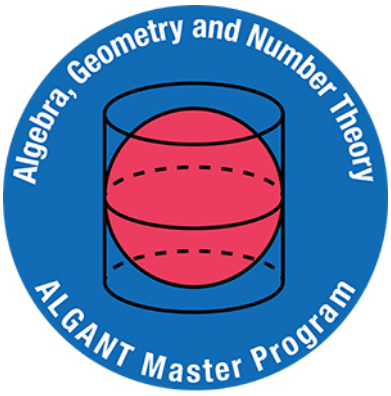
ALGANT Master Program

Master's Thesis

Chebyshev's bias in function fields

Author:
Shehzad Hathi

Supervisor:
Dr. Florent Jouve



July 15, 2018

Abstract

In this thesis, we look at the geometric analogue of Chebyshev's bias, a phenomenon that refers to the fact that primes are biased towards quadratic non-residues in most intervals $[2, x]$. In the case of number fields, this phenomenon was studied in a well-known paper by Rubinstein and Sarnak. Following that, Cha studies this bias in a function field setting. Under a linear independence hypothesis on zeros of L-function (LI), we see how irreducible monic polynomials in a polynomial ring over a finite field are distributed in a given set of residue classes modulo a fixed monic polynomial. As in the classical case, we obtain an asymptotic formula (Theorem 2.6) for a counting function measuring the number of prime quadratic residues minus prime quadratic non-residues. The proof we give here is based on a strategy suggested (but not pursued) in [Cha08]. Although quite a few results are analogous to the number field case, an important distinction is that LI can be proven to hold in some cases and can be violated in some other cases in the function field setting. Also, under the LI, we see that the bias dissipates as the degree of modulus under consideration tends to infinity (along with some necessary and sufficient conditions).

Since LI for function fields can be violated in certain cases, it is important to show that it holds in certain cases (which it does) for the above described work to be useful. Hence, this becomes the second part of the thesis. Using the sieve for Frobenius developed earlier by him, Kowalski showed that in a certain sense, the roots of the L-functions of most algebraic curves over finite fields do not satisfy any non-trivial (linear or multiplicative) dependency relations, which is essentially what LI says. Although we don't give the proof of the most general version of the aforementioned result, we illustrate the use of the sieve for Frobenius to prove LI for a certain family of hyperelliptic curves. We also give an improved bound in Proposition 3.11 for the number of hyperelliptic curves (in a family, indexed by integers) with a Jacobian that is not simple. This improvement is in comparison to the one in Proposition 6.3 of [Kow06] using the suggestion of C. Helsholtz which has been mentioned as a note in the paper.

Acknowledgements

The reason why I decided to do my thesis in analytic number theory was because I had developed an interest in it during my undergraduate years and over the course of my master's studies. The most important module in this context was taught by my advisor, Prof Florent Jouve. While I had already decided to do a master's thesis in the field of analytic number theory, it was still quite important to explain the motivation behind the topic of the thesis and he did that quite well, for which I am grateful. I would also like to thank him for his constant support, painstaking corrections, and the overall mathematical insight that he provided for the thesis.

I would like to thank my fellow classmates for the variety of discussions that we engaged in throughout this year, including, but not limited to, mathematics. I would also like to thank Prof Christine Bachoc and Prof Dajano Tossici as they coordinated the ALGANT activities at Bordeaux. Without them, this thesis and in fact, the entire year of my master's program at Bordeaux would not have been possible.

Finally, I would like to express my gratitude to Ms. Nicole Bergerot and other staff members, especially those involved with the ALGANT Program.

Shehzad Hathi

Contents

Chapter 1

Dirichlet characters over function fields

1.1 Primes and the reciprocity law

Let p be an odd prime number and q be a power of p. We will denote by $\mathbb{F}$, a finite field with q elements. A monic irreducible polynomial in $\mathbb{F}[T]$ will be denoted by P and henceforth, will be called "prime".

Let $a \in \mathbb{F}[T]$ such that P does not divide a and d a divisor of $q-1$ (q is the cardinality of $\mathbb{F}$). Since $\mathbb{F}^* \to (\mathbb{F}[T]/P)^*$ is one-to-one, there is a unique $\alpha \in \mathbb{F}^*$ such that

$$a^{\frac{|P|-1}{d}} \equiv \alpha \bmod P.$$

Definition 1.1. *If P does not divide a, let $(a/P)_d$ be the unique element of $\mathbb{F}^*$ such that*

$$a^{\frac{|P|-1}{d}} \equiv \left(\frac{a}{P}\right)_d \bmod P.$$

If $P|a$ define $(a/P)_d = 0$. Note that the above definition is also valid if P is irreducible but not necessarily monic.

Theorem 1.2 (The d-th power reciprocity law)**.** *Let P and Q be monic irreducible polynomials of degrees δ and ν respectively. Then,*

$$\left(\frac{Q}{P}\right)_d = (-1)^{\frac{q-1}{d}\delta\nu} \left(\frac{P}{Q}\right)_d$$

1.2 Dirichlet characters

Let m be an element of $\mathbb{F}[T]$ with non-zero degree M. A Dirichlet character χ modulo m is a function from $\mathbb{F}[T] \to \mathbb{C}$ such that

1. $\chi(a+bm) = \chi(a)$ for all $a, b \in \mathbb{F}[T]$
2. $\chi(a)\chi(b) = \chi(ab)$ for all $a, b \in \mathbb{F}[T]$
3. $\chi(a) \neq 0$ if and only if $(a, m) = 1$.

χ induces a homomorphism from $(\mathbb{F}[T]/m)^* \to \mathbb{C}^*$ and conversely, given such a homomorphism there is a unique Dirichlet character corresponding to it. It can be shown that there are exactly $\Phi(m) = \#(\mathbb{F}[T]/m)^*$ Dirichlet characters modulo m. In fact, the set of Dirichlet characters modulo m, say X_m, is a group that is isomorphic to $(\mathbb{F}[T]/m)^*$. The *principal* Dirichlet character χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

The Dirichlet characters modulo m satisfy the standard orthogonality relations.

Proposition 1.3. *Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of $\mathbb{F}[T]$ prime to m. Then*

1. $\sum_a \chi(a)\bar{\psi}(a) = \Phi(m)\delta(\chi,\psi)$.
2. $\sum_\chi \chi(a)\bar{\chi}(b) = \Phi(m)\delta(a,b)$.

The first sum is over any set of representatives for $\mathbb{F}[T]/m$ and the second sum is over all Dirichlet characters modulo m. Here δ represents the Kronecker delta function.

1.3 Zeta function and Dirichlet L-series

Definition 1.4. *The zeta function of $\mathbb{F}[T]$, denoted $\zeta(s)$ is defined by the infinite series*

$$\zeta(s) = \sum_{f \ monic} \frac{1}{|f|^s},$$

where $|f| := q^{deg(f)}$.

The above series converges for $\Re(s) > 1$. Since there are exactly q^d monic polynomials of degree d in $\mathbb{F}[T]$, we have

$$\sum_{\deg(f)\le d} |f|^{-s} = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots + \frac{q^d}{q^{ds}},$$

and consequently

$$\zeta(s) = \frac{1}{1-q^{1-s}} \tag{1.1}$$

for all complex numbers s with $\Re(s) > 1$. As in the classical case, we again have a unique decomposition of monic polynomials into primes which leads to the following identity

$$\zeta(s) = \prod_{P \text{ prime}} (1 - |P|^{-s})^{-1}. \tag{1.2}$$

This is also valid for all $\Re(s) > 1$. The identity above is quite useful as we will see below.

We can define a quantity similar to the prime counting function in case of positive integers, $\pi(N) := \#\{P \text{ prime} \mid deg(P) = N\}$. Then, from (1.2) we find

$$\zeta(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-\pi(d)}$$

Using (1.1) and substituting $u = q^{-s}$ (note that $|u| < 1$ if and only if $\Re(s) > 1$) we obtain the identity

$$\frac{1}{1-qu} = \prod_{d=1}^{\infty} (1-u^d)^{-\pi(d)}.$$

Taking the logarithmic derivative of both sides and multiplying the result by u yields

$$\frac{qu}{1-qu} = \sum_{d=1}^{\infty} \frac{d\pi(d)u^d}{1-u^d}.$$

Finally, we expand both sides into power series using the geometric series and compare coefficients of u^n, giving us

Proposition 1.5.

$$\sum_{d|n} d\pi(d) = q^n.$$

By applying the Möbius inversion formula to the above formula, we get

Corollary 1.6.

$$\pi(d) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}, \tag{1.3}$$

where $\mu(d)$ is the Möbius function.

In (1.3), the highest power of q that occurs is q^n and the next highest power that may occur is $q^{n/2}$ (this occurs if and only if 2|n). All the other terms have the form $\pm q^m$ where $m \leq n/3$. The total number of terms is $\sum_{d|n} |\mu(d)|$, which is easily seen to be 2^t, where t is the number of distinct prime divisors of n. Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing n. Then, $2^t \leq p_1 p_2 \ldots p_t \leq n$. Thus, we have the following estimate:

$$\left|\pi(n) - \frac{q^n}{n}\right| \leq \frac{q^{n/2}}{2} + q^{n/3}.$$

Thus, we have a result similar to the classical prime number theorem.

Theorem 1.7 (The prime number theorem for polynomials)**.**

$$\pi(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right)$$

We also have a function field analogue of the Riemann hypothesis. This was first proved by Weil in the late 1940s.

Theorem 1.8 (the Riemann Hypothesis for function fields)**.** *Let $K/\mathbb{F}$ be a function field with finite constant field, $\mathbb{F}$, having q elements. Let $\zeta_K(s)$ be the zeta function of K. All the zeros of $\zeta_K(s)$ lie on the line $\Re(s) = \frac{1}{2}$.*

The zeta function is a special case of the Dirichlet L-series (when "$\chi = 1$").

Definition 1.9. *Let χ be a Dirichlet character modulo m. The Dirichlet L-series corresponding to χ is defined by*

$$L(s, \chi) = \sum_{f \ monic} \frac{\chi(f)}{|f|^s}.$$

From the definition of the L-series and comparison with the zeta function, one sees immediately that the series for $L(s, \chi)$ converges absolutely for $\Re(s) > 1$. Also, since characters are multiplicative, we can deduce that the following product decomposition is valid in the same region.

$$L(s, \chi) = \prod_P \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1},$$

The zeta function also has a similar decomposition.

$$\zeta(s) = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1}$$

Using this, we can then derive a relation between $L(s, \chi_0)$ (where χ_0 is the principal character) and $\zeta(s)$.

$$\begin{aligned}\zeta(s) &= \prod_{P\nmid m}\left(1-\frac{1}{|P|^s}\right)^{-1}\prod_{P|m}\left(1-\frac{1}{|P|^s}\right)^{-1}\\ &= L(s,\chi_0)\prod_{P|m}\left(1-\frac{1}{|P|^s}\right)^{-1}\end{aligned}$$

which gives us

$$L(s,\chi_0)=\prod_{P|m}\left(1-\frac{1}{|P|^s}\right)\zeta(s). \tag{1.4}$$

Since $\zeta(s)$ is meromorphic over $\mathbb{C}$ with a simple pole at $s=1$, $L(s,\chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s=1$.

If χ is non-principal, then $L(s,\chi)$ can be analytically continued to an entire function on all of $\mathbb{C}$. This is due to the following proposition.

Proposition 1.10. *Let χ be a non-principal Dirichlet character modulo m. Then, $L(s,\chi)$ is a polynomial in q^{-s} of degree at most $M-1$.*

For the proof of this proposition, see [Ros13, Proposition 4.3].

Lemma 1.11. *Let χ be a non-principal Dirichlet character modulo m. Then*

$$\frac{L'}{L}(1,\chi)=O(\log M)$$

as $M\to\infty$.

The number-theoretic counterpart of this lemma is $(L'/L)(1,\chi)=O(\log\log q)$, where χ is a non-principal Dirichlet character modulo q. The proof of the above lemma is similar to that of its number-theoretic counterpart (given in [Lit28]) and can be found in [Cha08] (Lemma 6.3).

Since $L(s,\chi)$ is a polynomial in q^{-s}, let $\mathcal{L}(u,\chi):=L(s,\chi)$, obtained by the change of variable $u:=q^{-s}$.

χ is *primitive* if there is no proper divisor $m'|m$ so that $\chi(f)=1$ whenever $(f,m)=1$ and $f\equiv 1 \bmod m'$. Also, χ is *even* if $\chi(cf)=\chi(f)$ for all $0\neq c\in\mathbb{F}$.

Proposition 1.12. *Let χ^* be the primitive Dirichlet character modulo a polynomial $m(\chi^*)$ which induces a non-principal Dirichlet character χ modulo m. Also, let $M(\chi^*)$ be the degree of $m(\chi^*)$. Then we have:*

1. $$\mathcal{L}(u,\chi)=\mathcal{L}(u,\chi^*)\prod_{\substack{P|m\\ P\nmid m(\chi^*)}}(1-u^{deg(P)});$$

2. *$\mathcal{L}(u,\chi^*)$ is a polynomial in u of degree $M(\chi^*)-1$;*

3. *if χ^* is even,*
$$\mathcal{L}(u,\chi^*)=(1-u)\prod_{i=1}^{M(\chi^*)-2}(1-\gamma_i u),$$
and, otherwise,
$$\mathcal{L}(u,\chi^*)=\prod_{i=1}^{M(\chi^*)-1}(1-\gamma_i u)$$

for some complex numbers γ_i *with* $|\gamma_i| = \sqrt{q}$*;*

4. *if* m *is irreducible, then*

$$\mathcal{L}(u, \chi_{quad}) = (1-u) \prod_{i=1}^{(M-2)/2} (1-\gamma_i u)(1-\bar{\gamma}_i u)$$

for M *even, and*

$$\mathcal{L}(u, \chi_{quad}) = \prod_{i=1}^{(M-1)/2} (1-\gamma_i u)(1-\bar{\gamma}_i u)$$

for M *odd.*

Proof. These properties are essentially consequences of Theorem 1.8. Property (1) is immediate from our definition of Dirichlet L-series. Note that, for a non-principal character χ, the Dirichlet L-series can be modified to give the Artin L-function (see [Ros13, pp. 126-131]) by introducing a local factor at the infinite prime, which is $(1-q^{-s})^{-1}$ if χ is even, and one otherwise. This together with Theorem 1.8, proves (2) and (3) (see [Ros13, Proposition 14.10]). Lastly, property (4) is immediate from property (2), (3), and the fact that the inverse zeros of $\mathcal{L}(u, \chi_{\text{quad}})$ are stable under complex conjugation. □

Chapter 2

Chebyshev's bias in function fields

2.1 Introduction

Chebyshev noted in 1853 that for most values of x, there are more primes ($\leq x$) congruent to 3 than 1 modulo 4. More generally, it was observed that the prime quadratic non-residues of a given modulus predominate over the prime quadratic residues in most intervals $[2, x]$. This bias towards quadratic non-residues is referred to as *Chebyshev's bias*. In [RS94], one can find conditional results justifying the existence of this bias. This paper is crucial in understanding the analogous results obtained in [Cha08].

In this chapter, we look at the geometric analogue of Chebyshev's bias, i.e., in a rational function field setting, as studied in [Cha08]. We fix m, a monic polynomial in $\mathbb{F}[T]$ with degree at least two. As before, we will denote the degree of m by M and the irreducible monic polynomials in $\mathbb{F}[T]$ will be denoted by P. For any positive integer N, we define $\pi(N)$ as before. We also define another prime counting function for an element a in $\mathbb{F}[T]$ prime to m,

$$\pi(a, m, N) := \#\{P | P \equiv a \bmod m, \deg(P) = N\}.$$

For a positive integer X, we define $E_{m;a}(X)$ by

$$E_{m;a}(X) := \frac{X}{q^{X/2}} \sum_{N=1}^{X} (\Phi(m)\pi(a, m, N) - \pi(N)). \tag{2.1}$$

The function $E_{m;a}(X)$ can be thought as describing how much more (or less) primes there are in the residue class of a than its fair share. In § 2.2, the explicit formula of $E_{m;a}(X)$ is obtained (Theorem 2.5) by analyzing the coefficients of the power series of the logarithmic derivative of a Dirichlet L-function $L(s, \chi)$ for all Dirichlet characters modulo m. From the explicit formula, we also see the source of the bias ($-c(m, a)\mathcal{B}_q(X)$ term in the formula).

In § 2.3, we focus on the principal-real quadratic character χ_{quad} modulo an irreducible m. We again obtain an asymptotic formula (Theorem 2.6) for a counting function measuring the number of prime quadratic residues minus prime quadratic non-residues. The proof given here is different from the one given in [Cha08], although the strategy used was suggested in the original paper itself. From the formula, we can prove the existence of a certain limiting distribution $\mu_{m;R,N}$ that is constructed from $E_{m;R,N}(X)$ (see Theorem 2.9). We define a function field version of the *linear independence* hypothesis (LI) (Definition 2.10). As in [RS94], under LI for all

non-principal characters, we can find a formula (Theorem 2.11) of the Fourier transformation of $\mu_{m;R,N}$. From this, we can deduce that, if we define $P_{m;R,N}$ to be the set of all positive integers with

$$\sum_{N=1}^{X} a(N) > \sum_{N=1}^{X} b(N),$$

where $a(N) := \#\{P \in \mathbb{F}[T] | \chi_{\text{quad}}(P) = 1, \deg(P) = N\}$ and $b(N) := \#\{P \in \mathbb{F}[T] | \chi_{\text{quad}}(P) = -1, \deg(P) = N\}$, then

$$\delta(P_{m;R,N}) := \lim_{X\to\infty} \frac{\#(P_{m;R,N} \cap \{1, 2, \ldots, X\})}{X}$$

exists and $\delta(P_{m;R,N}) < 1/2$. As an application of this, we also prove that more primes of an affine line splits on a double covering of an irreducible plane curve than remain inert. Note that in the classical case, the natural density does not exist and one must work with logarithmic density. Hence, it is quite remarkable that in the case of function fields, we can work with the natural density as defined above.

In §2.4, we state the general result for existence of a certain limiting distribution μ that is constructed from $E_{m;a_1}(X), \ldots, E_{m;a_r}(X)$, for $a_1, \ldots, a_r$ in $\mathbb{F}[T]$ representing distinct classes in $(\mathbb{F}[T]/m)^*$ (see Theorem 2.14). As before, under LI for all non-principal characters, we find a formula (Theorem 2.15) of the Fourier transform of μ. From this, we can deduce that, if we define $P_{m;a_1,\ldots,a_r}$ to be the set of all positive integers X with

$$\sum_{N=1}^{X} \pi(a_1, m, N) > \sum_{N=1}^{X} \pi(a_2, m, N) > \cdots > \sum_{N=1}^{X} \pi(a_r, m, N),$$

then the limit

$$\delta(P_{m;a_1,\ldots,a_r}) := \lim_{X\to\infty} \frac{\#(P_{m;a_1,\ldots,a_r} \cap \{1, 2, \ldots, X\})}{X}$$

is equal to $\mu(\{x_1 > \cdots > x_r\} \subset \mathbb{R}^r)$, hence always exists.

