The Mertens and Pólya Conjectures in Function Fields

Peter Humphries

August 2012

A thesis submitted for the degree of Master of Philosophy
of The Australian National University

Declaration

The work in this thesis is my own except where otherwise stated.

Peter Humphries

Acknowledgements

Many thanks go to my supervisor, Jim Borger, whose willingness to take me on board was a godsend. I must also thank Andrew Hassell for his guidance and patience with me. I'd also like to thank Richard Brent for first introducing me to the problems in this thesis, and Tim Trudgian and Byungchul Cha for conversations and advice on my work.

Finally, I wish to thank my friends and family for all their support over the last eighteen months. I'm going to miss each and every one of you.

Abstract

The Mertens conjecture on the order of growth of the summatory function of the Möbius function has long been known to be false. We formulate an analogue of this conjecture in the setting of global function fields, and investigate the plausibility of this conjecture. First we give certain conditions, in terms of the zeroes of the associated zeta functions, for this conjecture to be true. We then show that in a certain family of function fields of low genus, the average proportion of curves satisfying the Mertens conjecture is zero, and we hypothesise that this is true for any genus. Finally, we also formulate a function field version of Pólya's conjecture, and prove similar results.

Contents

Acknowledgements **v**

Abstract **vii**

1 The Mertens Conjecture in Function Fields **1**

1.1 The Mertens Conjecture 1

1.2 Mertens Conjectures in Function Fields 3

2 Local Mertens Conjectures **9**

2.1 An Explicit Expression for $M_{C/\mathbb{F}_q}(X)$ 9

2.2 $M_{C/\mathbb{F}_q}(X)$ and Zeroes of Multiple Order 16

2.3 The Limiting Distribution of $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ 20

3 Examples in Low Genus **27**

3.1 Elliptic Curves over Finite Fields 27

3.2 Proof of Theorem 1.7 31

4 Global Mertens Conjectures **37**

4.1 Averages over Families of Curves 37

4.2 The Critical Point 47

4.3 Variants of the Mertens Conjecture 53

5 Pólya's Conjecture in Function Fields **57**

5.1 Pólya's Conjecture 57

5.2 Pólya Conjectures in Function Fields 59

6 Local Pólya Conjectures **63**

6.1 An Explicit Expression for $L_{C/\mathbb{F}_q}(X)$ 63

6.2 Examples in Low Genus 70

6.3 The Limiting Distribution of $L_{C/\mathbb{F}_q}(X)/q^{X/2}$ 74

7 Global Pólya Conjectures **79**
7.1 Averages over Families of Curves 79
7.2 Variants of Pólya's Conjecture 85

A Proof of the Kronecker–Weyl Theorem **89**

Bibliography **95**

Chapter 1

The Mertens Conjecture in Function Fields

1.1 The Mertens Conjecture

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

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

The Mertens conjecture states that the summatory function of the Möbius function,

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

satisfies the inequality

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

for all $x \geq 1$. This conjecture stems from the work of Mertens [17], who in 1897 calculated $M(x)$ from $x = 1$ up to $x = 10\,000$ and arrived at the conjecture (1.1). Notably, this conjecture implies that all of the nontrivial zeroes of the Riemann zeta function $\zeta(s)$ lie on the line $\Re(s) = 1/2$ (that is, that the Riemann hypothesis is true), and also that all such zeroes are simple. However, Ingham [12] later showed that the Mertens conjecture implies that the imaginary parts of the zeroes of $\zeta(s)$ in the upper half-plane must be linearly dependent over the rational numbers, a relation that seems unlikely; while there is yet to be found strong theoretical evidence for the falsity of such a linear dependence, some limited numerical calculations have failed to find any such linear relations [1]. Using methods closely related to the work of Ingham, Odlyzko and te Riele [22] disproved the Mertens conjecture, and in fact 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 [15].

Despite this disproof, a single counterexample to the Mertens conjecture has yet to be found. Indeed, numerical calculations of Amir Akbary and Nathan Ng (personal communication), based on the paper [21] of Ng, suggest that the set of counterexamples to the Mertens conjecture is sparsely distributed in $[1, \infty)$. More precisely, under the assumption of several strong yet plausible conjectures, they have shown that the logarithmic density

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

of the set $\mathcal{P}_\mu = \{x \in [1,\infty) : |M(x)| \leq \sqrt{x}\}$ is extremely close to 1 but strictly less than 1, satisfying the bounds

$$0.99999927 < \delta\left(\mathcal{P}_\mu\right) < 1. \tag{1.2}$$

So although the Mertens conjecture is false, the inequality $|M(x)| \leq \sqrt{x}$ nevertheless seems to hold for "most" $x \geq 1$; on the other hand, the set of x for which this inequality fails to hold is nevertheless nontrivial, in the sense that it has strictly positive, albeit extremely small, logarithmic density. The reason for this stems from the following explicit expression for $M(x)$ in terms of a sum over the nontrivial zeroes ρ of the Riemann zeta function.

Proposition 1.1 (Ng [21]). *Assume the Riemann hypothesis and the simplicity of the zeroes of $\zeta(s)$. Then there exists a sequence $\{T_v\}_{v=1}^{\infty}$ with $v \leq T_v \leq v+1$ such that for each positive integer v, for all $\varepsilon > 0$, and for x a positive noninteger,*

$$M(x) = \sum_{|\gamma|<T_v} \frac{1}{\zeta'(\rho)} \frac{x^\rho}{\rho} + O_\varepsilon\left(1 + \frac{x\log x}{T_v} + \frac{x}{T_v^{1-\varepsilon}\log x}\right),$$

where the sum is over the positive nontrivial zeroes $\rho = 1/2 + i\gamma$ of $\zeta(s)$ with $|\gamma| < T_v$.

So we see that for x a noninteger,

$$\frac{M(x)}{\sqrt{x}} = \sum_{\rho} \frac{1}{\zeta'(\rho)} \frac{x^{i\gamma}}{\rho} + O\left(\frac{1}{\sqrt{x}}\right), \tag{1.3}$$

where the sum $\sum_{\rho}$ is interpreted in the sense $\lim_{v\to\infty} \sum_{|\gamma|<T_v}$. Now the coefficients of $x^{i\gamma} = e^{i\gamma \log x}$ are generally quite small (in particular, much smaller than 1), so this sum is usually quite small. On the other hand, the coefficients are not insignificant, as the sum

$$\sum_{\rho} \frac{1}{|\rho\zeta'(\rho)|}$$

diverges, which suggests that if the collection of angles $\{\gamma \log x\}$ are equidistributed in $[0, 2\pi]$ as x tends to infinity, then we can find values of x for which the right-hand side of (1.3) is larger than 1. However, this does not occur for "most" x in the sense of logarithmic density, and hence the inequality $|M(x)| \leq \sqrt{x}$ holds "most" of the time.

1.2 Mertens Conjectures in Function Fields

A natural variant of this problem is to formulate a function field analogue of the Mertens conjecture and determine how often this conjecture holds. The advantage of this function field setting, as opposed to the classical case, is that we may prove unconditional results about the behaviour of the summatory function of the Möbius function function. In the function field setting, the Riemann hypothesis is proved, and the hypothesis that the imaginary parts of the zeroes of the zeta function of a function field are linearly independent over the rational numbers — that is to say, the Linear Independence hypothesis — is, at the very least, true in an averaged sense; see Theorem 4.4 for the precise formulation of this result. Throughout this thesis, the function fields we work with will be global function fields, that is, of transcendence degree one over a finite constant field; equivalently, these are the function field of a nonsingular projective curve over a finite field.

We define the Möbius function of a function field as follows. Let $q = p^m$ be an odd prime power, and let $\mathbb{F}_q$ be a finite field with q elements. Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus g; we write $C/\mathbb{F}_q$ for the function field of C over $\mathbb{F}_q$. Then for an effective divisor D of C, the Möbius function of

$C/\mathbb{F}_q$ is given by

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

We are interested in the summatory function of the Möbius function of $C/\mathbb{F}_q$:

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

where X is a positive integer. We wish to determine the validity of the following conjecture.

The Mertens Conjecture in Function Fields. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus g, and let $M_{C/\mathbb{F}_q}(X)$ be the summatory function of the Möbius function of $C/\mathbb{F}_q$. Then*

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

The presence of $q^{X/2}$ in the denominator, as opposed to $\sqrt{x}$ in the classical case, is due to the fact that we are summing over divisors D with $\deg(D) \leq X-1$, whose absolute norms $\mathcal{N}D$ are $q^{\deg(D)}$, as opposed to the classical case where we sum over all positive integers $n \leq x$, whose norm in each case is simply n itself.

Several natural questions arise from formulating this conjecture. We may first ask "local" questions: given a curve, how do we determine whether the Mertens conjecture for the function field of this curve holds?

Question 1.2. *For which curves does the Mertens conjecture hold?*

An further local problem is to consider the Mertens conjecture for each positive integer X.

Question 1.3. *Given a function field $C/\mathbb{F}_q$, how frequently does the inequality*

$$\left|M_{C/\mathbb{F}_q}(X)\right| \leq q^{X/2} \tag{1.4}$$

hold?

As there are many function fields of a given genus g over a finite field q, we may also consider a "global" question on the Mertens conjecture.

Question 1.4. *On average, in either the q or the g aspect, how often does the Mertens conjecture hold?*

We treat the local questions in Chapter 2. There we find that the major difference to the classical case is that Question 1.2 is non-trivial: there do exist curves for which the Mertens conjecture is true. In Section 2.1, we formulate certain conditions on the zeroes of $Z_{C/\mathbb{F}_q}(u)$, the zeta function of $C/\mathbb{F}_q$, to ensure that the Mertens conjecture for $C/\mathbb{F}_q$ is true, while in Section 2.2 we discuss when we can confirm that the Mertens conjecture for $C/\mathbb{F}_q$ is false. The results of these two sections combine to prove the following theorem.

Theorem 1.5. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$. Then the Mertens conjecture for $C/\mathbb{F}_q$ is false if the associated zeta function $Z_{C/\mathbb{F}_q}(u)$ has zeroes of multiple order. If $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes, then the Mertens conjecture for $C/\mathbb{F}_q$ is true provided*

$$\sum_{\gamma} \left| \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \right| \leq 1, \tag{1.5}$$

where the sum is over the inverse zeroes γ of $Z_{C/\mathbb{F}_q}(u)$. Furthermore, if C satisfies the Linear Independence hypothesis, then the converse is also true: the Mertens conjecture for $C/\mathbb{F}_q$ is true only when (1.5) *holds.*

We remark that this does not entirely answer Question 1.2; it is possible that $C/\mathbb{F}_q$ is such that (1.5) does not hold but that the Mertens conjecture for $C/\mathbb{F}_q$ is true; in order for this to happen, $Z_{C/\mathbb{F}_q}(u)$ must only has simple zeroes but C must fail to satisfy the Linear Independence hypothesis. In Section 3.2, we give an example of a family of curves of genus one for which this occurs.

Question 1.3 is the function field analogue of the problem of determining the logarithmic density of the set where the Mertens conjecture holds, as we discussed in Section 1.1. Section 2.3 deals with this question, where we are instead able to determine the natural density of the set of positive integers X for which (1.4) holds, under the proviso that the underlying curve satisfies the Linear Independence hypothesis; unlike the classical case, where this is conjectured to be true, this hypothesis can be violated for certain curves.

Theorem 1.6. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$, and suppose that C satisfies the Linear Independence hypothesis. The natural density*

$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = \lim_{Y \to \infty} \frac{1}{Y} \# \left\{1 \leq X \leq Y : \left|M_{C/\mathbb{F}_q}(X)\right| \leq q^{X/2}\right\}$$

exists and satisfies $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) > 0$, *with* $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = 1$ *if and only if*

$$\sum_{\gamma} \left| \frac{1}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \right| \leq 1.$$

We in fact describe this density $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right)$ in terms of the Lebesgue measure of the pullback of a certain function of $C/\mathbb{F}_q$, which allows us to determine this density exactly should we know the zeta function of the function field.

In Chapter 3 we analyse Questions 1.2 and 1.3 in the low genus case $g = 1$, so that $C/\mathbb{F}_q$ is the function field of an elliptic curve over a finite field. We give an explicit classification of all elliptic curves satisfying the Mertens conjecture in terms of the order q of the finite field q and of the trace a of the Frobenius endomorphism acting on the elliptic curve C, in the form of the following theorem.

Theorem 1.7. *Let* C *be an elliptic curve over a finite field* $\mathbb{F}_q$ *of characteristic* p. *Then the Mertens conjecture is true for* $C/\mathbb{F}_q$ *if and only if the order of the finite field* q *and the trace* a *of the Frobenius endomorphism acting on* C *over* $\mathbb{F}_q$ *satisfy precisely one of the following conditions:*

(1) $q = p^m$ *with* $a = 2$, *where either* m *is arbitrary and* $p \neq 2$, *or* $m = 1$ *and* $p = 2$,

(2) $q = p^m$ *with* $a = \sqrt{q}$, *where* m *is even and* $p \not\equiv 1 \pmod 3$,

(3) $q = p^m$ *with* $a = 0$, *where either* m *is even and* $p \not\equiv 1 \pmod 4$, *or* n *is odd.*

In all these cases, we have that

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

Furthermore, the natural density

$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = \lim_{Y \to \infty} \frac{1}{Y} \# \left\{1 \leq X \leq Y : \left|M_{C/\mathbb{F}_q}(X)\right| \leq q^{X/2}\right\}$$

exists, and this density is equal to 1 *if and only if* q *and* a *satisfy one of conditions (1)—(3).*

Finally, for Question 1.4, we study in Chapter 4 the average proportion of curves in a certain family satisfying the Mertens conjecture as the finite field $\mathbb{F}_q$ grows larger. This allows us to use Deligne's equidistribution theorem, a powerful result that links the average properties of curves to the Haar measure on certain groups of random matrices. We choose to average over a certain family of curves, namely a family of hyperelliptic curves $\mathcal{H}_{2g+1,q^n}$, for which most curves satisfy the Linear Independence hypothesis, where the notion of *most* curves satisfying a certain property is defined in Definition 4.3. Together with our resolution of Question 1.2, this allows us to relate the average proportion of hyperelliptic curves satisfying the Mertens conjecture to the Haar measure of the pullback of the region where a certain function of random matrices is at most 1. For low values of g, we may then calculate this Haar measure explicitly. Remarkably, we find that most curves in this family do not satisfy the Mertens conjecture.

Theorem 1.8. *Fix $1 \leq g \leq 2$, and suppose that the characteristic of $\mathbb{F}_q$ is odd. Then as n tends to infinity, most hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ do not satisfy the Mertens conjecture for $C/\mathbb{F}_{q^n}$.*

The proof involves checking that a certain function in g variables on $[0,\pi]^g$ is bounded below by 1: for large g, this becomes very difficult. Nevertheless, it seems likely that this inequality holds for all $g \geq 1$, as we indicate in Section 4.2, thereby leading us to formulate the following conjecture.

Conjecture 1.9. *Fix $g \geq 1$, and suppose that the characteristic of $\mathbb{F}_q$ is odd. Then as n tends to infinity, most hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ do not satisfy the Mertens conjecture for $C/\mathbb{F}_{q^n}$.*

We end Chapter 4 by discussing two variations of Question 1.4 and showing how minor modifications of the proof of Theorem 1.8 lead to proofs of these new questions.

These results build upon the work of Cha [5], who studies the closely related problem of determining the average size of

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

over $\mathcal{H}_{2g+1,q^n}$. Cha is able to show that a truncated form of this average converges to a certain integral over a particular space of random matrices, and by analysing this integral, Cha is led to conjecture the limiting behaviour of this average as the genus g tends to infinity. The purpose of this result is to formulate a function field analogue of a conjecture of Gonek (unpublished), which is studied by Ng in [21], stating that

$$0 < \limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}\,(\log\log\log x)^{5/4}} = -\liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}\,(\log\log\log x)^{5/4}} < \infty. \tag{1.6}$$

While Cha's results deviate in a different direction to the main results in this thesis, much of the groundwork is identical. We reproduce the proofs of many of these necessary results throughout this thesis, with attribution to Cha and identification of the location of the original proof in Cha's paper [5].

Chapter 2

Local Mertens Conjectures

2.1 An Explicit Expression for $M_{C/\mathbb{F}_q}(X)$

In order to study the summatory function of the Möbius function of a function field $C/\mathbb{F}_q$, we must first introduce the associated zeta function $\zeta_{C/\mathbb{F}_q}(s)$. Given a curve C over $\mathbb{F}_q$ of genus g, the zeta function $\zeta_{C/\mathbb{F}_q}(s)$ is defined initially for $\Re(s) > 1$ by the absolutely convergent Dirichlet series

$$\zeta_{C/\mathbb{F}_q}(s) = \sum_{D \geq 0} \frac{1}{\mathcal{N}D^s},$$

where the sum is over all effective divisors D of C, and $\mathcal{N}D = q^{\deg(D)}$ is the absolute norm of D. Note that q^{-s}, and hence $\zeta_{C/\mathbb{F}_q}(s)$, is periodic with period $2\pi i/\log q$. We also observe that much like the Riemann zeta function, $\zeta_{C/\mathbb{F}_q}(s)$ has an Euler product for $\Re(s) > 1$,

$$\zeta_{C/\mathbb{F}_q}(s) = \prod_{P} \frac{1}{1 - \mathcal{N}P^{-s}},$$

with the product over all prime divisors P of C. This in turn implies that $\zeta_{C/\mathbb{F}_q}(s)$ is nonvanishing in the open half-plane $\Re(s) > 1$. More than this is true, however; $\zeta_{C/\mathbb{F}_q}(s)$ extends meromorphically to the entire complex plane.

Theorem 2.1 ([24, Theorem 5.9])**.** *Given a nonsingular projective curve C over $\mathbb{F}_q$ of genus g, there exists a polynomial $P_{C/\mathbb{F}_q}(u)$ with integer coefficients of degree $2g$ such that for $\Re(s) > 1$,*

$$\zeta_{C/\mathbb{F}_q}(s) = \frac{P_{C/\mathbb{F}_q}(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}.$$

This yields a meromorphic extension of $\zeta_{C/\mathbb{F}_q}(s)$ to the whole complex plane, with simple poles at $s = 2\pi ik/\log q$ and $s = 1+2\pi ik/\log q$ for all $k \in \mathbb{Z}$. Furthermore, $\zeta_{C/\mathbb{F}_q}(s)$ satisfies the functional equation

$$q^{(g-1)s}\zeta_{C/\mathbb{F}_q}(s) = q^{(g-1)(1-s)}\zeta_{C/\mathbb{F}_q}(1-s).$$

The constant term of the polynomial $P_{C/\mathbb{F}_q}(u)$ is 1, and the coefficient of u^{2g} is q^g. Finally, the value $P_{C/\mathbb{F}_q}(1)$ is $h_{C/\mathbb{F}_q}$, the class number of $C/\mathbb{F}_q$.

The polynomial $P_{C/\mathbb{F}_q}(u)$ factorises over $\mathbb{C}$ as

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

for some complex numbers γ_j, which we call the inverse zeroes of $\zeta_{C/\mathbb{F}_q}(s)$. By the nonvanishing of $\zeta_{C/\mathbb{F}_q}(s)$ outside of $0 \leq \Re(s) \leq 1$ and the functional equation for $\zeta_{C/\mathbb{F}_q}(s)$, we must have that $1 \leq |\gamma_j| \leq q$. Moreover, the structure of the meromorphic continuation of $\zeta_{C/\mathbb{F}_q}(s)$ to the entire complex plane shows that $\overline{\zeta_{C/\mathbb{F}_q}(s)} = \zeta_{C/\mathbb{F}_q}(\overline{s})$. By this, we may conclude that the inverse zeroes γ_j must occur in reciprocal pairs; that is, we can order the inverse zeroes γ_j so that $\gamma_{j+g} = q\gamma_j^{-1}$ for all $1 \leq j \leq g$. Much more about the inverse zeroes is known; it has been proven that they all have absolute value $\sqrt{q}$.

Theorem 2.2 (Riemann Hypothesis for Function Fields [24, Theorem 5.10])**.** *Each inverse zero γ_j of $\zeta_{C/\mathbb{F}_q}(s)$ has absolute value $\sqrt{q}$. Equivalently, all of the zeroes of $\zeta_{C/\mathbb{F}_q}(s)$ lie along the line $\Re(s) = 1/2$.*

Consequently, we may write the inverse zeroes in the form $\gamma_j = \sqrt{q}e^{i\theta(\gamma_j)}$ with $0 \leq \theta(\gamma_j) \leq \pi$ and $\gamma_{j+g} = \overline{\gamma_j} = \sqrt{q}e^{-i\theta(\gamma_j)}$ for $1 \leq j \leq g$. Note in particular that the orders of the inverse zeroes $\gamma = \pm\sqrt{q}$ of $\zeta_{C/\mathbb{F}_q}(s)$ must be even.

Observe that $\zeta_{C/\mathbb{F}_q}(s)$ is in fact a function of q^{-s}. This allows us to define the zeta function $Z_{C/\mathbb{F}_q}(u)$ via the identification $u = q^{-s}$, so that

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

and hence $Z_{C/\mathbb{F}_q}(u)$ satisfies the functional equation

$$Z_{C/\mathbb{F}_q}(u) = q^{g-1}u^{2(g-1)}Z_{C/\mathbb{F}_q}\left(\frac{1}{qu}\right). \tag{2.2}$$

Returning to the summatory function of the Möbius function of a function field, we now approach the problem of obtaining an explicit description of this function by studying the Dirichlet series

$$\sum_{D\geq 0} \frac{\mu_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s}.$$

As $\mu_{C/\mathbb{F}_q}(D)$ is multiplicative and satisfies $\mu_{C/\mathbb{F}_q}(P) = -1$ and $\mu_{C/\mathbb{F}_q}(P^t) = 0$, $t \geq 2$, for a prime divisor P of C, this Dirichlet series has the Euler product expansion

$$\sum_{D\geq 0} \frac{\mu_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \prod_{P} \left(1 - \mathcal{N}P^{-s}\right)$$

for $\Re(s) > 1$, which upon comparing Euler products leads us to the identity

$$\sum_{D\geq 0} \frac{\mu_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \frac{1}{\zeta_{C/\mathbb{F}_q}(s)}, \tag{2.3}$$

which is valid for all $\Re(s) > 1$. On the other hand, note that for $\Re(s) > 1$, we may rearrange this Dirichlet series instead to be of the form

$$\sum_{D\geq 0} \frac{\mu_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \sum_{D\geq 0} \frac{\mu_{C/\mathbb{F}_q}(D)}{q^{\deg(D)s}} = \sum_{N=0}^{\infty} \frac{1}{q^{Ns}} \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D), \tag{2.4}$$

and so if we can determine an expression for the coefficients of the Dirichlet series for $1/\zeta_{C/\mathbb{F}_q}(s)$ using the known factorisation (2.1) of $\zeta_{C/\mathbb{F}_q}(s)$, then upon comparing coefficients, we will be able to construct an accurate formula for $M_{C/\mathbb{F}_q}(X) = \sum_{N=0}^{X-1} \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D)$.

This is particularly simple to do when $g = 0$, so that C is the projective line $\mathbb{P}^1$, and hence the function field $C/\mathbb{F}_q$ is simply $\mathbb{F}_q(t)$. In this case, we have that

$$\sum_{N=0}^{\infty} u^N \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D) = \frac{1}{Z_{C/\mathbb{F}_q}(u)} = (1-u)(1-qu),$$

and so by equating coefficients, we obtain the following result.

Proposition 2.3. *Let $g = 0$. Then*

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

In particular, the Mertens conjecture for $C/\mathbb{F}_q$ holds.

For $g \geq 1$, our method for determining an expression for these coefficients is via Cauchy's residue theorem. We will deal only with the case where all of the zeroes of $Z_{C/\mathbb{F}_q}(u)$ are simple, though it is nevertheless possible to determine an explicit expression for $M_{C/\mathbb{F}_q}(X)$ when $Z_{C/\mathbb{F}_q}(u)$ has zeroes of multiple order [5, Proposition 2.2].

Proposition 2.4 (Cha [5, Proposition 2.2, Corollary 2.3])**.** *Let $g \geq 1$, and suppose that the zeroes of $Z_{C/\mathbb{F}_q}(u)$ are all simple. Then as X tends to infinity,*

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = -\sum_{\gamma} \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} e^{iX\theta(\gamma)} + O_{q,g}\left(\frac{1}{q^{X/2}}\right). \tag{2.5}$$

In particular, the quantity

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

satisfies

$$B(C/\mathbb{F}_q) \leq \sum_{\gamma} \left| \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \right|. \tag{2.6}$$

It is useful to compare the explicit expression (2.5) to that for the classical case, (1.3). One can immediately see the similarities, with the chief difference being the replacement of x in the classical setting by q^X for the function field case.

Proof. This is proved by Cha in [5, Proposition 2.2]; we include the details of the proof for later comparison. Let $\mathcal{C}_T = \{z \in \mathbb{C} : |z| = q^T\}$ for $T > 0$, and consider the contour integral

$$\frac{1}{2\pi i} \oint_{\mathcal{C}_T} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)}\, du.$$

We can write $1/Z_{C/\mathbb{F}_q}(u)$ in two ways; via (2.3) and (2.1), and via (2.4), yielding the identities

$$\frac{1}{Z_{C/\mathbb{F}_q}(u)} = (1-u)(1-qu) \prod_{j=1}^{2g} \frac{1}{1 - \gamma_j u}, \tag{2.7}$$

$$\frac{1}{Z_{C/\mathbb{F}_q}(u)} = \sum_{N=0}^{\infty} u^N \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D), \tag{2.8}$$

where the first identity is valid for all $u \in \mathbb{C} \setminus \{\gamma_1^{-1}, \ldots, \gamma_{2g}^{-1}\}$, and the second identity is valid for all $|u| < q^{-1}$. So the singularities of the integrand inside $\mathcal{C}_T$

occur at $u = 0$ and at $u = \gamma^{-1}$ for each zero γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$. At the singularity $u = 0$, we have by (2.8) that

$$\operatorname*{Res}_{u=0} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} = \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D).$$

As $Z_{C/\mathbb{F}_q}(u)$ has a simple zero at each γ^{-1}, we obtain from (2.7) that

$$\operatorname*{Res}_{u=\gamma^{-1}} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} = \lim_{u \to \gamma^{-1}} \frac{1}{u^{N+1}} \frac{u - \gamma^{-1}}{Z_{C/\mathbb{F}_q}(u)} = \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \gamma^{N+1}.$$

So by Cauchy's residue theorem,

$$\frac{1}{2\pi i} \oint_{\mathcal{C}_T} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} \, du = \sum_{\gamma} \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \gamma^{N+1} + \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D). \tag{2.9}$$

Summing over all $0 \leq N \leq X - 1$ and evaluating the resulting geometric series, we find that

$$M_{C/\mathbb{F}_q}(X) = -\sum_{\gamma} \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \gamma^X + R_X(q, g, T), \tag{2.10}$$

where the error term $R_X(q, g, T)$ is

$$R_X(q, g, T) = \sum_{\gamma} \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} + \sum_{N=0}^{X-1} \frac{1}{2\pi i} \oint_{\mathcal{C}_T} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} \, du. \tag{2.11}$$

Now (2.7) and the fact that $|u| = q^T$ and $|\gamma_j| = \sqrt{q}$ imply that

$$\begin{aligned} \left| \frac{1}{2\pi i} \oint_{\mathcal{C}_T} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} \, du \right| &\leq \frac{1}{2\pi} \oint_{\mathcal{C}_T} \left| \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} \right| |du| \\ &\leq \frac{\left(q^T + 1\right)\left(q^{1+T} + 1\right)}{\left(q^{1/2+T} - 1\right)^{2g}} q^{-NT}. \end{aligned}$$

As the right-hand side of (2.9) is independent of T, we may take the limit as T tends to infinity in order to find that the contour integral above is zero if $N \geq 3 - 2g$ and at most q^{1-g} in absolute value if $N = 2(1 - g)$. As $g \geq 1$ and $N \geq 0$, this implies that for all $X \geq 1$, the second term in $R_X(q, g, T)$ vanishes if $g \geq 2$, and is a constant of absolute value at most 1 if $g = 1$. Thus $R_X(q, g, T)$ is constant, and hence bounded as X tends to infinity. Upon dividing through (2.10) by $q^{X/2}$ and using the fact that $\gamma = \sqrt{q} e^{i\theta(\gamma)}$, we obtain the result. $\square$

As there are precisely $2g$ zeroes of $Z_{C/\mathbb{F}_q}(u)$, the sum in (2.6) is finite, and hence $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ is bounded. Furthermore, (2.6) proves part of Theorem 1.5 in showing that if $Z_{C/\mathbb{F}_q}(u)$ has simple zeroes, then the inequality (1.5) holding implies that the Mertens conjecture for $C/\mathbb{F}_q$ is true.

We next show that the bound (2.6) is sharp if the zeroes of $Z_{C/\mathbb{F}_q}(u)$ are particularly well-behaved.

Definition 2.5. We say that C satisfies the *Linear Independence hypothesis*, which we abbreviate to LI, if the collection

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

is linearly independent over the rational numbers.

Notably, if C satisfies LI, then all of the zeroes of $Z_{C/\mathbb{F}_q}(u)$ are simple.

