$$\sum_{f \in \mathcal{M}_q} P_{GL}(f) \chi(f) u^{\deg(f)} = \sum_{f \in \mathcal{M}_q} \lim_{k \rightarrow \infty} (\alpha_1 * \dots * \alpha_k)(f) \chi(f) u^{\deg(f)}.$$

Lemma 2.3 then implies the theorem. \square

3.3 Character sums over $GL(n, q)$

We now treat averages of $\chi(\text{CharPoly}(M))$ for M ranging over $GL(n, q)$ and χ a fixed Hayes character. This information will be used to treat the distribution of traces of powers and characteristic polynomials of $M \in GL(n, q)$ in subsequent subsections. Recall the definition of $L_{GL}(u, \chi)$ in (3.1).

Theorem 3.6. *Let n be a positive integer. Let χ be a non-trivial Hayes character from $G(R_{\ell, H, q})$. We have*

$$L_{GL}(u, \chi) = L(u, \chi) \cdot (1 - \chi(T)u), \quad (3.5)$$

which is a polynomial of degree

$$d := \deg(L_{GL}(u, \chi)) \leq \ell + \deg(H). \quad (3.6)$$

Factorize L_{GL} as

$$L_{GL}(u, \chi) = \prod_{i=1}^d (1 - \gamma_i u). \quad (3.7)$$

(Note that γ_i will have a dependence on χ .) We have $|\gamma_i| \in \{1, \sqrt{q}\}$ for $i = 1, \dots, d$ and furthermore:

1. We have the identity

$$\frac{1}{|\text{GL}(n, q)|} \sum_{M \in \text{GL}(n, q)} \chi(\text{CharPoly}(M)) = (-1)^n \sum_{\substack{a_1 + \dots + a_d = n \\ a_1, \dots, a_d \geq 0}} \prod_{j=1}^d \frac{\gamma_j^{a_j}}{(q^{a_j} - 1)(q^{a_j-1} - 1) \dots (q - 1)}, \quad (3.8)$$

with the convention that $(q^a - 1) \dots (q - 1)$ is 1 when $a = 0$.

2. If $d > 0$ then the following estimate holds:

$$\left| \frac{1}{|\text{GL}(n, q)|} \sum_{M \in \text{GL}(n, q)} \chi(\text{CharPoly}(M)) \right| \leq q^{-\frac{n^2}{2d}} \left(1 + \frac{1}{q-1}\right)^n \binom{n+d-1}{n}. \quad (3.9)$$

Proof. (3.5) follows from (3.3) and (2.4). The degree bound (3.6) and bound on $|\gamma_i|$ follow directly from the bound on the degree of $L(u, \chi)$ and Riemann Hypothesis for Functions Fields discussed in §2.1.3.

For the exact formula (3.8), note that

$$\frac{1}{|\text{GL}(n, q)|} \sum_{M \in \text{GL}(n, q)} \chi(\text{CharPoly}(M)) = \sum_{f \in \mathcal{M}_{n,q}} P_{GL}(f) \chi(f) = [u^n] \prod_{i=1}^{\infty} L_{GL}\left(\frac{u}{q^i}, \chi\right),$$

with the second equality following from (3.2). Using (3.7) we obtain

$$\frac{1}{|\text{GL}(n, q)|} \sum_{M \in \text{GL}(n, q)} \chi(\text{CharPoly}(M)) = [u^n] \prod_{i=1}^{\infty} \prod_{j=1}^d (1 - \gamma_j \frac{u}{q^i}) = [u^n] \prod_{j=1}^d \prod_{i=1}^{\infty} (1 - \gamma_j \frac{u}{q^i}). \quad (3.10)$$

Using (2.10) with $y = \gamma_j u$ and $V = q$, we have

$$\prod_{i=1}^{\infty} (1 - \gamma_j \frac{u}{q^i}) = \sum_{a \geq 0} \frac{(-1)^a \gamma_j^a u^a}{(q^a - 1)(q^{a-1} - 1) \dots (q - 1)}. \quad (3.11)$$

From (3.10) and (3.11) we have

$$\frac{1}{|\mathrm{GL}(n, q)|} \sum_{M \in \mathrm{GL}(n, q)} \chi(\mathrm{CharPoly}(M)) = (-1)^n \sum_{a_1 + \dots + a_d = n} \prod_{j=1}^d \frac{\gamma_j^{a_j}}{(q^{a_j} - 1) \cdots (q - 1)}, \quad (3.12)$$

which establishes (3.8).

For the bound (3.9), we can apply the triangle inequality, the inequality $q^i - 1 \geq (\frac{q-1}{q})q^i$ and the bound $|\gamma_j| \leq \sqrt{q}$ to (3.12) and obtain

$$\begin{aligned} \left| \frac{1}{|\mathrm{GL}(n, q)|} \sum_{M \in \mathrm{GL}(n, q)} \chi(\mathrm{CharPoly}(M)) \right| &\leq q^{\frac{n}{2}} \sum_{a_1 + \dots + a_d = n} \prod_{j=1}^d \frac{1}{(q^{a_j} - 1) \cdots (q - 1)} \\ &\leq (1 + \frac{1}{q-1})^n q^{\frac{n}{2}} \sum_{a_1 + \dots + a_d = n} \prod_{j=1}^d \frac{1}{q^{a_j + (a_j - 1) + \dots + 1}} \\ &\leq (1 + \frac{1}{q-1})^n q^{\frac{n}{2}} \binom{n+d-1}{n} \max_{a_1 + \dots + a_d = n} q^{-\sum_{j=1}^d (a_j + 1)}. \end{aligned} \quad (3.13)$$

Let $S = \{(a_1, \dots, a_d) \in \mathbb{N}_{\geq 0} : a_1 + \dots + a_d = n\}$. The function

$$f(a_1, \dots, a_d) = \sum_{j=1}^d \binom{a_j + 1}{2}$$

on S is minimized when $g(a_1, \dots, a_d) = \max_{1 \leq j \leq d} a_j - \min_{1 \leq j \leq d} a_j$ is minimized, namely, equal to 0 (if $d \mid n$) or to 1 (otherwise). Indeed, if we assume in contradiction that the minimum is attained at $(a_1, \dots, a_d) \in S$ with $a_1 = \max_{1 \leq j \leq d} a_j$, $a_2 = \min_{1 \leq j \leq d} a_j$ and $a_1 - a_2 > 1$, then $(a_1 - 1, a_2 + 1, a_3, \dots, a_d) \in S$ and

$$f(a_1 - 1, a_2 + 1, a_3, \dots, a_d) - f(a_1, a_2, \dots, a_d) = a_2 + 1 - a_1 < 0,$$

a contradiction. If we write n as $dm + r$ ($m \in \mathbb{N}_{\geq 0}$, $0 \leq r < d$) then $g(a_1, \dots, a_d)$ is minimized for $a_1 = \dots = a_r = \lceil \frac{n}{d} \rceil$, $a_{r+1} = \dots = a_d = \lfloor \frac{n}{d} \rfloor$, in which case a short calculation shows that

$$\min_{\vec{x} \in S} f(\vec{x}) = f(a_1, \dots, a_d) = \frac{n^2}{2d} + \frac{n}{2} + \frac{r(1 - \frac{r}{d})}{2} \geq \frac{n^2}{2d} + \frac{n}{2}. \quad (3.14)$$

From (3.13) and (3.14), (3.9) is established. \square

3.4 The distribution of the characteristic polynomial: superexponential bounds for $\mathrm{GL}(n, q)$

We are now in a position to prove Theorem 1.3.

Proof of Theorem 1.3. By (2.3) with $H = 1$ and $\ell = n - h - 1$, we have,

$$\mathbf{1}_{\mathrm{CharPoly}(M) \in I(f; h)} = \frac{1}{q^{n-h-1}} \sum_{\chi \in G(R_{n-h-1, 1, q})} \bar{\chi}(f) \chi(\mathrm{CharPoly}(M)). \quad (3.15)$$

Thus,

$$\begin{aligned} \mathbb{P}_{M \in \mathrm{GL}(n, q)}(\mathrm{CharPoly}(M) \in I(f; h)) &= \frac{1}{q^{n-h-1}} \sum_{\chi \in G(R_{n-h-1, 1, q})} \bar{\chi}(f) \frac{\sum_{M \in \mathrm{GL}(n, q)} \chi(\mathrm{CharPoly}(M))}{|\mathrm{GL}(n, q)|} \\ &= q^{-(n-h-1)} \left(1 + \sum_{\substack{\chi \in G(R_{n-h-1, 1, q}) \\ \chi \neq \chi_0}} \bar{\chi}(f) \frac{\sum_{M \in \mathrm{GL}(n, q)} \chi(\mathrm{CharPoly}(M))}{|\mathrm{GL}(n, q)|} \right). \end{aligned} \quad (3.16)$$

When n is fixed, the right hand side of (3.9) is monotone increasing in d . From (3.16) and (3.9), we have

$$\begin{aligned} \left| \mathbb{P}_{M \in \mathrm{GL}(n,q)}(\mathrm{CharPoly}(M) \in I(f;h)) - q^{-(n-h-1)} \right| &\leq q^{-(n-h-1)} \sum_{\substack{\chi \in G(R_{n-h-1,1,q}) \\ \chi \neq \chi_0}} \left| \frac{\sum_{M \in \mathrm{GL}(n,q)} \chi(\mathrm{CharPoly}(M))}{|\mathrm{GL}(n,q)|} \right| \\ &\leq q^{-\frac{n^2}{2d_1}} \left(1 + \frac{1}{q-1}\right)^n \binom{n+d_1-1}{n}, \end{aligned} \quad (3.17)$$

where

$$d_1 = \max_{\substack{\chi \in G(R_{n-h-1,1,q}) \\ \chi \neq \chi_0}} \deg(L_{GL}(u, \chi)).$$

By §2.1.3, $d_1 \leq n - h - 1$. Hence, we see that (1.3) is established from (3.17). \square

3.5 The distribution of traces: superexponential bounds for $\mathrm{GL}(n, q)$

Proof of Theorem 1.1. Consider the additive character $\psi: \mathbb{F}_q \rightarrow \mathbb{C}$ defined as $\psi(a) = e^{\frac{2\pi i}{p} \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}$. For every $\lambda_1, \dots, \lambda_k \in \mathbb{F}_q$, set

$$S(n; \lambda_1, \dots, \lambda_k) := \frac{1}{|\mathrm{GL}(n, q)|} \sum_{M \in \mathrm{GL}(n, q)} \psi \left(\sum_{i=1}^k \lambda_i \mathrm{Tr}(M^{b_i}) \right).$$

By orthogonality of the characters of the additive group $(\mathbb{F}_q)^k$, we have

$$\mathbb{P}_{M \in \mathrm{GL}(n, q)}(\forall 1 \leq i \leq k : \mathrm{Tr}(M^{b_i}) = a_i) = q^{-k} \sum_{(\lambda_1, \dots, \lambda_k) \in (\mathbb{F}_q)^k} \psi \left(- \sum_{i=1}^k \lambda_i a_i \right) S(n; \lambda_1, \dots, \lambda_k).$$

The choice $\lambda_1 = \dots = \lambda_k = 0$ contributes q^{-k} . For the other choices, Lemma 2.2 says that

$$S(n; \lambda_1, \dots, \lambda_k) = \frac{\sum_{M \in \mathrm{GL}(n, q)} \chi_{\vec{\lambda}}(\mathrm{CharPoly}(M))}{|\mathrm{GL}(n, q)|},$$

where $\chi_0 \neq \chi_{\vec{\lambda}} \in G(R_{b_k, 1, q})$ was defined in the lemma. By Theorem 3.6,

$$|S(n; \lambda_1, \dots, \lambda_k)| \leq q^{-\frac{n^2}{2d}} \left(1 + \frac{1}{q-1}\right)^n \binom{n+d-1}{n} \quad (3.18)$$

where $d = \deg(L_{GL}(u, \chi_{\vec{\lambda}})) \leq b_k$. As in the proof of Theorem 1.3, we use the observation that the right hand side of (3.18) is monotone increasing in d , together with the bound $d \leq b_k$, to establish the theorem. \square

3.6 The characteristic polynomial in very short intervals for $\mathrm{GL}(n, q)$

Finally we treat the case of much smaller short intervals, in Theorem 1.4. Our method is a variant of the hyperbola method in analytic number theory. We need a few preliminary lemmas. For notational reasons, we let \sum^{gl} denote a sum with all summands restricted to \mathcal{M}_q^{gl} , so for instance

$$\sum_{d, \delta: d\delta=f}^{gl} = \sum_{d, \delta \in \mathcal{M}_q^{gl}, d\delta=f}.$$

Lemma 3.7. *For $f \in \mathcal{M}_q$ we have*

$$P_{GL}(f) = \frac{1}{|f|} (\mathbf{1}_{\mathcal{M}_q^{gl}} * P_{GL})(f) = \sum_{d, \delta: d\delta=f}^{gl} \frac{P_{GL}(\delta)}{|d\delta|}.$$

Proof. This follows directly from an examination of Theorem 3.4. The second equality is just a restatement of the first. \square

Lemma 3.8. For $n > h \geq 0$ and $\delta \in \mathcal{M}_q$, if $\deg(\delta) \leq h$, then

$$\sum_{d: d\delta \in I(f;h)}^{gl} 1 = \frac{q^{h+1}}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n,q}}^{gl} 1 \quad (3.19)$$

for any $f \in \mathcal{M}_{n,q}$. In particular the above expression is constant as f ranges over $\mathcal{M}_{n,q}$, for fixed n and q . Furthermore the right hand side of (3.19) simplifies. In fact for $\delta \in \mathcal{M}_q^{gl}$ and $\deg(\delta) \leq n$, we have

$$\frac{q^{h+1}}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n,q}}^{gl} 1 = \begin{cases} \frac{q^{h+1}}{|\delta|} (1 - q^{-1}) & \text{if } \deg(\delta) < n, \\ \frac{q^{h+1}}{|\delta|} & \text{if } \deg(\delta) = n. \end{cases} \quad (3.20)$$

Proof. Let $\Delta = \deg(\delta) \leq h$. By the orthogonality relation (2.3),

$$\sum_{d: d\delta \in I(f;h)}^{gl} 1 = \frac{1}{q^{n-h-1}} \sum_{\chi \in G(R_{n-h-1,1,q})} \bar{\chi}(f) \sum_{d \in \mathcal{M}_{n-\Delta,q}^{gl}} \chi(d) \chi(\delta).$$

But from Theorem 3.6, $L_{GL}(u, \chi)$ is a polynomial of degree no more than $n - h - 1$ for all non-trivial $\chi \in G(R_{n-h-1,1,q})$. For $\Delta \leq h$, we have $n - \Delta > n - h - 1$, so

$$\sum_{d \in \mathcal{M}_{n-\Delta,q}^{gl}} \chi(d) = 0, \quad \text{for } \chi \in G(R_{n-h-1,1,q}), \chi \neq \chi_0.$$

Hence

$$\sum_{d: d\delta \in I(f;h)}^{gl} 1 = \frac{1}{q^{n-h-1}} \chi_0(f) \sum_{d \in \mathcal{M}_{n-\Delta,q}^{gl}} \chi_0(d) \chi_0(\delta),$$

and this quantity does not depend on f as $\chi_0(f) = 1$ for all $f \in \mathcal{M}_{n,q}$. Hence, to see (3.19), note that because this expression is constant for all $f \in \mathcal{M}_{n,q}$,

$$\sum_{d: d\delta \in I(f;h)}^{gl} 1 = \frac{1}{q^n} \sum_{f \in \mathcal{M}_{n,q}} \sum_{d: d\delta \in I(f;h)}^{gl} 1 = \frac{q^{h+1}}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n,q}}^{gl} 1,$$

since in passing to the last equality, each $f \in \mathcal{M}_{n,q}$ will have been counted q^{h+1} times.

Finally, for (3.20), it is plain that if $\Delta \leq n$,

$$\sum_{d: d\delta \in \mathcal{M}_{n,q}}^{gl} 1 = |\mathcal{M}_{n-\Delta,q}^{gl}| = \begin{cases} q^{n-\Delta}(1 - q^{-1}) & \text{if } \Delta < n, \\ 1 & \text{if } \Delta = n, \end{cases}$$

and (3.20) follows from this. \square

Remark 9. Lemma 3.8 can be proved via a more elementary counting argument, but the argument given above will generalize to the other finite classical groups to be considered later.

Lemma 3.9. For $n > h \geq 0$ and $\delta \in \mathcal{M}_q$, if $\deg(\delta) \geq h + 1$, then

$$\left| \sum_{d: d\delta \in I(f;h)}^{gl} 1 \right| \leq 1 \quad (3.21)$$

for all $f \in \mathcal{M}_{n,q}$.

Proof. Plainly, if $\deg(\delta) \geq h + 1$, there will be either exactly one multiple of δ in $I(f;h)$, or no multiples of δ in $I(f;h)$. \square

We now use these lemmas to estimate the likelihood that a random $M \in \text{GL}(n, q)$ lands in a short interval.

Proof of Theorem 1.4. Note that

$$\begin{aligned}\mathbb{P}_{M \in \text{GL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) &= \sum_{g \in I(f;h)} P_{GL}(g) \\ &= \sum_{d, \delta: d\delta \in I(f;h)}^{gl} \frac{P_{GL}(\delta)}{|d\delta|},\end{aligned}$$

by Lemma 3.7. But this is

$$= \sum_{\deg(\delta) \leq h} \frac{P_{GL}(\delta)}{q^n} \sum_{d: d\delta \in I(f;h)}^{gl} 1 + \sum_{h+1 \leq \deg(\delta) \leq n} \frac{P_{GL}(\delta)}{q^n} \sum_{d: d\delta \in I(f;h)}^{gl} 1. \quad (3.22)$$

Utilizing (3.19), we have

$$\sum_{\deg(\delta) \leq h} \frac{P_{GL}(\delta)}{q^n} \sum_{d: d\delta \in I(f;h)}^{gl} 1 = \frac{q^{h+1}}{q^n} \sum_{\deg(\delta) \leq h} \frac{P_{GL}(\delta)}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n,q}}^{gl} 1,$$

with the advantage that the inner sum may be evaluated for any δ , not only for $\deg(\delta) \leq h$. Continuing, we have

$$\begin{aligned}\sum_{\deg(\delta) \leq h} \frac{P_{GL}(\delta)}{q^n} \sum_{d: d\delta \in I(f;h)}^{gl} 1 &= \frac{q^{h+1}}{q^n} \sum_{\delta \in \mathcal{M}_q} \frac{P_{GL}(\delta)}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n,q}}^{gl} 1 - \frac{q^{h+1}}{q^n} \sum_{\deg(\delta) > h} \frac{P_{GL}(\delta)}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n,q}}^{gl} 1 \\ &= \frac{q^{h+1}}{q^n} \sum_{f \in \mathcal{M}_{n,q}} P_{GL}(f) - \frac{1}{q^n} \sum_{n \geq \deg(\delta) > h} P_{GL}(\delta) \frac{q^{h+1}}{|\delta|} (1 - q^{-1} \cdot \mathbf{1}_{\deg(\delta) < n}),\end{aligned}$$

with the first term in the last line following from Lemma 3.7 and the second term in the last line following from (3.20). But, using the fact that P_{GL} is a probability measure on $\mathcal{M}_{n,q}$ to simplify both the first and second terms, the above simplifies to

$$= \frac{q^{h+1}}{q^n} - \frac{q^{h+1}}{q^n} \left((q^{-h-1} + q^{-h-2} + \dots + q^{-n+1})(1 - q^{-1}) + q^{-n} \right) = \frac{q^{h+1}}{q^n} - \frac{1}{q^n}. \quad (3.23)$$

On the other hand, turning to the second term in (3.22), we have

$$\sum_{h+1 \leq \deg(\delta) \leq n} \frac{P_{GL}(\delta)}{q^n} \sum_{\substack{d\delta \in I(f;h) \\ d, \delta \in \mathcal{M}_q^{gl}}} 1 \leq \sum_{h+1 \leq \deg(\delta) \leq n} \frac{P_{GL}(\delta)}{q^n} \leq \frac{n-h}{q^n}, \quad (3.24)$$

using (3.21) to bound the inner sum and then the fact that P_{GL} is a probability measure on $\mathcal{M}_{n,q}$.

Applying (3.23) and (3.24) to (3.22), we see that

$$\mathbb{P}_{M \in \text{GL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) = \frac{q^{h+1}}{q^n} - \frac{1}{q^n} + K \cdot \left(\frac{n-h}{q^n} \right),$$

where K is some number in between 0 and 1. This verifies Theorem 1.4. \square

4 Results for $\text{SL}(n, q)$

4.1 $\text{SL}(n, q)$ and the space of characteristic polynomials

The special linear group over \mathbb{F}_q is $\text{SL}(n, q) = \{M \in \text{Mat}(n, \mathbb{F}_q) : \det(M) = 1\}$. It is the kernel of the surjective group homomorphism $\det: \text{GL}(n, q) \rightarrow \mathbb{F}_q^\times$, and so we have the following.

Proposition 4.1. *We have $|\text{SL}(n, q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})/(q - 1)$.*

We define $\mathcal{M}_{n,q}^{sl} = \{f \in \mathcal{M}_{n,q} : (f, T) = 1, f(0) = (-1)^n\}$. It is plain for $M \in \text{SL}(n, q)$ that $\text{CharPoly}(M) \in \mathcal{M}_{n,q}^{sl}$, and it follows by considering companion matrices that in fact $\mathcal{M}_{n,q}^{sl} = \{\text{CharPoly}(M) : M \in \text{SL}(n, q)\}$. The reader should take a moment to verify

$$|\mathcal{M}_{n,q}^{sl}| = q^{n-1}, \quad n \geq 1.$$

Let $\mathcal{M}_q^{sl} = \cup_{n \geq 0} \mathcal{M}_{n,q}^{sl}$. It is easy to see that \mathcal{M}_q^{sl} is a submonoid of \mathcal{M}_q^{gl} .

4.2 Expression for $P_{SL}(f)$

Throughout this subsection we will take random $M \in \text{SL}(n, q)$ according to Haar measure (that is, uniform measure).

Definition 4.2. For $f \in \mathcal{M}_q$, we define the arithmetic function

$$P_{SL}(f) = \mathbb{P}_{M \in \text{SL}(n, q)}(\text{CharPoly}(M) = f) = \frac{|\{M \in \text{SL}(n, q) : \text{CharPoly}(M) = f\}|}{|\text{SL}(n, q)|},$$

where we take $n = \deg(f)$. For $f = 1$ we define $P_{SL}(1) = 1$.