In the last section, §2.6, we have proved analogues of Theorems 1.6, 1.4, and 1.5 of [RS94]. The first and the third (Theorems 2.20 and 2.23) describe certain central limit behaviours. Essentially, we see that as the degree of m goes to infinity, the bias dissipates. The second analogue (Theorem 2.21) gives the necessary and sufficient conditions for the density function of μ to remain unchanged under permutations of $(x_1, \ldots, x_r)$.

2.2 The asymptotic formula

In this section, we want to find an asymptotic formula of $E_{m;a}(X)$ as $X \to \infty$. By Theorem 1.7,

$$\pi(N) = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right) \tag{2.2}$$

and

$$\pi(a, m, N) = \frac{1}{\Phi(m)}\frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right). \tag{2.3}$$

For a proof of (2.3), see [Ros13, Theorem 4.8].

We will estimate $\Phi(m)\pi(a,m,N)-\pi(N)$ in (2.1) by calculating the coefficients of the power series of $\sum_\chi \bar{\chi}(a)u\frac{d}{du}\log\mathcal{L}(u,\chi)$ for all Dirichlet characters χ modulo m. For each character χ, define the numbers $c_N(\chi)$ by the equation

$$u\frac{d}{du}\log\mathcal{L}(u,\chi)=\sum_{N=1}^{\infty}c_N(\chi)u^N$$

From the Euler product $L(s,\chi)=\prod_{P\nmid m}(1-\chi(P)|P|^{-s})^{-1}$, we have

$$\mathcal{L}(u,\chi)=\prod_{d=1}^{\infty}\prod_{\substack{P\nmid m\\ \deg(P)=d}}(1-\chi(P)u^d)^{-1}. \tag{2.4}$$

Hence,

$$\begin{aligned}u\frac{d}{du}\log\mathcal{L}(u,\chi)&=u\frac{d}{du}\sum_{d=1}^{\infty}\sum_{\substack{P\nmid m\\ \deg(P)=d}}\log\left(1-\chi(P)u^d\right)^{-1}\\&=\sum_{d=1}^{\infty}\sum_{k=1}^{\infty}\sum_{\substack{P\nmid m\\ \deg(P)=d}}d\chi(P^k)u^{dk}\\&=\sum_{N=1}^{\infty}\left(\sum_{d\mid N}d\sum_{\substack{P\nmid m\\ \deg(P)=d}}\chi(P^{N/d})\right)u^N.\end{aligned}$$

From this, we obtain

$$c_N(\chi)=\sum_{d\mid N}d\sum_{\substack{P\nmid m\\ \deg(P)=d}}\chi(P^{N/d}). \tag{2.5}$$

Summing over all Dirichlet characters modulo m, we get

$$\sum_\chi\bar{\chi}(a)c_N(\chi)=\sum_{d\mid N}d\sum_{\substack{P\nmid m\\ \deg(P)=d}}\sum_\chi\bar{\chi}(a)\chi(P^{N/d}). \tag{2.6}$$

Let us introduce a notation to simplify the summation:

$$\pi(a,m,d,k):=\#\{P|P^k\equiv a \bmod m,\deg(P)=d\},$$

for any positive integers k and d. Clearly,

$$\pi(a,m,d,1)=\pi(a,m,d) \tag{2.7}$$

As in [RS94], we define

$$c(m,a):=-1+\sum_{\substack{b^2\equiv a \bmod m\\ b\in(\mathbb{F}[T]/m)^*}}1 \tag{2.8}$$

to simplify $\pi(a,m,d,2)$. If m is irreducible, the second term in the definition of $c(m,a)$ will be 0 if a is not a square residue and 2 if it is a square residue. Therefore, $c(m,a)$ is just the non-principal real quadratic character mod m. In general, $c(m,a)+1$ is

the number of square roots of a in $(\mathbb{F}[T]/m)^*$. So, from (2.3),

$$\pi(a,m,d,2) = \frac{c(m,a)+1}{\Phi(m)}\frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right). \tag{2.9}$$

From (2.2), for an arbitrary k, we have the trivial estimate

$$\pi(a,m,d,k) \leq \pi(d) = O\left(\frac{q^d}{d}\right). \tag{2.10}$$

By the definition of $\pi(a,m,d,k)$ and the orthogonality relations in Proposition 1.3, we can write (2.6) as

$$\sum_{\chi} \bar{\chi}(a) c_N(\chi) = \sum_{d|N} d\Phi(m)\pi(a,m,d,N/d)$$

We separate out the terms for $d = N$ and $d = N/2$ (which exists only when N is even) from above. By (2.7), the term corresponding to $d = N$ is $N\Phi(m)\pi(a,m,N)$. (2.9) implies that the term corresponding to $d = N/2$ (when N is even) is equal to

$$\frac{N}{2}\Phi(m)\left(\frac{c(m,a)+1}{\Phi(m)}.\frac{q^{N/2}}{N/2} + O(\frac{q^{N/4}}{N}\right) = (c(m,a)+1)q^{N/2} + O(q^{N/4}).$$

We now need to estimate the sum of the terms with $d < N/2$. Using (2.10) and the summation formula for a geometric progression, we have

$$\begin{aligned}\sum_{\substack{d|N \\ d\leq N/3}} d\Phi(m)\pi(a,m,d,N/d) &\leq \sum_{\substack{d|N \\ d\leq N/3}} dO\left(\frac{q^d}{d}\right) \\ &= \sum_{d\leq N/3} O(q^d) \\ &= O(q^{N/3}).\end{aligned}$$

Therefore, we proved that, for even N,

$$\sum_{\chi} \bar{\chi}(a) c_N(\chi) = N\Phi(m)\pi(a,m,N) + (c(m,a)+1)q^{N/2} + O(q^{N/3}) \tag{2.11}$$

and, if N is odd,

$$\sum_{\chi} \bar{\chi}(a) c_N(\chi) = N\Phi(m)\pi(a,m,N) + O(q^{N/3}). \tag{2.12}$$

Now, we will give another estimate of $\sum_{\chi} \bar{\chi}(a) c_N(\chi)$. Assuming that χ is a non-principal Dirichlet character mod m, we can write (using Proposition 1.10)

$$\mathcal{L}(u,\chi) = \prod_{\nu=1}^{d(\chi)} (1 - \alpha(\chi,\nu)u). \tag{2.13}$$

Here, $d(\chi)$ is the degree of $\mathcal{L}(u,\chi)$ as a polynomial in u and $\alpha(\chi,\nu)$ are complex numbers called *inverse zeros* of $\mathcal{L}(u,\chi)$. They have absolute values either $\sqrt{q}$ or 1. This is a consequence of a theorem of Weil, the function field analogue of the Riemann

hypothesis (see [Ros13, Theorem 5.10]). From (2.13), we obtain

$$u\frac{d}{du}\log\mathcal{L}(u,\chi) = -\sum_{N=1}^{\infty}\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N u^N.$$

Now, recall the definition of the numbers $c_N(\chi)$. It gives us

$$c_N(\chi) = -\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N, \tag{2.14}$$

for a non-principal character χ. For the principal character χ_0, we can use (1.1) and (1.4) to get

$$\mathcal{L}(u,\chi_0) = \frac{\prod_{P|m}(1-u^{\deg(P)})}{1-qu}.$$

This gives us

$$\begin{aligned} u\frac{d}{du}\log\mathcal{L}(u,\chi_0) &= u\left(\sum_{P|m}\frac{-\deg(P)u^{\deg(P)-1}}{1-u^{\deg(P)}}\right) \\ &= -\deg(P)\sum_{P|m}\sum_{k=1}^{\infty}u^{k\deg(P)} + \sum_{k=1}^{\infty}q^k u^k. \end{aligned}$$

The coefficient of u^N in the first sum is clearly bounded and that in the second term is q^N. Therefore,

$$c_N(\chi_0) = q^N + O(1). \tag{2.15}$$

Summing up, we have proved

$$\sum_{\chi}\bar{\chi}(a)c_N(\chi) = -\sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N + q^N + O(1). \tag{2.16}$$

Proposition 2.1. *Define* $\mathcal{B}(a,m,N)$ *by*

$$\mathcal{B}(a,m,N) := \begin{cases} 0 & \text{if } N \text{ is odd,} \\ c(m,a) & \text{if } N \text{ is even.} \end{cases}$$

Then, we have

$$N(\Phi(m)\pi(a,m,N) - \pi(N)) = -\mathcal{B}(a,m,N)q^{N/2} - \sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N + O(q^{N/3}).$$

Proof. By Corollary 1.6

$$\pi(N) = \frac{1}{N}\sum_{d|N}q^{N/d}\mu(d).$$

Separating out all terms of size $q^{N/2}$ or larger, we write this as

$$\pi(N) = \begin{cases} (q^N - q^{N/2})/N + O(q^{N/3}/N) & \text{if } N \text{ is even,} \\ q^N/N + O(q^{N/3}/N) & \text{if } N \text{ is odd.} \end{cases} \tag{2.17}$$

If N is odd, we use (2.12), (2.16) and (2.17) to obtain

$$\begin{aligned} N(\Phi(m)\pi(a,m,N)-\pi(N)) &= \sum_{\chi}\bar{\chi}(a)c_N(\chi)-q^N+O(q^{N/3}) \\ &= -\sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N+O(q^{N/3}). \end{aligned}$$

Similarly, in the case of even N, we will use (2.11), (2.16) and (2.17) to get

$$N(\Phi(m)\pi(a,m,N)-\pi(N)) = -c(m,a)q^{N/2}-\sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N+O(q^{N/3}),$$

which completes the proof. □

Lemma 2.2. *For any complex number β with $|\beta|>1$,*

$$\lim_{n\to\infty}\frac{n}{\beta^n}\left(\sum_{i=1}^{n}\frac{\beta^i}{i}\right)=\frac{\beta}{\beta-1}.$$

Proof. Let $h(n):=\beta^n$ and $f(x):=1/x$. Also, let $H(x):=\sum_{n\leq x}h(n)$. Then, clearly,

$$H(x)=\beta\cdot\frac{\beta^{[x]}-1}{\beta-1}.$$

To calculate $\sum_{i=1}^{n}\beta^i/i$, we apply the partial summation formula (see [CM05, Theorem 1.3.1]) which gives

$$\sum_{n\leq x}h(n)f(n)=H(x)f(x)-\int_1^x H(t)f'(t)dt.$$

Therefore,

$$\frac{N}{\beta^N}\sum_{n=1}^{N}\frac{\beta^n}{n}=\frac{\beta-\beta^{1-N}}{\beta-1}+\frac{N}{\beta^N}\cdot\beta\cdot\int_1^N\frac{\beta^{[t]}-1}{\beta-1}\frac{1}{t^2}dt,$$

and it remains to show that the second term on the right-hand side above tends to zero as $N\to\infty$. Since $\int_1^\infty(1/t^2)dt<\infty$ and $|\beta^{[t]}|\leq|\beta|^t$, it is sufficient to prove that

$$\frac{N}{\beta^N}\int_1^N\frac{|\beta|^{[t]}}{t^2}dt\to 0$$

as $N\to\infty$. Using integration by parts,

$$\frac{N}{\beta^N}\int_1^N\frac{|\beta|^{[t]}}{t^2}dt=\frac{N}{\beta^N}\frac{1}{\log|\beta|}\left(\frac{|\beta|^N}{N^2}-\frac{|\beta|}{1^2}\right)-\frac{N}{\beta^N}\frac{1}{\log|\beta|}\int_1^N(-2)\frac{|\beta|^t}{t^3}dt.$$

The first term is easily seen to tend to zero as $N\to\infty$, and, again, we only need to show

$$\frac{N}{\beta^N}\int_1^N\frac{|\beta|^t}{t^3}dt\to 0.$$

To do so,

$$\begin{aligned}\int_1^N \frac{|\beta|^t}{t^3}dt &= \int_1^{N/2} \frac{|\beta|^t}{t^3}dt + \int_{N/2}^N \frac{|\beta|^t}{t^3}dt \\ &\le \int_1^{N/2} \frac{|\beta|^{N/2}}{t^3}dt + \int_{N/2}^N \frac{|\beta|^N}{t^3}dt \\ &\le k\cdot|\beta|^{N/2} + |\beta|^N \cdot \left(\frac{-2}{N^2} - \frac{(-2)}{(N/2)^2}\right)\end{aligned}$$

for a constant k. We multiply N/β^N on both sides of this inequality, and this completes the proof. □

Corollary 2.3. *Define* $\mathcal{B}(N)$ *by*

$$\mathcal{B}(N) := \begin{cases} 0 & \text{if } N \text{ is odd,} \\ 1 & \text{if } N \text{ is even.}\end{cases}$$

Then

$$\frac{X}{q^{X/2}}\sum_{N=1}^{X}\mathcal{B}(N)\frac{q^{N/2}}{N} = \begin{cases} \sqrt{q}/(q-1)+o(1) & \text{if } X \text{ is odd,} \\ q/(q-1)+o(1) & \text{if } X \text{ is even.}\end{cases}$$

Proof. Suppose that X is even, $X = 2X'$. Since $\mathcal{B}(N)$ is zero for all odd N we have that

$$\begin{aligned}\frac{X}{q^{X/2}}\sum_{N=1}^{X}\mathcal{B}(N)\frac{q^{N/2}}{N} &= \frac{2X'}{q^{X'}}\sum_{n=1}^{X'}\frac{q^n}{2n} \\ &= \frac{q}{q-1}+o(1),\end{aligned}$$

where we use Lemma 2.2 for the last equality.

For an odd $X = 2X'+1$, we proceed similarly:

$$\begin{aligned}\frac{X}{q^{X/2}}\sum_{N=1}^{X}\mathcal{B}(N)\frac{q^{N/2}}{N} &= \frac{1}{\sqrt{q}}\frac{2X'+1}{q^{X'}}\sum_{n=1}^{X'}\frac{q^n}{2n} \\ &= \frac{\sqrt{q}}{q-1}+o(1),\end{aligned}$$

again, by Lemma 2.2. □

Corollary 2.4. *Let* γ *be a complex number with absolute value* $\sqrt{q}$ *and argument* θ*, that is* $\gamma = \sqrt{q}e^{i\theta}$*. Then*

$$\frac{X}{q^{X/2}}\sum_{N=1}^{X}\frac{\gamma^N}{N} = e^{i\theta X}\frac{\gamma}{\gamma-1}+o(1).$$

Proof. This is straightforward from Lemma 2.2, because

$$\frac{X}{q^{X/2}}\sum_{N=1}^{X}\frac{\gamma^N}{N} = X\frac{e^{i\theta X}}{\gamma^X}\frac{\gamma^N}{N} = e^{i\theta X}\frac{\gamma}{\gamma-1}+o(1).$$

□

Theorem 2.5. *Define* $\mathcal{B}_q(X)$ *by*

$$\mathcal{B}_q(X) := \begin{cases} \sqrt{q}/(q-1) & \text{if } X \text{ is odd,} \\ q/(q-1) & \text{if } X \text{ is even.} \end{cases}$$

Then

$$E_{m;a}(X) = -c(m,a)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \bar{\chi}(a) \sum_{\gamma_\chi} \left(e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} \right) + o(1),$$

as $X \to \infty$*, where* χ *denotes a non-principal Dirichlet character,* γ_χ *denotes an inverse zero of* $\mathcal{L}(u,\chi)$ *and* $\theta(\gamma_\chi)$ *denotes the argument of* γ_χ*.*

Proof. From Proposition 2.1, we know that we need to estimate the following three sums:

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \mathcal{B}(a,m,N) \frac{q^{N/2}}{N}, \quad \frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\bar{\chi}(a)\alpha(\chi,\nu)^N}{N}, \quad \frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{O(q^{N/3})}{N}.$$

The third sum is $o(1)$ because

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{O(q^{N/3})}{N} \leq \frac{X}{q^{X/2}} O(q^{X/3}) \sum_{N=1}^{X} \frac{1}{N} = \frac{X}{q^{X/2}} O(Xq^{X/3}).$$

Now, note that $\mathcal{B}(a,m,N) = c(m,a)\mathcal{B}(N)$ and so Corollary 2.3 gives us that the first sum is equal to $c(m,a)\mathcal{B}_q(X) + o(1)$. It remains to estimate the second sum. As mentioned earlier, the inverse zeros of $\mathcal{L}(u,\chi)$ have absolute values either $\sqrt{q}$ or 1. When $|\alpha(\chi,\nu)| = 1$, the second sum (its absolute value) is clearly $o(1)$. If $|\alpha(\chi,\nu)| = \sqrt{q}$, then we write $\alpha(\chi,\nu) = \gamma_\chi = \sqrt{q}e^{i\theta(\gamma_\chi)}$. From Corollary 2.4, we obtain

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\bar{\chi}(a)\alpha(\chi,\nu)^N}{N} = \frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\bar{\chi}(a){\gamma_\chi}^N}{N} = \bar{\chi}(a)e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} + o(1).$$

Summing this over all the inverse zeros and over all non-principal characters gives the second term in the expression for $E(m;a)$ (which has to be real since all the other terms are). Finally, we combine the three sums with appropriate signs to prove the theorem. □

2.3 The quadratic character and its applications

In this section, we assume that m is irreducible. We obtain an asymptotic formula (Theorem 2.6) for a counting function ($E_{m;R,N}(X)$) measuring the number of prime quadratic residues minus prime quadratic non-residues. In [Cha08], it is suggested that it may be possible to obtain Theorem 2.6 from Theorem 2.5 and so we have given a different proof here from the one given in the above cited paper.

As earlier, define $a(N)$ and $b(N)$ by

$$a(N) := \#\{P \in \mathbb{F}[T] | \chi_{\text{quad}}(P) = 1, \deg(P) = N\}$$
$$b(N) := \#\{P \in \mathbb{F}[T] | \chi_{\text{quad}}(P) = -1, \deg(P) = N\}.$$

Also, define

$$E_{m;R,N}(X) := \frac{X}{q^{X/2}} \sum_{N=1}^{X} (a(N) - b(N)).$$

Let χ_{quad} be the non-principal real quadratic character mod m. We enumerate, among all of the inverse zeros $\{\alpha(\chi_{\text{quad}}, \nu)\}_{\nu=1}^{M-1}$ of $\mathcal{L}(u, \chi_{\text{quad}})$, those whose absolute values are $\sqrt{q}$ as $\gamma_1, \bar{\gamma}_1, \ldots, \gamma_k, \bar{\gamma}_k$. Then we have the following asymptotic formula.

Theorem 2.6. *Let $\mathcal{B}_q(X)$ be defined as in Theorem 2.5. Then we have*

$$E_{m;R,N}(X) = -\mathcal{B}_q(X) - 2\sum_{j=1}^{k} \Re\left(e^{i\theta_j X} \frac{\gamma_j}{\gamma_j - 1}\right) + o(1),$$

as $X \to \infty$.

