ACTA ARITHMETICA
179.4 (2017)

The summatory function of the Möbius function in function fields

by

Byungchul Cha (Allentown, PA)

1. Introduction. Recall that the Möbius function $\mu(n)$ is defined for any positive integer n by

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not square free}, \\ (-1)^t & \text{if } n \text{ is a product of } t \text{ distinct primes}. \end{cases}$$

Let $M(x)$ be its summatory function,

$$M(x) := \sum_{n \le x} \mu(n).$$

Mertens's conjecture [19] states that

$$|M(x)| < \sqrt{x} \tag{1.1}$$

for all $x > 1$. This conjecture was disproved by Odlyzko and te Riele [21] in 1985. Still, understanding the growth of $M(x)$ remains the subject of intensive investigation by many authors in analytic number theory. For example, see [18] and [24] for some recent results. Relevant to us is a paper [20] of Ng, who gives certain conditional results on the growth of $M(x)$, using the techniques of Rubinstein and Sarnak [23]. In particular, Ng presents a probabilistic argument supporting the conjecture of Gonek that $M(x)/\sqrt{x}$ grows roughly as $(\log\log\log x)^{5/4}$. More precisely, there exists a number $B > 0$ such that

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}(\log\log\log x)^{5/4}} = B, \quad \liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}(\log\log\log x)^{5/4}} = -B. \tag{1.2}$$

2010 *Mathematics Subject Classification*: Primary 11N56; Secondary 11M50.
Key words and phrases: Möbius function, equidistribution theorem, random matrix theory, function fields.
Received 16 August 2016; revised 29 November 2016.
Published online 14 June 2017.

DOI: 10.4064/aa8590-1-2017

In this paper, we try to construct a function field analog of Ng's work and examine several issues that arise from this attempt. This is motivated by the present author's earlier paper [3], where a function field version of Rubinstein and Sarnak's work is established.

To describe our results in more detail, we fix some notation. Let C be a nonsingular projective curve of genus g defined over a finite field $\mathbb{F}_q$ of characteristic $p > 2$ with q elements. Define the Möbius function $\mu_{C/\mathbb{F}_q}(D)$ of $C/\mathbb{F}_q$ for all effective divisors D of C in the obvious way,

$$\mu_{C/\mathbb{F}_q}(D) := \begin{cases} 1 & \text{if } D = 0, \\ 0 & \text{if a prime divisor divides } D \text{ with order at least 2}, \\ (-1)^t & \text{if } D \text{ is a sum of } t \text{ distinct prime divisors.} \end{cases}$$

Also, define the summatory function

$$M_{C/\mathbb{F}_q}(X) := \sum_{\deg D \le X} \mu_{C/\mathbb{F}_q}(D)$$

for all positive integers X.

The starting point is an asymptotic formula for $M_{C/\mathbb{F}_q}(X)$ as $X \to \infty$ (Proposition 2.2). Roughly speaking, this formula says that $M_{C/\mathbb{F}_q}(X) = O(X^{r-1}q^{X/2})$, where r is the maximum order of all inverse zeros for $C/\mathbb{F}_q$ (see (2.2) for the definition of inverse zeros and their orders). From this, if all inverse zeros are simple, we deduce in Corollary 2.3 that the quantity

$$B(C/\mathbb{F}_q) := \limsup_{X\to\infty} \frac{M_{C/\mathbb{F}_q}(X)}{q^{(X+1)/2}} \tag{1.3}$$

exists as a finite number. This could be regarded as a (weak) function field analog of (1.1).

However, it is obvious that the boundedness of $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ when all inverse zeros are simple stems from the fact that there are only finitely many inverse zeros for any given C. So, rather than studying $B(C/\mathbb{F}_q)$ for a single curve C, it would be interesting to find the *average* of $B(C/\mathbb{F}_q)$ over a family $\mathcal{F}$ of curves whose genus g is large. Instead, what we would like to do in this paper is find the average of $B(C/\mathbb{F}_q)$ over $\mathcal{F}$ with the *scalar field* $\mathbb{F}_q$ *growing larger*. The advantage of dealing with this *geometric average* is that this set-up enables us to use the powerful tool of Katz and Sarnak's [11] reformulation of the equidistribution theorem of Deligne. Still, we do not quite succeed in computing the geometric average of $B(C/\mathbb{F}_q)$ but obtain something close to it. This is explained later in this introduction.

At this point, we need to give a definition of the *Linear Independence* property.

Definition 1.1 (Linear Independence (LI)). Let $\gamma_1 = \sqrt{q}\, e^{i\theta_1}, \dots, \gamma_{2g} = \sqrt{q}\, e^{i\theta_{2g}}$ be the inverse zeros of a curve $C/\mathbb{F}_q$. We say that C satisfies the

Linear Independence (LI) property if the set

$$\{\theta_j \mid 0 \le \theta_j \le \pi \text{ with } j = 1, \dots, 2g\} \cup \{\pi\},$$

listing the inverse zeros with multiplicity, is linearly independent over $\mathbb{Q}$.

The number field version of LI, which states that nonnegative ordinates of the critical zeros of the Riemann zeta function or Dirichlet L-functions are linearly independent over $\mathbb{Q}$, plays a key role in the aforementioned work of Ng [20], as well as in the work of Rubinstein and Sarnak [23] on the prime number race. Note that LI is called the *Grand Simplicity Hypothesis* in [23] and [3]. The fact that such a property of zeta zeros bears on understanding the exact growth of $M(x)$ had already been made clear by Ingham [10], well before Odlyzko and te Riele disproved Mertens's conjecture. Ingham proved in 1942 that $\limsup_{x\to\infty} M(x)/\sqrt{x} = \infty$ if LI holds true for the Riemann zeta function.

Unfortunately, there is currently very little direct theoretical or numerical evidence to support the number field version of LI. However, in the function field case, things are better understood. There are known examples (see [3], [4] and [17]) where LI can be confirmed and, in some other cases, disproved. Moreover, the work [17] of Kowalski shows that most curves in a certain one-parameter family of hyperelliptic curves satisfy LI. For more background and precise statements of Kowalski's results, the readers are referred to [17] and Remark 3.2 of this paper.

The importance of LI in our work comes from Theorem 2.6, which states that if C satisfies LI, then the bound

$$D(C/\mathbb{F}_q) := \frac{1}{q^{1/2}} \sum_{\gamma} \left| \frac{\gamma}{Z'_{C/\mathbb{F}_q}(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \right| \tag{1.4}$$

of $B(C/\mathbb{F}_q)$ we find in Corollary 2.3 becomes sharp, that is, $B(C/\mathbb{F}_q) = D(C/\mathbb{F}_q)$ under LI. It turns out that Kowalski's argument in [17] can be easily extended to prove that *most* curves in the family $\mathcal{H}_{2g+1}$ of hyperelliptic curves of genus g satisfy LI (Theorem 3.1). As a consequence, $B(C/\mathbb{F}_q) = D(C/\mathbb{F}_q)$ for most curves $C/\mathbb{F}_q$ in $\mathcal{H}_{2g+1}$. That is why we choose to work with $\mathcal{F} := \mathcal{H}_{2g+1}$ in this paper.

The next step is to use Deligne's equidistribution theorem to find the geometric average of $D(C/\mathbb{F}_q)$. We show in Theorem 3.3 that a certain *truncated* version of the geometric average of $D(C/\mathbb{F}_q)$ is equal to

$$\mathcal{I}(g) := \int_{\mathrm{USp}(2g,\mathbb{C})} \varphi(U)\, d\mu_{\mathrm{Haar}}(U).$$

Here, $d\mu_{\mathrm{Haar}}$ is the unique probability Haar measure on the unitary symplectic group $\mathrm{USp}(2g, \mathbb{C})$. The function φ is defined in (3.4) and (3.5). This situation is similar to the number field case in [20] where the discrete neg-

ative moments $J_{-k}(T)$ of $\zeta'(s)$ play an important role in understanding the growth of $M(x)$.

