ON THE MERTENS CONJECTURE FOR FUNCTION FIELDS

PETER HUMPHRIES

Abstract. We study the natural analogue of the Mertens conjecture in the setting of global function fields. Building on the work of Cha, we show that most hyperelliptic curves do not satisfy the Mertens conjecture, but that if we modify the Mertens conjecture to have a larger constant, then this modified conjecture is satisfied by a positive proportion of hyperelliptic curves.

1. The Mertens Conjecture

Let $\mu(n)$ denote the Möbius function, so that for a positive integer n,

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^t & \text{if } n \text{ is the product of } t \text{ distinct primes}, \\ 0 & \text{if } n \text{ is divisible by a perfect square}, \end{cases}$$

and let

$$M(x) = \sum_{n \leq x} \mu(n)$$

be the summatory function of the Möbius function. In 1897, Mertens [12] calculated $M(x)$ from $x = 1$ up to $x = 10\,000$ and conjectured the following inequality.

The Mertens Conjecture. *For all $x \geq 1$, the summatory function of the Möbius function satisfies the inequality*

$$\frac{|M(x)|}{\sqrt{x}} \leq 1. \tag{1}$$

The Mertens conjecture has several important consequences, the most notable of which are that the Riemann hypothesis is true and that all the zeroes of the Riemann zeta function, $\zeta(s)$, are simple; see [14, §2] for further details.

In this article, we study the natural analogue of this conjecture in the setting of global function fields, that is, for nonsingular projective curves over finite fields. Let C be a nonsingular projective curve of genus g over a finite field $\mathbb{F}_q$ of characteristic p; we will assume throughout that p is odd. For each effective divisor N of C, we define the Möbius function of $C/\mathbb{F}_q$ to be

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

so that the summatory function of the Möbius function of $C/\mathbb{F}_q$ is

$$M_{C/\mathbb{F}_q}(X) = \sum_{0 \leq \deg(N) \leq X-1} \mu_{C/\mathbb{F}_q}(N),$$

2010 *Mathematics Subject Classification.* 11N56 (primary); 11G20, 11M50 (secondary).

Key words and phrases. Mertens conjecture, function field, Möbius function, hyperelliptic curve.

This research was partially supported by an Australian Postgraduate Award.

where X is a positive integer. Our goal is to determine the validity of the following conjecture, the analogue of the Mertens conjecture in the function field setting.

The Mertens Conjecture for Function Fields. *Let C be a nonsingular projective curve over $\mathbb{F}_q$. The summatory function of the Möbius function of $C/\mathbb{F}_q$ satisfies*

$$\limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}} \leq 1.$$

While the classical Mertens conjecture states that the inequality (1) holds for all $x \geq 1$, the value 1 on the right-hand side of (1) is, in some sense, not particularly special. Indeed, Stieltjes [17] claimed in 1885 to have a proof that

$$M(x) = O\left(\sqrt{x}\right) \tag{2}$$

without specifying an explicit constant, before later rescinding his claim, though he did postulate that (1) was true. Similarly, von Sterneck [16] conjectured in 1912 that the stronger inequality

$$\frac{|M(x)|}{\sqrt{x}} \leq \frac{1}{2} \tag{3}$$

holds for all $x \geq 200$, based on calculations of $M(x)$ up to 5 000 000. So we may also consider the following variant of the Mertens conjecture for function fields.

The β-Mertens Conjecture for Function Fields. *Let C be a nonsingular projective curve over $\mathbb{F}_q$, and let $\beta > 0$. The summatory function of the Möbius function of $C/\mathbb{F}_q$ satisfies*

$$\limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}} \leq \beta.$$

In spite of the numerical calculations of Mertens and von Sterneck, the inequalities (1) and (3) are both now known to fail infinitely often. Odlyzko and te Riele [14] disproved the Mertens conjecture in 1985, and showed that

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}} > 1.06,$$
$$\liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}} < -1.009.$$

These bounds have since been improved to 1.218 and -1.229 respectively by Kotnik and te Riele [10], and most recently to 1.6383 and -1.6383 respectively by Best and Trudgian [2]. Stieltjes's claimed bound (2) has yet to be disproved, although it seems likely that

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}} = \infty,$$
$$\liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}} = -\infty.$$

Indeed, Ingham [8] showed much earlier in 1942 that this follows from the assumption of the Riemann hypothesis and the linear independence over the rational numbers of the imaginary parts of the zeroes of $\zeta(s)$ in the upper half-plane. The latter hypothesis is known as the Linear Independence hypothesis; while there is as yet a lack of strong theoretical evidence for the falsity of the existence of any rational linear dependence between these imaginary parts, some limited numerical calculations have failed to find any such linear relations [1], [2]. Most recently,

Ingham's result has been refined conditionally by Ng [13], who has shown that the logarithmic density

$$\delta\left(\mathcal{P}_\beta\right) = \lim_{X\to\infty} \frac{1}{\log X} \int_{\mathcal{P}_\beta \cap [1,X]} \frac{dx}{x}$$

of the set

$$\mathcal{P}_\beta = \left\{x \in [1,\infty) : |M(x)| \leq \beta\sqrt{x}\right\}$$

exists and satisfies the bound

$$\delta\left(\mathcal{P}_\beta\right) < 1$$

for all $\beta > 0$, and also that for all sufficiently large β,

$$\delta\left(\mathcal{P}_\beta\right) > 0,$$

all under the assumption of the Riemann hypothesis, the Linear Independence hypothesis, and that

$$J_{-1}(T) = \sum_{0<\gamma\leq T} \left|\zeta'\left(1/2+i\gamma\right)\right|^{-2} \ll T,$$

where the sum is over the nontrivial zeroes of $\zeta(s)$. Numerical calculations of Amir Akbary and Nathan Ng (personal communication) suggest that

$$\delta\left(\mathcal{P}_1\right) > 0.99999993366,$$

so that the set of counterexamples of the Mertens conjecture, despite conditionally having strictly positive logarithmic density, is nevertheless extremely sparsely distributed in $[1,\infty)$.

In the function field setting, on the other hand, the situation is markedly different: if the zeroes of the zeta function $Z_{C/\mathbb{F}_q}(u)$ of $C/\mathbb{F}_q$ are not too poorly behaved, in the sense that $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes, then Cha [3, Corollary 2.3] has shown that

$$\limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}}$$

is bounded. Here $Z_{C/\mathbb{F}_q}(u)$ is defined initially for a complex variable u in the open disc $|u| < q^{-1}$ via the absolutely convergent series

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

where $\#C\left(\mathbb{F}_{q^n}\right)$ denotes the number of points of C in the field extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. This function extends meromorphically to the whole complex plane; indeed,

$$Z_{C/\mathbb{F}_q}(u) = \frac{P_{C/\mathbb{F}_q}(u)}{(1-u)(1-qu)}, \tag{4}$$

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

$$P_{C/\mathbb{F}_q}(u) = \prod_{j=1}^{g} \left(1-\gamma_j u\right)\left(1-\overline{\gamma_j}u\right)$$

for some $\gamma_j = \sqrt{q}e^{i\theta(\gamma_j)}$ with $\theta\left(\gamma_j\right) \in [0,\pi]$; here g is the genus of the curve C. The fact that each γ_j satisfies $|\gamma_j| = \sqrt{q}$ is known as the Riemann hypothesis for function fields, and was proved by Weil in 1940 [19]; as it is already known that the Riemann hypothesis for the Riemann zeta function is intimately connected to the growth of $M(x)$, we can immediately see the benefit of the function field setting. Furthermore, there are only finitely many zeroes of $Z_{C/\mathbb{F}_q}(u)$, so it is actually possible to confirm, given the zeta function of a curve $C/\mathbb{F}_q$, the following function field analogue of the Linear Independence hypothesis.