Theorem 2.6 (Cha [5, Theorem 2.5]). *Suppose that C satisfies LI. Then*

$$B(C/\mathbb{F}_q) = \sum_{\gamma} \left| \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} \right|.$$

Consequently, if C satisfies LI, then the Mertens conjecture for $C/\mathbb{F}_q$ is true if and only if the inequality (1.5) *holds.*

The proof follows from a direct application of the Kronecker–Weyl theorem, which we prove in Appendix A in the following form.

Lemma 2.7 (Kronecker–Weyl Theorem). *Let $t_1, \ldots, t_g$ be real numbers, and let H be the topological closure in the g-torus*

$$\mathbb{T}^g = \{(z_1, \ldots, z_g) \in \mathbb{C}^g : |z_j| = 1 \text{ for all } 1 \leq j \leq g\}.$$

of the subgroup

$$\widetilde{H} = \left\{ \left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g} \right) \in \mathbb{T}^g : X \in \mathbb{Z} \right\}.$$

Then H is a closed subgroup of $\mathbb{T}^g$. In particular, when the collection $1, t_1, \ldots, t_g$ is linearly independent over the rational numbers, H is precisely $\mathbb{T}^g$. Furthermore, for arbitrary $t_1, \ldots, t_g$ and for any continuous function $h : \mathbb{T}^g \to \mathbb{C}$, we have that

$$\lim_{Y \to \infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g} \right) = \int_H h(z)\, d\mu_H(z),$$

where μ_H is the normalised Haar measure on H.

Proof of Theorem 2.6. As $\gamma_{j+g} = \overline{\gamma_j}$ for each $1 \leq j \leq g$ and as $Z_{C/\mathbb{F}_q}(\overline{u}) = \overline{Z_{C/\mathbb{F}_q}(u)}$,

$$\begin{aligned}
&\sum_{\gamma} \frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} e^{iX\theta(\gamma)} \\
&\qquad = \sum_{j=1}^{g} \left(\frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)} + \frac{1}{{Z_{C/\mathbb{F}_q}}'(\overline{\gamma_j}^{-1})} \frac{\overline{\gamma_j}}{\overline{\gamma_j} - 1} e^{-iX\theta(\gamma_j)} \right) \\
&\qquad = \sum_{j=1}^{g} \left(\frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)} + \overline{\frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)}} \right) \\
&\qquad = 2\Re \left(\sum_{j=1}^{g} \frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)} \right).
\end{aligned}$$

Thus we may write $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ as

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = -2\Re \left(\sum_{j=1}^{g} \frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)} \right) + O_{q,g}\left(\frac{1}{q^{X/2}} \right).$$

The assumption that C satisfies LI then allows us to apply the Kronecker–Weyl theorem with $t_j = \theta(\gamma_j)/2\pi$ for $1 \leq j \leq g$, which tells us that the set

$$\left\{ \left(e^{iX\theta(\gamma_1)}, \ldots, e^{iX\theta(\gamma_g)} \right) \in \mathbb{T}^g : X \in \mathbb{N} \right\}$$

is dense (in fact, equidistributed) in $\mathbb{T}^g$. This implies the existence of a subsequence (X_m) of $\mathbb{N}$ such that

$$\lim_{m \to \infty} \left(e^{iX_m\theta(\gamma_1)}, \ldots, e^{iX_m\theta(\gamma_g)} \right) = \left(e^{-i\omega(\gamma_1)}, \ldots, e^{-i\omega(\gamma_g)} \right),$$

where for $1 \leq j \leq g$,

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

Together with (2.6), this implies that

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

An analogous argument shows that

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

2.2 $M_{C/\mathbb{F}_q}(X)$ and Zeroes of Multiple Order

To complete the proof of Theorem 1.5, it remains to consider the case where $Z_{C/\mathbb{F}_q}(u)$ has zeroes of multiple order; we will show that in this situation, the Mertens conjecture can never hold. We first require the following trivial bound on $M_{C/\mathbb{F}_q}(X)$.

Lemma 2.8. *For any nonsingular curve C over $\mathbb{F}_q$ of genus $g \geq 1$, we have that*

$$M_{C/\mathbb{F}_q}(X) = O_{q,g}\left(q^X\right). \tag{2.12}$$

Proof. By taking absolute values, we trivially have that

$$\left|M_{C/\mathbb{F}_q}(X)\right| \leq \sum_{N=0}^{X-1} b_{C/\mathbb{F}_q}(N),$$

where $b_{C/\mathbb{F}_q}(N)$ is the number of effective divisors of degree N. From [24, Lemma 5.8], there exists a constant c dependent on $C/\mathbb{F}_q$ such that

$$b_{C/\mathbb{F}_q}(N) \sim cq^N$$

for all $N > 2g-2$, while $b_{C/\mathbb{F}_q}(N)$ is finite for $0 \leq N \leq 2g-2$. Summing over all $0 \leq N \leq X-1$ yields the result. □

Corollary 2.9. *For $|u| < q^{-1}$,*

$$\frac{1}{Z_{C/\mathbb{F}_q}(u)} = (1-u)\sum_{X=1}^{\infty} M_{C/\mathbb{F}_q}(X)u^{X-1}. \tag{2.13}$$

Proof. Via partial summation, we have that for $|u| < q^{-1}$ and for $Y \geq 1$ that

$$\sum_{N=0}^{Y-1} u^N \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D) = M_{C/\mathbb{F}_q}(Y)u^{Y-1} - \sum_{X=1}^{Y-1} M_{C/\mathbb{F}_q}(X)\left(u^X - u^{X-1}\right).$$

By taking the limit as Y tends to infinity and using (2.3) and (2.12), we obtain the result. □

The key result that we make use of is the following.

Lemma 2.10 (Landau's Theorem)**.** *Let $A(X)$ be real-valued sequence, and suppose that there exists a positive integer X_0 such that $A(X)$ is of constant sign* *for all $X \geq X_0$. Furthermore, suppose that the supremum v_c of the set of points $v \in [0, \infty)$ for which the sum*

$$\sum_{X=X_0}^{\infty} A(X) v^{X-1}$$

converges satisfies $v_c \leq 1$. Then the function

$$F(u) = \sum_{X=1}^{\infty} A(X) u^{X-1}$$

is holomorphic in the disc $|u| < v_c$ with a singularity at the point v_c.

Proof. By making the change of variables $v = e^{-\sigma}$, we have that

$$\begin{aligned}\sum_{X=X_0}^{\infty} A(X) v^{X-1} &= -\frac{\sigma e^{\sigma}}{1 - e^{-\sigma}} \int_{X_0}^{\infty} A\left(\lfloor X \rfloor\right) e^{-X\sigma}\, dX \\ &= -\frac{\sigma e^{\sigma}}{1 - e^{-\sigma}} \int_{e^{X_0}}^{\infty} \frac{A\left(\lfloor \log x \rfloor\right)}{x^{\sigma}} \frac{dx}{x},\end{aligned}$$

where $\lfloor X \rfloor$ denotes the integer part of X, and the second equality follows from the substitution $x = e^X$. Similarly, letting $u = e^{-s}$ for $\Re(s) > v_c$, we have that

$$\sum_{X=1}^{\infty} A(X) u^{X-1} = -\frac{s e^{s}}{1 - e^{-s}} \int_{e}^{\infty} \frac{A\left(\lfloor \log x \rfloor\right)}{x^{s}} \frac{dx}{x}.$$

The result now follows directly from [19, Lemma 15.1]. □

Finally, we also require the following combinatorial identity.

Lemma 2.11. *Let $|u| < 1$, and let r be a positive integer. Then*

$$\sum_{X=1}^{\infty} X^{r-1} u^X = \frac{1}{(1-u)^r} \sum_{k=0}^{r-1} A(r-1, k) u^{k+1}, \tag{2.14}$$

where the coefficients

$$A(r-1, k) = \sum_{j=0}^{k} \binom{r}{j} (-1)^j (k+1-j)^{r-1}$$

are Eulerian numbers, which satisfy the identity

$$\sum_{k=0}^{r-1} A(r-1, k) = r!.$$

We first deal with the case where $\sqrt{q}$ is an inverse zero of $Z_{C/\mathbb{F}_q}(u)$.

Proposition 2.12. *Let $g \geq 1$, and suppose that $\gamma = \sqrt{q}$ is an inverse zero of $Z_{C/\mathbb{F}_q}(u)$. Then γ has order $r \geq 2$, and*

$$\limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{X^{r-1}q^{X/2}} > 0.$$

In particular, the Mertens conjecture for the function field $C/\mathbb{F}_q$ is false.

Proof. If $u = \sqrt{q}$ is an inverse zero of $Z_{C/\mathbb{F}_q}(u)$, then this zero must be of order $r \geq 2$ due to the functional equation for $Z_{C/\mathbb{F}_q}(u)$. In this case,

$$\lim_{u\to q^{-1/2}} \frac{\left(u - q^{-1/2}\right)^r}{Z_{C/\mathbb{F}_q}(u)} = \frac{r!}{{Z_{C/\mathbb{F}_q}}^{(r)}\left(q^{-1/2}\right)},$$

and this is nonzero and real as $Z_{C/\mathbb{F}_q}(v)$ is real for all real v, so all derivatives of any order of $Z_{C/\mathbb{F}_q}(v)$ at real values v must be real.

Now if $(-1)^r/{Z_{C/\mathbb{F}_q}}^{(r)}\left(q^{-1/2}\right)$ is negative, then we suppose that there exists some $c \geq 0$ and a positive integer X_0 such that $M_{C/\mathbb{F}_q}(X) > -cX^{r-1}q^{X/2}$ for all $X \geq X_0$; we will show that for this to be the case, we must have that $c \geq c_0$ for a certain $c_0 > 0$, and hence that

$$\liminf_{X\to\infty} \frac{M_{C/\mathbb{F}_q}(X)}{X^{r-1}q^{X/2}} \leq -c_0 < 0.$$

Indeed, if $M_{C/\mathbb{F}_q}(X) > -cX^{r-1}q^{X/2}$ for all $X \geq X_0$, then by (2.13) and (2.14),

$$\begin{aligned}\sum_{X=1}^{\infty} &\left(M_{C/\mathbb{F}_q}(X) + cX^{r-1}q^{X/2}\right)u^{X-1} \\ &= \frac{1}{(1-u)Z_{C/\mathbb{F}_q}(u)} + \frac{c}{u\left(1-\sqrt{q}u\right)^r}\sum_{k=0}^{r-1} A(r-1,k)q^{(k+1)/2}u^{k+1}. \quad (2.15)\end{aligned}$$

The right-hand side of (2.15) is holomorphic for $|u| < q^{-1/2}$ and has a singularity at $u = q^{-1/2}$, so Landau's theorem implies that the sum on the left-hand side of (2.15) converges for all $|u| < q^{-1/2}$ and defines a holomorphic function $F(u)$ on this open half-plane. We then multiply both sides of (2.15) by $\left(1-\sqrt{q}u\right)^r$ and consider the limit as u tends to $q^{-1/2}$ from the left through real values; from the right-hand side of (2.15), we find that this limit exists and is equal to

$$\frac{(-1)^r q^{r/2} r!}{\left(1-q^{-1/2}\right){Z_{C/\mathbb{F}_q}}^{(r)}\left(q^{-1/2}\right)} + c\sqrt{q}r!.$$

Now if this were negative, then the left-hand side of (2.15) would tend to negative infinity as u approaches $q^{-1/2}$ from the left. This, however, is impossible, as we can split up this sum into two parts: a sum from $X = 1$ to $X_0 - 1$, and a sum from $X = X_0$ to infinity, and the former sum is uniformly bounded as u tends to $q^{-1/2}$, while the coefficients of the latter sum are nonnegative. Consequently, we conclude that the inequality $M_{C/\mathbb{F}_q}(X) > -cX^{r-1}q^{X/2}$ for all $X \geq X_0$ can only hold provided

$$c \geq \frac{(-1)^{r+1}q^{r/2}}{\left(\sqrt{q}-1\right) {Z_{C/\mathbb{F}_q}}^{(r)}\left(q^{-1/2}\right)} > 0.$$

If $(-1)^r/{\zeta_{C/\mathbb{F}_q}}^{(r)}(1/2)$ is positive, on the other hand, we instead suppose that the inequality $M_{C/\mathbb{F}_q}(X) < cX^{r-1}q^{X/2}$ holds for all $X \geq X_0$, in which case an analogous argument applied to the equation

$$\sum_{X=1}^{\infty} \left(M_{C/\mathbb{F}_q}(X) - cX^{r-1}q^{X/2}\right) u^{X-1} = \frac{1}{(1-u)Z_{C/\mathbb{F}_q}(u)} - \frac{c}{u\left(1-\sqrt{q}u\right)^r} \sum_{k=0}^{r-1} A(r-1,k) q^{(k+1)/2} u^{k+1}$$

shows that

$$\limsup_{X\to\infty} \frac{M_{C/\mathbb{F}_q}(X)}{X^{r-1}q^{X/2}} \geq \frac{(-1)^r q^{r/2}}{\left(\sqrt{q}-1\right) {Z_{C/\mathbb{F}_q}}^{(r)}\left(q^{-1/2}\right)} > 0. \qquad \square$$

The case when $Z_{C/\mathbb{F}_q}\left(q^{-1/2}\right) \neq 0$ but $Z_{C/\mathbb{F}_q}(u)$ nevertheless has a zero of multiple order follows by a similar but slightly more complicated argument.

Proposition 2.13. *Let $g \geq 1$, and suppose that $Z_{C/\mathbb{F}_q}(u)$ has an inverse zero $\gamma = \sqrt{q}e^{i\theta(\gamma)}$ of order $r \geq 2$, but that the order of the inverse zero at $\sqrt{q}$ is of order strictly less than r. Then*

$$\limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q}(X)\right|}{X^{r-1}q^{X/2}} > 0.$$

In particular, the Mertens conjecture for the function field $C/\mathbb{F}_q$ is false.

Proof. Suppose there exists some $c \geq 0$ and a positive integer X_0 such that $M_{C/\mathbb{F}_q}(X) > -cX^{r-1}q^{X/2}$ for all $X \geq X_0$. Once again, Landau's theorem shows that the equation

$$\sum_{X=1}^{\infty} \left(M_{C/\mathbb{F}_q}(X) + cX^{r-1}q^{X/2}\right) u^{X-1} = \frac{1}{(1-u)Z_{C/\mathbb{F}_q}(u)} + \frac{c}{u\left(1-\sqrt{q}u\right)^r} \sum_{k=0}^{r-1} A(r-1,k) q^{(k+1)/2} u^{k+1}.$$

is valid for $|u| < q^{-1/2}$ and defines a holomorphic function $F(u)$ in this disc. Then for $|u| < q^{-1/2}$,

$$\begin{aligned}&\sum_{X=1}^{\infty} \left(M_{C/\mathbb{F}_q}(X) + cq^{X/2}X^{r-1}\right) \left(1 + \cos\left(\phi(\gamma) - (X-1)\theta(\gamma)\right)\right) u^{X-1} \\ &= F(u) + \frac{e^{i\phi(\gamma)}}{2} \frac{1 - ue^{-i\theta(\gamma)}}{1-u} F\left(ue^{-i\theta(\gamma)}\right) + \frac{e^{-i\phi(\gamma)}}{2} \frac{1 - ue^{i\theta(\gamma)}}{1-u} F\left(ue^{i\theta(\gamma)}\right), \quad (2.16)\end{aligned}$$

where we let

$$\phi(\gamma) = \pi - \arg\left(\frac{(-1)^r \gamma^r}{Z_{C/\mathbb{F}_q}{}^{(r)}\left(\gamma^{-1}\right)}\right).$$

Upon multiplying both sides of (2.16) by $\left(1 - \sqrt{q}u\right)^r$, we find via the right-hand side of (2.16) that as u tends to $q^{-1/2}$ from the left through real values, this quantity converges to

$$c\sqrt{q}r! - \frac{q^{r/2} r!}{(1 - q^{-1/2}) \left|Z_{C/\mathbb{F}_q}{}^{(r)}\left(\gamma^{-1}\right)\right|},$$

which must be nonnegative: otherwise, the left-hand side of (2.16) would tend to negative infinity as u approaches $q^{-1/2}$ from the left, a contradiction given the uniform boundedness of the sum from $X = 0$ to X_0 as u tends to $q^{-1/2}$ and the fact that the sum from $X = X_0$ to infinity is nonnegative. Thus

$$c \geq \frac{q^{r/2}}{\left(\sqrt{q} - 1\right) \left|Z_{C/\mathbb{F}_q}{}^{(r)}\left(\gamma^{-1}\right)\right|} > 0,$$

and so

$$\liminf_{X \to \infty} \frac{M_{C/\mathbb{F}_q}(X)}{X^{r-1}q^{X/2}} \leq -\frac{q^{r/2}}{\left(\sqrt{q} - 1\right) \left|Z_{C/\mathbb{F}_q}{}^{(r)}\left(\gamma^{-1}\right)\right|} < 0.$$

An analogous argument shows that we also have that

$$\limsup_{X \to \infty} \frac{M_{C/\mathbb{F}_q}(X)}{X^{r-1}q^{X/2}} \geq \frac{q^{r/2}}{\left(\sqrt{q} - 1\right) \left|Z_{C/\mathbb{F}_q}{}^{(r)}\left(\gamma^{-1}\right)\right|} > 0. \qquad \square$$

2.3 The Limiting Distribution of $M_{C/\mathbb{F}_q}(X)/q^{X/2}$

Let m denote the Lebesgue measure on $[0,1]^g$. For a Borel set $B \subset \mathbb{R}$ and a Borel-measurable function $f : [0,1]^g \to \mathbb{R}$, we write $m(f(\theta_1, \ldots, \theta_g) \in B)$ for

$$m\left(\{(\theta_1, \ldots, \theta_g) \in [0,1]^g : f(\theta_1, \ldots, \theta_g) \in B\}\right).$$

Our main result for this section is the following expression for the natural density of the set of positive integers X for which $\left|M_{C/\mathbb{F}_q}(X)\right| \leq q^{X/2}$, the proof of which is similar to that of the key result of Cha in [4] on Chebyshev's bias in function fields, which in turn is based on the seminal work of Rubinstein and Sarnak in [25].

Proposition 2.14. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$, and suppose that C satisfies LI. The natural density*

$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = \lim_{Y \to \infty} \frac{1}{Y} \# \left\{1 \leq X \leq Y : \left|M_{C/\mathbb{F}_q}(X)\right| \leq q^{X/2}\right\}$$

exists and is equal to

$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = m\left(-1 \leq 2\sum_{j=1}^{g} \left|\frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1}\right| \cos(2\pi\theta_j) \leq 1\right). \tag{2.17}$$

From this, the proof of Theorem 1.6 follows quite easily: it is clear that this density is strictly positive, as there exists an open neighbourhood of the point $(1/4, \ldots, 1/4) \in [0,1]^g$ such that

$$-1 \leq 2\sum_{j=1}^{g} \left|\frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1}\right| \cos(2\pi\theta_j) \leq 1$$

inside this neighbourhood, while it is immediate that $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = 1$ when

$$\sum_{\gamma} \left|\frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)} \frac{\gamma}{\gamma - 1}\right| \leq 1.$$

If the inequality above does not hold, however, then $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) < 1$, for then there exists an open neighbourhood of $(0, \ldots, 0) \in [0,1]^g$ such that

$$2\sum_{j=1}^{g} \left|\frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1}\right| \cos(2\pi\theta_j) > 1$$

inside this neighbourhood.

In fact, we prove something slightly more general than Proposition 2.14: we show that $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ has a limiting distribution as X tends to infinity, the construction of which is based off the Kronecker–Weyl theorem. For any nonsingular projective curve C over $\mathbb{F}_q$ of genus $g \geq 1$, (2.5) allows us to write

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = E_{C/\mathbb{F}_q;\mu}(X) + \varepsilon_{C/\mathbb{F}_q;\mu}(X),$$

where

$$E_{C/\mathbb{F}_q;\mu}(X) = -\sum_{\gamma} \frac{1}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} e^{iX\theta(\gamma)},$$

$$\varepsilon_{C/\mathbb{F}_q;\mu}(X) = O_{q,g}\left(\frac{1}{q^{X/2}}\right),$$

provided that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. We begin by first constructing the limiting distribution of $E_{C/\mathbb{F}_q;\mu}(X)$.

Lemma 2.15. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. There exists a probability measure $\nu_{C/\mathbb{F}_q;\mu}$ on $\mathbb{R}$ that satisfies*

$$\lim_{Y \to \infty} \frac{1}{Y} \sum_{X=1}^{Y} f\left(E_{C/\mathbb{F}_q;\mu}(X)\right) = \int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\mu}(x)$$

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

Proof. By the Kronecker–Weyl theorem with $t_j = \theta(\gamma_j)/2\pi$ for $1 \leq j \leq g$, there exists a subtorus $H \subset \mathbb{T}^g$ satisfying

$$\lim_{Y \to \infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{iX\theta(\gamma_1)}, \ldots, e^{iX\theta(\gamma_g)}\right) = \int_H h(z)\, d\mu_H(z)$$

for every continuous function h on $\mathbb{T}^g$, where μ_H is the normalised Haar measure on H. We now define the probability measure $\nu_{C/\mathbb{F}_q;\mu}$ on $\mathbb{R}$ by

$$\nu_{C/\mathbb{F}_q;\mu}(B) = \mu_H(\widetilde{B})$$

for each Borel set $B \subset \mathbb{R}$, where

$$\widetilde{B} = \left\{(z_1, \ldots, z_g) \in H : -2\Re\left(\sum_{j=1}^{g} \frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} z_j\right) \in B\right\}.$$

The function

$$-2\Re\left(\sum_{j=1}^{g} \frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} z_j\right)$$

is continuous on H, so $\widetilde{B}$ is a Borel set in H, and $\nu_{C/\mathbb{F}_q;\mu}$ is a probability measure as μ_H is the normalised Haar measure on H. So for a bounded continuous function f on $\mathbb{R}$, we define the function $h(z_1, \ldots, z_g)$ on the g-torus $\mathbb{T}^g$ by

$$h(z_1, \ldots, z_g) = f\left(-2\Re\left(\sum_{j=1}^{g} \frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} z_j\right)\right),$$

so that h is continuous on $\mathbb{T}^g$ with

$$f\left(E_{C/\mathbb{F}_q;\mu}(X)\right) = h\left(e^{iX\theta(\gamma_1)}, \ldots, e^{iX\theta(\gamma_g)}\right).$$

Hence by the Kronecker–Weyl theorem,

$$\begin{aligned}\int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\mu}(x) &= \int_H h(z_1, \ldots, z_g)\, d\mu_H(z_1, \ldots, z_g) \\ &= \lim_{Y\to\infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{iX\theta(\gamma_1)}, \ldots, e^{iX\theta(\gamma_g)}\right) \\ &= \lim_{Y\to\infty} \frac{1}{Y} \sum_{X=1}^{Y} f\left(E_{C/\mathbb{F}_q;\mu}(X)\right). \qquad \square\end{aligned}$$

Next, we show using this construction that $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ has a limiting distribution on $\mathbb{R}$. The key tool is the following result that allows us to show that a sequence of measures is weakly convergent.

Lemma 2.16 (Portmanteau Theorem [2, Theorem 2.1]). *Let $\{\nu_Y\}_{Y=1}^{\infty}, \nu$ be probability measures on a metric space $\mathcal{X}$. Then the following are equivalent:*

(1) The sequence of measures ν_Y converges weakly to ν; that is,

$$\lim_{Y\to\infty} \int_{\mathcal{X}} f(x)\, d\nu_Y(x) = \int_{\mathcal{X}} f(x)\, d\nu(x).$$

for every bounded continuous function $f : \mathcal{X} \to \mathbb{R}$.

(2) For every Borel set $B \subset \mathcal{X}$ whose boundary has ν-measure zero,

$$\lim_{Y\to\infty} \nu_Y(B) = \nu(B).$$

(3) For every bounded Lipschitz continuous function $f : \mathcal{X} \to \mathbb{R}$,

$$\lim_{Y\to\infty} \int_{\mathcal{X}} f(x)\, d\nu_Y(x) = \int_{\mathcal{X}} f(x)\, d\nu(x).$$

We also require the following lemma to show the existence of a weak limit of measures. This relies on the notion of tightness of a sequence of measures: we say that a family of probability measures $\{\nu_Y\}$ on a metric space $\mathcal{X}$ is tight if for every $\varepsilon > 0$ there exists a compact set $K \subset \mathcal{X}$ such that $\nu_Y(K) > 1 - \varepsilon$ for all Y.

Lemma 2.17 (Prohorov's Theorem [2, Theorem 5.1]). *Let $\{\nu_Y\}_{Y=1}^{\infty}$ be probability measures on a metric space $\mathcal{X}$. If $\{\nu_Y\}_{Y=1}^{\infty}$ is tight, then every subsequence of $\{\nu_Y\}_{Y=1}^{\infty}$ has a weakly convergent subsubsequence.*

Proposition 2.18. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. The function $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ has a limiting distribution $\nu_{C/\mathbb{F}_q;\mu}$ on $\mathbb{R}$. That is, there exists a probability measure $\nu_{C/\mathbb{F}_q;\mu}$ on $\mathbb{R}$ such that*

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

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

Proof. For each positive integer Y, let $\nu_{Y,\mu}$ be the probability measure on $\mathbb{R}$ given by

$$\nu_{Y,\mu}(B) = \frac{1}{Y} \# \left\{1 \leq X \leq Y : \frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} \in B\right\}$$

for any Borel set $B \subset \mathbb{R}$, so that for any continuous function f on $\mathbb{R}$,

$$\int_{\mathbb{R}} f(x)\, d\nu_{Y,\mu}(x) = \frac{1}{Y} \sum_{X=1}^{Y} f\left(\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}}\right).$$

As $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ is bounded, the probability measures $\{\nu_{Y,\mu}\}$ are tight, so by Prohorov's Theorem, for every subsequence $\{Y_k\}$ there exists a subsubsequence $\{Y_{k_\ell}\}$ and a probability measure $\widetilde{\nu}_{C/\mathbb{F}_q;\mu}$ such that $\nu_{Y_{k_\ell};\mu}$ converges weakly to $\widetilde{\nu}_{C/\mathbb{F}_q;\mu}$. We will show that $\widetilde{\nu}_{C/\mathbb{F}_q;\mu} = \nu_{C/\mathbb{F}_q;\mu}$ for every such subsequence, which will imply that the probability measures $\{\nu_{Y,\mu}\}$ converge weakly to $\nu_{C/\mathbb{F}_q;\mu}$, as required.

