CURVES AND ZETA FUNCTIONS OVER FINITE FIELDS
ARIZONA WINTER SCHOOL 2014: ARITHMETIC STATISTICS

CHANTAL DAVID
ASSISTANT: ALINA BUCUR

1. Introduction

The lectures will be concerned with statistics for the zeroes of L-functions in natural families. This will include discussions of the number field and the function field case (the latter case being the study of zeta functions and L-functions of curves over finite fields), and comparing the two worlds. Those comparisons are usually through analogy, but we will also discuss some surprising recent work [ERGR13] where the results for L-functions of curves over finite fields (obtained from the deep equidistribution theorems of Katz and Sarnak) can be used to prove results for L-functions over number fields.

Since the work of Montgomery [Mon73] on the pair correlation of the zeroes of the Riemann zeta function, it is known that there are many striking similarities between the statistics attached to zeroes of L-functions and the statistics attached to eigenvalues of random matrices. The work of Montgomery was extended and generalised in many directions, in particular to the study of statistics of zeroes in *families of L-functions*. It is predicted by the Katz and Sarnak philosophy that the statistics for the zeroes in families of L-functions, in the limit when the conductor of the L-functions gets large, follow the distribution laws of classical random matrices. Those conjectures are based on the fact that for L-functions of curves over finite fields, those distribution laws can be proven at the q-limit (when the size of the finite field $\mathbb{F}_q$ tends to infinity). In this case, the zeroes of the L-functions have a spectral interpretation: the zeroes are the reciprocal of the eigenvalues of Frobenius acting on the first cohomology (with ℓ-adic coefficients) of the curve. In their seminal work, Katz and Sarnak [KS99a] used this spectral interpretation, and some deep equidistribution results due to Deligne, to prove that the pair correlation of zeroes of zeta functions of curves of large genus over large finite fields satisfy the Montgomery law (i.e. their result holds averaging over curves of genus g at the limit when q tends to infinity). Katz and Sarnak were then led to conjecture that the corresponding statistics for the zeroes of L-functions *over number fields* should also be given by the random matrix model as the limit for the large conductor. The statistics are then given by the scaling density associated to the random matrix measures when the size of the matrices goes to infinity. There is a vast literature of results investigating those conjectures over number fields, and obtaining partial results confirming the Katz and Sarnak philosophy.

In the last few years, a new approach to study statistics for zeroes of curves over finite fields emerged from the work of Rudnick and his collaborators, which is to obtain statistics for families of curves *for q fixed*, and when the genus of the curves (which is the analogue of the conductor for this case) tends to infinity. Then, one cannot use the powerful equidistribution theorems of Katz and Sarnak, and there are many similarities between the number field and the function field case. Some natural families of curves over finite fields that were studied in the recent years include hyperelliptic curves [KR09, FR10, Rud10, RG12], cyclic ℓ-covers [BDFL10b, CWZ, Xio10b], trigonal curves [Woo12, TX14], families of smooth curves embedded in a fixed ambient space [BDFL10a, EW12, BK12] and Artin-Schreier curves [BDF$^+$12, BDFL, Ent12, Ent13], and we will concentrate in the lectures on those families. We will give a picture of this body of recent work, stressing among others the similarities and differences between the number fields and function fields, the compatibility with the q-limit results of Katz and Sarnak, and the particular geometry of each family which influences the counting and the statistics. Some statistics are very robust, while some others are influenced

Date: March 13, 2014.

by the geometry of each family.

2. Statistics over number fields: n-correlation and n-level density

Let $\zeta(s)$ be the Riemann zeta function defined for $s > 1$ as

$$\zeta(s) \quad = \quad \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1 - p^{-s}\right)^{-1},$$

where the equality between the sum and the Euler product follows from the fundamental theorem of arithmetic. Riemann introduced the idea to look at $\zeta(s)$ as a function of the complex variable s in the complex plane, and he showed that $\zeta(s)$ has analytic continuation to the complex plane $\mathbb{C}$ with a simple pole at $s = 1$, and satisfies the functional equation

$$\Lambda(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \Lambda(1-s),$$

where

$$\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t}\,dt$$

is defined for $\mathrm{Re}(s) > 0$, and have analytic continuation to the whole complex plane with simple poles at $0, -1, -2, \ldots$. From the functional equation and the Euler product, it follows that the only zeroes of $\zeta(s)$ outside the critical strip $0 \leq \mathrm{Re}(s) < 1$ corresponds to the poles of $\Gamma(s/2)$, namely at $s = -2, -4, -6, \ldots$. Those are called the trivial zeroes of $\zeta(s)$.