In §4, which can be read independently of other parts of this paper, we study the integral $\mathcal{I}(g)$, especially its asymptotic behavior as $g \to \infty$. A key result here is Theorem 4.1, which finds an asymptotic expression for the average value of powers of the characteristic polynomials of random unitary symplectic matrices. The main tool is a formula by Deift, Its, and Krasovsky [6] for Hankel's determinants with singular weight functions. We note that Theorems 4.1 and 4.2 extend the earlier work of Keating and Snaith [14, 15] and that of Keating and Odgers [12] on the moments of characteristic polynomials. See Remark 4.3 for more detail.

Our result seems to suggest that the geometric average of $B(C/\mathbb{F}_q)$ over $\mathcal{H}_{2g+1}$ is given by the asymptotic formula in (4.14). However, there are at least two major issues we cannot resolve in this paper.

The first issue is the extent of the possible failure of LI in $\mathcal{H}_{2g+1}$. Without LI, it may happen that $B(C/\mathbb{F}_q) < D(C/\mathbb{F}_q)$, so the geometric average of $D(C/\mathbb{F}_q)$ might potentially overestimate that of $B(C/\mathbb{F}_q)$. Even though the set of conjugacy classes in $\mathrm{USp}(2g, \mathbb{C})$ whose eigenvalues have no (nontrivial multiplicative) relations form a measure zero subset with respect to the Haar measure, it is still dense in $\mathrm{USp}(2g, \mathbb{C})$, and it is unclear if one could utilize the equidistribution theorem to control the difference between the averages of $B(C/\mathbb{F}_q)$ and $D(C/\mathbb{F}_q)$.

The second issue is that we cannot (yet) finish the proof of the asymptotic formula (4.14) of $\mathcal{I}(g)$. It seems that to do so we need a finer control on the error term in the formula of Deift, Its, Krasovsky. For a more detailed explanation, see §4, especially Remark 4.4.

2. Asymptotic formula and the LI property. Throughout this paper, we write $\#A$ for the cardinality of a finite set A. We fix a power q of an odd prime $p > 2$ and denote by $\mathbb{F}_q$ a finite field with q elements. For each $n \geq 1$, we have a unique extension $\mathbb{F}_{q^n}$ (inside a chosen algebraic closure of $\mathbb{F}_q$) of $\mathbb{F}_q$ of degree n. For a nonsingular projective curve C over $\mathbb{F}_q$ of genus g, the *zeta function* $Z_{C/\mathbb{F}_q}(u)$ of C over $\mathbb{F}_q$ is defined by

$$Z_{C/\mathbb{F}_q}(u) := \exp\left(\sum_{n\geq 1} \frac{\#C(\mathbb{F}_{q^n})}{n} u^n\right),$$

initially viewed as a formal power series in u with rational coefficients. It is known from the Riemann Hypothesis for curves over finite fields that

$$Z_{C/\mathbb{F}_q}(u) = \frac{P_{C/\mathbb{F}_q}(u)}{(1-u)(1-qu)}, \tag{2.1}$$

where $P_{C/\mathbb{F}_q}(u)$ is a polynomial in u of degree $2g$ with integer coefficients, which factorizes as

$$P_{C/\mathbb{F}_q}(u) = \prod_{j=1}^{2g}(1-\gamma_j u) \tag{2.2}$$

for some complex numbers γ_j with $|\gamma_j| = \sqrt{q}$ for all $j = 1, \dots, 2g$. These numbers γ_j are called the *inverse zeros* of C. By the *order* of an inverse zero γ, we mean the multiplicity of γ^{-1} as a root of $P_{C/\mathbb{F}_q}(u)$. If γ is of order one, we will say that the inverse zero γ is *simple*.

2.1. Asymptotic formula for $M_{C/\mathbb{F}_q}(X)$. Let $Z_\mu(u)$ be the following Dirichlet series (in u) associated with $\mu_{C/\mathbb{F}_q}(D)$, for a divisor D, together with the change of variable $u := q^{-s}$:

$$Z_\mu(u) := \sum_{D\geq 0} \frac{\mu_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \sum_{N=0}^{\infty} c_\mu(N)u^N. \tag{2.3}$$

Here $\mathcal{N}D$ is the absolute norm of D, and $c_\mu(N) := \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D)$. From the Euler product expression of $Z_\mu(u)$, it is easy to show (see [22, Chapter 1] or follow the same argument as in the number field case) that

$$Z_\mu(u) = \frac{1}{Z_{C/\mathbb{F}_q}(u)} = \frac{(1-u)(1-qu)}{P_{C/\mathbb{F}_q}(u)}. \tag{2.4}$$

From (2.3) and the definition of $c_\mu(N)$, we have

$$M_{C/\mathbb{F}_q}(X) = \sum_{N\leq X} c_\mu(N). \tag{2.5}$$

Therefore, the crucial step in finding the asymptotic formula for $M_{C/\mathbb{F}_q}(X)$ is to estimate the coefficients $c_\mu(N)$.

First, we consider the easiest case when C is of genus zero. In this case, $P_{C/\mathbb{F}_q}(u) = 1$ and

$$Z_\mu(u) = (1-u)(1-qu) = 1-(q+1)u+qu^2.$$

So, $c_\mu(N) = 0$ for all $N \geq 3$ and $c_\mu(N) = 1, -(q+1), q$ if $N = 0, 1, 2$ respectively. This easily determines the values of $M_{C/\mathbb{F}_q}(X)$ for all X. In particular, we obtain the trivial bound $|M_{C/\mathbb{F}_q}(X)| \leq q$ for all X. We note here that even in this genus zero case, sums of the Möbius function become interesting if we restrict ourselves to short intervals. See the work of Keating and Rudnick [13] for more detail.

Next, we consider the case of arbitrary genus g. Let C_1 be a circular path in the complex plane of radius 1 centered at the origin, oriented coun-

terclockwise. We calculate the integral

$$\frac{1}{2\pi i}\int\limits_{C_1}\frac{Z_\mu(u)}{u^{N+1}}\,du$$

using Cauchy's theorem.

First, we note that the integral can be easily bounded independently of N. From (2.4) and (2.2),

$$\left|\frac{1}{2\pi i}\int\limits_{C_1}\frac{Z_\mu(u)}{u^{N+1}}\,du\right| \le \frac{1}{2\pi}\int\limits_{C_1}\left|\frac{Z_\mu(u)}{u^{N+1}}\right||du| \le \frac{2(1+q)}{(1-\sqrt{q})^{2g}}. \tag{2.6}$$

Next, we see from (2.2)–(2.4) that the function $Z_\mu(u)/u^{N+1}$ has poles at $u=0$ and $u=\gamma^{-1}$ for all inverse zeros γ. The series expression (2.3) implies that the residue of $Z_\mu(u)/u^{N+1}$ at $u=0$ is $c_\mu(N)$. Therefore, if we define $R_{C/\mathbb{F}_q}(N,\gamma)$ to be the residue of $Z_\mu(u)/u^{N+1}$ at $u=\gamma^{-1}$ for any inverse zero γ, Cauchy's theorem yields

$$\left|c_\mu(N)+\sum_\gamma R_{C/\mathbb{F}_q}(N,\gamma)\right| \le \frac{2(1+q)}{(1-\sqrt{q})^{2g}}.$$

By letting $N\to\infty$, we get

$$c_\mu(N) = -\sum_\gamma R_{C/\mathbb{F}_q}(N,\gamma)+O(1). \tag{2.7}$$

So, in order to obtain an asymptotic formula for $M_{C/\mathbb{F}_q}(X)$, we will need to calculate the residues $R_{C/\mathbb{F}_q}(N,\gamma)$. We do this by finding the Laurent series expansion of $Z_\mu(u)/u^{N+1} = 1/(Z_{C/\mathbb{F}_q}(u)u^{N+1})$ directly.