Definition 1.1. We say that C satisfies the *Linear Independence hypothesis*, which we abbreviate to LI, if the collection

$$\pi, \theta(\gamma_1), \dots, \theta(\gamma_g)$$

is linearly independent over the rational numbers.

See [11, §6] for examples of computationally determining whether a particular curve satisfies LI. Note also that the zeta function of a curve satisfying LI must only have simple zeroes.

In [3], Cha proves the following result about the maximal order of growth of $M_{C/\mathbb{F}_q}(X)$.

Theorem 1.2 (Cha [3, Theorem 2.5])**.** *Suppose that C is a nonsingular projective curve of genus $g \geq 1$ that satisfies* LI*. Then*

$$\limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}} = 2\sum_{j=1}^{g} \left| \frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} \right| < \infty. \tag{5}$$

Cha also shows [3, page 5] that the case $g = 0$ is trivial, where $C = \mathbb{P}^1$ is the projective line, so that $C/\mathbb{F}_q$ is simply the rational function field $\mathbb{F}_q(t)$, for then

$$M_{\mathbb{F}_q(t)}(X) = \begin{cases} 1 & \text{if } X = 1, \\ -q & \text{if } X = 2, \\ 0 & \text{if } X \geq 3. \end{cases}$$

Note that in this case

$$Z_{\mathbb{F}_q(t)}(u) = \frac{1}{(1-u)(1-qu)}$$

is the completed zeta function of the zeta function

$$Z_{\mathbb{F}_q[t]}(u) = \frac{1}{1-qu}$$

of the ring $\mathbb{F}_q[t]$. One can define the Möbius function of a polynomial in $\mathbb{F}_q[t]$ in the same fashion as for a global function field $C/\mathbb{F}_q$ and show similarly that

$$M_{\mathbb{F}_q[t]}(X) = \begin{cases} 1 & \text{if } X = 1, \\ -q+1 & \text{if } X \geq 2; \end{cases}$$

see [15, Chapter 2].

So if a curve C of genus $g \geq 1$ satisfies LI, then we need only determine the right-hand side of (5) in order to see whether $C/\mathbb{F}_q$ satisfies the Mertens conjecture. Unlike in the classical case, however, where we expect the Riemann zeta function to satisfy LI, there do exist curves C that do not satisfy LI; furthermore, in the particular case when $Z_{C/\mathbb{F}_q}(u)$ has zeroes of multiple order, then the work of Cha [3, Proposition 2.2] indicates that

$$\limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}} = \infty.$$

Nevertheless, we can ensure that such curves are extremely rare by restricting to certain families of curves, namely hyperelliptic curves. With this family, we also have the added bonus of a framework for certain equidistribution results and connections to random matrix theory via the work of Katz and Sarnak [9].

We define this family of curves as follows: for $\mathbb{F}_{q^n}$ a finite field of odd characteristic, and for $g \geq 1$, let f be a monic polynomial of degree $2g+1$ with coefficients in $\mathbb{F}_{q^n}$ whose discriminant is nonzero; equivalently, let f be a squarefree monic polynomial in $\mathbb{F}_{q^n}[x]$ of degree $2g+1$. Each such polynomial f thereby defines a hyperelliptic curve C_f of genus g over $\mathbb{F}_{q^n}$ via the affine model $y^2 = f(x)$. So we

let $\mathcal{H}_{2g+1,q^n}$ denote the set of these hyperelliptic curves $C = C_f$ over $\mathbb{F}_{q^n}$. We are interested in properties of such curves C shared by "most" $C \in \mathcal{H}_{2g+1,q^n}$. To define this notion, we consider $\mathcal{H}_{2g+1,q^n}$ as a probability space with the uniform probability measure, so that for a property D of a hyperelliptic curve $C \in \mathcal{H}_{2g+1,q^n}$,

$$\mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}(C \text{ satisfies } D) = \frac{\#\{C \in \mathcal{H}_{2g+1,q^n} : C \text{ satisfies } D\}}{\#\mathcal{H}_{2g+1,q^n}}.$$

Definition 1.3. We say that *most* hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ have the property $D = \{D_n\}_{n=1}^{\infty}$ as n tends to infinity if

$$\lim_{n\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}(C \text{ satisfies } D_n) = 1.$$

We are now able to state the main result of this article.

Theorem 1.4. *Let q and $g \geq 1$ be fixed. Then we have that*

$$\lim_{n\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}(C \text{ satisfies the } \beta\text{-Mertens conjecture}) = 0$$

for $0 < \beta \leq 1$, whereas when $\beta > 1$,

$$0 < \lim_{n\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}(C \text{ satisfies the } \beta\text{-Mertens conjecture}) < 1.$$

That is, as n tends to infinity, most hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ do not satisfy the Mertens conjecture, but for any $\beta > 1$, a positive proportion of hyperelliptic curves satisfy the β-Mertens conjecture.

So although the Mertens conjecture is false for most hyperelliptic curves, the value $\beta = 1$ is critical, in that it is the greatest value of β for which the β-Mertens conjecture is not satisfied for most hyperelliptic curves.

Results of this form were found by the author [7] in the low-genus case $g = 1$, so that C is an elliptic curve: the author used a classification due to Waterhouse [18] of isogeny classes of elliptic curves over finite fields in terms of their Frobenius angles in order to determine explicitly the isogeny classes for which the Mertens conjecture holds, in the form of the following result.

Theorem 1.5 (Humphries [7, Theorem 2.1])**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Then the Mertens conjecture for $E/\mathbb{F}_q$ is true if and only if the order of the finite field q and the trace a_E of the Frobenius endomorphism acting on E over $\mathbb{F}_q$ satisfy precisely one of the following conditions:*

1. *$q = p^m$ with $a_E = 2$, where either m is arbitrary and $p \neq 2$, or $m = 1$ and $p = 2$,*
2. *$q = p^m$ with $a_E = \sqrt{q}$, where m is even and $p \not\equiv 1 \pmod 3$,*
3. *$q = p^m$ with $a_E = 0$, where either m is even and $p \not\equiv 1 \pmod 4$, or m is odd.*

In all these cases, we have that

$$\limsup_{X\to\infty} \frac{\left|M_{E/\mathbb{F}_q}(X)\right|}{q^{X/2}} = 1.$$

While recent work of Howe, Nart, and Ritzenthaler [5] classifies the isogeny classes of curves of genus two, there is as yet no such classification for curves of genus $g \geq 3$, so this method does not generalise to curves of large genus; indeed, a classification of isogeny classes of curves of a given genus g would involve explicitly solving the (open) Schottky problem, namely giving an explicit description of all principally polarised abelian varieties that are Jacobian varieties of curves.

Instead, the methods for proving Theorem 1.4 involve relating the average

$$\lim_{n\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}(C \text{ satisfies the } \beta\text{-Mertens conjecture})$$

to the Haar measure on a certain compact group of random matrices, then analysing the behaviour of the resulting probability value. These methods are closely related to the work of Cha [3], from which many of the results in this paper originate; in [3], Cha introduces the summatory function $M_{C/\mathbb{F}_q}(X)$ and studies a truncated form of the average of $\left|M_{C/\mathbb{F}_q}(X)\right|/q^{X/2}$ over function fields,

$$\lim_{n\to\infty}\frac{1}{\#\mathcal{H}_{2g+1,q^n}}\sum_{C\in\mathcal{H}_{2g+1,q^n}}\left(\limsup_{X\to\infty}\frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}}\right).$$

Using random matrix methods, Cha is led to conjecture that this truncated average, after taking the limit as n tends to infinity, is asymptotic to $cg^{1/4}$ in the limit as g tends to infinity, where c is a specific given constant.