For the zeroes of $\zeta(s)$ in the critical strip $0 \leq \mathrm{Re}(s) \leq 1$, Riemann made several conjectures. First, if

$$N(T) = \#\left\{\gamma = \sigma + it \,:\, \zeta(\gamma) = 0,\ 0 \leq \sigma \leq 1,\ 0 < t < T\right\},$$

then the Riemann-Von Mangoldt formula states that

$$N(T) \quad = \quad \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + O(\log T) \sim \frac{T\log T}{2\pi}.$$

And of course the famous Riemman Hypothesis (RH): All non-trivial zeroes of $\zeta(s)$ are on the line $\mathrm{Re}(s) = 1/2$.

So, from the Riemann-Von Mangoldt formula, we know how many zeroes we have up to height T. How are they distributed? For example, do they look like $\frac{T\log T}{2\pi}$ random points on an interval of length T? In fact, they do not, for example, they do not cluster as random point tends to do, there is a *repulsion phenomenon* between the zeroes.

Trying to understand the distribution of the zeroes, Montgomery [Mon73] studied the pair correlation of the zeroes. Let

$$\tilde{\gamma} = \frac{\gamma\log T}{2\pi},$$

i.e. we normalise the zeroes so that they have mean spacing 1. Then, for any $\alpha < \beta$, how many zeroes γ, γ' are such that

$$\alpha < \tilde{\gamma} - \tilde{\gamma'} < \beta?$$

Conjecture 2.1 (Montgomery's Pair Correlation conjecture)**.** *Let f be a function in the Schwartz space $\mathcal{S}(\mathbb{R})$ (i.e. smooth and rapidly decreasing). Then*

$$\lim_{T\to\infty}\frac{1}{N(T)}\sum_{0<\gamma,\gamma'\leq T} f(\tilde{\gamma} - \tilde{\gamma'}) = \int_{\alpha}^{\beta} f(x)\left(1 - \left(\frac{\sin(\pi x)}{\pi x}\right)^2\right)dx$$

What Montgomery actually proved was that the above theorem holds for test functions f such that the support of the Fourier transform $\hat{f}$ is limited, giving evidence for the conjecture for general test functions f. We will see how to prove such results, over number fields and over functions fields.

Dyson noticed that Montgomery has found that the pair correlation between zeroes of the Riemann zeta function was given by the same distribution function which gives the pair correlation between eigenvalues of random unitary matrices, when the size of the matrices tends to infinity.

More precisely, let $U(N)$ be the set of $N \times N$ unitary matrices in $M_N(\mathbb{C})$. We recall that a unitary matrix U satisfies the condition

$$U^*U = UU^* = I_N$$

where I_N is the identity matrix and U^* is the conjugate transpose of U. Because U is unitary, its eigenvalues have absolute value 1.

Let $U \in U(N)$, and let $\lambda_k(U) = e^{i\theta_k(U)}$ be the eigenvalues, with $0 \le \theta_1(U) \le \theta_2(U) \cdots \le \theta_N(U) \le 2\pi$. Let $f \in \mathcal{S}(\mathbb{R})$. The pair correlation measures the distribution between pairs of eigenvalues of U, and is defined as

$$C_f(U) = \frac{1}{N} \sum_{\substack{1 \le j,k \le N \\ j \ne k}} f\left(\frac{N}{2\pi}(\theta_j(U) - \theta_k(U))\right).$$

Again, we have normalised the eigenangles in such a way that there are N angles on an interval of length N. Then, with the appropriate measure on $U(N)$ (which is the translation invariant Haar measure), one can show that (see [KS99a])

$$\lim_{N\to\infty} \int_{U(N)} C_f(U)\, dU = \int_\alpha^\beta f(x) \left(1 - \left(\frac{\sin(\pi x)}{\pi x}\right)^2\right) dx. \tag{1}$$

In the 1980s, Andrew Odlyzko began an intensive numerical study of the statistics of the zeros of $\zeta(s)$. He computed millions of zeroes at heights around 10^{20} and spectacularly confirmed the Montgomery's conjecture. We remark that even if we were able to prove Montgomery's Pair Correlation conjecture, it would not mean that the zeroes are distributed as the eigenvalues of large unitary matrix, but that the pair correlations are the same for the two sets. But Montgomery, and others, went on to conjecture that perhaps all the statistics, not just the pair correlation statistic, would match up for zeta-zeros and eigenvalues of random matrices. This conjecture has the flavor of a spectral interpretation of the zeros, though it gives no indication of what the particular operator is.

There is one case where zeroes of zeta functions have a spectral interpretation: the case of zeta functions of curves over finite fields, where the zeroes are the reciprocal of eigenvalues of Frobenius acting on the first cohomology (with ℓ-adic coefficients) of the curve. In their seminal work, Katz and Sarnak used this spectral interpretation, and the equidistribution results due to Deligne, to prove that Montgomery's conjecture is true for the zeta functions of most curves of large genus over large finite fields, i.e. their result holds averaging over curves of genus g at the limit when q and g tends to infinity, see [KS99a, Theorem 12.2.3].