Proof. Since m is irreducible, we clearly have

$$a(N) + b(N) = \pi(N),$$

if $N \neq M$ (which we recall as the degree of m). Also,

$$\begin{aligned} a(N) &= \sum_{\substack{t \\ \chi_{\text{quad}}(t)=1}} \pi(t, m, N) \\ b(N) &= \sum_{\substack{t \\ \chi_{\text{quad}}(t)=-1}} \pi(t, m, N). \end{aligned}$$

For convenience, let us denote the set of squares by S and the set of non-squares by NS. Then

$$\begin{aligned} \frac{q^{X/2}}{X} E_{m;R,N}(X) &= \sum_{N=1}^{X} \left(\sum_{t \in S} \pi(t, m, N) - \sum_{t \in NS} \pi(t, m, N)\right) \\ \Phi(m)\frac{q^{X/2}}{X} E_{m;R,N}(X) &= \sum_{N=1}^{X} \left(\sum_{t \in S} (\Phi(m)\pi(t, m, N) - \pi(N))\right) \\ &\quad - \sum_{N=1}^{X} \left(\sum_{t \in NS} (\Phi(m)\pi(t, m, N) - \pi(N))\right) + O(X), \end{aligned}$$

where the $O(X)$ term arises because the number of squares and non-squares might not be equal. Interchanging the order of summation, we get

$$\Phi(m)\frac{q^{X/2}}{X} E_{m;R,N}(X) = \frac{q^{X/2}}{X} \sum_{t \in S} E_{m;t}(X) - \frac{q^{X/2}}{X} \sum_{t \in NS} E_{m;t}(X) + O(X),$$

and so

$$\Phi(m) E_{m;R,N}(X) = \sum_{t \in S} E_{m;t}(X) - \sum_{t \in NS} E_{m;t}(X) + o(1).$$

Now we can invoke Theorem 2.5. This will give us

$$E_{m;R,N}(X) = \frac{1}{\Phi(m)} \sum_{t \in S} \left(-c(m,t)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \bar{\chi}(t) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} \right)$$
$$- \frac{1}{\Phi(m)} \sum_{t \in NS} \left(-c(m,t)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \bar{\chi}(t) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} \right) + o(1).$$

To simplify the expression we will denote $\sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1}$ by $I(\chi)$ (it is also dependent on X but for the summation only χ matters). Recall that $c(m,t)$ is the non-principal real quadratic character mod m. Therefore,

$$E_{m;R,N}(X) = \frac{1}{\Phi(m)} \sum_{t} -\mathcal{B}_q(X) - \frac{1}{\Phi(m)} \left(\sum_{t \in S} \sum_{\chi \neq \chi_0} \bar{\chi}(t) I(\chi) - \sum_{t \in NS} \sum_{\chi \neq \chi_0} \bar{\chi}(t) I(\chi) \right) + o(1).$$

The first term is just $-\mathcal{B}_q(X)$. In the second term, we can again interchange the order of summation.

$$E_{m;R,N}(X) = -\mathcal{B}_q(X) - \frac{1}{\Phi(m)} \left(\sum_{\chi \neq \chi_0} I(\chi) \left(\sum_{t \in S} \bar{\chi}(t) - \sum_{t \in NS} \bar{\chi}(t) \right) \right) + o(1).$$

We can rewrite $\sum_{t \in S} \bar{\chi}(t) - \sum_{t \in NS} \bar{\chi}(t)$ as $\sum_{t} \chi_{\text{quad}}(t)\bar{\chi}(t)$. By Proposition 1.3, this is equal to $\Phi(m)\delta(\chi_{\text{quad}}, \chi)$. So we end up with

$$\begin{aligned} E_{m;R,N}(X) &= -\mathcal{B}_q(X) - I(\chi_{\text{quad}}) + o(1) \\ &= -\mathcal{B}_q(X) - \Re(I(\chi)) + o(1). \end{aligned}$$

Using the enumeration of inverse zeros described earlier, we get the statement of the theorem. □

By Proposition 1.12, $\mathcal{L}(u, \chi_{\text{quad}})$ is a polynomial in u of degree $M-1$ (since m is irreducible) and so there will be $k = [(M-1)/2]$ pairs of inverse zeros.

Corollary 2.7. *For $M = 2$, $E_{m;R,N}(X) < 0$ for almost all X (i.e. all but finitely many X).*

This is true because for $M = 2$, the L-series has no inverse zeros with absolute values equal to $\sqrt{q}$ (see Proposition 1.12). This means that the prime non-residues predominate over prime residues.

Define

$$E^{(T)}(X) := -\mathcal{B}_q(X) - 2 \sum_{j=1}^{k} \Re \left(e^{i\theta_j X} \frac{\gamma_j}{\gamma_j - 1} \right) \tag{2.18}$$

so that $\epsilon_*(X) := E_{m;R,N}(X) - E^{(T)}(X)$ is $o(1)$ by Theorem 2.6.

Lemma 2.8. *For any continuous bounded function f on $\mathbb{R}$, the limit*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{X=1}^{N} f(E^{(T)}(X))$$

exists.

Proof. We denote the corresponding arguments of $\gamma_1, \ldots, \gamma_k$ as $\theta_1, \ldots, \theta_k$. Define $b_0, b_1, \ldots, b_k \in \mathbb{C}$ by

$$b_0 := -1$$

and

$$b_j := -\frac{\gamma_j}{\gamma_j - 1}$$

for $j = 1, \ldots, k$. Also define a function g on $\mathbb{R}^{k+1}$ by

$$g(\boldsymbol{x}) = g(x_0, x_1, \ldots, x_k) := f\left(b_0 \frac{q^{(3+\cos(2\pi x_0))/4}}{q-1} + 2\sum_{j=1}^{k} \Re(e^{2\pi i x_j} b_j)\right).$$

Then g gives rise to a continuous function on $\mathbb{R}^{k+1}/\mathbb{Z}^{k+1}$ and clearly

$$f(E^{(T)}(X)) = g\left(\frac{X}{2}, \frac{\theta_1 X}{2\pi}, \ldots, \frac{\theta_k X}{2\pi}\right).$$

Let

$$\Gamma := \left\{ \left(\frac{X}{2}, \frac{\theta_1 X}{2\pi}, \ldots, \frac{\theta_k X}{2\pi}\right) \in \mathbb{R}^{k+1}/\mathbb{Z}^{k+1} \,\middle|\, X = 1, 2, 3, \ldots \right\}. \tag{2.19}$$

Then, by Kronecker-Weyl Theorem, Γ is equidistributed in its topological closure $\bar{\Gamma}$, and we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} f(E^{(T)}(X)) = \int_{\bar{\Gamma}} g(\boldsymbol{x}) d\boldsymbol{x}. \tag{2.20}$$

where $d\boldsymbol{x}$ is the normalized Haar measure on $\bar{\Gamma}$. □

Theorem 2.9. *There exists a probability measure $\mu_{m;R,N}$ on all Borel sets in $\mathbb{R}$ such that*

$$\mu_{m;R,N}(f) = \lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} f(E_{m;R,N}(X)),$$

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

The proof of this theorem is along the lines of the proof of [Cha08, Theorem 3.2]. Here, we abbreviate $E_{m;R,N}(X)$ to $E(X)$ and the probability measure $\nu_N := m_N {E^{(T)}}^{-1}$ is defined on $\mathbb{R}$ (where m_N is the probability measure on the set $\{1, \ldots, N\}$ with $m_N(\{1\}) = \cdots = m_N(\{N\}) = 1/N$). The rest of the elements of the proof are identical.

Definition 2.10 (Linear Independence Hypothesis)**.** *Consider a set $\mathcal{I} = \{\chi \neq \chi_0\}$ of non-principal Dirichlet characters modulo m, which is closed under complex conjugation. Then we say that $\mathcal{I}$ satisfies LI if the set*

$$\{\theta | \gamma = \sqrt{q} e^{i\theta} \text{ is an inverse zero of } \mathcal{L}(u, \chi) \text{ for some } \chi \in \mathcal{I} \text{ with } 0 \leq \theta \leq \pi\} \cup \{2\pi\}$$

is linearly independent over $\mathbb{Q}$.

Theorem 2.11. *Assume that the set $\{\chi_{quad}\}$ satisfies LI. Then the Fourier transform $\hat{\mu}_{m;R,N}$ of $\mu_{m;R,N}$ is given by*

$$\hat{\mu}_{m;R,N}(\xi) = \mathcal{B}_{m;R,N}(\xi) \prod_{j=1}^{k} J_0\left(\left|\frac{2\gamma_j}{\gamma_j - 1}\right| \xi\right),$$

where

$$J_0(z) = \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{(n!)^2}$$

is the Bessel function of the first kind, and

$$\mathcal{B}_{m;R,N}(\xi) := \frac{1}{2}\left(\exp\left(i\frac{\sqrt{q}}{q-1}\xi\right) + \exp\left(i\frac{q}{q-1}\xi\right)\right).$$

Proof. We again use the enumeration of inverse zeros described previously. We also abbreviate $\mu_{m;R,N}$ as μ. The main consequence of LI for us is that the $\bar{\Gamma}$ in (2.19) is the union of two copies of a k-torus, more precisely,

$$\begin{aligned}\bar{\Gamma} =& \{(0, x_1, \ldots, x_k) \in \mathbb{R}^{k+1}/\mathbb{Z}^{k+1} | (x_1, \ldots, x_k) \ in \mathbb{R}^k/\mathbb{Z}^k\} \\ & \cup \{(1/2, x_1, \ldots, x_k) \in \mathbb{R}^{k+1}/\mathbb{Z}^{k+1} | (x_1, \ldots, x_k) \ in \mathbb{R}^k/\mathbb{Z}^k\}. \end{aligned} \tag{2.21}$$

Also, the normalized Haar measure $d\boldsymbol{x}$ on $\bar{\Gamma}$ is simply half of the usual Lebesgue measure on each k-torus.

Now, using Theorem 2.9, (2.20) and (2.21)

$$\hat{\mu}(\xi) = \int_{\mathbb{R}} e^{-i\xi x} d\mu(x) = \mathcal{B}_{m;R,N}(\xi) \prod_{j=1}^{k} \hat{\mu}_j(\xi) \tag{2.22}$$

where $\mu_1, \ldots, \mu_k$ is the distribution

$$-\left(2\Re\left(e^{i\theta_1 X}\frac{\gamma_1}{\gamma_1 - 1}\right), \ldots, 2\Re\left(e^{i\theta_k X}\frac{\gamma_k}{\gamma_k - 1}\right)\right)$$

of the terms in (2.18). Let ω_j be the argument of $\gamma_j/(\gamma_j - 1)$. Further, let $R_j := \left|\frac{2\gamma_j}{\gamma_j - 1}\right|$. Then we can write the distribution as

$$-(R_1 \cos(\theta_1 X + \omega_1), \ldots, R_k \cos(\theta_k X + \omega_k))$$

Then, as in [RS94, § 3.1] (also, see the proof of [Cha08, Theorem 3.4]),

$$\begin{aligned}\hat{\mu}_j(\xi) &= \frac{1}{\pi}\int_{-1}^{1} \cos\left(R_j \xi \sqrt{1-t^2}\right) \frac{dt}{\sqrt{1-t^2}} \\ &= J_0(R_j \xi).\end{aligned}$$

□

Note that J_0 is an even function and so is

$$\prod_{j=1}^{k} J_0\left(\left|\frac{2\gamma_j}{\gamma_j - 1}\right| \xi\right).$$

If we split the integral representing the inverse fourier transform of $2\hat{\mu}_{m;R,N}$ into two parts corresponding to the two terms of $2\mathcal{B}_{m;R,N}$,

$$\begin{aligned}2\mu_{m;R,N}(x) &= 2\int_{\mathbb{R}} e^{i\xi x}\mathcal{B}_{m;R,N}(\xi)\prod_{j=1}^{k} J_0\left(\left|\frac{2\gamma_j}{\gamma_j-1}\right|\xi\right)d\xi \\ &= \int_{\mathbb{R}} \exp\left(i\xi\left(x+\frac{\sqrt{q}}{q-1}\right)\right)\prod_{j=1}^{k} J_0\left(\left|\frac{2\gamma_j}{\gamma_j-1}\right|\xi\right)d\xi \\ &+ \int_{\mathbb{R}} \exp\left(i\xi\left(x+\frac{q}{q-1}\right)\right)\prod_{j=1}^{k} J_0\left(\left|\frac{2\gamma_j}{\gamma_j-1}\right|\xi\right)d\xi,\end{aligned}$$

then we find that the first integral is symmetric about $x=-\frac{\sqrt{q}}{q-1}<0$ and the second integral is symmetric about $x=-\frac{q}{q-1}<0$. Since $\mu_{m;R,N}$ is the average of the two integrals, we have

$$\mu_{m;R,N}(-\infty,0]>\frac{1}{2}.$$

In other words, the primes are biased toward quadratic non-residues, if we assume that LI holds on $\{\chi_{\text{quad}}\}$.

As an application of Theorem 2.6, we consider the double covering $C\longrightarrow \mathbb{A}^1_{\mathbb{F}}$ where C is an affine plane curve defined by the equation $y^2=m$ for a fixed irreducible monic $m\in\mathbb{F}[T]$ and $\mathbb{A}^1_{\mathbb{F}}$ is the affine line over $\mathbb{F}$. Define

$$\begin{aligned}a'(N) &:= \#\{P\in\mathbb{F}[T]|(m/P)=1,\deg(P)=N\},\\ b'(N) &:= \#\{P\in\mathbb{F}[T]|(m/P)=-1,\deg(P)=N\},\end{aligned}$$

and

$$E_{m;S,I}(X) := \frac{X}{q^{X/2}}\sum_{N=1}^{X}(a'(N)-b'(N)).$$

The function $E_{m;S,I}(X)$ counts the number of primes of $\mathbb{A}^1_{\mathbb{F}}$ splitting in C minus that of primes remaining inert in C, whose degrees are up to N. By Theorem 1.2 (for $d=2$), we have

$$\left(\frac{m}{P}\right)=(-1)^{M\deg(P).(q-1)/2}\left(\frac{P}{m}\right). \tag{2.23}$$

Therefore, if either M is even or $q\equiv 1(\text{mod }4)$, then $(m/P)=(P/m)$ for all P, and $E_{m;S,I}(X)=E_{m;R,N}(X)$. So in this case, the prime number race between splitting primes and inert primes is the same as prime residues and non-residues. For M odd and $q\equiv 3(\text{mod }4)$. Then,

$$\left(\frac{m}{P}\right)=(-1)^{\deg(P)}\left(\frac{P}{m}\right),$$

which implies

$$a'(N)-b'(N)=(-1)^N(a(N)-b(N)).$$

This gives us (see [Cha08, Proposition 4.2] and [Cha08, Theorem 4.3])

Theorem 2.12.

$$E_{m;S,I}(X)=-\mathcal{B}_q(X)-2\sum_{j=1}^{k}\Re\left(e^{i(\pi-\theta_j)X}\frac{\gamma_j}{\gamma_j-1}\right)+o(1), \tag{2.24}$$

as $X \to \infty$.

Hence, we see that the splitting primes outnumber the inert primes.

2.4 Limiting distribution

In this section, we look at the limiting distribution in the general case. The proofs of the results have been omitted since they are quite similar to the proofs in the quadratic character case which has been dealt with in the previous section. The omitted proofs in this section can be found in [Cha08, § 3].

Let $a_1, \dots, a_r$ be elements of $\mathbb{F}[T]$ prime to m, representing distinct residue classes modulo m. Define the vector-valued function

$$E_{m;a_1,\dots,a_r}(X) := (E_{m;a_1}(X), \dots, E_{m;a_r}(X)).$$

Define

$$E^{(T)}(X) := (E_1^{(T)}(X), \dots, E_r^{(T)}(X))$$

where

$$E_l^{(T)}(X) := -c(m,a)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \bar{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1}$$

for $l = 1, \dots, r$, and $\epsilon_*(X) := (E_{m;a_1}(X) - E_1^{(T)}(X), \dots, E_{m;a_r}(X) - E_r^{(T)}(X))$. By Theorem 2.5, $|\epsilon_*(X)| = o(1)$.

Lemma 2.13. *For any continuous bounded function* f *on* $\mathbb{R}^r$*, the limit*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} f(E^{(T)}(X))$$

exists.

Theorem 2.14. *There exists a probability measure* $\mu = \mu_{m;a_1,\dots,a_r}$ *on Borel sets in* $\mathbb{R}^r$ *such that*

$$\mu(f) = \lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} f(E_{m;a_1,\dots,a_r}(X))$$

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

Theorem 2.15. *Assume that the set of all non-principal Dirichlet characters mod* m *satisfies LI. Then, the Fourier transform* $\hat{\mu}$ *of the measure* μ *in Theorem 2.14 is given by*

$$\hat{\mu}(\xi) = \mathcal{B}_{m;a_1,\dots,a_r}(\xi) \prod_{\chi \neq \chi_0} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right| \left|\sum_{l=1}^{r} \chi(a_l)\xi_l\right|\right),$$

where

$$J_0(z) = \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{(n!)^2}$$

is the Bessel function of the first kind, and

$$\mathcal{B}_{m;a_1,\dots,a_r}(\xi) := \frac{1}{2}\left(\exp\left(i\frac{\sqrt{q}}{q-1}\sum_{l=1}^{r} c(m,a_l)\xi_l\right) + \exp\left(i\frac{q}{q-1}\sum_{l=1}^{r} c(m,a_l)\xi_l\right)\right).$$

The term $\mathcal{B}_{m;a_1,\dots,a_r}(\xi)$ in the above theorem is the cause of the bias.

2.5 Violation of the LI and examples

In the number field case, LI is conjectured to always hold but in the function field case, LI can be violated (as in the first three examples of this section), and the bias can be any of the following: towards squares, non-squares, or non-existent. However, the results in [Cha08] are still significant since LI holds for the roots of the L-functions of most algebraic curves as we will show in Chapter 3.

In this section, we continue to assume that m is irreducible. When the degree of m is small, it is possible to calculate $L(s, \chi_{\text{quad}})$ explicitly.

Example 2.16. *Let $p = 3$ and $m = T^3 + 2T + 1$. Then, we have*

$$\mathcal{L}(u) = 3u^2 - 3u + 1 = \left(1 - \frac{3+\sqrt{3}i}{2}u\right)\left(1 - \frac{3-\sqrt{3}i}{2}u\right).$$

Therefore, the only inverse zero (with argument between 0 and π) is

$$\gamma_1 = \frac{3+\sqrt{3}i}{2} = \sqrt{3}e^{i\pi/6}.$$

In particular, LI is violated. We now compute $E_{m;R,N}(X)$ using Theorem 2.6. It is easy to verify the following.

X mod 12	$E_{m;R,N}(X) (\text{mod } o(1))$
0 or 2	$-9/2$
1	$-5\sqrt{3}/2$
3 or 11	$-3\sqrt{3}/2$
4 or 10	$-3/2$
5 or 9	$\sqrt{3}/2$
6 or 8	$3/2$
7	$3\sqrt{3}/2$

This shows that $E_{m;R,N}(X)$ is negative for 7/12 of all (large enough) positive integers X. The bias is therefore towards non-squares. Also, the measure $\mu_{m;R,N}$ is concentrated at the seven points, more precisely,

$$\mu_{m;R,N}(\{P\}) := \begin{cases} 1/12 & \text{if } P = -5\sqrt{3}/2 \text{ or } P = 3\sqrt{3}/2 \\ 2/12 & \text{if } P = -9/2, -3\sqrt{3}/2, -3/2, \sqrt{3}/2, \text{ or } 3/2, \end{cases}$$

and $\mu_{m;R,N}(A) = 0$ for all A not containing the above points.

Example 2.17. *For $p = 5$ and $m = T^4 + 4T^3 + 4T^2 + 4T + 1$, we have*

$$\mathcal{L}(u) = -5u^3 + 5u^2 - u + 1 = (1-u)(1+5u^2),$$

and

$$\gamma_1 = \sqrt{5}i = \sqrt{5}e^{i\pi/2}.$$

The results are as follows.