So if $\nu_{Y_{k_\ell};\mu}$ converges weakly to $\widetilde{\nu}_{C/\mathbb{F}_q;\mu}$, then by the Portmanteau theorem,

$$\lim_{\ell\to\infty} \frac{1}{Y_{k_\ell}} \sum_{X=1}^{Y_{k_\ell}} f\left(\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}}\right) = \lim_{\ell\to\infty} \int_{\mathbb{R}} f(x)\, d\nu_{Y_{k_\ell};\mu}(x) = \int_{\mathbb{R}} f(x)\, d\widetilde{\nu}_{C/\mathbb{F}_q;\mu}(x)$$

for every bounded Lipschitz continuous function $f : \mathbb{R} \to \mathbb{R}$, that is, for every function f for which there exists a constant $c_f \geq 0$ such that

$$\sup_{\substack{x,y\in\mathbb{R} \\ x\neq y}} \frac{|f(x) - f(y)|}{|x - y|} = c_f < \infty.$$

The Lipschitz condition implies that

$$\frac{1}{Y_{k_\ell}} \sum_{X=1}^{Y_{k_\ell}} f\left(\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}}\right) \geq \frac{1}{Y_{k_\ell}} \sum_{X=1}^{Y_{k_\ell}} f\left(E_{C/\mathbb{F}_q;\mu}(X)\right) - \frac{c_f}{Y_{k_\ell}} \sum_{X=1}^{Y_{k_\ell}} |\varepsilon_{C/\mathbb{F}_q;\mu}(X)|.$$

As ℓ tends to infinity, the left-hand side converges to $\int_{\mathbb{R}} f(x)\, d\widetilde{\nu}_{C/\mathbb{F}_q;\mu}(x)$ by assumption. On the right-hand side, the first term converges to $\int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\mu}(x)$ by Lemma 2.15, while the second term tends to zero as $\varepsilon_{C/\mathbb{F}_q;\mu}(X) = O(q^{-X/2})$. Thus

$$\int_{\mathbb{R}} f(x)\, d\widetilde{\nu}_{C/\mathbb{F}_q;\mu}(x) \geq \int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\mu}(x).$$

Furthermore, the Lipschitz condition also implies that

$$\frac{1}{Y_{k_\ell}} \sum_{X=1}^{Y_{k_\ell}} f\left(\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}}\right) \leq \frac{1}{Y_{k_\ell}} \sum_{X=1}^{Y_{k_\ell}} f\left(E_{C/\mathbb{F}_q;\mu}(X)\right) + \frac{c_f}{Y_{k_\ell}} \sum_{X=1}^{Y_{k_\ell}} |\varepsilon_{C/\mathbb{F}_q;\mu}(X)|,$$

and hence

$$\int_{\mathbb{R}} f(x)\, d\widetilde{\nu}_{C/\mathbb{F}_q;\mu}(x) \leq \int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\mu}(x).$$

Combining both inequalities shows that $\nu_{Y_{k_\ell};\mu}$ converges weakly to $\nu_{C/\mathbb{F}_q;\mu}$. By the uniqueness of weak limits of measures, we conclude that $\widetilde{\nu}_{C/\mathbb{F}_q;\mu} = \nu_{C/\mathbb{F}_q;\mu}$. □

Proof of Proposition 2.14. The Portmanteau Theorem together with Proposition 2.18 implies that

$$\lim_{Y\to\infty} \frac{1}{Y} \# \left\{1 \leq X \leq Y : \frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} \in B\right\} = \nu_{C/\mathbb{F}_q;\mu}(B)$$

for every Borel set $B \subset \mathbb{R}$ whose boundary has $\nu_{C/\mathbb{F}_q;\mu}$-measure zero. From this, we can show that $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right)$ exists and is equal to $\nu_{C/\mathbb{F}_q;\mu}([-1,1])$ provided $\nu_{C/\mathbb{F}_q;\mu}(\{-1,1\}) = 0$. To prove this last point, we observe that the assumption that C satisfies LI implies that the topological closure of

$$\widetilde{H} = \left\{\left(e^{i\theta(\gamma_1)X}, \ldots, e^{i\theta(\gamma_g)X}\right) \in \mathbb{T}^g : X \in \mathbb{Z}\right\}$$

in $\mathbb{T}^g$ is $H = \mathbb{T}^g$. So the normalised Haar measure on H is the Lebesgue measure on the g-torus, and consequently for a Borel set $B \subset \mathbb{R}$,

$$\begin{aligned}\nu_{C/\mathbb{F}_q;\mu}(B) &= m\left(-2\Re\left(\sum_{j=1}^{g} \frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{2\pi i\theta_j}\right) \in B\right)\\ &= m\left(2\sum_{j=1}^{g} \left|\frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1}\right| \cos(2\pi\theta_j) \in B\right)\end{aligned}$$

by the translation invariance of the Lebesgue measure. Note that

$$2\sum_{j=1}^{g} \left|\frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1}\right| \cos(2\pi\theta_j)$$

is real analytic on $[0,1]^g$ and not uniformly constant. As the zero set of a non-uniformly zero real analytic function has Lebesgue measure zero, we determine that

$$m\left(2\sum_{j=1}^{g}\left|\frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma_j^{-1}\right)}\frac{\gamma_j}{\gamma_j-1}\right|\cos(2\pi\theta_j)=c\right)=0$$

for any $c\in\mathbb{R}$. Thus $\nu_{C/\mathbb{F}_q;\mu}$ is atomless, and hence $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right)$ is equal to $\nu_{C/\mathbb{F}_q;\mu}([-1,1])$. $\square$

Chapter 3

Examples in Low Genus

3.1 Elliptic Curves over Finite Fields

In this chapter, we study local Mertens conjectures in the simplest nontrivial case, namely $g = 1$, where we suppose that $C/\mathbb{F}_q$ is the function field of an elliptic curve over a finite field. That is, we suppose that C is a nonsingular projective algebraic curve of genus one over $\mathbb{F}_q$ with a given point defined over $\mathbb{F}_q$. Then $Z_{C/\mathbb{F}_q}(u)$ is of the form

$$Z_{C/\mathbb{F}_q}(u) = \frac{(1-\gamma u)(1-\overline{\gamma}u)}{(1-u)(1-qu)} = \frac{1-au+qu^2}{(1-u)(1-qu)}$$

for some $\gamma = \sqrt{q}e^{i\theta(\gamma)}$ with $0 \leq \theta(\gamma) \leq \pi$, so that the integer a satisfies

$$a = 2\Re(\gamma) = 2\sqrt{q}\cos\theta(\gamma).$$

Equivalently, γ can be defined in terms of the integer a via

$$\theta(\gamma) = \arccos\left(\frac{a}{2\sqrt{q}}\right).$$

Geometrically, the integer a is the trace of the Frobenius endomorphism acting on the elliptic curve C over $\mathbb{F}_q$. Notably, there are several restrictions on the possible values that a may take. The following lemma fully characterises the possible values of a.

Lemma 3.1 (Waterhouse [29, Theorem 4.1])**.** *Let a be an integer. Then a is the trace of the Frobenius endomorphism acting on some elliptic curve C over a finite field $\mathbb{F}_q$ of characteristic p if and only if one of the following conditions is satisfied:*

(1) $a \not\equiv 0 \pmod p$ *and* $|a| < 2\sqrt{q}$*; for such an integer* a*, the corresponding angle* $\theta(\gamma)$ *is such that* $\theta(\gamma)/\pi$ *is irrational,*

(2) (i) $q = p^m$ *with* $a = 2\sqrt{q}$*, where* m *is even, so that* $\theta(\gamma) = 0$*,*

(2) (ii) $q = p^m$ *with* $a = -2\sqrt{q}$*, where* m *is even, so that* $\theta(\gamma) = \pi$*,*

(3) (i) $q = p^m$ *with* $a = \sqrt{q}$*, where* m *is even and* $p \not\equiv 1 \pmod 3$*, so that* $\theta(\gamma) = \pi/3$*,*

(3) (ii) $q = p^m$ *with* $a = -\sqrt{q}$*, where* m *is even and* $p \not\equiv 1 \pmod 3$*, so that* $\theta(\gamma) = 2\pi/3$*,*

(4) (i) $q = 2^m$ *with* $a = \sqrt{2q}$*, where* m *is odd, so that* $\theta(\gamma) = \pi/4$*,*

(4) (ii) $q = 2^m$ *with* $a = -\sqrt{2q}$*, where* m *is odd, so that* $\theta(\gamma) = 3\pi/4$*,*

(4) (iii) $q = 3^m$ *with* $a = \sqrt{3q}$*, where* m *is odd, so that* $\theta(\gamma) = \pi/6$*,*

(4) (iv) $q = 3^m$ *with* $a = -\sqrt{3q}$*, where* m *is odd, so that* $\theta(\gamma) = 5\pi/6$*,*

(5) $q = p^m$ *with* $a = 0$*, where either* m *is even and* $p \not\equiv 1 \pmod 4$*, or* m *is odd, so that* $\theta(\gamma) = \pi/2$*.*

From the second part of this lemma, we may completely determine which elliptic curves satisfy LI.

Corollary 3.2. *Let* C *be an elliptic curve over a finite field* $\mathbb{F}_q$ *of characteristic* p*, so that* a *and* q *satisfying one of conditions (1)—(5) of Lemma 3.1. Then* C *satisfies LI if and only if condition (1) is satisfied,* $Z_{C/\mathbb{F}_q}(u)$ *has zeroes of multiple order if and only if condition (2) is satisfied, and* C *fails to satisfy LI but* $Z_{C/\mathbb{F}_q}(u)$ *has only simple zeroes if and only if one of conditions (3)—(5) is satisfied.*

Next, we determine an explicit expression for $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ using Proposition 2.4; remarkably, we may eliminate any error term for this expression. We must consider two cases: when $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes, and when $Z_{C/\mathbb{F}_q}(u)$ has a zero of order 2. For the first case, we have the following result.

Proposition 3.3. *Let* C *be an elliptic curve over* $\mathbb{F}_q$*, and suppose that* $Z_{C/\mathbb{F}_q}(u)$

has only simple zeroes. Then

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = 2\sqrt{\frac{q+1-a}{4q-a^2}}\cos\left(\omega + X\theta\right), \tag{3.1}$$

where a is the trace of the Frobenius endomorphism, and $\omega \in (-\pi/2, \pi/2)$, $\theta \in [0, \pi]$ are given by

$$\omega = \arctan\left(\frac{a-2}{2\sqrt{4q-a^2}}\right), \tag{3.2}$$

$$\theta = \arccos\left(\frac{a}{2\sqrt{q}}\right). \tag{3.3}$$

We remark that (3.1) is equivalent to

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = \cos(X\theta) - \frac{a-2}{\sqrt{4q-a^2}}\sin(X\theta). \tag{3.4}$$

Proof. The fact that $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes is equivalent to $\gamma \neq \overline{\gamma}$. Now using the fact that

$$Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right) = -\frac{\gamma(1-\overline{\gamma}\gamma^{-1})}{(1-\gamma^{-1})(1-q\gamma^{-1})} = -\frac{\gamma}{\gamma-1}\frac{\overline{\gamma}-\gamma}{\overline{\gamma}-1},$$

we find from (2.10) that

$$\begin{aligned}\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} &= \frac{\overline{\gamma}-1}{\overline{\gamma}-\gamma}e^{iX\theta(\gamma)} + \frac{\gamma-1}{\gamma-\overline{\gamma}}e^{-iX\theta(\gamma)} + \frac{1}{q^{X/2}}R_X(q,1,T) \\ &= 2\Re\left(\frac{\overline{\gamma}-1}{\overline{\gamma}-\gamma}e^{iX\theta(\gamma)}\right) + \frac{1}{q^{X/2}}R_X(q,1,T),\end{aligned}$$

with $R_X(q,1,T)$ as in (2.11). As $\gamma = \sqrt{q}e^{i\theta(\gamma)}$, we see that

$$\frac{\overline{\gamma}-1}{\overline{\gamma}-\gamma} = \frac{\sqrt{q}\cos\theta(\gamma) - 1 - i\sqrt{q}\sin\theta(\gamma)}{-2i\sqrt{q}\sin\theta(\gamma)} = \frac{\sqrt{q+1-2\sqrt{q}\cos\theta(\gamma)}}{2\sqrt{q}\sin\theta(\gamma)}e^{i\omega(\gamma)},$$

where

$$\omega(\gamma) = \arctan\left(\frac{\sqrt{q}\cos\theta(\gamma)-1}{\sqrt{q}\sin\theta(\gamma)}\right),$$

and consequently

$$\begin{aligned}\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} &= \frac{\sqrt{q+1-2\sqrt{q}\cos\theta(\gamma)}}{\sqrt{q}\sin\theta(\gamma)}\cos\left(\omega(\gamma) + X\theta(\gamma)\right) + \frac{1}{q^{X/2}}R_X(q,1,T) \\ &= \cos(X\theta(\gamma)) - \frac{\sqrt{q}\cos\theta(\gamma)-1}{\sqrt{q}\sin\theta(\gamma)}\sin(X\theta(\gamma)) + \frac{1}{q^{X/2}}R_X(q,1,T),\end{aligned} \tag{3.5}$$

where the second equality follows from the cosine angle-sum formula. Now the proof of Proposition 2.4 shows that $R_X(q, g, T)$ is constant for $X \geq 3 - 2g$, and hence for all $X \geq 1$ when $g = 1$. We can therefore determine the value of $R_X(q, 1, T)$ simply by taking $X = 1$ in (3.5), so that

$$M_{C/\mathbb{F}_q}(1) = 1 + R_1(q, 1, T).$$

On the other hand,

$$M_{C/\mathbb{F}_q}(1) = \sum_{\deg(D)=0} \mu_{C/\mathbb{F}_q}(D) = 1$$

as the only divisor of degree zero is the zero divisor, and so $R_X(q, 1, T) = 0$. We complete the proof by noting that $a = 2\sqrt{q}\cos\theta(\gamma)$ with $0 \leq \theta(\gamma) \leq \pi$, so that

$$2\sqrt{q}\sin\theta(\gamma) = \sqrt{4q - a^2}. \qquad \square$$

The analogous result in the case where $Z_{C/\mathbb{F}_q}(u)$ has a zero of multiple order is the following.

Proposition 3.4. *Let C be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p, and suppose that $Z_{C/\mathbb{F}_q}(u)$ has zeroes of multiple order, so that $q = p^m$ with $a = \pm 2\sqrt{q}$, where m is even. Then*

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = -(\pm 1)^X \left(1 \mp \frac{1}{\sqrt{q}}\right) X + (\pm 1)^X. \tag{3.6}$$

Proof. If $a = \pm 2\sqrt{q}$, then $\gamma = \overline{\gamma} = \pm\sqrt{q}$. From the proof of Proposition 2.4, we have that for $N \geq 0$,

$$\sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D) = -\operatorname*{Res}_{u=\pm q^{-1/2}} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} + \frac{1}{2\pi i} \oint_{\mathcal{C}_T} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)}\, du,$$

with the last term equal to zero for $N \geq 1$. Now

$$\begin{aligned}\operatorname*{Res}_{u=\pm q^{-1/2}} \frac{1}{u^{N+1}} \frac{1}{Z_{C/\mathbb{F}_q}(u)} &= \lim_{u \to \pm q^{-1/2}} \frac{d}{du} \frac{\left(u \mp q^{-1/2}\right)^2}{u^{N+1}} \frac{(1-u)(1-qu)}{\left(1 \mp \sqrt{q}u\right)^2} \\ &= (\pm 1)^{N+1} \left(\sqrt{q} \mp 1\right)^2 N q^{(N-1)/2}.\end{aligned}$$

This vanishes when $N = 0$, whereas $\sum_{\deg(D)=0} \mu_{C/\mathbb{F}_q}(D) = 1$, and so

$$\frac{1}{2\pi i} \oint_{\mathcal{C}_T} \frac{1}{u} \frac{1}{Z_{C/\mathbb{F}_q}(u)}\, du = 1.$$

Consequently,

$$\sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D) = -(\pm 1)^{N+1} \left(\sqrt{q} \mp 1\right)^2 N q^{(N-1)/2} + \begin{cases} 1 & \text{if } N = 0, \\ 0 & \text{otherwise,} \end{cases}$$

which leads to the result upon summing over all $0 \leq N \leq X-1$ and then dividing through by $q^{X/2}$. $\square$

These two results can now be used to find the values

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

$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = \lim_{Y\to\infty} \frac{1}{Y} \# \left\{1 \leq X \leq Y : \left|M_{C/\mathbb{F}_q}(X)\right| \leq q^{X/2}\right\}$$

for each elliptic curve C over a given finite field $\mathbb{F}_q$. In the following section, we determine these two values for each possible combination of values for q and a as determined in Lemma 3.1, culminating in a proof of Theorem 1.7.

3.2 Proof of Theorem 1.7

We must determine $B(C/\mathbb{F}_q)$ and $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right)$ for the restricted values of q and a found in conditions (1)—(5) of Lemma 3.1.

(1) If $q = p^m$ with $a \not\equiv 0 \pmod{p}$ and $|a| < 2\sqrt{q}$, then θ/π is irrational, with θ as in (3.3). The Kronecker–Weyl theorem then shows that $X\theta$ is equidistributed modulo π as X tends to infinity, and so from (3.1),

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

$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = 1 - \frac{1}{\pi} \arccos\left(\frac{1}{2}\sqrt{\frac{4q-a^2}{q+1-a}}\right).$$

The Mertens conjecture for $C/\mathbb{F}_q$ therefore holds precisely when

$$2\sqrt{\frac{q+1-a}{4q-a^2}} \leq 1.$$

Upon squaring both sides and simplifying, we arrive at the inequality

$$(a-2)^2 \leq 0,$$

which has only the solution $a = 2$, provided $p \neq 2$. Similarly, $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = 1$ if and only if

$$\arccos\left(\frac{1}{2}\sqrt{\frac{4q-a^2}{q+1-a}}\right) = 0,$$

which again holds only when $a = 2$ and $p \neq 2$.

(2) If $q = p^m$ with $a = \pm 2\sqrt{q}$, where m is even, then from (3.6),

$$B(C/\mathbb{F}_q) = \infty,$$
$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = 0.$$

For conditions (3)—(5), we find that $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ takes only finitely many values, so that the limiting distribution of $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ is simply a finite sum of point masses. The natural density $d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right)$ in each case is therefore given by the proportion of values taken by $M_{C/\mathbb{F}_q}(X)/q^{X/2}$ that lie between -1 and 1.

(3) (i) If $q = p^m$ with $a = \sqrt{q}$, where m is even and $p \not\equiv 1 \pmod 3$, we have from (3.4) that

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = \cos\left(\frac{\pi X}{3}\right) - \frac{\sqrt{3}}{3}\left(1 - \frac{2}{\sqrt{q}}\right)\sin\left(\frac{\pi X}{3}\right).$$

We calculate the 6 cases of $X \pmod 6$:

$X \pmod 6$	$M_{C/\mathbb{F}_q}(X)/q^{X/2}$
0	1
1	$1/\sqrt{q}$
2	$-1+1/\sqrt{q}$
3	-1
4	$-1/\sqrt{q}$
5	$1-1/\sqrt{q}$

So

$$B(C/\mathbb{F}_q) = 1,$$
$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = 1.$$

(3) (ii) Similarly, if $q = p^m$ with $a = -\sqrt{q}$, where m is even and $p \not\equiv 1 \pmod 3$,

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = \cos\left(\frac{2\pi X}{3}\right) + \frac{\sqrt{3}}{3}\left(1 + \frac{2}{\sqrt{q}}\right)\sin\left(\frac{2\pi X}{3}\right).$$

The 3 cases of $X \pmod 3$ are

$X \pmod 3$	$M_{C/\mathbb{F}_q}(X)/q^{X/2}$
0	1
1	$1/\sqrt{q}$
2	$-1-1/\sqrt{q}$

This shows that

$$B(C/\mathbb{F}_q) = 1 + \frac{1}{\sqrt{q}},$$
$$d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) = \frac{2}{3}.$$

(4) (i) If $q = 2^m$ with $a = \sqrt{2q}$, where m is odd, then

$$\frac{M_{C/\mathbb{F}_{2^m}}(X)}{2^{mX/2}} = \cos\left(\frac{\pi X}{4}\right) - \left(1 - \frac{1}{2^{(m-1)/2}}\right)\sin\left(\frac{\pi X}{4}\right).$$

We analyse the 8 cases of $X \pmod 8$:

$X \pmod 8$	$M_{C/\mathbb{F}_{2^m}}(X)/2^{mX/2}$
0	1
1	$2^{-m/2}$
2	$-1+2^{-(m-1)/2}$
3	$-\sqrt{2}+2^{-m/2}$
4	-1
5	$-2^{-m/2}$
6	$1-2^{-(m-1)/2}$
7	$\sqrt{2}-2^{-m/2}$

So

$$B(C/\mathbb{F}_{2^m}) = \begin{cases} 1 & \text{if } m = 1, \\ \sqrt{2} - \dfrac{1}{2^{m/2}} & \text{if } m \geq 3, \end{cases}$$
$$d\left(\mathcal{P}_{C/\mathbb{F}_{2^m};\mu}\right) = \begin{cases} 1 & \text{if } m = 1, \\ 3/4 & \text{if } m \geq 3. \end{cases}$$

(4) (ii) Likewise, if $q = 2^m$ with $a = -\sqrt{2q}$, where m is odd, then

$$\frac{M_{C/\mathbb{F}_{2^m}}(X)}{2^{mX/2}} = \cos\left(\frac{3\pi X}{4}\right) + \left(1 + \frac{1}{2^{(m-1)/2}}\right)\sin\left(\frac{3\pi X}{4}\right).$$

The table of values of $X \pmod 8$ is

$X \pmod 8$	$M_{C/\mathbb{F}_{2^m}}(X)/2^{mX/2}$
0	1
1	$2^{-m/2}$
2	$1+2^{-(m-1)/2}$
3	$\sqrt{2}+2^{-m/2}$
4	-1
5	$-2^{-m/2}$
6	$-1-2^{-(m-1)/2}$
7	$-\sqrt{2}-2^{-m/2}$

Thus

$$B(C/\mathbb{F}_{2^m}) = \sqrt{2} + \frac{1}{2^{m/2}},$$
$$d\left(\mathcal{P}_{C/\mathbb{F}_{2^m};\mu}\right) = \frac{1}{2}.$$

(4) (iii) If $q = 3^m$ with $a = \sqrt{3q}$, where m is odd, then

$$\frac{M_{C/\mathbb{F}_{3^m}}(X)}{3^{mX/2}} = \cos\left(\frac{\pi X}{6}\right) - \left(1 - \frac{2}{3^{m/2}}\right)\sin\left(\frac{\pi X}{6}\right).$$

The 12 cases of $X \pmod{12}$ are

$X \pmod{12}$	$M_{C/\mathbb{F}_{3^m}}(X)/3^{mX/2}$
0	1
1	$(\sqrt{3}-1)/2+3^{-m/2}$
2	$-(\sqrt{3}-1)/2+3^{-(m-1)/2}$
3	$-1+2\times 3^{-m/2}$
4	$-(\sqrt{3}+1)/2-3^{-(m-1)/2}$
5	$-(\sqrt{3}+1)/2+3^{-m/2}$
6	-1
7	$-(\sqrt{3}-1)/2-3^{-m/2}$
8	$(\sqrt{3}-1)/2-3^{-(m-1)/2}$
9	$1-2\times 3^{-m/2}$
10	$(\sqrt{3}+1)/2+3^{-(m-1)/2}$
11	$(\sqrt{3}+1)/2-3^{-m/2}$

Consequently,

$$B(C/\mathbb{F}_{3^m}) = \frac{\sqrt{3}+1}{2} + \frac{1}{3^{(m-1)/2}},$$
$$d\left(\mathcal{P}_{C/\mathbb{F}_{3^m};\mu}\right) = \frac{2}{3}.$$

(4) (iv) Next, if $q = 3^m$ with $a = -\sqrt{3q}$, where m is odd, then

$$\frac{M_{C/\mathbb{F}_{3^m}}(X)}{3^{mX/2}} = \cos\left(\frac{5\pi X}{6}\right) + \left(1 + \frac{2}{3^{m/2}}\right)\sin\left(\frac{5\pi X}{6}\right).$$

Now

$X \pmod{12}$	$M_{C/\mathbb{F}_{3^m}}(X)/3^{mX/2}$
0	1
1	$-(\sqrt{3}-1)/2 + 3^{-m/2}$
2	$-(\sqrt{3}-1)/2 - 3^{-(m-1)/2}$
3	$1 + 2 \times 3^{-m/2}$
4	$-(\sqrt{3}+1)/2 - 3^{-(m-1)/2}$
5	$(\sqrt{3}+1)/2 - 3^{-m/2}$
6	-1
7	$(\sqrt{3}-1)/2 - 3^{-m/2}$
8	$(\sqrt{3}-1)/2 + 3^{-(m-1)/2}$
9	$-1 - 2 \times 3^{-m/2}$
10	$(\sqrt{3}+1)/2 + 3^{-(m-1)/2}$
11	$-(\sqrt{3}+1)/2 + 3^{-m/2}$

So we have that

$$\begin{aligned} B(C/\mathbb{F}_{3^m}) &= \frac{\sqrt{3}+1}{2} + \frac{1}{3^{(m-1)/2}}, \\ d\left(\mathcal{P}_{C/\mathbb{F}_{3^m};\mu}\right) &= \frac{1}{2}. \end{aligned}$$

(5) Finally, if $q = p^m$ with $a = 0$, where either m is even and $p \not\equiv 1 \pmod 4$, or m is odd, then

$$\frac{M_{C/\mathbb{F}_q}(X)}{q^{X/2}} = \cos\left(\frac{\pi X}{2}\right) + \frac{1}{\sqrt{q}}\sin\left(\frac{\pi X}{2}\right).$$

The 4 cases of $X \pmod 4$ are

$X \pmod 4$	$M_{C/\mathbb{F}_q}(X)/q^{X/2}$
0	1
1	$1/\sqrt{q}$
2	-1
3	$-1/\sqrt{q}$

Thus

$$
\begin{aligned}
B(C/\mathbb{F}_q) &= 1, \\
d\left(\mathcal{P}_{C/\mathbb{F}_q;\mu}\right) &= 1.
\end{aligned}
$$

Chapter 4

Global Mertens Conjectures

4.1 Averages over Families of Curves

In this section, we find a matrix theoretic expression for the average proportion of curves in a certain family for which the Mertens conjecture is true as the finite field $\mathbb{F}_q$ grows larger. This involves expressing the quantity

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

in the language of unitary symplectic matrices. The space of unitary symplectic matrices $\mathrm{USp}_{2g}(\mathbb{C})$ consists of $2g \times 2g$ matrices U with complex entries satisfying $U^\dagger U = I$ and $U^T JU = J$, where $J = \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$. 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 $\mathrm{USp}_{2g}(\mathbb{C})$. Thus the set of conjugacy classes $\mathrm{USp}_{2g}(\mathbb{C})^\#$ of $\mathrm{USp}_{2g}(\mathbb{C})$ corresponds to $[0, \pi]^g$.

Definition 4.1. For each $U \in \mathrm{USp}_{2g}(\mathbb{C})$, 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,

$$\mathcal{Z}_U(\theta) = \prod_{j=1}^{2g} \left(1 - e^{i(\theta_j - \theta)}\right) = 2^g \prod_{j=1}^{g} e^{i\theta} \left(\cos\theta - \cos\theta_j\right). \tag{4.1}$$

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

$$\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}(\theta) = P_{C/\mathbb{F}_q}\left(\frac{e^{-i\theta}}{\sqrt{q}}\right) = \prod_{j=1}^{2g}\left(1 - e^{i(\theta(\gamma_j)-\theta)}\right). \tag{4.2}$$

That is, the eigenangles $(\theta_1, \ldots, \theta_g)$ corresponding to the unitarised Frobenius conjugacy class $\vartheta(C/\mathbb{F}_q)$ are precisely $(\theta(\gamma_1), \ldots, \theta(\gamma_g))$.

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

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

where $e^{i\theta_1}, \ldots, e^{i\theta_{2g}}$ are the eigenvalues of U. We observe that φ depends only on the conjugacy class $(\theta_1, \ldots, \theta_g)$ 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 $\mathrm{USp}_{2g}(\mathbb{C})$ with repeated eigenvalues has measure zero with respect to the normalised Haar measure on $\mathrm{USp}_{2g}(\mathbb{C})$.

Lemma 4.2 (Cha [5, Equation (26)]). *Suppose that C satisfies LI. Then we have that*

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

in the large q limit.

Proof. As C satisfies LI, we have from Theorem 2.6 that

$$B(C/\mathbb{F}_q) = \sum_{\gamma}\left|\frac{1}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|.$$

Now by (2.1),

$$\frac{1}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1} = \frac{1-\overline{\gamma}}{P_{C/\mathbb{F}_q}{}'(\gamma^{-1})},$$

whereas differentiating (4.2) shows that

$$\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta) = -\frac{ie^{-i\theta}}{\sqrt{q}}P_{C/\mathbb{F}_q}{}'\left(\frac{e^{-i\theta}}{\sqrt{q}}\right), \tag{4.3}$$

and so by taking $\theta = \theta(\gamma)$, so that $e^{-i\theta(\gamma)}/\sqrt{q} = \gamma^{-1}$, we find that

$$\frac{1}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1} = \frac{ie^{-2i\theta(\gamma)}}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))} - \frac{1}{\sqrt{q}}\frac{ie^{-i\theta(\gamma)}}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))}.$$

This yields the asymptotic

$$\left|\frac{1}{{Z_{C/\mathbb{F}_q}}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right| = \frac{1}{|{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}}'(\theta(\gamma))|} + O_g\left(\frac{1}{\sqrt{q}}\frac{1}{|{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}}'(\theta(\gamma))|}\right),$$

so by summing over all inverse zeroes γ, we obtain the desired identity. □

We wish to determine the proportion of a family of curves that satisfy the Mertens conjecture. While we would like to choose this family to be as general as possible, it is imperative that we ensure that most curves in such a family satisfy LI, for otherwise it becomes significantly more difficult to analyse the behaviour of $B(C/\mathbb{F}_q)$. For this reason, we choose a family of hyperelliptic curves, as we shall show that we are then assured that LI holds for most such curves, with the added bonus of a framework for certain equidistribution results to hold. Via Theorem 2.6, the former property yields yield a precise formula for $B(C/\mathbb{F}_q)$, while the latter allows us to use random matrix theory to compute averages in terms of integrals over $\mathrm{USp}_{2g}(\mathbb{C})$.

Let $q = p^m$ be a prime power with $p > 2$, $n \geq 1$, and let $\mathbb{F}_{q^n}$ be a finite field with q^n elements. 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 polynomials 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" $C \in \mathcal{H}_{2g+1,q^n}$.

Definition 4.3. 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

$$\lim_{n\to\infty} \frac{\#\{C \in \mathcal{H}_{2g+1,q^n} : C \text{ satisfies } D_n\}}{\#\mathcal{H}_{2g+1,q^n}} = 1.$$

Theorem 4.4 (Chavdarov [6], Kowalski [16]; see [5, Theorem 3.1])**.** *For fixed q and $g \geq 1$,*

$$\lim_{n\to\infty} \frac{\#\{C \in \mathcal{H}_{2g+1,q^n} : C \textit{ satisfies } \mathrm{LI}\}}{\#\mathcal{H}_{2g+1,q^n}} = 1.$$

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

For brevity's sake, we write $C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{LI}$ if C satisfies LI, and conversely if C does not satisfy LI, we write $C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{LI}^c$.