The following observation allows us to use our formula for $P_{GL}(f)$ (given in Theorem 3.4) in order to study P_{SL} .

Lemma 4.3. For $f \in \mathcal{M}_q$ with $\deg(f) > 0$, we have

$$P_{SL}(f) = \begin{cases} (q-1)P_{GL}(f) & \text{if } f \in \mathcal{M}_q^{sl}, \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, for all $f \in \mathcal{M}_q$,

$$P_{SL}(f) = P_{GL}(f) \sum_{\chi_T \in G(R_{0,T,q})} \chi_T((T^n + (-1)^n)) \overline{\chi_T}(f).$$

Proof. The first part follows from $|\text{GL}(n, q)|/|\text{SL}(n, q)| = q-1$. A special case of (2.3), with $\ell = 1$ and $H = T$, is the following orthogonality relation:

$$\frac{1}{q-1} \sum_{\chi_T \in G(R_{0,T,q})} \overline{\chi_T}(T + (-1)^n) \chi_T(f) = \mathbf{1}_{f(0)=(-1)^n} \quad (4.1)$$

for all $f \in \mathcal{M}_q^{gl}$. Since $f \in \mathcal{M}_q^{sl}$ if and only if $f(0) = (-1)^n$, the second part follows. \square

4.3 Character sums over $\text{SL}(n, q)$

We have the following result on character sums, which allows us to use our results for character sums over $\text{GL}(n, q)$ (given in Theorem 3.6) in order to study corresponding sums over $\text{SL}(n, q)$.

Lemma 4.4. Let n be a positive integer. Let χ be a non-trivial Hayes character from $G(R_{\ell, H, q})$. We have

$$\frac{1}{|\text{SL}(n, q)|} \sum_{M \in \text{SL}(n, q)} \chi(\text{CharPoly}(M)) = \sum_{\chi_T \bmod T} \overline{\chi_T}(T + (-1)^n) \frac{\sum_{M \in \text{GL}(n, q)} (\chi \cdot \chi_T)(\text{CharPoly}(M))}{|\text{GL}(n, q)|}, \quad (4.2)$$

where the sum in the right hand side is over all $q-1$ Dirichlet characters χ_T modulo T (i.e. $G(R_{0,T,q})$).

Proof. Plugging $f = \text{CharPoly}(M)$ in (4.1), multiplying by $\chi(\text{CharPoly}(M))$ and averaging over $M \in \text{GL}(n, q)$ yields the result. \square

4.4 The distribution of the characteristic polynomial: superexponential bounds for $\text{SL}(n, q)$

Theorem 4.5. Let $M \in \text{SL}(n, q)$ be a random matrix chosen according to Haar measure. Then for $0 \leq h < n-1$ and for $f \in \mathcal{M}_{n,q}$,

$$\left| \mathbb{P}_{M \in \text{SL}(n, q)}(\text{CharPoly}(M) \in I(f; h)) - \frac{q^{h+1}}{q^n} \right| \leq q^{-\frac{n^2}{2(n-h-1)}} (q-1) \left(1 + \frac{1}{q-1}\right)^n \binom{2n-h-2}{n}. \quad (4.3)$$

Proof. The proof follows the line of Theorem 1.3. Using (4.2) and the same argument that gave us (3.16), we obtain

$$\mathbb{P}_{M \in \text{SL}(n, q)}(\text{CharPoly}(M) \in I(f; h)) = \frac{1}{q^{n-h-1}} \sum_{\substack{\chi \in G(R_{n-h-1, 1, q}) \\ \chi_T \bmod T}} \overline{\chi}(f) \overline{\chi_T}((-1)^n) \frac{\sum_{M \in \text{GL}(n, q)} (\chi \cdot \chi_T)(\text{CharPoly}(M))}{|\text{GL}(n, q)|}, \quad (4.4)$$

and so from (4.4) and Theorem 3.6, letting $\psi = \chi \cdot \chi_T \in G(R_{n-h-1,T,q})$, we have

$$\begin{aligned} \left| \mathbb{P}_{M \in \text{SL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) - q^{-(n-h-1)} \right| &\leq q^{-(n-h-1)} \sum_{\chi_0 \neq \psi \in G(R_{n-h-1,T,q})} \left| \frac{\sum_{M \in \text{GL}(n,q)} \psi(\text{CharPoly}(M))}{|\text{GL}(n,q)|} \right| \\ &\leq q^{-\frac{n^2}{2d_2}} (q-1) \left(1 + \frac{1}{q-1}\right)^n \binom{n+d_2-1}{n}, \end{aligned} \quad (4.5)$$

where $d_2 = \max_{\chi_0 \neq \psi \in G(R_{n-h-1,T,q})} \deg(L_{GL}(u, \psi))$. Since $\psi(T) = 0$ for $\psi \in G(R_{n-h-1,T,q})$, it follows that $d_2 \leq \max_{\chi_0 \neq \psi \in G(R_{n-h-1,T,q})} \deg(L(u, \psi)) \leq n-h-1$. Thus, (4.3) is established from (4.5). \square

4.5 The distribution of traces: superexponential bounds for $\text{SL}(n, q)$

Theorem 4.6. *Let $M \in \text{SL}(n, q)$ be a random matrix chosen according to Haar measure. Fix a strictly increasing sequence b_1, \dots, b_k of positive integers coprime to p . Then for any sequence a_1, \dots, a_k of elements of elements from \mathbb{F}_q , we have*

$$\left| \mathbb{P}_{M \in \text{SL}(n,q)}(\forall 1 \leq i \leq k : \text{Tr}(M^{b_i}) = a_i) - q^{-k} \right| \leq q^{-\frac{n^2}{2b_k}} (q-1) \left(1 + \frac{1}{q-1}\right)^n \binom{n-1+b_k}{n}.$$

The proof is omitted, as it follows closely the proof of Theorem 1.1.

4.6 The characteristic polynomial in very short intervals for $\text{SL}(n, q)$

We have the following lemma, whose proof follows the proofs of Lemmas 3.8 and 3.9.

Lemma 4.7. *Let χ_T be a non-trivial Dirichlet character modulo T . Let $n > h \geq 0$, $\delta \in \mathcal{M}_q$ and $f \in \mathcal{M}_{n,q}$. If $\deg(\delta) \leq h$, then*

$$\sum_{d: d\delta \in I(f;h)}^{gl} \chi_T(d) = 0.$$

If $\deg(\delta) \geq h+1$, then

$$\left| \sum_{d: d\delta \in I(f;h)}^{gl} \chi_T(d) \right| \leq 1. \quad (4.6)$$

Theorem 4.8. *Let $M \in \text{SL}(n, q)$ be a random matrix chosen according to Haar measure. Then for $0 \leq h < n$ and $f \in \mathcal{M}_{n,q}$,*

$$\left| \mathbb{P}_{M \in \text{SL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) - \frac{q^{h+1}}{q^n} \right| \leq \frac{n-h}{q^n/(q-1)}.$$

Proof. Note that

$$\begin{aligned} &\mathbb{P}_{M \in \text{SL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) - \mathbb{P}_{M \in \text{GL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) \\ &= \sum_{\chi_0 \neq \chi_T \bmod T} \chi_T(T + (-1)^n) \sum_{g \in I(f;h)} P_{GL}(g) \overline{\chi_T(g)} \\ &= \sum_{\chi_0 \neq \chi_T \bmod T} \chi_T(T + (-1)^n) \sum_{d, \delta: d\delta \in I(f;h)}^{gl} \frac{P_{GL}(\delta) \overline{\chi_T(d\delta)}}{|d\delta|}, \end{aligned}$$

by Lemma 3.7. But this is

$$\begin{aligned} &= \sum_{\chi_0 \neq \chi_T \bmod T} \chi_T(T + (-1)^n) \sum_{\deg(\delta) \leq h} \frac{P_{GL}(\delta) \overline{\chi_T(\delta)}}{q^n} \sum_{d: d\delta \in I(f;h)}^{gl} \overline{\chi_T(d)} \\ &\quad + \sum_{\chi_0 \neq \chi_T \bmod T} \chi_T(T + (-1)^n) \sum_{h+1 \leq \deg(\delta) \leq n} \frac{P_{GL}(\delta) \overline{\chi_T(\delta)}}{q^n} \sum_{d: d\delta \in I(f;h)}^{gl} \overline{\chi_T(d)}. \end{aligned} \quad (4.7)$$

According to the first part of Lemma 4.7, the first term in (4.7) vanishes, while by the second part of it, we have

$$\left| \chi_T(T + (-1)^n) \sum_{h+1 \leq \deg(\delta) \leq n} \frac{P_{GL}(\delta) \overline{\chi_T}(\delta)}{q^n} \sum_{d: d\delta \in I(f;h)} \overline{\chi_T}(d) \right| \leq \sum_{h+1 \leq \deg(\delta) \leq n} \frac{P_{GL}(\delta)}{q^n} \leq \frac{n-h}{q^n}$$

for any $\chi_0 \neq \chi_T \bmod T$, using (4.6) to bound the inner sum and then the fact that P_{GL} is a probability measure on $\mathcal{M}_{n,q}$. We see that

$$\left| \mathbb{P}_{M \in \text{SL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) - \mathbb{P}_{M \in \text{GL}(n,q)}(\text{CharPoly}(M) \in I(f;h)) \right| \leq \frac{(q-2)(n-h)}{q^n}. \quad (4.8)$$

Applying the triangle inequality to (4.8) and (1.4), this verifies the theorem. \square

From Theorem 4.8 we may deduce immediately using Lemma 2.1 an analogous result for traces.

Theorem 4.9. *Let $M \in \text{SL}(n,q)$ be a random matrix chosen according to Haar measure. Then for $1 \leq k \leq n$ and for $\{a_i\}_{1 \leq i \leq k, p \nmid i} \subseteq \mathbb{F}_q$, we have*

$$\left| \mathbb{P}_{M \in \text{SL}(n,q)}(\forall 1 \leq i \leq k, p \nmid i : \text{Tr}(M^i) = a_i) - \frac{1}{q^{k - \lfloor \frac{k}{p} \rfloor}} \right| \leq \frac{(k+1)q^{\lfloor \frac{k}{p} \rfloor}}{q^n/(q-1)}.$$

Remark 10. The above ideas can be used similarly to obtain results for $\text{SU}(n,q)$ from results for $\text{U}(n,q)$, and for $\text{SO}^\pm(n,q)$ from results for $\text{O}^\pm(n,q)$. In fact, one may study other cosets, e.g. $g\text{SL}(n,q) \subseteq \text{GL}(n,q)$ for $g \notin \text{SL}(n,q)$.

5 Results for $\text{U}(n,q)$

5.1 $\text{U}(n,q)$ and the space of characteristic polynomials

Recall that $\text{U}(n,q) = \{M \in \text{GL}(n,q^2) : M\overline{M}^t = I\}$, where \overline{M} is the matrix obtained by replacing entries of M by their q -th powers, and t is a transpose.¹

Proposition 5.1. [Tay92, Ch. 10] *We have $|\text{U}(n,q)| = q^{\binom{n}{2}} \prod_{i=1}^n (q^i - (-1)^i)$.*

In order to treat characteristic polynomials of matrices from $\text{U}(n,q) \subseteq \text{GL}(n,q^2)$, we require the following setup. Recall for $a \in \mathbb{F}_{q^2}$, the map $a \mapsto a^q$ is an involution of \mathbb{F}_{q^2} . For $f \in \mathcal{M}_{q^2}$, let $\sigma(f)$ be the map which raises each coefficient to the q -th power.

Definition 5.2. *For $n \geq 0$ and $f \in \mathcal{M}_{n,q^2}^{gl}$, define $\tilde{f} \in \mathcal{M}_{n,q^2}^{gl}$ by*

$$\tilde{f}(T) = \frac{T^n \sigma(f)(T^{-1})}{\sigma(f)(0)}.$$

That is, if $f(T) = a_0 + \dots + a_{n-1}T^{n-1} + T^n$, we have

$$\tilde{f}(T) = \left(\frac{1}{a_0}\right)^q + \left(\frac{a_{n-1}}{a_0}\right)^q T + \dots + T^n. \quad (5.1)$$

Note that $f \mapsto \tilde{f}$ is an involution of \mathcal{M}_{n,q^2}^{gl} .

Definition 5.3. *We say that a polynomial $f \in \mathcal{M}_{n,q^2}^{gl}$ is unitary self-reciprocal if $f = \tilde{f}$, and write*

$$\mathcal{M}_{n,q^2}^{usr} = \{f \in \mathcal{M}_{n,q^2}^{gl} : f = \tilde{f}\}.$$

Furthermore we write $\mathcal{M}_{q^2}^{usr} = \cup_{n \geq 0} \mathcal{M}_{n,q^2}^{usr}$.

It is easy to see that $\mathcal{M}_{q^2}^{usr}$ is a submonoid of $\mathcal{M}_{q^2}^{gl}$. By definition, if $M \in \text{U}(n,q)$ we have $M = (\overline{M}^t)^{-1}$, and so $\text{CharPoly}(M) = \text{CharPoly}((\overline{M}^t)^{-1}) = \text{CharPoly}(M)$, which forces the inclusion $\{\text{CharPoly}(M) : M \in \text{U}(n,q)\} \subseteq \mathcal{M}_{n,q^2}^{usr}$. In fact, from Theorem 5.8 below, these two sets are equal.

¹More generally, one may consider the group $\{M \in \text{GL}(n,q^2) : M A \overline{M}^t = A\}$ for a fixed Hermitian invertible matrix $A \in \text{GL}(n,q^2)$, i.e. $A = \overline{A}^t$. When varying A , we obtain groups which are conjugate to one another in $\text{GL}(n,q^2)$, see [Tay92, Ch. 10].

Proposition 5.4. *We have $|\mathcal{M}_{n,q^2}^{usr}| = q^n(1 + q^{-1})$ for $n \geq 1$.*

Proof. This is clear by analyzing explicit description (5.1) of \tilde{f} , considering n odd and n even separately. One uses the fact that $\mathbb{F}_{q^2}^\times$ is a cyclic group, and in particular that $a_0^{q+1} = 1$ has $q + 1$ solutions $a_0 \in \mathbb{F}_{q^2}^\times$. \square

From Definition 5.2, one sees for $f, g \in \mathcal{M}_{q^2}^{gl}$ that $\widetilde{fg} = \tilde{f} \cdot \tilde{g}$. As a consequence of this it follows that $\mathcal{M}_{q^2}^{usr}$ is a submonoid of $\mathcal{M}_{q^2}^{gl}$ under multiplication. Furthermore a polynomial $P \in \mathcal{M}_{q^2}^{gl}$ is irreducible if and only if \tilde{P} is irreducible.

In fact we have

Theorem 5.5. *Every $f \in \mathcal{M}_{q^2}^{usr}$ factorizes uniquely into irreducibles as*

$$f = \prod_{i=1}^r P_i^{e_i} \prod_{j=1}^s (Q_j \tilde{Q}_j)^{e'_j},$$

where $P_i = \tilde{P}_i$ for all i and $Q_j \neq \tilde{Q}_j$ for all j , and $P_i, Q_j \in \mathcal{M}_{q^2} \setminus \{T\}$ are irreducible for all i, j . Conversely, every such product is in $\mathcal{M}_{q^2}^{usr}$.

Proof. Consider some $f \in \mathcal{M}_{q^2}^{usr}$. We can write f as a product of irreducibles:

$$f = \prod_{P \in \mathcal{M}_{q^2} \setminus \{T\}, \tilde{P}=P} P^{e_P} \prod_{\{Q, \tilde{Q}\} \subseteq \mathcal{M}_{q^2} \setminus \{T\}, \tilde{Q} \neq Q} Q^{g_Q} \tilde{Q}^{g_{\tilde{Q}}}. \quad (5.2)$$

As $g \mapsto \tilde{g}$ is an involution which is completely multiplicative, we can compute \tilde{f} to be

$$\tilde{f} = \prod_{P \in \mathcal{M}_{q^2} \setminus \{T\}, \tilde{P}=P} P^{e_P} \prod_{\{Q, \tilde{Q}\} \subseteq \mathcal{M}_{q^2} \setminus \{T\}, \tilde{Q} \neq Q} \tilde{Q}^{g_Q} Q^{g_{\tilde{Q}}}. \quad (5.3)$$

Since $f = \tilde{f}$, the right hand side of (5.2) and the right hand side of (5.3) are equal. By unique factorization in $\mathbb{F}_{q^2}[T]$, it follows that $g_{\tilde{Q}} = g_Q$, as needed.

Conversely, $\mathcal{M}_{q^2}^{usr}$ contains $Q\tilde{Q}$ for any irreducible $Q \in \mathcal{M}_{q^2} \setminus \{T\}$ (again since $g \mapsto \tilde{g}$ is a multiplicative involution). By definition, $\mathcal{M}_{q^2}^{usr}$ contains every irreducible $P \in \mathcal{M}_{q^2} \setminus \{T\}$ such that $P = \tilde{P}$. As $\mathcal{M}_{q^2}^{usr}$ is a monoid, it follows that it contains every product of the kind described in the theorem. \square

For an element of $\mathcal{M}_{q^2}^{usr}$ to be irreducible imposes a restriction on its possible degree:

Theorem 5.6 (Fulman). *If $P \in \mathcal{M}_{q^2}^{usr}$ is an irreducible polynomial, then $\deg(P)$ is odd.*

This is a consequence of [Ful99, Thm. 9], but we give a different short and self-contained proof here.

Proof. If P is irreducible, we may write $P(T) = \prod_{i=0}^{\deg(P)-1} (T - z^{q^{2i}})$ for some $z \in \mathbb{F}_{q^{2 \deg(P)}}$ which is not in any $\mathbb{F}_{q^{2d}}$ for $d < \deg(P)$. In fact, for such z we have that $z \in \mathbb{F}_{q^{2d}}$ if and only if d is a multiple of $\deg(P)$.

Since $\tilde{P} = P$, this means that $t \mapsto t^{-q}$ is a permutation on the roots of P . In particular z^{-q} is a root of P also, so $z^{-q} = z^{q^{2i}}$ for some $0 \leq i < \deg(P)$, i.e. $(z^{q^{2i-1}+1})^q = 1$. Since we are in a field of characteristic p , it follows that $z^{q^{2i-1}+1} = 1$. Since the polynomial $T^{q^{2i-1}+1} - 1$ divides $T^{q^{2(2i-1)}-1} - 1$, it follows that $z \in \mathbb{F}_{q^{2(2i-1)}}$. Thus $2i-1$ is a multiple of $\deg(P)$. But $-1 \leq 2i-1 < 2 \deg(P)$, so necessarily $\deg(P) = 2i-1$. \square

5.2 Expressions for $P_U(f)$

Throughout this subsection we will take random $M \in \mathcal{U}(n, q)$ according to Haar measure (that is, uniform measure).

Definition 5.7. *For $f \in \mathcal{M}_q$, we define the arithmetic function*

$$P_U(f) = \mathbb{P}_{M \in \mathcal{U}(n, q)}(\text{CharPoly}(M) = f) = \frac{|\{M \in \mathcal{U}(n, q) : \text{CharPoly}(M) = f\}|}{|\mathcal{U}(n, q)|},$$

where we take $n = \deg(f)$. For $f = 1$ we have $P_U(1) = 1$.

Fulman [Ful99, Thm. 18] has proved a closed formula for the count $|\{M \in \mathcal{U}(n, q) : \text{CharPoly}(M) = f\}|$. We have found it natural to phrase his formula in the language of probability as above.

Theorem 5.8 (Fulman). *Suppose $f \in \mathcal{M}_{q^2}^{usr}$ factorizes as*

$$f = \prod_{i=1}^r P_i^{e_i} \prod_{j=1}^s (Q_j \tilde{Q}_j)^{e'_j},$$

with $P_i = \tilde{P}_i$ for all i and $Q_j \neq \tilde{Q}_j$ for all j , with $P_i, Q_j \in \mathcal{M}_{q^2}$ irreducible for all i, j . Set

$$m_i = \deg(P_i), \quad m'_j = \deg(Q_j).$$

Then

$$P_U(f) = \prod_{i=1}^r \frac{q^{m_i e_i (e_i - 1)}}{|\mathcal{U}(e_i, q^{m_i})|} \prod_{j=1}^s \frac{q^{2m'_j e'_j (e'_j - 1)}}{|\text{GL}(e'_j, q^{2m'_j})|}.$$

If f is a monic polynomial but $f \notin \mathcal{M}_{q^2}^{usr}$, then $P_U(f) = 0$.

As above, we observe that $P_U(f)$ can be written as an infinite Dirichlet convolution of simple arithmetic functions defined on \mathcal{M}_{q^2} .

Theorem 5.9. *Let $\lambda: \mathcal{M}_{q^2} \rightarrow \{-1, 1\}$ be the Liouville function, namely, the unique completely multiplicative function with $\lambda(P) = -1$ for every irreducible P in \mathcal{M}_{q^2} . For $g \in \mathcal{M}_{q^2}$, define the arithmetic functions*

$$\begin{aligned} \beta^U(g) &= |g|^{1/2} \mathbf{1}_{\mathcal{M}_{q^2}^{usr}}(g), \\ \gamma^U(g) &= \lambda(g) \mathbf{1}_{\mathcal{M}_{q^2}^{usr}}(g), \end{aligned}$$

and further define

$$\alpha_i^U(g) = \frac{1}{|g|^i} (\beta^U * \gamma^U)(g)$$

for $i \geq 1$. Then for $f \in \mathcal{M}_{q^2}$,

$$P_U(f) = \lim_{k \rightarrow \infty} (\alpha_1^U * \alpha_2^U * \cdots * \alpha_k^U)(f).$$

The proof of Theorem 5.9 is given below. It is a corollary of the following theorem:

Theorem 5.10. *For a Hayes character χ , define*

$$L_{usr}(u, \chi) = \sum_{f \in \mathcal{M}_{q^2}^{usr}} \chi(f) u^{\deg(f)}, \quad (5.4)$$

$$L_{usr}(u, \chi\lambda) = \sum_{f \in \mathcal{M}_{q^2}^{usr}} \chi(f) \lambda(f) u^{\deg(f)} \quad (5.5)$$

and

$$L_U(u, \chi) = L_{usr}(qu, \chi) L_{usr}(u, \chi\lambda).$$

The sums (5.4) and (5.5) converge absolutely for $|u| < 1/q$, and for $|u| < 1$ we have

$$\sum_{f \in \mathcal{M}_{q^2}} P_U(f) \chi(f) u^{\deg(f)} = \prod_{i=1}^{\infty} L_U\left(\frac{u}{q^{2i}}, \chi\right), \quad (5.6)$$

with both the left hand sum and the right hand product converging absolutely.