Since the measure $\mu_{m;R,N}$ is concentrated evenly in this example, there is no bias.

X mod 4	$E_{m;R,N}(X)(\text{mod } o(1))$
0	$-35/12$
1	$-7\sqrt{5}/12$
2	$5/12$
3	$\sqrt{5}/12$

Example 2.18. *Taking $p = 5$ and $m = T^5 + 3T^4 + 4T^3 + 2T + 2$, we have*

$$\begin{aligned}\mathcal{L}(u) &= 25u^4 - 25u^3 + 15u^2 - 5u + 1\\ &= \left(1 + \frac{5+\sqrt{5}}{2}u + 5u^2\right)\left(1 - \frac{5-\sqrt{5}}{2}u + 5u^2\right)\\ &= (1 - 2\sqrt{5}\cos(4\pi/5)u + 5u^2)(1 - 2\sqrt{5}\cos(2\pi/5)u + 5u^2).\end{aligned}$$

and so

$$\gamma_1 = \sqrt{5}e^{i2\pi/5} \text{ and } \gamma_2 = \sqrt{5}e^{i4\pi/5}.$$

Using these, we can verify the following. Here, for more than half the values of X,

X mod 10	(Approximate value of) $E_{m;R,N}(X)(\text{mod } o(1))$
0	-5.80
1	-4.83
2	-2.16
3	1.27
4	0.57
5	0.25
6	0.11
7	2.29
8	1.02
9	-1.79

$E_{m;R,N}(X)$ is positive and so the bias is towards squares.

We now give an example where LI holds.

Example 2.19. *Take $q = 3$ and $m = T^4 + 2T^3 + 2T^2 + T + 2$. Then*

$$\mathcal{L}(u) = -3u^3 + 5u^2 - 3u + 1,$$

and

$$\gamma_1 = 1 + i\sqrt{2} = \sqrt{3}e^{i\theta}$$

where $\theta = \tan^{-1}\sqrt{2}$. $\sqrt{2}$ is not in the list of quadratic irrational numbers that can arise as values of the tangent function at rational multiple values of π (see [Cal06]). Therefore, $(\tan^{-1}\sqrt{2})/\pi$ is irrational and LI holds.

We compute $\mu_{m;R,N}(-\infty, 0]$ for the case $k = 1$. Let $\tilde{\mu}$ be a measure whose Fourier transform is $J_0(2r\xi)$, with $r := |\gamma_1/(\gamma - 1)|$. Then the density of $\tilde{\mu}$ is given by

$$\begin{cases} \frac{1}{2r}\frac{1}{\sqrt{1-(t/2r)^2}}\frac{1}{\pi} & \text{if } -2r < t < 2r,\\ 0 & \text{otherwise.}\end{cases}$$

Let μ_1 and μ_2 be the shifts of $\tilde{\mu}$ by $-q/(q-1)$ and $-\sqrt{q}/(q-1)$, respectively. Then,

$$\mu_1(-\infty, 0] = \frac{1}{\pi}\left(\sin^{-1}\left(\frac{q}{q-1}\frac{1}{2r}\right) + \frac{\pi}{2}\right) \sim 0.71,$$
$$\mu_2(-\infty, 0] = \frac{1}{\pi}\left(\sin^{-1}\left(\frac{\sqrt{q}}{q-1}\frac{1}{2r}\right) + \frac{\pi}{2}\right) \sim 0.62.$$

Hence,

$$\mu_{m;R,N}(-\infty, 0] = \frac{\mu_1(-\infty, 0] + \mu_2(-\infty, 0]}{2} \sim 0.67$$

which means that the bias is towards non-squares.

2.6 Symmetry and central limit behaviours

Theorem 2.20. *Suppose that m is irreducible of degree M. Assume that LI holds for $\{\chi_{quad}\}$. Let $\tilde{\mu}_{m;R,N}$ be the limiting distribution of*

$$\sqrt{\frac{q-1}{q}}\frac{E_{m;R,N}(X)}{\sqrt{M}}.$$

Then $\tilde{\mu}_{m;R,N}$ converges in measure to the Gaussian $(2\pi)^{-1/2}e^{-X^2/2}dX$ as $M \to \infty$.

Proof. We fix an irreducible m whose degree is M. Recall that, if we enumerate the inverse zeros (whose absolute values are $\sqrt{q}$) of $\mathcal{L}(u, \chi_{\text{quad}})$ as $\{\gamma_1, \bar{\gamma}_1, \ldots, \gamma_k, \bar{\gamma}_k\}$, then $k = [(M-1)/2]$. We will abbreviate $\hat{\mu}_{m;R,N}$ as $\hat{\mu}$ during the proof. From Theorem 2.11, we have

$$\begin{aligned}\log\hat{\mu}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) &= \log\mathcal{B}_{m;R,N}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) \\ &\quad + \sum_{j=1}^{k}\log J_0\left(\left|\frac{2\gamma_j}{\gamma_j - 1}\right|\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) \end{aligned} \tag{2.25}$$

Fix a large constant A. Then, for $|\xi| \le A$,

$$\begin{aligned}\left|\log\mathcal{B}_{m;R,N}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right)\right| &\le \log\left(\exp\left|\frac{i\xi}{\sqrt{q-1}}.\frac{1}{\sqrt{M}}\right| + \exp\left|\frac{i\xi\sqrt{q}}{\sqrt{q-1}}.\frac{1}{\sqrt{M}}\right|\right) \\ &= \log\left(O\left(\exp\frac{A}{\sqrt{M}}\right)\right) \\ &= O\left(\frac{A}{\sqrt{M}}\right), \end{aligned} \tag{2.26}$$

as $M \to \infty$, directly from the definition of $\mathcal{B}_{m;R,N}(\xi)$ in Theorem 2.11. Also, from the power series expansion of $J_0(z) = 1 - \frac{1}{4}z^2 + \cdots$, we see that

$$\sum_{j=1}^{k}\log J_0\left(\left|\frac{2\gamma_j}{\gamma_j - 1}\right|\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) = -\sum_{j=1}^{k}\left|\frac{\gamma_j}{\gamma_j - 1}\right|^2\frac{q-1}{q}\frac{\xi^2}{M} + \cdots \tag{2.27}$$

For all $|\xi| \leq A$, it can be shown that the higher term is $O(A^4/M)$. To estimate the first term, let

$$I := \sum_{j=1}^{k} \left| \frac{\gamma_j}{\gamma_j - 1} \right|^2. \tag{2.28}$$

We define

$$\tilde{\mathcal{L}}(u) = \tilde{\mathcal{L}}(u, \chi_{\text{quad}}) := \prod_{j=1}^{k} (1 - \gamma_j u)(1 - \bar{\gamma}_j u). \tag{2.29}$$

By taking logarithmic derivative of $\tilde{\mathcal{L}}(u)$ and then evaluating at $u = 1$, we obtain

$$-\frac{\tilde{\mathcal{L}}'}{\tilde{\mathcal{L}}}(1) = \sum_{j=1}^{k} \frac{\gamma_j + \bar{\gamma}_j}{|\gamma_j - 1|^2} - 2I.$$

Also,

$$\begin{aligned} k + \sum_{j=1}^{k} \frac{\gamma_j + \bar{\gamma}_j}{|\gamma_j - 1|^2} &= \sum_{j=1}^{k} \left(\frac{\gamma_j + \bar{\gamma}_j}{|\gamma_j - 1|^2} + 1 \right) \\ &= \sum_{j=1}^{k} \frac{\gamma_j + \bar{\gamma}_j + (\gamma_j - 1)(\bar{\gamma}_j - 1)}{|\gamma_j - 1|^2} \\ &= \sum_{j=1}^{k} \frac{1 + |\gamma_j|^2}{|\gamma_j - 1|^2} = \frac{1+q}{q} I. \end{aligned}$$

Therefore, from these two equalities, we deduce

$$I = \frac{q}{q-1} \left(\frac{\tilde{\mathcal{L}}'}{\tilde{\mathcal{L}}}(1) - k \right) \tag{2.30}$$

We can estimate $\tilde{\mathcal{L}}'/\tilde{\mathcal{L}}(1)$ using the functional equation (which can be derived easily from (2.29))

$$\tilde{\mathcal{L}}(u, \chi_{\text{quad}}) = \epsilon(\chi_{\text{quad}}) q^k u^{2k} \tilde{\mathcal{L}}(1/qu, \chi_{\text{quad}}) \tag{2.31}$$

for some constant $\epsilon(\chi_{\text{quad}})$ of absolute value 1. We take the logarithmic derivative of (2.31). Taking into account the fact that $\tilde{\mathcal{L}}(u) = \mathcal{L}(u, \chi_{\text{quad}})$ if M is odd, and $\tilde{\mathcal{L}}(u)(1-u) = \mathcal{L}(u, \chi_{\text{quad}})$ if M is even (see Proposition 1.12), it follows that

$$\frac{\tilde{\mathcal{L}}'}{\tilde{\mathcal{L}}}(1) = 2k - \frac{1}{q} \frac{\mathcal{L}'}{\mathcal{L}}(1/q) - C$$

where

$$C := \begin{cases} 0 & \text{for an odd } M, \\ 1/(q-1) & \text{for an even } M. \end{cases}$$

Switching back to the variable s using $u = q^{-s}$. Then, from (2.30),

$$I = \frac{q}{q-1} \left(k + \frac{1}{\log q} \frac{\mathcal{L}'}{\mathcal{L}}(1, \chi_{\text{quad}}) + C \right) = \frac{q}{q-1} \frac{M}{2} + O(\log M), \tag{2.32}$$

where we use Lemma 1.11 for the last equality. Combining (2.25), (2.26), (2.27), (2.28), and (2.32), we obtain

$$\log \hat{\mu}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) = -\frac{\xi^2}{2} + O\left(\frac{A}{\sqrt{M}} + \frac{A^2 \log M}{M} + \frac{A^4}{M}\right), \tag{2.33}$$

for all $|\xi| \leq A$. Now, as in [RS94], we can use Levy's Theorem to prove that the measures $\hat{\mu}_{m;R,N}$ converge in measure to the standard Gaussian. This concludes the proof. □

Theorem 2.21. *Assume that the set of all non-principal Dirichlet characters mod m satisfies LI. The density function of $\mu_{m;a_1,\dots,a_r}$ is symmetric in $(x_1,\dots,x_r)$ if and only if either:*

1. *$r = 2$ and $c(m,a_1) = c(m,a_2)$; or*
2. *$r = 3$ and there exists $\rho \neq 1$ satisfying these congruences modulo m:*

$$\rho^3 \equiv 1,\ a_2 \equiv a_1\rho,\ \text{and}\ a_3 \equiv a_1\rho^2.$$

Since the product of the Bessel functions in the expression for $\hat{\mu}(\xi)$ in Theorem 2.15 is even, it is only the factor $\mathcal{B}_{m;a_1,\dots,a_r}(\xi)$ that shifts the mean of μ. Hence, if μ is symmetric, $c(m,a_j) = c(m,a_l)$ for all $1 \leq j,l \leq r$. If we assume this, then μ is symmetric if the product of the Bessel functions is symmetric. For this, we have the following lemma.

Lemma 2.22. *$B_\chi(\xi_1,\dots,\xi_r) := \sum_{l=1}^r \chi(a_l)\xi_l$ is symmetric in $(\xi_1,\dots,\xi_r)$ for all χ if and only if one of the two conditions in Theorem 2.21 obtains.*

For the proof of this lemma, see [RS94, Lemma 3.2].

We can now prove Theorem 2.21. If $r = 2$ and $c(m,a_1) = c(m,a_2)$, then since $B_\chi(\xi_1,\xi_2)$ is symmetric, so is $\hat{\mu}(\xi_1,\xi_2)$ and also μ. If $r = 3$ and $a_2 \equiv a_1\rho \bmod m$, $a_3 \equiv a_1\rho^2 \bmod m$, then $c(m,a_1) = c(m,a_2) = c(m,a_3)$, so the exponential factor in $\hat{\mu}$ is symmetric in (ξ_1,ξ_2,ξ_3) and by the lemma, so is $B_\chi(\xi_1,\xi_2,\xi_3)$. This shows that $\hat{\mu}$ is symmetric, and therefore also μ.

Conversely, if $r \geq 4$ or if condition (2) of Theorem 2.21 fails, then

$$B_\chi(\xi_1,\dots,\xi_r) \neq B_\chi^\sigma(\xi_1,\dots,\xi_r)$$

for some permutation σ. Assume that

$$\begin{aligned}&\mathcal{B}_{m;a_1,\dots,a_r}(\xi) \prod_{\chi\neq\chi_0} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right| |B_\chi(\xi)|\right)\\ &\equiv \mathcal{B}_{m;a_{\sigma(1)},\dots,a_{\sigma(r)}}(\xi) \prod_{\chi\neq\chi_0} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right| |B_\chi^\sigma(\xi)|\right).\end{aligned}$$

First, any χ for which $B_\chi(\xi) \equiv B_\chi^\sigma(\xi)$ can be removed on both sides of this identity without altering the relation. So we may assume that the above product over χ contains only terms such that $B_\chi(\xi) \not\equiv B_\chi^\sigma(\xi)$. In view of our earlier assumption, the product is non-empty. Now we choose ξ generically so that:

1. $B_\chi(\xi) \neq 0$ and $B_\chi^\sigma(\xi) \neq 0$, for all $\chi \bmod m$;

2. if $B_\chi(\xi)/B_\lambda^\sigma(\xi) \neq 1$, then

$$\frac{B_\chi(\xi)}{B_\lambda^\sigma(\xi)} \neq \left|\frac{\gamma_\lambda(\gamma_\chi - 1)}{\gamma_\chi(\gamma_\lambda - 1)}\right|$$

for all $\chi, \lambda \bmod m$.

This can be done because our set of γ_χ's is finite. As a corollary to Theorem 2.20, we deduce that $\delta(P_{m;R,N}) = \tilde{\mu}_{m;R,N}[0,\infty)$ satisfies

$$\delta(P_{m;R,N}) \to \frac{1}{2} \text{ as } M \to \infty.$$

From this corollary we have that, for ξ fixed as above and all $t \in \mathbb{R}$,

$$\begin{aligned}
&\mathcal{B}_{m;a_1,\ldots,a_r}(t\xi) \prod_{\chi \neq \chi_0} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2t\gamma_\chi}{\gamma_\chi - 1}\right| |B_\chi(\xi)|\right) \\
&\equiv \mathcal{B}_{m;a_{\sigma(1)},\ldots,a_{\sigma(r)}}(t\xi) \prod_{\chi \neq \chi_0} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2t\gamma_\chi}{\gamma_\chi - 1}\right| |B_\chi^\sigma(\xi)|\right).
\end{aligned}$$

The smallest zero in t of the left-hand side occurs at a number of the form

$$\frac{w|\gamma_\chi - 1|}{2|\gamma_\chi| B_\chi(\xi)},$$

where w is the smallest zero of $J_0(z)$. The smallest zero on the right-hand side is at some

$$\frac{w|\gamma_\lambda - 1|}{2|\gamma_\lambda| B_\lambda^\sigma(\xi)}.$$

So we must have

$$\frac{w|\gamma_\chi - 1|}{2|\gamma_\chi| B_\chi(\xi)} = \frac{w|\gamma_\lambda - 1|}{2|\gamma_\lambda| B_\lambda^\sigma(\xi)}.$$

Due to the second condition above, this implies

$$\frac{B_\chi(\xi)}{B_\lambda^\sigma(\xi)} = 1 = \left|\frac{\gamma_\lambda(\gamma_\chi - 1)}{\gamma_\chi(\gamma_\lambda - 1)}\right|.$$

. But the γ's are distinct, since we are assuming LI, so $\chi = \lambda$. We conclude that $B_\chi(\xi) = B_\chi^\sigma(\xi)$, which contradicts an earlier condition. This completes the proof of Theorem 2.21.

The next theorem shows that the bias towards a particular residue modulo m dissipates as $M \to \infty$. This is similar to the classical case where $\hat{\mu}$ becomes unbiased as $q \to \infty$ (see [RS94]).

Theorem 2.23. *Suppose that m is an arbitrary (not necessarily irreducible) element in $\mathbb{F}[T]$ of degree M. Assume that the set of all non-principal Dirichlet characters modulo m satisfies LI. For a fixed r,*

$$\max_{a_1,\ldots,a_r \in (\mathbb{F}[T]/m)^*} \left|\delta(P_{m;a_1,\ldots,a_r}) - \frac{1}{r!}\right| \to 0$$

as $M \to \infty$.

Proof. Take m to be of arbitrary degree M, and $a_1, \ldots, a_r$, with r fixed, are distinct elements in $(\mathbb{F}[T]/m)^*$. Recall that $\hat{\mu}$ is the Fourier transform of a measure who

existence is established in Theorem 2.15. Let $\tilde{\mu}_{m;a_1,\dots,a_r}$ be the measure on $\mathbb{R}^r$ whose Fourier transform is

$$\hat{\mu}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{\Phi(m)M}}\right).$$

Then, as in [RS94, §3.2], it is sufficient to prove that $\tilde{\mu}_{m;a_1,\dots,a_r}$ converges in measure to the Gaussian

$$\frac{e^{-(x_1^2+\cdots+x_r^2)}}{(2\pi)^{r/2}}dx_1\dots dx_r$$

as $M\to\infty$. Fix a large A. For $\xi\in\mathbb{R}^r$ with $|\xi|\le A$, we obtain

$$\begin{aligned}\log\hat{\tilde{\mu}}_{m;a_1,\dots,a_r}(\xi) &= \log\mathcal{B}_{m;a_1,\dots,a_r}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{\Phi(m)M}}\right)\\ &\quad+\sum_{\chi\neq\chi_0}\sum_{\Im(\gamma_\chi)>0}\log J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi-1}\right|\sqrt{\frac{q-1}{q}}\frac{|\sum_{l=1}^r\chi(a_l)\xi_l|}{\sqrt{\Phi(m)M}}\right)\end{aligned}\tag{2.34}$$

from Theorem 2.15. The most significant term in (2.34) comes from the first non-constant term in the expansion of log of the Bessel function, and is given by

$$S:=-\frac{1}{4}\sum_{\chi\neq\chi_0}\sum_{\Im(\gamma_\chi)>0}\left|\frac{2\gamma_\chi}{\gamma_\chi-1}\right|^2\left(\frac{q-1}{q}\right)\frac{|\sum_{l=1}^r\chi(a_l)\xi_l|^2}{\Phi(m)M}.$$

Define, for any non-principal Dirichlet character χ,

$$I(\chi):=\frac{1}{2}\sum_{\gamma_\chi}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2.$$

Note that here the summation is over all inverse zeros. Since

$$\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|=\left|\frac{\bar{\gamma}_\chi}{\bar{\gamma}_\chi-1}\right|,$$

we have that

$$I(\chi)=\sum_{\Im(\gamma_\chi)>0}\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2.$$

Therefore,

$$\begin{aligned}S&=-\frac{1}{4}\sum_{\chi\neq\chi_0}\left(\frac{q-1}{q}\right)\frac{|\sum_{l=1}^r\chi(a_l)\xi_l|^2}{\Phi(m)M}\sum_{\Im(\gamma_\chi)>0}4\left|\frac{\gamma_\chi}{\gamma_\chi-1}\right|^2\\ &=-\frac{q-1}{q}\frac{1}{\Phi(m)M}\sum_{\chi\neq\chi_0}I(\chi)\left|\sum_{l=1}^r\chi(a_l)\xi_l\right|^2.\end{aligned}\tag{2.35}$$

Let χ^* be the primitive Dirichlet character which induces χ, and let $M(\chi^*)$ be the degree of its modulus. Then, $I(\chi)=I(\chi^*)$ (see Proposition 1.12). Also, the technique used to establish (2.32) applies to $I(\chi^*)$ to yield

$$I(\chi^*)=\frac{q}{q-1}\frac{M(\chi^*)}{2}+O(\log M(\chi^*)).$$

Applying this to (2.35) (recall $|\xi| \leq A$), we get

$$S = -\frac{1}{2\Phi(m)M} \sum_{\chi \neq \chi_0} M(\chi^*) \left| \sum_{l=1}^{r} \chi(a_l)\xi_l \right|^2 + O\left(A^2 \frac{\log M}{M}\right). \tag{2.36}$$

To simplify the above summation, we can apply an argument similar to the one on [RS94, p. 186]. If we write $|\sum_{l=1}^{r} \chi(a_l)\xi_l|^2$ as the product of the complex sum and its conjugate, we will get

$$\sum_{\chi \neq \chi_0} M(\chi^*) \left| \sum_{l=1}^{r} \chi(a_l)\xi_l \right|^2 = \sum_{l,k} \xi_l \xi_k \sum_{\chi \neq \chi_0} \chi\left(\frac{a_l}{a_k}\right) M(\chi^*).$$

Essentially, this argument shows that the asymptotic behaviour of S remains unchanged if $M(\chi^*)$ is replaced by M and if all of the cross terms in $|\sum_{l=1}^{r} \chi(a_l)\xi_l|^2$ are dropped. We conclude

$$S \to -\frac{1}{2} \sum_{l=1}^{r} {\xi_l}^2, \tag{2.37}$$

as $M \to \infty$. It remains to estimate the other terms in (2.34) than S.