Katz and Sarnak also studied other families of curves over finite fields, and it is believed that the statistics for families of L-functions of curves over finite fields should match up the statistics for eigenvalues of classical matrix groups at the q-limit, provided that the monodromy group of the family is big enough, i.e. for families where one can prove an analogue of Deligne's equidistribution theorem [Del74, Del80], which is one of the main ingredient for proving Montgomery's conjecture for L-functions of curves over finite fields.

Back to the number field world, the work of Montgomery was massively generalised by Rudnick and Sarnak [RS96] to the n-correlation of L-functions $L(s,\pi)$ attached to cuspidal automorphic representations of GL_m over $\mathbb{Q}$, again for test functions f with Fourier transform of limited support. Let $C_f^{(n)}(T)$ be the n-correlation between the zeroes of $L(s,\pi)$ at height T with test function $f \in \mathcal{S}(\mathbb{R}^n)$ (i.e. $C_f^{(n)}(T)$ measures the distribution of the differences between the normalised imaginary parts of all sets of n zeroes at height T). Then, it is shown in [RS96] that

$$\lim_{T\to\infty} C_f^{(n)}(T) = \int_{\mathbb{R}^n} f(x_1,\dots,x_n)\, W^{(n)}(x_1,\dots,x_n)\, dx_1 \dots dx_n,$$

where the test function $f(x_1,\dots,x_n)$ is such that its Fourier transform $\hat{f}(u_1,\dots,u_n)$ has support contained in $\sum_{j=1}^n |u_j| < 2/m$, and where $W^{(n)}(x_1,\dots,x_n)$ is the scaling density for the n-correlation between eigenvalues of large unitary matrices. For $n = 1$ and $L(s,\pi) = \zeta(s)$, we have that

$$\begin{aligned} C_f^{(1)}(T) &= \frac{1}{N(T)} \sum_{0<\gamma,\gamma'\le T} f(\tilde{\gamma} - \tilde{\gamma'}) \\ W^{(1)}(x) &= 1 - \left(\frac{sin(\pi x)}{\pi x}\right)^2, \end{aligned}$$

and we retrieve the result of Montgomery. We will define the scaling density more precisely in the context of the n-level density in Section 2.1.

Then, the scaling density for the n-level correlation is universal, i.e. it is the same for all L-functions. However, other statistics, as the one-level density, or in general the n-level density, will differ depending of the "symmetry type" of the family (unitary, symplectic, orthogonal, even orthogonal and odd orthogonal).

2.1. **One-level density.** The pair correlation is a universal statistics, and it is believed to be the same for all families of L-functions. We will see other examples of such statistics, as the number of (normalised) zeroes in intervals for families of curves over finite fields. There are some statistics which depend on the symmetry type of the family, as the one-level density, or in general the n-level density. We discuss in this section the n-level density for 2 families of L-functions: Dirichlet L-functions (with symplectic symmetries) and L-functions attached to elliptic curves (with orthogonal symmetries). In particular, we explain how the explicit formulas can be used to get results about the n-level density for test functions with Fourier transform of limited support. This should be compared with case of function fields that we will study afterwards.

The one-level density is about the behavior of low-lying zeroes of L-functions, so we need to consider families of L-functions, as inspired by the work of Katz and Sarnak, in order to get statistics. We first consider families of L-functions attached to elliptic curves.

Let E be an elliptic curve over $\mathbb{Q}$ with L-function

$$L(s,E) = \prod_{p\nmid N_E} \left(1 - \frac{a_p(E)}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \prod_{p|N_E} \left(1 - \frac{a_p(E)}{p^s}\right)^{-1},$$

where N_E is the conductor of E, and functional equation

$$\Lambda(s,E) := \frac{\sqrt{N_E}}{2\pi}\Gamma(s)L(s,E) = w_E\Lambda(2-s,E),$$

where $w_E = \pm 1$ is the root number of E.

Let f be an even Schwartz test function, and $\mathcal{F}$ be a family of elliptic curves (we will consider precise families of elliptic curves that will be defined later). For each $E \in \mathcal{F}$, we define

$$W_f(E) = \sum_{\gamma_E} f\left(\frac{\gamma_E}{2\pi}\log X\right). \tag{2}$$

where the sum runs over the imaginary part of the zeroes $\rho_E = 1 + \gamma_E$ of the L-function $L(s,E)$ in the critical strip. The scaling factor $(2\pi)^{-1}\log X$ is inserted to normalise the number of zeroes counted by the test function (then, X is about the size of the conductor of E). Since f is rapidly decreasing, $W_f(E)$ should be thought as counting the number of low-lying zeroes of $L(s,E)$.