From the binomial theorem,

$$u^{-(N+1)} = \gamma^{N+1}\sum_{k=0}^{\infty}(-1)^k\binom{N+k}{k}\gamma^k(u-\gamma^{-1})^k. \tag{2.8}$$

Let r be the order of γ. Then the power series expansion of $Z_{C/\mathbb{F}_q}(u)$ at $u=\gamma^{-1}$ starts with

$$Z_{C/\mathbb{F}_q}(u) = \frac{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}{r!}(u-\gamma^{-1})^r+\cdots.$$

Here $Z^{(r)}_{C/\mathbb{F}_q}(u)$ is the rth derivative of $Z_{C/\mathbb{F}_q}(u)$ (with respect to u). Then the Laurent series expansion of $1/Z_{C/\mathbb{F}_q}(u)$ at $u=\gamma^{-1}$ begins with

$$\frac{1}{Z_{C/\mathbb{F}_q}(u)} = \frac{r!}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}(u-\gamma^{-1})^{-r}+\cdots. \tag{2.9}$$

Therefore, the residue $R_{C/\mathbb{F}_q}(N,\gamma)$ is obtained by multiplying the two series

(2.8) and (2.9) and extracting the coefficient of $(u-\gamma^{-1})^{-1}$. To be precise,

$$\begin{aligned}(2.10)\qquad R_{C/\mathbb{F}_q}(N,\gamma) &= \frac{r!}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}\gamma^{N+1}(-1)^{r-1}\binom{N+r-1}{r-1}\gamma^{r-1}+\cdots\\ &= \frac{r!}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}\gamma^{N+1}(-1)^{r-1}\frac{N^{r-1}}{(r-1)!}\gamma^{r-1}+\cdots\\ &= \frac{\gamma^{N+r}(-1)^{r-1}r}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}N^{r-1}+\cdots,\end{aligned}$$

where all the suppressed terms are polynomials in N of degree $r-2$ or less.

If we sum (2.10) over $N=1,\dots,X$, we get

$$(2.11)\qquad \sum_{N=1}^{X} R_{C/\mathbb{F}_q}(N,\gamma) = \frac{\gamma^r(-1)^{r-1}r}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}\,\frac{\gamma}{\gamma-1}X^{r-1}\gamma^X + O(X^{r-2}\gamma^X)$$

as $X\to\infty$. This is an immediate consequence of Lemma 2.1, which can be proven by partial summation [2, Theorem 4.2], as outlined in [3, Lemma 2.2]. So, we omit the proof.

LEMMA 2.1. *Let β be a complex number with $|\beta|>1$ and k be a non-negative integer. Then*

$$\lim_{X\to\infty}\frac{1}{X^k\beta^X}\sum_{N=1}^{X}N^k\beta^N=\frac{\beta}{\beta-1}.$$

Denote by $\theta(\gamma)$ the argument of the complex number γ, so that $\gamma=\sqrt{q}\,e^{i\theta(\gamma)}$. Then (2.11) becomes

$$(2.12)\qquad -\frac{1}{X^{r-1}q^{X/2}}\sum_{N=1}^{X}R_{C/\mathbb{F}_q}(N,\gamma)=\frac{(-\gamma)^r r}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}\,\frac{\gamma}{\gamma-1}e^{iX\theta(\gamma)}+o(1).$$

Now, (2.5), (2.7), (2.12) together yield the estimate of $M_{C/\mathbb{F}_q}(X)$ in the proposition below.

PROPOSITION 2.2. *For an inverse zero γ, let $\theta(\gamma)$ be the argument of γ, so that $\gamma=\sqrt{q}\,e^{i\theta(\gamma)}$. Also, let r be the maximum order among all the inverse zeros γ of $Z_{C/\mathbb{F}_q}(u)$, that is,*

$$r=\max\{\operatorname{ord}\gamma_j\}_{j=1}^{2g}.$$

Then, as $X\to\infty$,

$$\frac{M_{C/\mathbb{F}_q}(X)}{X^{r-1}q^{X/2}}=\sum_{\operatorname{ord}\gamma=r}\frac{(-\gamma)^r r}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})}\,\frac{\gamma}{\gamma-1}e^{iX\theta(\gamma)}+o(1).$$

In particular, if all inverse zeros $\{\gamma_j\}_{j=1}^{2g}$ *are simple, then*

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = -\sum_{j=1}^{2g} \frac{\gamma_j}{Z'_{C/\mathbb{F}_q}(\gamma_j{}^{-1})} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)} + o(1).$$

Corollary 2.3. *With the above notation,*

$$\limsup_{X\to\infty} \frac{M_{C/\mathbb{F}_q}(X)}{X^{r-1}q^{X/2}} \le \sum_{\operatorname{ord}\gamma=r} \left| \frac{\gamma^r r}{Z^{(r)}_{C/\mathbb{F}_q}(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \right|.$$

Remark 2.4. It is interesting to compare the (upper) bound of $M_{C/\mathbb{F}_q}(X)$ in the above corollary with the corresponding bound in the number field case. First of all, from the obvious fact $r \le 2g$, Corollary 2.3 gives

$$M_{C/\mathbb{F}_q}(X) = O(X^{2g-1}q^{X/2}). \tag{2.13}$$

With the usual "dictionary" ($q^X \leftrightarrow x$ and $X \leftrightarrow \log x$) between function fields and number fields, we see that (2.13) provides a stronger bound than the following number field version of the corresponding upper bound of $M(x) = \sum_{n\le x} \mu(n)$:

$$M(x)/\sqrt{x} \ll \exp\big((\log x)^{1/2}(\log\log x)^{14}\big),$$

which was proven by Soundararajan [24] under RH. The reason why we have a stronger upper bound in the function field case is essentially that there are only finitely many zeta zeros for a (fixed) base curve $C/\mathbb{F}_q$.

The next theorem follows from the adaptation of Rubinstein and Sarnak's [23] argument to the function field setting; the proof is identical to that of [3, Theorem 3.2], so we omit it.

Theorem 2.5. *With the notation of Proposition* 2.2*, the function* $M_{C/\mathbb{F}_q}(X)/(X^{r-1}q^{X/2})$ *has a limiting distribution* μ *on* $\mathbb{R}$*, that is,*

$$\lim_{Y\to\infty} \frac{1}{Y} \sum_{X=1}^{Y} f\left(\frac{M_{C/\mathbb{F}_q}(X)}{X^{r-1}q^{X/2}}\right) = \int_{-\infty}^{\infty} f(x)\, d\mu(x)$$

for all bounded continuous functions f *on* $\mathbb{R}$*.*

2.2. Application of LI. Suppose that the curve C has the Linear Independence property (Definition 1.1). One immediate consequence of LI is that all the inverse zeros of C are simple, so the formula in Proposition 2.2 becomes

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = -\sum_{j=1}^{2g} \left| \frac{\gamma_j}{Z'_{C/\mathbb{F}_q}(\gamma_j{}^{-1})} \frac{\gamma_j}{\gamma_j - 1} \right| \cos\big(\omega(\gamma_j) + X\theta(\gamma_j)\big) + o(1), \tag{2.14}$$

where

$$\omega(\gamma_j) := \arg\left(\frac{\gamma_j}{Z'_{C/\mathbb{F}_q}(\gamma_j{}^{-1})}\,\frac{\gamma_j}{\gamma_j-1}\right).$$

Another consequence of LI is that, thanks to the Kronecker–Weyl equidistirbution theorem, the trigonometric terms on the right side of (2.14) behave independently of each other. As a result, we have

THEOREM 2.6. *If C satisfies LI, then*

$$\limsup_{X\to\infty}\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = \sum_{j=1}^{2g}\left|\frac{\gamma_j}{Z'_{C/\mathbb{F}_q}(\gamma_j{}^{-1})}\,\frac{\gamma_j}{\gamma_j-1}\right|.$$