From the definition of $\mathcal{B}_{m;a_1,\ldots,a_r}$, we have

$$\begin{aligned} 2\mathcal{B}_{m;a_1,\ldots,a_r}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{\Phi(m)M}}\right) &= \exp\left(i\frac{1}{\sqrt{q-1}}\frac{1}{\sqrt{\Phi(m)M}}\sum_{l=1}^{r} c(m,a_l)\xi_l\right) \\ &\quad + \exp\left(i\frac{\sqrt{q}}{\sqrt{q-1}}\frac{1}{\sqrt{\Phi(m)M}}\sum_{l=1}^{r} c(m,a_l)\xi_l\right). \end{aligned}$$

Let $d(m)$ be the number of monic divisors of m. Then we have that $c(m,a) < d(m)$ for any $a \in (\mathbb{F}[T]/m)^*$ and $d(m) = O_\epsilon((q^M)^\epsilon)$ for any $\epsilon > 0$. Therefore,

$$\mathcal{B}_{m;a_1,\ldots,a_r}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{\Phi(m)M}}\right) = O\left(\exp\frac{d(m)A}{\sqrt{\Phi(m)M}}\right). \tag{2.38}$$

Also, the higher terms in $\log J_0$ than S is $O(A^4/(\Phi(m)^2 M))$. Combining all of these results, we get

$$\hat{\tilde{\mu}}_{m;a_1,\ldots,a_r}(\xi) \to \exp\left(-\frac{1}{2}\sum_{l=1}^{r} {\xi_l}^2\right).$$

Again, by Levy's theorem, this implies the necessary convergence of $\tilde{\mu}_{m;a_1,\ldots,a_r}$ which completes the proof of the theorem. □

Chapter 3

Linear independence

3.1 Introduction

In the previous chapter, there arises the issue of the existence of linear dependence relations, with rational coefficients, among zeros (or rather arguments of inverse zeros) of Dirichlet L-functions. This was analogous to the *Grand Simplicity Hypothesis*, introduced in [RS94] as the statement that the set of all ordinates $\gamma \geq 0$ of the non-trivial zeros ρ of Dirichlet L-functions $L(s, \chi)$ are $\mathbb{Q}$-linearly independent when χ runs over primitive Dirichlet characters and the zeros are counted with multiplicity (in fact, they are conjectured to be simple). In [Kow08b], the author considers analogues of this type of independence questions in the context of finite fields since the current knowledge of the behaviour of zeros of zeta functions of algebraic curves over finite fields is somewhat more extensive than in the case of number fields. To tackle this issue, the author uses results developed by him in [Kow06].

In [Cha+97], Chavdarov proves that, in an algebraic family $C \to U$ of smooth projective curves of genus g over a finite field $\mathbb{F}_q$, if the monodromy groups mod l of the family are "as large as possible" for almost all l, then the numerators $\det(1 - T\mathrm{Fr}|H^1(\bar{C}_u, \mathbb{Q}_l))$ of the zeta functions of the curves C_u of the family are "almost all" irreducible, and have splitting field "as large as possible" (not necessarily the symmetric group).

Chavdarov's method is similar in principle to the method used by van der Waerden to show that "most" polynomials of given degree d with integer coefficients have splitting field as large as possible. This latter result was reproved in a simpler way and stronger form by Gallagher ([Gal73]) using the large sieve inequalities. Applying similar ideas to Chavdarov's problem is possible to some extent. This yields stronger results than in [Cha+97] (see Theorem 3.9 and Theorem 3.10).

In the next two sections, we introduce the data involved and then state our main bilinear form estimate from which we derive a "large sieve" statement. Then we apply the sieve statement to prove Theorem 3.10. We also prove an easy consequence of the theorem (Proposition 3.11). Note that the statement here is slightly different (an improved bound) from the one in [Kow06].

Finally, we want to use the sieve for Frobenius to show that in a certain sense, the roots of the L-functions of most algebraic curves over finite fields do not satisfy any non-trivial (linear or multiplicative) dependency relations. Although we won't prove the most general results given in [Kow08b], we will show this for a certain family of hyperelliptic curves (see Theorem 3.1). To show this, we use a result very similar to Theorem 3.10.

Let $C/\mathbb{F}_q$ be a smooth, projective, and geometrically connected algebraic curve over a finite field with q elements and characteristic p, and let $g \geq 0$ be its genus. Its zeta function $Z(C, s)$ is defined (first for $s \in \mathbb{C}$ with $\Re(s)$ large enough) by either of

the equivalent expressions

$$Z(C,s) = \exp\left(\sum_{n\geq 1} \frac{|C(\mathbb{F}_{q^n})|}{n} q^{-ns}\right) = \prod_{\substack{x \text{ closed} \\ \text{point in } C}} (1 - N(x)^{-s})^{-1}.$$

It was proved by Schmidt that this can be expressed as

$$Z(C,s) = \frac{L(C,s)}{(1-q^{-s})(1-q^{1-s})}$$

where $L(C,s) = P_C(q^{-s})$ for some polynomial $P_C(T) \in \mathbb{Z}[T]$ of degree $2g$. This polynomial is also called the L-function of $C/\mathbb{F}_q$, and can be factored as

$$P_C(T) = \prod_{1\leq j\leq 2g} (1 - \alpha_j T).$$

Here, $\alpha_j, 1 \leq j \leq 2g$ are the inverse zeros (sometimes referred to as "zeros", even in this chapter). By the analogue of Riemann Hypothesis in function fields, we have that $|\alpha_j| = \sqrt{q}$.

When we investigate the possible linear relations among the ordinates of these zeros, if we allow all imaginary parts, many "trivial" relations come from the fact that, e.g., the $\theta_j + k, k \in \mathbb{Z}$, are $\mathbb{Q}$-linearly dependent. One must therefore consider θ_j up to integers, and the simplest way to do this is to consider multiplicative relations

$$\prod_{1\leq j\leq 2g} e(n_j\theta_j) = 1$$

with $n_j \in \mathbb{Q}$ or, raising to a large power to eliminate the denominator, relations

$$\prod_{1\leq j\leq 2g} \left(\frac{\alpha_j}{\sqrt{q}}\right)^{n_j} = 1$$

with $n_j \in \mathbb{Z}$.

In the multiplicative case, it is immediately clear that we have to take into account the functional equation

$$L(C,s) = q^{g(1-2s)} L(C, 1-s),$$

which may be interpreted as stating that for any j, q/α_j is also among the inverse roots. In particular, except if $\alpha_j = \pm\sqrt{q}$, there are identities $\alpha_j\alpha_k = q$ with $j \neq k$, leading to multiplicative relations of the form

$$\alpha_j\alpha_k = \alpha_{j'}\alpha_{k'}$$

(this is similar to the fact that a root $1/2 + i\gamma$ of $L(s,\chi)$, for a Dirichlet character χ, gives a root $1/2 - i\gamma$ of $L(s,\bar{\chi})$, which leads to the restriction of the Grand Simplicity Hypothesis to non-negative ordinates of zeros). Hence the most natural question is whether those "trivial" relations are the only multiplicative relations.

Finally, since dealing with a single curve seems still far away of this Grand Simplicity Hypothesis, which involves all Dirichlet L-functions, an even more natural-looking analogue would be to ask the following: given a family of curves, interpreted as an algebraic family $C \to U$ of curves of genus g over some parameter variety $U/\mathbb{F}_q$, what (if any) multiplicative relations can exist among the $\alpha_j(t)/\sqrt{q}$ which are the inverse

roots of the polynomials $P_{C_t}(T)$, for all $t \in U(\mathbb{F}_q)$?

Here is now a result concerning a specific family of curves. We use the following notation: given a finite family $\alpha = (\alpha_j)$ of non-zero complex numbers, we write $\langle \alpha \rangle_a$ for the $\mathbb{Q}$-vector subspace of $\mathbb{C}$ generated by the α_j, and $\langle \alpha \rangle_m$ for the multiplicative subgroup of $\mathbb{C}^*$ generated by the α_j. For an algebraic curve C over a finite field, we denote by $\mathcal{Z}(C)$ the multiset of inverse zeros of $P_C(T)$, and similarly with $\tilde{\mathcal{Z}}(C)$ for the multiset of normalized inverse zeros $\alpha/\sqrt{q}$.

Theorem 3.1. *Let $f \in \mathbb{Z}[X]$ be a squarefree monic polynomial of degree $2g$, where $g \geq 1$ is an integer. Let p be an odd prime such that p does not divide the discriminant of f, and let $U/\mathbb{F}_p$ be the open subset of the affine t-line where $f(t) \neq 0$. Consider the algebraic family $C_f \to U$ of smooth projective hyperelliptic curves of genus g given as the smooth projective models of the curves with affine equations*

$$C_t : y^2 = f(x)(x - t), \text{ for } t \in U.$$

Then for any extension $\mathbb{F}_q/\mathbb{F}_p$, we have

$$|\{t \in U(\mathbb{F}_q) | \text{ there is a non-trivial linear relation among } \mathcal{Z}(C)\}| \ll q^{1-\gamma}(\log q), \tag{3.1}$$

$$|\{t \in U(\mathbb{F}_q) | \text{ there is a non-trivial multiplicative relation among } \tilde{\mathcal{Z}}(C)\}| \ll q^{1-\gamma}(\log q), \tag{3.2}$$

where $\gamma = \frac{1}{4g^2+2g+4} > 0$, the implied constants depending only on g.

In order to explain precisely the meaning of the statements,we introduce the following notation: for any finite set M of complex numbers, we define

$$\mathrm{Rel}(M)_a = \{(t_\alpha) \in \mathbb{Q}^M | \sum_{\alpha \in M} t_\alpha \alpha = 0\}, \tag{3.3}$$

$$\mathrm{Rel}(M)_m = \{(n_\alpha) \in \mathbb{Z}^M | \prod_{\alpha \in M} \alpha^{n_\alpha} = 1\}, \tag{3.4}$$

the additive relation $\mathbb{Q}$-vector space and multiplicative relation group, respectively. Note that $\mathrm{Rel}(M)_m$ is a free abelian group.

Then, the condition in (3.1) for a given curve may be phrased equivalently as

$$\mathrm{Rel}(\mathcal{Z}(C))_a = 0, \text{ or } \dim_{\mathbb{Q}} \langle \mathcal{Z}(C) \rangle_a < 2g \text{ or } \langle \mathcal{Z}(C) \rangle_a \simeq \mathbb{Q}^{2g}.$$

From the functional equation, it follows that we can arrange the $2g$ normalized roots $\tilde{\alpha} = \alpha/\sqrt{q}$ in g pairs of inverses $(\tilde{\alpha}, \tilde{\alpha}^{-1})$, so that the multiplicative subgroup $\langle \tilde{\mathcal{Z}}(C_t) \rangle_m \subset \mathbb{C}^*$ is of rank $\leq g$. Denote by $\mathrm{Triv}(M)_m$ the abelian group

$$\{(n_{\tilde{\alpha}}) \in \mathbb{Z}^M | n_{\tilde{\alpha}} - n_{\tilde{\alpha}^{-1}} = 0\} \tag{3.5}$$

which is a subset of $\mathrm{Rel}(M)_m$, and let $\mathrm{Rel}_0(M)_m = \mathrm{Rel}(M)_m/\mathrm{Triv}(M)_m$ (the group of non-trivial relations). The interpretation of (3.2) is that most of the time, there is equality:

$$\mathrm{Rel}(\tilde{\mathcal{Z}}(C_t))_m = \mathrm{Triv}(\tilde{\mathcal{Z}}(C_t))_m, \text{ or } \mathrm{Rel}_0(\tilde{\mathcal{Z}}(C_t))_m = 0. \tag{3.6}$$

3.2 Preliminaries

Our main tool is a general estimate for a bilinear form made up from representations of a system of lisse $\bar{\mathbb{F}}_l$-sheaves on a variety over a finite field.

The first basic data is therefore a base variety $U/\mathbb{F}_q$, where as usual $\mathbb{F}_q$ denotes a finite field of characteristic p with q elements. We assume that U is smooth, affine, and geometrically connected of dimension $d \geq 1$.

We denote by $\bar{\eta}$ the geometric generic point of U and by $\bar{U}$ the variety U extended to $\bar{\mathbb{F}}_q$. We therefore have the arithmetic fundamental group $\pi_1(U, \bar{\eta})$ and the geometric fundamental group $\pi_1(\bar{U}, \bar{\eta})$. We have an exact sequence

$$1 \to \pi_1(\bar{U}, \bar{\eta}) \to \pi_1(U, \bar{\eta}) \xrightarrow{d} \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}} \to 1. \tag{3.7}$$

For $n \geq 1$ and $u \in U(\mathbb{F}_{q^n}$, we denote by Fr_{u,q^n} the geometric Frobenius automorphism at u in $\pi_1(U, \bar{\eta})$, i.e., the image of the inverse of the canonical generator $x \mapsto x^{q^n}$ of the Galois group of $\mathbb{F}_{q^n}$ via the map

$$\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to \pi_1(U, \bar{\eta})$$

induced from the inclusion $\mathrm{Spec}\ \mathbb{F}_{q^n} \to U$ which "is" u. In the above exact sequence we have then

$$d(\mathrm{Fr}_{u,q^n}) = -n.$$

In most of our results, the base field (i.e., q) will be considered fixed, although the results will be uniform in q so they can be applied to $U \times \mathbb{F}_{q^n}$ for any $n \geq 1$. So most of the time we just write Fr_u instead of $\mathrm{Fr}_{u,q}$ for $u \in U(\mathbb{F}_q)$.

We also denote generically by Fr the global geometric Frobenius automorphism.

We now come to the sheaves on U that we consider. We assume given a set Λ of primes $\neq p$, and for $l \in \Lambda$, a lisse sheaf $\tilde{\mathcal{F}}_l$ of $\mathbb{F}_\lambda$-vector spaces of (fixed) rank $r \geq 1$, where $\mathbb{F}_\lambda$ is a finite field characteristic l (the degree if which over $\mathbb{F}_l$ may depend on l). The basic example is when we have lisse sheaves $\mathcal{F}_l$ of $\mathbb{Z}_\lambda$-modules and

$$\tilde{\mathcal{F}}_l = \mathcal{F}_l/\mathfrak{m}_\lambda \mathcal{F}_l,$$

where $\mathbb{Z}_\lambda$ is the ring of integers in a finite extension of $\mathbb{Q}_l$ with residue field $\mathbb{F}_\lambda$ and maximal ideal $\mathfrak{m}_\lambda$.

Equivalently, $\tilde{\mathcal{F}}_l$ "is" a representation

$$\rho_l : \pi_1(U, \bar{\eta}) \to \mathrm{GL}(r, \mathbb{F}_\lambda).$$

From this description, we can easily define the monodromy groups of $\tilde{\mathcal{F}}_l$, or of ρ_l: the arithmetic monodromy group $G_l \subset \mathrm{GL}(r, \mathbb{F}_\lambda)$ is the image of ρ_l, and the geometric monodromy group G_l^g is the image of the subgroup $\pi_1(\bar{U}, \bar{\eta}$. Thus from (3.7) we derive a commutative diagram with exact rows and surjective downward arrows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(\bar{U}, \bar{\eta}) & \longrightarrow & \pi_1(U, \bar{\eta}) & \xrightarrow{d} & \hat{\mathbb{Z}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & G_l^g & \longrightarrow & G_l & \xrightarrow{m} & \Gamma_l & \longrightarrow & 1\,, \end{array} \tag{3.8}$$

where Γ_l is a finite commutative (cyclic) group.

In the case where the sheaves $\tilde{\mathcal{F}}_l$ arise by reduction of $\mathbb{Z}_\lambda$-sheaves $\mathcal{F}_l$, as described previously, one says that they form a *compatible* system if for every extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, every $u \in U(\mathbb{F}_{q^n})$ and every $l \in \Lambda$, the reversed characteristic polynomial of Fr_{u,q^n} acting on $\mathcal{F}_l$, i.e., the polynomial

$$\det(1 - T\mathrm{Fr}_{u,q^n} \mid \mathcal{F}_l)$$

has coefficients in $\bar{\mathbb{Q}}$ and is independent of l.

For any l we will consider various sums involving irreducible (complex valued) linear representations of G_l. Say that two representations of G_l are geometrically equivalent if their restrictions to G_l^g are equivalent, or (by the lemma) if and only if they differ by a twist by a character of Γ_l. We now assume chosen a set Π_l of representatives of the irreducible representations of G_l for this equivalence relation. Using these and characters of Γ_l, one can parametrize all irreducible representations of G_l as follows: they are of the form $\pi \otimes \psi$ where $\pi \in \Pi_l$ and $\psi \in \hat{\Gamma}_l$; the representation π is unique, but ψ is only unique up to multiplication by an element of the group

$$\hat{\Gamma}_l^\pi := \{\psi \in \hat{\Gamma}_l \mid \pi \simeq \pi \otimes (\psi \circ m)\}$$

where $\hat{\Gamma}_l$ is the character group of Γ_l.

This ambiguity requires us to control the size of those groups $\hat{\Gamma}_l^\pi$. We will assume that for all $l \in \Lambda$ and $\pi \in \Pi_l$, we have

$$|\hat{\Gamma}_l^\pi| \leq \kappa \tag{3.9}$$

for some fixed $\kappa \geq 1$. Here is a useful case when we can get such a bound.