Let $\mathcal{F}(X)$ be the set of curves in the family indexed by the parameter X (in particular, the average of $\log N_E$ over the family is asymptotic to $\log X$.) The one-level density over the family $\mathcal{F}(X)$ is then defined as

$$W_f(\mathcal{F}(X)) := \frac{1}{\#\mathcal{F}(X)} \sum_{E\in\mathcal{F}(X)} W_f(E).$$

Katz and Sarnak predicted that one-level density should satisfy

$$\lim_{X\to\infty} W_f(\mathcal{F}(X)) = \int_{\mathbb{R}} f(t)\,\mathcal{W}(t)\,dt, \tag{3}$$

where $\mathcal{W}(G)$ is the one-level scaling density of eigenvalues near 1 in the group of random matrices corresponding to the symmetry type of the family $\mathcal{F}$. By the *scaling density* of a group of random matrices, we mean the limit of the Haar measure in the large matrix size. More precisely, for any $N\times N$ matrix U in one of the classical compact group $G(N)$, we write the eigenvalues as $\lambda_j(U) = e^{i\theta_j}$ with

$$0 \le \theta_1 \le \theta_2 \cdots \le \theta_N < 2\pi.$$

Let $f \in \mathcal{S}(\mathbb{R})$ be a test function, and let

$$W_f(U) = \sum_{j=1}^{N} f\left(\frac{N\theta_j}{2\pi}\right).$$

Let dU be the normalized Haar measure on $G(N)$. It is shown by Katz and Sarnak [KS99a, Appendix] that

$$\lim_{N\to\infty}\int_{G(N)} W_f(U)\,dU = \int_{\mathbb{R}} f(t)\,\mathcal{W}_G(t)\,dt, \tag{4}$$

where

$$\mathcal{W}_G(t) = \begin{cases} 1 & \text{if } G = U; \\ 1-\frac{\sin(2\pi t)}{2\pi t} & \text{if } G = \mathrm{Sp}; \\ 1+\frac{1}{2}\delta_0(t) & \text{if } G = O; \\ 1+\frac{\sin(2\pi t)}{2\pi t} & \text{if } G = SO(\text{even}); \\ 1+\delta_0(t)-\frac{\sin(2\pi t)}{2\pi t} & \text{if } G = SO(\text{odd}); \end{cases} \tag{5}$$

where δ_0 is the Dirac distribution, and $U, \mathrm{Sp}, O, SO(\text{even}), SO(\text{odd})$, are the groups of unitary, symplectic, orthogonal, even orthogonal and odd orthogonal matrices respectively. The function $\mathcal{W}_G(t)$ is called the one-level scaling density of the group G. We refer the reader to [KS99a] for details.

Computing the one-level density for families of curves allow us to identify the symmetry type G of the family, provided that the support of the Fourier transform can be taken large enough, as one cannot distinguish between O, SO(odd) and SO(even) for small support. Indeed, the Fourier transforms of the distributions above are given by

$$\widehat{\mathcal{W}}_G(t) = \begin{cases} \delta_0(t) & \text{if } G = U; \\ \delta_0(t)-\frac{1}{2}\eta(t) & \text{if } G = \mathrm{Sp}; \\ \frac{1}{2}+\delta_0(t) & \text{if } G = O; \\ \delta_0(t)+\frac{1}{2}\eta(t) & \text{if } G = SO(\text{even}); \\ 1+\delta_0(t)-\frac{1}{2}\eta(t) & \text{if } G = SO(\text{odd}); \end{cases} \tag{6}$$

where

$$\eta(t) = \begin{cases} 1 & \text{if } |t|<1; \\ \frac{1}{2} & \text{if } |t|=1; \\ 0 & \text{if } |t|>1. \end{cases} \tag{7}$$

The fact that one cannot distinguish between the three orthogonal distributions for small support of test functions f then follows from Plancherel Theorem. Suppose that the support of $\hat{f}$ is contained in $(-a,a)$. Then, for distributions $\mathcal{W}$, we have

$$\int_{-\infty}^{\infty} f(t)\mathcal{W}(t)dt = \int_{-\infty}^{\infty} \widehat{f}(t)\widehat{\mathcal{W}}(\tau)dt = \int_{-a}^{a} \widehat{f}(t)\widehat{\mathcal{W}}(t)dt$$

and for $G = O, SO(\text{even})$ or $SO(\text{odd})$, $\hat{\mathcal{W}}_G(\tau)$ are undistinguishable for $a<1$ (but are distinguishable for $a>1$).