Proposition 4.5 (Deligne's Equidistribution Theorem [13, Theorem 10.8.2])**.** *Let f be a continuous function on $\mathrm{USp}_{2g}(\mathbb{C})$ that is central, so that f is dependent only on the conjugacy class $(\theta_1, \ldots, \theta_g)$ of each matrix $U \in \mathrm{USp}_{2g}(\mathbb{C})$. Then for $g \geq 1$,*

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

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

Equivalently, consider the sequence of probability measures

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

on $\mathrm{USp}_{2g}(\mathbb{C})$, where $\delta_{U^\#}$ is a point mass at a conjugacy class $U^\# \in \mathrm{USp}_{2g}(\mathbb{C})^\#$. Then Deligne's equidistribution theorem merely states that the sequence of measures μ_n converges weakly to μ_{Haar} as n tends to infinity. As $\mathrm{USp}_{2g}(\mathbb{C})$ is a connected Lie group, and hence metrisable, we may apply the Portmanteau theorem to the sequence of probability measures μ_n in order to obtain an equivalent reformulation of Deligne's equidistribution theorem.

Corollary 4.6. *For $g \geq 1$,*

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

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

One can calculate this Haar measure precisely by using the following formula to convert it into an integral over $[0, \pi]^g$.

Proposition 4.7 (Weyl Integration Formula [13, §5.0.4])**.** *Let f be a bounded, Borel-measurable complex-valued central function on $\mathrm{USp}_{2g}(\mathbb{C})$. Then*

$$\int_{\mathrm{USp}_{2g}(\mathbb{C})} f(U)\, d\mu_{\mathrm{Haar}}(U) = \int_0^\pi \cdots \int_0^\pi f(\theta_1, \ldots, \theta_g)\, d\mu_{\mathrm{USp}}(\theta_1, \ldots, \theta_g), \tag{4.4}$$

where

$$d\mu_{\mathrm{USp}}(\theta_1, \ldots, \theta_g) = \frac{2^{g^2}}{g!\pi^g} \prod_{1\leq m<n\leq g} (\cos\theta_n - \cos\theta_m)^2 \prod_{\ell=1}^{g} \sin^2\theta_\ell\, d\theta_1 \cdots d\theta_g. \tag{4.5}$$

Lemma 4.8. *Let B be an interval in $\mathbb{R}$. Then the boundary of the set*

$$\left\{U \in \mathrm{USp}_{2g}(\mathbb{C}) : \varphi(U) \in B\right\}$$

has Haar measure zero.

Proof. By differentiating (4.1), we have that

$$\varphi(U) = \varphi(\theta_1, \ldots, \theta_g) = \frac{1}{2^{g-1}} \sum_{j=1}^{g} \operatorname{cosec} \theta_j \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{|\cos \theta_k - \cos \theta_j|}. \tag{4.6}$$

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

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

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

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

have μ_{USp}-measure zero; furthermore, the function φ is continuous on

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

for each permutation σ of the set $\{1, \ldots, g\}$. It therefore suffices to show that for each $c \in \mathbb{R}$ and for each permutation σ of $\{1, \ldots, g\}$, the set

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

has μ_{USp}-measure zero. But in the region where $0 < \theta_{\sigma(1)} < \ldots < \theta_{\sigma(g)} < \pi$, the function $\varphi(\theta_1, \ldots, \theta_g)$ 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. □

Lemma 4.9. *For all $g \geq 1$, the function φ on $\mathrm{USp}_{2g}(\mathbb{C})$ is integrable and satisfies the bounds*

$$0 \leq \int_{\mathrm{USp}_{2g}(\mathbb{C})} \varphi(U)\, d\mu_{\mathrm{Haar}}(U) \leq \frac{2^{2g}}{\pi}.$$

This result follows from the following lemma in conjunction with the bound $0 \leq |\mathcal{Z}_U(\theta)| \leq 2^{2(g-1)}$ for all $U \in \mathrm{USp}_{2(g-1)}(\mathbb{C})$ and $\theta \in [0, \pi]$, which is found by applying the triangle inequality to (4.1).

Lemma 4.10 (Cha [5, §4])**.** *For $g = 1$, we have that*

$$\int_{\mathrm{USp}_2(\mathbb{C})} \varphi(U) \, d\mu_{\mathrm{Haar}}(U) = \frac{4}{\pi},$$

while for $g \geq 2$, we have the identity

$$\int_{\mathrm{USp}_{2g}(\mathbb{C})} \varphi(U) \, d\mu_{\mathrm{Haar}}(U) = \frac{2}{\pi} \int_0^{\pi} \sin\theta \int_{\mathrm{USp}_{2(g-1)}(\mathbb{C})} |\mathcal{Z}_U(\theta)| \, d\mu_{\mathrm{Haar}}(U) \, d\theta.$$

Proof. This is proved by Cha in [5, §4]; we include the details of the proof for later comparison. The $g = 1$ case is trivial, as in this case $\varphi(U) = \operatorname{cosec}\theta$, and hence by the Weyl integration formula,

$$\int_{\mathrm{USp}_2(\mathbb{C})} \varphi(U) \, d\mu_{\mathrm{Haar}}(U) = \frac{2}{\pi} \int_0^{\pi} \sin\theta \, d\theta = \frac{4}{\pi}.$$

We note that, strictly speaking, we require $\varphi(U)$ to be bounded to use the Weyl integration formula, but we may replace $\varphi(U)$ by $\varphi^T(U) = \min\{\varphi(U), T\}$ and then apply the monotone convergence theorem to obtain the above identity. For $g \geq 2$, the Weyl integration formula together with the expression (4.6) for $\varphi(U)$ gives

$$\begin{aligned} &\int_{\mathrm{USp}_{2g}(\mathbb{C})} \sum_{j=1}^{2g} \frac{1}{|\mathcal{Z}_U{}'(\theta_j)|} \, d\mu_{\mathrm{Haar}}(U) \\ &\quad = \frac{2^{g^2}}{g!\pi^g} \int_0^{\pi} \cdots \int_0^{\pi} \left(\frac{1}{2^{g-1}} \sum_{j=1}^{g} \operatorname{cosec}\theta_j \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{|\cos\theta_k - \cos\theta_j|} \right) \\ &\qquad \times \prod_{1 \leq m < n \leq g} (\cos\theta_n - \cos\theta_m)^2 \prod_{\ell=1}^{g} \sin^2\theta_\ell \, d\theta_1 \cdots d\theta_g. \end{aligned}$$

Now the expression in the brackets above is symmetric in the θ_n variables, so the summation on j may be replaced by g times a single summand, which we take to be θ_g. This allows us to rewrite the right-hand side as

$$\frac{2^{g^2-g+1}}{g!\pi^g} g \int_0^\pi \cdots \int_0^\pi \operatorname{cosec}\theta_g \prod_{k=1}^{g-1} \frac{1}{|\cos\theta_k - \cos\theta_g|}$$

$$\times \prod_{1\le m<n\le g} (\cos\theta_n - \cos\theta_m)^2 \prod_{\ell=1}^{g} \sin^2\theta_\ell \, d\theta_1 \cdots d\theta_g$$

$$= \frac{2}{\pi} \int_0^\pi \sin\theta_g \left(\frac{2^{(g-1)^2}}{(g-1)!\pi^{g-1}} \int_0^\pi \cdots \int_0^\pi 2^{g-1} \prod_{k=1}^{g-1} |\cos\theta_k - \cos\theta_g| \right.$$

$$\left. \times \prod_{1\le m<n\le g-1} (\cos\theta_n - \cos\theta_m)^2 \prod_{\ell=1}^{g-1} \sin^2\theta_\ell \, d\theta_1 \cdots d\theta_{g-1} \right) d\theta_g.$$

From (4.1), we have that

$$2^{g-1} \prod_{k=1}^{g-1} |\cos\theta_k - \cos\theta_g| = |\mathcal{Z}_U(\theta_g)|,$$

where U is an element of $\mathrm{USp}_{2(g-1)}(\mathbb{C})$ in the conjugacy class $(\theta_1, \ldots, \theta_{g-1})$. We therefore have by the Weyl integration formula that

$$\int_{\mathrm{USp}_{2g}(\mathbb{C})} \varphi(U)\, d\mu_{\mathrm{Haar}}(U) = \frac{2}{\pi} \int_0^\pi \sin\theta_g \int_{\mathrm{USp}_{2(g-1)}(\mathbb{C})} |\mathcal{Z}_U(\theta_g)|\, d\mu_{\mathrm{Haar}}(U)\, d\theta_g. \quad \square$$

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

$$\frac{\#\{C \in \mathcal{H}_{2g+1,q^n} : C \text{ satisfies the Mertens conjecture}\}}{\#\mathcal{H}_{2g+1,q^n}},$$

which may be thought of as a geometric average of the number of hyperelliptic curves in $\mathcal{H}_{2g+1,q^n}$ satisfying the Mertens conjecture. For brevity's sake, we write this average as

$$\frac{\#\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Mertens}\}}{\#\mathcal{H}_{2g+1,q^n}}.$$

Proposition 4.11. *We have that*

$$\lim_{n\to\infty} \frac{\#\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Mertens}\}}{\#\mathcal{H}_{2g+1,q^n}} = \mu_{\mathrm{Haar}}\left(\left\{U \in \mathrm{USp}_{2g}(\mathbb{C}) : \varphi(U) \le 1\right\}\right).$$

Proof. For any $\varepsilon > 0$, we may write

$$\#\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Mertens}\} = A_1 + A_2 + A_3 + A_4 + A_5 + A_6 + A_7,$$

where

$$
\begin{aligned}
A_1 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} : \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 1\right\}, \\
A_2 &= -\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{LI}^c : \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 1\right\}, \\
A_3 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{Mertens} \cap \mathrm{LI}^c\right\}, \\
A_4 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{LI} : B\left(C/\mathbb{F}_{q^n}\right) \le 1, 1 < \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 1+\varepsilon\right\}, \\
A_5 &= -\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{LI} : B\left(C/\mathbb{F}_{q^n}\right) > 1, 1-\varepsilon \le \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 1\right\}, \\
A_6 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{LI} : B\left(C/\mathbb{F}_{q^n}\right) \le 1, \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) > 1+\varepsilon\right\}, \\
A_7 &= -\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{LI} : B\left(C/\mathbb{F}_{q^n}\right) > 1, \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) < 1-\varepsilon\right\},
\end{aligned}
$$

By Deligne's equidistribution theorem,

$$\lim_{n\to\infty} \frac{A_1}{\#\mathcal{H}_{2g+1,q^n}} = \mu_{\mathrm{Haar}}(\varphi(U) \le 1),$$

while Theorem 4.4 implies that

$$\lim_{n\to\infty} \frac{A_2}{\#\mathcal{H}_{2g+1,q^n}} = \lim_{n\to\infty} \frac{A_3}{\#\mathcal{H}_{2g+1,q^n}} = 0.$$

Next, we note that

$$|A_4| + |A_5| \le \#\left\{C \in \mathcal{H}_{2g+1,q^n} : 1-\varepsilon \le \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 1+\varepsilon\right\},$$

and hence

$$\limsup_{n\to\infty} \frac{|A_4| + |A_5|}{\#\mathcal{H}_{2g+1,q^n}} \le \mu_{\mathrm{Haar}}(1-\varepsilon \le \varphi(U) \le 1+\varepsilon).$$

by Deligne's equidistribution theorem. Finally, Lemma 4.2 implies the existence of a constant $c(g) > 0$ such that

$$|A_6| + |A_7| \le \#\left\{C \in \mathcal{H}_{2g+1,q^n} : \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \ge \varepsilon c(g) q^{n/2}\right\}.$$

Lemma 4.10 shows that $\varphi(U)$ is integrable, which implies that for any $\varepsilon' > 0$ there exists some $T_0 > 0$ such that $\mu_{\mathrm{Haar}}\left(\varphi(U) \ge T\right) \le \varepsilon'$ for all $T \ge T_0$. Thus for any $\varepsilon' > 0$, we have by Deligne's equidistribution theorem that

$$
\begin{aligned}
\limsup_{n\to\infty} \frac{|A_6| + |A_7|}{\#\mathcal{H}_{2g+1,q^n}} &\le \limsup_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} : \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \ge \varepsilon c(g) q^{n/2}\right\}}{\#\mathcal{H}_{2g+1,q^n}} \\
&\le \lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} : \varphi\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \ge T\right\}}{\#\mathcal{H}_{2g+1,q^n}} \\
&= \mu_{\mathrm{Haar}}\left(\varphi(U) \ge T\right) \\
&\le \varepsilon'.
\end{aligned}
$$

As $\varepsilon' > 0$ was arbitrary,

$$\lim_{n\to\infty} \frac{A_6}{\#\mathcal{H}_{2g+1,q^n}} = \lim_{n\to\infty} \frac{A_7}{\#\mathcal{H}_{2g+1,q^n}} = 0.$$

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

$$\left| \lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \mathrm{Mertens}\right\}}{\#\mathcal{H}_{2g+1,q^n}} - \mu_{\mathrm{Haar}}\left(\varphi(U) \leq 1\right) \right| \\ \leq \mu_{\mathrm{Haar}}\left(1 - \varepsilon \leq \varphi(U) \leq 1 + \varepsilon\right).$$

As $\varepsilon > 0$ was arbitrary, and

$$\lim_{\varepsilon\to 0} \mu_{\mathrm{Haar}}\left(1 - \varepsilon \leq \varphi(U) \leq 1 + \varepsilon\right) = \mu_{\mathrm{Haar}}\left(\varphi(U) = 1\right) = 0,$$

we obtain the result. □

So in order to prove Theorem 1.8, we must show that $\mu_{\mathrm{Haar}}\left(\varphi(U) \leq 1\right) = 0$ for $1 \leq g \leq 2$. Here the minimum of φ can be determined explicitly, and in particular it can be shown that the set

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

is finite; this then implies the result via the Weyl integration formula, together with the fact that the measure μ_{USp} is atomless, with μ_{USp} as in (4.5). More precisely, for each permutation σ of the set $\{1, \ldots, g\}$, there is precisely one global minimum of φ in the region

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

with this minimum occurring at the critical point $\left(\widetilde{\theta}_{\sigma(1)}, \ldots, \widetilde{\theta}_{\sigma(g)}\right)$, where

$$\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) = \left(\frac{\pi}{2g}, \frac{3\pi}{2g}, \ldots, \frac{(2g-1)\pi}{2g}\right). \tag{4.7}$$

One can interpret this result via a geometric argument. If $z_1, \ldots, z_g$ are g 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 $g-1$ points and also to the complex conjugate of z_j. We can then think of φ as the sum over the inverse of this product for each starting point z_j. Intuitively, we would expect the product of chord lengths to be largest when averaged over the starting points when the g-tuple of points on the unit circle are evenly spaced while simultaneously being as far as possible from the points ± 1; consequently, we would expect φ to be smallest at this same g-tuple.

Proof of Theorem 1.8. For $g = 1$, we have from (4.6) that

$$\varphi(\theta_1) = \operatorname{cosec}\theta_1,$$

which is always at least 1, and is exactly 1 only at the point $\theta_1 = \pi/2$.

For $g = 2$,

$$\varphi(\theta_1, \theta_2) = \frac{1}{2}\frac{1}{|\cos\theta_1 - \cos\theta_2|}(\operatorname{cosec}\theta_1 + \operatorname{cosec}\theta_2)$$

so for this to be at most 1, we must have that

$$f(\theta_1, \theta_2) = 2|\cos\theta_1 - \cos\theta_2| - \operatorname{cosec}\theta_1 - \operatorname{cosec}\theta_2 \geq 0.$$

Now when $0 < \theta_1 < \theta_2 < \pi$, we have that

$$\begin{aligned}
\frac{\partial f}{\partial \theta_1} &= -2\sin\theta_1 + \operatorname{cosec}\theta_1 \cot\theta_1, \\
\frac{\partial f}{\partial \theta_2} &= 2\sin\theta_2 + \operatorname{cosec}\theta_2 \cot\theta_2.
\end{aligned}$$

We set both of these to zero, multiply through by $\sin^3\theta$ (with $\theta = \theta_1$ for the former and θ_2 for the latter), subtract $\cos\theta$, and then square both sides, finding that in both cases,

$$4x^6 + x^2 - 1 = \left(2x^2 - 1\right)\left(2x^4 + x^2 + 1\right) = 0,$$

where $x = \sin\theta$. As $0 < \theta < \pi$, this has only the solution $x = 1/\sqrt{2}$, or equivalently $\theta \in \{\pi/4, 3\pi/4\}$. So the only critical point of f in the region $0 < \theta_1 < \theta_2 < \pi$ occurs at $(\theta_1, \theta_2) = (\pi/4, 3\pi/4)$; we may easily confirm that $\partial f/\partial\theta_1 = \partial f/\partial\theta_2 = 0$ at this point, and also determine that $f(\pi/4, 3\pi/4) = 0$. So it remains to show that this is a local maximum of f. Indeed,

$$\begin{aligned}
\frac{\partial^2 f}{\partial \theta_1^2} &= -2\cos\theta_1 - \operatorname{cosec}\theta_1 \cot^2\theta_1 - \operatorname{cosec}^3\theta_1, \\
\frac{\partial f}{\partial \theta_2} &= 2\cos\theta_2 - \operatorname{cosec}\theta_2 \cot^2\theta_2 - \operatorname{cosec}^3\theta_2, \\
\frac{\partial^2 f}{\partial \theta_1 \partial \theta_2} &= \frac{\partial^2 f}{\partial \theta_2 \partial \theta_1} = 0,
\end{aligned}$$

and in particular, the Hessian matrix of second partial derivatives of f evaluated at $(\pi/4, 3\pi/4)$ is

$$\begin{pmatrix} -4\sqrt{2} & 0 \\ 0 & -2\sqrt{2} \end{pmatrix},$$

which is negative definite. So $(\pi/4, 3\pi/4)$ is a local maximum of f, and as f tends to negative infinity as either θ_1 or θ_2 tends to 0 or π, and $f(\theta_1, \theta_1) = -2 \operatorname{cosec} \theta_1 < 0$, the point $(\pi/4, 3\pi/4)$ is the unique global maximum of f on the set where $0 < \theta_1 < \theta_2 < \pi$. The same argument shows that the unique global maximum of f when $0 < \theta_2 < \theta_1 < \pi$ occurs at the point $(3\pi/4, \pi/4)$, with $f(3\pi/4, \pi/4) = 0$. Consequently, these are the only two points where $\varphi(\theta_1, \theta_2) \leq 1$. □

While we we can prove this result for $1 \leq g \leq 2$, we are in fact able to show that the critical point (4.7) is a local minimum of φ for every positive integer g; however, we are yet to be able to prove that this is also a global minimum. The proof is long, and so we dedicate the entirety of the next section to showing this result.

4.2 The Critical Point

We first demonstrate that $\varphi(\theta_1, \ldots, \theta_g) = 1$ at the critical point.

Lemma 4.12. *Let* $\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right)$ *be as in* (4.7)*. Then for each permutation* σ *of* $\{1, \ldots, g\}$*, we have that*

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

Proof. It suffices to prove this when σ is the identity, as φ is invariant under permutations of the variables. So by differentiating (4.1), we have that

$$\varphi(\theta_1, \ldots, \theta_g) = 2 \sum_{j=1}^{g} \frac{1}{|\mathcal{Z}_U{}'(\theta_j)|} = 2 \sum_{j=1}^{g} \varphi_j(\theta_1, \ldots, \theta_g),$$

where for each $1 \leq j \leq g$,

$$\begin{aligned} \varphi_j(\theta_1, \ldots, \theta_g) &= \frac{1}{|1 - e^{2i\theta_j}|} \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{|1 - e^{i(\theta_j - \theta_k)}|\,|1 - e^{i(\theta_j + \theta_k)}|} \\ &= \frac{1}{2^g} \operatorname{cosec} \theta_j \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{|\cos \theta_k - \cos \theta_j|}, \end{aligned} \tag{4.8}$$

so that

$$\begin{aligned} \varphi_j\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) &= \frac{1}{|1 - e^{2\pi i(2j-1)/(2g)}|} \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{|1 - e^{2\pi i(j-k)/(2g)}|\,|1 - e^{2\pi i(j+k-1)/(2g)}|} \\ &= \prod_{k=1}^{2g-1} \frac{1}{|1 - e^{2\pi i k/(2g)}|}, \end{aligned}$$

as for each j, the set $\{2j-1, j-k, j+k-1 : 1 \leq k \leq g,\ k \neq j\}$ forms a complete set of residues modulo $2g$ but for an element 0 modulo $2g$. Taking $x = 1$ in the identity

$$\sum_{j=0}^{2g-1} x^j = \prod_{k=1}^{2g-1} \left(x - e^{2\pi i k/(2g)}\right),$$

we find that for each $1 \leq j \leq g$,

$$\varphi_j\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) = \frac{1}{2g}, \tag{4.9}$$

which yields the result. $\square$

To confirm that the point $\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right)$ is indeed correctly identified as a critical point, we must next show that the derivative of φ vanishes at $\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right)$.

Lemma 4.13. *Let $\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right)$ be as in (4.7). Then for each permutation σ of $\{1, \ldots, g\}$, the derivative of φ vanishes at the point $\left(\widetilde{\theta}_{\sigma(1)}, \ldots, \widetilde{\theta}_{\sigma(g)}\right)$.*

Proof. Again, we need only prove this when σ is the identity. Upon differentiating (4.8), we have that for $1 \leq j, m \leq g$ with $j \neq m$,

$$\begin{aligned} \frac{\partial \varphi_j}{\partial \theta_m} &= \frac{\sin \theta_m}{\cos \theta_m - \cos \theta_j} \varphi_j \\ &= -\frac{1}{2}\left(\cot\left(\frac{\theta_m - \theta_j}{2}\right) + \cot\left(\frac{\theta_m + \theta_j}{2}\right)\right)\varphi_j, \end{aligned} \tag{4.10}$$

with $\varphi_j = \varphi_j(\theta_1, \ldots, \theta_g)$ as in (4.8); here the second equality follows from the sine angle-sum and cosine sum-to-product formulæ. If $j = m$, then

$$\frac{\partial \varphi_m}{\partial \theta_m} = -\frac{1}{2} \sum_{\substack{j=1 \\ j \neq m}}^{g} \left(\cot\left(\frac{\theta_m - \theta_j}{2}\right) + \cot\left(\frac{\theta_m + \theta_j}{2}\right)\right)\varphi_m - \cot \theta_m \varphi_m. \tag{4.11}$$

Letting $\theta_k = \widetilde{\theta}_k = (2k-1)\pi/(2g)$ for $1 \leq k \leq g$ and using (4.9), we find that for $j \neq m$,

$$\frac{\partial \varphi_j}{\partial \theta_m}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) = -\frac{1}{4g}\left(\cot\left(\frac{(m-j)\pi}{2g}\right) + \cot\left(\frac{(m+j-1)\pi}{2g}\right)\right), \tag{4.12}$$

while when $j = m$,

$$\begin{aligned} &\frac{\partial \varphi_m}{\partial \theta_m}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) \\ &= -\frac{1}{4g} \sum_{\substack{j=1 \\ j \neq m}}^{g} \left(\cot\left(\frac{(m-j)\pi}{2g}\right) + \cot\left(\frac{(m+j-1)\pi}{2g}\right)\right) - \frac{1}{2g}\cot\left(\frac{(2m-1)\pi}{2g}\right). \end{aligned}$$

Now the cotangent function has period π and is odd about the origin, and consequently

$$\begin{aligned}\sum_{\substack{j=1\\j\neq m}}^{g}\left(\cot\left(\frac{(m-j)\pi}{2g}\right)+\cot\left(\frac{(m+j-1)\pi}{2g}\right)\right) &= \sum_{\substack{j=1\\j\neq 2m-1}}^{2g-1}\cot\left(\frac{j\pi}{2g}\right)\\ &= -\cot\left(\frac{(2m-1)\pi}{2g}\right).\end{aligned} \tag{4.13}$$

So

$$\frac{\partial\varphi_m}{\partial\theta_m}\left(\widetilde{\theta}_1,\ldots,\widetilde{\theta}_g\right) = -\frac{1}{4g}\cot\left(\frac{(2m-1)\pi}{2g}\right), \tag{4.14}$$

while

$$\sum_{\substack{j=1\\j\neq m}}^{g}\frac{\partial\varphi_j}{\partial\theta_m}\left(\widetilde{\theta}_1,\ldots,\widetilde{\theta}_g\right) = \frac{1}{4g}\cot\left(\frac{(2m-1)\pi}{2g}\right).$$

We therefore find that for each $1\leq m\leq g$,

$$\frac{\partial\varphi}{\partial\theta_m}\left(\widetilde{\theta}_1,\ldots,\widetilde{\theta}_g\right) = 2\sum_{j=1}^{g}\frac{\partial\varphi_j}{\partial\theta_m}\left(\widetilde{\theta}_1,\ldots,\widetilde{\theta}_g\right) = 0,$$

as required. □

Next, we show that $\left(\widetilde{\theta}_1,\ldots,\widetilde{\theta}_g\right)$ is a local minimum of φ, by calculating the Hessian matrix of φ at $\left(\widetilde{\theta}_1,\ldots,\widetilde{\theta}_g\right)$ and proving it to be positive definite.

Lemma 4.14. *Let $\left(\widetilde{\theta}_1,\ldots,\widetilde{\theta}_g\right)$ be as in* (4.7)*. Then for each permutation σ of $\{1,\ldots,g\}$, the point $\left(\widetilde{\theta}_{\sigma(1)},\ldots,\widetilde{\theta}_{\sigma(g)}\right)$ is a local minimum of φ.*

Proof. Again, we need only take σ to be the identity. We first determine the mixed partial derivatives of φ. When $1\leq j,m,n\leq g$ with j,m,n distinct, we differentiate (4.10) to find that

$$\frac{\partial^2\varphi_j}{\partial\theta_n\partial\theta_m} = \frac{\partial^2\varphi_j}{\partial\theta_m\partial\theta_n} = -\frac{1}{2}\left(\cot\left(\frac{\theta_m-\theta_j}{2}\right)+\cot\left(\frac{\theta_m+\theta_j}{2}\right)\right)\frac{\partial\varphi_j}{\partial\theta_n},$$

while when $m\neq n$, differentiating (4.11) yields

$$\begin{aligned}\frac{\partial^2\varphi_m}{\partial\theta_n\partial\theta_m} = \frac{\partial^2\varphi_m}{\partial\theta_m\partial\theta_n} &= -\frac{1}{2}\left(\cot\left(\frac{\theta_n-\theta_m}{2}\right)+\cot\left(\frac{\theta_n+\theta_m}{2}\right)\right)\frac{\partial\varphi_m}{\partial\theta_m}\\ &\quad -\frac{1}{4}\left(\operatorname{cosec}^2\left(\frac{\theta_n-\theta_m}{2}\right)-\operatorname{cosec}^2\left(\frac{\theta_n+\theta_m}{2}\right)\right)\varphi_m.\end{aligned}$$

So taking $\theta_k = \widetilde{\theta}_k = (2k-1)\pi/(2g)$ for $1 \leq k \leq g$, we have by (4.12) that

$$\begin{aligned}\frac{\partial^2 \varphi_j}{\partial\theta_n \partial\theta_m}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) = \frac{1}{8g}&\left(\cot\left(\frac{(m-j)\pi}{2g}\right) + \cot\left(\frac{(m+j-1)\pi}{2g}\right)\right) \\ &\times\left(\cot\left(\frac{(n-j)\pi}{2g}\right) + \cot\left(\frac{(n+j-1)\pi}{2g}\right)\right).\end{aligned}$$

By expanding this product and using the cosine and sine angle-sum formulæ on each term, as well as the fact that the cotangent function is odd about the origin, we find that this is identical to

$$\begin{aligned}&\frac{1}{8g}\left(\cot\left(\frac{(m-n)\pi}{2g}\right) + \cot\left(\frac{(m+n-1)\pi}{2g}\right)\right) \\ &\qquad\times\left(\cot\left(\frac{(n-j)\pi}{2g}\right) + \cot\left(\frac{(n+j-1)\pi}{2g}\right)\right) \\ &\quad+\frac{1}{8g}\left(\cot\left(\frac{(n-m)\pi}{2g}\right) + \cot\left(\frac{(n+m-1)\pi}{2g}\right)\right) \\ &\qquad\times\left(\cot\left(\frac{(m-j)\pi}{2g}\right) + \cot\left(\frac{(m+j-1)\pi}{2g}\right)\right).\end{aligned}$$

Also, (4.14) and (4.9) show that

$$\begin{aligned}&\frac{\partial^2 \varphi_m}{\partial\theta_n \partial\theta_m}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) \\ &\quad= \frac{1}{8g}\left(\cot\left(\frac{(n-m)\pi}{2g}\right) + \cot\left(\frac{(n+m-1)\pi}{2g}\right)\right)\cot\left(\frac{(2m-1)\pi}{2g}\right) \\ &\qquad - \frac{1}{8g}\left(\operatorname{cosec}^2\left(\frac{(n-m)\pi}{2g}\right) - \operatorname{cosec}^2\left(\frac{(n+m-1)\pi}{2g}\right)\right).\end{aligned}$$

We therefore find that for $1 \leq m, n \leq g$ with $m \neq n$,

$$\begin{aligned}\frac{\partial^2 \varphi}{\partial\theta_n \partial\theta_m}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) &= 2\sum_{j=1}^{g}\frac{\partial^2 \varphi_j}{\partial\theta_n \partial\theta_m}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) \\ &= \frac{1}{2g}\left(\cot^2\left(\frac{(n-m)\pi}{2g}\right) - \cot^2\left(\frac{(n+m-1)\pi}{2g}\right)\right) \\ &\quad - \frac{1}{2g}\left(\operatorname{cosec}^2\left(\frac{(n-m)\pi}{2g}\right) - \operatorname{cosec}^2\left(\frac{(n+m-1)\pi}{2g}\right)\right) \\ &= 0,\end{aligned}$$

where we have used (4.13), the fact that the cotangent function is odd about the origin, and the Pythagorean trigonometric identity $\operatorname{cosec}^2\theta - \cot^2\theta = 1$.