Lemma 3.2. *Assume that r is even and that for all l we have $G_l^g = \mathrm{Sp}(r, \mathbb{F}_l)$, the symplectic group for some non-degenerate alternating form $\langle \cdot, \cdot \rangle$ on $\mathbb{F}_l^r$, and that G_l is a subgroup of the group $\mathrm{SSp}(r, \mathbb{F}_l)$ of symplectic similitudes, i.e, for $g \in G_l$ we have $\langle gv, gw \rangle = m(g)\langle v, w \rangle$ for some $m(g) \in \mathbb{F}_l^*$, called the multiplicator of g. Then (3.9) holds with $\kappa = 2$.*

Proof. If π is an irreducible representation of G_l and $\psi \in \hat{\Gamma}_l^\pi$, then ψ is trivial on the center Z_l of G_l. For any $x \in G_l$, we can write

$$x^2 = m(x)y$$

with $y \in \mathrm{Sp}(r, \mathbb{F}_l) = G_l^g$ (since $m(ax) = a^2 x$ for scalar a), so $\psi(x)^2 = 1$. This means that ψ is of order at most 2, and since it is character of a cyclic group, there are at most 2 such characters, giving (3.9) with $\kappa = 2$. □

We need various estimates involving sums of dimensions of the representations in Π_l. We will phrase them in terms of upper bound for the "dimensions" of G_l and of the set $G_l^\#$ of its conjugacy classes: let s and t be such that the inequalities

$$|G_l| \leq c_1 l^s, |G_l^\#| \leq c_2 l^t \tag{3.10}$$

hold for all primes $l \in \Lambda, c_1$ and c_2 being two given constants. Note that of course $s = t = r^2$ is always possible with $c_1 = c_2 = 1$ (and that in fact this does not in general significantly affect the applications).

Lemma 3.3. *1. We have*

$$\sum_{\pi \in \Pi_l} \dim \pi \leq (c_1 c_2 l^{s+t})^{1/2},$$

and for all $\pi \in \Pi_l$ we have

$$\dim \pi \leq (c_1 l^s)^{1/2}.$$

2. *If r is even, $G_l^g = \mathrm{Sp}(r, \mathbb{F}_l)$ and $G_l \subset \mathrm{SSp}(r, \mathbb{F}_l)$, the estimates (3.10) hold with*

$$c_1 = 1, s = 1 + \frac{r(r+1)}{2}, c_2 = 6^{r/2}, t = r/2 + 1.$$

Proof. 1. For a representation of a finite group G, the dimension is always $\leq |G|^{1/2}$, and the sum of the dimension is bounded by Cauchy's inequality by

$$\sum_{\pi} \dim \pi \leq |G^{\#}|^{1/2} |G|^{1/2}.$$

Using (3.10) in the above inequalities, the result follows.

2. It follows from the formula for the cardinality of $\mathrm{Sp}(r, \mathbb{F}_l)$, and [LP97, Lemmas 1.3 and 1.6].

□

We now define what it means for a family of sheaves to be linearly disjoint.

Definition 3.4. *The family $(\tilde{\mathcal{F}}_l)$ is linearly disjoint if for all l and l' in Λ, with $l \neq l'$, the product map*

$$\pi_1(\bar{U}, \bar{\eta}) \to G_l^g \times G_{l'}^g$$

is surjective.

The next couple of results will be useful later and are quoted here without proofs.

Lemma 3.5. *Let G_1 and G_2 be finite groups such that every normal subgroup of G_i is contained in the center C_i, and such that G_1/C_1 and G_2/C_2 are distinct, simple and non-abelian. Then no proper subgroup $G \subset G_1 \times G_2$ projects surjectively on both G_1 and G_2.*

This is typically applied with $G_1 = G_l^g, G_2 = G_l^g$, and G the image of $\pi_1(\bar{U}, \bar{\eta}) \to G_1 \times G_2$ which projects surjectively on both factors. For instance, we have the following corollary:

Corollary 3.6. *Let r be even and let $(\tilde{\mathcal{F}}_l)$ be a family of sheaves as above such that $G_l^g = \mathrm{Sp}(r, \mathbb{F}_l)$ for all l in Λ, with $l \geq 5$ is $r = 2$ and $l \geq 3$ if $r = 4$. Then the family is linearly disjoint.*

3.3 Bilinear form estimates and large sieve for algebraic families

We write

$$\sum_{\pi \neq 1}^{*} \alpha(\pi, l, \ldots)$$

for a sum over all the irreducible representations $\pi \in \Pi_l$ of G_l^g which are non-trivial. Using this notation, we now state the bilinear form estimate which is our main tool.

Theorem 3.7. *Let U be a variety and $(\tilde{\mathcal{F}}_l)$ a family of sheaves as above, with given sets Π_l of irreducible representations which are representatives for geometric equivalence. Assume that the family is linearly disjoint, that it satisfies (3.9) and moreover that U and $(\tilde{\mathcal{F}}_l)$ satisfy one of the following conditions:*

1. *U is a smooth affine curve and $(\tilde{\mathcal{F}}_l)$ arises from a a compatible system of integral l-adic sheaves.*

2. For all $l \in \Lambda$, the order of G_l^g is prime to p.

Then there exist constants $C \geq 0$ and $A \geq 0$ such that we have

$$\sum_{l \leq L} \sum_{\pi \neq 1}^{*} \left| \sum_{u \in U(\mathbb{F}_q)} \alpha(u) \mathrm{Tr}(\pi \circ \rho_l)(\mathrm{Fr}_u) \right|^2 \leq (\kappa q^d + C q^{d-1/2} L^A) \sum_{u \in U(\mathbb{F}_q)} |\alpha(u)|^2, \quad (3.11)$$

for any $L \geq 1$ and any complex coefficients $\alpha(u)$.

In case 1, we can take $A = 1 + s + t/2$, and the constant C depends only on $\bar{U}$, the "geometric" compatible system $(\mathcal{F}_l)$ on $\bar{U}$ and the constants c_1 and c_2. In case 2, we can take $A = 1 + 3s + t/2$, and the constant C depends only on $\bar{U}, c_1$ and c_2.

In particular the estimate can be applied uniformly for $U \otimes \mathbb{F}_{q^n}$ for any $n \geq 1$.

Note that the left-hand side of (3.11) is in fact independent of the choice of representative sets Π_l.

The proof of Theorem 3.7 can be found in [Kow06, § 5]. Here, we derive a large sieve estimate concerning the average distribution of the Frobenius conjugacy classes in G_l.

Let $L \geq 2$ and suppose that for $l \in \Lambda, l \leq L$, we select some conjugacy-invariant subset $\Omega(l)$ of G_l with cardinality $\omega(l)$, such that

$$m(x) = \varphi(-1) \in \Gamma_l$$

for all x and l (where $m : G_l \to \Gamma_l$ and φ are defined by the commutative diagram (3.8).

Let then

$$P(u, L) = \sum\nolimits_{\substack{l \leq L \\ \rho_l(\mathrm{Fr}_u) \in \Omega(l)}} 1$$

for $u \in U(\mathbb{F}_q)$ and

$$P(L) = \sum_{l \leq L} \omega(l) |G_l^g|^{-1}.$$

The large sieve statement says that for "most" u, the value of $P(u, L)$ is close to the average value $P(L)$ (in terms of variance).

Proposition 3.8. *With U and $(\tilde{\mathcal{F}}_l)$ satisfying one of the assumptions of Theorem 3.7, we have*

$$\sum_{u \in U(\mathbb{F}_q)} (P(u, L) - P(L))^2 \leq (\kappa q^d + C q^{d-1/2} L^A) P(L), \quad (3.12)$$

where the constants C and A are the same as in Theorem 3.7. In particular, the cardinality of the sifted set

$$S(U, \Omega; L) = \{u \in U(\mathbb{F}_q) | \mathrm{Fr}_u \notin \Omega(l) \text{ for all } l \leq L\}$$

satisfies

$$|S(U, \Omega; L)| \leq (\kappa q^d + C q^{d-1/2} L^A) P(L)^{-1}. \quad (3.13)$$

The above proposition is [Kow06, Proposition 3.3] and its proof can also be found there.

3.4 Zeta functions of families of curves

We now come to the application of the large sieve to a strong form of Chavdarov's theorem on the generic behaviour of the numerators of zeta functions of curves in families. We will look for arguments uniform with respect to g so that, in some cases at least, we obtain results valid even for g large (though not for q fixed, $g \to +\infty$).

Let $C/\mathbb{F}_q$ be a smooth, projective, and geometrically connected curve of genus g over a finite field. If $Z(C)$ is its zeta function, we recall that there exists a polynomial $P_C \in \mathbb{Z}[T]$ of degree $2g$ with $P_C(0) = 1$ such that

$$Z(C) = \frac{P_C(T)}{(1-T)(1-qT)}.$$

The cohomological definition is that the polynomial $P_C(T)$ can be described as the (reversed) characteristic polynomial of the geometric Frobenius automorphism acting on a suitable étale cohomology group, specifically

$$P_C(T) = \det(1 - T\mathrm{Fr}|H^1(\bar{C}, \mathbb{Z}_l)). \tag{3.14}$$

The question investigated by Chavdarov concerns the splitting field of this integer polynomial as C varies in an algebraic family, e.g. in a hyperelliptic family

$$C_u : y^2 = f(x)(x-u)$$

where f is a fixed polynomial in $\mathbb{F}_q[X]$ of degree $2g$ with distinct roots in $\bar{\mathbb{F}}_q$, and u is the parameter that can take any value in $\bar{\mathbb{F}}_q$ which is not a zero of f.

The polynomial P_c satisfies the "functional equation"

$$T^{2g} P_c \frac{q}{T} = P_c(T).$$

It is clear from the functional equation that the roots of P_c are paired, i.e. if $\alpha \in \mathbb{C}$ is a root of P_c, then $q\alpha^{-1}$ is also a root. This means that the "splitting algebra" $\mathbb{Q}[T]/(f)$ has Galois group G which can be seen as a subgroup of the group W_{2g} of signed permutations of $\{1, \dots, 2g\}$. In particular, if the polynomial is irreducible, its splitting field has maximal Galois group $G \simeq W_{2g}$ if and only if the splitting field is of maximal degree $|W_{2g}| = 2^g g!$.

In terms of étale cohomology, the functional equation above is a consequence of the Poincaré duality which states that there is a natural non-degenerate alternating pairing

$$H^1(\bar{C}, \mathbb{Z}_l) \otimes H^1(\bar{C}, \mathbb{Z}_l) \to \mathbb{Z}_l(-1). \tag{3.15}$$

Note that this implies that the "global" geometric Frobenius Fr of $\mathbb{F}_q$ acts on $H^1(\bar{C}, \mathbb{Z}_l)$ as a symplectic similitude for this pairing, with multiplicator q.

Here is now our first general result about the behaviour of the splitting fields in a suitable family, which significantly strengthens the results of Chavdarov. We won't give the proof of this result (see [Kow06, § 9] for the proof) since it is not directly applicable to the objective at hand; however, it does complement the second result that we will state and prove.

Theorem 3.9. *Fix an integer $g \geq 1$. Let $q = p^k$ and let $U/\mathbb{F}_q$ be a geometrically irreducible smooth affine scheme of dimension $d \geq 1$ such that one of the following two conditions is satisfied:*

1. *U is a curve, i.e., $d = 1$.*

2. *We have* $p > 2g + 1$.

Let $\pi : C \to U$ *be a proper smooth family of projective curves of genus* g *over* U. *Assume that for all* $l > L_0$ *the geometric monodromy group of the integral sheaves* $R^1\pi_!\mathbb{Z}_l$ *is the full symplectic group* $Sp(2g)$. *Then the number* $N(U/\mathbb{F}_q)$ *of* $u \in U(\mathbb{F}_q$ *such that the numerator*

$$P_u = \det(1 - T\mathrm{Fr}|H^1(\bar{C}_u, \mathbb{Q}_l)) \in \mathbb{Z}[T] \tag{3.16}$$

of the zeta function of the curve $C_u = \pi^{-1}(u)$ *is reducible or has splitting field with degree strictly less than* $2^g g!$ *satisfies*

$$N(U/\mathbb{F}_q) \ll q^{d-\gamma}(\log q)$$

for $\gamma = \frac{1}{4g^2+3g+5}$ *in case* (1) *and* $\gamma = \frac{1}{12g^2+7g+9}$ *in case* (2), *where the implied constant depends only on* L_0, g *and* $\bar{U}/\bar{\mathbb{F}}_q$.

The second result is a uniform version (in terms of g) for the families of hyperelliptic curves already introduced.

Theorem 3.10. *Let* $g \geq 1, p \neq 2, q = p^k$ *with* $k \geq 1$. *Let* $f \in \mathbb{F}_q[X]$ *be a monic polynomial of degree* $2g$ *with distinct roots in* $\bar{\mathbb{F}}_q, U \subset \mathbb{A}^1$ *be the complement of the set of zeros of* f *and denote by* $\pi : C \to U$ *the family of hyperelliptic curves of genus* g *given by*

$$C_u : y^2 = f(x)(x - u)$$

completed by the section at ∞, *with projection* $\pi(x, y, u) = u$.

Then the number $N(f, q)$ *of* $u \in U(\mathbb{F}_q)$ *such that the polynomial*

$$P_u = \det(1 - T\mathrm{Fr}|H^1(\bar{C}_u, \mathbb{Q}_l)) \in \mathbb{Z}[T]$$

is either reducible or has splitting field with degree strictly smaller than $2^g g!$ *satisfies*

$$N(f, q) \ll q^{1-\gamma}(\log q)$$

for $\gamma = \frac{1}{4g^2+3g+5}$, *where the implied constant is absolute.*

Note that the uniform bound in this last result is only non-trivial if g^2 is somewhat smaller than $\log q$.

We will prove the theorem in § 3.6 after some common preliminaries. Here we include an additional result which is of independent interest.

Since the estimate of Theorem 3.10 is (in particular) uniform in q, it can also be used in "horizontal" direction, i.e., with $q = p$ varying. For instance, we deduce the following proposition. In [Kow06], this result is slightly different (Proposition 6.3). Here, we improve the bound to a power of the logarithm following the suggestion of C. Helsholtz which has been mentioned as a note in [Kow06].

Proposition 3.11. *Let* $g \geq 1$ *be an integer,* $f \in \mathbb{Q}[X]$ *be a polynomial of degree* $2g$ *with distinct complex roots. For* $n \in \mathbb{Z}$ *not a root of* f, *let* $C_n/\mathbb{Q}$ *be the hyperelliptic curve of genus* g *with equation*

$$C_n : y^2 = f(x)(x - n)$$

and let J_n be its Jacobian. Then for $N \geq 3$, the set $S(N)$ of integers n with $|n| \leq N$ such that $J_n/\mathbb{Q}$ is not simple up to isogeny satisfies

$$|S(N)| \ll N^{1/2-\delta} \log N$$

where $\delta = \frac{1}{2}\frac{1}{4g^2+3g+5}$. The implied constant depends on g and the splitting field of f.

Proof. Denote first by Q_f the set of primes p totally split in the splitting field of f. Notice that for any $y \geq 2$ we have the sieving estimate

$$|S(N)| \leq |\{n \in \mathbb{Z} \mid |n| \leq N \text{ and } n(\text{mod } p) \notin \Omega(p) \text{ for } p \in Q_f, p \leq y\}|$$

where

$$\Omega(p) = \{t \in \mathbb{Z}/p\mathbb{Z} \mid f(t) \not\equiv 0(\text{mod } p) \text{ and } \det(1 - T\text{Fr}_t \mid H^1(\bar{C}_t, \mathbb{Q}_l)) \text{ is irreducible}\}.$$

By Theorem 3.10, there exists a constant $C \geq 0$ such that for all p we have

$$|\Omega(p)| \geq p - Cp^{1-\gamma}(\log p) \tag{3.17}$$

with $\gamma = \frac{1}{4g^2+3g+5}$. We want to apply Gallagher's larger sieve, as described in [CM05, § 2.2]. $S(N)$ is a (non-empty) finite set of integers and our set of prime powers will just be all primes $\leq y$ for some $y \leq N$ that we will choose later. For each $p \leq y$, we have

$$|S(N)(\text{mod } p)| \leq p - |\Omega(p)|.$$

Using (3.17),

$$\begin{aligned}\sum_{p \leq y} \frac{\log p}{p - |\Omega(p)|} - \log 2N &\geq \sum_{p \leq y} \frac{\log p}{Cp^{1-\gamma}(\log p)} - \log 2N \\ &= \sum_{p \leq y} Cp^{\gamma-1} - \log 2N\end{aligned}$$

Note that we always use the same symbol C for the constant even though it might change in value from one expression to another (as in the case above). Now, $\gamma - 1 < 0$ and so $p^{\gamma-1} \geq y^{\gamma-1}$. Using this, we have

$$\begin{aligned}\sum_{p \leq y} Cp^{\gamma-1} - \log 2N &\geq Cy^{\gamma-1}\left(\sum_{p \leq y} 1\right) - \log 2N \\ &\geq C\frac{y^\gamma}{\log y} - \log 2N\end{aligned}$$

for large enough N. Choose $y = \sqrt{N}$. Then

$$\sum_{p \leq y} \frac{\log p}{p - |\Omega(p)|} - \log 2N \geq C\frac{N^\delta}{\log N} - \log 2N > 0 \tag{3.18}$$

for large enough N. In this case, we can apply Gallagher's larger sieve ([CM05, Theorem 2.2.1]) and use (3.18) to get

$$\begin{aligned}|S(N)| &\leq \frac{\sum\limits_{p\leq y}\log p - \log 2N}{\sum\limits_{p\leq y}\frac{\log p}{p-|\Omega(p)|} - \log 2N}\\ &\leq \frac{\sum\limits_{p\leq y}\log p - \log 2N}{C\frac{N^\delta}{\log N} - \log 2N}\end{aligned}$$

for large enough N. By Chebyshev's theorem, we know that $\sum\limits_{p\leq\sqrt{N}}\log p < C'\sqrt{N}$ for some $C' > 0$. Therefore,

$$\begin{aligned}|S(N)| &\leq \frac{C'\sqrt{N} - \log 2N}{C\frac{N^\delta}{\log N} - \log 2N}\\ &\ll N^{1/2-\delta}\log N.\end{aligned}$$

□

3.5 Preliminaries for the proof of Chavdarov's theorem

We start with some preliminaries related to the group W_{2g} and to setting up a sieve for characteristic polynomials of symplectic similitudes.

From the description of W_{2g} we see that there is an exact sequence

$$1 \to \{\pm 1\}^g \to W_{2g} \xrightarrow{p} S_g \to 1.$$

We also denote by i the natural inclusion $i : W_{2g} \to S_{2g}$.

The first lemma describes various ways of ensuring that a subgroup of W_{2g} is equal to W_{2g}.

Lemma 3.12. *Let $g \geq 1$ and $W \subset W_{2g}$ be a subgroup of W_{2g}. Assume that one of the following conditions is true, where $i : W_{2g} \to S_{2g}$ is the embedding above:*

1. *For any conjugacy class $c \subset W_{2g}$, we have $c \cap W \neq \emptyset$.*
2. *The subgroup $i(W)$ contains a 2-cycle, a 4-cycle, a $(2g-2)$-cycle and a $2g$-cycle.*
3. *The subgroup $i(W)$ contains a transposition and acts transitively on $\{1,\dots,2g\}$; moreover, the projection $p(W)$ contains a transposition and an m-cycle with $m > g/2$ prime.*

Then in all cases we have $W = W_{2g}$.