2. Preliminary Results

We begin by converting this problem to a related problem for a certain family of random matrices. Our first step is to express the quantity

$$B\left(C/\mathbb{F}_q\right)=\limsup_{X\to\infty}\frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}}$$

in the language of unitary symplectic matrices. Recall that the space of unitary symplectic matrices $\mathrm{USp}(2g)$ consists of $2g\times 2g$ matrices U with complex entries satisfying $U^{\dagger}U=I$ and $U^{T}JU=J$, where

$$J=\begin{pmatrix}0 & I_g\\ -I_g & 0\end{pmatrix}$$

and I_g denotes the $g\times g$ identity matrix. The eigenvalues of U lie on the unit circle and come in complex conjugate pairs, so that we may order the eigenvalues $e^{i\theta_1},\dots,e^{i\theta_{2g}}$ such that $\theta_{j+g}=-\theta_j$ with $0\leq\theta_j\leq\pi$ for $1\leq j\leq g$. Conversely, given $(\theta_1,\dots,\theta_g)\in[0,\pi]^g$, the diagonal matrix with diagonal entries $e^{i\theta_1},\dots,e^{i\theta_g},e^{-i\theta_1},\dots,e^{-i\theta_g}$ lies in $\mathrm{USp}(2g)$. Thus the set of conjugacy classes $\mathrm{USp}(2g)^{\#}$ of $\mathrm{USp}(2g)$ corresponds to $[0,\pi]^g$.

Definition 2.1. For each $U\in\mathrm{USp}(2g)$, we define the *characteristic polynomial* $\mathcal{Z}_U(\theta)$ for real θ by

$$\mathcal{Z}_U(\theta)=\det\left(I-Ue^{-i\theta}\right).$$

Equivalently,

$$\mathcal{Z}_U(\theta)=\prod_{j=1}^{2g}\left(1-e^{i(\theta_j-\theta)}\right)=2^g\prod_{j=1}^{g}e^{i\theta}\left(\cos\theta-\cos\theta_j\right). \tag{6}$$

For a nonsingular projective curve C over $\mathbb{F}_q$ of genus $g\geq 1$, there exists a conjugacy class $\vartheta\left(C/\mathbb{F}_q\right)$ in $\mathrm{USp}(2g)^{\#}$, called the unitarised Frobenius conjugacy class attached to $C/\mathbb{F}_q$, satisfying

$$\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}(\theta)=P_{C/\mathbb{F}_q}\left(\frac{e^{-i\theta}}{\sqrt{q}}\right)=\prod_{j=1}^{g}\left(1-e^{i(\theta(\gamma_j)-\theta)}\right)\left(1-e^{-i(\theta(\gamma_j)+\theta)}\right). \tag{7}$$

That is, the eigenangles $(\theta_1,\dots,\theta_g)$ corresponding to the unitarised Frobenius conjugacy class $\vartheta\left(C/\mathbb{F}_q\right)$ are precisely $\left(\theta\left(\gamma_1\right),\dots,\theta\left(\gamma_g\right)\right)$, the angles of the inverse zeroes $\gamma_j=\sqrt{q}e^{i\theta(\gamma_j)}$, $1\leq j\leq g$, of $Z_{C/\mathbb{F}_q}(u)$.

We require an expression for $B\left(C/\mathbb{F}_q\right)$ in terms of $\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}(\theta)$ in the large q limit. For $U\in\mathrm{USp}(2g)$, we define the function $\varphi(U)$ by

$$\varphi(U)=2\sum_{j=1}^{g}\frac{1}{\left|\mathcal{Z}_U{}'\left(\theta_j\right)\right|},$$

where $e^{i\theta_1}, \dots, e^{i\theta_g}, e^{-i\theta_1}, \dots, e^{i\theta_g}$ are the eigenvalues of U, with $0 \leq \theta_j \leq \pi$ for $1 \leq j \leq g$. We observe that φ depends only on the conjugacy class $(\theta_1, \dots, \theta_g)$ of U, and that φ is always nonnegative, though it blows up if U has a repeated eigenvalue. Note, however, that the set of matrices in $\mathrm{USp}(2g)$ with repeated eigenvalues has measure zero with respect to the normalised Haar measure on $\mathrm{USp}(2g)$.

Lemma 2.2 (Cha [3, Equation (26)])**.** *Suppose that C satisfies* LI*. Then we have that*

$$\left(1 - \frac{1}{\sqrt{q}}\right) \varphi\left(\vartheta\left(C/\mathbb{F}_q\right)\right) \leq B\left(C/\mathbb{F}_q\right) \leq \left(1 + \frac{1}{\sqrt{q}}\right) \varphi\left(\vartheta\left(C/\mathbb{F}_q\right)\right).$$

Of course, we cannot say which individual curves satisfy LI without studying their zeroes. Nevertheless, we have the following remarkable result for the family of hyperelliptic curves.

Theorem 2.3 (Cha–Chavdarov–Kowalski [3, Theorem 3.1], [4], [11])**.** *Let q and $g \geq 1$ be fixed. Then*

$$\lim_{n \to \infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}\left(C \text{ satisfies LI}\right) = 1.$$

That is, as n tends to infinity, most hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ satisfy LI*.*

This result is our reason for restricting ourselves to the family of hyperelliptic curves, as well as the usefulness of the following equidistribution theorem.

Theorem 2.4 (Deligne's Equidistribution Theorem [9, Theorem 10.8.2])**.** *Let f be a continuous function on $\mathrm{USp}(2g)$ that is central, so that f is dependent only on the conjugacy class $(\theta_1, \dots, \theta_g)$ of each matrix $U \in \mathrm{USp}(2g)$. Let q and $g \geq 1$ be fixed. Then*

$$\lim_{n \to \infty} \frac{1}{\#\mathcal{H}_{2g+1,q^n}} \sum_{C \in \mathcal{H}_{2g+1,q^n}} f\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) = \int_{\mathrm{USp}(2g)} f(U)\, d\mu_{\mathrm{Haar}}(U),$$

where μ_{Haar} is the normalised Haar measure on $\mathrm{USp}(2g)$.

Equivalently, consider the sequence of probability measures

$$\mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}} = \frac{1}{\#\mathcal{H}_{2g+1,q^n}} \sum_{C \in \mathcal{H}_{2g+1,q^n}} \delta_{\vartheta\left(C/\mathbb{F}_{q^n}\right)}$$

on $\mathrm{USp}(2g)$, where $\delta_{U^\#}$ is a point mass at a conjugacy class $U^\# \in \mathrm{USp}(2g)^\#$. Then Deligne's equidistribution theorem merely states that the sequence of probability measures $\mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}$ converges weakly to the probability measure

$$\mathrm{Prob}_{\mathrm{USp}(2g)} = \mu_{\mathrm{Haar}}$$

as n tends to infinity. By applying the Portmanteau theorem to the sequence of probability measures $\mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}$, we obtain an equivalent reformulation of Deligne's equidistribution theorem.

Corollary 2.5. *For fixed $g \geq 1$,*

$$\lim_{n \to \infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}\left(\vartheta\left(C/\mathbb{F}_{q^n}\right) \in A\right) = \mathrm{Prob}_{\mathrm{USp}(2g)}\left(U \in A\right)$$

for any Borel set $A \subset \mathrm{USp}(2g)$ whose boundary has Haar measure zero.

Remark 2.6. In fact, Deligne's equidistribution theorem holds not only for fixed q in the limit as n tends to infinity, but rather for *any* sequence of prime powers q tending to infinity, with $\mathcal{H}_{2g+1,q}$ in place of $\mathcal{H}_{2g+1,q^n}$. However, Theorem 2.3 requires the restriction that q be fixed, which is why we have this condition in Theorem 1.4. It would be of interest to determine whether this restriction could be removed, so that Theorem 1.4 would hold for any sequence of prime powers q tending to infinity.