3. Universal families of hyperelliptic curves. We define $\mathcal{H}_{2g+1}$ to be the space of monic polynomials of degree $2g+1$ with distinct roots (see [11, (10.1.18.1)]). One can think of $\mathcal{H}_{2g+1}$ as an open subvariety of the affine scheme $\mathbb{A}^{2g+1}$ over $\mathbb{Z}$. In particular, for each $n \ge 1$, $\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})$ is the set of monic polynomials $f(x) = a_0 + a_1x + \cdots + a_{2g}x^{2g} + x^{2g+1}$ with coefficients a_i in $\mathbb{F}_{q^n}$ and nonzero discriminant. Therefore, each $f \in \mathcal{H}_{2g+1}(\mathbb{F}_{q^n})$ defines a hyperelliptic curve C_f of genus g over $\mathbb{F}_{q^n}$, the nonsingular projective model of the plane curve defined by $y^2 = f(x)$. At this point, it will be convenient to introduce a terminology from [5]. We will say that *most* points of $\mathcal{H}_{2g+1}$ have the property $D = \{D_n\}_{n=1}^{\infty}$ if

$$\lim_{n\to\infty}\frac{\#\{f \in \mathcal{H}_{2g+1}(\mathbb{F}_{q^n}) \mid C_f \text{ satisfies } D_n\}}{\#\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})} = 1.$$

3.1. LI for most curves in $\mathcal{H}_{2g+1}$

THEOREM 3.1 (Chavdarov [5], Kowalski [17]). *For fixed q and g,*

$$\lim_{n\to\infty}\frac{\#\{f \in \mathcal{H}_{2g+1}(\mathbb{F}_{q^n}) \mid C_f \text{ satisfies LI}\}}{\#\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})} = 1.$$

In other words, most points of $\mathcal{H}_{2g+1}$ satisfy LI.

Proof. Let f and C_f be as above. Then one can show that, for most points of $\mathcal{H}_{2g+1}$, the sum of the inverse zeros of C_f is nonzero. This directly follows from Deligne's equidistribution theorem [11, Theorem 10.8.2] because the set of conjugacy classes with zero trace is a measure zero subset of the space $\mathrm{USp}(2g,\mathbb{C})^{\#}$ of conjugacy classes of $\mathrm{USp}(2g,\mathbb{C})$, with respect to the (direct image of) Haar measure.

The second step is to apply Chavdarov's theorem [5, Theorem 2.3] which says that, for most points of $\mathcal{H}_{2g+1}$, the Galois group of the splitting field of $P_{C_f}(u)$ is as large as possible, that is, isomorphic to the Weyl group W_{2g} corresponding to the symplectic group $\mathrm{Sp}(2g)$. To apply Chavdarov's theorem, we need to ensure that the mod-ℓ geometric monodromy group of

$\mathcal{H}_{2g+1}$ is $\mathrm{Sp}(2g, \mathbb{F}_\ell)$ for all large ℓ. But this had been previously shown by J. K. Yu (unpublished). More recently, Hall [7] and independently Achter and Pries [1] proved this result.

The last step is now to follow Kowalski's argument in [17, §3]. His proof of [17, Proposition 1.1 in §3] can be applied to $\mathcal{H}_{2g+1}$ without any change to show that if the sum of the inverse zeros of C is nonzero and the Galois group of $P_{C_f}(u)$ is as large as possible, then C satisfies LI. This concludes the proof of our theorem that most elements of $\mathcal{H}_{2g+1}$ satisfy LI [5].

We note that the assumption of odd characteristic $p > 2$ is essential in this proof. To show that the geometric monodromy group in $\mathrm{Sp}(2g)$ is as large as possible we need the prime 2 to be invertible in the base field $\mathbb{F}_q$ (see [7] and [1]). ∎

Remark 3.2. The aforementioned Chavdarov theorem has a quantitatively refined version, first proven by Kowalski [16, Theorems 6.1 and 6.2], who gives a quantitative bound on the number of curves in a family whose zeta functions are either reducible or have splitting fields with Galois group strictly smaller than the maximum possible one. Using this result, Kowalski derives a bound on the number of curves which do not satisfy LI in the one-parameter family of hyperelliptic curves

$$C_t : y^2 = f(x)(x - t),$$

where $f(x)$ is a monic irreducible polynomial with coefficients in $\mathbb{Z}$ whose discriminant is not divisible by p [17, Proposition 1.1]. In fact, if we assume that $p > 2g + 1$, then [16, Theorem 6.1(ii)] is directly applicable to the family $\mathcal{H}_{2g+1}$, and we can deduce from it that the number $N(\mathcal{H}_{2g+1}(\mathbb{F}_q))$ of curves in $\mathcal{H}_{2g+1}(\mathbb{F}_q)$ such that $P_{C_f}(u)$ is either reducible or has splitting field smaller than W_{2g} satisfies, as $q \to \infty$,

$$N(\mathcal{H}_{2g+1}(\mathbb{F}_q)) \ll q^{2g-\gamma}(\log q)$$

for $\gamma := 1/(10g^2 + 6g + 8)$. Therefore, the same bound applies to the number of curves that do not satisfy LI.

3.2. Average over the family. Let C be a nonsingular projective curve over a finite field $\mathbb{F}$ of characteristic $p > 2$. As in §2, let r be the maximum order of all inverse zeros of $C/\mathbb{F}$. Define

$$B(C/\mathbb{F}) := \limsup_{X \to \infty} \frac{M_{C/\mathbb{F}}(X)}{\#\mathbb{F}^{(X+1)/2} X^{r-1}}. \tag{3.1}$$

Further, we let

$$D(C/\mathbb{F}) := \frac{1}{(\#\mathbb{F})^{1/2}} \sum_{\mathrm{ord}\,\gamma = r} \left| \frac{\gamma^r r}{Z^{(r)}_{C/\mathbb{F}}(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \right|. \tag{3.2}$$

(Note that if all inverse zeros are assumed to be simple, then the above definitions (3.1) and (3.2) are the same as in (1.3) and (1.4) of the introduction.) Corollary 2.3 and Theorem 2.6 can then be summarized by saying that

$$B(C/\mathbb{F}) \le D(C/\mathbb{F}), \tag{3.3}$$

and equality holds true if C satisfies LI. In this subsection, we investigate the relationship between the average value of $D(C_f, \mathbb{F}_{q^n})$ over all f in $\mathcal{H}_{2g+1}(\mathbb{F}_{2g+1})$ and a certain integral over the unitary symplectic group $\mathrm{USp}(2g, \mathbb{C})$.

To describe this relationship, we start by defining the characteristic polynomial $\mathcal{Z}_U(\theta)$. (A typographical note: in the literature, this characteristic polynomial is denoted by $Z_U(\theta)$ or $Z(U, \theta)$. We use the calligraphic font to distinguish it from the zeta function $Z_{C/\mathbb{F}_q}(u)$ of a curve C.) Let N be a positive integer. For a $2N \times 2N$ unitary matrix U and a real number θ, we define

$$\mathcal{Z}_U(\theta) := \det(I - Ue^{-i\theta}) = \prod_{m=1}^{2N} (1 - e^{i(\theta_m - \theta)}), \tag{3.4}$$

where $e^{i\theta_1}, \dots, e^{i\theta_{2N}}$ are the eigenvalues of U. When U has no repeated eigenvalues, we define

$$\varphi(U) := \sum_{j=1}^{2N} \frac{1}{|\mathcal{Z}'_U(\theta_j)|}. \tag{3.5}$$

Note that $\varphi(U)$ depends only on the conjugacy class of U. We will be mostly interested in $\varphi(U)$ for $U \in \mathrm{USp}(2g, \mathbb{C})$. Then $\varphi(U)$ is continuous and well-defined outside the measure zero subset where U has a repeated eigenvalue.