Proof. 1. It is a standard result in finite group theory which is not specific to W_{2g} (see [Cha+97, Lemma 5.8]).

2. See [DDS98, Lemma 2].

3. Observe that the first condition already implies that $W = W_{2g}$ if $g = 1$. Otherwise we see that $p(W)$ acts transitively on $\{1,\dots,g\}$ and so with the second and third conditions, we get $p(W) = S_g$ by the result of Bauer given in [Gal73,

Lemma, p. 98]. Since $i(W)$ contains a transposition, we deduce that $W = W_{2g}$ by [Cha+97, Lemma 5.5].

□

To set up our sieve, it will be convenient to say that a polynomial $f \in A[T]$ (A any commutative ring) of degree $2g$ such that $f(0) = 1$ and

$$T^{2g} f\left(\frac{q}{T}\right) = f(T),$$

is *q-symplectic of degree $2g$*. Hence the numerator of the zeta function of a curve $C/\mathbb{F}_q$ is q-symplectic.

We now state a general result comparing a sieve related to characteristic polynomials of elements with multiplicator q in the finite group $\mathrm{SSp}(2g, \mathbb{F}_l)$ of symplectic similitudes to the "same" sieve applied to all q-symplectic polynomials of degree $2g$.

Recall that we denote by $m(g)$ the multiplicator for a symplectic similitude, i.e.,

$$\langle gv, gw\rangle = m(g)\langle v, w\rangle.$$

Lemma 3.13. *Let $g \geq 1$ and l a prime. Put*

$$\Upsilon_{g,l} = \{f \in \mathbb{F}_l[T] | f \text{ is } q\text{-symplectic of degree } 2g\}.$$

Let $\tilde{\Omega}(l) \subset \Upsilon_{g,l}$ be an arbitrary subset of cardinality $\tilde{\omega}(l)$ and

$$\Omega(l) = \{g \in \mathrm{SSp}(2g, \mathbb{F}_l) | m(g) = q, \text{ and } \deg(1 - Tg) \in \tilde{\Omega}(l)\},$$

with cardinality $\omega(l)$.

Then we have

$$\omega(l)|\mathrm{Sp}(2g, \mathbb{F}_l)|^{-1} \geq \tilde{\omega}(l)(l+1)^{-g}.$$

The proof of the above lemma, although short, is quite technical and can be found as the proof of Lemma 7.2 in [Kow06].

The next results are technical estimates which won't be proved since they are only required in this precise form for the proof of the uniform version of Chavdarov's theorem. The proofs can be found in [Kow06] (see Lemma 7.3).

Recall the following terminology: if f is a monic polynomial of degree g in $\mathbb{Z}[T]$ which factorizes modulo a prime l as

$$f = f_1 \cdots f_r$$

with the f_i coprime, irreducible, of degree $d_i \geq 1$, then one says that the *cycle type* (or the conjugacy class) associated to f is the conjugacy class in S_g of elements which are product of disjoint cycles of lengths $d_1, \ldots, d_r$.

Lemma 3.14. *1. Let $g \geq 1$ and let c be a conjugacy class in S_g. For l prime, let*

$$\hat{\Omega}_c(l) = \{f \in \mathbb{F}_l[T] | f \text{ is monic of degree } g \text{ and the cycle type associated to } f \text{ is } c\},$$

and $\hat{\omega}_c(l) = |\hat{\Omega}_c(l)|$. Then we have for $l > 4g^2$

$$\hat{\omega}_c(l) \geq \frac{|c|}{|S_g|}(l-1)^g \left(1 - \frac{1}{\sqrt{l}}\right)^g.$$

2. *Let $g \geq 1$ and for l prime let $\omega_1(l)$ be the number of q-symplectic irreducible polynomials in $\mathbb{F}_l[T]$ of degree $2g$. Then for $l > 4g^2$ we have*

$$\omega_1(l) \geq \frac{l^g}{2g}\left(1 - \frac{1}{l}\right)^g - l^{g/2}.$$

3. *Let $g \geq 1$ and for l prime let $\omega_2(l)$ be the number of q-symplectic polynomials of degree $2g$ which factorize as a product of an irreducible quadratic polynomial and a product of irreducible polynomials of odd degrees. Then we have for $l > 4g^2$*

$$\omega_2(l) \geq \frac{l^g}{4g}\left(1 - \frac{1}{l}\right)^g.$$

3.6 Proof of the uniform version of Chavdarov's theorem

We will now prove Theorem 3.10. We will apply Proposition 3.8 with the following data: in addition to U, which is a smooth geometrically connected affine curve over $\mathbb{F}_q$, we take the sheaves $\tilde{\mathcal{F}}_l = R^1 f_! \mathbb{F}_l$ for $l \in \Lambda$, where Λ is the set of odd primes.

These sheaves are obtained by reduction modulo l from the compatible system $\mathcal{F}_l = R^1 f_! \mathbb{Z}_l$. The existence of the symplectic pairing (3.15) implies that the arithmetic monodromy group of $\tilde{\mathcal{F}}_l$ can be seen as a subgroup of $\mathrm{SSp}(2g, \mathbb{F}_l$, and for any $u \in U(\mathbb{F}_q)$, the image of Fr_u has multiplicator q.

Crucially, for $l > 2$, we use the unpublished result by Yu ([Yu97]) which states that the geometric monodromy group for $\tilde{\mathcal{F}}_l$ is equal to $\mathrm{Sp}(2g, \mathbb{F}_l)$. Then the sheaves $(\tilde{\mathcal{F}}_l)$ are also linearly disjoint as a consequence of Goursat's lemma (see Corollary 3.6), and by Lemma 3.2 we have (3.9) with $\kappa = 2$. And finally, Lemma 3.3 (2) give us (3.10) with $s = 2g^2 + g + 1, t = g + 1$ and $c_1 = 1, c_2 = 6^g$.

Thus all conditions needed to apply Proposition 3.8 in the case of a one-parameter family (such as in Theorem 3.10) are valid. We now set up the sieving problem. As in Lemma 3.13, for any choice of sets $\tilde{\Omega}(l) \subset \Upsilon_{g,l}$ defined for $l > 2$ we let

$$\Omega(l) = \{g \in \mathrm{SSp}(2g, \mathbb{F}_l) | m(g) = q, \text{ and } \deg(1 - Tg) \in \tilde{\Omega}(l)\}.$$

Applying Proposition 3.8 (see (3.13)) to this sieving problem, we get

$$|S(U, \Omega; L)| \leq (2q + 4gq^{1/2}(6L)^A)P(L)^{-1}, \tag{3.19}$$

where $A = 2g^2 + 3g/2 + 5/2$ and

$$P(L) = \sum_{2<l\leq L} \omega(l)|G_l^g|^{-1}, \tag{3.20}$$

and here we have taken the constant $C = 4g$. Moreover, by Lemma 3.13, we have

$$P(L) \geq \sum_{2<l\leq L} \tilde{\omega}(l)(l+1)^{-g}. \tag{3.21}$$

To use this sieve estimate to study the characteristic polynomials P_u, we will recall the following two facts:

1. If $f \in \mathbb{Z}[T]$ is a polynomial of degree d that factorizes in $\mathbb{F}_l[T]$ as a product of coprime polynomials $f_1 \cdots f_r$, with f_i irreducible of degree d_i, then the Galois group of f, seen as a permutation group of the complex roots of f, contains a

cycle c of type $(d_1, \dots, d_r)$, i.e., a product of disjoint cycles of respective length $d_1, \dots, d_r$.

2. The reduction modulo a prime l of a polynomial P_u (the numerator of the zeta function of the curve $C_u = \pi^{-1}(u)$) is the characteristic polynomial of Fr_u acting on $\tilde{\mathcal{F}}_l$.

Thus (2) allows us to control the reduction of a polynomial P_u, while (1) tells us that the reduction gives information on the Galois group of P_u.

In particular, for any sieving sets $\Omega(l) \subset \mathrm{SSp}(2g, \mathbb{F}_l)$, an element $u \in S(U, \Omega; L)$ will have the property that the Galois group of P_u, seen as a subgroup of S_{2g}, does not contain a cycle c associated to an $f \in \Omega(l)$, where l ranges over primes $2 < l \leq L$.

If we have finitely many sieving sets Ω_i, $1 \leq i \leq m$, defined by the condition that the cycle associated to $\det(1 - Tg)$ is in a certain conjugacy classes, and if moreover those c_i have the property that the only subgroup $W \subset W_{2g}$ containing an element of each c_i is W_{2g}, then it follows that the set of exceptional $u \in U(\mathbb{F}_q)$ with P_u having small Galois group will be a subset of the union of the $S(U, \Omega_i; L)$. So in such a situation we have

$$\begin{aligned} N(U/\mathbb{F}_q) &\leq S(U, \Omega_1; L) + \cdots + S(U, \Omega_m; L) \\ &\leq (2q + 4gq^{1/2}L^A) \sum_{1 \leq i \leq m} P_i(L)^{-1}. \end{aligned} \tag{3.22}$$

Lemma 3.12 describes three possible choices of sets c_i; however, the first and the second involve some c_i which are "too" small, so the dependency on g in the estimate for $P_c(L)$ is bad. Thus we use case (3) of Lemma 3.12. Precisely, we have $m = 4$ and the four sets Ω_i can be described as follows:

1. Ω_1 is the set of irreducible polynomials $f \in \Upsilon_{g,l}$.

2. Ω_2 is the set of polynomials $f \in \Upsilon_{g,l}$ which factorize as a product of an irreducible quadratic polynomial and a product of irreducible polynomials of odd degrees.

   To define Ω_3 and Ω_4, recall that any $f \in \Upsilon_{g,l}$ can be written uniquely

   $$f = T^g h(qT + T^{-1})$$

   where $h \in \mathbb{F}_l[T]$ is a monic polynomial of degree g.

3. Ω_3 is the set of $f \in \Upsilon_{g,l}$ such that the corresponding h has an irreducible factor of prime degree $> g/2$.

4. Ω_4 is the set of $f \in \Upsilon_{g,l}$ such that the corresponding h has a single quadratic irreducible factor and no other irreducible factor of even degree.

These sets allow us to sieve the exceptional elements u. From the relation between the factorization of P_u modulo l and the existence of elements in the Galois group of P_u with the associated cycle type, we see that:

1. If P_u is reducible then $u \in S(U, \Omega_1; L)$.

2. If P_u is irreducible but the Galois group W does not contain a transposition, then $u \in S(U, \Omega_2; L)$, since having $P_u (\mathrm{mod}\ l) \in \Omega_2(l)$ implies that W contains

an element with cycle type consisting of one 2-cycle and further cycles of odd length, a power of which will be a transposition.

For the next two facts, we note that the cycle in S_g associated to the polynomial Q_u such that $P_u = T^g Q_u(qT + T^{-1}$ is the image by the map $p : W_{2g} \to S_g$ of the cycle associated to P_u.

3. If P_u is irreducible but $p(W)$ does not contain a cycle of prime order $m > g/2$, then $u \in S(U, \Omega_3; L)$.

4. If P_u is irreducible but $p(W)$ does not contain a transposition, then $u \in S(U, \Omega_4; L)$.

Therefore, by case (3) of Lemma 3.12, the $u \in U(\mathbb{F}_q)$ that should be excluded are in the union of the $S(U, \Omega_i; L)$, and we conclude that

$$\begin{aligned} N(U/\mathbb{F}_q) &\leq S(U, \Omega_1; L) + \cdots + S(U, \Omega_4; L) \\ &\leq 4(2q + 4gq^{1/2}(6L)^A) \left(\min \sum_{1 \leq i \leq 4} P_i(L) \right)^{-1}. \end{aligned} \tag{3.23}$$

It remains to give appropriate lower bounds of $P_i(L)$. For Ω_3 and Ω_4, since the correspondence between polynomials $f \in \Upsilon g, l$ and the $h \in \mathbb{F}_l[T]$ such that $f = T^g h(qT + T^{-1})$ is one-to-one, we can count the corresponding h by Lemma 3.14, applied to the cycle types (i.e., conjugacy classes) in S_g associated to the polynomials in Ω_i. For $l > 4g^2$ and $i \in \{3, 4\}$, denoting by C_i the set of elements in S_g having the associated cycle type, we get

$$\tilde{\omega_i}(l) \geq \frac{|C_i|}{|S_g|}(l-1)^g \left(1 - \frac{1}{\sqrt{l}}\right)^g,$$

and thus for $L > 4g^2$ we have

$$P_i(L) \geq \frac{|C_i|}{|S_g|} \sum_{4g^2 < l \leq L} \left(\frac{l-1}{l+1}\right)^g \left(1 - \frac{1}{\sqrt{l}}\right)^g.$$

By the mean value theorem we have for any $l \geq 2$

$$\left(\frac{l-1}{l+1}\right)^g \left(1 - \frac{1}{\sqrt{l}}\right)^g = 1 - gh(l) + O(g^2 h(l)^2)$$

with

$$h(l) = \frac{2}{l+1} + \frac{1}{\sqrt{l}} - \frac{2}{\sqrt{l}(l+1)},$$

and an absolute implied constant. Inserting this in the sum and using the prime number theorem, we get for $L > 4g^2$ that

$$P_i(L) \geq \frac{|C_i|}{|S_g|}(\pi(L) + O(g\sqrt{L}(\log L)^{-1} + g^2 \log\log L)), \tag{3.24}$$

with an absolute implied constant.

By [Gal73, p. 99] (where our C_3 is denoted P and C_4 is denoted T), we have for $g \geq 1$

$$\frac{|C_3|}{|S_g|} \gg \frac{1}{\log 2g} \quad \text{and} \quad \frac{|C_4|}{|S_g|} \gg \frac{1}{\sqrt{g}}. \tag{3.25}$$

Using (3.24), this gives the lower bounds

$$P_3(L) \gg \frac{1}{\log 2g} L(\log L)^{-1}, \quad \text{and} \quad P_4(L) \gg \frac{1}{\sqrt{g}} L(\log L)^{-1} \tag{3.26}$$

with absolute implied constants for $L \gg g^2(\log 2g)$ (i.e. for $L \geq \alpha_1 g^2(\log 2g)$, where the absolute constant α_1 can be specified from the implied constants in (3.24) and (3.25)).

Coming to Ω_1, we have by (2) of Lemma 3.14 that for $l > 4g^2$

$$\tilde{\omega}_1(l) \geq \frac{l^g}{2g}\left(1 - \frac{1}{l^g}\right) - l^{g/2}$$

and so by (3.21), the prime number theorem and the mean-value theorem as before, we get for $L > 4g^2$ that

$$P_1(L) \geq \frac{1}{2g}(\pi(L) + O(g \log\log L + g^2 + \sqrt{L}))$$

with an absolute implied constant, and hence for $L \gg g^2(\log 2g)$, we have

$$P_1(L) \gg \frac{1}{g} L(\log L)^{-1} \tag{3.27}$$

with absolute implied constant.

Finally, by (3) of Lemma 3.14 we have for $l > 4g^2$

$$\tilde{\omega}_2(l) \geq \frac{1}{4g}\left(1 - \frac{1}{l}\right)^g \quad \text{and} \quad P_2(L) \geq \frac{1}{4g}(\pi(L) + O(g \log\log L + g^2))$$

and for $L \gg g^2(\log 2g)$ we obtain also

$$P_2(L) \gg \frac{1}{g} L(\log L)^{-1} \tag{3.28}$$

with absolute implied constant.

In conclusion, from (3.23), (3.26), (3.27) and (3.28) we get

$$N(U/\mathbb{F}_q) \ll g^2(2q + q^{1/2}(6L)^A)L^{-1}(\log L)$$

with an absolute implied constant. We can choose this constant in a way so that the inequality is valid for all $L \geq 2$ and $g \geq 1$, since it becomes trivial for $g^2 \gg L(\log L)^{-1}$. Choosing $6L = q^{(2A)^{-1}} = q^{(4g^2+3g+5)^{-1}}$, with $\log L \ll g^{-2}\log q$, this gives the announced uniform estimate

$$N(U/\mathbb{F}_q) \ll q^{1-\gamma}(\log q)$$

with $\gamma = (4g^2 + 3g + 5)^{-1}$, and an implied constant depending only on g.

3.7 An algebraic criterion for independence

Let $g \geq 1$ be a fixed integer, and let W_{2g} be the finite group of order $2^g g!$ which is described by the following equivalent definitions:

- it is the group of permutations of a finite set M of order $2g$ which commute with a give involution c on M without fixed points:

$$\sigma(c(\alpha)) = c(\sigma(\alpha)) \text{ for all } \alpha \in M;$$

  we write usually $c(\alpha) = \bar{\alpha}$, so that $\overline{\sigma(\alpha)} = \sigma(\bar{\alpha})$.

- given a set of M with $2g$ elements which is partitioned in a set N of g couples $\{x, y\}$, W_{2g} is the subgroup of the group of permutations of M which permute the set of pairs N.

The second definition provides a short exact sequence

$$1 \to \{\pm 1\}^g \to W_{2g} \to S_g \to 1. \tag{3.29}$$

The set N of the second definition can also be described as the quotient of M modulo the equivalence relation induced by c ($\alpha \sim \bar{\alpha}$). We now state some properties of the group W_{2g}, which we assume to be given with some set M and set N of couples on which W_{2g} acts, as in the second definition.

We let $F(M) = \mathbb{Q}^M$ be the $\mathbb{Q}$-vector space generated by M. We will denote the canonical basis of $F(M)$ by $(f_\alpha)_{\alpha \in M}$. We will also consider $F(M)$ as given with the associated permutation representation of W_{2g}.

Lemma 3.15. *Let $g \geq 2$ be any integer, W_{2g}, M, N and $F(M)$ as before. Then*

1. *The group W_{2g} acts transitively on M, and acts on $M \times M$ with three orbits:*
   - $\Delta = \{(\alpha, \alpha) | \alpha \in M\}$,
   - $\Delta_c = \{(\alpha, \bar{\alpha}) | \alpha \in M\}$,
   - $O = \{(\alpha, \beta) | \alpha \neq \beta, \bar{\alpha} \neq \beta\}$.
2. *The representation of W_{2g} on $F(M)$ decomposes as the direct sum*

$$F(M) = \mathbf{1} \oplus G(M) \oplus H(M)$$

   of the three subspaces defined by

$$\mathbf{1} = \mathbb{Q}\psi \subset F(M), \text{ where } \psi = \sum_{\alpha \in M} f_\alpha,$$

$$G(M) = \left\{ \sum_{\alpha \in M} t_\alpha f_\alpha \in F(M) | t_\alpha - t_{\bar{\alpha}} = 0, \alpha \in M, \text{ and } \sum_{\alpha \in M} t_\alpha = 0 \right\},$$

$$H(M) = \left\{ \sum_{\alpha \in M} t_\alpha f_\alpha \in F(M) | t_\alpha + t_{\bar{\alpha}} = 0, \alpha \in M \right\},$$

   which are absolutely irreducible representations of W_{2g}.