When $1 \le j, m \le g$ with $j \ne m$, we also have by differentiating (4.10) that

$$\frac{\partial^2 \varphi_j}{\partial \theta_m^2} = -\frac{1}{2}\left(\cot\left(\frac{\theta_m - \theta_j}{2}\right) + \cot\left(\frac{\theta_m + \theta_j}{2}\right)\right)\frac{\partial \varphi_j}{\partial \theta_m} + \frac{1}{4}\left(\operatorname{cosec}^2\left(\frac{\theta_m - \theta_j}{2}\right) + \operatorname{cosec}^2\left(\frac{\theta_m + \theta_j}{2}\right)\right)\varphi_j,$$

while differentiating (4.11) shows that when $j = m$,

$$\frac{\partial^2 \varphi_m}{\partial \theta_m^2} = -\frac{1}{2}\sum_{\substack{j=1 \\ j \ne m}}^{g}\left(\cot\left(\frac{\theta_m - \theta_j}{2}\right) + \cot\left(\frac{\theta_m + \theta_j}{2}\right)\right)\frac{\partial \varphi_m}{\partial \theta_m} + \frac{1}{4}\sum_{\substack{j=1 \\ j \ne m}}^{g}\left(\operatorname{cosec}^2\left(\frac{\theta_m - \theta_j}{2}\right) + \operatorname{cosec}^2\left(\frac{\theta_m + \theta_j}{2}\right)\right)\varphi_m - \cot\theta_m \frac{\partial \varphi_m}{\partial \theta_m} + \operatorname{cosec}^2\theta_m \varphi_m.$$

So when $\theta_k = \widetilde{\theta}_k = (2k-1)\pi/(2g)$ for $1 \le k \le g$, we have by (4.12) and (4.9) that

$$\frac{\partial^2 \varphi_j}{\partial \theta_m^2}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) = \frac{1}{8g}\left(\cot\left(\frac{(m-j)\pi}{2g}\right) + \cot\left(\frac{(m+j-1)\pi}{2g}\right)\right)^2 + \frac{1}{8g}\left(\operatorname{cosec}^2\left(\frac{(m-j)\pi}{2g}\right) + \operatorname{cosec}^2\left(\frac{(m+j-1)\pi}{2g}\right)\right),$$

while (4.14), (4.13), and (4.9) imply that

$$\frac{\partial^2 \varphi_m}{\partial \theta_m^2}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) = \frac{1}{8g}\sum_{\substack{j=1 \\ j \ne m}}^{g}\left(\operatorname{cosec}^2\left(\frac{(m-j)\pi}{2g}\right) + \operatorname{cosec}^2\left(\frac{(m+j-1)\pi}{2g}\right)\right) + \frac{1}{8g}\cot^2\left(\frac{(2m-1)\pi}{2g}\right) + \frac{1}{2g}\operatorname{cosec}^2\left(\frac{(2m-1)\pi}{2g}\right).$$

Thus

$$\begin{aligned}\frac{\partial^2 \varphi}{\partial \theta_m^2}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) &= 2\sum_{j=1}^{g}\frac{\partial^2 \varphi_j}{\partial \theta_m^2}\left(\widetilde{\theta}_1, \ldots, \widetilde{\theta}_g\right) \\ &= \frac{1}{4g}\sum_{j=1}^{2g-1}\cot^2\left(\frac{j\pi}{2g}\right) + \frac{1}{2g}\sum_{j=1}^{2g-1}\operatorname{cosec}^2\left(\frac{j\pi}{2g}\right) \\ &\quad + \frac{1}{2g}\sum_{\substack{j=1 \\ j \ne m}}^{g}\cot\left(\frac{(m-j)\pi}{2g}\right)\cot\left(\frac{(m+j-1)\pi}{2g}\right) \\ &\quad + \frac{1}{2g}\operatorname{cosec}^2\left(\frac{(2m-1)\pi}{2g}\right),\end{aligned}$$

where we have used the fact that $\cot^2\theta$ and $\operatorname{cosec}^2\theta$ have period π. Now using the cosine and sine angle-sum formulæ, as well as (4.13), we determine that

$$\frac{1}{2g}\sum_{\substack{j=1\\j\neq m}}^{g}\cot\left(\frac{(m-j)\pi}{2g}\right)\cot\left(\frac{(m+j-1)\pi}{2g}\right)=\frac{1}{2}-\frac{1}{2g}-\frac{1}{2g}\cot^2\left(\frac{(2m-1)\pi}{2g}\right),$$

so our previous calculations simplify to

$$\frac{\partial^2\varphi}{\partial\theta_m^2}\left(\widetilde{\theta}_1,\dots,\widetilde{\theta}_g\right)=\frac{1}{4g}\sum_{j=1}^{2g-1}\cot^2\left(\frac{j\pi}{2g}\right)+\frac{1}{2g}\sum_{j=1}^{2g-1}\operatorname{cosec}^2\left(\frac{j\pi}{2g}\right)+\frac{1}{2},$$

where we have once again used the Pythagorean trigonometric identity.

So we have shown that the Hessian matrix of second partial derivatives of φ evaluated at $\left(\widetilde{\theta}_1,\dots,\widetilde{\theta}_g\right)$ is diagonal, and furthermore each diagonal entry is strictly positive. Thus this matrix is positive definite, and so $\left(\widetilde{\theta}_1,\dots,\widetilde{\theta}_g\right)$ is a local minimum of φ. □

This result does not preclude the possibility of the existence of other, possible smaller, local minima of φ. Brendan Harding (personal communication) has performed numerical calculations for small values of g to find other possible local minima of φ. Via the gradient descent method, he has searched for local minima of φ for each $1\leq g\leq 50$; his results have so far only indicated the existence of a local minimum at the critical point $\left(\widetilde{\theta}_1,\dots,\widetilde{\theta}_g\right)$ as in (4.7). Nevertheless, this does not eliminate the possibility of other such local minima, though it does seem extremely unlikely.

We must also mention that despite these results being formulated only for unitary symplectic matrices, they can easily be extended to hold for unitary matrices. Indeed, if U is an $N\times N$ unitary matrix, so that U has eigenvalues $e^{i\theta_1},\dots,e^{i\theta_N}$ with $-\pi\leq\theta_j\leq\pi$ for all $1\leq j\leq N$, then for real θ,

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

so that

$$\varphi(U)=\sum_{j=1}^{N}\frac{1}{|\mathcal{Z}_U{}'(\theta_j)|}=\sum_{j=1}^{N}\prod_{\substack{k=1\\k\neq j}}^{N}\frac{1}{\left|1-e^{i(\theta_k-\theta_j)}\right|}.$$

Then the same methods as in Lemmata 4.12, 4.13, and 4.14 show that any permutation σ and any one-dimensional translation ϕ modulo 2π of the critical point

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

is a local minimum of φ, with

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

Furthermore, we are led to conjecture that these points are precisely the global minima of φ. We recover our conjecture for unitary symplectic matrices by letting $N=2g$ and restricting ourselves to the subgroup of matrices for which $\theta_{j+g}=-\theta_j$ with $0\leq\theta_j\leq\pi$ for $1\leq j\leq g$.

4.3 Variants of the Mertens Conjecture

It is worth noting that there are variants of $M_{C/\mathbb{F}_q}(X)$ that can be studied. One can consider certain weights involved in the summatory function of the Möbius function. In the classical case, we may instead look at the properties of the weighted sum

$$M_\alpha(x)=\sum_{n\leq x}\frac{\mu(n)}{n^\alpha}$$

for $\alpha\in\mathbb{R}$. The function field analogue is

$$M_{C/\mathbb{F}_q,\alpha}(X)=\sum_{N=0}^{X-1}\frac{1}{q^{\alpha(N+1)}}\sum_{\deg(D)=N}\mu_{C/\mathbb{F}_q}(D),$$

and we may well ask whether the α-Mertens conjecture,

$$\limsup_{X\to\infty}\frac{\left|M_{C/\mathbb{F}_q,\alpha}(X)\right|}{q^{(1/2-\alpha)X}}\leq 1, \tag{4.15}$$

holds for the function field $C/\mathbb{F}_q$. For $\alpha>1$, this is easily resolved; (2.3) and (2.4) show that $M_{C/\mathbb{F}_q,\alpha}(X)$ converges to the infinite series

$$\frac{1}{q^\alpha}\sum_{N=0}^{\infty}\frac{1}{q^{\alpha N}}\sum_{\deg(D)=N}\mu_{C/\mathbb{F}_q}(D)=\frac{1}{q^\alpha Z_{C/\mathbb{F}_q}\left(q^{-\alpha}\right)}. \tag{4.16}$$

Though this series is only absolutely convergent for $|u|<q^{-1}$, one can show that it is also conditionally convergent for $|u|<q^{-1/2}$ due to the lack of poles of $1/Z_{C/\mathbb{F}_q}(u)$ inside this disc, and so $M_{C/\mathbb{F}_q,\alpha}(X)$ also converges to the quantity in (4.16) for $1/2<\alpha\leq 1$. For $\alpha<1/2$, on the other hand, a minor modification of the proof of Proposition 2.4, essentially involving dividing (2.9) by $q^{\alpha(N+1)}$ and summing over all $0\leq N\leq X-1$, shows that

$$\frac{M_{C/\mathbb{F}_q,\alpha}(X)}{q^{(1/2-\alpha)X}}=-\sum_{\gamma}\frac{1}{Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)}\frac{\gamma}{\gamma-q^\alpha}e^{i\theta(\gamma)X}+O_{q,g}\left(\frac{1}{q^{(1/2-\alpha)X}}\right)$$

provided $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes. A similarly simple modification of the proof of Lemma 4.2 then shows that if C satisfies LI, the quantity

$$B_\alpha(C/\mathbb{F}_q) = \limsup_{X\to\infty} \frac{\left|M_{C/\mathbb{F}_q,\alpha}(X)\right|}{q^{(1/2-\alpha)X}}$$

satisfies the asymptotic

$$B_\alpha(C/\mathbb{F}_q) = \varphi\left(\vartheta(C/\mathbb{F}_q)\right) + O_{g,\alpha}\left(\frac{1}{q^{1/2-\alpha}}\varphi\left(\vartheta(C/\mathbb{F}_q)\right)\right)$$

as q tends to infinity. So for $\alpha < 1/2$, the proof of Theorem 1.8 can be adapted essentially unchanged with the Mertens conjecture for the function field $C/\mathbb{F}_q$ replaced by (4.15). Thus for $\alpha < 1/2$, while any formulation of a local Mertens conjecture for $M_{C/\mathbb{F}_q,\alpha}(X)$ may differ to those involving $M_{C/\mathbb{F}_q}(X)$, a global Mertens conjecture would not.

For $\alpha = 1/2$, it is more prudent to analyse the the properties of the Möbius function more locally by merely studying the behaviour of

$$\frac{1}{q^{(N+1)/2}} \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D)$$

for each $N \geq 0$, rather than $M_{C/\mathbb{F}_q,1/2}(X)$, its average over $0 \leq N \leq X-1$. While this is not useful in the classical case, where this would simply be ascertaining $\mu(n)$ for each $n \geq 1$, the function field case is quite practical. From the proof of Proposition 2.4,

$$\frac{1}{q^{(N+1)/2}} \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D) = -\sum_{\gamma} \frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma^{-1}\right)} e^{i\theta(\gamma)(N+1)} + O_{q,g}\left(\frac{1}{q^{N/2}}\right),$$

and then a minor modification of the proof of Lemma 4.2 shows that the quantity

$$B_{1/2}(C/\mathbb{F}_q) = \limsup_{N\to\infty} \frac{1}{q^{(N+1)/2}} \left| \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D)\right|$$

satisfies

$$B_{1/2}(C/\mathbb{F}_q) = \varphi\left(\vartheta(C/\mathbb{F}_q)\right) + O_g\left(\frac{1}{\sqrt{q}}\varphi\left(\vartheta(C/\mathbb{F}_q)\right)\right)$$

as q tends to infinity, just as $B(C/\mathbb{F}_q)$ does so, and hence that Theorem 1.8 remains true with the Mertens conjecture for the function field $C/\mathbb{F}_q$ being replaced by the modified Mertens conjecture

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

A further variant follows from noting that while the classical Mertens conjecture states that the inequality

$$\frac{|M(x)|}{\sqrt{x}} \leq 1 \tag{4.17}$$

holds for all $x \geq 1$, the value 1 on the right-hand side above is, in some sense, not particularly special. Indeed, Stieltjes [27] claimed to have a proof that

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

without specifying an explicit constant, before later rescinding his claim, though he did postulate that (4.17) was true. Similarly, von Sterneck [26] conjectured that the stronger inequality

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

holds for all $x \geq 200$, based on calculations of $M(x)$ up to 5 000 000. In spite of these naïve conjectures, however, it seems most likely that

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

It is not difficult to prove this to be true should the Riemann hypothesis prove to be false, while Ingham [12] showed that this result also follows if one assumes the Riemann hypothesis and the Linear Independence hypothesis for the Riemann zeta function. Furthermore, the work of Ng [21] does not merely conditionally show that the set of counterexamples to the Mertens conjecture has strictly positive logarithmic density: the same can actually be said for the set $\{x \in [1,\infty) : |M(x)| > \beta\sqrt{x}\}$ for any $\beta > 0$.

One may very well then ask if the value 1 on the right-hand side of the Mertens conjecture in function fields,

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

is crucial in our analysis so far. We may instead consider the following generalisation of the Mertens conjecture in function fields: for $\beta > 0$, we say that the function field of a curve C over a finite field $\mathbb{F}_q$ satisfies the β-Mertens conjecture if

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

We can then study the average

$$\frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} : C \text{ satisfies the } \beta\text{-Mertens conjecture}\right\}}{\#\mathcal{H}_{2g+1,q^n}},$$

which we abbreviate to

$$\frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \beta\text{-Mertens}\right\}}{\#\mathcal{H}_{2g+1,q^n}}.$$

Theorem 4.15. *If $0 < \beta \leq 1$, and if $1 \leq g \leq 2$ is fixed, most hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ of genus g do not satisfy the β-Mertens conjecture for $C/\mathbb{F}_{q^n}$. If $\beta > 1$, then for any fixed $g \geq 1$,*

$$0 < \lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \beta\text{-Mertens}\right\}}{\#\mathcal{H}_{2g+1,q^n}} < 1. \tag{4.18}$$

Proof. A simple modification of the proof of Proposition 4.11 shows that

$$\lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \beta\text{-Mertens}\right\}}{\#\mathcal{H}_{2g+1,q^n}} = \mu_{\mathrm{Haar}}\left(\left\{U \in \mathrm{USp}_{2g}(\mathbb{C}) : \varphi(U) \leq \beta\right\}\right).$$

It is clear that this is nondecreasing in β, and so the proof of Theorem 1.8 implies that this is equal to zero for $0 < \beta \leq 1$ and $1 \leq g \leq 2$. To prove the inequalities (4.18) for $\beta > 1$, we recall from Lemma 4.12 that the equality $\varphi\left(\theta_1, \ldots, \theta_g\right) = 1$ is attained in the region $0 < \theta_1 < \ldots < \theta_g < 1$, and φ is real analytic and not uniformly constant in this region, and hence there exists an open neighbourhood of the point in this region where $1 \leq \varphi\left(\theta_1, \ldots, \theta_g\right) \leq \beta$. This open neighbourhood must have positive μ_{USp}-measure, as $d\mu_{\mathrm{USp}}\left(\theta_1, \ldots, \theta_g\right)$ does not vanish on open subsets of $[0, \pi]^g$. Consequently, $\mu_{\mathrm{Haar}}\left(\varphi(U) \leq \beta\right) > 0$. On the other hand, we must also have that $\mu_{\mathrm{Haar}}\left(\varphi(U) \leq \beta\right) < 1$, 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 $\varphi\left(\theta_1, \ldots, \theta_g\right) > \beta$ in this neighbourhood. □

The situation in function fields is therefore markedly different to the classical case. The work of Ng shows that in the classical case, the set of “local” counterexamples $x \in [1, \infty)$ to the β-Mertens conjecture $|M(x)| \leq \beta\sqrt{x}$ has positive logarithmic density for all $\beta > 0$. In the function field case, where we instead “globally” consider the proportion of curves for which the β-Mertens conjecture is true, the value $\beta = 1$ truly is the optimal value of β, in the sense that it is the largest such β for which most hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$, of genus $1 \leq g \leq 2$ do not satisfy the β-Mertens conjecture.

Chapter 5

Pólya's Conjecture in Function Fields

5.1 Pólya's Conjecture

The Liouville function $\lambda(n)$ is the arithmetic function that counts, modulo 2, the number of prime numbers dividing a positive integer, counting multiplicity. That is,

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ -1 & \text{if } n \text{ has an odd number of prime factors, counting multiplicity,} \\ 1 & \text{if } n \text{ has an even number of prime factors, counting multiplicity.} \end{cases}$$

In particular, the Liouville function agrees with the Möbius function on the squarefree positive integers. In 1919, Pólya [23] conjectured that the summatory function of the Liouville function,

$$L(x) = \sum_{n \leq x} \lambda(n),$$

satisfies the inequality

$$L(x) \leq 0 \tag{5.1}$$

for all $x \geq 2$; Pólya remarked in [23] that he had checked the validity of his conjecture up to $x = 1500$. Much like the Mertens conjecture, this conjecture implies that the Riemann hypothesis is true and that the Riemann zeta function has only simple zeroes. Pólya's conjecture also shared the same fate as the Mertens conjecture, in that it was proven to be false; it was disproved by Haselgrove [9] in 1958 using methods closely related to the work of Ingham [12]. The first counterexample was later shown to occur at $x = 906\,150\,257$ [28], and it is now known [3] that

$$\limsup_{x\to\infty} \frac{L(x)}{\sqrt{x}} > 0.062,$$
$$\liminf_{x\to\infty} \frac{L(x)}{\sqrt{x}} < -1.389.$$

It seems likely that

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

and this is known to follow from the assumption of the Linear Independence hypothesis for the Riemann zeta function [12].

In spite of these results, numerical evidence [3] suggests that regions for which the conjectured inequality (5.1) fails are distributed rather sparsely amongst the positive integers. Analogously to the Mertens conjecture, this can be explained heuristically through the following explicit expression for $L(x)$ in terms of a sum over the nontrivial zeroes ρ of the Riemann zeta function.

Proposition 5.1 (Fawaz [8], Humphries [11, Theorem 4.5]; cf. Proposition 1.1)**.** *Assume the Riemann hypothesis and the simplicity of the zeroes of $\zeta(s)$. Then there exists a sequence $\{T_v\}_{v=1}^{\infty}$ with $v \leq T_v \leq v+1$ such that for each positive integer v, for all $\varepsilon > 0$, and for x a positive noninteger,*

$$L(x) = \frac{\sqrt{x}}{\zeta(1/2)} + \sum_{|\gamma|<T_v} \frac{\zeta(2\rho)}{\zeta'(\rho)} \frac{x^{\rho}}{\rho} + 1 + O_{\varepsilon}\left(\frac{1}{\sqrt{x}} + \frac{x\log x}{T_v} + \frac{x}{T_v^{1-\varepsilon}\log x}\right).$$

In particular, for x a positive noninteger,

$$\frac{L(x)}{\sqrt{x}} = \frac{1}{\zeta(1/2)} + \sum_{\rho} \frac{\zeta(2\rho)}{\zeta'(\rho)} \frac{x^{i\gamma}}{\rho} + \frac{1}{\sqrt{x}} + O\left(\frac{1}{x}\right), \tag{5.2}$$

where the sum $\sum_{\rho}$ is interpreted in the sense $\lim_{v\to\infty} \sum_{|\gamma|<T_v}$. The leading term here is $1/\zeta(1/2) \approx -0.685$, which ought to lead to a negative bias of $L(x)$, but the sum over the zeroes of $\zeta(s)$ can be large enough for certain values of x to overcome this bias. However, for "most" x, this does not occur, and hence the inequality $L(x) \leq 0$ holds "most" of the time.

Once again, we can make this notion of "most" more rigorous by studying the logarithmic density $\delta(\mathcal{P}_{\lambda})$ of the set $\mathcal{P}_{\lambda} = \{x \in [1,\infty) : L(x) \leq 0\}$ of values where

Pólya's conjecture holds. We can guarantee the existence of this logarithmic density, and more, if in addition to the Riemann hypothesis we assume the Linear Independence hypothesis as well as a certain conjecture on the growth rate of $\zeta'(\rho)$ for each nontrivial zero ρ of $\zeta(s)$; that is, we assume that $\sum_{|\gamma|<T} |\zeta'(\rho)|^{-2} \ll T$ as T tends to infinity. We note that random matrix models suggest a more precise bound, namely that $\sum_{|\gamma|<T} |\zeta'(\rho)|^{-2} \sim 6T/\pi^3$; see [10].

Theorem 5.2 (Humphries [11, Theorem 5.1]; cf. [21], [25])**.** *Assume the Riemann hypothesis, the Linear Independence hypothesis, and that* $\sum_{|\gamma|<T} |\zeta'(\rho)|^{-2} \ll T$*. Then the function* $L(x)/\sqrt{x}$ *has a limiting logarithmic distribution. That is, there exists a probability measure* ν_λ *such that*

$$\lim_{X\to\infty} \frac{1}{\log X} \int\limits_{\left\{x\in[1,X]:L(x)/\sqrt{x}\in B\right\}} \frac{dx}{x} = \nu_\lambda(B)$$

for every Borel set $B \subset \mathbb{R}$ *whose boundary has Lebesgue measure zero. Furthermore, the median of* ν_λ *is* $1/\zeta(1/2)$.

The last point here yields an upper bound on the logarithmic density of $\mathcal{P}_\lambda$, while a method of Montgomery [18] also yields a lower bound.

Corollary 5.3 (Humphries [11, Theorem 1.5])**.** *Under the same assumptions as Theorem 5.2, we have the bounds*

$$1/2 \le \delta\left(\mathcal{P}_\lambda\right) < 1.$$

Richard Brent (personal communication) has subsequently performed calculations that suggest that the true value of this logarithmic density is

$$\delta\left(\mathcal{P}_\lambda\right) \approx 0.99988,$$

In any case, we may say that conditionally $L(x)$ does indeed have a bias towards being nonpositive, but that the set of counterexamples to Pólya's conjecture is not insignificant, in that it has positive, although very small, logarithmic density.

5.2 Pólya Conjectures in Function Fields

Here we formulate several function field analogues of Pólya's conjecture. We first define the Liouville function of a function field. For C a nonsingular projective curve over $\mathbb{F}_q$ of genus g and D an effective divisor of C, the Liouville function of $C/\mathbb{F}_q$ is given by

$$\lambda_{C/\mathbb{F}_q}(D) = \begin{cases} 1 & \text{if } D \text{ is the zero divisor,} \\ -1 & \text{if the sum of the orders of the prime divisors of } D \text{ is odd,} \\ 1 & \text{if the sum of the orders of the prime divisors of } D \text{ is even.} \end{cases}$$

We then study the summatory function of the Liouville function of $C/\mathbb{F}_q$,

$$L_{C/\mathbb{F}_q}(X) = \sum_{N=0}^{X-1} \sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D).$$

We wish to know whether there are biases in the behaviour of $L_{C/\mathbb{F}_q}(X)$. Like the classical case, we find that $L_{C/\mathbb{F}_q}(X)$ may have a bias towards being nonpositive.

Pólya's Conjecture in Function Fields. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus g, and let $L_{C/\mathbb{F}_q}(X)$ be the summatory function of the Liouville function of $C/\mathbb{F}_q$. Then*

$$\limsup_{X\to\infty} L_{C/\mathbb{F}_q}(X) \leq 0.$$

As with the Mertens conjecture, we may consider both local and global questions pertaining to Pólya's conjecture in function fields.

Question 5.4. *For which curves does Pólya's conjecture hold?*

Question 5.5. *Given a function field of a curve C over a finite field $\mathbb{F}_q$, how frequently does the inequality*

$$L_{C/\mathbb{F}_q}(X) \leq 0 \tag{5.3}$$

hold?

Question 5.6. *On average, in either the q or the g aspect, how often does Pólya's conjecture hold?*

The local questions are addressed in Chapter 6. In Section 6.1, we formulate certain conditions on the zeroes of $Z_{C/\mathbb{F}_q}(u)$ to ensure that Pólya's conjecture for $C/\mathbb{F}_q$ is true.

Theorem 5.7 (cf. Theorem 1.5). *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$. If $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes, then Pólya's conjecture for $C/\mathbb{F}_q$ is true provided*

$$-\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})}+\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} \leq -\sum_{\gamma}\left|\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|, \tag{5.4}$$

where $h_{C/\mathbb{F}_q}$ is the class number of the function field $C/\mathbb{F}_q$. Furthermore, if C satisfies LI, then the converse is also true: Pólya's conjecture for $C/\mathbb{F}_q$ is true only when (5.4) *holds.*

This does not entirely answer Question 5.4; it is possible that $C/\mathbb{F}_q$ is such that (5.4) does not hold but that Pólya's conjecture for $C/\mathbb{F}_q$ is true; in order for this to happen, $Z_{C/\mathbb{F}_q}(u)$ must only has simple zeroes but C must fail to satisfy LI.

We deal with Question 5.5 in Section 6.3, where we determine the natural density of the set of positive integers X for which (5.3) holds, provided that C satisfies LI.

Theorem 5.8 (cf. Theorem 1.6). *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$, and suppose that C satisfies LI. The natural density*

$$d(\mathcal{P}_{C/\mathbb{F}_q;\lambda}) = \lim_{Y\to\infty}\frac{1}{Y}\#\left\{1 \leq X \leq Y : L_{C/\mathbb{F}_q}(X) \leq 0\right\}$$

exists and satisfies

$$\begin{aligned} d(\mathcal{P}_{C/\mathbb{F}_q;\lambda}) &= 1/2 && \text{if } -\phi_1(C/\mathbb{F}_q)+\phi_2(C/\mathbb{F}_q) \geq \phi_3(C/\mathbb{F}_q), \\ 1/2 < d(\mathcal{P}_{C/\mathbb{F}_q;\lambda}) &< 1 && \text{if } -\phi_3(C/\mathbb{F}_q) < -\phi_1(C/\mathbb{F}_q)+\phi_2(C/\mathbb{F}_q) < \phi_3(C/\mathbb{F}_q), \\ d(\mathcal{P}_{C/\mathbb{F}_q;\lambda}) &= 1 && \text{if } -\phi_1(C/\mathbb{F}_q)+\phi_2(C/\mathbb{F}_q) \leq -\phi_3(C/\mathbb{F}_q), \end{aligned}$$

where

$$\begin{aligned} \phi_1(C/\mathbb{F}_q) &= \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})}, \\ \phi_2(C/\mathbb{F}_q) &= \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})}, \\ \phi_3(C/\mathbb{F}_q) &= \sum_{\gamma}\left|\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|. \end{aligned} \tag{5.5}$$

For Question 5.6, we study in Chapter 7 the average proportion of hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ satisfying Pólya's conjecture as the finite field $\mathbb{F}_q$ grows larger.

Much as we do with the Mertens conjecture, we are able to relate this average proportion to the Haar measure of the pullback of the region where a certain function of random matrices is nonnegative, which we are then able to calculate explicitly for low values of g. We find that most curves in this family do not satisfy Pólya's conjecture.

Theorem 5.9 (cf. Theorem 1.8)**.** *Fix $1 \leq g \leq 2$, and suppose that the characteristic of $\mathbb{F}_q$ is odd. Then as n tends to infinity, most hyperelliptic curves $C \in \mathcal{H}_{2g+1,q^n}$ do not satisfy Pólya's conjecture for $C/\mathbb{F}_{q^n}$.*

Chapter 6

Local Pólya Conjectures

6.1 An Explicit Expression for $L_{C/\mathbb{F}_q}(X)$

We obtain an explicit description for the summatory function of the Liouville function in function fields by studying the Dirichlet series

$$\sum_{D\geq 0} \frac{\lambda_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s},$$

which converges absolutely for $\Re(s) > 1$. As $\lambda_{C/\mathbb{F}_q}(D)$ is completely multiplicative and satisfies $\lambda(P) = -1$ for a prime divisor P of C, this has the Euler product expansion

$$\sum_{D\geq 0} \frac{\lambda_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \prod_P \frac{1}{1+\mathcal{N}P^{-s}}$$

for $\Re(s) > 1$, which upon comparing Euler products leads us to the identity

$$\sum_{D\geq 0} \frac{\lambda_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \frac{\zeta_{C/\mathbb{F}_q}(2s)}{\zeta_{C/\mathbb{F}_q}(s)}, \tag{6.1}$$

which is valid for all $\Re(s) > 1$. On the other hand, note that for $\Re(s) > 1$, we may rearrange this Dirichlet series instead to be of the form

$$\sum_{D\geq 0} \frac{\lambda_{C/\mathbb{F}_q}(D)}{\mathcal{N}D^s} = \sum_{D\geq 0} \frac{\lambda_{C/\mathbb{F}_q}(D)}{q^{\deg(D)s}} = \sum_{N=0}^{\infty} \frac{1}{q^{Ns}} \sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D). \tag{6.2}$$

We will determine an expression for the coefficients of the Dirichlet series for $\zeta_{C/\mathbb{F}_q}(2s)/\zeta_{C/\mathbb{F}_q}(s)$ using (2.1) and compare coefficients in order to find a formula for $L_{C/\mathbb{F}_q}(X) = \sum_{N=0}^{X-1} \sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D)$. Along the way, we will require the following lemma.