Next, for a curve C_f over $\mathbb{F}_{q^n}$, we recall that there exists a certain conjugacy class $\vartheta(C_f/\mathbb{F}_{q^n}) \in \mathrm{USp}(2g, \mathbb{C})^{\#}$, called the *unitarized Frobenius conjugacy class attached to* $C_f/\mathbb{F}_{q^n}$. For its definition, the readers are referred to [11, Chapters 9 and 10 (especially §9.2 and §§10.7.2)]. In this paper, it will be sufficient to say that this is the unique conjugacy class with the property that

$$P_{C_f/\mathbb{F}_{q^n}}(u) = \det\bigl(1 - uq^{n/2}\vartheta(C_f/\mathbb{F}_{q^n})\bigr). \tag{3.6}$$

Finally, we define a *truncated version* of $D(C_f, \mathbb{F}_{q^n})$ using $\varphi(U)$ above. Fix $T > 0$. Then

$$D^T(C_f/\mathbb{F}_{q^n}) := \begin{cases} D(C_f, \mathbb{F}_{q^n}) & \text{if } \varphi(\vartheta(C_f/\mathbb{F}_{q^n})) \le T, \\ 0 & \text{otherwise.} \end{cases} \tag{3.7}$$

Note that the second case in the above definition is used when either $\varphi(\vartheta(C_f/\mathbb{F}_{q^n})) > T$, or $\vartheta(C_f/\mathbb{F}_{q^n})$ has a repeated eigenvalue. The *truncated*

average over $\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})$ is defined by

$$\overline{D}^T(\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})) := \frac{1}{\#\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})} \sum_{f\in\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})} D^T(C_f/\mathbb{F}_{q^n}). \tag{3.8}$$

We are ready to state the main theorem of this section.

THEOREM 3.3. *With the above notation,*

$$\lim_{T\to\infty}\lim_{n\to\infty} \overline{D}^T(\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})) = \int_{\mathrm{USp}(2g,\mathbb{C})} \varphi(U)\, d\mu_{\mathrm{Haar}}(U).$$

Here, $d\mu_{\mathrm{Haar}}$ is the unique probability Haar measure on $\mathrm{USp}(2g,\mathbb{C})$.

REMARK 3.4. The above theorem essentially calculates the first (truncated) moment of $D(C_f,\mathbb{F}_{q^n})$. The work [9] of Humphries, which is based on the present paper in preprint form, carries out a similar calculation to instead determine the cumulative distributive function of $D(C_f,\mathbb{F}_{q^n})$.

Another remark is that it is common in the context of function fields to define $M_{C/\mathbb{F}_q}(X)$ to be the sum over all effective divisors D of $\deg(D)=X$ (that is, our $c_\mu(X)$ in (2.3)), instead of the sum of those with $\deg(D)\le X$. If we adopt this new definition, the expression $D(C_f,\mathbb{F}_q)$ will be slightly different. But, as was shown in [9, §4], this difference is negligible in the large q limit. On the other hand, a similar observation cannot be made in the study of Chebyshev's bias in [3], as one has to sum over all $N\le X$ to make the bias emerge.

Using (3.4) and (3.6), we can easily deduce that

$$\mathcal{Z}_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta) = P_{C_f/\mathbb{F}_{q^n}}((q^{n/2}e^{i\theta})^{-1}) \tag{3.9}$$

for any real θ. Assume that C_f has only simple inverse zeros and write $\gamma_j = q^{n/2}e^{i\theta_j}$. Then we differentiate (3.9) to obtain

$$\frac{\gamma_j}{Z'_{C_f/\mathbb{F}_{q^n}}(\gamma_j{}^{-1})}\,\frac{\gamma_j}{\gamma_j-1} = \frac{1-q^n/\gamma_j}{i\mathcal{Z}'_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta_j)}. \tag{3.10}$$

Further, assume that $\varphi(\vartheta(C_f/\mathbb{F}_{q^n}))\le T$. Then we sum (3.10) over $j=1,\dots,2g$; by setting $r=1$ in (3.2), this yields

$$\begin{aligned} D(C_f/\mathbb{F}_{q^n}) &= \frac{1}{q^{n/2}}\sum_{j=1}^{2g}\left|\frac{1-q^n/\gamma_j}{i\mathcal{Z}'_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta_j)}\right| \\ &= \sum_{j=1}^{2g}\left(\frac{1}{|\mathcal{Z}'_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta_j)|} + \frac{1}{q^{n/2}}\,\frac{A(f,j)}{|\mathcal{Z}'_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta_j)|}\right), \end{aligned} \tag{3.11}$$

where $A(f,j)$ is a constant with $|A(f,j)|\le 1$.

Now, we compute $\overline{D}^T(\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})$ from its definition (3.8) by summing (3.11) over all $f \in \mathcal{H}_{2g+1}$ with $\varphi(\vartheta(C_f/\mathbb{F}_{q^n})) \le T$. As a result,

$$\overline{D}^T(\mathcal{H}_{2g+1}(\mathbb{F}_{q^n}) = \frac{1}{\#\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})} \sum_{\varphi(\vartheta(C_f/\mathbb{F}_{q^n}))\le T} \sum_{j=1}^{2g} \frac{1}{|\mathcal{Z}'_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta_j)|} + \frac{1}{\#\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})} \sum_{\varphi(\vartheta(C_f/\mathbb{F}_{q^n}))\le T} \sum_{j=1}^{2g} O\Big(\frac{1}{q^{n/2}} \frac{1}{|\mathcal{Z}'_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta_j)|}\Big). \tag{3.12}$$

The next step is to let $n \to \infty$ in (3.12) and to apply Deligne's equidistribution theorem [11, Theorem 10.8.2]. The right side of the first line of (3.12) then becomes

$$\lim_{n\to\infty} \frac{1}{\#\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})} \sum_{\varphi(\vartheta(C_f/\mathbb{F}_{q^n}))\le T} \sum_{j=1}^{2g} \frac{1}{|\mathcal{Z}'_{\vartheta(C_f/\mathbb{F}_{q^n})}(\theta_j)|} = \int_{\varphi\le T} \varphi(U)\, d\mu_{\mathrm{Haar}}(U).$$

The second line of (3.12) converges to zero as $n \to \infty$ due to the $q^{n/2}$ term in the denominator and the convergence of the first line. In other words, we have proved that

$$\lim_{n\to\infty} \overline{D}^T(\mathcal{H}_{2g+1}(\mathbb{F}_{q^n})) = \int_{\varphi\le T} \varphi(U)\, d\mu_{\mathrm{Haar}}(U).$$

The proof of Theorem 3.3 is now completed by letting $T \to \infty$.

4. Averages of characteristic polynomials on unitary symplectic groups. Recall that, for a $2N \times 2N$ unitary matrix U and a real number θ, the function $\mathcal{Z}_U(\theta)$ was defined in (3.4) by

$$\mathcal{Z}_U(\theta) := \det(I - Ue^{-i\theta}) = \prod_{m=1}^{2N} (1 - e^{i(\theta_m - \theta)}),$$

where $e^{i\theta_1}, \dots, e^{i\theta_{2N}}$ are the eigenvalues of U. Also, the function $\varphi(U)$ is defined in (3.5) by

$$\varphi(U) := \sum_{j=1}^{2N} \frac{1}{|\mathcal{Z}'_U(\theta_j)|}$$

whenever U has no repeated eigenvalues. When $U \in \mathrm{USp}(2N, \mathbb{C})$, its eigenangles $\theta_1, \dots, \theta_{2N}$ come in complex conjugate pairs; we will enumerate them so that $0 \le \theta_j \le \pi$ for $j = 1, \dots, N$ and $\theta_{N+1} = -\theta_1, \dots, \theta_{2N} = -\theta_N$. The main theorem of this section is Theorem 4.1, where we give an asymptotic formula for the $2s$th moment of $\mathcal{Z}_U(\theta)$ in $\mathrm{USp}(2N, \mathbb{C})$ using the work of Deift, Its, and Krasovsky [6]. Additionally, we prove a similar result for $\mathrm{SO}(2N)$ in Theorem 4.2 as well.