One can calculate the Haar measure for $\mathrm{USp}(2g)$ precisely by using the following formula to convert it into an integral over $[0,\pi]^g$.

Proposition 2.7 (Weyl Integration Formula [9, §5.0.4])**.** *Let f be a bounded, Borel-measurable complex-valued central function on* $\mathrm{USp}(2g)$*. Then*

$$\int_{\mathrm{USp}(2g)} f(U)\, d\mu_{\mathrm{Haar}}(U) = \int_0^{\pi} \cdots \int_0^{\pi} f\left(\theta_1, \ldots, \theta_g\right)\, d\mu_{\mathrm{USp}}\left(\theta_1, \ldots, \theta_g\right),$$

where

$$d\mu_{\mathrm{USp}}\left(\theta_1, \ldots, \theta_g\right) = \frac{2^{g^2}}{g!\pi^g} \prod_{1 \le j < k \le g} \left(\cos\theta_k - \cos\theta_j\right)^2 \prod_{\ell=1}^{g} \sin^2\theta_\ell \, d\theta_1 \cdots d\theta_g. \tag{8}$$

To make use of Corollary 2.5, we need to ensure that the boundaries of the sets with which we work have Haar measure zero.

Lemma 2.8. *Let A be an interval in $\mathbb{R}$. Then the boundary of the set*

$$\{U \in \mathrm{USp}(2g) : \varphi(U) \in A\}$$

has Haar measure zero.

Proof. By differentiating (6), we have that

$$\varphi(U) = \varphi\left(\theta_1, \ldots, \theta_g\right) = \frac{1}{2^{g-1}} \sum_{j=1}^{g} \operatorname{cosec}\theta_j \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{\left|\cos\theta_k - \cos\theta_j\right|}. \tag{9}$$

So by the Weyl integration formula, we must show that for any interval A, the boundary of the set

$$\{(\theta_1, \ldots, \theta_g) \in [0,\pi]^g : \varphi\left(\theta_1, \ldots, \theta_g\right) \in A\}$$

has μ_{USp}-measure zero. Observe that μ_{USp} is absolutely continuous with respect to the Lebesgue measure on $[0,\pi]^g$, and hence the sets

$$\{(\theta_1, \ldots, \theta_g) \in [0,\pi]^g : \theta_j = \theta_k \text{ for some } 1 \le j < k \le g\}$$

and

$$\{(\theta_1, \ldots, \theta_g) \in [0,\pi]^g : \theta_j \in \{0,\pi\} \text{ for some } 1 \le j \le g\}$$

have μ_{USp}-measure zero; furthermore, for each permutation σ of $\{1, \ldots, g\}$, the function φ is continuous on the set

$$\left\{(\theta_1, \ldots, \theta_g) \in [0,\pi]^g : 0 < \theta_{\sigma(1)} < \ldots < \theta_{\sigma(g)} < \pi\right\}.$$

It therefore suffices to show that for each $a \in \mathbb{R}$ and for each $\sigma \in S_g$, the set

$$\left\{(\theta_1, \ldots, \theta_g) \in [0,\pi]^g : \varphi\left(\theta_1, \ldots, \theta_g\right) = a,\ 0 < \theta_{\sigma(1)} < \ldots < \theta_{\sigma(g)} < \pi\right\}$$

has μ_{USp}-measure zero. But in the region where $0 < \theta_{\sigma(1)} < \ldots < \theta_{\sigma(g)} < \pi$, the expression (9) shows that the function $\varphi\left(\theta_1, \ldots, \theta_g\right)$ is not only continuous but real analytic and non-uniformly constant. As the zero set of a non-uniformly zero real analytic function has Lebesgue measure zero, and μ_{USp} is absolutely continuous with respect to the Lebesgue measure, we obtain the result. □

3. Proof of Theorem 1.4

We have now developed the necessary machinery needed in order to study the limit as n tends to infinity of the average

$$\mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}\left(C \text{ satisfies the } \beta\text{-Mertens conjecture}\right).$$

For brevity's sake, we write this average as

$$\mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}\left(B\left(C/\mathbb{F}_{q^n}\right) \leq \beta\right).$$

We also write $C \in \mathrm{LI}$ if C satisfies LI, and conversely if C does not satisfy LI, we write $C \notin \mathrm{LI}$.

Proposition 3.1. *For $\beta > 0$, we have that*

$$\lim_{n\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}\left(B\left(C/\mathbb{F}_{q^n}\right) \leq \beta\right) = \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\varphi(U) \leq \beta\right). \tag{10}$$

Note that (10) is equivalent to

$$\lim_{n\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}\left(B\left(C/\mathbb{F}_{q^n}\right) > \beta\right) = \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\varphi(U) > \beta\right). \tag{11}$$

for $\beta > 0$. If we let

$$B^T\left(C/\mathbb{F}_q\right) = \min\left\{B\left(C/\mathbb{F}_q\right), T\right\}$$

for $T > 0$, then by integrating (11) with respect to β from 0 to T and taking the limit as T tends to infinity, we find via the dominated convergence theorem and Fubini's theorem that

$$\lim_{T\to\infty}\lim_{n\to\infty} \frac{1}{\#\mathcal{H}_{2g+1,q^n}} \sum_{C\in\mathcal{H}_{2g+1,q^n}} B^T\left(C/\mathbb{F}_{q^n}\right) = \int_{\mathrm{USp}(2g)} \varphi(U)\, d\mu_{\mathrm{Haar}}(U),$$

thereby obtaining a slightly modified version of a result of Cha [3, Theorem 3.3].

Proof. For any $\varepsilon > 0$ with $\varepsilon < \beta$, let

$$\begin{aligned}
A &= \left\{C \in \mathcal{H}_{2g+1,q^n} : B\left(C/\mathbb{F}_{q^n}\right) \leq \beta,\ \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \leq \beta,\ C \in \mathrm{LI}\right\},\\
A_1 &= \left\{C \in \mathcal{H}_{2g+1,q^n} : B\left(C/\mathbb{F}_{q^n}\right) \leq \beta\right\},\\
A_2 &= \left\{C \in \mathcal{H}_{2g+1,q^n} : B\left(C/\mathbb{F}_{q^n}\right) \leq \beta,\ C \notin \mathrm{LI}\right\},\\
A_3 &= \left\{C \in \mathcal{H}_{2g+1,q^n} : B\left(C/\mathbb{F}_{q^n}\right) \leq \beta,\ \beta < \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \leq \beta+\varepsilon,\ C \in \mathrm{LI}\right\},\\
A_4 &= \left\{C \in \mathcal{H}_{2g+1,q^n} : B\left(C/\mathbb{F}_{q^n}\right) \leq \beta,\ \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) > \beta+\varepsilon,\ C \in \mathrm{LI}\right\},\\
A_{1'} &= \left\{C \in \mathcal{H}_{2g+1,q^n} : \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \leq \beta\right\},\\
A_{2'} &= \left\{C \in \mathcal{H}_{2g+1,q^n} : \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \leq \beta,\ C \notin \mathrm{LI}\right\},\\
A_{3'} &= \left\{C \in \mathcal{H}_{2g+1,q^n} : B\left(C/\mathbb{F}_{q^n}\right) > \beta,\ \beta-\varepsilon \leq \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \leq \beta,\ C \in \mathrm{LI}\right\},\\
A_{4'} &= \left\{C \in \mathcal{H}_{2g+1,q^n} : B\left(C/\mathbb{F}_{q^n}\right) > \beta,\ \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) < \beta-\varepsilon,\ C \in \mathrm{LI}\right\}.
\end{aligned}$$