Lemma 6.1 ([24, Proposition 8.16]). *Let $\mathbb{F}_{q^2}$ be the quadratic field extension of $\mathbb{F}_q$, which is unique up to isomorphism, and let*

$$Z_{C/\mathbb{F}_{q^2}}(u) = \frac{P_{C/\mathbb{F}_{q^2}}(u)}{(1-u)(1-q^2u)}$$

be the zeta function of $C/\mathbb{F}_{q^2}$. Then for all $u \in \mathbb{C}$,

$$P_{C/\mathbb{F}_{q^2}}\left(u^2\right) = P_{C/\mathbb{F}_q}(u)P_{C/\mathbb{F}_q}(-u).$$

Consequently,

$$P_{C/\mathbb{F}_q}(-1) = \frac{h_{C/\mathbb{F}_{q^2}}}{h_{C/\mathbb{F}_q}},$$

where $h_{C/\mathbb{F}_q} = P_{C/\mathbb{F}_q}(1)$ is the class number of the function field $C/\mathbb{F}_q$.

Proposition 6.2 (cf. Proposition 2.4). *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 0$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. Then for each $N \geq 0$,*

$$\begin{aligned}\sum_{\deg(D)=N} & \lambda_{C/\mathbb{F}_q}(D) \\ = & -\frac{1}{2}\frac{\sqrt{q}-1}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(q^{-1/2}\right)}q^{(N+1)/2} - (-1)^{N+1}\frac{1}{2}\frac{\sqrt{q}+1}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(-q^{-1/2}\right)}q^{(N+1)/2} \\ & -\sum_{\gamma}\frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)}\gamma^{N+1} + (-1)^{N+1}\frac{q+1}{q-1}\frac{h_{C/\mathbb{F}_q}{}^2}{h_{C/\mathbb{F}_{q^2}}} + R(N,q,g,T), \quad (6.3)\end{aligned}$$

where the sum is over the inverse zeroes of $Z_{C/\mathbb{F}_q}(u)$, $T > 0$ is sufficiently small, and the error term $R(N,q,g,T)$ satisfies $R(N,q,g,T) = 0$ if $N \geq \max\{2g-1, 0\}$.

Proof. We let $\mathcal{C}_T = \{z \in \mathbb{C} : |z| = q^T\}$ for $T > 0$, and we study the contour integral

$$\frac{1}{2\pi i}\oint_{\mathcal{C}_T}\frac{1}{u^{N+1}}\frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)}\,du.$$

There are two different identities for $Z_{C/\mathbb{F}_q}\left(u^2\right)/Z_{C/\mathbb{F}_q}(u)$, obtainable from (6.1) and (2.1) and from (6.2), which give the identities

$$\frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)} = \frac{1-qu}{\left(1-\sqrt{q}u\right)\left(1+\sqrt{q}u\right)(1+u)}\prod_{j=1}^{2g}\frac{1-\gamma_j u^2}{1-\gamma_j u}, \quad (6.4)$$

$$\frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)} = \sum_{N=0}^{\infty}u^N\sum_{\deg(D)=N}\lambda_{C/\mathbb{F}_q}(D), \quad (6.5)$$

with the first identity valid for all $u \in \mathbb{C} \setminus \{\pm q^{-1/2}, -1, \gamma_1^{-1}, \ldots, \gamma_{2g}^{-1}\}$, and the second identity valid for all $|u| < q^{-1}$. If $Z_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right) \neq 0$, the singularities of the integrand inside $\mathcal{C}_T$ occur at $u = 0$, $u = -1$, $u = \pm q^{-1/2}$, and $u = \gamma^{-1}$ for each zero γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$; note that the assumption of the simplicity of the zeroes of $Z_{C/\mathbb{F}_q}(u)$ means that none of these zeroes can occur at $u = \pm q^{-1/2}$. At the singularity $u = 0$, we have by (6.5) that

$$\operatorname*{Res}_{u=0} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)} = \sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D).$$

At the singularity $u = -1$, (6.4) and Lemma 6.1 show that

$$\operatorname*{Res}_{u=-1} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)} = (-1)^N \frac{q+1}{q-1} \frac{P_{C/\mathbb{F}_q}(1)}{P_{C/\mathbb{F}_q}(-1)} = (-1)^N \frac{q+1}{q-1} \frac{{h_{C/\mathbb{F}_q}}^2}{h_{C/\mathbb{F}_{q^2}}}.$$

At the singularities $u = \pm q^{-1/2}$,

$$\begin{aligned}
&\operatorname*{Res}_{u=\pm q^{-1/2}} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)} \\
&\quad = \lim_{u \to \pm q^{-1/2}} \left(u \mp \frac{1}{\sqrt{q}}\right) \frac{1}{u^{N+1}} \frac{1 - qu}{\left(1 - \sqrt{q}u\right)\left(1 + \sqrt{q}u\right)(1+u)} \frac{P_{C/\mathbb{F}_q}\left(u^2\right)}{P_{C/\mathbb{F}_q}(u)} \\
&\quad = (\pm 1)^{N+1} \frac{1}{2} \frac{\sqrt{q} \mp 1}{\sqrt{q} \pm 1} \frac{q^{-g} h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right)} q^{(N+1)/2},
\end{aligned}$$

where we have used the fact that

$$P_{C/\mathbb{F}_q}\left(\frac{1}{q}\right) = q^{-g} P_{C/\mathbb{F}_q}(1) = q^{-g} h_{C/\mathbb{F}_q},$$

which follows from the functional equation (2.2) for $Z_{C/\mathbb{F}_q}(u)$. Finally, as $Z_{C/\mathbb{F}_q}(u)$ has a simple zero at each γ^{-1},

$$\operatorname*{Res}_{u=\gamma^{-1}} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)} = \frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{{Z_{C/\mathbb{F}_q}}'\left(\gamma^{-1}\right)} \gamma^{N+1}.$$

So by Cauchy's residue theorem,

$$\begin{aligned}
&\frac{1}{2\pi i} \oint_{\mathcal{C}_T} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}\left(u^2\right)}{Z_{C/\mathbb{F}_q}(u)}\, du \\
&= \frac{1}{2} \frac{\sqrt{q} - 1}{\sqrt{q} + 1} \frac{q^{-g} h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(q^{-1/2}\right)} q^{(N+1)/2} + (-1)^{N+1} \frac{1}{2} \frac{\sqrt{q} + 1}{\sqrt{q} - 1} \frac{q^{-g} h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(-q^{-1/2}\right)} q^{(N+1)/2} \\
&\quad + \sum_{\gamma} \frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{{Z_{C/\mathbb{F}_q}}'\left(\gamma^{-1}\right)} \gamma^{N+1} - (-1)^{N+1} \frac{q+1}{q-1} \frac{{h_{C/\mathbb{F}_q}}^2}{h_{C/\mathbb{F}_{q^2}}} + \sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D), \quad (6.6)
\end{aligned}$$

which yields (6.3), with

$$R(N,q,g,T) = \frac{1}{2\pi i}\oint_{\mathcal{C}_T} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}(u^2)}{Z_{C/\mathbb{F}_q}(u)}\, du.$$

By (6.4) and the fact that $|u| = q^T$ and $|\gamma_j| = \sqrt{q}$,

$$\begin{aligned} |R(N,q,g,T)| &\leq \frac{1}{2\pi}\oint_{\mathcal{C}_T} \left|\frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}(u^2)}{Z_{C/\mathbb{F}_q}(u)}\right| |du| \\ &\leq \frac{\left(q^{1+T}+1\right)\left(q^{1/2+2T}+1\right)^{2g}}{\left(q^T-1\right)\left(q^{1+2T}-1\right)\left(q^{1/2+T}-1\right)^{2g}} q^{-NT}. \end{aligned} \tag{6.7}$$

If $g \geq 1$ and $N = 2(g-1)$, then the right-hand side tends to one as T tends to infinity, while for all $g \geq 0$ and for all $N \geq \max\{2g-1, 0\}$, the right-hand side tends to zero as T tends to infinity. As the right-hand side of (6.6) is independent of T, we may take the limit as T tends to infinity on both sides, which implies that the left-hand side of (6.6) has absolute value at most than one if $g \geq 1$ and $N = 2(g-1)$, while for $N \geq \max\{2g-1, 0\}$ the left-hand side of (6.6) is equal to zero. □

We obtain an explicit expression for $L_{C/\mathbb{F}_q}(X)$ by summing (6.3) over all $0 \leq N \leq X-1$ and evaluating the resulting geometric progressions, which yields

$$\begin{aligned} L_{C/\mathbb{F}_q}(X) = &-\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} q^{X/2} - (-1)^X \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} q^{X/2} \\ &- \sum_{\gamma} \frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\gamma^X + R_X(q,g,T), \end{aligned} \tag{6.8}$$

where

$$\begin{aligned} R_X(q,g,T) = &\frac{q}{q-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} + \sum_{\gamma} \frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1} \\ &+ \frac{(-1)^X-1}{2}\frac{q+1}{q-1}\frac{h_{C/\mathbb{F}_q}{}^2}{h_{C/\mathbb{F}_{q^2}}} + \sum_{N=0}^{X-1} R(N,q,g,T). \end{aligned} \tag{6.9}$$

In particular, after fixing $T > 0$ we have that $R_X(q,g,T) = O_{q,g}(1)$ as X tends to infinity. The expression (6.8) suggests that $L_{C/\mathbb{F}_q}(X)$ grows at a rate comparable to $q^{X/2}$. Indeed, by using the fact that each simple inverse zero can be written in the form $\gamma = \sqrt{q}e^{i\theta(\gamma)}$ with $-\pi < \theta(\gamma) < \pi$, we can convert (6.8) into an asymptotic equation for $L_{C/\mathbb{F}_q}(X)/q^{X/2}$.

Corollary 6.3. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 0$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. Then as X tends to infinity,*

$$\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}} = -\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} - (-1)^X\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} - \sum_{\gamma}\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}e^{iX\theta(\gamma)} + O_{q,g}\left(\frac{1}{q^{X/2}}\right). \tag{6.10}$$

Recalling that $Z_{C/\mathbb{F}_q}(u) = \zeta_{C/\mathbb{F}_q}(s)$ with $u = q^{-s}$, we see that we can rewrite (6.10) as

$$\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}} = \frac{1}{2}\frac{q\left(\sqrt{q}+1\right)}{(q-1)^2}\frac{q^{-g}h_{C/\mathbb{F}_q}}{\zeta_{C/\mathbb{F}_q}(1/2)} - (-1)^X\frac{1}{2}\frac{q\left(\sqrt{q}-1\right)}{(q-1)^2}\frac{q^{-g}h_{C/\mathbb{F}_q}}{\zeta_{C/\mathbb{F}_q}(1/2+\pi i/\log q)} + \log q\sum_{\rho}\frac{\zeta_{C/\mathbb{F}_q}(2\rho)}{\zeta_{C/\mathbb{F}_q}{}'(\rho)}\frac{q^{iX\Im(\rho)}}{q^{\rho}-1} + O_{q,g}\left(\frac{1}{q^{X/2}}\right),$$

where the sum is over the $2g$ zeroes $\rho = 1/2 + i\Im(\rho)$ of $\zeta_{C/\mathbb{F}_q}(s)$ that lie in the range $-\pi/\log q < \Im(\rho) < \pi/\log q$. On the other hand, we have the explicit expression (5.2) for $L(x)/\sqrt{x}$:

$$\frac{L(x)}{\sqrt{x}} = \frac{1}{\zeta(1/2)} + \sum_{\rho}\frac{\zeta(2\rho)}{\zeta'(\rho)}\frac{x^{i\Im(\rho)}}{\rho} + O\left(\frac{1}{\sqrt{x}}\right).$$

We see many similarities between our explicit expressions (5.2) for $L(x)/\sqrt{x}$ and (6.10) for $L_{C/\mathbb{F}_q}(X)/q^{X/2}$, though several new features appear in the function field case, most notably additional leading terms. In the number field case, this is merely the reciprocal of the zeta function evaluated at the critical point $s = 1/2$. In the function field case, the leading term is no longer constant: here we have an additional critical point at $s = 1/2 + \pi i/\log q$, halfway up the critical line (recalling that $\zeta_{C/\mathbb{F}_q}(s)$ is periodic with period $2\pi i/\log q$), which leads to oscillations of $L_{C/\mathbb{F}_q}(X)/q^{X/2}$ according to whether X is even or odd. Finally, the coefficients of these leading terms are heavily dependent on the genus of C and on the size q of the finite field $\mathbb{F}_q$ over which C is defined.

We are interested in using the explicit expression (6.10) to study sign changes, or lack thereof, of $L_{C/\mathbb{F}_q}(X)$. To understand the behaviour of $L_{C/\mathbb{F}_q}(X)$ when the genus of the curve C is greater than zero, we must first determine the signs of three important quantities that appear in (6.3): the class number $h_{C/\mathbb{F}_q}$ and the values $P_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right)$.

Lemma 6.4 ([24, Proposition 5.11]). *For the class number $h_{C/\mathbb{F}_q}$ of the function field $C/\mathbb{F}_q$, we have the bounds*

$$(\sqrt{q}-1)^{2g} \leq h_{C/\mathbb{F}_q} \leq (\sqrt{q}+1)^{2g}.$$

In particular, $q^{-g}h_{C/\mathbb{F}_q}$ is always positive, and we have the asymptotic

$$q^{-g}h_{C/\mathbb{F}_q} = 1 + O_g\left(\frac{1}{\sqrt{q}}\right) \tag{6.11}$$

as q tends to infinity.

Next, we observe we can write $P_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right)$ explicitly in terms of the inverse zeroes $\gamma = \sqrt{q}e^{i\theta(\gamma)}$ of $Z_{C/\mathbb{F}_q}(u)$. Using the fact that the $2g$ inverse zeroes γ satisfy $\gamma_{j+g} = q\gamma_j^{-1}$ for $1 \leq j \leq g$, we see that

$$P_{C/\mathbb{F}_q}\left(\pm\frac{1}{\sqrt{q}}\right) = \prod_{j=1}^{g}\left(1 \mp \frac{\gamma_j}{\sqrt{q}}\right)\left(1 \mp \frac{\sqrt{q}}{\gamma_j}\right) = \prod_{j=1}^{g}\left(1 \mp e^{i\theta(\gamma_j)}\right)\left(1 \mp e^{-i\theta(\gamma_j)}\right).$$

From this, standard trigonometric identities allow us to show the following.

Lemma 6.5. *We have that*

$$P_{C/\mathbb{F}_q}\left(\frac{1}{\sqrt{q}}\right) = 2^g\prod_{j=1}^{g}(1-\cos\theta(\gamma_j)),$$
$$P_{C/\mathbb{F}_q}\left(-\frac{1}{\sqrt{q}}\right) = 2^g\prod_{j=1}^{g}(1+\cos\theta(\gamma_j)).$$

In particular, $P_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right)$ are both always nonnegative, and are strictly positive when $Z_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right) \neq 0$: that is, when $\pm\sqrt{q}$ are not inverse zeroes of $Z_{C/\mathbb{F}_q}(u)$.

So by using the triangle inequality on (6.10), we obtain the following bounds for $L_{C/\mathbb{F}_q}(X)/q^{X/2}$; in particular, we prove part of Theorem 5.7 in showing that if $Z_{C/\mathbb{F}_q}(u)$ has simple zeroes, then Pólya's conjecture for $C/\mathbb{F}_q$ is true when the inequality (5.4) holds.

Corollary 6.6. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. Let*

$$B^+(C/\mathbb{F}_q) = \limsup_{X\to\infty}\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}},$$
$$B^-(C/\mathbb{F}_q) = \liminf_{X\to\infty}\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}}.$$

Then we have the bounds

$$B^+(C/\mathbb{F}_q) \leq -\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} + \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} + \sum_{\gamma}\left|\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|,$$

$$B^-(C/\mathbb{F}_q) \geq -\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} - \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} - \sum_{\gamma}\left|\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|.$$

The assumption that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple implies that the bounds above are finite, that is, that $L_{C/\mathbb{F}_q}(X)/q^{X/2}$ is bounded. This highlights a notable difference in the behaviour of $L_{C/\mathbb{F}_q}(X)/q^{X/2}$ to that of $L(x)/\sqrt{x}$. While the former is bounded as X tends to infinity, the latter is conjectured to grow unboundedly in both the positive and negative directions as x tends to infinity. The key difference here is that the explicit expression (5.2) for $L(x)/\sqrt{x}$ involves an infinite sum over the zeroes of $\zeta(s)$, while for $L_{C/\mathbb{F}_q}(X)/q^{X/2}$ the analogous sum has only finitely many terms, as there only finitely many zeroes of $Z_{C/\mathbb{F}_q}(u)$.

Next, we show that the bounds in Corollary 6.6 are strict when C satisfies LI, from which it follows that when C satisfies LI, Pólya's conjecture for $C/\mathbb{F}_q$ is true if and only if the inequality (5.4) holds.

Theorem 6.7 (cf. Theorem 2.6)**.** *Suppose that C satisfies LI. Then*

$$B^+(C/\mathbb{F}_q) = -\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} + \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} + \sum_{\gamma}\left|\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|,$$

$$B^-(C/\mathbb{F}_q) = -\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} - \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} - \sum_{\gamma}\left|\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|.$$

Proof. We have that

$$\sum_{\gamma} \frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})} \frac{\gamma}{\gamma - 1} e^{iX\theta(\gamma)} = 2\Re\left(\sum_{j=1}^{g} \frac{Z_{C/\mathbb{F}_q}\left(\gamma_j^{-2}\right)}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)}\right),$$

so that

$$\begin{aligned}\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}} = &-\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} - (-1)^X \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} \\ &- 2\Re\left(\sum_{j=1}^{g} \frac{Z_{C/\mathbb{F}_q}\left(\gamma_j^{-2}\right)}{Z_{C/\mathbb{F}_q}{}'\left(\gamma_j^{-1}\right)} \frac{\gamma_j}{\gamma_j - 1} e^{iX\theta(\gamma_j)}\right) + O_{q,g}\left(\frac{1}{q^{X/2}}\right).\end{aligned}$$

The assumption that C satisfies LI along with the Kronecker–Weyl theorem inform us that the set

$$\left\{\left(e^{\pi i X}, e^{iX\theta(\gamma_1)}, \ldots, e^{iX\theta(\gamma_g)}\right) \in \mathbb{T}^{g+1} : X \in \mathbb{N}\right\}$$

is equidistributed in $\{\pm 1\} \times \mathbb{T}^g$. This implies the existence of a subsequence (X_m) of $\mathbb{N}$ such that

$$\begin{aligned}\lim_{m\to\infty} \frac{L_{C/\mathbb{F}_q}(X_m)}{q^{X_m/2}} = &-\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})} + \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} \\ &+ \sum_{\gamma}\left|\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\gamma}{\gamma-1}\right|,\end{aligned}$$

and hence the upper bound for $B^+(C/\mathbb{F}_q)$ is sharp. Similarly, a subsequence exists that ensures that the lower bound for $B^-(C/\mathbb{F}_q)$ is also sharp. □

We remark that we may also study the behaviour of $L_{C/\mathbb{F}_q}(X)$ when $Z_{C/\mathbb{F}_q}(u)$ has multiple zeroes, but that the situation is not so easily resolved as with $M_{C/\mathbb{F}_q}(X)$, as analysed in Section 2.2. The key difference is the behaviour of $L_{C/\mathbb{F}_q}(X)$ when $Z_{C/\mathbb{F}_q}(u)$ has a zero of multiple order at $u = q^{-1/2}$. If there is a zero elsewhere of higher order than the zero at $q^{-1/2}$, however, then one can mimic the proofs of Propositions 2.12 and 2.13 to show that $L_{C/\mathbb{F}_q}(X)$ changes sign infinitely often; we omit the details.

6.2 Examples in Low Genus

When $g = 0$, so that $C = \mathbb{P}^1$ and hence that $C/\mathbb{F}_q = \mathbb{F}_q(t)$, it is particularly easy to determine the limiting behaviour of $L_{C/\mathbb{F}_q}(X)$ via (6.8) and (6.9), as $h_{C/\mathbb{F}_q}, P_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right)$ are all equal to 1 and there are no inverse zeroes γ.

Proposition 6.8 (cf. Proposition 2.3)**.** *Let $g = 0$. Then*

$$L_{C/\mathbb{F}_q}(X) = \begin{cases} \dfrac{q^{(X+1)/2} - 1}{q-1} & \text{if } X \text{ is odd,} \\ -\dfrac{q^{X/2+1} - q}{q-1} & \text{if } X \text{ is even.} \end{cases} \tag{6.12}$$

Consequently, $L_{C/\mathbb{F}_q}(X)$ changes sign infinitely often, and

$$B^+(C/\mathbb{F}_q) = \frac{\sqrt{q}}{q-1},$$
$$B^-(C/\mathbb{F}_q) = -\frac{q}{q-1}.$$

In particular, Pólya's conjecture for $C/\mathbb{F}_q$ is false.

Alternatively, one can prove the identity (6.12) by noting that from (6.4) and (6.5), we have that for $|u| < q^{-1}$,

$$\begin{aligned} \sum_{N=0}^{\infty} u^N \sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D) &= \frac{(1-qu)}{(1+u)(1-qu^2)} \\ &= (1-qu) \sum_{A=0}^{\infty} (-1)^A u^A \sum_{B=0}^{\infty} q^B u^{2B} \\ &= \sum_{N=0}^{\infty} u^N \left(\sum_{\substack{A+B=N \\ B \text{ even}}} (-1)^A q^{B/2} - \sum_{\substack{A+B=N-1 \\ B \text{ even}}} (-1)^A q^{B/2+1} \right). \end{aligned}$$

Equating coefficients of u^N, we find that $\sum_{\deg(D)=0} \lambda_{C/\mathbb{F}_q}(D) = 1$, while for $N \geq 1$,

$$\sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D) = \begin{cases} \dfrac{2q^{N/2+1} - q - 1}{q-1} & \text{if } N \text{ is even,} \\ -\dfrac{q^{(N+3)/2} + q^{(N+1)/2} - q - 1}{q-1} & \text{if } N \text{ is odd.} \end{cases}$$

Summing over all $0 \leq N \leq X-1$ yields (6.12).

Similar results can be determined when $g = 1$, so that C is an elliptic curve over a finite field $\mathbb{F}_q$. When C satisfies LI, we have the following result.

Proposition 6.9. *Let C be an elliptic curve over $\mathbb{F}_q$, and suppose that C satisfies LI. Then*

$$B^+(C/\mathbb{F}_q) = -\frac{\sqrt{q}}{q-1} \frac{q+1-a}{4q-a^2}(a-2) + \frac{2}{4q-a^2} \sqrt{\frac{q+1-a}{q+1+a}} \sqrt{q^2+q+3aq-a^3},$$
$$B^-(C/\mathbb{F}_q) = -\frac{\sqrt{q}}{q-1} \frac{q+1-a}{4q-a^2}(2q-a) - \frac{2}{4q-a^2} \sqrt{\frac{q+1-a}{q+1+a}} \sqrt{q^2+q+3aq-a^3},$$

where a is the trace of the Frobenius endomorphism.

Proof. Using the fact that $P_{C/\mathbb{F}_q}(u) = 1 - au + qu^2$, so that $h_{C/\mathbb{F}_q} = q + 1 - a$ and $P_{C/\mathbb{F}_q}\left(\pm q^{-1/2}\right) = 2 \mp aq^{-1/2}$, we have that

$$-\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(q^{-1/2}\right)} + \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(-q^{-1/2}\right)} = -\frac{\sqrt{q}}{q-1}\frac{q+1-a}{4q-a^2}(a-2),$$
$$-\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(q^{-1/2}\right)} - \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(-q^{-1/2}\right)} = -\frac{\sqrt{q}}{q-1}\frac{q+1-a}{4q-a^2}(2q-a).$$

Next, the fact that $\gamma = \sqrt{q}e^{i\theta(\gamma)}$ implies that

$$\begin{aligned} Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right) &= \frac{\left(1-\gamma^{-1}\right)\left(1-\overline{\gamma}\gamma^{-2}\right)}{\left(1-\gamma^{-2}\right)\left(1-q\gamma^{-2}\right)} \\ &= \frac{\gamma^2-\overline{\gamma}}{\left(\gamma-\overline{\gamma}\right)\left(\gamma+1\right)} \\ &= \frac{q\cos 2\theta(\gamma) - \sqrt{q}\cos\theta(\gamma) + iq\sin 2\theta(\gamma) + i\sqrt{q}\sin\theta(\gamma)}{2i\sqrt{q}\sin\theta(\gamma)\left(\sqrt{q}\cos\theta(\gamma) + 1 + i\sqrt{q}\sin\theta(\gamma)\right)}. \end{aligned}$$

So by the Pythagorean trigonometric identity and the cosine angle-difference and triple-angle formulæ,

$$\begin{aligned} \left|Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)\right| &= \frac{1}{2\sqrt{q}\sin\theta(\gamma)}\sqrt{\frac{q^2+q+6q^{3/2}\cos\theta(\gamma) - 8q^{3/2}\cos^3\theta(\gamma)}{q+1+2\sqrt{q}\cos\theta(\gamma)}} \\ &= \sqrt{\frac{q^2+q+3aq-a^3}{\left(4q-a^2\right)\left(q+1+a\right)}}, \end{aligned}$$

as

$$\begin{aligned} 2\sqrt{q}\cos\theta(\gamma) &= a, \\ 2\sqrt{q}\sin\theta(\gamma) &= \sqrt{4q-a^2}. \end{aligned}$$

Finally, the proof of Proposition 3.3 shows that

$$2\left|\frac{1}{{Z_{C/\mathbb{F}_q}}'\left(\gamma^{-1}\right)}\frac{\gamma}{\gamma-1}\right| = 2\sqrt{\frac{q+1-a}{4q-a^2}},$$

and the result now follows from Theorem 6.7. $\square$

Via *Mathematica*, we have found that for q a prime power and a an integer satisfying $|a| < 2\sqrt{q}$, the function

$$-\frac{\sqrt{q}}{q-1}\frac{q+1-a}{4q-a^2}(a-2) + \frac{2}{4q-a^2}\sqrt{\frac{q+1-a}{q+1+a}}\sqrt{q^2+q+3aq-a^3}$$

is always positive; consequently, Pólya's conjecture is always false for $C/\mathbb{F}_q$ when the elliptic curve C satisfies LI.

In spite of this, when q is a perfect square, we are ensured an elliptic curve C over $\mathbb{F}_q$ for which Pólya's conjecture holds, via the curve whose trace of the Frobenius a is equal to $2\sqrt{q}$, so that $Z_{C/\mathbb{F}_q}(u)$ has a zero of order two at $u = q^{-1/2}$.

Proposition 6.10. *Let C be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p, and suppose that $Z_{C/\mathbb{F}_q}(u)$ has a zero of multiple order at $u = q^{-1/2}$, so that $q = p^m$ with $a = \pm 2\sqrt{q}$, where m is even. Then*

$$\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}} = -\frac{1}{4\sqrt{q}} \frac{\left(\sqrt{q}-1\right)^2}{\sqrt{q}+1} X^2 + O_q(X).$$

In particular, Pólya's conjecture holds for $C/\mathbb{F}_q$.