THEOREM 4.1 (cf. [12, Theorem 5]). *Fix a complex number s with $\Re(s) > -1/2$ and a (real) θ with $0 < \theta < \pi$. As $N \to \infty$,*

$$\int_{\mathrm{USp}(2N,\mathbb{C})} |\mathcal{Z}_U(\theta)|^{2s}\, d\mu_{\mathrm{Haar}}(U) \sim N^{s^2} 2^{-s} (\sin\theta)^{-s(s+1)} \frac{G(1+s)^2}{G(1+2s)}.$$

Here, $G(z)$ is the Barnes G-function.

Proof. During the proof, we use the notation

$$\langle |\mathcal{Z}_U(\theta)|^{2s} \rangle_{\mathrm{USp}(2N,\mathbb{C})} := \int_{\mathrm{USp}(2N,\mathbb{C})} |\mathcal{Z}_U(\theta)|^{2s}\, d\mu_{\mathrm{Haar}}(U). \tag{4.1}$$

We first rewrite

$$|\mathcal{Z}_U(\theta)| = \prod_{j=1}^{N} |1 - e^{i(\theta_j - \theta)}|\, |1 - e^{i(\theta_j + \theta)}| = 2^N \prod_{j=1}^{N} |\cos\theta_j - \cos\theta|. \tag{4.2}$$

This can be done by applying to (3.4) the straightforward trigonometric identity

$$|1 - e^{i(\theta_j - \theta_k)}|\, |1 - e^{i(\theta_j + \theta_k)}| = 2|\cos\theta_j - \cos\theta_k|. \tag{4.3}$$

To integrate (4.2), we use the Weyl integration formula, which describes the Haar measures on classical matrix groups explicitly in terms of eigenangles. The version we use here is [11, (5.0.4)], recalled below. Define the measure $\mu(\mathrm{USp}(2N))$ on $[0,\pi]^N$ to be

$$d\mu(\mathrm{USp}(2N)) = \frac{2^{N^2}}{N!\pi^N} \prod_{1 \le j < k \le N} (\cos\theta_j - \cos\theta_k)^2 \prod_{j=1}^{N} \sin^2\theta_j \prod_{j=1}^{N} d\theta_j, \tag{4.4}$$

where $d\theta_1, \ldots, d\theta_N$ refer to the usual Lebesgue measure on $[0,\pi]$. Then the Weyl integration formula says that, for a bounded, Borel measurable $\mathbb{R}$-valued central function g on $\mathrm{USp}(2N,\mathbb{C})$, we have

$$\int_{\mathrm{USp}(2N,\mathbb{C})} g(U)\, d\mu_{\mathrm{Haar}}(U) = \int_{[0,\pi]^N} \tilde{g}(\theta_1, \ldots, \theta_N)\, d\mu(\mathrm{USp}(2N)). \tag{4.5}$$

Here, $\tilde{g}$ is the function on $[0,\pi]^N$ defined by the property

$$\tilde{g}(\theta_1, \ldots, \theta_N) = g(U),$$

whenever $\theta_1, \ldots, \theta_N, -\theta_1, \ldots, -\theta_N$ are the eigenangles of $U \in \mathrm{USp}(2N,\mathbb{C})$. Now, from (4.1), (4.2), (4.4) and (4.5), we have

$$\langle |\mathcal{Z}_U(\theta)|^{2s} \rangle_{\mathrm{USp}(2N,\mathbb{C})} = \frac{2^{N^2+2sN}}{N!\pi^N} \int\limits_{[0,\pi]^N} \prod_{1\le j<k\le N} (\cos\theta_j - \cos\theta_k)^2 \times \prod_{j=1}^{N} |\cos\theta_j - \cos\theta|^{2s} \sin^2\theta_j \, d\theta_j.$$

Note that the expression $\prod_{1\le j<k\le N}(\cos\theta_k - \cos\theta_j)$ is the same as the Vandermonde determinant $\Delta(\cos\theta_1, \dots, \cos\theta_j)$ where

$$\Delta(x_1, \dots, x_N) := \det\,(x_i^{j-1})_{1\le i,j\le N}.$$

Set $y = \cos\theta$. Then clearly $0 < y < 1$. Also, we use the change of variables $x_j = \cos\theta_j$ to obtain

$$\langle |\mathcal{Z}_U(\theta)|^{2s} \rangle_{\mathrm{USp}(2N,\mathbb{C})} = \frac{2^{N^2+2sN}}{N!\pi^N} \int\limits_{[-1,1]^N} \Delta(x_1, \dots, x_N)^2 \prod_{j=1}^{N} w_y(x_j)\, dx_j. \tag{4.6}$$

Here, the weight function $w_y(x)$ is defined by

$$w_y(x) := |x - y|^{2s} \sqrt{1 - x^2}.$$

Now, we will use the *Andréief identity*

$$\frac{1}{N!} \int\limits_{X^n} \det\,[f_j(x_k)]_{1\le j,k\le N} \det\,[g_j(x_k)]_{1\le j,k\le N} \prod_{j=1}^{N} w(x_j)\, dx_j = \det\Big[\int\limits_X f_j(x) g_k(x) w(x)\, dx \Big]_{1\le j,k\le N} \tag{4.7}$$

for any interval X in $\mathbb{R}$. Setting $f_j(x) = g_j(x) = x^{j-1}$ and $X = [-1, 1]$ in (4.7), we can rewrite (4.6) as

$$\langle |\mathcal{Z}_U(\theta)|^{2s} \rangle_{\mathrm{USp}(2N,\mathbb{C})} = \frac{2^{N^2+2sN}}{\pi^N} \det\Big[\int\limits_{-1}^{1} x^{j+k} w_y(x)\, dx \Big]_{0\le j,k\le N-1}. \tag{4.8}$$

The determinant in (4.8) is called a *determinant of Hankel's type* [25] with weight $w_y(x)$. We need an asymptotic expression for Hankel's determinant when the weight function is not differentiable. We use a result of Deift, Its, and Krasovsky [6], which can be applied to much more general weight functions than our $w_y(x)$. In particular, Theorem 1.20 of [6] with

$$V \equiv 0, \quad b_\pm \equiv 1, \quad \begin{cases} \alpha_0 = 1/4, \\ \alpha_1 = s, \\ \alpha_2 = 1/4, \end{cases} \quad \begin{cases} \lambda_0 = 1, \\ \lambda_1 = y, \\ \lambda_2 = -1, \end{cases} \quad \beta_i = 0 \text{ for all } i \tag{4.9}$$

gives

(4.10)

$$\det\Big[\int_{-1}^{1} x^{j+k} w_y(x)\,dx\Big]_{0\le j,k\le N-1} = 4^{-(sN+N/2+s/2+3/16)}(2\pi)^{1/2}N^{s^2+1/4}$$
$$\times 2^{-1/8}|1-y^2|^{-s/2}G(3/2)^{-2}(1-y^2)^{-s^2/2}\frac{G(1+s)^2}{G(1+2s)}\,\frac{\pi^{N+1/2}G(1/2)^2}{2^{N(N-1)}N^{1/4}}(1+o(1))$$

as $N\to\infty$. Further simplification yields

$$\det\Big[\int_{-1}^{1} x^{j+k} w_y(x)\,dx\Big]_{0\le j,k\le N-1} = \frac{\pi^N}{2^{N^2+2sN}}2^{-s}N^{s^2}(1-y^2)^{-(s^2+s)/2}\frac{G(1+s)^2}{G(1+2s)}(1+o(1)).$$

Combining this with (4.8) (and remembering $y=\cos\theta$), we finish the proof of the theorem. ∎

Even though we do not need it in this paper, we prove a similar formula for $\mathrm{SO}(2N)$ in place of $\mathrm{USp}(2N,\mathbb{C})$, as its proof can be obtained with very little change.