Proof. We treat claims about convergence first. For (5.4) and (5.5), note that $\sum_{f \in \mathcal{M}_{n, q^2}^{usr}} |\chi(f)| \leq 2q^n$ from Prop. 5.4, which furthermore implies $|L_{usr}(u, \chi)|, |L_{usr}(u, \chi\lambda)| \leq 1/(1 - |qu|)^2$. For the convergence of the left hand side of (5.6) note that $\sum_{f \in \mathcal{M}_{n, q^2}} |P_U(f)| \leq 1$, and for the convergence of the right hand side note that $L_U(u/q^{2i}) \leq 1/(1 - |u/q^{2i-2}|)^4$.

We have the Euler products

$$L_{usr}(u, \chi) = \prod_{\substack{P \neq T \\ P = \tilde{P}}} \frac{1}{1 - \chi(P) u^{\deg(P)}} \prod_{Q \neq \tilde{Q}} \frac{1}{1 - \chi(Q \tilde{Q}) u^{2 \deg(Q)}} \quad (5.7)$$

$$L_{usr}(u, \chi\lambda) = \prod_{\substack{P \neq T \\ P = \tilde{P}}} \frac{1}{1 + \chi(P)u^{\deg(P)}} \prod_{Q \neq \tilde{Q}} \frac{1}{1 - \chi(Q\tilde{Q})u^{2\deg(Q)}} \quad (5.8)$$

following from Theorem 5.5 and the fact that $\lambda(P) = -1$ and $\lambda(Q\tilde{Q}) = 1$ for all P, Q . Here and in what follows, the products are respectively over all irreducible monics P such that $P = \tilde{P}$ and $P \neq T$, and likewise over pairs of irreducible monics $\{Q, \tilde{Q}\}$, with $Q, \tilde{Q} \neq T$, and $Q \neq \tilde{Q}$, as in (5.2) and (5.3).

By using the facts that $|\{P \in \mathcal{M}_{n,q^2}^{usr} : P \text{ irreducible}\}| \leq |\mathcal{M}_{n,q^2}^{usr}| \leq q^n(1+q^{-1})$ and $|\{Q \in \mathcal{M}_{n,q^2} : Q \neq \tilde{Q}, Q \text{ irreducible}\}| \leq |\mathcal{M}_{n,q^2}| \leq q^{2n}$, it can be seen that the products in (5.7) and (5.8) converge absolutely for $|u| < 1/q$. Hence

$$L_U\left(\frac{u}{q^{2i}}, \chi\right) = \prod_{\substack{P \neq T \\ P = \tilde{P}}} \frac{1}{1 - \chi(P)u^{\deg(P)}/|P|^{(2i-1)/2}} \cdot \frac{1}{1 + \chi(P)u^{\deg(P)}/|P|^i} \\ \times \prod_{Q \neq \tilde{Q}} \frac{1}{1 - \chi(Q\tilde{Q})(u^{\deg(Q)}/|Q|^{(2i-1)/2})^2} \cdot \frac{1}{1 - \chi(Q\tilde{Q})(u^{\deg(Q)}/|Q|^i)^2},$$

and

$$\prod_{i=1}^{\infty} L_U\left(\frac{u}{q^{2i}}, \chi\right) = \prod_{\substack{P \neq T \\ P = \tilde{P}}} \prod_{j=1}^{\infty} \frac{1}{1 + \chi(P)u^{\deg(P)}(-|P|^{1/2})^{-j}} \prod_{Q \neq \tilde{Q}} \prod_{j=1}^{\infty} \frac{1}{1 - \chi(Q\tilde{Q})(u^{\deg(Q)}|Q|^{-j/2})^2}. \quad (5.9)$$

But from Theorem 5.8, one sees that $P_U(\prod_i P_i^{e_i} \prod_j (Q_j \tilde{Q}_j)^{e'_j}) = \prod P_U(P_i^{e_i}) \prod P_U((Q_j \tilde{Q}_j)^{e'_j})$, with

$$P_U(P^e) = \frac{|P|^{e(e-1)/4}}{\prod_{i=1}^e (|P|^{i/2} - (-1)^i)}, \\ P_U((Q\tilde{Q})^e) = \frac{|Q|^{e(e-1)}}{(|Q|^e - 1)(|Q|^e - |Q|) \cdots (|Q|^e - |Q|^{e-1})},$$

for $P = \tilde{P}$ and $Q \neq \tilde{Q}$. Hence

$$\sum_{f \in \mathcal{M}_{q^2}} P_U(f) \chi(f) u^{\deg(f)} = \prod_{\substack{P \neq T \\ P = \tilde{P}}} \left(1 + \sum_{e=1}^{\infty} \frac{|P|^{e(e-1)/4}}{\prod_{i=1}^e (|P|^{i/2} - (-1)^i)} (\chi(P) u^{\deg(P)})^e\right) \\ \times \prod_{Q \neq \tilde{Q}} \left(1 + \sum_{e=1}^{\infty} \frac{|Q|^{e(e-1)}}{(|Q|^e - 1) \cdots (|Q|^e - |Q|^{e-1})} (\chi(Q\tilde{Q}) u^{2\deg(Q)})^e\right).$$

By (2.9) with $y = -\chi(P)u^{\deg(P)}$, $V = -|P|^{1/2}$ and (2.8) with $y = \chi(Q\tilde{Q})u^{2\deg(Q)}$, $V = |Q|$, this agrees with the right hand side of (5.9). \square

Proof of Theorem 5.9. We proceed as in the proof of Theorem 3.4. We have from Theorem 5.10 that

$$\sum_{f \in \mathcal{M}_{q^2}} P_U(f) \chi(f) u^{\deg(f)} = \lim_{k \rightarrow \infty} \sum_{f \in \mathcal{M}_{q^2}} (\alpha_1^U * \cdots * \alpha_k^U)(f) \chi(f) u^{\deg(f)}.$$

And exactly as in the proof of Theorem 3.4, we may swap the order of limit and summation here and obtain the desired result by using Lemma 2.3. \square

5.3 The zeros of $L_{usr}(u, \chi)$

We examine the L -function $L_{usr}(u, \chi)$ defined in (5.4).

Lemma 5.11. *Let χ be a Hayes character of the form χ_1 or $\chi_1 \cdot \chi_T$, where χ_1 is a non-trivial short interval character of ℓ coefficients and χ_T is a Dirichlet character modulo T . The power series $L_{usr}(u, \chi)$ is a polynomial in u of degree at most 2ℓ .*

Proof. We denote the coefficients of $f \in \mathcal{M}_{n,q^2}$ by a_i :

$$f = T^n + a_1 T^{n-1} + \cdots + a_{n-1} T + a_n.$$

The condition $f \in \mathcal{M}_{n,q^2}^{usr}$ can be described in terms of the coefficients of f as follows:

$$a_n^{q+1} = 1, \forall 1 \leq i \leq \lfloor \frac{n}{2} \rfloor : a_{n-i} = \frac{a_i^q}{a_n^q}.$$

We first treat the case where $\chi = \chi_1$ or $\chi_1 \cdot \chi_T$, where χ_T is the trivial character modulo T . For $n \geq 2\ell + 1$, the number of $f \in \mathcal{M}_{n,q^2}^{usr}$ with given $a_1, \dots, a_\ell \in \mathbb{F}_{q^2}$ is $q^{n-2\ell} + q^{n-2\ell-1}$ and does not depend on the values of a_1, \dots, a_ℓ . In other words, $\mathcal{M}_{n,q^2}^{usr}$ is a disjoint union of $q^{n-2\ell-1}(q+1)$ representative sets modulo $R_{\ell,1,q^2}$. Thus, by the orthogonality relation (2.1), we have for all $n \geq 2\ell + 1$

$$\sum_{f \in \mathcal{M}_{n,q^2}} \chi(f) = q^{n-2\ell-1}(q+1) \cdot 0 = 0.$$

This shows that $L_{usr}(u, \chi)$ is a polynomial of degree at most 2ℓ . If $\chi = \chi_1 \cdot \chi_T$ where χ_T is non-trivial, and $n \geq 2\ell + 1$, then the number of $f \in \mathcal{M}_{n,q^2}^{usr}$ with given $a_1, \dots, a_\ell, a_n \in \mathbb{F}_{q^2}$ with $a_n^{q+1} = 1$ is $q^{n-2\ell-1}$ and does not depend on the values a_1, \dots, a_ℓ, a_n . As $\chi_1(f)$ depends only on a_1, \dots, a_ℓ while χ_T depends only on a_n , for all $n \geq 2\ell + 1$ we may write

$$\begin{aligned} \sum_{f \in \mathcal{M}_{n,q^2}^{usr}} \chi(f) &= \sum_{f \in \mathcal{M}_{n,q^2}^{usr}} \chi_1(f) \chi_T(f) \\ &= q^{n-2\ell-1} \sum_{a_1, \dots, a_\ell \in \mathbb{F}_{q^2}, a_n^{q+1}=1} \chi_1(T^n + a_1 T^{n-1} + \dots + a_\ell T^\ell + \dots) \chi_T(T^n + \dots + a_n) \\ &= q^{n-2\ell-1} \left(\sum_{a_1, \dots, a_\ell \in \mathbb{F}_{q^2}} \chi_1(T^n + a_1 T^{n-1} + \dots + a_\ell T^\ell + \dots) \right) \left(\sum_{a_n^{q+1}=1} \chi_T(T^n + \dots + a_n) \right) = 0, \end{aligned}$$

where in the last passage we have again used the orthogonality relation (2.1) applied to χ_1 . Thus $\deg(L_{usr}(u, \chi))$ is at most 2ℓ again, as needed. \square

Corollary 5.12. *Let χ be a Hayes character of the form χ_1 or $\chi_1 \cdot \chi_T$, where χ_1 is a non-trivial short interval character of ℓ coefficients and χ_T is a Dirichlet character modulo T . Then*

$$L_{usr}(u, \chi) = \prod_{i=1}^{\deg(L_{usr}(u, \chi))} (1 - \gamma_i u),$$

with $|\gamma_i| \leq q$ for all i and $\deg(L_{usr}(u, \chi)) \leq 2\ell$. (Note that γ_i will have a dependence on χ .)

Proof. The degree bound follows directly from Lemma 5.11. That $|\gamma_i| \leq q$ for all i follows from the convergence of the Euler product (5.7) for $|u| < 1/q$, which implies that $L(u, \chi) \neq 0$ for $|u| < 1/q$. If for some i we have $|\gamma_i| > q$, then we would have a contradiction that $L(u, \chi) = 0$ for some $|u| < 1/q$. \square

We expect that the L -function $L_{usr}(u, \chi)$, for χ a Hayes character in $\chi \in G(R_{\ell,T,q^2})$, will satisfy the Riemann Hypothesis, in the sense that its inverse roots will have absolute value $q^{-1/2}$ or 1. In fact, Li [Li92, Li06] proved this for certain characters χ , by showing that $L_{usr}(u, \chi)$ is essentially an L -function of a Hayes character in $G(R_{\ell,M,q})$. See also Curtis and Shinoda [CS99]. We do not pursue this here, as it can only lead to a modest saving of $q^{\frac{n}{2}}$ in Theorem 1.2 and in (5.11) below.

5.4 $\lambda(f)$ and $L_{usr}(u, \chi\lambda)$

We now turn to $L_{usr}(u, \chi\lambda)$. It ends up that this function is no more complicated than $L_{usr}(u, \chi)$. This is due to a peculiar feature of $\lambda(f)$ for $f \in \mathcal{M}_{q^2}^{usr}$.

Theorem 5.13. *For $f \in \mathcal{M}_{q^2}^{usr}$, we have $\lambda(f) = (-1)^{\deg(f)}$.*

Proof. Note that both $\lambda(f)$ and $(-1)^{\deg(f)}$ are completely multiplicative functions. Thus by factorization in $\mathcal{M}_{q^2}^{usr}$ (Theorem 5.5), to prove the theorem we need only show that for irreducible $P = \tilde{P}$ we have $\lambda(P) = (-1)^{\deg(P)}$ and for irreducible $Q \neq \tilde{Q}$ we have $\lambda(Q\tilde{Q}) = (-1)^{\deg(Q\tilde{Q})}$. But $\lambda(P) = -1$ by definition, and likewise $(-1)^{\deg(P)} = -1$ by Theorem 5.6. And obviously $\lambda(Q\tilde{Q}) = 1 = (-1)^{\deg(Q\tilde{Q})}$. \square

Corollary 5.14. *For a Hayes character χ , $L_{usr}(u, \chi\lambda) = L_{usr}(-u, \chi)$.*

Proof. This is evident from Theorem 5.13 and the definitions (5.4), (5.5) of $L_{usr}(u, \chi)$ and $L_{usr}(u, \chi\lambda)$. \square

Hence (5.6) can be rewritten

$$\sum_{f \in \mathcal{M}_{q^2}} P_U(f) \chi(f) u^{\deg(f)} = \prod_{j=1}^{\infty} L_{usr}\left(\frac{u}{q^j(-1)^{j+1}}, \chi\right),$$

for $|u| < 1$.

5.5 Character sums over $U(n, q)$

Theorem 5.15. *Let n be a positive integer. Let χ be a Hayes character of the form χ_1 or $\chi_1 \cdot \chi_T$, where χ_1 is a non-trivial short interval character of ℓ coefficients, and χ_T is a Dirichlet character modulo T .*

We have (for $L_{usr}(u, \chi)$ defined in (5.4)),

$$L_{usr}(u, \chi) = \prod_{i=1}^d (1 - \gamma_i u)$$

with

$$d := \deg(L_{usr}(u, \chi)) \leq 2\ell.$$

1. *We have the identity*

$$\frac{1}{|U(n, q)|} \sum_{M \in U(n, q)} \chi(\text{CharPoly}(M)) = \sum_{\substack{a_1 + \dots + a_d = n \\ a_1, \dots, a_d \geq 0}} \prod_{j=1}^d \frac{(-1)^{\binom{a_j}{2}} \gamma_j^{a_j}}{(q^{a_j} - (-1)^{a_j}) \cdots (q^2 - 1)(q + 1)} \quad (5.10)$$

with the convention that $(q^a - (-1)^a) \cdots (q^2 - 1)(q + 1) = 1$ when $a = 0$.

2. *If $d > 0$ then the following estimate holds:*

$$\left| \frac{1}{|U(n, q)|} \sum_{M \in U(n, q)} \chi(\text{CharPoly}(M)) \right| \leq q^{-\frac{n^2}{2d}} q^{\frac{n}{2}} \left(1 + \frac{1}{q-1}\right)^n \binom{n+d-1}{n}. \quad (5.11)$$

Proof. The proof proceeds in the same way as the proof of Theorem 3.6 with two minor differences: when applying (2.10) to deduce (5.10), let $y = -\gamma_j u$ and $V = -q$, and in the passage from (5.10) to (5.11), we use the bound $|\gamma_i| \leq q$ from Corollary 5.12 rather than the Riemann Hypothesis bound we used for $GL(n, q)$. \square

Remark 11. In the next subsections we only use Theorem 5.15 with χ a short interval character. It is possible to extend our results from $U(n, q)$ to $SU(n, q)$ by using Theorem 5.15 with $\chi \in G(R_{\ell, T, q^2})$.

5.6 The distribution of the characteristic polynomial: superexponential bounds for $U(n, q)$

Theorem 5.16. *Let $M \in U(n, q)$ be a random matrix chosen according to Haar measure. Then for $0 \leq h < n - 1$ and for $f \in \mathcal{M}_{n, q^2}$,*

$$\left| \mathbb{P}_{M \in U(n, q)}(\text{CharPoly}(M) \in I(f; h)) - \frac{q^{2(h+1)}}{q^{2n}} \right| \leq q^{-\frac{n^2}{4(n-h-1)}} q^{\frac{n}{2}} \left(1 + \frac{1}{q-1}\right)^n \binom{3n-2h-3}{n}.$$

Proof of Theorem 5.16. By (2.3) with $H = 1$ and $\ell = n - h - 1$, we have

$$\mathbf{1}_{\text{CharPoly}(M) \in I(f; h)} = \frac{1}{q^{2(n-h-1)}} \sum_{\chi \in G(R_{n-h-1, 1, q^2})} \bar{\chi}(f) \chi(\text{CharPoly}(M)).$$

Thus,

$$\begin{aligned} \mathbb{P}_{M \in \mathbf{U}(n,q)}(\text{CharPoly}(M) \in I(f;h)) &= \frac{1}{q^{2(n-h-1)}} \sum_{\chi \in G(R_{n-h-1,1,q^2})} \bar{\chi}(f) \frac{\sum_{M \in \mathbf{U}(n,q)} \chi(\text{CharPoly}(M))}{|\mathbf{U}(n,q)|} \\ &= q^{-2(n-h-1)} \left(1 + \sum_{\substack{\chi \in G(R_{n-h-1,1,q^2}) \\ \chi \neq \chi_0}} \bar{\chi}(f) \frac{\sum_{M \in \mathbf{U}(n,q)} \chi(\text{CharPoly}(M))}{|\mathbf{U}(n,q)|} \right). \end{aligned} \quad (5.12)$$

When n is fixed, the right hand side of (5.11) is monotone increasing in d . From (5.12) and (5.11), we have

$$\begin{aligned} \left| \mathbb{P}_{M \in \mathbf{U}(n,q)}(\text{CharPoly}(M) \in I(f;h)) - q^{-2(n-h-1)} \right| &\leq q^{-2(n-h-1)} \sum_{\substack{\chi \in G(R_{n-h-1,1,q^2}) \\ \chi \neq \chi_0}} \left| \frac{\sum_{M \in \mathbf{U}(n,q)} \chi(\text{CharPoly}(M))}{|\mathbf{U}(n,q)|} \right| \\ &\leq q^{-\frac{n^2}{2d_1}} q^{\frac{n}{2}} \left(1 + \frac{1}{q-1} \right)^n \binom{n+d_1-1}{n}, \end{aligned}$$

where

$$d_1 = \max_{\substack{\chi \in G(R_{n-h-1,1,q}) \\ \chi \neq \chi_0}} \deg(L_{usr}(u, \chi)).$$

By Corollary 5.12, $d_1 \leq 2(n-h-1)$, which concludes the proof. \square

5.7 The distribution of traces: superexponential bounds for $\mathbf{U}(n, q)$

Proof of Theorem 1.2. Consider the additive character $\psi: \mathbb{F}_{q^2} \rightarrow \mathbb{C}$ defined as $\psi(a) = e^{\frac{2\pi i}{p} \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_p}(a)}$. For every $\lambda_1, \dots, \lambda_k \in \mathbb{F}_{q^2}$, set

$$S(n; \lambda_1, \dots, \lambda_k) := \frac{1}{|\mathbf{U}(n,q)|} \sum_{M \in \mathbf{U}(n,q)} \psi \left(\sum_{i=1}^k \lambda_i \text{Tr}(M^{b_i}) \right).$$

By orthogonality of the characters of the additive group $(\mathbb{F}_{q^2})^k$, we have

$$\mathbb{P}_{M \in \mathbf{U}(n,q)}(\forall 1 \leq i \leq k : \text{Tr}(M^{b_i}) = a_i) = q^{-2k} \sum_{(\lambda_1, \dots, \lambda_k) \in (\mathbb{F}_{q^2})^k} \psi \left(- \sum_{i=1}^k \lambda_i a_i \right) S(n; \lambda_1, \dots, \lambda_k).$$

The choice $\lambda_1 = \dots = \lambda_k = 0$ contributes q^{-2k} . For the other choices, Lemma 2.2 says that

$$S(n; \lambda_1, \dots, \lambda_k) = \frac{\sum_{M \in \mathbf{U}(n,q)} \chi_{\bar{\lambda}}(\text{CharPoly}(M))}{|\mathbf{U}(n,q)|},$$

where $\chi_0 \neq \chi_{\bar{\lambda}} \in G(R_{b_k,1,q^2})$ was defined in the lemma. By Theorem 5.15,

$$|S(n; \lambda_1, \dots, \lambda_k)| \leq q^{-\frac{n^2}{2d}} q^{\frac{n}{2}} \left(1 + \frac{1}{q-1} \right)^n \binom{n+d-1}{n} \quad (5.13)$$

where $d = \deg(L_{usr}(u, \chi_{\bar{\lambda}})) \leq 2b_k$ by Corollary 5.12. As in the proof of Theorem 1.3, we use the observation that the right hand side of (5.13) is monotone increasing in d , together with the bound $d \leq 2b_k$, to establish the theorem. \square

5.8 The characteristic polynomial in very short intervals for $U(n, q)$

Finally we treat the case of short intervals which may contain only a small number of elements of $\mathcal{M}_{n, q^2}^{usr}$. In $\mathcal{M}_{n, q^2}^{usr}$ a polynomial is determined by only half its coefficients, and for this reason short intervals may contain no elements.

Proposition 5.17. *For any $f \in \mathcal{M}_{n, q^2}$ and $h < n$, we have*

$$|\mathcal{M}_{n, q^2}^{usr} \cap I(f; h)| = \begin{cases} q^{2(h+1)-n}(1+q^{-1}) & \text{if } h \geq (n-1)/2 \\ 1 & \text{if } h \leq (n-2)/2 \text{ and } f \in \mathcal{M}_{n, q^2}^{usr} \\ 0 & \text{if } h \leq (n-2)/2 \text{ and } f \notin \mathcal{M}_{n, q^2}^{usr}. \end{cases}$$

Proof. Those cases in which $h \leq (n-2)/2$ are evident. For $h \geq (n-1)/2$, this result is a minor generalization of Prop. 5.4, and follows likewise from analyzing the explicit description (5.1) of \tilde{f} . \square

Thus for $M \in U(n, q)$, it is only if h is larger than $(n-1)/2$ that there exists the possibility that the characteristic polynomial $\text{CharPoly}(M)$ equidistributes in all short intervals $I(f; h)$ of \mathcal{M}_{n, q^2} . But we show that for h only slightly larger than $(n-1)/2$ that equidistribution does indeed occur.

Theorem 5.18. *Let $M \in U(n, q)$ be a random matrix chosen according to Haar measure. Then for $(n-1)/2 \leq h < n$ and $f \in \mathcal{M}_{n, q^2}$,*

$$\left| \mathbb{P}_{M \in U(n, q)}(\text{CharPoly}(M) \in I(f; h)) - \frac{(q^2)^{h+1}}{(q^2)^n} \right| \leq \frac{2(n-h)}{q^n}.$$

Remark 12. Note that working within \mathcal{M}_{n, q^2} , $|I(f; h)|/|\mathcal{M}_{n, q^2}| = (q^2)^{h+1}/(q^2)^n$, so this result describes equidistribution, at least as long as

$$\frac{h - (n-1)/2}{\log_q(n)} \rightarrow \infty,$$

since in this case $2(n-h)/q^n = o((q^2)^{h+1}/(q^2)^n)$. As in the other examples we have considered, for $h - (n-1)/2$ growing sufficiently slowly we expect that equidistribution will cease, but we have not investigated this.