In order to prove results about the one-level density (or other statistics on zeroes of L-functions as the n-correlation), one uses the *Explicit formulas* for L-functions due to André Weil, in which sum sover the zeroes of $L(s,E)$ are rewritten as sums over the coefficients of $L(s,E)$. To get the explicit formulas, one consider the line integral of the logarithmic derivative

$$\int_{(1+\epsilon)} h(s)\frac{\Lambda_E'(s)}{\Lambda_E(s)}\,ds,$$

for some appropriate test function h. By moving the countour to the line $(-1-\epsilon)$, we pick the residues at the non-trivial zeroes ρ_E of $L(s,E)$, and we can use the functional equation to rewrite the integral on the line $(-1-\epsilon)$ as the original integral, which gives a formula of the type.

$$\int_{(1+\epsilon)} \frac{\Lambda_E'(s)}{\Lambda_E(s)}\,h(s)\,ds = \frac{1}{2\pi i}\sum_{\rho_E} h(\rho_E). \tag{8}$$

By choosing the test function h appropriately, and computing explicitely the integral in (8), we get the explicit formula as follows (see [ILS00] for this version of the explicit formula).

Theorem 2.2. *Let f is an even Schwartz function, and $W_f(E)$ as defined by (2). Then,*

$$W_f(E) = \widehat{f}(0)\frac{\log N_E}{\log X} + \frac{1}{2}f(0) - \sum_{p>3}\frac{2a_p(E)\log p}{p\log X}\ \widehat{f}\left(\frac{\log p}{\log X}\right) + O\left(\frac{\log\log N_E}{\log X}\right),$$

where the Fourier transform is $\hat{f}(u) = \int_{\mathbb{R}} f(x)e^{-2\pi ixu}\,dx$.

Some application of the explicit formulas for elliptic curves include the bound

$$\mathrm{rank}(E) \ll \frac{\log N_E}{\log\log N_E}$$

on the analytic rank (or the rank using the Birch and Swinnerton-Dyer conjectures) under GRH due to Mestre [Mes86], and bounds on the average analytic rank for all elliptic curves over $\mathbb{Q}$ under GRH [Bru92, HB04, You06].

For the one-level density, using the explicit formulas, one can show the following:

Theorem 2.3. [You06] *Let $\mathcal{F}(X)$ the family of all elliptic curves given by Weierstrass equations $E_{a,b} : y^2 = x^3 + ax + b$, with a, b positive integers and such that $|a| \le X^{1/3}, |b| \le X^{1/2}$. Then, as $X \to \infty$,*

$$W_f(\mathcal{F}(X)) \sim \widehat{f}(0) + \frac{1}{2}f(0), \tag{9}$$

for test functions f such that supp$(\widehat{f}) \subseteq (-7/9, 7/9)$.

Remark: What is proven in [You06] is a weighted version of the above, where the sums are smoothed by a smooth and compactly supported function, and we simplified the statement of his results.

It is believed that the family $\mathcal{F}(X)$ has orthogonal symmetries, i.e. the one-level density should be given by the scaling density $\mathcal{W}_{\mathrm{O}}(t)$, and since

$$\int_{\mathbb{R}} f(t)\mathcal{W}_{\mathrm{O}}(t)\,dt = \int_{\mathbb{R}} f(t)\left(1 + \frac{1}{2}\delta_0(t)\right)\,dt = \widehat{f}(0) + \frac{1}{2}f(0),$$

Theorem 2.3 agrees with the belief that the family of all elliptic curves have orthogonal symmetry type. But the limited support of the Fourier transform would also agree with SO(even) or SO(odd) since for any of those three groups, the integrals

$$\int_{\mathbb{R}} f(t)\mathcal{W}_G(t)\,dt = \int_{\mathbb{R}} \widehat{f}(t)\widehat{\mathcal{W}_G}(t)\,dt$$

agree when supp$(\widehat{f}) \subseteq (-1, 1)$.

Theorem 2.4. [You06] *Let $\mathcal{F}(X)$ the family of all elliptic curves given by Weierstrass equations $E_{a,b} : y^2 = x^3 + ax + b^2$, with a, b positive integers and such that $|a| \le X^{1/3}, |b| \le X^{1/4}$. Then, as $X \to \infty$,*

$$W_f(\mathcal{F}(X)) \sim \widehat{f}(0) + \frac{3}{2}f(0), \tag{10}$$

for test functions f such that supp$(\widehat{f}) \subseteq (-23/48, 23/48)$.

This agrees with the belief that the scaling density should be $\delta_0(t) + \mathcal{W}_{\mathrm{O}}(t)$ for this family (where the Dirac function accounts for the fact that each elliptic curve $E_{a,b}$ have positive algebraic rank due to the point of infinite order $(0, b) \in E_{a,b}$).