THEOREM 4.2. *Fix a complex number s with $\Re(s)>-1/2$ and a (real) θ with $0<\theta<\pi$. As $N\to\infty$,*

$$\int_{\mathrm{SO}(2N)} |\mathcal{Z}_U(\theta)|^{2s}\,d\mu_{\mathrm{Haar}}(U) \sim N^{s^2}2^s(\sin\theta)^{-s(s-1)}\frac{G(1+s)^2}{G(1+2s)}.$$

Here, $G(z)$ is the Barnes G-function.

Proof. The proof is almost entirely analogous to that of Theorem 4.1 with very minor modification. Start with [11, (5.0.6)], which simplifies to

$$d\mu(\mathrm{SO}(2N)) = \frac{2^{(N-1)^2}}{N!\pi^N}\prod_{1\le j<k\le N}(\cos\theta_j-\cos\theta_k)^2\prod_{j=1}^{N}d\theta_j. \tag{4.11}$$

The analogue of (4.8) becomes

$$\langle|\mathcal{Z}_U(\theta)|^{2s}\rangle_{\mathrm{SO}(2N)} = \frac{2^{(N-1)^2+2sN}}{\pi^N}\det\Big[\int_{-1}^{1} x^{j+k} w_y(x)\,dx\Big]_{0\le j,k\le N-1} \tag{4.12}$$

with the (slightly different) weight function

$$w_y(x) := \frac{|x-y|^{2s}}{\sqrt{1-x^2}}.$$

Then we apply [6, Theorem 1.20] again with the same parameters as in (4.9), except for $\alpha_0 = \alpha_2 = -1/4$. The result follows from this. ∎

REMARK 4.3. Theorems 4.1 and 4.2 extend the previous work of Keating and Snaith [14] and [15], and that of Keating and Odgers [12] on the (asymptotic) formulas for the $2s$th moments $\langle |\mathcal{Z}_U(\theta)|^{2s} \rangle$ for different values of θ and $G \in \{\mathrm{U}(N), \mathrm{SO}(2N), \mathrm{USp}(2N, \mathbb{C})\}$. This is summarized in Table 1. The first three rows in the table are due to Keating and Snaith, the next two rows are proved by Keating and Odgers, and Theorems 4.1 and 4.2 give the last two.

Table 1. Known cases of moments of characteristic polynomials

θ	s	G
θ arbitrary	$\Re(s) > -1$	$\mathrm{U}(N)$
$\theta = 0$	$\Re(s) > -3/2$	$\mathrm{USp}(2N, \mathbb{C})$
$\theta = 0$	$\Re(s) > -1/2$	$\mathrm{SO}(2N)$
θ arbitrary	$s \in \mathbb{N}$	$\mathrm{USp}(2N, \mathbb{C})$
θ arbitrary	$s \in \mathbb{N}$	$\mathrm{SO}(2N)$
θ arbitrary	$\Re(s) > -1/2$	$\mathrm{USp}(2N, \mathbb{C})$
θ arbitrary	$\Re(s) > -1/2$	$\mathrm{SO}(2N)$

In view of Theorem 3.3, it would be desirable to obtain an asymptotic expression of

$$\mathcal{I}(N) := \int_{\mathrm{USp}(2N,\mathbb{C})} \varphi(U)\, d\mu_{\mathrm{Haar}}(U) \tag{4.13}$$

as $N \to \infty$, because this could be thought of as a function field analog (for the family $\mathcal{H}_{2g+1}$) of the $(\log\log\log x)^{5/4}$ term in (1.2). Using Theorem 4.1 (for $s = 1/2$), we present some evidence in support of the formula

$$\mathcal{I}(N) \sim \sqrt{2}\, G(1/2)^2 B(5/8, 1/2) N^{1/4}. \tag{4.14}$$

Here, $G(z)$ is the Barnes G-function and $B(x, y)$ is the beta function

$$B(x, y) = \int_0^1 t^{x-1}(1-t)^{y-1}\, dt.$$

The rest of the paper is devoted to presenting the argument in support of (4.14). Our computation closely follows the strategy used by Hughes, Keating, and O'Connell in [8, proof of Theorem 1.2].

Straightforward differentiation of $\mathcal{Z}_U(\theta)$ in (3.4) gives

$$|\mathcal{Z}_U'(\theta_j)| = |1 - e^{2i\theta_j}| \prod_{\substack{k=1 \\ k \neq j}}^{N} |1 - e^{i(\theta_j - \theta_k)}|\, |1 - e^{i(\theta_j + \theta_k)}| \tag{4.15}$$

for $j = 1, \dots, N$. Using (4.3) and another easy trigonometric identity,

$$|1 - e^{2i\theta_j}| = 2|\sin\theta_j|,$$

one easily deduces from (4.15) that

$$|\mathcal{Z}'_U(\theta_j)| = 2^N |\sin\theta_j| \prod_{\substack{k=1 \\ k\neq j}}^{N} |\cos\theta_j - \cos\theta_k|.$$

Also, obviously $|\mathcal{Z}_U(\theta_{N+j})| = |\mathcal{Z}_U(-\theta_j)| = |\mathcal{Z}_U(\theta_j)|$ for $j = 1, \dots, N$. Hence,

$$\varphi(U) = \sum_{m=1}^{2N} |\mathcal{Z}'_U(\theta_m)|^{-1} = 2^{1-N} \sum_{j=1}^{N} |\sin\theta_j|^{-1} \prod_{\substack{k=1 \\ k\neq j}}^{N} |\cos\theta_j - \cos\theta_k|^{-1}. \tag{4.16}$$

To integrate $\varphi(U)$ over $\mathrm{USp}(2N, \mathbb{C})$, we use the Weyl integration formula again: from (4.16), (4.4) and (4.5),

$$\begin{aligned}
\mathcal{I}(N) &= \int_{\mathrm{USp}(2N,\mathbb{C})} \varphi(U)\, d\mu_{\mathrm{Haar}}(U) \\
&= \frac{2^{N^2-N+1}}{N!\pi^N} \int_{[0,\pi]^N} \Big[\sum_{j=1}^{N} |\sin\theta_j|^{-1} \prod_{\substack{k=1 \\ k\neq j}}^{N} |\cos\theta_j - \cos\theta_k|^{-1} \Big] \\
&\qquad \times \prod_{1\le j<k\le N} (\cos\theta_j - \cos\theta_k)^2 \prod_{j=1}^{N} \sin^2\theta_j \prod_{j=1}^{N} d\theta_j.
\end{aligned}$$

Since the expression in square brackets inside the above integral is symmetric in θ_j's, we can replace the summation on j by N times any single summand, say, the $j = N$ term. This yields

$$\begin{aligned}
\mathcal{I}(N) &= \frac{2^{N^2-N+1}}{(N-1)!\pi^N} \int_{[0,\pi]^N} \Big[|\sin\theta_N|^{-1} \prod_{k=1}^{N-1} |\cos\theta_N - \cos\theta_k|^{-1} \Big] \\
&\qquad \times \prod_{1\le j<k\le N} (\cos\theta_j - \cos\theta_k)^2 \prod_{j=1}^{N} \sin^2\theta_j \prod_{j=1}^{N} d\theta_j \\
&= \frac{2^{N^2-N+1}}{(N-1)!\pi^N} \int_{[0,\pi]^N} \Big[|\sin\theta_N| \prod_{k=1}^{N-1} |\cos\theta_N - \cos\theta_k| \Big] \\
&\qquad \times \prod_{1\le j<k\le N-1} (\cos\theta_j - \cos\theta_k)^2 \prod_{j=1}^{N-1} \sin^2\theta_j \prod_{j=1}^{N} d\theta_j.
\end{aligned} \tag{4.17}$$