Our method is similar to that of §3.6. We use the notation that \sum^{usr} denotes a sum with all summands restricted to $\mathcal{M}_{n, q^2}^{usr}$, so for instance

$$\sum_{d, \delta: d\delta=f}^{usr} = \sum_{d, \delta \in \mathcal{M}_{n, q^2}^{usr}, d\delta=f}.$$

Lemma 5.19. *For $f \in \mathcal{M}_{q^2}$, define $P_U^\diamond(f) = (-1)^{\deg(f)} P_U(f)$. Then we have*

$$P_U(f) = \frac{1}{|f|^{1/2}} (\mathbf{1}_{\mathcal{M}_{q^2}^{usr}} * P_U^\diamond)(f) = \sum_{d, \delta: d\delta=f}^{usr} \frac{P_U^\diamond(\delta)}{|d\delta|^{1/2}}$$

Proof. The middle and last identity here are obviously equal.

In order to show that $P_U(f)$ is equal to these, note that from Theorem 5.9 we have

$$P_U(f) = \lim_{k \rightarrow \infty} \underbrace{\sum_{\substack{d_1, \dots, d_{2k} \\ d_1 d_2 \cdots d_{2k} = f}}^{usr} \frac{1}{|d_1|^{1/2}} \frac{\lambda(d_2)}{|d_2|} \frac{1}{|d_3|^{3/2}} \frac{\lambda(d_4)}{|d_4|^2} \cdots \frac{1}{|d_{2k-1}|^{k-1/2}} \frac{\lambda(d_{2k})}{|d_{2k}|^k}}_{=: A_k(f)}. \quad (5.14)$$

We also have

$$P_U(f) = \lim_{k \rightarrow \infty} \underbrace{\sum_{\substack{d_1, \dots, d_{2k-1} \\ d_1 d_2 \cdots d_{2k-1} = f}}^{usr} \frac{1}{|d_1|^{1/2}} \frac{\lambda(d_2)}{|d_2|} \frac{1}{|d_3|^{3/2}} \frac{\lambda(d_4)}{|d_4|^2} \cdots \frac{1}{|d_{2k-1}|^{k-1/2}}}_{=: B_k(f)}. \quad (5.15)$$

(5.15) is a consequence of (5.14) by the following argument. We have

$$A_k(f) = B_k(f) + \sum_{d|f, d \neq 1}^{usr} A_k(f/d) \frac{\lambda(d)}{|d|^k}. \quad (5.16)$$

The set of divisors $\{d : d|f, d \neq 1\}$ is finite and $\lambda(d)/|d|^k \rightarrow 0$ for all $d \neq 1$ as $k \rightarrow \infty$, so for fixed f the second term in (5.16) tends to 0 as $k \rightarrow \infty$, so

$$\lim_{k \rightarrow \infty} A_k(f) = \lim_{k \rightarrow \infty} B_k(f),$$

implying (5.15).

Working with (5.14), note that from Theorem 5.13 we have

$$\begin{aligned} P_U(f) &= \lim_{k \rightarrow \infty} \sum_{\substack{d_1, \dots, d_{2k} \\ d_1 d_2 \dots d_{2k} = f}}^{usr} \frac{1}{|d_1|^{1/2}} \frac{(-1)^{\deg(d_2)}}{|d_2|} \dots \frac{1}{|d_{2k-1}|^{k-1/2}} \frac{(-1)^{\deg(d_{2k})}}{|d_{2k}|^k} \\ &= \lim_{k \rightarrow \infty} \sum_{d, \delta: d\delta=f}^{usr} \frac{(-1)^{\deg(\delta)}}{|d|^{1/2} |\delta|^{1/2}} \sum_{\substack{d_2, \dots, d_{2k} \\ d_2 d_3 \dots d_{2k} = \delta}}^{usr} \frac{1}{|d_2|^{1/2}} \frac{(-1)^{\deg(d_3)}}{|d_3|} \dots \frac{(-1)^{\deg(d_{2k-1})}}{|d_{2k-1}|^{k-1}} \frac{1}{|d_{2k}|^{k-1/2}} \\ &= \sum_{d, \delta: d\delta=f}^{usr} \frac{P_U^\circ(\delta)}{|d\delta|^{1/2}}, \end{aligned}$$

where in the final step we use (5.15). We can exchange sum and limit because f is fixed and the sum is finite. \square

Lemma 5.20. *Take $n > 0$, $f \in \mathcal{M}_{n,q^2}$, and $n > h \geq (n-1)/2$. For $\delta \in \mathcal{M}_{q^2}^{usr}$, if $\deg(\delta) \leq 2h - n + 1$, we have*

$$\sum_{d: d\delta \in I(f;h)}^{usr} 1 = \frac{(q^2)^{h+1}}{(q^2)^n} \sum_{d: d\delta \in \mathcal{M}_{n,q^2}}^{usr} 1. \quad (5.17)$$

In particular the above expression is constant as f ranges over \mathcal{M}_{n,q^2} for fixed n and q . Furthermore the right hand side of (5.17) simplifies. In fact for $\delta \in \mathcal{M}_{q^2}^{usr}$ and $\deg(\delta) \leq n$, we have

$$\frac{(q^2)^{h+1}}{(q^2)^n} \sum_{d: d\delta \in \mathcal{M}_{n,q^2}}^{usr} 1 = \begin{cases} (q^{2(h+1)-n}/|\delta|^{1/2})(1+q^{-1}) & \text{if } \deg(\delta) < n, \\ q^{2(h+1)-n}/|\delta|^{1/2} & \text{if } \deg(\delta) = n. \end{cases} \quad (5.18)$$

(Note that $|\delta| = q^{2\deg(\delta)}$ in this setting.)

Proof. The details are very similar to the proof of Lemma 3.8, but because of some important changes (e.g. in the degree of relevant L -functions) we give a full proof.

Let $\Delta = \deg(\delta)$. By the orthogonality relation (2.3),

$$\sum_{d: d\delta \in I(f;h)}^{usr} 1 = \frac{1}{(q^2)^{n-h-1}} \sum_{\chi \in G(R_{n-h-1,1,q^2})} \bar{\chi}(f) \sum_{d \in \mathcal{M}_{n-\Delta,q^2}^{usr}} \chi(d) \chi(\delta).$$

By Lemma 5.11, $L_{usr}(u, \chi)$ is a polynomial of degree no more than $2(n-h-1)$, and for $\Delta \leq 2h-n+1$ we have $n-\Delta > 2(n-h-1)$, so

$$\sum_{d \in \mathcal{M}_{n-\Delta,q^2}^{usr}} \chi(d) = 0, \quad \text{for } \chi \in G(R_{n-h-1,1,q^2}), \chi \neq \chi_0.$$

Hence

$$\sum_{d: d\delta \in I(f;h)}^{usr} 1 = \frac{1}{(q^2)^{n-h-1}} \chi_0(f) \sum_{d \in \mathcal{M}_{n-\Delta,q^2}^{usr}} \chi_0(d) \chi_0(\delta),$$

which does not depend on f as $\chi_0(f) = 1$ for all $f \in \mathcal{M}_{n,q^2}$. To see (5.17), note that because this expression is constant for all $f \in \mathcal{M}_{n,q^2}$,

$$\sum_{d: d\delta \in I(f;h)}^{usr} 1 = \frac{1}{(q^2)^n} \sum_{f \in \mathcal{M}_{n,q^2}} \sum_{d: d\delta \in I(f;h)}^{usr} 1 = \frac{(q^2)^{h+1}}{(q^2)^n} \sum_{d: d\delta \in \mathcal{M}_{n,q^2}}^{usr} 1,$$

as in passing to the last equality, each $f \in \mathcal{M}_{n,q^2}$ will have been counted $(q^2)^{h+1}$ times.

Finally, in passing to (5.18), note that for $\delta \in \mathcal{M}_{\Delta, q^2}^{usr}$,

$$\sum_{d: d\delta \in \mathcal{M}_{n, q^2}}^{usr} 1 = |\mathcal{M}_{n-\Delta, q^2}^{usr}| = \begin{cases} q^{n-\Delta}(1+q^{-1}) & \text{for } \Delta < n, \\ 1 & \text{for } \Delta = n. \end{cases}$$

and (5.18) follows from this. \square

Lemma 5.21. *For $n > 0$, $n > h \geq (n-1)/2$ and $\delta \in \mathcal{M}_{q^2}^{usr}$, if $\deg(\delta) \geq 2h - n + 2$, then*

$$\left| \sum_{d: d\delta \in I(f; h)}^{usr} 1 \right| \leq 1$$

for all $f \in \mathcal{M}_{n, q^2}$.

Proof. We are counting elements d in $\mathcal{M}_{n-\deg(\delta), q^2}^{usr}$ such that $d\delta \equiv f \pmod{R_{n-h-1, 1, q^2}}$, or equivalently, $d \equiv \delta^{-1}f \pmod{R_{n-h-1, 1, q^2}}$. This gives a unique choice for the first $n-h-1 \geq (n-\deg(\delta))/2$ next-to-leading coefficients of d , which by definition of unitary self-reciprocals gives at most one option for d . \square

We now have all the tools for Theorem 5.18.

Proof of Theorem 5.18. We have

$$\mathbb{P}_{M \in \mathcal{U}(n, q)}(\text{CharPoly}(M) \in I(f; h)) = \sum_{d, \delta: d\delta \in I(f; h)}^{usr} \frac{P_U^\diamond(\delta)}{|d\delta|^{1/2}}$$

by Lemma 5.19. Letting $H = 2h - n + 1$ for notational reasons, this is

$$= \sum_{\deg(\delta) \leq H} \frac{P_U^\diamond(\delta)}{q^n} \sum_{d: d\delta \in I(f; h)}^{usr} 1 + \sum_{H+1 \leq \deg(\delta) \leq n} \frac{P_U^\diamond(\delta)}{q^n} \sum_{d: d\delta \in I(f; h)}^{usr} 1. \quad (5.19)$$

Utilizing (5.17), we have for the first term of (5.19),

$$\begin{aligned} \sum_{\deg(\delta) \leq H} \frac{P_U^\diamond(\delta)}{q^n} \sum_{d: d\delta \in I(f; h)}^{usr} 1 &= \frac{(q^2)^{h+1}}{(q^2)^n} \sum_{\deg(\delta) \leq H} \frac{P_U^\diamond(\delta)}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n, q^2}}^{usr} 1 \\ &= \frac{(q^2)^{h+1}}{(q^2)^n} \sum_{\delta \in \mathcal{M}_q} \frac{P_U^\diamond(\delta)}{q^n} \sum_{d: d\delta \in \mathcal{M}_{n, q^2}}^{usr} 1 - \frac{(q^2)^{h+1}}{(q^2)^n} \sum_{\deg(\delta) > H} \frac{P_U^\diamond(\delta)}{q^n} \sum_{d\delta \in \mathcal{M}_{n, q^2}}^{usr} 1 \\ &= \frac{(q^2)^{h+1}}{(q^2)^n} \sum_{f \in \mathcal{M}_{n, q^2}}^{usr} P_U(f) - \frac{1}{q^n} \sum_{n \geq \deg(\delta) > H} P_U^\diamond(\delta) \frac{q^{2(h+1)-n}}{|\delta|^{1/2}} (1 + q^{-1} \mathbf{1}_{\deg(\delta) < n}). \end{aligned}$$

But P_U is a probability measure on $\mathcal{M}_{n, q}$ and $P_U^\diamond(f) = (-1)^{\deg(f)} P_U(f)$ and so using this to simplify both terms above, that expression becomes

$$\begin{aligned} &= \frac{(q^2)^{h+1}}{(q^2)^n} - (-1)^{H+1} q^{2(h+1)-2n} \left(\left(\frac{1}{q^{H+1}} - \frac{1}{q^{H+2}} + \cdots \pm \frac{1}{q^{(n-1)}} \right) (1 + q^{-1}) \mp \frac{1}{q^n} \right) \\ &= \frac{(q^2)^{h+1}}{(q^2)^n} - \frac{(-1)^n}{q^n}, \end{aligned} \quad (5.20)$$

summing the geometric sum and recalling $H = 2h - n + 1$.

On the other hand, turning to the second term in (5.19), we have from Lemma 5.21,

$$\begin{aligned} \left| \sum_{H+1 \leq \deg(\delta) \leq n} \frac{P_U^\diamond(\delta)}{q^n} \sum_{d: d\delta \in I(f; h)}^{usr} 1 \right| &\leq \sum_{H+1 \leq \deg(\delta) \leq n} \frac{|P_U^\diamond(\delta)|}{q^n} \\ &\leq \frac{n-H}{q^n} \\ &= \frac{2n-2h-1}{q^n}. \end{aligned} \quad (5.21)$$

Applying (5.20) and (5.21) to (5.19), we see that

$$\mathbb{P}_{M \in \mathcal{U}(n,q)}(\text{CharPoly}(M) \in I(f; h)) = \frac{(q^2)^{h+1}}{(q^2)^n} - \frac{(-1)^n}{q^n} + K \cdot \left(\frac{2n-2h-1}{q^n} \right),$$

where K is a number in between -1 and 1 . This implies Theorem 5.18. \square

From Theorem 5.18 we may immediately deduce an analogous result for traces using Lemma 2.1.

Theorem 5.22. *Let $M \in \mathcal{U}(n, q)$ be a random matrix chosen according to Haar measure. Then for $1 \leq k \leq (n-1)/2$ and for $\{a_i\}_{1 \leq i \leq k, p \nmid i} \subseteq \mathbb{F}_{q^2}$, we have*

$$\left| \mathbb{P}_{M \in \mathcal{U}(n,q)}(\forall 1 \leq i \leq k, p \nmid i : \text{Tr}(M^i) = a_i) - \frac{1}{(q^2)^{k - \lfloor \frac{k}{p} \rfloor}} \right| \leq \frac{2(k+1)q^{2\lfloor \frac{k}{p} \rfloor}}{q^n}.$$

6 Results for $\text{Sp}(2n, q)$

In this section, q is an odd prime power.

6.1 $\text{Sp}(2n, q)$ and the space of characteristic polynomials

The symplectic group $\text{Sp}(2n, q) \subseteq \text{GL}(2n, q)$ is defined to be

$$\text{Sp}(2n, q) = \{g \in \text{GL}(2n, q) : g^t J_{2n} g = J_{2n}\},$$

where J_{2n} is any fixed invertible anti-symmetric matrix – the different choices giving rise to groups that are conjugate in $\text{GL}(2n, q)$.²

Proposition 6.1. [Tay92, Ch. 8] *We have $|\text{Sp}(2n, q)| = q^{n^2} \prod_{i=1}^n (q^{2i} - 1)$.*

In order to treat characteristic polynomials of matrices from $\text{Sp}(2n, q) \subseteq \text{GL}(2n, q)$, we require an involution defined on \mathcal{M}_q^{gl} .

Definition 6.2. *For $n \geq 0$ and $f \in \mathcal{M}_{n,q}^{gl}$, define $\bar{f} \in \mathcal{M}_{n,q}^{gl}$ by*

$$\bar{f}(T) = \frac{T^n f(T^{-1})}{f(0)}.$$

That is, if $f(T) = a_0 + \dots + a_{n-1}T^{n-1} + T^n$, we have

$$\bar{f}(T) = \frac{1}{a_0} + \frac{a_{n-1}}{a_0}T + \dots + T^n. \quad (6.1)$$

Definition 6.3. *We say that a polynomial $f \in \mathcal{M}_{n,q}^{gl}$ is self-reciprocal if $f = \bar{f}$, and write*

$$\mathcal{M}_{n,q}^{sr} = \{f \in \mathcal{M}_{n,q}^{gl} : f = \bar{f}\},$$

and $\mathcal{M}_q^{sr} = \cup_{n \geq 0} \mathcal{M}_{n,q}^{sr}$. Additionally, let

$$\begin{aligned} \mathcal{M}_{2n,q}^{sr,0} &= \{f \in \mathcal{M}_{2n,q}^{sr} : (f, (T-1)(T+1)) = 1\}, \\ \mathcal{M}_{2n,q}^{sr,1} &= \{f \in \mathcal{M}_{2n,q}^{sr} : f(0) = 1\}, \end{aligned}$$

and write $\mathcal{M}_q^{sr,i} = \cup_{n \geq 0} \mathcal{M}_{2n,q}^{sr,i}$ for $i = 0, 1$.

By definition, if $M \in \text{Sp}(2n, q)$ we have $M = J_{2n}^{-1}(M^t)^{-1}J_{2n}$, and so

$$\text{CharPoly}(M) = \text{CharPoly}((M^t)^{-1}) = \overline{\text{CharPoly}(M)},$$

so $\text{CharPoly}(M)$ is self-reciprocal. Moreover, $\text{Sp}(2n, q) \subseteq \text{SL}(2n, q)$ [Tay92, Cor. 6]. Thus, we have the inclusion $\{\text{CharPoly}(M) : M \in \text{Sp}(2n, q)\} \subseteq \mathcal{M}_{2n,q}^{sr,1}$. In fact, from Theorem 6.9 below, these two sets are equal.

²For instance, it is typical to take $J_{2n} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$.

Proposition 6.4. *We have $|\mathcal{M}_{n,q}^{sr}| = q^{\lfloor \frac{n}{2} \rfloor} + q^{\lfloor \frac{n-1}{2} \rfloor}$, $|\mathcal{M}_{2n,q}^{sr,1}| = q^n$ and $|\mathcal{M}_{2n,q}^{sr,0}| = q^n - 2q^{n-1} + q^{n-2}\mathbf{1}_{n>1}$ for $n \geq 1$.*

Proof. The first part is clear by analyzing explicit description (6.1) of \bar{f} , considering n odd and n even separately. The second part is similar. As $T \pm 1$ are self-reciprocal, the third part is solved by inclusion-exclusion, namely $|\mathcal{M}_{2n,q}^{sr,0}| = |\mathcal{M}_{2n,q}^{sr}| - 2|\mathcal{M}_{2n-1,q}^{sr}| + |\mathcal{M}_{2n-2,q}^{sr}|$. \square

From Definition 6.2, one sees for $f, g \in \mathcal{M}_q^{gl}$ that $\overline{fg} = \bar{f} \cdot \bar{g}$ and that $\deg(f) = \deg(\bar{f})$. As a consequence of this it follows that \mathcal{M}_q^{sr} and $\mathcal{M}_q^{sr,i}$ are submonoids of \mathcal{M}_q^{gl} under multiplication. Furthermore a polynomial $P \in \mathcal{M}_q^{gl}$ is irreducible if and only if \bar{P} is irreducible.

In fact we have

Theorem 6.5. *Every $f \in \mathcal{M}_q^{sr}$ factorizes uniquely into irreducibles as*

$$f = (T-1)^a (T+1)^b \prod_{i=1}^r P_i^{e_i} \prod_{j=1}^s (Q_j \bar{Q}_j)^{e'_j}, \quad (6.2)$$

where $P_i = \bar{P}_i$ for all i and $Q_j \neq \bar{Q}_j$ for all j , and $P_i, Q_j \in \mathcal{M}_q \setminus \{T, T-1, T+1\}$ are irreducible for all i, j . Conversely, every such product is in \mathcal{M}_q^{sr} .

Proof. The proof is completely analogous to that of Theorem 5.5. \square

For an element of \mathcal{M}_q^{sr} to be irreducible imposes a restriction on its possible degree, as shown e.g. in [Car67] and in [Ful99, Thm. 11]. We give a different proof of this, with additional information, in the following theorem.

Theorem 6.6. *If $P \in \mathcal{M}_q^{sr}$ is an irreducible polynomial, then either $P \in \{T-1, T+1\}$, or $\deg(P)$ is even. In the later case, $P(0) = 1$.*

If $Q \in \mathcal{M}_q^{gl} \setminus \mathcal{M}_q^{sr}$ is an irreducible polynomial, then $Q\bar{Q} \in \mathcal{M}_q^{sr}$ and $(Q\bar{Q})(0) = 1$.

Proof. We may write $P(T) = \prod_{i=0}^{\deg(P)-1} (T - z_i)$ for some distinct z_i in the algebraic closure. Since $\bar{P} = P$, this means that $t \mapsto t^{-1}$ is a permutation on the roots of P . If $P(T) \neq T \pm 1$ then there are no fixed points for the permutation induced by $t \mapsto t^{-1}$, and so its cycle structure consists of $\deg(P)/2$ transpositions, forcing $\deg(P)$ to be even. In this case, assuming $z_i^{-1} = z_{\deg(P)-i-1}$ w.l.o.g, $P(0) = \prod_{i=0}^{\deg(P)-1} z_i = \prod_{i=0}^{\frac{\deg(P)}{2}-1} (z_i z_i^{-1}) = 1$.

Since $f \mapsto \bar{f}$ is an involution, clearly $Q\bar{Q} \in \mathcal{M}_q^{sr}$. Again, since $t \mapsto t^{-1}$ permutes the roots of $Q\bar{Q}$ and has no fixed points, we find that $(Q\bar{Q})(0) = 1$. \square

By comparing degrees and constant coefficients in (6.2), we obtain the following corollary.

Corollary 6.7. *In the notation of Theorem 6.5, $f \in \mathcal{M}_q^{sr}$ is in $\mathcal{M}_q^{sr,1}$ if and only if a and b are both even, and $f \in \mathcal{M}_q^{sr}$ is in $\mathcal{M}_q^{sr,0}$ if and only if a and b are both 0. In particular, $\mathcal{M}_q^{sr,0} \subseteq \mathcal{M}_q^{sr,1}$.*

6.2 Expressions for $P_{Sp}(f)$

Throughout this subsection we will take random $M \in \text{Sp}(2n, q)$ according to Haar measure (that is, uniform measure).

Definition 6.8. *For $f \in \mathcal{M}_q$, we define the arithmetic function*

$$P_{Sp}(f) = \mathbb{P}_{M \in \text{Sp}(2n, q)}(\text{CharPoly}(M) = f) = \frac{|\{M \in \text{Sp}(2n, q) : \text{CharPoly}(M) = f\}|}{|\text{Sp}(2n, q)|}$$

where we take $2n = \deg(f)$ if $\deg(f)$ is even, and where we set $P_{Sp}(f) = 0$ if $\deg(f)$ is odd. For $f = 1$ we define $P_{Sp}(1) = 1$.