The fact that one cannot distinguish between symmetry types O, SO(odd) or SO(even) for functions with Fourier transform of limited support can be problematic in families where it is not obvious to guess the symmetry type a priori, as it was for the two families above. Let $\mathcal{F}$ be the one-parameter family of elliptic curves with equation

$$E_t : y^2 = x^3 + tx^2 - (t+3)x + 1, \quad t \in \mathbb{Z}. \tag{11}$$

This is a family of rank 1 over $\mathbb{Q}(t)$, and the sign of the functional equation is -1 for all the specialisation with $t \in \mathbb{Z}$ [Was87, Riz03].

Theorem 2.5. [Mil04] *Let $\mathcal{F}(X)$ be the family of curves $E_t \in \mathcal{F}$ with $t \in \mathbb{Z}$ and $|t| \leq X^{1/6}$. Then, as $X \to \infty$,*

$$W_f(\mathcal{F}(X)) \sim \widehat{f}(0) + \frac{3}{2} f(0), \tag{12}$$

for test functions f such that supp$(\widehat{f}) \subseteq (-1/3, 1/3)$.

Since the sign of the functional equation of every specialisation is -1, it would make sense to conclude that the scaling density should be $\delta_0(t) + \mathcal{W}_{\mathrm{SO(odd)}}(t)$ (where the Dirac function accounts for the global point of infinite order on $E/\mathbb{Q}(t)$), and it was remarked in [Mil04] that the scaling density agrees with this. However, recent work on the one-level density of the same family by David, Huynh and Parks [DHP] show that under the ratios conjecture of Conrey, Farmer and Zirnbauer [CFZ08], the scaling density of this family is

$$\mathcal{W}(t) = \delta_0(t) + \mathcal{W}_{\mathrm{SO(even)}}(t),$$

and the global point induces a shift of the symmetry from SO(odd) to SO(even).

We now discuss the one-level density of another family of L-functions, namely Dirichlet L-functions. Let d be a fundamental discriminant, and let χ_d be the Kronecker symbol

$$\chi_d(n) = \left(\frac{d}{n}\right)$$

which is a primitive quadratic character of conductor d. We denote the non-trivial zeroes of the Dirichlet L-function $L(s, \chi_d)$ by

$$\frac{1}{2} + i\gamma_{d,j}, \quad j = \pm 1, \pm 2, \ldots,$$

where

$$0 \leq \mathrm{Re}\, \gamma_{d,1} \leq \mathrm{Re}\, \gamma_{d,2} \leq \mathrm{Re}\, \gamma_{d,3} \ldots$$

and such that $\gamma_{d,-j} = -\gamma_{d,j}$. We do not assume the GRH here, but if $1/2 + i\gamma$ is a zero, so is $1/2 - i\gamma$ using complex conjugation and the functional equation.

We want to study statistics for the low-lying zeroes of $L(s, \chi_d)$ where d belongs to

$$\mathcal{D}(X) = \{X/2 \leq |d| \leq X \ : \ d \text{ fundamental discriminant}\}.$$

As above, let f be an even Schwartz test function $f \in \mathcal{S}(\mathbb{R})$, and let

$$W_f(d) = \sum_j f\left(\frac{\gamma_{d,j}}{2\pi} \log X\right),$$

where the parameter X is approximately the conductor of the family. We define the one-level density as

$$W_f(\mathcal{D}(X)) = \langle W_f(d) \rangle_{\mathcal{D}(X)} = \frac{1}{\#\mathcal{D}(X)} \sum_{d \in \mathcal{D}(X)} W_f(d).$$

The one-level density for the families of Dirichlet L-function $L(s, \chi_d)$ was studied by Katz and Sarnak [KS99b] and Ozluk and Snyder [ÖS93, ÖS06] who showed when X tends to infinity

$$\langle W_f(d) \rangle_{\mathcal{D}(X)} \sim \int_{\mathbb{R}} f(x) \left(1 - \frac{\sin(2\pi x)}{2\pi x}\right) dx,$$

provided that the support of Fourier transform $\widehat{f}(u)$ is limited to the interval $|u| < 2$. This coincide with the random matrix model as $1 - \frac{\sin(2\pi x)}{2\pi x}$ is the scaling density for the one-level density associated to the group of unitary symplectic matrices, which comes from taking the limit of the average with respect to the Haar probability measure on the matrix groups $\mathrm{USp}(g)$ as in (4).