Then we have that

$$\begin{aligned}
A_1 &= A \sqcup A_2 \sqcup A_3 \sqcup A_4,\\
A_{1'} &= A \sqcup A_{2'} \sqcup A_{3'} \sqcup A_{4'},
\end{aligned}$$

where the unions are all disjoint, and consequently

$$\#A_1 = \#A_{1'} + \#A_2 - \#A_{2'} + \#A_3 - \#A_{3'} + \#A_4 - \#A_{4'}.$$

By Deligne's equidistribution theorem and Lemma 2.8,

$$\lim_{n\to\infty} \frac{\#A_{1'}}{\#\mathcal{H}_{2g+1,q^n}} = \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\varphi(U) \leq \beta\right),$$

while Theorem 2.3 implies that

$$\lim_{n\to\infty} \frac{\#A_2}{\#\mathcal{H}_{2g+1,q^n}} = \lim_{n\to\infty} \frac{\#A_{2'}}{\#\mathcal{H}_{2g+1,q^n}} = 0.$$

Next, we note that

$$A_3 \sqcup A_{3'} \subset \{C \in \mathcal{H}_{2g+1,q^n} : \beta - \varepsilon \leq \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \leq \beta + \varepsilon\},$$

and hence

$$\limsup_{n\to\infty} \frac{|\#A_3 - \#A_{3'}|}{\#\mathcal{H}_{2g+1,q^n}} \leq \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\beta - \varepsilon \leq \varphi(U) \leq \beta + \varepsilon\right).$$

by Deligne's equidistribution theorem and Lemma 2.8. Finally, Lemma 2.2 implies that

$$A_4 \subset \left\{C \in \mathcal{H}_{2g+1,q^n} : \beta + \varepsilon < \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \leq \frac{1}{1-q^{-n/2}}\beta,\ C \in \mathrm{LI}\right\},$$

which is empty for all $n \geq 2\log_q(\beta/\varepsilon + 1)$, and similarly that

$$A_{4'} \subset \left\{C \in \mathcal{H}_{2g+1,q^n} : \frac{1}{1+q^{-n/2}}\beta < \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) < \beta - \varepsilon,\ C \in \mathrm{LI}\right\},$$

which is empty for all $n \geq 2\log_q(\beta/\varepsilon - 1)$. So

$$\lim_{n\to\infty} \frac{\#A_4}{\#\mathcal{H}_{2g+1,q^n}} = \lim_{n\to\infty} \frac{\#A_{4'}}{\#\mathcal{H}_{2g+1,q^n}} = 0.$$

So we have shown that for any $\varepsilon > 0$ with $\varepsilon < \beta$,

$$\limsup_{n\to\infty} \left|\mathrm{Prob}_{\mathcal{H}_{2g+1,q^n}}\left(B\left(C/\mathbb{F}_{q^n}\right) \leq \beta\right) - \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\varphi(U) \leq \beta\right)\right| \leq \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\beta - \varepsilon \leq \varphi(U) \leq \beta + \varepsilon\right).$$

As $\varepsilon > 0$ was arbitrary, and

$$\lim_{\varepsilon\to 0} \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\beta - \varepsilon \leq \varphi(U) \leq \beta + \varepsilon\right) = \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\varphi(U) = \beta\right) = 0$$

by Lemma 2.8, we obtain the result. □

So in order to prove Theorem 1.4, we must show that for each fixed $g \geq 1$,

$$\mathrm{Prob}_{\mathrm{USp}(2g)}\left(\varphi(U) \leq \beta\right) = 0$$

for $0 < \beta \leq 1$, whereas for any $\beta > 1$,

$$0 < \mathrm{Prob}_{\mathrm{USp}(2g)}\left(\varphi(U) \leq \beta\right) < 1.$$

This follows from the following result, which we prove in Section 5 in a more general form.

Proposition 3.2. *Let $U \in \mathrm{USp}(2g)$ be a unitary symplectic matrix with eigenvalues $e^{i\theta_1}, \ldots, e^{i\theta_g}, e^{-i\theta_1}, \ldots, e^{i\theta_g}$, with $0 \leq \theta_j \leq \pi$ for $1 \leq j \leq g$. Then the global minimum of*

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

occurs precisely at the set of points

$$\left(\widetilde{\theta}_{\sigma(1)}, \ldots, \widetilde{\theta}_{\sigma(g)}\right),$$

where σ is a permutation on $\{1, \ldots, g\}$, and

$$\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) = \left(\frac{\pi}{2g}, \frac{3\pi}{2g}, \ldots, \frac{(2g-1)\pi}{2g}\right).$$

Furthermore,

$$\varphi\left(\widetilde{\theta}_{\sigma(1)}, \ldots, \widetilde{\theta}_{\sigma(g)}\right) = 1.$$

Proof of Theorem 1.4. As Proposition 3.2 implies that the set

$$\{(\theta_1,\dots,\theta_g)\in[0,\pi]^g : \varphi(\theta_1,\dots,\theta_g)\leq 1\}$$

is finite, we must have that

$$\mathrm{Prob}_{\mathrm{USp}(2g)}(\varphi(U)\leq\beta)=0$$

for all $0<\beta\leq 1$ via the Weyl integration formula and the fact that the measure μ_{USp} is atomless, with μ_{USp} as in (8). To prove that

$$0<\mathrm{Prob}_{\mathrm{USp}(2g)}(\varphi(U)\leq\beta)<1$$

for $\beta>1$, we note that from Proposition 3.2, the equality $\varphi(\theta_1,\dots,\theta_g)=1$ is attained at the point

$$\left(\widetilde{\theta}_1,\dots,\widetilde{\theta}_g\right)=\left(\frac{\pi}{2g},\frac{3\pi}{2g},\dots,\frac{(2g-1)\pi}{2g}\right),$$

which lies in the region $0<\theta_1<\ldots<\theta_g<\pi$. As φ is real analytic and non-uniformly constant in this region, there must exist an open neighbourhood of $\left(\widetilde{\theta}_1,\dots,\widetilde{\theta}_g\right)$ in this region where $1\leq\varphi(\theta_1,\dots,\theta_g)\leq\beta$. This open neighbourhood must have positive μ_{USp}-measure, as $d\mu_{\mathrm{USp}}(\theta_1,\dots,\theta_g)$ does not vanish on open subsets of $[0,\pi]^g$. Consequently,

$$\mathrm{Prob}_{\mathrm{USp}(2g)}(\varphi(U)\leq\beta)>0.$$

On the other hand, we must also have that

$$\mathrm{Prob}_{\mathrm{USp}(2g)}(\varphi(U)\leq\beta)<1,$$

as φ blows up when $\theta_j=\theta_k$ for any $j\neq k$, and so for any such point there exists some open neighbourhood with $\varphi(\theta_1,\dots,\theta_g)>\beta$ within this neighbourhood. □

It is worth noting that for $\beta>1$, the quantity

$$\mathrm{Prob}_{\mathrm{USp}(2g)}(\varphi(U)\leq\beta)$$

is in fact strictly increasing as a function of β; this follows from the argument above together with the fact that there exists a point $(\theta_1,\dots,\theta_g)$ for which $\varphi(\theta_1,\dots,\theta_g)=\beta$, which follows from the mean value theorem.