Fulman [Ful99, Thm. 19] has proved a closed formula for the count $|\{M \in \text{Sp}(2n, q) : \text{CharPoly}(M) = f\}|$. We have found it natural to phrase his formula in the language of probability as above.

Theorem 6.9 (Fulman). Suppose $f \in \mathcal{M}_q^{sr,1}$ factorizes as

$$f = (T-1)^{2a}(T+1)^{2b} \prod_{i=1}^r P_i^{e_i} \prod_{j=1}^s (Q_j \overline{Q_j})^{e'_j},$$

with $P_i = \overline{P_i}$ for all i and $Q_j \neq \overline{Q_j}$ for all j , with $P_i, Q_j \in \mathcal{M}_q \setminus \{T, T-1, T+1\}$ irreducible for all i, j . Set

$$m_i = \deg(P_i), \quad m'_j = \deg(Q_j).$$

Then

$$P_{Sp}(f) = \frac{q^{2a^2}}{|\mathrm{Sp}(2a, q)|} \frac{q^{2b^2}}{|\mathrm{Sp}(2b, q)|} \prod_{i=1}^r \frac{q^{\frac{m_i e_i (e_i - 1)}{2}}}{|\mathrm{U}(e_i, q^{\frac{m_i}{2}})|} \prod_{j=1}^s \frac{q^{m'_j e'_j (e'_j - 1)}}{|\mathrm{GL}(e'_j, q^{m'_j})|}.$$

If f is a monic polynomial but $f \notin \mathcal{M}_q^{sr,1}$, then $P_{Sp}(f) = 0$.

We observe that $P_{Sp}(f)$ can be written as an infinite Dirichlet convolution of simple arithmetic functions defined on \mathcal{M}_q .

Theorem 6.10. Let $\lambda: \mathcal{M}_q \rightarrow \{-1, 1\}$ be the Liouville function, namely, the unique completely multiplicative function with $\lambda(P) = -1$ for every irreducible P in \mathcal{M}_q . For $g \in \mathcal{M}_q$, define the arithmetic functions

$$\begin{aligned} \beta^{Sp}(g) &= |g|^{1/2} \mathbf{1}_{\mathcal{M}_q^{sr,1}}(g), \\ \gamma^{Sp}(g) &= \lambda(g) \mathbf{1}_{\mathcal{M}_q^{sr,0}}(g), \end{aligned}$$

and further define

$$\alpha_i^{Sp}(g) = \frac{1}{|g|^i} (\beta^{Sp} * \gamma^{Sp})(g)$$

for $i \geq 1$. Then for $f \in \mathcal{M}_q$,

$$P_{Sp}(f) = \lim_{k \rightarrow \infty} (\alpha_1^{Sp} * \alpha_2^{Sp} * \cdots * \alpha_k^{Sp})(f).$$

The proof of Theorem 6.10 is given below. It is a corollary of the following theorem:

Theorem 6.11. For a Hayes character χ , define

$$L_{sr,i}(u, \chi) = \sum_{f \in \mathcal{M}_q^{sr,i}} \chi(f) u^{\deg(f)}, \quad (6.3)$$

$$L_{sr,i}(u, \chi\lambda) = \sum_{f \in \mathcal{M}_q^{sr,i}} \chi(f) \lambda(f) u^{\deg(f)} \quad (6.4)$$

for $i = 0, 1$, and

$$L_{Sp}(u, \chi) = L_{sr,1}(\sqrt{q}u, \chi) L_{sr,0}(u, \chi\lambda). \quad (6.5)$$

The sums (6.3) and (6.4) converge absolutely for $|u| < 1/\sqrt{q}$, and for $|u| < 1$ we have

$$\sum_{f \in \mathcal{M}_q} P_{Sp}(f) \chi(f) u^{\deg(f)} = \prod_{i=1}^{\infty} L_{Sp}\left(\frac{u}{q^i}, \chi\right), \quad (6.6)$$

with both the left hand sum and the right hand product converging absolutely.

Proof. We treat claims about convergence first. For (6.3) and (6.4), note that $\sum_{f \in \mathcal{M}_{n,q}^{sr}} |\chi(f)| \leq 2q^{\frac{n}{2}}$ from Prop. 6.4, which furthermore implies $|L_{sr,1}(u, \chi)|, |L_{sr,0}(u, \chi\lambda)| \leq 1/(1 - |\sqrt{q}u|)^2$. For the convergence of the left hand side of (6.6) note that $\sum_{f \in \mathcal{M}_{n,q}} |P_{Sp}(f)| \leq 1$, and for the convergence of the right hand side note that $|L_{Sp}(u/q^i)| \leq 1/(1 - |u/q^{i-1}|)^4$.

We have the Euler products

$$\begin{aligned} L_{sr,1}(u, \chi) &= \frac{1}{1 - \chi^2(T-1)u^2} \frac{1}{1 - \chi^2(T+1)u^2} \\ &\quad \times \prod_{\substack{P \neq T, T \pm 1 \\ P = \overline{P}}} \frac{1}{1 - \chi(P)u^{\deg(P)}} \prod_{Q \neq \overline{Q}} \frac{1}{1 - \chi(Q\overline{Q})u^{2\deg(Q)}}, \end{aligned} \quad (6.7)$$

$$L_{sr,0}(u, \chi\lambda) = \prod_{\substack{P \neq T, T \pm 1 \\ P = \overline{P}}} \frac{1}{1 + \chi(P)u^{\deg(P)}} \prod_{Q \neq \overline{Q}} \frac{1}{1 - \chi(Q\overline{Q})u^{2\deg(Q)}} \quad (6.8)$$

following from Theorem 6.5, Corollary 6.7 and the fact that $\lambda(P) = -1$ and $\lambda(Q\bar{Q}) = 1$ for all P, Q . Here the products are respectively over all irreducible monics P such that $P = \bar{P}$ and $P \neq T, T \pm 1$, and likewise over irreducible monics Q such that $Q \neq \bar{Q}$. By using the facts that $|\{P \in \mathcal{M}_{n,q}^{sr} : P \text{ irreducible}\}| \leq |\mathcal{M}_{n,q}^{sr}| \leq 2q^{\frac{n}{2}}$ and $|\{Q \in \mathcal{M}_{n,q} : Q \neq \bar{Q}, Q \text{ irreducible}\}| \leq |\mathcal{M}_{n,q}| \leq q^n$, it can be seen that the products in (6.7) and (6.8) converge absolutely for $|u| < 1/\sqrt{q}$. Hence

$$\begin{aligned} L_{Sp}\left(\frac{u}{q^i}, \chi\right) &= \frac{1}{1 - \chi^2(T-1)u^2/q^{2i-1}} \frac{1}{1 - \chi^2(T+1)u^2/q^{2i-1}} \\ &\quad \times \prod_{\substack{P \neq T, T \pm 1 \\ P = \bar{P}}} \left(\frac{1}{1 - \chi(P)u^{\deg(P)}/|P|^{(2i-1)/2}} \cdot \frac{1}{1 + \chi(P)u^{\deg(P)}/|P|^i} \right) \\ &\quad \times \prod_{Q \neq \bar{Q}} \left(\frac{1}{1 - \chi(Q\bar{Q})(u^{\deg(Q)}/|Q|^{(2i-1)/2})^2} \cdot \frac{1}{1 - \chi(Q\bar{Q})(u^{\deg(Q)}/|Q|^i)^2} \right), \end{aligned}$$

and

$$\begin{aligned} \prod_{i=1}^{\infty} L_{Sp}\left(\frac{u}{q^i}, \chi\right) &= \prod_{j=1}^{\infty} \left(\frac{1}{1 - \chi^2(T-1)u^2/q^{2j-1}} \frac{1}{1 - \chi^2(T+1)u^2/q^{2j-1}} \right) \\ &\quad \prod_{\substack{P \neq T, T \pm 1 \\ P = \bar{P}}} \prod_{j=1}^{\infty} \frac{1}{1 + \chi(P)u^{\deg(P)}(-|P|^{1/2})^{-j}} \prod_{Q \neq \bar{Q}} \prod_{j=1}^{\infty} \frac{1}{1 - \chi(Q\bar{Q})(u^{\deg(Q)}/|Q|^{-j/2})^2}. \quad (6.9) \end{aligned}$$

But from Theorem 6.9, one sees that $P_{Sp}((T-1)^{2a}(T+1)^{2b} \prod P_i^{e_i} \prod (Q_j \bar{Q}_j)^{e'_j}) = P_{Sp}((T-1)^{2a})P_{Sp}((T+1)^{2b}) \prod P_{Sp}(P_i^{e_i}) \prod P_{Sp}((Q_j \bar{Q}_j)^{e'_j})$, with

$$\begin{aligned} P_{Sp}((T \pm 1)^{2e}) &= \frac{q^{e^2}}{(q^{2e} - 1)(q^{2(e-1)} - 1) \cdots (q^2 - 1)}, \\ P_{Sp}(P^e) &= \frac{|P|^{e(e-1)/4}}{\prod_{i=1}^e (|P|^{i/2} - (-1)^i)}, \\ P_{Sp}((Q\bar{Q})^e) &= \frac{|Q|^{e(e-1)}}{(|Q|^e - 1)(|Q|^e - |Q|) \cdots (|Q|^e - |Q|^{e-1})}, \end{aligned}$$

for $P = \bar{P} \neq T \pm 1$ and $Q \neq \bar{Q}$. Hence

$$\begin{aligned} \sum_{f \in \mathcal{M}_q} P_{Sp}(f) \chi(f) u^{\deg(f)} &= \\ &\left(1 + \sum_{e=1}^{\infty} \frac{q^{e^2}}{\prod_{i=1}^e (q^{2i} - 1)} (\chi(T-1)u)^{2e}\right) \left(1 + \sum_{e=1}^{\infty} \frac{q^{e^2}}{\prod_{i=1}^e (q^{2i} - 1)} (\chi(T+1)u)^{2e}\right) \\ &\quad \times \prod_{\substack{P \neq T, T \pm 1 \\ P = \bar{P}}} \left(1 + \sum_{e=1}^{\infty} \frac{|P|^{e(e-1)/4}}{\prod_{i=1}^e (|P|^{i/2} - (-1)^i)} (\chi(P)u^{\deg(P)})^e\right) \\ &\quad \times \prod_{Q \neq \bar{Q}} \left(1 + \sum_{e=1}^{\infty} \frac{|Q|^{e(e-1)}}{(|Q|^e - 1) \cdots (|Q|^e - |Q|^{e-1})} (\chi(Q\bar{Q})u^{2\deg(Q)})^e\right). \end{aligned}$$

By (2.9) with $(y, V) \in \{(q(\chi(T \pm 1)u)^2, q^2), (-\chi(P)u^{\deg(P)}, -|P|^{1/2})\}$ and (2.8) with $y = \chi(Q\bar{Q})u^{2\deg(Q)}$, $V = |Q|$, this agrees with the right hand side of (6.9). \square

Proof of Theorem 6.10. We proceed as in the proof of Theorem 3.4. We have from Theorem 6.11 that

$$\sum_{f \in \mathcal{M}_q} P_{Sp}(f) \chi(f) u^{\deg(f)} = \lim_{k \rightarrow \infty} \sum_{f \in \mathcal{M}_q} (\alpha_1^{Sp} * \cdots * \alpha_k^{Sp})(f) \chi(f) u^{\deg(f)}.$$

And exactly as in the proof of Theorem 3.4, we may swap the order of limit and summation here and obtain the desired result by using Lemma 2.3. \square

6.3 The zeros of $L_{sr,1}(u, \chi)$

We examine the L -function $L_{sr,1}(u, \chi)$ defined in (6.3).

Lemma 6.12. *Consider the homomorphism $\Psi: \mathcal{M}_q \rightarrow \mathcal{M}_q^{sr}$ defined by $\Psi(g(T)) = g(T + \frac{1}{T})T^{\deg(g)}$.*

1. $\deg(\Psi(g)) = 2 \deg(g)$.
2. Ψ is injective.
3. *The k -th next-to-leading coefficient of $\Psi(g)$ (for $1 \leq k \leq \deg(g)$) is a linear function of the first k next-to-leading coefficients of g .*
4. *The image of Ψ is $\mathcal{M}_q^{sr,1}$.*

Proof. The first two parts are simple, and the third part follows by expanding $g(T + \frac{1}{T})$. For the fourth part, note that if $g(T) = \prod_{i=1}^{\deg(g)} (T - \alpha_i)$ then $\Psi(g) = \prod_{i=1}^{\deg(g)} (T^2 - \alpha_i T + 1)$, which is self-reciprocal of even degree, and moreover, the multiplicity of $T \pm 1$ in it is even, as these factors may only come from $\alpha_i = \pm 1$. Hence $\Psi(g) \in \mathcal{M}_{2\deg(g),q}^{sr,1}$. A counting argument using Prop. 6.4 shows that $\Psi(\mathcal{M}_{n,q}) = \mathcal{M}_{2n,q}^{sr,1}$. \square

Let us denote the inverse of Ψ by Φ .

Proposition 6.13. *Given a short interval character of ℓ coefficients χ , there is a unique short interval character of ℓ coefficients χ' such that $\chi(f) = \chi'(\Phi(f))$ for all $f \in \mathcal{M}_q^{sr,1}$. Moreover,*

$$L_{sr,1}(u, \chi) = L(u^2, \chi').$$

Moreover, χ is non-trivial if and only if χ' is non-trivial. Here $L(u^2, \chi')$ refers to the usual L -function, defined in §2.1.3.

Proof. The condition $\chi(f) = \chi'(\Phi(f))$ for all $f \in \mathcal{M}_q^{sr,1}$ is the same as

$$\chi'(g(T)) = \chi(g(T + \frac{1}{T})T^{\deg(g)})$$

for all $g \in \mathcal{M}_q$. This definition determines χ' uniquely, and we get for free the multiplicativity of χ' and the fact that $\chi'(1) = 1$. To see that χ' is well-defined, one uses Lemma 6.12 which tells us that the first ℓ next-to-leading coefficients of $g(T + \frac{1}{T})T^{\deg(g)}$ depend only on the first ℓ next-to-leading coefficients of g . This shows that $\chi'(g)$ depends only on the first ℓ next-to-leading coefficients of g .

If χ' is trivial then $\chi(f) = 1$ for all $f \in \mathcal{M}_q^{sr,1}$. Since for any given ℓ next-to-leading coefficients a_1, a_2, \dots, a_ℓ one may find a polynomial f in $\mathcal{M}_q^{sr,1}$ with such next-to-leading coefficients (e.g. $f = T^{2\ell} + a_1 T^{2\ell-1} + \dots + a_\ell T^\ell + a_{\ell-1} T^{\ell-1} + \dots + 1$), it follows that χ is trivial as well. The other direction is immediate.

By the last part of Lemma 6.12,

$$L_{sr,1}(u, \chi) = \sum_{f \in \mathcal{M}_q^{sr,1}} \chi(f) u^{\deg(f)} = \sum_{f \in \mathcal{M}_q^{sr,1}} \chi'(\Phi(f)) u^{2 \deg(\Phi(f))} = \sum_{g \in \mathcal{M}_q} \chi'(g) u^{2 \deg(g)} = L(u^2, \chi'),$$

as needed. \square

In particular, the Riemann Hypothesis over Function Fields gives us the following corollary:

Corollary 6.14. *Let χ be a non-trivial short interval character of ℓ coefficients. Then*

$$L_{sr,1}(u, \chi) = \prod_{i=1}^{\deg(L_{sr,1}(u, \chi))/2} (1 - \gamma'_i u^2),$$

with $|\gamma'_i| \in \{\sqrt{q}, 1\}$ for all i and $\deg(L_{sr,1}(u, \chi)) \leq 2(\ell - 1)$. (Note that γ'_i will have a dependence on χ .)

6.4 $\lambda(f)$ and $L_{sr,0}(u, \chi\lambda)$

We now turn to $L_{sr,0}(u, \chi\lambda)$.

Definition 6.15. Define the quadratic character $\chi_{sr}: \mathbb{F}_q[T] \rightarrow \{-1, 0, 1\}$ by

$$\chi_{sr}(f) = \left(\frac{f}{T^2 - 4} \right), \quad (6.10)$$

where $(\frac{\cdot}{\cdot})$ is the Jacobi symbol.

Set

$$S = \{f \in \mathcal{M}_q : (f, (T-2)(T+2)) = 1\}.$$

The following lemma is due to Carlitz [Car67]. We give an independent proof.

Lemma 6.16 (Carlitz). *For all $g \in S$, we have*

$$\lambda(\Psi(g)) = \chi_{sr}(g(T)). \quad (6.11)$$

Proof. Any element of S can be expressed as a product of squarefree elements of S . Since both sides of (6.11) are completely multiplicative, it suffices to establish (6.11) for squarefree $g \in S$.

One may verify that $\Psi|_S$ takes squarefree polynomials to squarefree polynomials. A formula due to Pellet [Con05, Lem. 4.1] gives

$$\lambda(f(T)) = (-1)^{\deg(f)} \chi_2(\text{Disc}(f)),$$

for any squarefree f , where $\text{Disc}(f)$ is the discriminant of f , and χ_2 is the unique non-trivial quadratic character of \mathbb{F}_q^\times , extended to \mathbb{F}_q by 0. As $\deg(\Psi(g)) = 2 \deg(g)$, we have

$$\lambda(\Psi(g)) = (-1)^{\deg(\Psi(g))} \chi_2(\text{Disc}(\Psi(g))) = \chi_2(\text{Disc}(\Psi(g))),$$

and so it suffices to show that

$$\chi_2(\text{Disc}(\Psi(g))) = \chi_{sr}(g)$$

for squarefree g . Writing g as $g(T) = \prod_{i=1}^n (T - \beta_i)$, we have $\Psi(g) = \prod_{i=1}^n (T - \alpha_i)(T - \alpha_i^{-1})$ where α_i are defined via $\alpha_i + \alpha_i^{-1} = \beta_i$, and so

$$\text{Disc}(\Psi(g)) = \prod_{i < j} (\alpha_i - \alpha_j)^2 \prod_{i < j} (\alpha_i^{-1} - \alpha_j^{-1})^2 \prod_{i,j} (\alpha_i - \alpha_j^{-1})^2 = A^2 \cdot B,$$

where

$$A = \prod_{i < j} (\alpha_i - \alpha_j)^2 \prod_{i < j} (\alpha_i \alpha_j - 1)^2 \prod_{i < j} (\alpha_i \alpha_j)^{-2}, \quad B = \prod_i (\alpha_i - \alpha_i^{-1})^2.$$

Since $\beta_i - \beta_j = (\alpha_i - \alpha_j)(\alpha_i \alpha_j - 1)(\alpha_i \alpha_j)^{-1}$ and $(2 - \beta_i)(-2 - \beta_i) = (\alpha_i - \alpha_i^{-1})^2$, we have

$$A = \text{Disc}(g), \quad B = g(2)g(-2),$$

and so $\chi_2(\text{Disc}(\Psi(g))) = \chi_2(\text{Disc}(g)^2) \chi_2(g(2)g(-2)) = \chi_2^2(\text{Disc}(g)) \chi_2(g(2)g(-2)) = \chi_{sr}(g)$, as needed. \square

Lemma 6.17. *The restriction $\Psi|_S$ is a bijection from S to $\mathcal{M}_q^{sr,0}$.*

Proof. As in the proof of the last part of Lemma 6.12, one can see that $\Psi(S \cap \mathcal{M}_{n,q}) \subseteq \mathcal{M}_{2n,q}^{sr,0}$, and a counting argument using Prop. 6.4 implies equality. \square

Proposition 6.18. *In the notation of Prop. 6.13 and (6.10),*

$$L_{sr,0}(u, \chi\lambda) = L(u^2, \chi' \chi_{sr}).$$

Proof. By Lemmas 6.16 and 6.17,

$$\begin{aligned} L_{sr,0}(u, \chi\lambda) &= \sum_{f \in \mathcal{M}_q^{sr,0}} \chi(f) \lambda(f) u^{\deg(f)} = \sum_{f \in \mathcal{M}_q^{sr,0}} \chi'(\Phi(f)) \lambda(f) u^{2 \deg(\Phi(f))} \\ &= \sum_{g \in S} \chi'(g) \lambda(\Psi(g)) u^{2 \deg(g)} = \sum_{g \in \mathcal{M}_q} \chi'(g) \chi_{sr}(g) u^{2 \deg(g)} = L(u^2, \chi' \chi_{sr}), \end{aligned}$$

as needed. \square

In particular, the Riemann Hypothesis over Function Fields gives us the following corollary:

Corollary 6.19. *Let χ be a short interval character of ℓ coefficients. Then*

$$L_{sr,0}(u, \chi\lambda) = \prod_{i=1}^{\deg(L_{sr,0}(u, \chi\lambda))/2} (1 - \gamma_i^\circ u^2),$$

with $|\gamma_i^\circ| \in \{\sqrt{q}, 1\}$ for all i and $\deg(L_{sr,0}(u, \chi\lambda)) \leq 2(\ell + 1)$. (Note that γ_i° will have a dependence on $\chi \cdot$)

6.5 Character sums over $\text{Sp}(2n, q)$

Theorem 6.20. *Let n be a positive integer. Let χ be a non-trivial short interval character of ℓ coefficients. We have (for $L_{Sp}(u, \chi)$ defined in (6.5))*

$$L_{Sp}(u, \chi) = \prod_{i=1}^d (1 - \gamma_i u^2)$$

with

$$d := \frac{\deg(L_{Sp}(u, \chi))}{2} \leq 2\ell. \quad (6.12)$$

1. We have the identity

$$\frac{1}{|\text{Sp}(2n, q)|} \sum_{M \in \text{Sp}(2n, q)} \chi(\text{CharPoly}(M)) = (-1)^n \sum_{a_1 + \dots + a_d = n} \prod_{j=1}^d \frac{\gamma_j^{a_j}}{(q^{2a_j} - 1) \dots (q^2 - 1)}. \quad (6.13)$$

2. If $d > 0$ then the following estimate holds:

$$\left| \frac{1}{|\text{Sp}(2n, q)|} \sum_{M \in \text{Sp}(2n, q)} \chi(\text{CharPoly}(M)) \right| \leq q^{-\frac{n^2}{d}} q^{\frac{n}{2}} \left(1 + \frac{1}{q^2 - 1}\right)^n \binom{n + d - 1}{n}. \quad (6.14)$$

Proof. By Corollaries 6.14 and 6.19 we have (6.12). The rest of the proof proceeds in the same way as the proof of Theorem 3.6 with two minor differences: when applying (2.10) to deduce (6.13), let $y = \gamma_j u$ and $V = q^2$, and in the passage from (6.13) to (6.14), we use the bound $|\gamma_i| \leq q\sqrt{q}$ which follows from Corollaries 6.14 and 6.19. \square