We now define the n-level density for this family. Let f be a Schwartz function in $\mathcal{S}(\mathbb{R}^n)$ which is even in all the variables, and let

$$W_f^{(n)}(d) = \sum_{\substack{j_1, \ldots, j_n = \pm 1, \pm 2, \ldots \\ |j_k| \text{ distinct}}} f\left(\frac{\gamma_{d,j_1}}{2\pi} \log X, \ldots, \frac{\gamma_{d,j_n}}{2\pi} \log X\right).$$

As for the one-level density, we want to show that

$$W_f^{(n)}(\mathcal{D}(X)) = \left\langle W_f^{(n)}(d) \right\rangle_{\mathcal{D}(X)} \sim \int_{\mathbb{R}} f(x)\, W_{USp}^{(n)}(x)\, dx,$$

where $W_{USp}^{(n)}(x)$ is the scaling density for the n-level density associated to the symplectic symmetries, which comes from taking the scaling limit of the average with respect to the Haar probability measure on the symplectic group. Let $U \in \mathrm{USp}(2g)$. Because of the symplectic pairing, it $e^{i\theta}$ is an eigenvalue, so is $e^{-i\theta}$, and we can label the eigenvalues as $e^{i\theta_{\pm j}}$, for $j = 1, \dots, g$, where $\theta_{-j} = -\theta_j$. We then define

$$W_f^{(n)}(U) = \sum_{\substack{j_1,\dots,j_n = \pm 1,\dots,\pm g \\ |j_k| \text{ distinct}}} f(\theta_{j_1}, \dots, \theta_{j_n}).$$

Then, it is shown in Katz and Sarnak [KS99a, Appendix] that

$$\lim_{g\to\infty} \int_{\mathrm{USp}(g)} W_f^{(n)}(U)\, dU = \int_{\mathbb{R}^n} f(x)\, W_{\mathrm{USp}}^{(n)}(x)\, dx,$$

where the scaling densities $W_{\mathrm{USp}}^{(n)}(x)$ are given by

$$W_{\mathrm{USp}}^{(n)}(x) = \det\left(K(x_i, x_j)\right)_{i,j=1,\dots,n},$$

where

$$K(x,y) = \frac{\sin \pi(x-y)}{\pi(x-y)} - \frac{\sin \pi(x+y)}{\pi(x+y)}.$$

The n-level densities of the family of L-functions of quadratic Dirichlet characters were investigated by Rubinstein [Rub01, Theorem 3.1], who showed that for all $n \geq 2$, one has

$$\lim_{X\to\infty} \left\langle W_f^{(n)}(d) \right\rangle_{\mathcal{D}(X)} = \int_{\mathbb{R}^n} f(x)\, W_{\mathrm{USp}}^{(n)}(x)\, dx$$

for test functions

$$f(x_1, \dots, x_n) = f_1(x_1) \dots f_n(x_n)$$

where each f_i is even and in $\mathcal{S}(\mathbb{R})$, and $\widehat{f}(u_1, \dots, u_n) = \widehat{f_1}(u_1) \dots \widehat{f_n}(u_n)$ is supported in $\sum_{i=1}^n |u_i| < 1$.

In his Ph.D. thesis, Gao [Gaoa, Gaob] tried to extend this support to match the support obtained for the one-level density. Under GRH, he showed that for test functions $f(x_1, \dots, x_n) = f_1(x_1) \dots f_n(x_n)$ as above such that $\widehat{f}(u_1, \dots, u_n)$ supported in $\sum_{i=1}^n |u_i| < 2$, then

$$\lim_{X\to\infty} \left\langle W_f^{(n)}(d) \right\rangle_{\mathcal{D}(X)} = A(f) + \underline{o}(1),$$

where $A(f)$ is a complicated combinatorial expression. Then, to show that the n-level density has the correct scaling density for $\sum_{i=1}^n |u_i| < 2$, it remains to show that

$$A(f) = \int_{\mathbb{R}^n} f(x)\, W_{\mathrm{USp}}^{(n)}(x)\, dx,$$

which was done by Gao [Gaoa, Gaob] for $n = 2, 3$, and by Levinson and Miller [LM] for $n = 4, 5, 6, 7$.

Recently, this was resolved for all n.

Theorem 2.6. *(Entin, Roddity-Gershon and Rudnick, 2013) Assume GRH. Then, for test functions f as above with $\widehat{f}(u_1, \dots, u_n)$ supported in the region $\sum_{i=1}^n |u_i| < 2$, we have for all n that*

$$\lim_{X\to\infty} \left\langle W_f^{(n)}(d) \right\rangle_{\mathcal{D}(X)} = \int_{\mathbb{R}^n} f(x)\, W_{USp}^{(n)}(x)\, dx.$$

The authors of [ERGR13] proved their results by comparing the n-level densities of Dirichlet L-functions by their function field analogue, namely the L-functions of hyperelliptic curves of genus g over a finite field $\mathbb{F}_q$. They can then use the powerful equidistribution theorem of Katz and Sarnak (Theorem 6.1) to pass to the finite field limit and identify the limit with the random matrix model. We will explain this phenomenon at the end of the lectures, after defining L-functions of curves over finite fields, and statistics at the q-limit, or for finite q.