Proof. When $a = 2\sqrt{q}$, we have that $\gamma = \overline{\gamma} = \sqrt{q}$, and so the proof of Proposition 6.2 shows that for $N \geq 0$,

$$\begin{aligned}\sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D) = &- \operatorname*{Res}_{u=q^{-1/2}} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}(u^2)}{Z_{C/\mathbb{F}_q}(u)} + (-1)^N \frac{q-1}{8q} q^{(N+1)/2} \\ &- (-1)^N \frac{q+1}{q-1} \left(\frac{\sqrt{q}-1}{\sqrt{q}+1}\right)^2 + \frac{1}{2\pi i} \oint_{C_T} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}(u^2)}{Z_{C/\mathbb{F}_q}(u)} \, du,\end{aligned}$$

with the last term equal to zero for $N \geq 1$. Now by the binomial theorem,

$$\frac{1}{u^{N+1}} = q^{(N+1)/2} \sum_{k=0}^{\infty} (-1)^k \binom{N+k}{k} q^{k/2} \left(u - \frac{1}{\sqrt{q}}\right)^k,$$

whereas

$$\begin{aligned}\frac{Z_{C/\mathbb{F}_q}(u^2)}{Z_{C/\mathbb{F}_q}(u)} &= \frac{(1-qu)\left(1-\sqrt{q}u^2\right)^2}{(1+u)\left(1+\sqrt{q}u\right)\left(1-\sqrt{q}u\right)^3} \\ &= \frac{1}{2q^2} \frac{\left(\sqrt{q}-1\right)^3}{\sqrt{q}+1} \left(u - \frac{1}{\sqrt{q}}\right)^{-3} + O_q\left(\left(u - \frac{1}{\sqrt{q}}\right)^{-2}\right)\end{aligned}$$

in a neighbourhood of $u = q^{-1/2}$, and as for fixed k,

$$\binom{N+k}{k} = \frac{N^k}{k!} + O\left(N^{k-1}\right)$$

in the large N limit, we find via Laurent series about $u = q^{-1/2}$ that

$$\operatorname*{Res}_{u=q^{-1/2}} \frac{1}{u^{N+1}} \frac{Z_{C/\mathbb{F}_q}(u^2)}{Z_{C/\mathbb{F}_q}(u)} = \frac{1}{4q} \frac{\left(\sqrt{q}-1\right)^3}{\sqrt{q}+1} N^2 q^{(N+1)/2} + O_q\left(N q^{(N+1)/2}\right)$$

as N grows large. Thus

$$\sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D) = -\frac{1}{4q}\frac{\left(\sqrt{q}-1\right)^3}{\sqrt{q}+1}N^2 q^{(N+1)/2} + O_q\left(Nq^{(N+1)/2}\right),$$

and summing over all $0 \leq N \leq X-1$ and then dividing through by $q^{X/2}$ yields the result. $\square$

6.3 The Limiting Distribution of $L_{C/\mathbb{F}_q}(X)/q^{X/2}$

This section mimics Section 2.3 in determining the natural density of the set of natural numbers for which $L_{C/\mathbb{F}_q}(X) \leq 0$. From Corollary 6.3, for any nonsingular projective curve C over $\mathbb{F}_q$ of genus $g \geq 1$ we may write

$$\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}} = E_{C/\mathbb{F}_q;\lambda}(X) + \varepsilon_{C/\mathbb{F}_q;\lambda}(X),$$

where

$$\begin{aligned} E_{C/\mathbb{F}_q;\lambda}(X) &= -\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(q^{-1/2}\right)} - (-1)^X \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(-q^{-1/2}\right)} \\ &\qquad - \sum_{\gamma} \frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)}\frac{\gamma}{\gamma-1}e^{iX\theta(\gamma)}, \\ \varepsilon_{C/\mathbb{F}_q;\lambda}(X) &= O_{q,g}\left(\frac{1}{q^{X/2}}\right), \end{aligned}$$

provided that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. Using this, we may prove the existence of a limiting distribution of $L_{C/\mathbb{F}_q}(X)/q^{X/2}$ by first constructing the limiting distribution of $E_{C/\mathbb{F}_q;\lambda}(X)$.

Lemma 6.11 (cf. Lemma 2.15)**.** *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 1$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. There exists a probability measure $\nu_{C/\mathbb{F}_q;\lambda}$ on $\mathbb{R}$ that satisfies*

$$\lim_{Y\to\infty}\frac{1}{Y}\sum_{X=1}^{Y} f\left(E_{C/\mathbb{F}_q;\lambda}(X)\right) = \int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\lambda}(x)$$

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

Proof. The proof is essentially the same as that of Lemma 2.15, though notably the subtorus H is different. This time, we apply the Kronecker–Weyl theorem with $t_0 = \pi/2$, $t_j = \theta(\gamma_j)/2\pi$ for $1 \le j \le g$, in order to deduce the existence of a subtorus $H \subset \mathbb{T}^{g+1}$ satisfying

$$\lim_{Y\to\infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{\pi i X}, e^{iX\theta(\gamma_1)}, \ldots, e^{iX\theta(\gamma_g)}\right) = \int_H h(z)\, d\mu_H(z)$$

for every continuous function h on $\mathbb{T}^{g+1}$. We then define the probability measure $\nu_{C/\mathbb{F}_q;\lambda}$ on $\mathbb{R}$ by

$$\nu_{C/\mathbb{F}_q;\lambda}(B) = \mu_H(\widetilde{B})$$

for each Borel set $B \subset \mathbb{R}$, where

$$\widetilde{B} = \left\{ (z_0, z_1, \ldots, z_g) \in H : -\phi_1 - \phi_2 z_0 - 2\Re\left(\sum_{j=1}^{g} \phi_3^j z_j\right) \in B \right\}.$$

Here for brevity's sake $\phi_1 = \phi_1(C/\mathbb{F}_q)$ and $\phi_2 = \phi_2(C/\mathbb{F}_q)$ are as in (5.5), while for $1 \le j \le g$,

$$\phi_3^j = \phi_3^j(C/\mathbb{F}_q) = \frac{Z_{C/\mathbb{F}_q}(\gamma_j^{-2})}{{Z_{C/\mathbb{F}_q}}'(\gamma_j^{-1})} \frac{\gamma_j e^{i\theta(\gamma_j)}}{\gamma_j - 1}, \tag{6.13}$$

so that

$$\phi_3 = \phi_3(C/\mathbb{F}_q) = 2\sum_{j=1}^{g} \left|\phi_3^j\right|.$$

For f a bounded continuous function on $\mathbb{R}$, $h(z_0, z_1, \ldots, z_g)$ on $\mathbb{T}^{g+1}$ is defined by

$$h(z_0, z_1, \ldots, z_g) = f\left(-\phi_1 - \phi_2 z_0 - 2\Re\left(\sum_{j=1}^{g} \phi_3^j z_j\right)\right),$$

so that h is continuous on $\mathbb{T}^{g+1}$, and consequently

$$\begin{aligned}\int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\lambda}(x) &= \int_H h(z_0, z_1, \ldots, z_g)\, d\mu_H(z_0, z_1, \ldots, z_g) \\ &= \lim_{Y\to\infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{\pi i X}, e^{iX\theta(\gamma_1)}, \ldots, e^{iX\theta(\gamma_g)}\right) \\ &= \lim_{Y\to\infty} \frac{1}{Y} \sum_{X=1}^{Y} f\left(E_{C/\mathbb{F}_q;\lambda}(X)\right). \qquad \square\end{aligned}$$

The proof of the next result is essentially unchanged from the proof of Proposition 2.18.

Proposition 6.12 (cf. Proposition 2.18)**.** *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \ge 1$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are* *simple. The function $L_{C/\mathbb{F}_q}(X)/q^{X/2}$ has a limiting distribution $\nu_{C/\mathbb{F}_q;\lambda}$ on $\mathbb{R}$. That is, there exists a probability measure $\nu_{C/\mathbb{F}_q;\lambda}$ on $\mathbb{R}$ such that*

$$\lim_{Y\to\infty} \frac{1}{Y} \sum_{X=1}^{Y} f\left(\frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}}\right) = \int_{\mathbb{R}} f(x)\, d\nu_{C/\mathbb{F}_q;\lambda}(x)$$

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

We are now able to prove Theorem 5.8.

Proof of Theorem 5.8. The Portmanteau Theorem in conjunction with Proposition 6.12 implies that

$$\lim_{Y\to\infty} \frac{1}{Y} \# \left\{1 \leq X \leq Y : \frac{L_{C/\mathbb{F}_q}(X)}{q^{X/2}} \in B\right\} = \nu_{C/\mathbb{F}_q;\lambda}(B)$$

for every Borel set $B \subset \mathbb{R}$ whose boundary has $\nu_{C/\mathbb{F}_q;\lambda}$-measure zero, and hence $d(\mathcal{P}_{C/\mathbb{F}_q;\lambda})$ exists and is equal to $\nu_{C/\mathbb{F}_q;\lambda}((-\infty,0])$ if $\nu_{C/\mathbb{F}_q;\lambda}(\{0\}) = 0$. This follows as the assumption that C satisfies LI implies that $H = \{\pm 1\} \times \mathbb{T}^g$, that is, that H is the union of two disjoint subtori, and hence the normalised Haar measure on H is half the Lebesgue measure on each subtorus. Thus for a Borel set $B \subset \mathbb{R}$,

$$\begin{aligned}
\nu_{C/\mathbb{F}_q;\lambda}(B) &= \frac{1}{2} m\left(-\phi_1 - \phi_2 - 2\Re\left(\sum_{j=1}^{g} \phi_3^j e^{2\pi i\theta_j}\right) \in B\right) \\
&\quad + \frac{1}{2} m\left(-\phi_1 + \phi_2 - 2\Re\left(\sum_{j=1}^{g} \phi_3^j e^{2\pi i\theta_j}\right) \in B\right) \\
&= \frac{1}{2} m\left(-\phi_1 - \phi_2 - 2\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) \in B\right) \\
&\quad + \frac{1}{2} m\left(-\phi_1 + \phi_2 - 2\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) \in B\right).
\end{aligned}$$

The function $\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j)$ is real analytic on $[0,1]^g$ and not uniformly constant, so $m\left(\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) = c\right) = 0$ for all $c \in \mathbb{R}$, from which it follows that $\nu_{C/\mathbb{F}_q;\lambda}$ is atomless.

Finally, the fact that

$$m\left(\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) \geq c\right) = m\left(\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) \leq -c\right)$$

for any $c \in \mathbb{R}$ implies that

$$\begin{aligned} d(\mathcal{P}_{C/\mathbb{F}_q;\lambda}) &= \frac{1}{2} + \frac{1}{2} m\left(-\phi_1 - \phi_2 \leq 2\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) \leq \phi_1 - \phi_2 \right) \\ &= 1 - \frac{1}{2} m\left(2\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) < -\phi_1 - \phi_2 \right) \\ &\qquad\qquad - \frac{1}{2} m\left(2\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) < -\phi_1 + \phi_2 \right). \end{aligned}$$

From this, it is clear that

$$d(\mathcal{P}_{C/\mathbb{F}_q;\lambda}) = \begin{cases} 1/2 & \text{if } -\phi_1(C/\mathbb{F}_q) + \phi_2(C/\mathbb{F}_q) \geq \phi_3(C/\mathbb{F}_q), \\ 1 & \text{if } -\phi_1(C/\mathbb{F}_q) + \phi_2(C/\mathbb{F}_q) \leq -\phi_3(C/\mathbb{F}_q). \end{cases}$$

If $-\phi_3 < -\phi_1 + \phi_2 < \phi_3$, then there exists an open neighbourhood of $(0, \ldots, 0) \in [0,1]^g$ such that for all $(\theta_1, \ldots, \theta_g)$ in this neighbourhood,

$$|-\phi_1 + \phi_2| \leq 2\sum_{j=1}^{g} \left|\phi_3^j\right| \cos(2\pi\theta_j) \leq \phi_1 + \phi_2$$

and consequently $1/2 < d(\mathcal{P}_{C/\mathbb{F}_q;\lambda}) < 1$. □

Chapter 7

Global Pólya Conjectures

7.1 Averages over Families of Curves

We wish to find the average, as the finite field $\mathbb{F}_q$ grows larger, of the number of curves for which Pólya's conjecture is true. Our first step is determine expressions for $\phi_k(C/\mathbb{F}_q)$, $1 \leq k \leq 3$, in terms of $\mathcal{Z}_{\vartheta(C/\mathbb{F}_{q^n})}(\theta)$, the characteristic polynomial of $\vartheta(C/\mathbb{F}_{q^n}) \in \mathrm{USp}_{2g}(\mathbb{C})^{\#}$, in the large q limit. The resulting expressions involve particular functions related to $\mathcal{Z}_U(\theta)$; these are the functions

$$\begin{aligned}
\psi_1(U) &= \frac{1}{2}\frac{1}{\mathcal{Z}_U(0)}, \\
\psi_2(U) &= \frac{1}{2}\frac{1}{\mathcal{Z}_U(\pi)}, \\
\psi_3(U) &= \frac{1}{2}\sum_{j=1}^{2g}\frac{|\operatorname{cosec}\theta_j|}{|\mathcal{Z}_U{}'(\theta_j)|}.
\end{aligned}$$

We also define the functions

$$\psi_{\pm}(U) = -\psi_1(U) \pm \psi_2(U) \pm \psi_3(U).$$

Note that ψ_1, ψ_2, ψ_3 are always nonnegative, but that they can be infinite: $\psi_1(U)$ blows up if U has an eigenvalue equal to 1 (which is necessarily a repeated eigenvalue), while $\psi_2(U)$ blows up when U has an eigenvalue equal to -1 (which must also be a repeated eigenvalue), and $\psi_3(U)$ blows up whenever U has a repeated eigenvalue. Recall, however, that the set of matrices in $\mathrm{USp}_{2g}(\mathbb{C})$ with repeated eigenvalues has measure zero with respect to the normalised Haar measure on $\mathrm{USp}_{2g}(\mathbb{C})$.

Lemma 7.1 (cf. Lemma 4.2)**.** *Suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. Then for $1 \leq k \leq 3$,*

$$\phi_k(C/\mathbb{F}_q) = \psi_k\left(\vartheta(C/\mathbb{F}_q)\right) + O_g\left(\frac{1}{\sqrt{q}}\psi_k\left(\vartheta(C/\mathbb{F}_q)\right)\right).$$

Consequently,

$$B^+(C/\mathbb{F}_q) = \psi_+\left(\vartheta(C/\mathbb{F}_q)\right) + O_g\left(-\frac{1}{\sqrt{q}}\psi_-\left(\vartheta(C/\mathbb{F}_q)\right)\right).$$

Proof. From the definitions of $\phi_1(C/\mathbb{F}_q)$ and $\phi_2(C/\mathbb{F}_q)$ and from (4.2), we have that

$$\phi_1(C/\mathbb{F}_q) = \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}(0)},$$
$$\phi_2(C/\mathbb{F}_q) = \frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}(\pi)}.$$

The desired identities for $\phi_1(C/\mathbb{F}_q)$ and $\phi_2(C/\mathbb{F}_q)$ then follow from the asymptotic (6.11). For $\phi_3(C/\mathbb{F}_q)$, we have by (2.1), (4.2), and (4.3) that

$$\begin{aligned}\frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)}\frac{\gamma}{\gamma-1} &= \frac{P_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{P_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)}\frac{\overline{\gamma}-1}{\gamma^2-1}\frac{\gamma^3}{\overline{\gamma}-\gamma}\\ &= \frac{P_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))}\frac{\overline{\gamma}-1}{\gamma^2-1}\frac{i\gamma^2}{\gamma-\overline{\gamma}}.\end{aligned}$$

As $\gamma_j = \sqrt{q}e^{i\theta(\gamma_j)}$ for each $1 \leq j \leq 2g$, we may rewrite this as

$$\begin{aligned}&\frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)}\frac{\gamma}{\gamma-1}\\ &\quad= \frac{\prod_{j=1}^{2g}\left(1-q^{-1/2}e^{i(\theta(\gamma_j)-2\theta(\gamma))}\right)}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))}\frac{\sqrt{q}e^{-i\theta(\gamma)}-1}{qe^{2i\theta(\gamma)}-1}\frac{iqe^{2i\theta(\gamma)}}{\sqrt{q}e^{i\theta(\gamma)}-\sqrt{q}e^{-i\theta(\gamma)}}\\ &\quad= \frac{1}{2}\frac{e^{-i\theta(\gamma)}\operatorname{cosec}\theta(\gamma)}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))} + \frac{c}{\sqrt{q}}\frac{e^{-i\theta(\gamma)}\operatorname{cosec}\theta(\gamma)}{\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))}\end{aligned}$$

for some coefficient $c \in \mathbb{C}$ dependent on $q, g, \theta(\gamma), \theta(\gamma_1), \ldots, \theta(\gamma_g)$ and uniformly bounded in $q, \theta(\gamma), \theta(\gamma_1), \ldots, \theta(\gamma_g)$. This yields the asymptotic

$$\left|\frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{Z_{C/\mathbb{F}_q}{}'\left(\gamma^{-1}\right)}\frac{\gamma}{\gamma-1}\right| = \frac{1}{2}\frac{|\operatorname{cosec}\theta(\gamma)|}{|\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))|} + O_g\left(\frac{1}{\sqrt{q}}\frac{|\operatorname{cosec}\theta(\gamma)|}{|\mathcal{Z}_{\vartheta(C/\mathbb{F}_q)}{}'(\theta(\gamma))|}\right),$$

and by summing over all inverse zeroes γ, we obtain the desired identity for $\phi_3(C/\mathbb{F}_q)$. □

Lemma 7.2 (cf. Lemma 4.8)**.** *Let B be an interval in $\mathbb{R}$. Then the boundaries of the sets*

$$\left\{U \in \mathrm{USp}_{2g}(\mathbb{C}) : \psi_\pm(U) \in B\right\}$$

have Haar measure zero.

Proof. By (4.1), we have that

$$\begin{aligned}\psi_\pm(\theta_1, \ldots, \theta_g) = -\frac{1}{2^{g+1}} \prod_{j=1}^{g} \frac{1}{(1-\cos\theta_j)} \pm \frac{1}{2^{g+1}} \prod_{j=1}^{g} \frac{1}{(1+\cos\theta_j)} \\ \pm \frac{1}{2^g} \sum_{j=1}^{g} \operatorname{cosec}^2 \theta_j \prod_{\substack{k=1 \\ k\neq j}}^{g} \frac{1}{|\cos\theta_k - \cos\theta_j|}.\end{aligned}$$

It suffices to show that for each permutation σ of $\{1, \ldots, g\}$ and for each $c \in \mathbb{R}$, the sets

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

have Lebesgue measure zero, and this is true as when $0 < \theta_1 < \ldots < \theta_g < \pi$, the functions $\psi_\pm(\theta_{\sigma(1)}, \ldots, \theta_{\sigma(g)})$ are real analytic and non-uniformly constant. □

Lemma 7.3 (cf. Lemma 4.9)**.** *For all $g \geq 1$, the function ψ_- on $\mathrm{USp}_{2g}(\mathbb{C})$ is integrable and satisfies the bounds*

$$-1 - 2^{2(g-1)} \leq \int_{\mathrm{USp}_{2g}(\mathbb{C})} \psi_-(U)\, d\mu_{\mathrm{Haar}}(U) \leq -1.$$

The proof of this result follows from the following two lemmata, together with the bound $0 \leq |\mathcal{Z}_U(\theta)| \leq 2^{2(g-1)}$ for all $U \in \mathrm{USp}_{2(g-1)}(\mathbb{C})$ and $\theta \in [0,\pi]$.

Lemma 7.4 (Keating–Snaith [14])**.** *We have the identities*

$$\int_{\mathrm{USp}_{2g}(\mathbb{C})} \psi_1(U)\, d\mu_{\mathrm{Haar}}(U) = \int_{\mathrm{USp}_{2g}(\mathbb{C})} \psi_2(U)\, d\mu_{\mathrm{Haar}}(U) = \frac{1}{2}.$$

Proof. Keating and Snaith show that [14, §2.1 Equation (10)]

$$\int_{\mathrm{USp}_{2g}(\mathbb{C})} \frac{1}{\mathcal{Z}_U(0)}\, d\mu_{\mathrm{Haar}}(U) = 1.$$

The Haar measure is invariant under left multiplication by matrices $V \in \mathrm{USp}_{2g}(\mathbb{C})$, so by taking $V = -I$, so that $\mathcal{Z}_{VU}(0) = \det(I+U) = \mathcal{Z}_U(\pi)$, we find that

$$\int_{\mathrm{USp}_{2g}(\mathbb{C})} \frac{1}{\mathcal{Z}_U(\pi)}\, d\mu_{\mathrm{Haar}}(U) = \int_{\mathrm{USp}_{2g}(\mathbb{C})} \frac{1}{\mathcal{Z}_U(0)}\, d\mu_{\mathrm{Haar}}(U) = 1. \qquad \square$$

Lemma 7.5 (cf. Lemma 4.10)**.** *For $g = 1$, we have that*

$$\int_{\mathrm{USp}_2(\mathbb{C})} \psi_3(U)\, d\mu_{\mathrm{Haar}}(U) = 1,$$

while for $g \geq 2$, we have the identity

$$\int_{\mathrm{USp}_{2g}(\mathbb{C})} \psi_3(U)\, d\mu_{\mathrm{Haar}}(U) = \frac{1}{\pi} \int_0^{\pi} \int_{\mathrm{USp}_{2(g-1)}(\mathbb{C})} |\mathcal{Z}_U(\theta)|\; d\mu_{\mathrm{Haar}}(U)\, d\theta.$$

Proof. The $g = 1$ case is trivial. For $g \geq 2$, we differentiate (4.1) in order to find that

$$\frac{1}{2} \sum_{j=1}^{2g} \frac{|\operatorname{cosec} \theta_j|}{|\mathcal{Z}_U{}'(\theta_j)|} = \frac{1}{2^g} \sum_{j=1}^{g} \operatorname{cosec}^2 \theta_j \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{|\cos \theta_k - \cos \theta_j|}.$$

By the Weyl integration formula,

$$\begin{aligned} &\frac{1}{2} \int_{\mathrm{USp}_{2g}(\mathbb{C})} \sum_{j=1}^{2g} \frac{|\operatorname{cosec} \theta_j|}{|\mathcal{Z}_U{}'(\theta_j)|}\, d\mu_{\mathrm{Haar}}(U) \\ &\qquad = \frac{2^{g^2}}{g!\pi^g} \int_0^{\pi} \cdots \int_0^{\pi} \left(\frac{1}{2^g} \sum_{j=1}^{g} \operatorname{cosec}^2 \theta_j \prod_{\substack{k=1 \\ k \neq j}}^{g} \frac{1}{|\cos \theta_k - \cos \theta_j|} \right) \\ &\qquad\qquad \times \prod_{1 \leq m < n \leq g} (\cos \theta_n - \cos \theta_m)^2 \prod_{\ell=1}^{g} \sin^2 \theta_\ell \, d\theta_1 \cdots d\theta_g, \end{aligned}$$

and by the symmetry in the θ_j variables, this is the same as

$$\begin{aligned} &\frac{2^{g(g-1)}}{g!\pi^g} g \int_0^{\pi} \cdots \int_0^{\pi} \operatorname{cosec}^2 \theta_g \prod_{k=1}^{g-1} \frac{1}{|\cos \theta_k - \cos \theta_g|} \\ &\qquad \times \prod_{1 \leq m < n \leq g} (\cos \theta_n - \cos \theta_m)^2 \prod_{\ell=1}^{g} \sin^2 \theta_\ell \, d\theta_1 \cdots d\theta_g \\ &\quad = \frac{1}{\pi} \int_0^{\pi} \left(\frac{2^{(g-1)^2}}{(g-1)!\pi^{g-1}} \int_0^{\pi} \cdots \int_0^{\pi} 2^{g-1} \prod_{k=1}^{g-1} |\cos \theta_k - \cos \theta_g| \right. \\ &\qquad \left. \times \prod_{1 \leq m < n \leq g-1} (\cos \theta_n - \cos \theta_m)^2 \prod_{\ell=1}^{g-1} \sin^2 \theta_\ell \, d\theta_1 \cdots d\theta_{g-1} \right) d\theta_g. \end{aligned}$$

The result then follows via the Weyl integration formula □

We now study the limit as n tends to infinity of the average

$$\frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} : C \text{ satisfies Pólya's Conjecture}\right\}}{\#\mathcal{H}_{2g+1,q^n}},$$

which we write as
$$\frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Pólya}\right\}}{\#\mathcal{H}_{2g+1,q^n}}.$$

Proposition 7.6 (cf. Proposition 4.11)**.** *We have that*
$$\lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Pólya}\right\}}{\#\mathcal{H}_{2g+1,q^n}} = \mu_{\text{Haar}}\left(\psi_+(U) \le 0\right).$$

Proof. For any $\varepsilon > 0$, we may write
$$\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Pólya}\right\} = A_1 + A_2 + A_3 + A_4 + A_5 + A_6 + A_7,$$
where
$$\begin{aligned}
A_1 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} : \psi_+\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 0\right\},\\
A_2 &= -\#\left\{C \in \mathcal{H}_{2g+1,q^n} \setminus \text{LI} : \psi_+\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 0\right\},\\
A_3 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Pólya} \setminus \text{LI}\right\},\\
A_4 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{LI} : B^+\left(C/\mathbb{F}_{q^n}\right) \le 0, 0 < \psi_+\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le \varepsilon\right\},\\
A_5 &= -\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{LI} : B^+\left(C/\mathbb{F}_{q^n}\right) > 0, -\varepsilon \le \psi_+\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le 0\right\},\\
A_6 &= \#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{LI} : B^+\left(C/\mathbb{F}_{q^n}\right) \le 0, \psi_+\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) > \varepsilon\right\},\\
A_7 &= -\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{LI} : B^+\left(C/\mathbb{F}_{q^n}\right) > 0, \psi_+\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) < -\varepsilon\right\}.
\end{aligned}$$

Then we have that
$$\begin{aligned}
\lim_{n\to\infty} \frac{A_1}{\#\mathcal{H}_{2g+1,q^n}} &= \mu_{\text{Haar}}(\psi_+(U) \le 0),\\
\lim_{n\to\infty} \frac{A_2}{\#\mathcal{H}_{2g+1,q^n}} &= \lim_{n\to\infty} \frac{A_3}{\#\mathcal{H}_{2g+1,q^n}} = 0.
\end{aligned}$$

Furthermore,
$$\begin{aligned}
\limsup_{n\to\infty} \frac{|A_4| + |A_5|}{\#\mathcal{H}_{2g+1,q^n}} &\le \lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} : -\varepsilon \le \psi_+\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \le \varepsilon\right\}}{\#\mathcal{H}_{2g+1,q^n}}\\
&= \mu_{\text{Haar}}(-\varepsilon \le \psi_+(U) \le \varepsilon).
\end{aligned}$$

Finally, Lemma 7.1 implies the existence of a constant $c(g) > 0$ such that
$$|A_6| + |A_7| \le \#\left\{C \in \mathcal{H}_{2g+1,q^n} : -\psi_-\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \ge \varepsilon c(g) q^{n/2}\right\}.$$

As ψ_- is integrable by Lemma 7.3, for any $\varepsilon' > 0$ there exists some $T_0 > 0$ such that $\mu_{\text{Haar}}\left(-\psi_-(U) \ge T\right) \le \varepsilon'$ for all $T > T_0$, and hence
$$\begin{aligned}
\limsup_{n\to\infty} \frac{|A_6| + |A_7|}{\#\mathcal{H}_{2g+1,q^n}} &\le \lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} : -\psi_-\left(\vartheta\left(C/\mathbb{F}_{q^n}\right)\right) \ge T\right\}}{\#\mathcal{H}_{2g+1,q^n}}\\
&= \mu_{\text{Haar}}\left(-\psi_-(U) \ge T\right)\\
&\le \varepsilon'.
\end{aligned}$$

As $\varepsilon' > 0$ was arbitrary,

$$\lim_{n\to\infty} \frac{A_6}{\#\mathcal{H}_{2g+1,q^n}} = \lim_{n\to\infty} \frac{A_7}{\#\mathcal{H}_{2g+1,q^n}} = 0.$$

Thus for any $\varepsilon > 0$,

$$\left| \lim_{n\to\infty} \frac{\#\left\{C \in \mathcal{H}_{2g+1,q^n} \cap \text{Pólya}\right\}}{\#\mathcal{H}_{2g+1,q^n}} - \mu_{\text{Haar}}\left(\psi_+(U) \leq 0\right) \right| \\ \leq \mu_{\text{Haar}}\left(-\varepsilon \leq \psi_+(U) \leq \varepsilon\right),$$

which yields the result because

$$\lim_{\varepsilon\to 0} \mu_{\text{Haar}}\left(-\varepsilon \leq \psi_+(U) \leq \varepsilon\right) = \mu_{\text{Haar}}\left(\psi_+(U) = 0\right) = 0. \qquad \square$$

Proof of Theorem 5.9. We must show that $\mu_{\text{Haar}}\left(\psi_+(U) \leq 0\right) = 0$. By making the change of variables $\cos\theta_j \mapsto x_j$, this is equivalent to showing that the set of $(x_1, \ldots, x_g) \in [-1,1]^g$ for which the function

$$\widetilde{\psi}_+(x_1, \ldots, x_g) \\ = -\frac{1}{2^{g+1}} \prod_{j=1}^{g} \frac{1}{(1-x_j)} + \frac{1}{2^{g+1}} \prod_{j=1}^{g} \frac{1}{(1+x_j)} + \frac{1}{2^g} \sum_{j=1}^{g} \frac{1}{1-x_j^2} \prod_{\substack{k=1 \\ k\neq j}}^{g} \frac{1}{|x_k - x_j|}$$

is nonpositive has measure zero with respect to the measure

$$d\widetilde{\mu}_{\text{USp}}(x_1, \ldots, x_g) = \frac{2^{g^2}}{g!\pi^g} \prod_{1\leq j<k\leq g} (x_k - x_j)^2 \prod_{\ell=1}^{g} \sqrt{1-x_\ell^2}\, dx_1 \cdots dx_g$$

on $[-1,1]^g$. Now we may write $\widetilde{\psi}_+ = f/h$, with

$$f(x_1, \ldots, x_g) = -\prod_{j=1}^{g} (1-x_j) \prod_{1\leq k<\ell\leq g} |x_\ell - x_k| + \prod_{j=1}^{g} (1+x_j) \prod_{1\leq k<\ell\leq g} |x_\ell - x_k| \\ + 2\sum_{j=1}^{g} \prod_{\substack{k=1 \\ k\neq j}}^{g} (1-x_k^2) \prod_{\substack{1\leq \ell<m\leq g \\ \ell,m\neq j}} |x_m - x_\ell|,$$

$$h(x_1, \ldots, x_g) = 2^{g+1} \prod_{j=1}^{g} (1-x_j^2) \prod_{1\leq k<\ell\leq g} |x_\ell - x_k|.$$

Note that h is positive on $[-1,1]^g$ outside the $\widetilde{\mu}_{\text{USp}}$-measure zero subset of $[-1,1]^g$ where either $x_j = \pm 1$ for some $1 \leq j \leq g$ or $x_\ell = x_k$ for some $1 \leq k < \ell \leq g$. So it suffices to show that the set

$$\{(x_1, \ldots, x_g) \in [-1,1]^g : f(x_1, \ldots, x_g) \leq 0\}$$

has $\widetilde{\mu}_{\mathrm{USp}}$-measure zero. As $f(x_1,\ldots,x_g)$ is invariant under a permutation σ of $\{1,\ldots,g\}$, we will be done if we can show that for each such permutation σ, the function $f(x_1,\ldots,x_g)$ is always positive on the set

$$\left\{(x_1,\ldots,x_g)\in[-1,1]^g : -1 < x_{\sigma(1)} < \ldots < x_{\sigma(g)} < 1\right\}.$$

For $g=1$, this is elementary, as

$$f(x_1) = 2\,(1-x_1)\,,$$

which is always positive for $-1 < x_1 < 1$. In fact, one can show that

$$\lim_{x_1\to 1}\widetilde{\psi}_+(x_1) = \frac{1}{4},$$

and that this is the global minimum of $\widetilde{\psi}_+(x_1)$.