6.6 The distribution of the characteristic polynomial: superexponential bounds for $\text{Sp}(2n, q)$

Theorem 6.21. *Let $M \in \text{Sp}(2n, q)$ be a random matrix chosen according to Haar measure. Then for $0 \leq h < 2n - 1$ and for $f \in \mathcal{M}_{n, q}$,*

$$\left| \mathbb{P}_{M \in \text{Sp}(2n, q)}(\text{CharPoly}(M) \in I(f; h)) - \frac{q^{h+1}}{q^{2n}} \right| \leq q^{-\frac{n^2}{4n-2h-2}} q^{\frac{n}{2}} \left(1 + \frac{1}{q^2 - 1}\right)^n \binom{5n - 2h - 3}{n}.$$

Proof of Theorem 6.21. As in the proof of Theorem 1.3, from (3.15) we have

$$\mathbb{P}_{M \in \text{Sp}(2n, q)}(\text{CharPoly}(M) \in I(f; h)) = q^{-(2n-h-1)} \left(1 + \sum_{\substack{\chi \in G(R_{2n-h-1, 1, q}) \\ \chi \neq \chi_0}} \bar{\chi}(f) \frac{\sum_{M \in \text{Sp}(2n, q)} \chi(\text{CharPoly}(M))}{|\text{Sp}(2n, q)|} \right). \quad (6.15)$$

When n is fixed, the right hand side of (6.14) is monotone increasing in d . From (6.15) and (6.14), we have

$$\begin{aligned} \left| \mathbb{P}_{M \in \text{Sp}(2n, q)}(\text{CharPoly}(M) \in I(f; h)) - q^{-(2n-h-1)} \right| &\leq q^{-(2n-h-1)} \sum_{\substack{\chi \in G(R_{2n-h-1, 1, q}) \\ \chi \neq \chi_0}} \left| \frac{\sum_{M \in \text{Sp}(2n, q)} \chi(\text{CharPoly}(M))}{|\text{Sp}(2n, q)|} \right| \\ &\leq q^{-\frac{n^2}{d_1}} q^{\frac{n}{2}} \left(1 + \frac{1}{q^2 - 1}\right)^n \binom{n + d_1 - 1}{n}, \end{aligned}$$

where

$$d_1 = \max_{\substack{\chi \in G(R_{2n-h-1,1,q}) \\ \chi \neq \chi_0}} \deg(L_{Sp}(u, \chi))/2.$$

By (6.12) we have $d_1 \leq 2(2n - h - 1)$ which concludes the proof. \square

6.7 The distribution of traces: superexponential bounds for $\mathrm{Sp}(2n, q)$

Theorem 6.22. *Let $M \in \mathrm{Sp}(2n, q)$ be a random matrix chosen according to Haar measure. Fix a strictly increasing sequence b_1, \dots, b_k of positive integers coprime to p . Then for any sequence a_1, \dots, a_k of elements of elements from \mathbb{F}_q , we have*

$$\left| \mathbb{P}_{M \in \mathrm{Sp}(2n, q)} (\forall 1 \leq i \leq k : \mathrm{Tr}(M^{b_i}) = a_i) - q^{-k} \right| \leq q^{-\frac{n^2}{2b_k}} q^{\frac{n}{2}} \left(1 + \frac{1}{q^2 - 1}\right)^n \binom{n-1+2b_k}{n}.$$

The proof is omitted, as it follows closely the proof of Theorem 1.1.

6.8 The characteristic polynomial in very short intervals for $\mathrm{Sp}(2n, q)$

Finally we treat the case of short intervals which are sufficiently small that they contain few elements of $\mathcal{M}_{n,q}^{sr,1}$. In this space a polynomial is determined by only half its coefficients, and for this reason short intervals may contain no elements.

Indeed, from an analysis of the explicit formula (6.1) for \bar{f} one may prove

Proposition 6.23. *For any $f \in \mathcal{M}_{2n,q}$ and $h < 2n$, we have*

$$|\mathcal{M}_q^{sr,1} \cap I(f; h)| = \begin{cases} q^{h+1-n} & \text{if } h \geq n, \\ 1 & \text{if } h \leq n-1 \text{ and } f \in \mathcal{M}_q^{sr,1}, \\ 0 & \text{if } h \leq n-1 \text{ and } f \notin \mathcal{M}_q^{sr,1}. \end{cases}$$

Thus for h smaller than n one cannot expect characteristic polynomials to equidistribute in short intervals $I(f; h)$. For h only slightly larger than n however one may show that equidistribution occurs.

Theorem 6.24. *Let $M \in \mathrm{Sp}(2n, q)$ be a random matrix chosen according to Haar measure. Then for $n \leq h < 2n$ and $f \in \mathcal{M}_{2n,q}$,*

$$\left| \mathbb{P}_{M \in \mathrm{Sp}(2n, q)} (\mathrm{CharPoly}(M) \in I(f; h)) - \frac{q^{h+1}}{q^{2n}} \right| \leq B \frac{2n-h}{q^n},$$

where B is an absolute constant (independent of n, h and q).

This result implies equidistribution as long as $(h-n)/\log_q(n) \rightarrow \infty$.

Remark 13. The constant B in Theorem 6.24 can be seen to be the same constant as in Lemma 6.27 below. We give a crude bound for this constant after that lemma, but with additional tools (see Remark 14), it can be seen that one may take $B = 2$.

The proof of this result requires some changes from the proofs in previous sections but is nonetheless similar. For this reason the proofs that follow will be somewhat abbreviated.

For $g \in \mathcal{M}_q$, define the arithmetic functions

$$\begin{aligned} \beta^{Sp, \diamond}(g) &= \lambda(g) |g|^{1/2} \mathbf{1}_{\mathcal{M}_q^{sr,0}}(g), \\ \gamma^{Sp, \diamond}(g) &= \mathbf{1}_{\mathcal{M}_q^{sr,1}}(g), \end{aligned}$$

and further define

$$\alpha_i^{Sp, \diamond}(g) = \frac{1}{|g|^i} (\beta^{Sp, \diamond} * \gamma^{Sp, \diamond})(g)$$

for $i \geq 1$. For $f \in \mathcal{M}_q$, set

$$P_{Sp}^\diamond(f) = \lim_{k \rightarrow \infty} (\alpha_1^{Sp, \diamond} * \alpha_2^{Sp, \diamond} * \dots * \alpha_k^{Sp, \diamond})(f). \quad (6.16)$$

For notational reasons, we let $\sum^{sr,1}$ denote a sum with all summands restricted to $\mathcal{M}_q^{sr,1}$. We need the following lemmas.

Lemma 6.25. For $f \in \mathcal{M}_q$,

$$P_{Sp}(f) = \frac{1}{|f|^{1/2}} (\mathbf{1}_{\mathcal{M}_q^{sr,1}} * P_{Sp}^\diamond)(f) = \sum_{d, \delta: d\delta=f}^{sr,1} \frac{P_{Sp}^\diamond(\delta)}{|d\delta|^{1/2}}.$$

Proof. This follows from Theorem 6.10, following the same strategy as the proof of Lemma 5.19 for $U(n, q)$. \square

Lemma 6.26. For all $f \in \mathcal{M}_q$,

$$\lambda(f) P_{Sp}^\diamond(f) \geq 0.$$

Proof. Using Lemma 2.3 together with q -series identities one can verify, in the notation of Theorem 6.9, that if $f \in \mathcal{M}_q^{sr,1}$,

$$P_{Sp}^\diamond(f) = \frac{q^{2a(a-1)}}{|\mathrm{GL}(a, q^2)|} \frac{q^{2b(b-1)}}{|\mathrm{GL}(b, q^2)|} \prod_{i=1}^r \frac{q^{\frac{m_i e_i (e_i - 1)}{2}} (-1)^{e_i}}{|\mathrm{U}(e_i, q^{\frac{m_i}{2}})|} \prod_{j=1}^s \frac{q^{m'_j e'_j (e'_j - 1)}}{|\mathrm{GL}(e'_j, q^{m'_j})|}, \quad (6.17)$$

and if $f \notin \mathcal{M}_q^{sr,1}$ then $P_{Sp}^\diamond(f) = 0$. The lemma then follows from an examination of this formula. \square

Note that we have $P_{Sp}^\diamond(f) = 0$ if $\deg(f)$ is odd, because $\deg(f)$ is even for all $f \in \mathcal{M}_q^{sr,1}$ (see §6.1).

Lemma 6.27. There exists an absolute constant B such that for all $n \geq 0$ and all prime powers q ,

$$\sum_{f \in \mathcal{M}_{2n, q}} |P_{Sp}^\diamond(f)| \leq B.$$

Proof. We outline a proof using generating series. Define for $i = 0, 1$,

$$Z_{sr, i}(u) = \sum_{f \in \mathcal{M}_q^{sr, i}} u^{\deg(f)}, \quad Z_{sr, i}^\lambda(u) = \sum_{f \in \mathcal{M}_q^{sr, i}} \lambda(f) u^{\deg(f)}.$$

(These are just the already-defined L -functions at trivial characters, and the sums converge absolutely for $|u| < 1/\sqrt{q}$.) Corollary 6.7 implies that all elements of $\mathcal{M}_q^{sr,1}$ can be written uniquely as $(T-1)^a (T+1)^b g$ for a, b even and $g \in \mathcal{M}_q^{sr,0}$. This implies that

$$Z_{sr, 1}(u) = \frac{1}{(1-u^2)^2} Z_{sr, 0}(u), \quad Z_{sr, 1}^\lambda(u) = \frac{1}{(1-u^2)^2} Z_{sr, 0}^\lambda(u). \quad (6.18)$$

Theorem 6.10 (or Theorem 6.11) implies

$$\sum_{f \in \mathcal{M}_q} P_{Sp}(f) u^{\deg(f)} = \prod_{i=1}^{\infty} Z_{sr, 1}\left(\frac{u}{q^{i-1/2}}\right) Z_{sr, 0}^\lambda\left(\frac{u}{q^i}\right),$$

while the same reasoning implies

$$\sum_{f \in \mathcal{M}_q} \lambda(f) P_{Sp}^\diamond(f) u^{\deg(f)} = \prod_{i=1}^{\infty} Z_{sr, 0}\left(\frac{u}{q^{i-1/2}}\right) Z_{sr, 1}^\lambda\left(\frac{u}{q^i}\right).$$

Applying (6.18) to these identities, we have

$$\begin{aligned} \sum_{f \in \mathcal{M}_q} \lambda(f) P_{Sp}^\diamond(f) u^{\deg(f)} &= \left(\prod_{i=1}^{\infty} \frac{(1-u^2/q^{2i-1})^2}{(1-u^2/q^{2i})^2} \right) \left(\sum_{f \in \mathcal{M}_q} P_{Sp}(f) u^{\deg(f)} \right) \\ &= \left(\prod_{i=1}^{\infty} \frac{(1-u^2/q^{2i-1})^2}{(1-u^2/q^{2i})^2} \right) \frac{1}{1-u^2}, \end{aligned}$$

with the second line following from the fact that P_{Sp} is a probability measure on $\mathcal{M}_{2n, q}$. For notational reasons we write the product on the last line as $G(u^2, q) := \prod (1-u^2/q^{2i-1})^2 / (1-u^2/q^{2i})^2$.

We therefore have

$$\begin{aligned}
\sum_{f \in \mathcal{M}_{2n,q}} |P_{Sp}^\circ(f)| &= \sum_{f \in \mathcal{M}_{2n,q}} \lambda(f) P_{Sp}^\circ(f) \\
&= [u^{2n}] G(u^2, q) \frac{1}{1-u^2} \\
&= \frac{1}{2\pi i} \int_{|z|=\rho} G(z, q) \frac{1}{1-z} z^{-(n+1)} dz,
\end{aligned}$$

for any radius $\rho < 1$. Due to the rapid convergence of the product defining G , a little work shows

$$G(z, q) = G(1, q) + O(|z-1|), \quad \text{for } q \geq 2, |z| \leq 1,$$

where the implies constant is absolute. Thus for all $\rho < 1$,

$$\begin{aligned}
\sum_{f \in \mathcal{M}_{2n,q}} |P_{Sp}^\circ(f)| &= \frac{1}{2\pi i} \int_{|z|=\rho} \left(\frac{G(1, q)}{1-z} + O(1) \right) z^{-(n+1)} dz \\
&= G(1, q) + \frac{1}{2\pi i} \int_{|z|=\rho} O(|z|^{-(n+1)}) dz.
\end{aligned}$$

As $G(1, q) = O(1)$ and $\rho < 1$ is arbitrary, we can let $\rho \rightarrow 1^-$ and see that the above is bounded by an absolute constant as claimed. \square

The following two lemmas are proved analogously to Lemmas 5.20 and 5.21.

Lemma 6.28. *Take $n > 0$, $f \in \mathcal{M}_{2n,q}$, and $2n > h \geq n$. For $\delta \in \mathcal{M}_q^{sr,1}$, if $\deg(\delta) \leq 2h + 2 - 2n$, we have*

$$\sum_{d: d\delta \in I(f;h)}^{sr,1} 1 = \frac{q^{h+1}}{q^{2n}} \sum_{d: d\delta \in \mathcal{M}_{2n,q}}^{sr,1} 1. \quad (6.19)$$

In particular the above expression is constant as f ranges over $\mathcal{M}_{2n,q}$ for fixed n and q . Furthermore the right hand side of (6.19) simplifies. In fact for $\delta \in \mathcal{M}_q^{sr,1}$ and $\deg(\delta) \leq 2n$, we have

$$\frac{q^{h+1}}{q^{2n}} \sum_{d: d\delta \in \mathcal{M}_{2n,q}}^{sr,1} 1 = \frac{q^{h+1-n}}{|\delta|^{1/2}}.$$

Lemma 6.29. *For $n > 0$, $2n > h \geq n$ and $\delta \in \mathcal{M}_q^{sr,1}$, if $\deg(\delta) > 2h + 2 - 2n$, then*

$$\left| \sum_{d: d\delta \in I(f;h)}^{sr,1} 1 \right| \leq 1$$

for all $f \in \mathcal{M}_{2n,q}$.

Proof of Theorem 6.24. With the lemmas above, this proof follows in the same way as Theorems 1.4 and 5.18. \square

From Theorem 6.24 we may immediately deduce an analogous result for traces using Lemma 2.1.

Theorem 6.30. *Let $M \in \text{Sp}(2n, q)$ be a random matrix chosen according to Haar measure. Then for $1 \leq k \leq n-1$ and for $\{a_i\}_{1 \leq i \leq k, p \nmid i} \subseteq \mathbb{F}_q$, we have*

$$\left| \mathbb{P}_{M \in \text{Sp}(2n,q)}(\forall 1 \leq i \leq k, p \nmid i : \text{Tr}(M^i) = a_i) - \frac{1}{q^{k - \lfloor \frac{k}{p} \rfloor}} \right| \leq B \frac{(k+1)q^{\lfloor \frac{k}{p} \rfloor}}{q^n},$$

where B is an absolute constant (independent of n, k , and q).

7 Results for $O^+(n, q)$ and $O^-(n, q)$

In this section, q is an odd prime power.

7.1 $O^+(n, q)$, $O^-(n, q)$ and the space of characteristic polynomials

For any symmetric matrix $K \in \text{GL}(n, q)$, we define the orthogonal group preserving the quadratic form with matrix K to be

$$O(n, q, K) = \{g \in \text{GL}(n, q) : g^t K g = K\}.$$

When K_1 and K_2 are congruent, $O(n, q, K_1)$ and $O(n, q, K_2)$ are conjugate in $\text{GL}(n, q)$. Let χ_2 be the non-trivial quadratic character of \mathbb{F}_q^\times . For each n , there are two congruence classes for invertible symmetric matrices of size n : one for symmetric matrices with $\chi_2(\det(K)(-1)^{\lfloor \frac{n}{2} \rfloor}) = 1$ and another for symmetric matrices with $\chi_2(\det(K)(-1)^{\lfloor \frac{n}{2} \rfloor}) = -1$. For $\epsilon \in \{-, +\}$, we set

$$O^\epsilon(n, q) = O(n, q, K_n^\epsilon)$$

where K_n^ϵ is a symmetric matrix with $\chi_2(\det(K_n^\epsilon)(-1)^{\lfloor \frac{n}{2} \rfloor}) = \epsilon 1$. For odd n , given K_n^+ , one may choose K_n^- to be $K_n^- = cK_n^+$ for a non-square $c \in \mathbb{F}_q^\times$. This shows that $O^+(n, q)$ and $O^-(n, q)$ are always conjugate in $\text{GL}(n, q)$ (for odd n). Still, the distinction between the two groups will be useful. For even n , $O^+(n, q)$ and $O^-(n, q)$ are not isomorphic, and in fact have different orders.³

Proposition 7.1. [Tay92, Ch. 11] We have $|O(2n+1, q)| = 2q^{n^2} \prod_{i=1}^n (q^{2i} - 1)$, $|O^+(2n, q)| = 2q^{n^2-n} (q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$ and $|O^-(2n, q)| = 2q^{n^2-n} (q^n + 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$.

By definition, if $M \in O(n, q, K)$ then $M = K^{-1}(M^t)^{-1}K$, and so $\text{CharPoly}(M) = \text{CharPoly}((M^t)^{-1}) = \text{CharPoly}(M)$ where $f \mapsto \bar{f}$ is defined in Definition 6.2. Hence $\text{CharPoly}(M)$ is self-reciprocal, so that $\{\text{CharPoly}(M) : M \in O(n, q, K)\} \subseteq \mathcal{M}_{n,q}^{sr}$. In fact, from Theorem 7.3 below,

$$\cup_{\epsilon \in \{+, -\}} \{\text{CharPoly}(M) : M \in O^\epsilon(n, q)\} = \mathcal{M}_{n,q}^{sr}.$$

7.2 Expressions for $P_O^+(f)$ and $P_O^-(f)$

Definition 7.2. Fix $\epsilon \in \{+, -\}$. For $f \in \mathcal{M}_q$, we define the arithmetic function

$$P_O^\epsilon(f) = \mathbb{P}_{M \in O^\epsilon(n, q)}(\text{CharPoly}(M) = f) = \frac{|\{M \in O^\epsilon(n, q) : \text{CharPoly}(M) = f\}|}{|O^\epsilon(n, q)|}$$

with $n = \deg(f)$. For $f = 1$ we define $P_O^+(1) = 1$, $P_O^-(1) = 0$.

Fulman [Ful99, Thm. 20] has proved a closed formula for the sum of counts $|\{M \in O^+(n, q) : \text{CharPoly}(M) = f\}| + |\{M \in O^-(n, q) : \text{CharPoly}(M) = f\}|$. We have found it natural to phrase this formula in the language of probability as above.

Theorem 7.3 (Fulman). Suppose $f \in \mathcal{M}_q^{sr}$ factorizes as

$$f = (T-1)^a (T+1)^b \prod_{i=1}^r P_i^{e_i} \prod_{j=1}^s (Q_j \overline{Q_j})^{e'_j},$$

with $P_i = \overline{P_i}$ for all i and $Q_j \neq \overline{Q_j}$ for all j , with $P_i, Q_j \in \mathcal{M}_q \setminus \{T, T-1, T+1\}$ irreducible for all i, j . Set

$$m_i = \deg(P_i), \quad m'_j = \deg(Q_j).$$

Then

$$P_O^+(f) + P_O^-(f) = F(a)F(b) \prod_{i=1}^r \frac{q^{\frac{m_i e_i (e_i - 1)}{2}}}{|U(e_i, q^{\frac{m_i}{2}})|} \prod_{j=1}^s \frac{q^{m'_j e'_j (e'_j - 1)}}{|GL(e'_j, q^{m'_j})|},$$

where

$$F(n) := \begin{cases} |\text{Sp}(n, q)|^{-1} q^{\frac{1}{2}n^2} & \text{if } n \equiv 0 \pmod{2}, \\ |\text{Sp}(n-1, q)|^{-1} q^{\frac{1}{2}(n-1)^2} & \text{if } n \equiv 1 \pmod{2}. \end{cases}$$

If f is a monic polynomial but $f \notin \mathcal{M}_q^{sr}$, then $P_O^+(f) = P_O^-(f) = 0$.

We have the following formula for $P_O^+(f) - P_O^-(f)$, which does not seem to have appeared in the literature, but which follows from Fulman's methods. We fill in the details of the proof in an appendix.

Theorem 7.4. In the notation of Theorem 7.3 and (6.16),

$$P_O^+ - P_O^- = P_{Sp}^\circ.$$

³Concrete choices for K_n^+ and K_n^- can be found in [Ful99, §4.3] for instance.

Remark 14. Theorem 7.4 can be used to quickly give an alternative proof of Lemma 6.27 with $B = 2$.

By definition $P_O^+ - P_O^- = P_{Sp}^\circ$ is an infinite Dirichlet convolution of simple arithmetic functions defined on \mathcal{M}_q . The same is true for $P_O^+ + P_O^-$ as well.

Theorem 7.5. *For $g \in \mathcal{M}_q$, define the arithmetic function*

$$\Delta(g) = \mathbf{1}_{g|T^2-1}.$$

Then for $f \in \mathcal{M}_q$,

$$P_O^+ + P_O^- = \Delta * P_{Sp}. \quad (7.1)$$

One may verify (7.1) directly using Theorems 6.9 and 7.3.

We also need the following theorem.

Theorem 7.6. *For any Hayes character χ , let*

$$L_O(u, \chi) = L_{sr,0}(\sqrt{q}u, \chi\lambda)L_{sr,1}(u, \chi). \quad (7.2)$$

For $|u| < 1$ we have

$$\sum_{f \in \mathcal{M}_q} (P_O^+(f) - P_O^-(f))\chi(f)u^{\deg(f)} = \prod_{i=1}^{\infty} L_O\left(\frac{u}{q^i}, \chi\right) = L_{sr,0}\left(\frac{u}{\sqrt{q}}, \chi\lambda\right) \prod_{i=1}^{\infty} L_{Sp}\left(\frac{u}{q^{1/2+i}}, \chi\right), \quad (7.3)$$

with both the left hand sum and the right hand product converging absolutely.

The proof is a direct consequence of (6.16). In fact, we may show the following.