Again, (4.3) can be used to rewrite the expression in square brackets as

$$|\sin\theta_N| \prod_{k=1}^{N-1} |\cos\theta_N - \cos\theta_k| = |\sin\theta_N| \prod_{k=1}^{N-1} \tfrac{1}{2}|1 - e^{i(\theta_k-\theta_N)}|\,|1 - e^{i(\theta_k+\theta_N)}|$$
$$= 2^{1-N}|\sin\theta_N|\,|\mathcal{Z}_U(\theta_N)|,$$

where $U \in \mathrm{USp}(2(N-1))$ has eigenangles $\pm\theta_1, \dots, \pm\theta_{N-1}$. So, we continue (4.17) to get

$$\mathcal{I}(N) = \frac{2^{(N-1)^2}}{(N-1)!\pi^N} \int_{[0,\pi]^N} 2|\sin\theta_N|\,|\mathcal{Z}_U(\theta_N)| \times \prod_{1\le j<k\le N-1} (\cos\theta_j - \cos\theta_k)^2 \prod_{j=1}^{N-1} \sin^2\theta_j \prod_{j=1}^{N} d\theta_j$$
$$= \frac{2}{\pi} \int_{[0,\pi]} \sin\theta_N \Big(\int_{\mathrm{USp}(2(N-1))} |\mathcal{Z}_U(\theta_N)|\, d\mu_{\mathrm{Haar}}(U) \Big) d\theta_N, \tag{4.18}$$

where the last equality is again from the Weyl integration formula (4.4) and (4.5), applied to $\mathrm{USp}(2(N-1))$. The integral in parentheses is precisely $\langle |\mathcal{Z}_U(\theta_N)|^{2s} \rangle_{\mathrm{USp}(2(N-1))}$ with $s = 1/2$, whose asymptotic expression is found in Theorem 4.1. Therefore, after some simplification, we find that

$$\mathcal{I}(N) = \sqrt{2}\, G(1/2)^2 N^{1/4} \int_0^\pi (\sin\theta)^{1/4}(1 + o(1))\, d\theta \tag{4.19}$$

as $N \to \infty$.

Remark 4.4. In order to prove (4.14), we let $N \to \infty$ in (4.19). If we can exchange limit and integral, then the integral of $(\sin\theta)^{1/4}$ is expressed in terms of the beta function, which would finish the proof of (4.14). The key step here, therefore, is to estimate the size of the $o(1)$-term in (4.19) with respect to θ.

This error term comes from the formula of Deift, Its, and Krasovsky, quoted in (4.10). See [6, Remark 1.6] for some general discussion on the size of their error term. Let $\epsilon_N(\theta)$ be the $o(1)$-term in (4.19). If one can show that $(\sin\theta)^{1/4}\epsilon_N(\theta)$ is bounded by a function in $L^1([0,\pi])$ independently of N, then the dominated convergence theorem can be used to justify the exchange of limit and integral.

In fact, we can show that $\epsilon_N(\theta)$ does *not* tend to zero uniformly in θ as follows. Define

$$f_N(\theta) := \int_{\mathrm{USp}(2N,\mathbb{C})} |\mathcal{Z}_U(\theta)|\, d\mu_{\mathrm{Haar}}(U).$$

Then it is known that

$$f_N(0) \sim N,$$

from a result in [15]. (Alternatively, one can use the formula of Deift, Its, and Krasovsky and proceed exactly as in the proof of Theorem 4.1.) If we assume that the error term in Theorem 4.1 is bounded uniformly in θ, we can pick N large enough, so that $f_N(\theta)$ is about (a constant times) $N^{1/4}(\sin\theta)^{-3/4}$, for all θ close to 0. If we now choose θ in the range $0 < \theta < 1/N^2$, then this contradicts the continuity of $f_N(\theta)$ at $\theta = 0$. So, $\epsilon_N(\theta)$ does not tend to 0 uniformly in θ as $N \to \infty$. Therefore, further investigation of $\epsilon_N(\theta)$ is warranted to justify the exchange of limit and integral in (4.19).

Acknowledgements. The author is greatly indebted to Emmanuel Kowalski for a helpful discussion, and to Jinho Baik who brought to the author's attention the work of Deift, Its and Krasovsky [6] and explained its usefulness in proving Theorem 4.1. Also, the author is grateful to Peter Humphries, who found an error in Proposition 2.2 in an earlier version of this paper, in addition to offering many other helpful remarks. Finally, he is grateful to the anonymous referee for making numerous corrections and suggestions.

References

[1] J. D. Achter and R. Pries, *The integral monodromy of hyperelliptic and trielliptic curves*, Math. Ann. 338 (2007), 187–206.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[3] B. Cha, *Chebyshev's bias in function fields*, Compos. Math. 144 (2008), 1351–1374.

[4] B. Cha and B.-H. Im, *Chebyshev's bias in Galois extensions of global function fields*, J. Number Theory 131 (2011), 1875–1886.

[5] N. Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. 87 (1997), 151–180.

[6] P. Deift, A. Its and I. Krasovsky, *Asymptotics of Toeplitz, Hankel, and Toeplitz +Hankel determinants with Fisher–Hartwig singularities*, Ann. of Math. (2) 174 (2011), 1243–1299.

[7] C. Hall, *Big symplectic or orthogonal monodromy modulo l*, Duke Math. J. 141 (2008), 179–203.

[8] C. P. Hughes, J. P. Keating and N. O'Connell, *Random matrix theory and the derivative of the Riemann zeta function*, Roy. Soc. London Proc. Ser. A Math. Phys. Engrg. Sci. 456 (2000), 2611–2627.

[9] P. Humphries, *On the Mertens conjecture for function fields*, Int. J. Number Theory 10 (2014), 341–361.

[10] A. E. Ingham, *On two conjectures in the theory of numbers*, Amer. J. Math. 64 (1942), 313–319.

[11] N. M. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*, Amer. Math. Soc. Colloq. Publ. 45, Amer. Math. Soc., Providence, RI, 1999.

[12] J. P. Keating and B. E. Odgers, *Symmetry transitions in random matrix theory & L-functions*, Comm. Math. Phys. 281 (2008), 499–528.
[13] J. Keating and Z. Rudnick, *Squarefree polynomials and Möbius values in short intervals and arithmetic progressions*, Algebra Number Theory 10 (2016), 375–420.
[14] J. P. Keating and N. C. Snaith, *Random matrix theory and* $\zeta(1/2 + it)$, Comm. Math. Phys. 214 (2000), 57–89.
[15] J. P. Keating and N. C. Snaith, *Random matrix theory and L-functions at* $s = 1/2$, Comm. Math. Phys. 214 (2000), 91–110.
[16] E. Kowalski, *The large sieve, monodromy and zeta functions of curves*, J. Reine Angew. Math. 601 (2006), 29–69.
[17] E. Kowalski, *The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros*, Int. Math. Res. Notices 2008, art. ID rnn 091, 57 pp.
[18] H. Maier and H. L. Montgomery, *The sum of the Möbius function*, Bull. London Math. Soc. 41 (2009), 213–226.
[19] F. Mertens, *Über eine zahlentheoretische Funktion*, Sitzungsberichte Akad. Wien 106 (1897), 761–830.
[20] N. Ng, *The distribution of the summatory function of the Möbius function*, Proc. London Math. Soc. (3) 89 (2004), 361–389.
[21] A. M. Odlyzko and H. J. J. te Riele, *Disproof of the Mertens conjecture*, J. Reine Angew. Math 357 (1985), 138–160.
[22] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, New York, 2002.
[23] M. Rubinstein and P. Sarnak, *Chebyshev's bias*, Experiment. Math. 3 (1994), 173–197.
[24] K. Soundararajan, *Partial sums of the Möbius function*, J. Reine Angew. Math. 631 (2009), 141–152.
[25] G. Szegő, *Orthogonal polynomials*, 4th ed., Amer. Math. Soc. Colloq. Publ. 23, Amer. Math. Soc., Providence, RI, 1975.

Byungchul Cha
Department of Mathematics and Computer Science
Muhlenberg College
2400 Chew St.
Allentown, PA 18104, U.S.A.
E-mail: cha@muhlenberg.edu