4. Generalisations

The definition of the summatory function of the Möbius function of $C/\mathbb{F}_q$ studied in this article involves a sum over all effective divisors N of C with $0\leq\deg(N)\leq X-1$, following the same definition as used previously in the literature in [3] and [7] (though note that Cha in [3] defines this sum to be over all N with $0\leq\deg(N)\leq X$, and then normalises $B(C/\mathbb{F}_q)$ by a factor of $1/\sqrt{q}$ to compensate for this alteration). On the other hand, it is more common to define the summatory functions of arithmetic functions of function fields as only involving a sum over effective divisors N of a fixed degree, $\deg(N)=X$; for example, see [15, Chapter 17]. Here we shall observe that this distinction is moot: we will show that Theorem 1.4 remains valid after replacing the β-Mertens conjecture

$$\limsup_{X\to\infty}\frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{q^{X/2}}=\limsup_{X\to\infty}\frac{1}{q^{X/2}}\left|\sum_{0\leq\deg(N)\leq X-1}\mu_{C/\mathbb{F}_q}(N)\right|\leq\beta$$

by the "localised" β-Mertens conjecture

$$\limsup_{X\to\infty}\frac{1}{q^{X/2}}\left|\sum_{\deg(N)=X-1}\mu_{C/\mathbb{F}_q}(N)\right|\leq\beta.$$

That is, we need not average over all effective divisors of degree at most $X-1$, but merely study the growth of the Möbius function of the effective divisors of degree $X-1$. To prove this, we only require the following analogue of Lemma 2.2, for then the associated analogue of Proposition 3.1 holds with only trivial modifications to the proof.

Lemma 4.1 (cf. Lemma 2.2)**.** *Suppose that C satisfies* LI*. Then*

$$\limsup_{X\to\infty}\frac{1}{q^{X/2}}\left|\sum_{\deg(N)=X-1}\mu_{C/\mathbb{F}_q}(N)\right|\geq\left(1-\frac{1}{\sqrt{q}}\right)^2\varphi\left(\vartheta\left(C/\mathbb{F}_q\right)\right),$$

$$\limsup_{X\to\infty}\frac{1}{q^{X/2}}\left|\sum_{\deg(N)=X-1}\mu_{C/\mathbb{F}_q}(N)\right|\leq\left(1+\frac{1}{\sqrt{q}}\right)^2\varphi\left(\vartheta\left(C/\mathbb{F}_q\right)\right),$$

Proof. From the method of proof of [3, Proposition 2.2], if $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes, then as X tends to infinity,

$$\sum_{\deg(N)=X-1}\mu_{C/\mathbb{F}_q}(N)=-2\Re\left(\sum_{j=1}^{g}\frac{\gamma_j^X}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)}\right)+O(1),$$

and so if C satisfies LI, the Kronecker–Weyl theorem and the fact that $\gamma_j^X=q^{X/2}e^{iX\theta(\gamma_j)}$ imply that

$$\limsup_{X\to\infty}\frac{1}{q^{X/2}}\left|\sum_{\deg(N)=X-1}\mu_{C/\mathbb{F}_q}(N)\right|=2\sum_{j=1}^{g}\frac{1}{\left|Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)\right|}.$$

By (4), (7), and the fact that $\gamma_j=\sqrt{q}e^{i\theta(\gamma_j)}$, we have that

$$\frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)}=i\frac{q+1-2\sqrt{q}\cos\theta\left(\gamma_j\right)}{qe^{2i\theta(\gamma_j)}}\frac{1}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'\left(\theta\left(\gamma_j\right)\right)}.$$

As

$$\left(\sqrt{q}-1\right)^2\leq\left|q+1-2\sqrt{q}\cos\theta\left(\gamma_j\right)\right|\leq\left(\sqrt{q}+1\right)^2,$$

we can take absolute values and then sum from $j=1$ to $j=g$, yielding the result. □

We also note that we can prove a weaker form of Theorem 1.4 for families of curves other than hyperelliptic curves. Indeed, let $\mathcal{F}=\{\mathcal{F}_q\}$ be a family of curves indexed by a set of prime powers q tending to infinity, such that each $\mathcal{F}_q$ consists of a finite set of nonsingular projective curves over $\mathbb{F}_q$; note that we do not require that the sequence q consist only of powers of a single fixed prime, and also that there is no restriction whatsoever on the genus of a curve in each $\mathcal{F}_q$. For a property D of a curve $C\in\mathcal{F}_q$, we define the probability

$$\mathrm{Prob}_{\mathcal{F}_q}\left(C\text{ satisfies }D\right)=\frac{\#\left\{C\in\mathcal{F}_q:C\text{ satisfies }D\right\}}{\#\mathcal{F}_q}.$$

Theorem 4.2. *Suppose that*

$$\lim_{q\to\infty}\mathrm{Prob}_{\mathcal{F}_q}\left(C\text{ satisfies LI}\right)=1.$$

Then

$$\lim_{q\to\infty}\mathrm{Prob}_{\mathcal{F}_q}\left(B(C/\mathbb{F}_q)<1\right)=0. \tag{12}$$

Furthermore, there exists a family $\mathcal{F}$ for which C satisfies LI *for all $C \in \mathcal{F}$, but with*

$$\lim_{q\to\infty} \mathrm{Prob}_{\mathcal{F}_q}\left(B(C/\mathbb{F}_q) = 1\right) = 1, \tag{13}$$

and similarly for every fixed $b > a > 1$ there exists a family $\mathcal{F}$ for which C satisfies LI *for all $C \in \mathcal{F}$, but with*

$$\lim_{q\to\infty} \mathrm{Prob}_{\mathcal{F}_q}\left(a < B(C/\mathbb{F}_q) < b\right) = 1. \tag{14}$$

Proof. For (12), we copy the proof of Proposition 3.1 with $\mathcal{F}_q$ replacing $\mathcal{H}_{2g+1,q^n}$, taking the limit as q tends to infinity as opposed to n tending to infinity, and choosing $\beta = 1-\delta$ for fixed $0 < \delta < 1$, so that $0 < \varepsilon < 1-\delta$. We treat the sets $A_2, A_{2'}, A_4, A_{4'}$ using the same method as in Proposition 3.1, obtaining

$$\lim_{q\to\infty} \frac{\#A_2}{\#\mathcal{F}_q} = \lim_{q\to\infty} \frac{\#A_{2'}}{\#\mathcal{F}_q} = \lim_{q\to\infty} \frac{\#A_4}{\#\mathcal{F}_q} = \lim_{q\to\infty} \frac{\#A_{4'}}{\#\mathcal{F}_q} = 0.$$

For A_3 and A_3', we have that

$$A_3 \sqcup A_{3'} \subset \left\{C \in \mathcal{F}_q : 1-\delta-\varepsilon \le \varphi\left(\vartheta\left(C/\mathbb{F}_q\right)\right) \le 1-\delta+\varepsilon\right\},$$

and as $1-\delta+\varepsilon < 1$, Proposition 3.2 implies that this set is empty, so that

$$\lim_{q\to\infty} \frac{\#A_3}{\#\mathcal{F}_q} = \lim_{q\to\infty} \frac{\#A_{3'}}{\#\mathcal{F}_q} = 0.$$

Finally, for $A_{1'}$ we write

$$A_{1'} = A_{2'} \sqcup A_{5'}$$

with

$$A_{5'} = \left\{C \in \mathcal{F}_q : \varphi\left(\vartheta\left(C/\mathbb{F}_q\right)\right) \le 1-\delta,\ C \in \mathrm{LI}\right\}.$$

Again,

$$\lim_{q\to\infty} \frac{\#A_{2'}}{\#\mathcal{F}_q} = 0,$$

and Proposition 3.2 shows that $A_{5'}$ is empty, so that

$$\lim_{q\to\infty} \frac{\#A_{5'}}{\#\mathcal{F}_q} = 0$$

as well. Thus

$$\mathrm{Prob}_{\mathcal{F}_q}\left(B(C/\mathbb{F}_q) \le 1-\delta\right) = \lim_{q\to\infty} \frac{\#A_1}{\#\mathcal{F}_q} = 0,$$

and as $\delta > 0$ was arbitrary, we obtain (12).