Proposition 7.7. *For all $f \in \mathcal{M}_q$,*

$$P_{Sp}^\circ(f) = \sum_{\substack{d, \delta: d\delta=f \\ d \in \mathcal{M}_q^{sr,0}}}^{sr,1} \frac{\lambda(d)P_{Sp}(\delta)}{|d\delta|^{1/2}}.$$

7.3 Character sums over $O^+(n, q)$, $O^-(n, q)$

Theorem 7.8. *Let n be a positive integer. Let χ be a Hayes character of the form χ_1 or $\chi_1 \cdot \chi_T$, where χ_1 is a non-trivial short interval character of ℓ coefficients and χ_T is a Dirichlet character modulo T . For $L_{Sp}(u, \chi)$ defined in (6.5), we have the factorization*

$$L_{Sp}(u, \chi) = \prod_{i=1}^d (1 - \gamma_i u^2), \quad (7.4)$$

and for $L_O(u, \chi)$ defined in (7.2), we have the factorization

$$L_O(u, \chi) = \prod_{i=1}^{d^\dagger} (1 - \gamma_i^\dagger u^2) \quad (7.5)$$

with

$$d = d^\dagger \leq 2\ell. \quad (7.6)$$

(Note that γ_i, γ_j' will have a dependence on χ .)

1. *We have the following identities. For odd n ,*

$$\begin{aligned} & \frac{1}{|O^+(n, q)|} \sum_{M \in O^+(n, q)} \chi(\text{CharPoly}(M)) + \frac{1}{|O^-(n, q)|} \sum_{M \in O^-(n, q)} \chi(\text{CharPoly}(M)) \\ &= (-1)^{\frac{n-1}{2}} (\chi(T-1) + \chi(T+1)) \sum_{a_1 + \dots + a_d = (n-1)/2} \prod_{j=1}^d \frac{\gamma_j^{a_j}}{(q^{2a_j} - 1) \dots (q^2 - 1)} \end{aligned} \quad (7.7)$$

and (still for odd n)

$$\frac{1}{|O^+(n, q)|} \sum_{M \in O^+(n, q)} \chi(\text{CharPoly}(M)) - \frac{1}{|O^-(n, q)|} \sum_{M \in O^-(n, q)} \chi(\text{CharPoly}(M)) = 0. \quad (7.8)$$

And for even n ,

$$\begin{aligned} & \frac{1}{|\mathcal{O}^+(n, q)|} \sum_{M \in \mathcal{O}^+(n, q)} \chi(\text{CharPoly}(M)) + \frac{1}{|\mathcal{O}^-(n, q)|} \sum_{M \in \mathcal{O}^-(n, q)} \chi(\text{CharPoly}(M)) \\ &= (-1)^{\frac{n}{2}} \left(\sum_{a_1 + \dots + a_d = n/2} \prod_{j=1}^d \frac{\gamma_j^{a_j}}{(q^{2a_j} - 1) \dots (q^2 - 1)} - \chi(T^2 - 1) \sum_{a_1 + \dots + a_d = (n-2)/2} \prod_{j=1}^d \frac{\gamma_j^{a_j}}{(q^{2a_j} - 1) \dots (q^2 - 1)} \right) \end{aligned} \quad (7.9)$$

and (still for even n)

$$\begin{aligned} & \frac{1}{|\mathcal{O}^+(n, q)|} \sum_{M \in \mathcal{O}^+(n, q)} \chi(\text{CharPoly}(M)) - \frac{1}{|\mathcal{O}^-(n, q)|} \sum_{M \in \mathcal{O}^-(n, q)} \chi(\text{CharPoly}(M)) \\ &= (-1)^{\frac{n}{2}} \sum_{a_1 + \dots + a_d = n/2} \prod_{j=1}^d \frac{\gamma_j^{\dagger a_j}}{(q^{2a_j} - 1) \dots (q^2 - 1)}. \end{aligned} \quad (7.10)$$

2. The following estimate holds for $\epsilon \in \{\pm\}$:

$$\left| \frac{1}{|\mathcal{O}^\epsilon(n, q)|} \sum_{M \in \mathcal{O}^\epsilon(n, q)} \chi(\text{CharPoly}(M)) \right| \leq 3q^{-\frac{(n-2)^2}{4d}} q^{\frac{n}{4}} \left(1 + \frac{1}{q^2 - 1}\right)^{\frac{n}{2}} \left(\frac{n}{2} + d - 1\right). \quad (7.11)$$

Proof. Note that all $f \in \mathcal{M}_q^{sr,1}$ satisfy $f(0) = 1$, and so any Dirichlet character modulo T is identically 1 on $\mathcal{M}_q^{sr,1}$. It follows that $L_{sr,1}(u, \chi) = L_{sr,1}(u, \chi\chi_T)$ and $L_{sr,0}(u, \chi\lambda) = L_{sr,0}(u, \chi\chi_T\lambda)$, where χ is any short interval character. Hence (7.4) was already proved in Theorem 6.20. (7.5) and the degree bound (7.6) follow from Corollaries 6.14 and 6.19. The equality $d = d^\dagger$ follows from the fact that $\deg L_{sr,1}(u, \chi) = \deg L_{sr,1}(\sqrt{q}u, \chi)$ and similarly $\deg L_{sr,0}(u, \chi\lambda) = \deg L_{sr,0}(\sqrt{q}u, \chi\lambda)$.

For the exact formulas (7.7), (7.9), note that

$$\begin{aligned} & \frac{1}{|\mathcal{O}^+(n, q)|} \sum_{M \in \mathcal{O}^+(n, q)} \chi(\text{CharPoly}(M)) + \frac{1}{|\mathcal{O}^-(n, q)|} \sum_{M \in \mathcal{O}^-(n, q)} \chi(\text{CharPoly}(M)) \\ &= \sum_{f \in \mathcal{M}_{n,q}} (P_O^+(f) + P_O^-(f)) \chi(f) = [u^n] (1 + \chi(T-1)u) (1 + \chi(T+1)u) \prod_{i=1}^{\infty} L_{sp}\left(\frac{u}{q^i}, \chi\right) \end{aligned}$$

with the second equality following from (7.1) and (6.6). For the exact formulas (7.8), (7.10) note that

$$\begin{aligned} & \frac{1}{|\mathcal{O}^+(n, q)|} \sum_{M \in \mathcal{O}^+(n, q)} \chi(\text{CharPoly}(M)) - \frac{1}{|\mathcal{O}^-(n, q)|} \sum_{M \in \mathcal{O}^-(n, q)} \chi(\text{CharPoly}(M)) \\ &= \sum_{f \in \mathcal{M}_{n,q}} (P_O^+(f) - P_O^-(f)) \chi(f) = [u^n] \prod_{i=1}^{\infty} L_o\left(\frac{u}{q^i}, \chi\right) \end{aligned}$$

with the second equality following from (7.3). Using (7.4) and (7.5) we obtain

$$\begin{aligned} & \frac{1}{|\mathcal{O}^+(n, q)|} \sum_{M \in \mathcal{O}^+(n, q)} \chi(\text{CharPoly}(M)) + \frac{1}{|\mathcal{O}^-(n, q)|} \sum_{M \in \mathcal{O}^-(n, q)} \chi(\text{CharPoly}(M)) \\ &= [u^n] (1 + \chi(T-1)u) (1 + \chi(T+1)u) \prod_{j=1}^d \prod_{i=1}^{\infty} (1 - \gamma_j \frac{u^2}{q^{2i}}) \end{aligned} \quad (7.12)$$

and

$$\begin{aligned} & \frac{1}{|\mathcal{O}^+(n, q)|} \sum_{M \in \mathcal{O}^+(n, q)} \chi(\text{CharPoly}(M)) - \frac{1}{|\mathcal{O}^-(n, q)|} \sum_{M \in \mathcal{O}^-(n, q)} \chi(\text{CharPoly}(M)) \\ &= [u^n] \prod_{j=1}^d \prod_{i=1}^{\infty} (1 - \gamma_j^{\dagger} \frac{u^2}{q^{2i}}). \end{aligned} \quad (7.13)$$

Using (2.10) with $y = \gamma_j u^2$ and $V = q^2$, we have

$$\prod_{i=1}^{\infty} (1 - \gamma_j \frac{u^2}{q^{2i}}) = \sum_{a \geq 0} \frac{(-1)^a \gamma_j^a u^{2a}}{(q^{2a} - 1)(q^{2(a-1)} - 1) \cdots (q^2 - 1)},$$

which together with (7.12) and (7.13) gives (7.7), (7.9) and (7.8), (7.9). (Note that (7.8) follows more simply: for odd n , the groups $O^+(n, q)$ and $O^-(n, q)$ are conjugate.)

We may bound (7.7), (7.9) much in the same way as in the proof of Theorem 3.6, and obtain

$$\begin{aligned} & \left| \frac{1}{|O^+(n, q)|} \sum_{M \in O^+(n, q)} \chi(\text{CharPoly}(M)) + \frac{1}{|O^-(n, q)|} \sum_{M \in O^-(n, q)} \chi(\text{CharPoly}(M)) \right| \\ & \leq 2q^{\frac{n}{4}} \left(1 + \frac{1}{q^2 - 1}\right)^{\frac{n}{2}} \binom{\frac{n}{2} + d - 1}{\frac{n}{2}} q^{-\frac{(n-2)^2}{4d}}. \end{aligned}$$

Bounding (7.10) is similar, and gives

$$\begin{aligned} & \left| \frac{1}{|O^+(n, q)|} \sum_{M \in O^+(n, q)} \chi(\text{CharPoly}(M)) - \frac{1}{|O^-(n, q)|} \sum_{M \in O^-(n, q)} \chi(\text{CharPoly}(M)) \right| \\ & \leq q^{\frac{n}{4}} \left(1 + \frac{1}{q^2 - 1}\right)^{\frac{n}{2}} \binom{\frac{n}{2} + d - 1}{\frac{n}{2}} q^{-\frac{n^2}{4d}}. \end{aligned}$$

Together, we obtain (7.11). \square

Remark 15. In the next subsections we only use Theorem 7.8 with χ a short interval character. We have recorded the theorem for more general characters because it is possible to extend our later results from $O^\epsilon(n, q)$ to $SO^\epsilon(n, q)$ using the more general characters.

7.4 The distribution of the characteristic polynomial: superexponential bounds for $O^+(n, q)$, $O^-(n, q)$

Theorem 7.9. Fix $\epsilon \in \{-, +\}$. Let $M \in O^\epsilon(n, q)$ be a random matrix chosen according to Haar measure. Then for $0 \leq h < n - 1$ and for $f \in \mathcal{M}_{n, q}$,

$$\left| \mathbb{P}_{M \in O^\epsilon(n, q)}(\text{CharPoly}(M) \in I(f; h)) - \frac{q^{h+1}}{q^n} \right| \leq 3q^{-\frac{(n-2)^2}{8(n-h-1)}} q^{\frac{n}{4}} \left(1 + \frac{1}{q^2 - 1}\right)^{\frac{n}{2}} \binom{\frac{5n}{2} - 2h - 3}{\frac{n}{2}}.$$

The proof proceeds along the lines of the proof of Theorem 1.3.

7.5 The distribution of traces: superexponential bounds for $O^+(n, q)$, $O^-(n, q)$

Theorem 7.10. Fix $\epsilon \in \{-, +\}$. Let $M \in O^\epsilon(n, q)$ be a random matrix chosen according to Haar measure. Fix a strictly increasing sequence b_1, \dots, b_k of positive integers coprime to p . Then for any sequence a_1, \dots, a_k of elements of elements from \mathbb{F}_q , we have

$$\left| \mathbb{P}_{M \in O^\epsilon(n, q)}(\forall 1 \leq i \leq k : \text{Tr}(M^{b_i}) = a_i) - q^{-k} \right| \leq 3q^{-\frac{(n-2)^2}{8b_k}} q^{\frac{n}{4}} \left(1 + \frac{1}{q^2 - 1}\right)^{\frac{n}{2}} \binom{\frac{n}{2} + 2b_k - 1}{\frac{n}{2}}.$$

The proof is omitted, as it follows closely the proof of Theorem 1.1.

7.6 The characteristic polynomial in very short intervals for $O^+(n, q)$, $O^-(n, q)$

As for other groups, an element of \mathcal{M}_q^{sr} is described by roughly half its coefficients and so there may exist short intervals with no elements of \mathcal{M}_q^{sr} .

From an analysis of the involution \bar{f} of Definition 6.2, considering odd and even degrees separately, one may prove

Proposition 7.11. *For any $f \in \mathcal{M}_{n,q}$ and $h < n$, we have*

$$|\mathcal{M}_q^{sr} \cap I(f; h)| = \begin{cases} q^{h+1-\lceil n/2 \rceil} + q^{h+1-\lceil (n+1)/2 \rceil} & \text{if } h \geq \lceil n/2 \rceil, \\ O(1) & \text{if } h < \lceil n/2 \rceil. \end{cases}$$

Hence as before we cannot expect equidistribution at all scales. But the same phenomenon we have seen for all other groups persists: as long as h is slightly larger than $n/2$, equidistribution of the characteristic polynomial in intervals $I(f; h)$ occurs for both the groups $O^+(n, q)$ and $O^-(n, q)$.

Theorem 7.12. *Fix $\epsilon \in \{-, +\}$. Let $M \in O^\epsilon(n, q)$ be a random matrix chosen according to Haar measure. Then for $n \geq 3$ and $(n+1)/2 \leq h < n$, if $f \in \mathcal{M}_{n,q}$,*

$$\left| \mathbb{P}_{M \in O^\epsilon(n,q)}(\text{CharPoly}(M) \in I(f; h)) - \frac{q^{h+1}}{q^n} \right| \leq C \frac{n-h}{q^{n/2-1}},$$

where C is an absolute constant (independent of n, h and q).

This result implies equidistribution as long as $(h - n/2)/\log_q(n) \rightarrow \infty$.

Remark 16. More careful book-keeping shows that the argument below allows one to replace the upper bound $C(n-h)/q^{n/2-1}$ by $2(n-h+1)/q^{n/2-1}$.

Theorem 7.12 is a consequence of estimates below for sums over short intervals of $P_O^+(f) + P_O^-(f)$ and $P_O^+(f) - P_O^-(f)$. For notational reasons, we let $\sum^{sr,0}$ denote a sum with all summands restricted to $\mathcal{M}_q^{sr,0}$.

Lemma 7.13 (An estimate for $P_O^+ + P_O^-$). *For $n \geq 3$ and $(n+1)/2 \leq h < n$, if $f \in \mathcal{M}_{n,q}$,*

$$\sum_{g \in I(f; h)} (P_O^+(g) + P_O^-(g)) = 2 \frac{q^{h+1}}{q^n} + O\left(\frac{n-h}{q^{n/2-1}}\right),$$

where the implied constant is absolute.

Proof. Note that from Theorem 7.5,

$$\begin{aligned} \sum_{g \in I(f; h)} (P_O^+(g) + P_O^-(g)) &= \sum_{g \in I(f; h)} (\Delta * P_{Sp})(g) \\ &= \sum_{g \in I(f; h)} P_{Sp}(g) + \sum_{(T+1)g \in I(f; h)} P_{Sp}(g) \\ &\quad + \sum_{(T-1)g \in I(f; h)} P_{Sp}(g) + \sum_{(T^2-1)g \in I(f; h)} P_{Sp}(g). \end{aligned}$$

Because P_{Sp} is supported on even degree polynomials, this simplifies to

$$= \begin{cases} \sum_{(T+1)g \in I(f; h)} P_{Sp}(g) + \sum_{(T-1)g \in I(f; h)} P_{Sp}(g) & \text{for } n = \deg(f) \text{ odd,} \\ \sum_{g \in I(f; h)} P_{Sp}(g) + \sum_{(T^2-1)g \in I(f; h)} P_{Sp}(g) & \text{for } n = \deg(f) \text{ even.} \end{cases}$$

But from Theorem 6.24, considering the case of odd and even n separately, one can verify that if n is odd and $(n+1)/2 \leq h < n$, or if n even and $n/2 + 1 \leq h < n$, the above is

$$= 2 \frac{q^{h+1}}{q^n} + O\left(\frac{n-h}{q^{n/2-1}}\right).$$

Inspecting these ranges of h for odd and even n verifies the claim of the lemma. \square

Lemma 7.14 (An estimate for $P_O^+ - P_O^-$). *For $n \geq 3$ and $(n+1)/2 \leq h < n$, if $f \in \mathcal{M}_{n,q}$,*

$$\sum_{g \in I(f; h)} (P_O^+(g) - P_O^-(g)) = O\left(\frac{n-h}{q^{n/2-1}}\right),$$

where the implied constant is absolute.

If n is odd this is evident – in fact the left hand side is 0 from Theorem 7.4. In the case that n is even we will need the following two preliminary lemmas.

Lemma 7.15. *If n is even, for $(n+1)/2 \leq h < n$ and $\delta \in \mathcal{M}_q^{sr,1}$, if $\deg(\delta) \leq 2h - n - 2$, then*

$$\sum_{d: d\delta \in I(f;h)}^{sr,0} \lambda(d) = 0$$

for any $f \in \mathcal{M}_{n,q}$. In particular the above expression is constant as f ranges over $\mathcal{M}_{n,q}$, for fixed n and q .

Proof. Let $\Delta = \deg(\delta)$. For $\Delta \leq 2h - n - 2$, we have $n - \Delta \geq 2(n - h - 1) + 4$. Yet

$$\sum_{d: d\delta \in I(f;h)}^{sr,0} \lambda(d) = \frac{1}{q^{n-h-1}} \sum_{\chi \in G(R_{n-h-1,1,q})} \bar{\chi}(f) \sum_{d \in \mathcal{M}_{n-\Delta,q}^{sr,0}} \lambda(d) \chi(d) \chi(\delta).$$

For $\chi \in G(R_{n-h-1,1,q})$, the inner sum above evaluates to 0 by Corollary 6.19. \square

Lemma 7.16. *If n is even, for $n > h \geq n/2$ and $\delta \in \mathcal{M}_q^{sr,1}$, if $\deg(\delta) \geq 2h - n$, then*

$$\left| \sum_{d: d\delta \in I(f;h)}^{sr,0} 1 \right| \leq q$$

for all $f \in \mathcal{M}_{n,q}$.

Proof. As $\mathcal{M}_q^{sr,0} \subseteq \mathcal{M}_q^{sr,1}$, we have,

$$\left| \sum_{d: d\delta \in I(f;h)}^{sr,0} 1 \right| \leq \left| \sum_{d: d\delta \in I(f;h)}^{sr,1} 1 \right| \leq q,$$

using Lemmas 6.28 and 6.29 for the final bound. \square

Remark 17. If $\deg(\delta) \geq 2h - n + 2$, then we can replace q with 1, but we do not use this.

Proof of Lemma 7.14. We can assume n is even, since otherwise as already noted the left hand side is 0. Theorem 7.4 reduces the lemma to evaluating short interval sums of P_{Sp}° .

From Proposition 7.7, one has

$$\sum_{g \in I(f;h)} P_{Sp}^\circ(g) = \sum_{d, \delta: d\delta \in I(f;h)}^{sr,0} \frac{\lambda(d) P_{Sp}(\delta)}{|d\delta|^{1/2}}.$$

Using Lemma 7.15, it follows that this sum may be restricted to δ with $2h - n \leq \deg(\delta) \leq n$; the contribution from δ not in this range sums to 0. On the other hand, by Lemma 7.16 and the fact that $P_{Sp}(\delta)$ is a probability measure for $\delta \in \mathcal{M}_{k,q}$ for even k , the magnitude of the above expression is then no more than

$$\sum_{\substack{d, \delta: d\delta \in I(f;h) \\ 2h-n \leq \deg(\delta) \leq n}}^{sr,0} \frac{P_{Sp}(\delta)}{|d\delta|^{1/2}} \leq \frac{1}{q^{n/2}} q \cdot ([n - (2h - n)]/2 + 1) = \frac{n - h + 1}{q^{n/2-1}},$$

which yields the claimed bound. \square

Proof of Theorem 7.12. This is just a matter of differencing the estimates in Lemmas 7.13 and 7.14. \square

From Theorem 7.12 we may immediately deduce an analogous result for traces using Lemma 2.1.

Theorem 7.17. *Fix $\epsilon \in \{-, +\}$. Let $M \in \mathcal{O}^\epsilon(n, q)$ be a random matrix chosen according to Haar measure. Then for $n \geq 3$, and $1 \leq k \leq (n-1)/2$ and for $\{a_i\}_{1 \leq i \leq k, p \nmid i} \subseteq \mathbb{F}_q$, we have*

$$\left| \mathbb{P}_{M \in \mathcal{O}^\epsilon(n, q)}(\forall 1 \leq i \leq k, p \nmid i : \text{Tr}(M^i) = a_i) - \frac{1}{q^{k - \lfloor \frac{k}{p} \rfloor}} \right| \leq C \frac{(k+1)q^{\lfloor \frac{k}{p} \rfloor}}{q^{n/2-1}},$$

where C is an absolute constant (independent of n, k , and q).

A Cycle indices for $\mathcal{O}^+(n, q)$ and $\mathcal{O}^-(n, q)$

We fill in the proof of Theorem 7.4. It is largely based on Fulman's paper [Ful99, §4.3, §6.1], and we refer the reader to this source for further details.

A.1 Parametrization of conjugacy classes

We describe a parametrization of the conjugacy classes in $O^+(n, q)$ and $O^-(n, q)$, due to Wall [Wal63, pp. 38-40]. Here we think of $O^+(n, q)$, $O^-(n, q)$ as disjoint, abstract groups. Denote by $\mathcal{P}_q \subseteq \mathcal{M}_q$ the subset of monic irreducible polynomials, not including T , and by \mathbb{Y} the set of partitions, which includes the empty partition.