For $g=2$,

$$f(x_1,x_2) = \begin{cases} 4\left(1-x_2^2\right) & \text{when } -1 < x_1 < x_2 < 1, \\ 4\left(1-x_1^2\right) & \text{when } -1 < x_2 < x_1 < 1, \end{cases}$$

and in particular is always positive when $x_1, x_2 \neq \pm 1$. Furthermore, it can be shown that

$$\lim_{x_1\to 1}\widetilde{\psi}_+\left(x_1, -\frac{x_1}{3}\right) = \frac{27}{64},$$

and that this is the global minimum of $\widetilde{\psi}_+(x_1,x_2)$. □

Already when $g=3$, the calculations become extremely complicated. However, numerical calculations suggest that the global minimum of ψ_+ is approximately 0.530915.

7.2 Variants of Pólya's Conjecture

Just as we discussed the α- and β-variants of the Mertens conjecture, we may do the same for Pólya's conjecture. Here the properties of the weighted sum

$$L_\alpha(x) = \sum_{n\le x}\frac{\lambda(n)}{n^\alpha}$$

for $\alpha\in\mathbb{R}$ have recently been studied by Mossinghoff and Trudgian [20]; they ask whether for fixed α such sums are of constant sign for sufficiently large x.

For $\alpha > 1$, the inequality $L_\alpha(x) > 0$ will always hold for sufficiently large x, and indeed, $L_\alpha(x)$ converges to the absolutely convergent infinite series

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^\alpha} = \frac{\zeta(2\alpha)}{\zeta(\alpha)},$$

which is strictly positive. Under the assumption of the Riemann hypothesis, this infinite series is conditionally convergent for $1/2 < \alpha < 1$, and as $\zeta(2\alpha)/\zeta(\alpha)$ is negative in this range, we would expect the inequality $L_\alpha(x) < 0$ to hold for all sufficiently large x. For $0 \leq \alpha < 1/2$ and $\alpha = 1$, the eventual constancy of sign of $L_\alpha(x)$ implies the Riemann hypothesis and the simplicity of the zeroes of the Riemann zeta function. However, Mossinghoff and Trudgian modify a result of Ingham [12] to show that the Linear Independence hypothesis for the Riemann zeta function implies that $L_\alpha(x)$ changes sign infinitely often for these values of α; consequently, we would expect $L_\alpha(x)$ to change sign infinitely often for α in this range.

Finally, for $\alpha = 1/2$, Mossinghoff and Trudgian mimic the proof of Proposition 5.1 in order to show that

$$L_{1/2}(x) = \frac{\log x}{2\zeta(1/2)} + \frac{\gamma_0}{\zeta(1/2)} - \frac{\zeta'(1/2)}{2\zeta(1/2)^2} + \sum_{|\gamma|<T_v} \frac{\zeta(2\rho)}{\zeta'(\rho)} \frac{x^{i\gamma}}{i\gamma} + R_{1/2}(x, T_v)$$

under the assumption of the Riemann hypothesis and that all of the zeroes of $\zeta(s)$ are simple. Here γ_0 is the Euler–Mascheroni constant and $R_{1/2}(x, T_v)$ is a small error term, similar to that in Proposition 5.1. Heuristically, one would expect the leading term $\log x/(2\zeta(1/2))$ in this explicit expression for $L_{1/2}(x)$ to dominate the other terms as x grows large; this is in accordance with the conjecture (1.6) of Gonek on the maximal order of growth of $M(x)$. As $\zeta(1/2) < 0$, this leads to the following conjecture of Mossinghoff and Trudgian, which has has been verified computationally up to $x = 10^{12}$ [20, Figure 2].

Conjecture 7.7 (The $\alpha = 1/2$ Conjecture [20, Problem 3])**.** *For all $x \geq 17$,*

$$L_{1/2}(x) = \sum_{n \leq x} \frac{\lambda(n)}{\sqrt{n}} \leq 0.$$

Here we study the function field analogue of this problem, namely for which $\alpha \in \mathbb{R}$ the weighted sum

$$L_{C/\mathbb{F}_q,\alpha}(X) = \sum_{N=0}^{X-1} \frac{1}{q^{\alpha(N+1)}} \sum_{\deg(D)=N} \lambda_{C/\mathbb{F}_q}(D)$$

is of constant sign. For $\alpha > 1/2$, the weighted sum $L_{C/\mathbb{F}_q,\alpha}(X)$ converges to the infinite series

$$\frac{1}{q^{\alpha}} \sum_{N=0}^{\infty} \frac{1}{q^{\alpha N}} \sum_{\deg(D)=N} \mu_{C/\mathbb{F}_q}(D) = \frac{Z_{C/\mathbb{F}_q}\left(q^{-2\alpha}\right)}{q^{\alpha} Z_{C/\mathbb{F}_q}\left(q^{-\alpha}\right)}.$$

Thus for $\alpha > 1$, $L_{C/\mathbb{F}_q,\alpha}(X)$ is eventually positive, while $L_{C/\mathbb{F}_q,\alpha}(X)$ is eventually negative in the range $1/2 < \alpha < 1$; however, $L_{C/\mathbb{F}_q,1}(X)$ converges to zero, as $Z_{C/\mathbb{F}_q}(u)$ has a pole at $u = q^{-1}$, so further analysis is necessary to determine sign changes for this particular weighted sum. For $\alpha < 1/2$, we divide (6.3) by $q^{\alpha(N+1)}$ and sum over all $0 \leq N \leq X-1$, showing that when $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes,

$$\begin{aligned}
&\frac{L_{C/\mathbb{F}_q,\alpha}(X)}{q^{(1/2-\alpha)X}} \\
&= -\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}-q^{\alpha}}\frac{\sqrt{q}-1}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(q^{-1/2}\right)} - (-1)^X\frac{1}{2}\frac{\sqrt{q}}{\sqrt{q}+q^{\alpha}}\frac{\sqrt{q}+1}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}\left(-q^{-1/2}\right)} \\
&\qquad - \sum_{\gamma} \frac{Z_{C/\mathbb{F}_q}\left(\gamma^{-2}\right)}{{Z_{C/\mathbb{F}_q}}'\left(\gamma^{-1}\right)}\frac{\gamma}{\gamma - q^{\alpha}} + O_{q,g}\left(\frac{1}{q^{(1/2-\alpha)X}}\right).
\end{aligned}$$

The proof of Lemma 7.1 can then be modified to show that as q tends to infinity, the quantity

$$B_{\alpha}^{+}(C/\mathbb{F}_q) = \limsup_{X\to\infty} \frac{L_{C/\mathbb{F}_q,\alpha}(X)}{q^{(1/2-\alpha)X}}$$

satisfies the asymptotic

$$B_{\alpha}^{+}(C/\mathbb{F}_q) = \varphi_{+}\left(\vartheta(C/\mathbb{F}_q)\right) + O_{g,\alpha}\left(-\frac{1}{q^{1/2-\alpha}}\varphi_{-}\left(\vartheta(C/\mathbb{F}_q)\right)\right)$$

when C satisfies LI, and consequently the proof of Theorem 5.9 is still true with Pólya's conjecture for the function field $C/\mathbb{F}_q$ replaced by the conjecture that for fixed $\alpha < 1/2$,

$$\limsup_{X\to\infty} L_{C/\mathbb{F}_q,\alpha}(X) \leq 0.$$

It remains to study the function field version of the $\alpha = 1/2$ conjecture. By dividing (6.3) by $q^{(N+1)/2}$ and summing over all $0 \leq N \leq X-1$, we are able to determine the following expression for $L_{C/\mathbb{F}_q,1/2}(X)$ when $Z_{C/\mathbb{F}_q}(u)$ has only simple zeroes.

Proposition 7.8. *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 0$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. Then for each*

$X \geq 1$,

$$\begin{aligned} L_{C/\mathbb{F}_q,1/2}(X) = &-\frac{1}{2}\frac{\sqrt{q}-1}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})}X - \frac{(-1)^X-1}{4}\frac{\sqrt{q}+1}{\sqrt{q}-1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(-q^{-1/2})} \\ &- \sum_{\gamma}\frac{Z_{C/\mathbb{F}_q}(\gamma^{-2})}{Z_{C/\mathbb{F}_q}{}'(\gamma^{-1})}\frac{\sin(X\theta(\gamma)/2)}{\sin(\theta(\gamma)/2)}e^{i(X+1)\theta(\gamma)/2} \\ &+ \frac{(-1)^X q^{-X/2}-1}{\sqrt{q}+1}\frac{q+1}{q-1}\frac{h_{C/\mathbb{F}_q}{}^2}{h_{C/\mathbb{F}_{q^2}}} + R_{X,1/2}(q,g,T), \end{aligned} \tag{7.1}$$

where the sum is over the inverse zeroes of $Z_{C/\mathbb{F}_q}(u)$, $T > 0$ is sufficiently small, and the error term $R_{X,1/2}(q,g,T)$ is constant for $X \geq \max\{2g-3, 1\}$.

The notable difference here to the number field case is that there are only finitely many zeroes of $Z_{C/\mathbb{F}_q}(u)$, and hence the sum over the inverse zeroes is bounded. Consequently, we have that

$$L_{C/\mathbb{F}_q,1/2}(X) = -\frac{1}{2}\frac{\sqrt{q}-1}{\sqrt{q}+1}\frac{q^{-g}h_{C/\mathbb{F}_q}}{P_{C/\mathbb{F}_q}(q^{-1/2})}X + O_{q,g}(1)$$

as X tends to infinity, which resolves the function field analogue of the $\alpha = 1/2$ conjecture.

Theorem 7.9 (The $\alpha = 1/2$ Conjecture in Function Fields)**.** *Let C be a nonsingular projective curve over $\mathbb{F}_q$ of genus $g \geq 0$, and suppose that all of the zeroes γ^{-1} of $Z_{C/\mathbb{F}_q}(u)$ are simple. Then for all sufficiently large X, the inequality*

$$L_{C/\mathbb{F}_q,1/2}(X) = \sum_{N=0}^{X-1}\frac{1}{q^{(N+1)/2}}\sum_{\deg(D)=N}\lambda_{C/\mathbb{F}_q}(D) < 0 \tag{7.2}$$

holds.

Appendix A

Proof of the Kronecker–Weyl Theorem

In this appendix, we prove the following lemma.

Lemma 2.7 (Kronecker–Weyl Theorem)**.** *Let $t_1, \ldots, t_g$ be real numbers, and let H be the topological closure in $\mathbb{T}^g$ of the subgroup*

$$\widetilde{H} = \left\{ \left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) \in \mathbb{T}^g : X \in \mathbb{Z} \right\}.$$

Then H is a closed subgroup of $\mathbb{T}^g$. In particular, when the collection $1, t_1, \ldots, t_g$ is linearly independent over the rational numbers, H is precisely $\mathbb{T}^g$. Furthermore, for arbitrary $t_1, \ldots, t_g$ and for any continuous function $h : \mathbb{T}^g \to \mathbb{C}$, we have that

$$\lim_{Y \to \infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) = \int_H h(z)\, d\mu_H(z),$$

where μ_H is the normalised Haar measure on H.

The proof of this result makes use of several notable properties of $\mathbb{T}^g$; namely that it is an abelian group that is also compact as a topological space. It is no surprise then that the method of proof uses abstract harmonic analysis. We must therefore first recall some definitions and results from this field.

Lemma A.1 ([7, Lemma 1.1.3])**.** *Let $\widetilde{H}$ be a subgroup of a locally compact abelian group G. Then its topological closure H in G is also a subgroup of G.*

Corollary A.2. *Let $t_1, \ldots, t_g$ be arbitrary real numbers, and let H be the topological closure in $\mathbb{T}^g$ of*

$$\widetilde{H} = \left\{ \left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) \in \mathbb{T}^{g+1} : X \in \mathbb{Z} \right\}.$$

Then H is a closed subgroup of $\mathbb{T}^g$.

Proof. Indeed, $\widetilde{H}$ is the image of the group homomorphism $\phi : \mathbb{Z} \to \mathbb{T}^g$ given by $\phi(X) = \left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right)$, and so $\widetilde{H}$ is a subgroup of $\mathbb{T}^g$. The result then follows by Lemma A.1. $\square$

Definition A.3. Let G be a locally compact abelian group. A *character* on G is a continuous group homomorphism $\chi : G \to \mathbb{T}$, where $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ is the circle group. The set of all characters on G is called the *dual group* of G and is denoted $\widehat{G}$.

Proposition A.4 ([7, Theorem 3.2.1])**.** *Let G be a locally compact abelian group. Then the dual group $\widehat{G}$ of G is also a locally compact abelian group.*

Theorem A.5 (Pontryagin Duality [7, Theorem 3.5.5])**.** *Let G be a locally compact abelian group. Then the dual group $\widehat{\widehat{G}}$ of $\widehat{G}$ is canonically isomorphic to G via the isomorphism $x \mapsto \delta_x$, where $\delta_x(\chi) = \chi(x)$ for each $\chi \in \widehat{G}$.*

The importance of showing earlier that H is a closed subgroup of $\mathbb{T}^g$ becomes evident through certain results involving the annihilator of H.

Definition A.6. Let H be a closed subgroup of a locally compact abelian group G. The *annihilator* $H^\perp$ of H is the set of all characters $\chi \in \widehat{G}$ satisfying $\chi|_H = 1$.

Proposition A.7 ([7, Lemma 3.6.1])**.** *Let G be a locally compact abelian group, and H a closed subgroup of G. Then $H^\perp$ is isomorphic to $\widehat{G/H}$ via the isomorphism $\chi \mapsto \widetilde{\chi}$, where $\widetilde{\chi}(xH) = \chi(x)$ for all $xH \in G/H$, and $\widehat{G}/H^\perp$ is isomorphic to $\widehat{H}$ via the isomorphism $\chi H^\perp \mapsto \chi|_H$.*

Finally, we must determine exactly the characters of $\mathbb{T}^g$ and its dual group.

Lemma A.8. *Let $\mathbb{T}^g$ be the g-torus. Then a character $\chi : \mathbb{T}^g \to \mathbb{T}$ is of the form*

$$\chi(z_1, \ldots, z_g) = z_1^{k_1} \cdots z_g^{k_g}$$

for some $(k_1, \ldots, k_g) \in \mathbb{Z}^g$. Conversely, for any $(k_1, \ldots, k_g) \in \mathbb{Z}^g$, χ is a character of $\mathbb{T}^g$. In particular, the dual group of $\mathbb{T}^g$ is isomorphic to $\mathbb{Z}^g$.

Of course, an analogous result holds for $\mathbb{Z}^g$.

Corollary A.9. *A character $\chi : \mathbb{Z}^g \to \mathbb{T}$ is of the form*

$$\chi(k_1, \ldots, k_g) = z_1^{k_1} \cdots z_g^{k_g}$$

for some $(z_1, \ldots, z_g) \in \mathbb{T}^g$. Conversely, for any $(z_1, \ldots, z_g) \in \mathbb{T}^g$, χ is a character of $\mathbb{Z}^g$. In particular, the dual group of $\mathbb{Z}^g$ is isomorphic to $\mathbb{T}^g$.

We now have the framework necessary to determine $H^\perp$ for H the topological closure in $\mathbb{T}^g$ of the set $\widetilde{H} = \left\{\left(e^{2\pi i X t_1}, \dots, e^{2\pi i X t_g}\right) \in \mathbb{T}^g : X \in \mathbb{Z}\right\}$.

Lemma A.10. *Let $t_1, \dots, t_g$ be arbitrary real numbers, and let H be the topological closure of $\widetilde{H} = \left\{\left(e^{2\pi i X t_1}, \dots, e^{2\pi i X t_g}\right) \in \mathbb{T}^g : X \in \mathbb{Z}\right\}$ in $\mathbb{T}^g$. Then $H^\perp$ is isomorphic to $\{k \in \mathbb{Z}^g : t_1 k_1 + \cdots + t_g k_g \in \mathbb{Z}\}$. In particular, if the collection $1, t_1, \dots, k_g$ is linearly independent over the rational numbers, then $H = \mathbb{T}^g$.*

Proof. Each character $\chi \in H^\perp$ is of the form $\chi(z_1, \dots, z_g) = z_1^{k_1} \cdots z_g^{k_g}$ for some $(k_1, \dots, k_g) \in \mathbb{Z}^g$ with the property that for all $X \in \mathbb{Z}$,

$$1 = \chi\left(e^{2\pi i X t_1}, \dots, e^{2\pi i X t_g}\right) = e^{2\pi i (t_1 k_1 + \cdots + t_g k_g) X},$$

and hence $t_1 k_1 + \cdots + t_n k_n \in \mathbb{Z}$. Conversely, if $t_1 k_1 + \cdots + t_n k_n \in \mathbb{Z}$, then the homomorphism $\chi(z_1, \dots, z_g) = z_1^{k_1} \cdots z_g^{k_g}$ satisfies $\chi|_H = 1$.

Now the set

$$\{k \in \mathbb{Z}^g : t_1 k_1 + \cdots + t_g k_g \in \mathbb{Z}\}$$

is isomorphic to

$$\left\{k \in \mathbb{Z}^{g+1} : k_0 + t_1 k_1 + \cdots + t_g k_g = 0\right\},$$

and if $1, t_1, \dots, k_g$ forms a linearly independent collection over the rational numbers, then this is equal to the set $\{k = 0\}$. Thus $H^\perp \cong \{0\}$, and hence $H = \mathbb{T}^g$. $\square$

Next, we show that for any trigonometric polynomial h on $\mathbb{T}^g$,

$$\lim_{Y \to \infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \dots, e^{2\pi i X t_g}\right) = \int_H h(z)\, d\mu_H(z).$$

The proof again makes use of the properties of the annihilator of H, this time via the Poisson summation formula.

Definition A.11. Let G be a locally compact abelian group, and let $h : G \to \mathbb{C}$ be a continuous compactly supported function. The *Fourier transform* of h with respect to a Haar measure μ_G on G is the function $\widehat{h}$ on $\widehat{G}$ given by

$$\widehat{h}(\chi) = \int_G h(x) \overline{\chi(x)}\, d\mu_G(x).$$

Proposition A.12 (Poisson Summation Formula [7, Theorem 3.6.3]). *Let H be a closed subgroup of a locally compact abelian group G, and let $h : G \to \mathbb{C}$ be a continuous compactly supported function. Then we have that*

$$\int_H h(z)\, d\mu_H(z) = \int_{H^\perp} \widehat{h}(\chi)\, d\mu_{H^\perp}(\chi),$$

where μ_H is a Haar measure on H and $\mu_{H^\perp}$ is the induced Haar measure on $H^\perp$.

Lemma A.13. *Let $t_1, \ldots, t_g$ be arbitrary real numbers, and let $h : \mathbb{T}^g \to \mathbb{C}$ be a trigonometric polynomial; that is, a function of the form*

$$h(z) = \sum_{k \in \mathbb{Z}^g} c_k z_1^{k_1} \cdots z_g^{k_g}$$

for $z = (z_1, \ldots, z_g) \in \mathbb{T}^g$, where all but finitely many of the coefficients $c_k \in \mathbb{C}$ are zero. Then we have that

$$\lim_{Y \to \infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) = \int_H h(z)\, d\mu_H(z),$$

where μ_H is the normalised Haar measure on H.

Proof. Let $\chi : \mathbb{T}^g \to \mathbb{T}$ be a character corresponding to $\widetilde{k} \in \mathbb{Z}^g$. Then

$$\widehat{h}(\chi) = \int_{\mathbb{T}^g} h(z)\overline{\chi(z)}\, dz = \int_{\mathbb{T}} \cdots \int_{\mathbb{T}} \sum_{k \in \mathbb{Z}^g} c_k z_1^{k_1} \cdots z_g^{k_g} \overline{z_1^{\widetilde{k}_1} \cdots z_g^{\widetilde{k}_g}}\, dz_1 \cdots dz_g.$$

We may interchange the order of summation and integration as there are only finitely many nonzero members in this sum. Thus

$$\begin{aligned}
\widehat{h}(\chi) &= \sum_{k \in \mathbb{Z}^g} c_k \prod_{j=1}^{g} \int_{\mathbb{T}} z_j^{k_j - \widetilde{k}_j}\, dz_j \\
&= \sum_{k \in \mathbb{Z}^g} c_k \prod_{j=1}^{g} \int_0^1 e^{2\pi i \left(k_j - \widetilde{k}_j\right)\theta}\, d\theta \\
&= \sum_{k \in \mathbb{Z}^g} c_k \prod_{j=1}^{g} \begin{cases} 1 & \text{if } k_j = \widetilde{k}_j, \\ 0 & \text{otherwise,} \end{cases} \\
&= c_{\widetilde{k}}.
\end{aligned}$$

Recalling that $H^\perp$ is isomorphic to $\{k \in \mathbb{Z}^g : t_1 k_1 + \cdots + t_g k_g \in \mathbb{Z}\}$, so that the Haar measure $\mu_{H^\perp}$ on $H^\perp$ is simply the counting measure, we therefore obtain by the Poisson summation formula that

$$\int_H h(z)\, d\mu_H(z) = \int_{H^\perp} \widehat{h}(\chi)\, d\mu_{H^\perp}(\chi) = \sum_{\substack{k \in \mathbb{Z}^g \\ t_1 k_1 + \cdots + t_g k_g \in \mathbb{Z}}} c_k.$$

On the other hand,

$$\begin{aligned}
&\sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) \\
&\qquad = \sum_{k\in\mathbb{Z}^g} c_k \sum_{X=1}^{Y} e^{2\pi i (t_1k_1+\cdots+t_gk_g)X} \\
&\qquad = \sum_{\substack{k\in\mathbb{Z}^g \\ t_1k_1+\cdots+t_gk_g\in\mathbb{Z}}} c_k Y + \sum_{\substack{k\in\mathbb{Z}^g \\ t_1k_1+\cdots+t_gk_g\notin\mathbb{Z}}} \frac{c_k\left(e^{2\pi i(t_1k_1+\cdots+t_gk_g)Y}-1\right)}{1-e^{-2\pi i(t_1k_1+\cdots+t_gk_g)}}.
\end{aligned}$$

Thus

$$\lim_{Y\to\infty}\frac{1}{Y}\sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) = \sum_{\substack{k\in\mathbb{Z}^g \\ t_1k_1+\cdots+t_gk_g\in\mathbb{Z}}} c_k = \int_H h(z)\, d\mu_H(z). \qquad \square$$

From this, we may easily obtain the result in the general case where h is merely a continuous function. Indeed, this follows simply from the density of the trigonometric polynomials in the space of continuous complex-valued functions on $\mathbb{T}^g$ with regards to the supremum norm, that is to say, the Stone–Weierstrass theorem.

Lemma A.14. *For any continuous function $h : \mathbb{T}^g \to \mathbb{C}$, we have that*

$$\lim_{Y\to\infty}\frac{1}{Y}\sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) = \int_H h(z)\, d\mu_H(z).$$

Proof. Given a continuous function $h : \mathbb{T}^n \to \mathbb{C}$ and a fixed $\varepsilon > 0$, the Stone–Weierstrass theorem shows the existence of a trigonometric polynomial

$$\widetilde{h}(z) = \sum_{k\in\mathbb{Z}^g} c_k z_1^{k_1}\cdots z_g^{k_g},$$

where all but finitely many of the coefficients $c_k \in \mathbb{C}$ are zero, such that

$$\max_{z\in\mathbb{T}^g}\left|h(z)-\widetilde{h}(z)\right| < \varepsilon/2.$$

Then

$$\lim_{Y\to\infty}\frac{1}{Y}\sum_{X=1}^{Y}\left|h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right)-\widetilde{h}\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right)\right| < \frac{\varepsilon}{2},$$

and similarly

$$\int_H \left|h(z)-\widetilde{h}(z)\right|\, d\mu_H(z) < \frac{\varepsilon}{2}$$

as $\mu_H(H) = 1$, and consequently

$$\left| \lim_{Y \to \infty} \frac{1}{Y} \sum_{X=1}^{Y} h\left(e^{2\pi i X t_1}, \ldots, e^{2\pi i X t_g}\right) - \int_H h(z)\, d\mu_H(z) \right| < \varepsilon.$$

As $\varepsilon > 0$ was arbitrary, we obtain the result. $\square$

This completes the proof of the Kronecker–Weyl theorem.

Bibliography

[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] Patrick Billingsley, *Convergence of Probability Measures,* 2^{nd} *Edition*, John Wiley and Sons, New York, 1999.

[3] Peter Borwein, Ron Ferguson, and Michael J. Mossinghoff, "Sign Changes in Sums of the Liouville Function", *Mathematics of Computation* **77** (2008), no. 263, 1681–1694.

[4] Byungchul Cha, "Chebyshev's Bias in Function Fields", *Compositio Mathematica* **144** (2008), no. 6, 1351–1374.

[5] 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.

[6] Nick Chavdarov, "The General Irreducibility of the Numerator of the Zeta Function in a Family of Curves with Large Monodromy", *Duke Mathematical Journal* **87** (1997), no. 1, 151–180.

[7] Anton Deitmar and Siegfried Echterhoff, *Principles of Harmonic Analysis*, Universitext, Springer, New York, 2009.

[8] A. Y. Fawaz, "The Explicit Formula for $L_0(x)$", *Proceedings of the London Mathematical Society* **1** (1951), no. 3, 86–103.

[9] C. B. Haselgrove, "A Disproof of a Conjecture of Pólya", *Mathematika* **5** (1958), 141–145.

[10] 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.

[11] Peter Humphries, "The Distribution of Weighted Sums of the Liouville Function and Pólya's Conjecture", to appear in *Journal of Number Theory*, arXiv:math.NT/1108.1524 (7 August 2011), 32 pages.

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

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

[14] J. P. Keating and N. C. Snaith, "Random Matrix Theory and L-functions at $s = 1/2$", *Communications in Mathematical Physics* **214** (2000), no. 1, 91–110.

[15] 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.

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

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

[18] Hugh L. Montgomery, "The Zeta Function and Prime Numbers", in *Proceedings of the Queen's Number Theory Conference, 1979*, editor P. Ribenboim, Queen's Papers in Pure and Applied Mathematics **54**, Queen's University, Kingston, Ontario, 1980, 1–31.

[19] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative Number Theory: I. Classical Theory*, Cambridge Studies in Advanced Mathematics **97**, Cambridge University Press, Cambridge, 2007.

[20] Michael J. Mossinghoff and Timothy S. Trudgian, "Between the Problems of Pólya and Turán", to appear in *Journal of the Australian Mathematical Society*, `http://www.davidson.edu/math/mossinghoff/BetweenPolyaTuran_MT.pdf` (28 September 2011), 13 pages.

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

[22] 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.

[23] Georg Pólya, "Verschiedene Bemerkungen zur Zahlentheorie", *Jahresbericht der Deutschen Mathematiker-Vereinigung* **28** (1919), 31–40.

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

[25] Michael Rubinstein and Peter Sarnak, "Chebyshev's Bias", *Experimental Mathematics* **3** (1994), no. 3, 173–197.

[26] 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.

[27] 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.

[28] M. Tanaka, "A Numerical Investigation on Cumulative Sum of the Liouville Function", *Tokyo Journal of Mathematics* **3** (1980), 187–189.

[29] William C. Waterhouse, "Abelian Varieties over Finite Fields", *Annales Scientifiques de l'École Normale Supérieure* **4** (1969), t. 2, 521–560.