For (13), we take q to be any odd prime power and $\mathcal{F}_q$ to consist solely of the elliptic curve E over $\mathbb{F}_q$ whose trace of the Frobenius is equal to 2; by the proof of [18, Theorem 4.1], such an E exists and satisfies LI, and by Theorem 1.5, $B(E/\mathbb{F}_q) = 1$.

Finally, for (14), we take $q = p^m$ for some prime p and we take $\mathcal{F}_q$ to consist of the set of elliptic curves E over $\mathbb{F}_q$ whose trace a_E of the Frobenius is an integer satisfying $a_E \not\equiv 0 \pmod{p}$, $|a_E| < 2\sqrt{q}$, and

$$\frac{2}{b^2}\left(1 - \sqrt{(qb^2-1)(b^2-1)}\right) < a_E < \frac{2}{a^2}\left(1 - \sqrt{(qa^2-1)(a^2-1)}\right).$$

Note that for all sufficiently large q there exists such an integer a_E for which this inequality holds, and hence by the proof of [18, Theorem 4.1] there exists an elliptic curve E over $\mathbb{F}_q$ satisfying LI with trace of the Frobenius equal to a_E. It follows that

$$a < 2\sqrt{\frac{q+1-a_E}{4q-a_E^2}} < b$$

and as it is shown in [7, §3] that

$$B(E/\mathbb{F}_q) = 2\sqrt{\frac{q+1-a_E}{4q-a_E^2}},$$

the result follows. □

5. The Minimum of $\varphi(U)$

Let $\mathrm{U}(N)$ denote the space of $N \times N$ unitary matrices, so that a matrix $U \in \mathrm{U}(N)$ has eigenvalues $e^{i\theta_1}, \dots, e^{i\theta_N}$ with $-\pi \leq \theta_j \leq \pi$ for all $1 \leq j \leq N$. For real θ, the characteristic polynomial $Z_U(\theta)$ of U is defined to be

$$\mathcal{Z}_U(\theta) = \det\left(I - Ue^{-i\theta}\right) = \prod_{j=1}^{N}\left(1 - e^{i(\theta_j - \theta)}\right).$$

Let

$$\varphi(U) = \sum_{j=1}^{N} \frac{1}{\left|\mathcal{Z}_U{}'(\theta_j)\right|}, \tag{15}$$

so that

$$\begin{aligned}\varphi(U) = \varphi(\theta_1, \dots, \theta_N) &= \sum_{j=1}^{N}\prod_{\substack{k=1\\k\neq j}}^{N}\frac{1}{\left|1 - e^{i(\theta_k - \theta_j)}\right|} \\ &= \frac{1}{2^{N-1}}\sum_{j=1}^{N}\prod_{\substack{k=1\\k\neq j}}^{N}\left|\operatorname{cosec}\left(\frac{\theta_k - \theta_j}{2}\right)\right|.\end{aligned} \tag{16}$$

We prove the following generalisation of Proposition 3.2.

Proposition 5.1. *Let $U \in \mathrm{U}(N)$ be a unitary matrix with eigenvalues $e^{i\theta_1}, \dots, e^{i\theta_N}$, and let $\varphi(U) = \varphi(\theta_1, \dots, \theta_N)$ be as in (15). Then the global minimum of φ occurs precisely at the set of points*

$$\left(\widetilde{\theta}_{\sigma(1)} + \phi, \dots, \widetilde{\theta}_{\sigma(N)} + \phi\right),$$

where $\sigma \in S_N$, ϕ is a one-dimensional translation modulo 2π, and

$$\left(\widetilde{\theta}_1, \dots, \widetilde{\theta}_N\right) = \left(-\frac{(N-1)\pi}{N}, -\frac{(N-3)\pi}{N}, \dots, \frac{(N-1)\pi}{N}\right).$$

Furthermore,

$$\varphi\left(\widetilde{\theta}_{\sigma(1)} + \phi, \dots, \widetilde{\theta}_{\sigma(N)} + \phi\right) = 1. \tag{17}$$

From this, we obtain the result for the subgroup of unitary symplectic matrices, namely Proposition 3.2, by setting $N = 2g$ and restricting our values of $(\theta_1, \dots, \theta_{2g})$ to be such that $\theta_{j+g} = -\theta_j$ with $0 \leq \theta_j \leq \pi$ for each $1 \leq j \leq g$; note that this restriction means that we lose the one-dimensional translation invariance modulo 2π of the variables of φ.

One can interpret Proposition 5.1 via a geometric argument. If $z_1, \dots, z_N$ are N points on the unit circle in the complex plane, then we may consider the product of the chord lengths of chords from a single point z_j to the other $N-1$ points. We can then think of φ as the sum of the inverses of these products indexed by the starting points z_j. Intuitively, we would expect the product of chord lengths to be largest when averaged over the starting points when the N-tuple of points on the unit circle are evenly spaced; consequently, we would expect φ to be smallest at this same N-tuple.

Proof of Proposition 5.1. We first prove that (17) holds. It suffices to prove this when σ is the identity and $\phi = 0$, as φ is invariant under permutations and one-dimensional translations of the variables. From (16), we have that

$$\varphi\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_N\right) = \sum_{j=1}^{N} \prod_{\substack{k=1 \\ k \neq j}}^{N} \frac{1}{\left|1 - e^{2\pi i(k-j)/N}\right|},$$

as $\theta_j = (2j - 1 - N)\pi/N$. We obtain (17) by noting that for any $1 \leq j \leq N$,

$$\prod_{\substack{k=1 \\ k \neq j}}^{N} \frac{1}{\left|1 - e^{2\pi i(k-j)/N}\right|} = \prod_{k=1}^{N-1} \frac{1}{\left|1 - e^{2\pi ik/N}\right|} = \frac{1}{N},$$

where the last step follows by taking $x = 1$ in the identity

$$\sum_{j=0}^{N-1} x^j = \prod_{k=1}^{N-1} \left(x - e^{2\pi ik/N}\right).$$

To prove that $\varphi(\theta_1, \ldots, \theta_N) \geq 1$ for all $(\theta_1, \ldots, \theta_N) \in [-\pi, \pi]^N$, we first note that we may assume without loss of generality that $-\pi < \theta_1 < \ldots < \theta_N < \pi$ and that $\theta_1 = -(N-1)\pi/N$, as φ is invariant under permutations and one-dimensional translations modulo 2π of the variables. By applying the arithmetic mean–geometric mean inequality to (16), we have that

$$\varphi(\theta_1, \ldots, \theta_N) \geq \frac{N}{2^{N-1}} \prod_{\substack{j,k=1 \\ j \neq k}}^{N} \left|\operatorname{cosec}\left(\frac{\theta_k - \theta_j}{2}\right)\right|^{1/N} = \frac{N}{2^{N-1}} \prod_{j=1}^{N-1} \prod_{k=1}^{N} \left(\operatorname{cosec} \omega_{jk}\right)^{1/N},$$

where $\omega_{jk} = \omega_{jk}(\theta_1, \ldots, \theta_N) \in (0, \pi)$ is given by

$$\omega_{jk} = \begin{cases} \dfrac{\theta_{j+k} - \theta_k}{2} & \text{if } j + k \leq N, \\ \pi - \dfrac{\theta_k - \theta_{j+k-N}}{2} & \text{if } j + k > N, \end{cases}$$

and we have used the fact that $|\operatorname{cosec}\theta| = \operatorname{cosec}|\theta|$ and that $\operatorname{cosec}(\pi - \theta) = \operatorname{cosec}\theta$ for $-\pi < \theta < \pi$, $\theta \neq 0$. As

$$\prod_{k=1}^{N} \left(\operatorname{cosec} \omega_{jk}\right)^{1/N} = \exp\left(\frac{1}{N} \sum_{k=1}^{N} \log \operatorname{cosec} \omega_{jk}\right),$$

and as the function $f(\theta) = \log \operatorname{cosec}\theta$ is convex on the interval $(0, \pi)$, Jensen's inequality implies that

$$\varphi(\theta_1, \ldots, \theta_N) \geq \frac{N}{2^{N-1}} \prod_{j=1}^{N-1} \operatorname{cosec}\left(\frac{1}{N} \sum_{k=1}^{N} \omega_{jk}\right).$$