Proof. 1. The transitivity of W_{2g} on M is clear since by definition, elements of W_{2g} only permute the elements of M. Furthermore, it is obvious that the sets Δ, Δ_c, O form a partition of $M \times M$, and that Δ is the orbit of any fixed $(\alpha, \alpha) \in \Delta$ by transitivity.

Δ_c is also an orbit. To check this, fix some $x_0 = (\alpha_0, \bar{\alpha}_0 \in \Delta_c$, and let $x = (\alpha, \bar{\alpha}) \in \Delta_c$ be arbitrary. If σ is any element of W_{2g} such that $\sigma(\alpha_0) = \alpha$, we have $\sigma(\bar{\alpha}) = \bar{\alpha}_0$, hence $\sigma(x_0) = x$.

Finally, we need to check that O is an orbit. $O \neq \emptyset$ because $g \geq 2$ (so that there exist $(\alpha, \beta) \in M \times M$ with $\beta \notin \{\alpha, \bar{\alpha}\}$). Using the fact that for any $\gamma \neq \delta$ in M, there exists $\sigma \in W_{2g}$ such that $\sigma(\gamma) = \delta$ and σ acts as identity on $M \setminus \{\gamma, \bar{\gamma}, \delta, \bar{\delta}\}$, it is clear that if $y = (\alpha, \beta) \in O$, then all elements of O of the form (α, γ) are in the orbit of y, and so are all elements of the form (γ, β).

So given $y_1 = (\alpha, \beta)$ and $y_2 = (\gamma, \delta) \in O$, we can find σ_1 such that $\sigma(y_1) = (\alpha, \delta)$, then σ_2 such that

$$\sigma_1\sigma_2(\alpha, \beta) = \sigma_2(\alpha, \delta) = (\gamma, \delta) = y_2,$$

so O is a single orbit as desired.

2. Again from the definition, it is clear that $\mathbf{1}, G(M)$ and $H(M)$ are W_{2g}-invariant subspaces of $F(M)$, and it suffices to check that the representation $F(M) \otimes \mathbb{C}$ is a direct sum of three irreducible components. This means that we must show that
$$\langle \chi, \chi \rangle = 3$$
where χ is the character of the representation of W_{2g} on $F(M) \otimes \mathbb{C}$, as 3 can only be written as $1+1+1$ as sum of squares of positive integers. Since χ is real-valued, we have $\langle \chi, \chi \rangle = \langle \chi^2, 1 \rangle$; further χ^2 is the character of the permutation presentation of W_{2g} on $M \times M$, and hence, as for any permutation character, the inner product $\langle \chi^2, 1 \rangle$ is the number of orbits of the action of W_{2g} on $M \times M$, which is equal to 3 as argued before.

□

Corollary 3.16. *Let $k \geq 1$ be an integer and $W = W_{2g} \times \cdots \times W_{2g}$, the product of k copies of W_{2g}, the j-th copy acting on M_j. Consider the action of W on the disjoint union*

$$M = \bigsqcup_{1 \leq j \leq k} M_j$$

where the j-th factor acts trivially on M_i for $i \neq j$. Let $F(M)$ denote the permutation representation of W on the $\mathbb{Q}$-vector space $\mathbb{Q}^M$ of dimension $2kg$. Then $F(M)$ is $\mathbb{Q}$-isomorphic to the direct sum

$$F(M) \simeq k \cdot \mathbf{1} \oplus \bigoplus_{1 \leq j \leq k} G_j \oplus \bigoplus_{1 \leq j \leq k} H_j$$

of geometrically irreducible representations of W, where G_j is the representation $G(M_j)$ of the previous lemma, $\sigma_1, \ldots, \sigma_k$ acting as σ_j, and similarly H_j is $H(M_j)$ acting through the j-th factor W_{2g}.

Proof. This is clear from Lemma 3.15 and the definition of M. □

Since Corollary 3.16 has described explicitly the decomposition of $F(M)$ as sum of irreducible representations of W, the theory of linear representations of finite groups shows that there are very few possibilities for the subrepresentations $\mathrm{Rel}(M)_a$ and $\mathrm{Rel}(M)_m \otimes \mathbb{Q}$.

Proposition 3.17. *Let $k \geq 1$ and $g \geq 2$ be integers. Let $P_1, \ldots, P_k$ be polynomials satisfying the conditions above. With notation as above, in particular $P = P_1 \cdots P_k$*

and M the set of zeros of P, assume in addition that for any pair of roots $(\alpha, \bar{\alpha}$, we have $\alpha\bar{\alpha} \in \mathbb{Q}^*$.

1. *We have*
$$\mathrm{Rel}(M)_a = \bigoplus_{1\le j\le k} \mathrm{Rel}(M_j)_a,$$
and for each j, we have either $\mathrm{Rel}(M_j)_a = 0$, or $\mathrm{Rel}(M_j)_a = 1$. The latter alternative holds if and only if
$$\sum_{\alpha\in M_j} \alpha = 0$$
or equivalently if $\mathrm{Tr}_{K/E}(\alpha) = 0$ for any $\alpha \in M_j$.

2. *We have*
$$\mathrm{Rel}(M)_m \otimes \mathbb{Q} = \bigotimes_{1\le j\le k} \mathrm{Rel}(M_j)_m \otimes \mathbb{Q}.$$
Moreover, assume that the rational number $\alpha\bar{\alpha} \in \mathbb{Q}$ is positive ad independent of α, say equal to m. Then for $g \ge 5$ in the general case and for $g \ge 2$ if $m = 1$, we have for each j that
$$\mathrm{Rel}(M_j)_m \otimes \mathbb{Q} = \begin{cases} \mathbf{1} \oplus G(M_j) & \text{if } m = 1, \\ G(M_j) & \text{otherwise.} \end{cases}$$

Proof. 1. From representation theory, we know that $\mathrm{Rel}(M)_a$ is the direct sum of some subset of the irreducible components of $F(M)$ corresponding to the decomposition in Corollary 3.16. This isomorphism shows that $F(M)$ decomposes as a direct sum over j of representations $F(M_j)$ depending on the j-th factor of W, each of which is given by Lemma 3.15. Accordingly, $\mathrm{Rel}(M)_a$ is the direct sum over j of subrepresentations of $F(M_j)$. Those are representations of the j-th factor W_{2g} extended by the identity to W, and tautologically, they correspond exactly to the relation space $\mathrm{Rel}(M_j)_a$ among zeros of P_j.

To finish the proof, it suffices therefore to treat each P_j in turn, so we might as well assume $k = 1$ and remove the subscript j, using notation in Lemma 3.15 (in particular, writing now M instead of M_j). Noting that, for any $\alpha \in M$, the relation $\mathrm{Tr}_{K/E}(\alpha) = 0$ is equivalent with $\mathbf{1} \subset \mathrm{Rel}(M)_a$, the claim then amounts to saying that $G(M)$ and $H(M)$ cannot occur in $\mathrm{Rel}(M)_a$.

First, $G(M) \subset \mathrm{Rel}(M)_a$ means that
$$\sum_{\alpha} t_\alpha \alpha = 0 \tag{3.30}$$
whenever $(t_\alpha) \in \mathbb{Q}^M$ sum to zero and satisfy $t_\alpha - t_{\bar{\alpha}} = 0$ for $\alpha \in M$. In particular, fix a root α of P; we find that for any $\sigma \in W_{2g}$ with $\sigma(\alpha) \ne \alpha$, say $\sigma(\alpha) = \beta$, we have
$$(\alpha + \bar{\alpha}) - (\beta + \bar{\beta}) = (\alpha + \bar{\alpha}) - \sigma(\alpha + \bar{\alpha}) = 0$$
for all $\sigma \in W_{2g} = \mathrm{Gal}(K/\mathbb{Q})$ not fixing α. Since the last relation is trivially valid for σ fixing α (hence $\bar{\alpha}$), it follows that $\alpha + \bar{\alpha} \in \mathbb{Q}$. From the assumption $\alpha\bar{\alpha} \in \mathbb{Q}^*$, it follows that $\mathbb{Q}(\alpha)$ is a quadratic field. It must be the splitting field K of the polynomial P, and hence this cannot occur under the conditions $g \ge 2$ and $\mathrm{Gal}(K/\mathbb{Q}) = W_{2g}$.

Similarly $H(M) \subset \mathrm{Rel}(M)_a$ means that (3.30) holds whenever $(t_\alpha) \in \mathbb{Q}^M$ satisfy $t_\alpha + t_{\bar\alpha} = 0$. Using again a fixed root α of P, we obtain in particular

$$\alpha - \bar\alpha = 0 \tag{3.31}$$

which contradicts the fact that the elements α and $\bar\alpha$ are distinct.

2. The proof of the direct sum decomposition for $\mathrm{Rel}(M)_m \otimes \mathbb{Q}$ is the same as that for additive relations, and hence we are again reduced to the case $k = 1$ (and we write M instead of M_j). We first show that $G(M) \subset \mathrm{Rel}(M)_m \otimes \mathbb{Q}$ in all cases. Indeed, considering the generators of $G(M)$ (given by $(f_{\alpha_i}+f_{\bar\alpha_i})-(f_{\alpha_{i+1}}+f_{\bar\alpha_{i+1}})$, $1 \le i \le g-1$), it suffices to show that

$$\frac{\alpha\bar\alpha}{\beta\bar\beta} = 1$$

for all α and β, and this is correct from our assumption that $\alpha\bar\alpha$ is independent of α.

Now we consider the consequences of the possible inclusion of the subrepresentations $\mathbf{1}$, and $H(M)$ in $\mathrm{Rel}(M)_m \otimes \mathbb{Q}$. First, $\mathbf{1} \subset \mathrm{Rel}(M)_m \otimes \mathbb{Q}$ means exactly that for some integer $n \ge 1$, we have

$$n\psi = \sum_{\alpha \in M} n f_\alpha \in \mathrm{Rel}(M)_m,$$

which is equivalent to

$$\prod_{\alpha \in M} \alpha^n = \left(\prod_{\alpha \in M} \alpha\right)^n = (N_{K/E}(\alpha))^n = 1.$$

But the assumption that $\alpha\bar\alpha = m$ be a positive rational number independent of α implies that $N_{K/E}(\alpha) = m^g$, so $\mathbf{1} \subset \mathrm{Rel}(M)_m \otimes \mathbb{Q}$ if and only if $m = 1$.

It remains to exclude the possibility that $H(M) \subset \mathrm{Rel}(M)_m \otimes \mathbb{Q}$ to conclude the proof. But instead of (3.31), this possibility implies now that, for some integer $n \ge 1$, we have

$$\alpha^{2n} = m^n \left(\frac{\alpha^{2n}}{m^n}\right) = m^n \left(\frac{\alpha}{\bar\alpha}\right)^n = m^n.$$

Hence $K/\mathbb{Q}$ would be the Kummer extension $\mathbb{Q}(\sqrt{m}, \mu_{2n})$, where μ_{2n} is the group of $2n$-th roots of unity. In particular, the Galois group of K/E would be solvable, which is false for W_{2g} if $g \ge 5$ (the non-solvable group A_g occurs as one composition factor). For $m = 1$, the Galois group would be abelian, which is not the case of W_{2g} for $g \ge 2$.

□

3.8 Proof of Theorem 3.1

Consider a squarefree monic polynomial $f \in \mathbb{Z}[X]$ of degree $2g$ and an odd prime p not dividing the discriminant of f. Let $q \ne 1$ be a power of p. For each $t \in \mathbb{F}_q$ with $f(t) \ne 0$, we consider the (smooth projective model of the) hyperelliptic curve

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

which is of genus g so that the L-function $P_t \in \mathbb{Z}[T]$ of C_t, as defined in the introduction, has degree $2g$.

For a fixed q, we say that $t \in \mathbb{F}_q$ is *special* if any one of the following condition holds:

- $f(t) = 0$.
- The Galois group of the splitting field of P_t is not isomorphic to W_{2g}.
- The sum of the inverse roots $\alpha \in \mathcal{Z}(C_t)$ is 0.

Then, under the assumptions stated, it follows from Theorem 8.15 in [Kow08a] (which is similar to Theorem 3.10) that

$$|\{t \in \mathbb{F}_q | t \text{ is special}\}| \ll q^{1-\gamma}(\log q),$$

where $\gamma = \frac{1}{4g^2+2g+4}$ and the implied constant depends only on g. We will show that the roots of the zeta function of C_t, if t is not special, satisfy the two independence conditions in Theorem 3.1, and this will finish the proof.

For convenience, we drop the dependency on t (t is fixed) from the notation now on in cases where it does not lead to any ambiguity. The additive case is clear from (1) of Proposition 3.17 applied with $k = 1, m = q$ and

$$P = T^{2g} P_t(T^{-1}) \in \mathbb{Z}[T]$$

(which has the $\alpha \in \mathcal{Z}(C_t)$ as roots), since the splitting field of K of this polynomial is the same as that of P_t, hence its Galois group is indeed W_{2g}, and the sum of the roots of P is non zero for t not special, from the definition.

Now we come to the multiplicative independence of the normalized inverse roots. Recall first that with $M = \tilde{\mathcal{Z}}(C_t)$, and involution given by

$$\bar{\alpha} = c(\alpha) = \frac{1}{\alpha}$$

the desired conclusion (3.6) can be rephrased as

$$\mathrm{Rel}(\tilde{\mathcal{Z}}(C_t))_m = \{(n_{\tilde{\alpha}}) \in \mathbb{Z}^M | n_{\tilde{\alpha}} - n_{\tilde{\alpha}^{-1}} = 0\},$$

and the left-hand side does contain the right-hand side, so only the reverse inclusion is required.

The elements of M are roots of the polynomial

$$Q_t = T^{2g} P_t(q^{-1/2} T^{-1}) \in \mathbb{Q}(\sqrt{q})[T],$$

which creates a slight complication: if we extend scalars to $E = \mathbb{Q}(\sqrt{q})$ so that $Q_t \in \mathbb{E}[T]$, there is a possibility that the Galois group of its splitting field (over E) is not W_{2g} any more (for example, when $\sqrt{q}$ is in the splitting field of P_t). We deal with this by looking at the squares of the inverse roots.

Let

$$M' = \{\tilde{\alpha}^2 | \tilde{\alpha} \in M = \tilde{\mathcal{Z}}(C_t)\} = \{\alpha^2/q | \alpha \in \mathcal{Z}(C_t)\};$$

the second expression shows that $M' \subset K = \mathbb{Q}(\mathcal{Z}(C_t))$, so the field $F = \mathbb{Q}(M')$ is a subfield of K. Its Galois group is the group of those $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ which fix all α^2 for $\alpha \in \mathcal{Z}(C_t)$, i.e., such that $\sigma(\alpha) \in \{\alpha, -\alpha\}$ for all α. If $\sigma \in \mathrm{Gal}(K/F)$ is not the identity, there exists some $\alpha \in \mathbb{Z}(C_t)$ such that $\beta = \sigma(\alpha)$ is equal to $-\alpha$, and

this leads to $\alpha + \beta = 0$, in particular to $\mathrm{Rel}(\mathcal{Z}(C_t))_a \neq 0$. Since this contradicts the previous observation that the elements of $\mathcal{Z}(C_t)$ are $\mathbb{Q}$-linearly independent when t is not special, we have in fact $\mathrm{Gal}(K/F) = 1$, and so $F = K$.

We can now apply (2) of Proposition 3.17, with $k = m = 1$ and P taken to be the polynomial with zeros M', namely

$$\prod_{\gamma \in M'} (T - \gamma) = \prod_{\tilde{\alpha} \in M} (T - \tilde{\alpha}^2) \in \mathbb{Q}[T],$$

with $F = K$ such that $\mathrm{Gal}(F/\mathbb{Q}) = W_{2g}$, acting by permutation of the set M' with the involution

$$c(\gamma) = \gamma^{-1}, \text{ i.e. } c(\tilde{\alpha}^2) = \tilde{\alpha}^{-2}.$$

Since $\gamma c(\gamma) = 1$ for all $\gamma \in M'$, we obtain

$$\mathrm{Rel}(M')_m \otimes_{\mathbb{Z}} \mathbb{Q} = 1 \oplus G(M') = \{(n_\gamma) \in \mathbb{Q}^M | n_\gamma - n_{c(\gamma)} = 0, \gamma \in M'\}.$$

Since $\mathrm{Rel}(M')_m$ is free, the natural map $\mathrm{Rel}(M')_m \to \mathrm{Rel}(M')_m \otimes \mathbb{Q}$ is injective. Note also the tautological embedding $\mathrm{Rel}(M)_m \xrightarrow{i} \mathrm{Rel}(M')_m$ induced by the map $\mathbb{Z}^M \to \mathbb{Z}^M$ which maps any basis vector $f_{\tilde{\alpha}}$ of $\mathbb{Z}^M$ to $f_{\tilde{\alpha}^2}$ of $\mathbb{Z}^M$. If $m \in \mathrm{Rel}(M)_m$, we have

$$i(m) \in \{(n_\gamma) \in \mathbb{Q}^M | n_\gamma - n_{c(\gamma)} = 0, \gamma \in M'\}$$

and this means that $\mathrm{Rel}(M)_m = \mathrm{Triv}(M)_m$, as desired.

Bibliography

[Cal06] JS Calcut. "Rationality and the tangent function". In: *preprint* (2006).

[Cha+97] Nick Chavdarov et al. "The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy". In: *Duke Mathematical Journal* 87.1 (1997), pp. 151–180.

[Cha08] Byungchul Cha. "Chebyshev's bias in function fields". In: *Compositio Mathematica* 144.6 (2008), pp. 1351–1374.

[CM05] Alina Carmen Cojocaru and M Ram Murty. *An introduction to sieve methods and their applications*. Vol. 66. Cambridge University Press, 2005.

[DDS98] S Davis, W Duke, and X Sun. "Probabilistic Galois theory of reciprocal polynomials". In: *Expositiones Mathematicae* 16 (1998), pp. 263–270.

[Gal73] Patrick X Gallagher. "The large sieve and probabilistic Galois theory". In: *Proc. Sympos. Pure Math.* Vol. 24. 1973, pp. 91–101.

[Kow06] Emmanuel Kowalski. "The large sieve, monodromy and zeta functions of curves". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 2006.601 (2006), pp. 29–69.

[Kow08a] Emmanuel Kowalski. *The large sieve and its applications: arithmetic geometry, random walks and discrete groups*. Vol. 175. Cambridge University Press, 2008.

[Kow08b] Emmanuel Kowalski. "The large sieve, monodromy, and zeta functions of algebraic curves, 2: independence of the zeros". In: *International Mathematics Research Notices* 2008 (2008).

[Lit28] John E Littlewood. "On the Class-Number of the Corpus P $(\sqrt{-k})$". In: *Proceedings of the London Mathematical Society* 2.1 (1928), pp. 358–372.

[LP97] Martin W Liebeck and László Pyber. "Upper bounds for the number of conjugacy classes of a finite group". In: *Journal of Algebra* 198.2 (1997), pp. 538–562.

[Ros13] Michael Rosen. *Number theory in function fields*. Vol. 210. Springer Science & Business Media, 2013.

[RS94] Michael Rubinstein and Peter Sarnak. "Chebyshev's bias". In: *Experimental Mathematics* 3.3 (1994), pp. 173–197.

[Yu97] Jiu-Kang Yu. "Toward a proof of the Cohen-Lenstra conjecture in the function field case". In: *preprint* (1997).