An “orthogonal signed partition” λ^\pm is a partition of some natural number $|\lambda^\pm|$ such that the even parts have even multiplicity, together with a choice of sign for the set of parts of size i for each odd i . We denote by \mathbb{Y}_O the set of all orthogonal signed partitions. There is a certain way to associate with each $g \in O^+(n, q) \cup O^-(n, q)$ a pair of functions $\lambda_P(g): \mathcal{P}_q \setminus \{T \pm 1\} \rightarrow \mathbb{Y}$, $\lambda_P^\pm(g): \{T \pm 1\} \rightarrow \mathbb{Y}_O$ which enjoys several properties:

- $g_1, g_2 \in O^\epsilon(n, q)$ are conjugate in $O^\epsilon(n, q)$ if and only if $\lambda_P(g_1) = \lambda_P(g_2)$ for all $P \in \mathcal{P}_q \setminus \{T \pm 1\}$ and $\lambda_P^\pm(g_1) = \lambda_P^\pm(g_2)$ for all $P \in \{T \pm 1\}$ ($\epsilon \in \{+, -\}$).
- The pairs of functions $(\lambda_P(g), \lambda_P^\pm(g))$, $(\lambda_P(h), \lambda_P^\pm(h))$ are distinct if $g \in O^+(n, q)$ while $h \in O^-(n, q)$.
- $|\lambda_P| = |\lambda_{\bar{P}}|$ and $\sum_{P \in \{T \pm 1\}} |\lambda_P^\pm| \deg(P) + \sum_{P \in \mathcal{P}_q \setminus \{T \pm 1\}} |\lambda_P| \deg(P) = n$.
- The characteristic polynomial of $g \in O^+(n, q) \cup O^-(n, q)$ is

$$\text{CharPoly}(g) = \prod_{P \in \{T \pm 1\}} P^{|\lambda_P^\pm(g)|} \prod_{P \in \mathcal{P}_q \setminus \{T \pm 1\}} P^{|\lambda_P(g)|}.$$

A.2 Cycles indices for $O^+(n, q)$, $O^-(n, q)$

Definition A.1. *The cycle indices for $O^+(n, q)$, $O^-(n, q)$ are the following polynomials in variables $\mathbf{x} = \{x_{P, \lambda}\}_{P \in \mathcal{P}_q \setminus \{T \pm 1\}, \lambda \in \mathbb{Y}} \cup \{x_{P, \lambda^\pm}\}_{P \in \{T \pm 1\}, \lambda \in \mathbb{Y}_O}$:*

$$Z(O^+(n, q), \mathbf{x}) = \frac{1}{|O^+(n, q)|} \sum_{g \in O^+(n, q)} \prod_{P \in \{T \pm 1\}} x_{P, \lambda_P^\pm(g)} \prod_{P \in \mathcal{P}_q \setminus \{T \pm 1\}} x_{P, \lambda_P(g)},$$

$$Z(O^-(n, q), \mathbf{x}) = \frac{1}{|O^-(n, q)|} \sum_{g \in O^-(n, q)} \prod_{P \in \{T \pm 1\}} x_{P, \lambda_P^\pm(g)} \prod_{P \in \mathcal{P}_q \setminus \{T \pm 1\}} x_{P, \lambda_P(g)}.$$

Fulman has proved the following identity of formal power series [Ful99, Thm. 14]

$$1 + \sum_{n \geq 1} (Z(O^+(n, q), \mathbf{x}) + Z(O^-(n, q), \mathbf{x})) u^n$$

$$= \left(\sum_{\lambda^\pm \in \mathbb{Y}_O} x_{T-1, \lambda^\pm} \frac{u^{|\lambda^\pm|}}{c_{O, q}(\lambda^\pm)} \right) \left(\sum_{\lambda^\pm \in \mathbb{Y}_O} x_{T+1, \lambda^\pm} \frac{u^{|\lambda^\pm|}}{c_{O, q}(\lambda^\pm)} \right)$$

$$\prod_{P=\bar{P}} \left(\sum_{\lambda \in \mathbb{Y}} x_{P, \lambda} \frac{(-u^{\deg(P)})^{|\lambda|}}{c_{GL, -q^{\deg(P)/2}}(\lambda)} \right) \prod_{Q \neq \bar{Q}} \left(\sum_{\lambda \in \mathbb{Y}} x_{Q, \lambda} x_{\bar{Q}, \lambda} \frac{u^{|\lambda| \deg(Q\bar{Q})}}{c_{GL, q^{\deg(Q)}}(\lambda)} \right), \quad (\text{A.1})$$

where $c_{GL, z}(\lambda)$ is a rational function satisfying the following identity due to Stong [Sto88, Lem. 6, Prop. 19]

$$\sum_{\lambda \in \mathbb{Y}} \frac{u^{|\lambda|}}{c_{GL, z}(\lambda)} = \sum_{j \geq 0} \frac{z^{j(j-1)}}{\prod_{i=0}^{j-1} (z^j - z^i)} u^j \quad (\text{A.2})$$

for $|u| \leq 1 < |z|$, and $c_{O, z}(\lambda^\pm)$ is also a rational function in z .

A.3 The Witt group of \mathbb{F}_q , q odd

Let q be an odd prime power, and let $W(\mathbb{F}_q)$ be the Witt group of \mathbb{F}_q , considered as an additive group (we ignore the multiplicative structure). For a non-degenerate quadratic form Q over \mathbb{F}_q , we denote its equivalence class in $W(\mathbb{F}_q)$ by $[Q]$. It is useful to extend the notation $[\cdot]$ as follows. For a symmetric matrix $K \in \text{GL}(n, q)$, we write $[O(n, q, K)]$ for the equivalence class in $W(\mathbb{F}_q)$ of the quadratic form associated with K .

Fixing a non-square element $c \in \mathbb{F}_q^\times$, the elements of the Witt group $W(\mathbb{F}_q)$ may be described as follows:

$$W(\mathbb{F}_q) = \{[0], [x^2], [cx^2], [x^2 - cy^2]\}.$$

If $q \equiv 1 \pmod{4}$, we identify $W(\mathbb{F}_q)$ with the group $(\mathbb{Z}/2\mathbb{Z})^2$ as follows:

$$[0] = (0, 0), [x^2] = (1, 0), [cx^2] = (1, 1), [x^2 - cy^2] = (0, 1).$$

One can verify from [Ful99, Prop. 1] that

$$[O^\epsilon(n, q)] = (n \bmod 2, \epsilon')$$

for all n and $\epsilon \in \{\pm\}$, where $\epsilon' = 0$ if $\epsilon = +$ and $\epsilon' = 1$ if $\epsilon = -$.

If $q \equiv 3 \pmod{4}$, we identify $W(\mathbb{F}_q)$ with the group $\mathbb{Z}/4\mathbb{Z}$ as follows:

$$[0] = 0, [x^2] = 1, [cx^2] = 3, [x^2 - cy^2] = 2.$$

One can verify from [Ful99, Prop. 1] that

$$[O^\epsilon(n, q)] = (n \bmod 2) + 2\epsilon'$$

for all n and $\epsilon \in \{\pm\}$, where $(n \bmod 2)$ is the unique integer in $\{0, 1\}$ congruent to n modulo 2.

If $g \in O^\epsilon(n, q)$ for some ϵ and n , we set $[g] := [O^\epsilon(n, q)]$.

A.4 Cycles indices twisted by characters of $W(\mathbb{F}_q)$

We give a generalization of (A.1) which requires some notation. If i is an odd integer appearing in λ^\pm , let us denote by $\epsilon_i(\lambda^\pm)$ its sign and by $m_i(\lambda^\pm)$ the multiplicity in which i appears. As shown by Wall [Wal63, pp. 38-40] (cf. [Ful99, Thm. 13]), given $g \in O^\epsilon(n, q)$ for some $\epsilon \in \{\pm\}$, the precise orthogonal group to which g belongs may be determined by the data $\lambda_{T\pm 1}^\pm(g)$, $\lambda_P(g)$ as follows:

$$[g] = \sum_{\substack{P \in \{T-1, T+1\} \\ i \text{ odd}}} [O^{\epsilon_i(\lambda_P^\pm(g))}(m_i(\lambda_P^\pm(g)))] + [x^2 - cy^2] \sum_{P \in \mathcal{P}_q \setminus \{T-1, T+1\}} |\lambda_P(g)|.$$

Let $\psi: W(\mathbb{F}_q) \rightarrow \mathbb{C}^\times$ be a multiplicative character, and set $\psi(\lambda^\pm) = \psi\left(\sum_{i \text{ odd}} [O^{\epsilon_i(\lambda^\pm(g))}(m_i(\lambda^\pm(g)))]\right)$. The method of proof of [Ful99, Thm. 14] in fact shows

$$\begin{aligned} 1 + \sum_{n \geq 1} (\psi([O^+(n, q)]) Z(O^+(n, q), \mathbf{x}) + \psi([O^-(n, q)]) Z(O^-(n, q), \mathbf{x})) u^n \\ = \left(\sum_{\lambda^\pm \in \mathbb{Y}_O} x_{T-1, \lambda^\pm} \psi(\lambda^\pm) \frac{u^{|\lambda^\pm|}}{c_{O, q}(\lambda^\pm)} \right) \left(\sum_{\lambda^\pm \in \mathbb{Y}_O} x_{T+1, \lambda^\pm} \psi(\lambda^\pm) \frac{u^{|\lambda^\pm|}}{c_{O, q}(\lambda^\pm)} \right) \\ \prod_{P=\overline{P}} \left(\sum_{\lambda \in \mathbb{Y}} x_{P, \lambda} \psi([x^2 - cy^2]^{|\lambda|}) \frac{u^{\deg(P)|\lambda|}}{c_{GL, -q^{\deg(P)/2}}(\lambda)} \right) \prod_{Q \neq \overline{Q}} \left(\sum_{\lambda \in \mathbb{Y}} x_{Q, \lambda} x_{\overline{Q}, \lambda} \frac{u^{|\lambda| \deg(Q\overline{Q})}}{c_{GL, q^{\deg(Q)}}(\lambda)} \right). \quad (\text{A.3}) \end{aligned}$$

For $\psi \equiv 1$ we recover (A.1). We leave the details to the reader.

A.5 Proof of Theorem 7.4

Let χ be a Hayes character, and let us specialize (A.3) to $x_{T\pm 1, \lambda^\pm} = \chi(T \pm 1)^{|\lambda^\pm|}$ and $x_{P, \lambda} = \chi(P^{|\lambda|})$ for all $P \in \mathcal{P}_q \setminus \{T-1, T+1\}$ and $\lambda \in \mathbb{Y}$. We work with formal power series, and so do not check convergence. Additionally we take $\psi(a, b) = (-1)^b$ if $q \equiv 1 \pmod{4}$ and $\psi(a) = i^a$ if $q \equiv 3 \pmod{4}$.

We obtain, by appealing to (A.2) with $(u, z) = (\chi(P)u^{\deg(P)}, -q^{\deg(P)/2})$ and $(u, z) = (\chi(Q\overline{Q})u^{\deg(Q\overline{Q})}, q^{\deg(Q)})$, and using the formulas for the orders of $GL(n, q)$ and $U(n, q)$,

$$\begin{aligned} 1 + \sum_{n \geq 1, 2|n} \left(\frac{\sum_{M \in O^+(n, q)} \chi(\text{CharPoly}(M))}{|O^+(n, q)|} - \frac{\sum_{M \in O^-(n, q)} \chi(\text{CharPoly}(M))}{|O^-(n, q)|} \right) u^n \\ = \left(\sum_{\lambda^\pm \in \mathbb{Y}_O} \psi(\lambda^\pm) \frac{(\chi(T-1)u)^{|\lambda^\pm|}}{c_{O, q}(\lambda^\pm)} \right) \left(\sum_{\lambda^\pm \in \mathbb{Y}_O} \psi(\lambda^\pm) \frac{(\chi(T+1)u)^{|\lambda^\pm|}}{c_{O, q}(\lambda^\pm)} \right) \\ \prod_{P=\overline{P}} \left(\sum_{j \geq 0} \frac{|P|^{\frac{j(j-1)}{2}} (-1)^j}{|U(j, q^{\frac{\deg(P)}{2}})|} (\chi(P)u^{\deg(P)})^j \right) \prod_{Q \neq \overline{Q}} \left(\sum_{j \geq 0} \frac{q^{\deg(Q)j(j-1)}}{|GL(j, q^{\deg(Q)})|} (\chi(Q\overline{Q})u^{\deg(Q\overline{Q})})^j \right). \quad (\text{A.4}) \end{aligned}$$

Here we have used the fact that for odd n , $O^+(n, q)$ and $O^-(n, q)$ are conjugate and $\psi([O^+(n, q)]) = -\psi([O^-(n, q)])$, so we may omit the odd n from the left hand side of (A.4). By comparing coefficients and using Lemma 2.3, we find that $\alpha := P_O^+ - P_O^-$ is supported on \mathcal{M}_q^{sr} , and if $f \in \mathcal{M}_q^{sr}$ factorizes as

$$f = (T-1)^a (T+1)^b \prod_{i=1}^r P_i^{e_i} \prod_{j=1}^s (Q_j \overline{Q_j})^{e'_j}$$

with the same notation as in Theorem 6.5, then

$$\alpha(f) = \alpha((T-1)^a) \alpha((T+1)^b) \prod_{i=1}^r \alpha(P_i^{e_i}) \prod_{j=1}^s \alpha((Q_j \overline{Q_j})^{e'_j}) \quad (\text{A.5})$$

with

$$\alpha(P_i^{e_i}) = \frac{q^{\frac{m_i e_i (e_i - 1)}{2}} (-1)^{e_i}}{|U(e_i, q^{\frac{m_i}{2}})|}, \quad \alpha((Q_j \overline{Q_j})^{e'_j}) = \frac{q^{m'_j e'_j (e'_j - 1)}}{|GL(e'_j, q^{m'_j})|}, \quad \alpha((T-1)^a) = \alpha((T+1)^a). \quad (\text{A.6})$$

By (6.17), $P_{S_p}^\circ$ is also supported on \mathcal{M}_q^{sr} and satisfies (A.5) and (A.6) with $P_{S_p}^\circ$ in place of α . Additionally, the expectation of α over $\mathcal{M}_{n,q}$ ($n \geq 1$) is 0, as well as the expectation of $P_{S_p}^\circ$ (as follows e.g. from Lemma 6.25). By induction on n one may show that $\alpha((T-1)^n) = P_{S_p}^\circ((T-1)^n)$, which concludes the proof. \square

References

- [Art88] E. Artin. *Geometric algebra*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1988. Reprint of the 1957 original, A Wiley-Interscience Publication.
- [BBSR15] Efrat Bank, Lior Bary-Soroker, and Lior Rosenzweig. Prime polynomials in short intervals and in arithmetic progressions. *Duke Math. J.*, 164(2):277–295, 2015.
- [BD02] Daniel Bump and Persi Diaconis. Toeplitz minors. *J. Combin. Theory Ser. A*, 97(2):252–271, 2002.
- [BG06] Daniel Bump and Alex Gamburd. On the averages of characteristic polynomials from classical groups. *Comm. Math. Phys.*, 265(1):227–274, 2006.
- [Car67] L. Carlitz. Some theorems on irreducible reciprocal polynomials over a finite field. *J. Reine Angew. Math.*, 227:212–220, 1967.
- [CDSS17] Alina Carmen Cojocaru, Rachel Davis, Alice Silverberg, and Katherine E. Stange. Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre). *Int. Math. Res. Not. IMRN*, (12):3557–3602, 2017.
- [CFHS12] Wouter Castryck, Amanda Folsom, Hendrik Hubrechts, and Andrew V. Sutherland. The probability that the number of points on the Jacobian of a genus 2 curve is prime. *Proc. Lond. Math. Soc. (3)*, 104(6):1235–1270, 2012.
- [CH18] Gilyoung Cheong and Yifeng Huang. Cohen-Lenstra distributions via random matrices over complete discrete valuation rings with finite residue fields. *arXiv preprint arXiv:1812.11728*, 2018.
- [Cha97] Nick Chavdarov. The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke Math. J.*, 87(1):151–180, 1997.
- [CK03] Hi-joon Chae and Dae San Kim. L functions of some exponential sums of finite classical groups. *Math. Ann.*, 326(3):479–487, 2003.
- [CK08] Hi-joon Chae and Dae San Kim. Identities arising from Gauss sums for finite classical groups. *J. Number Theory*, 128(7):2010–2024, 2008.
- [CL84] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.
- [Con05] Keith Conrad. Irreducible values of polynomials: a non-analogy. In *Number fields and function fields—two parallel worlds*, volume 239 of *Progr. Math.*, pages 71–85. Birkhäuser Boston, Boston, MA, 2005.

- [CS99] Charles W. Curtis and Ken-ichi Shinoda. Unitary Kloosterman sums and the Gelfand-Graev representation of GL_2 . *J. Algebra*, 216(2):431–447, 1999.
- [Dic58] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications, Inc., New York, 1958.
- [Die71] Jean A. Dieudonné. *La géométrie des groupes classiques*. Springer-Verlag, Berlin-New York, 1971. Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5.
- [DJ10] Maurice Duits and Kurt Johansson. Powers of large random unitary matrices and Toeplitz determinants. *Trans. Amer. Math. Soc.*, 362(3):1169–1187, 2010.
- [DS94] Persi Diaconis and Mehrdad Shahshahani. On the eigenvalues of random matrices. *J. Appl. Probab.*, 31A:49–62, 1994. Studies in applied probability.
- [EH91] Gove W. Effinger and David R. Hayes. *Additive number theory of polynomials over a finite field*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1991. Oxford Science Publications.
- [Eic38] M. Eichler. Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörper und ihre L -Reihen. *J. Reine Angew. Math.*, 179:227–251, 1938.
- [FG04] Jason Fulman and Robert Guralnick. Conjugacy class properties of the extension of $GL(n, q)$ generated by the inverse transpose involution. *J. Algebra*, 275(1):356–396, 2004.
- [FS16] Jason Fulman and Dennis Stanton. On the distribution of the number of fixed vectors for the finite classical groups. *Ann. Comb.*, 20(4):755–773, 2016.
- [FST12] Jason Fulman, Jan Saxl, and Pham Huu Tiep. Cycle indices for finite orthogonal groups of even characteristic. *Trans. Amer. Math. Soc.*, 364(5):2539–2566, 2012.
- [Ful99] Jason Fulman. Cycle indices for the finite classical groups. *J. Group Theory*, 2(3):251–289, 1999.
- [FW89] Eduardo Friedman and Lawrence C. Washington. On the distribution of divisor class groups of curves over a finite field. In *Théorie des nombres (Quebec, PQ, 1987)*, pages 227–239. de Gruyter, Berlin, 1989.
- [Ger61] Murray Gerstenhaber. On the number of nilpotent matrices with coefficients in a finite field. *Illinois J. Math.*, 5:330–333, 1961.
- [Gor20] Ofir Gorodetsky. Mean values of arithmetic functions in short intervals and in arithmetic progressions in the large-degree limit. *Mathematika*, 66(2):373–394, 2020.
- [GR04] George Gasper and Mizan Rahman. *Basic hypergeometric series*, volume 96 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 2004. With a foreword by Richard Askey.
- [GS20] Ofir Gorodetsky and Will Sawin. Correlation of arithmetic functions over $\mathbb{F}_q[T]$. *Math. Ann.*, 376(3-4):1059–1106, 2020.
- [Hay65] David R. Hayes. The distribution of irreducibles in $GF[q, x]$. *Trans. Amer. Math. Soc.*, 117:101–127, 1965.
- [JL20] Kurt Johansson and Gaultier Lambert. Multivariate normal approximation for traces of random unitary matrices. *arXiv preprint arXiv:2002.01879*, 2020.
- [Joh97] Kurt Johansson. On random matrices from the compact classical groups. *Ann. of Math. (2)*, 145(3):519–545, 1997.
- [Kim97a] Dae San Kim. Gauss sums for general and special linear groups over a finite field. *Arch. Math. (Basel)*, 69(4):297–304, 1997.
- [Kim97b] Dae San Kim. Gauss sums for $O^-(2n, q)$. *Acta Arith.*, 80(4):343–365, 1997.
- [Kim97c] Dae San Kim. Gauss sums for $U(2n + 1, q^2)$. *J. Korean Math. Soc.*, 34(4):871–894, 1997.
- [Kim98a] Dae San Kim. Gauss sums for $O(2n + 1, q)$. *Finite Fields Appl.*, 4(1):62–86, 1998.
- [Kim98b] Dae San Kim. Gauss sums for symplectic groups over a finite field. *Monatsh. Math.*, 126(1):55–71, 1998.
- [Kim98c] Dae San Kim. Gauss sums for $U(2n, q^2)$. *Glasgow Math. J.*, 40(1):79–95, 1998.
- [KL96] Dae San Kim and In-Sok Lee. Gauss sums for $O^+(2n, q)$. *Acta Arith.*, 78(1):75–89, 1996.

- [KP97] Dae San Kim and Young Ho Park. Gauss sums for orthogonal groups over a finite field of characteristic two. *Acta Arith.*, 82(4):331–357, 1997.
- [KR14] Jonathan P. Keating and Zeév Rudnick. The variance of the number of prime polynomials in short intervals and in residue classes. *Int. Math. Res. Not. IMRN*, (1):259–288, 2014.
- [Lam57] Erich Lamprecht. Struktur und Relationen allgemeiner Gausscher Summen in endlichen Ringen. I, II. *J. Reine Angew. Math.*, 197:1–26, 27–48, 1957.
- [Li92] Wen-Ch'ing Winnie Li. Character sums and abelian Ramanujan graphs. *J. Number Theory*, 41(2):199–217, 1992. With an appendix by Ke Qin Feng and the author.
- [Li06] Wen-Ching Winnie Li. Character sums over norm groups. *Finite Fields Appl.*, 12(1):1–15, 2006.
- [PG18] Corentin Perret-Gentil. Exponential Sums Over Finite Fields and the Large Sieve. *International Mathematics Research Notices*, 08 2018.
- [PG19] Corentin Perret-Gentil. Distribution questions for trace functions with values in cyclotomic integers and their reductions. *Trans. Amer. Math. Soc.*, 371(7):4585–4629, 2019.
- [Rai97] E. M. Rains. High powers of random elements of compact Lie groups. *Probab. Theory Related Fields*, 107(2):219–241, 1997.
- [Rei61] Irving Reiner. On the number of matrices with given characteristic polynomial. *Illinois J. Math.*, 5:324–329, 1961.
- [Rhi72] Georges Rhin. Répartition modulo 1 dans un corps de séries formelles sur un corps fini. *Dissertationes Math. (Rozprawy Mat.)*, 95:75, 1972.
- [RS88] A. Rudvalis and K. Shinoda. An enumeration in finite classical groups. *U-Mass Amherst Department of Mathematics Technical Report, Amherst, MA*, 1988.
- [Sto88] Richard Stong. Some asymptotic results on finite vector spaces. *Adv. in Appl. Math.*, 9(2):167–199, 1988.
- [Tay92] Donald E. Taylor. *The geometry of the classical groups*, volume 9 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, 1992.
- [Wal63] G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Austral. Math. Soc.*, 3:1–62, 1963.
- [Wei74] André Weil. *Basic number theory*. Springer-Verlag, New York-Berlin, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.
- [Wie02] K. Wieand. Eigenvalue distributions of random unitary matrices. *Probab. Theory Related Fields*, 123(2):202–224, 2002.
- [Woo19] Melanie Matchett Wood. Random integral matrices and the Cohen-Lenstra heuristics. *Amer. J. Math.*, 141(2):383–398, 2019.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OXFORD, UK
E-mail address: ofir.goro@gmail.com

DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO, K7L 3N6, CANADA
E-mail address: brad.rodgers@queensu.ca