Now

$$\sum_{k=1}^{N} \omega_{jk} = j\pi, \tag{18}$$

as this is a telescoping sum, and consequently

$$\varphi(\theta_1, \ldots, \theta_N) \geq \frac{N}{2^{N-1}} \prod_{j=1}^{N-1} \operatorname{cosec}\left(\frac{j\pi}{N}\right) = N \prod_{j=1}^{N-1} \frac{1}{\left|1 - e^{2\pi ij/N}\right|} = 1.$$

Finally, the function $f(\theta) = \log \operatorname{cosec} \theta$ is strictly convex on $(0, \pi)$, so equality from the use of Jensen's inequality can only occur if for each fixed $1 \leq j \leq N$,

$$\omega_{jk} = \omega_{jk'}$$

for all $1 \leq k, k' \leq N$, which, together with (18), implies that

$$\omega_{jk} = \frac{j\pi}{N}$$

for all $1 \leq j, k \leq N$. As we assumed that $\theta_1 = -(N-1)\pi/N$, it follows that equality can only hold when

$$(\theta_1, \dots, \theta_N) = \left(\widetilde{\theta}_1, \dots, \widetilde{\theta}_N\right) = \left(-\frac{(N-1)\pi}{N}, -\frac{(N-3)\pi}{N}, \dots, \frac{(N-1)\pi}{N}\right). \quad \square$$

It is worth noting that this method also works for the more general function

$$\sum_{j=1}^{N} \left|\mathcal{Z}_U{}'(\theta_j)\right|^{2k}$$

where $k < 0$, which was studied by Hughes, Keating, and O'Connell [6] for its relation to discrete moments of the derivative of the Riemann zeta function. They calculated the asymptotics for large N of the integral

$$\int_{\mathrm{U}(N)} \sum_{j=1}^{N} \left|\mathcal{Z}_U{}'(\theta_j)\right|^{2k} d\mu_{\mathrm{Haar}}(U),$$

where μ_{Haar} is the Haar measure on $\mathrm{U}(N)$, and used this to conjecture the growth in the variable T of the sum

$$J_k(T) = \sum_{0<\gamma\leq T} \left|\zeta'(1/2 + i\gamma)\right|^{2k},$$

where we are assuming the Riemann hypothesis and the simplicity of the zeroes of $\zeta(s)$. The method of proof of Proposition 5.1 shows that for $k < 0$, the global minimum of

$$\sum_{j=1}^{N} \left|\mathcal{Z}_U{}'(\theta_j)\right|^{2k}$$

is 2^{2k+1}, and occurs at the points $\left(\widetilde{\theta}_{\sigma(1)} + \phi, \dots, \widetilde{\theta}_{\sigma(N)} + \phi\right)$.

Acknowledgements. The author would like to thank Jim Borger for his helpful advice and support, Byungchul Cha for his useful discussions on his work, and the anonymous referee for their many suggestions and corrections. Most of all, the author is indebted to Ruixiang Zhang for his sketch of a simple proof of Proposition 5.1.

References

[1] P. T. Bateman, J. W. Brown, R. S. Hall, K. E. Kloss, and Rosemarie M. Stemmler, "Linear Relations Connecting the Imaginary Parts of the Zeros of the Zeta Function", in *Computers in Number Theory*, editors A. O. L. Atkin and B. J. Birch, Academic Press, London, 1971, 11–19.

[2] D. G. Best and T. S. Trudgian, "Linear Relations of Zeroes of the Zeta-Function", preprint, arXiv:math.NT/1209.3843 (18 September 2012), 12 pages.

[3] Byungchul Cha, "The Summatory Function of the Möbius Function in Function Fields", submitted for publication, arXiv:math.NT/1008.4711v2 (14 November 2011), 16 pages.

[4] Nick Chavdarov, "The Generic Irreducibility of the Numerator of the Zeta Function in a Family of Curves with Large Monodromy", *Duke Mathematical Journal* **87** (1997), 151–180.

[5] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, "Jacobians in Isogeny Classes of Abelian Surfaces over Finite Fields", *Annales de l'Institut Fourier* **59** (2009), 239–289.

[6] C. P. Hughes, J. P. Keating, and Neil O'Connell, "Random Matrix Theory and the Derivative of the Riemann Zeta-Function", *Proceedings of the Royal Society of London Serial A* **456** (2000), 2611–2627.

[7] Peter Humphries, "On the Mertens Conjecture for Elliptic Curves over Finite Fields", to appear in *Bulletin of the Australian Mathematical Society*, dx.doi.org/10.1017/S0004972712001116 (28 February 2013), 15 pages.

[8] A. E. Ingham, "On Two Conjectures in the Theory of Numbers", *American Journal of Mathematics* **64** (1942), 313–319.

[9] Nicholas M. Katz and Peter Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, 1999.

[10] Tadej Kotnik and Herman te Riele, "The Mertens Conjecture Revisited", in *Algorithmic Number Theory; 7th International Symposium, ANTS-VII; Berlin, Germany, July 2006; Proceedings*, editors Florian Hess, Sebastian Pauli, and Michael Pohst, Lecture Notes in Computer Science **4076**, Springer, Berlin, 2006, 156–167.

[11] Emmanuel Kowalski, "The Large Sieve, Monodromy, and Zeta Functions of Algebraic Curves, 2: Independence of the Zeros", *International Mathematics Research Notices* (2008), Article ID rnn091, 57 pages.

[12] F. Mertens, "Über eine zahlentheoretische Funktion", *Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Mathematisch-Naturwissenschaftliche Klasse, Abteilung 2a* **106** (1897), 761–830.

[13] Nathan Ng, "The Distribution of the Summatory Function of the Möbius Function", *Proceedings of the London Mathematical Society* **89** (2004), 361–389.

[14] A. M. Odlyzko and H. J. J. te Riele, "Disproof of the Mertens Conjecture", *Journal für die Reine und Angewandte Mathematik* **357** (1985), 138–160.

[15] Michael Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics **210**, Springer, New York, 2002.

[16] R. D. von Sterneck, "Neue empirische Daten über die zahlentheoretischen Funktion $\sigma(n)$", in *Proceedings of the Fifth International Congress of Mathematics, Cambridge, 22–28 August 1912, Volume 1*, editors E. W. Hobson and A. E. H. Love, Cambridge, 1913, 341–343.

[17] T. J. Stieltjes, Lettre à Hermite de 11 juillet 1885, Lettre #79, in *Correspondance d'Hermite et de Stieltjes, Tome 1*, editors B. Baillaud and H. Bourget, Paris, Gauthier–Villars, 1905, 160–164.

[18] William C. Waterhouse, "Abelian Varieties over Finite Fields", *Annales Scientifiques de l'École Normale Supérieure, Série 4* **2** (1969), 521–560.

[19] André Weil, "Sur les Fonctions Algébriques à Corps de Constantes Fini", *Comptes Rendus de l'Académie des Sciences de Paris, Serie I. Mathematique* **210** (1940), 592–594.

E-mail address: peterch@math.princeton.edu

Department of Mathematics, Princeton University, Princeton, New Jersey 08544, USA