3. Zeta functions and L-functions over function fields

Let q be a power of a prime, and $\mathbb{F}_q$ the finite field with q elements. We study in this section zeta functions and L-functions of function fields over $\mathbb{F}_q$. The main reference for this section is the fantastic book of Michael Rosen *Number theory in function fields* [Ros02].

We first begin by the study of the analogue of the Riemann zeta function, which is basically the zeta function of the function field $\mathbb{F}_q(X)$. For this simple case, we have the following dictionary between the world of number fields and the world of function fields.

Number Fields		Function Fields
$\mathbb{Q}$	$\leftrightarrow$	$\mathbb{F}_q(X)$
$\mathbb{Z}$	$\leftrightarrow$	$\mathbb{F}_q[X]$
p positive prime	$\leftrightarrow$	$P(X)$ monic irreducible polynomial
$\lvert n\rvert$	$\leftrightarrow$	$\lvert F(X)\rvert = q^{\deg F}$

where $\mathbb{F}_q[X]$ is the ring of polynomials over F_q, and $F_q(X)$ is the field of rational functions. Unless otherwise mentioned, all polynomials considered (F, P, etc) are monic.

The analogue of the Riemann zeta function in this context, which we denote by $\zeta_q(s)$, is

$$\zeta_q(s) = \sum_{F \in \mathbb{F}_q[X]} |F|^{-s} = \prod_{P \text{ irreducible}} \left(1 - |P|^{-s}\right)^{-1}, \tag{13}$$

where the Euler product follows from the fact that $F_q[X]$ is a UFD, so every monic polynomial factors as a product of monic irreducible polynomials in a unique way.

As there are q^d monic polynomials of degree d, we can rewrite $\zeta_q(s)$ as

$$\zeta_q(s) = \sum_{d \geq 0} q^d q^{-ds} = (1 - q^{1-s})^{-1}. \tag{14}$$

So, the Riemann Hypothesis is then trivially true for $\zeta_q(s)$ because it has no zeroes!

We now prove the prime number theorem for polynomials. Let a_d be the number of monic irreducible polynomials of degree d. Then, using (13) and (14), we write

$$\zeta_q(s) = \prod_{d=1}^{\infty} \left(1 - q^{-ds}\right)^{-a_d} = (1 - q^{1-s})^{-1},$$

or using $u = q^{-s}$

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

Taking the logarithmic derivative on both sides and multiplying by u, we get

$$\begin{aligned} u\frac{d}{du}\log\left(1-qu\right) &= u\sum_{d=1}^{\infty} a_d \frac{d}{du}\log\left(1-u^d\right) \\ \iff \left(\frac{qu}{1-qu}\right) &= \sum_{d=1}^{\infty} \frac{d a_d\, u^d}{(1-u^d)}. \end{aligned}$$

Expanding both sides into power series using geometric series, and equating coefficients of u^n, we get

$$\sum_{d|n} d\, a_d = q^n,$$

and applying Moebius inversion formula, we get

$$a_n = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}. \tag{15}$$

Theorem 3.1. [Ros02, Theorem 2.2] *(The prime number theorem for polynomials) Let a_n denote the number of irreducible polynomials in $\mathbb{F}_q[X]$. Then,*

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

Proof. From (15), we have that

$$a_n = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n} + \frac{q^{n/3}}{n} \sum_{\substack{d|n \\ d\neq n,\, \frac{n}{2}}} |\mu(d)|\right),$$

and $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime divisors of n. Since $2^{\omega(n)} \leq n$, the result follow. □

One can also use $\zeta_q(s)$ to count the number of square-free polynomials of degree d, which will be needed later.

Lemma 3.2. *Let $\mathcal{F}_d$ be the set of square-free monic polynomials of degree d. Then,*

$$\#\mathcal{F}_d \quad = \quad \begin{cases} q^d - q^{d-1} = \dfrac{q^d}{\zeta_q(2)} & \text{if } d \geq 2 \\ q^d & \text{if } d = 0, 1. \end{cases}$$

Proof. One starts with the identity

$$\zeta_q(s) = \zeta_q(2s) \sum_{d\geq 0} |\mathcal{F}_d|\, q^{-ds},$$

and using $u = q^{-s}$, this writes as

$$\frac{1-qu^2}{1-qu} = \sum_{d\geq 0} |\mathcal{F}_d|\, q^d$$

$$\iff \qquad 1 + qu + \sum_{d=2}^{\infty} (q^d - q^{d-1}) u^d = \sum_{d\geq 0} |\mathcal{F}_d|\, q^d.$$

This shows Lemma 3.2. □

Remark: This is analogous to the result over number fields, namely that the number of square-free positive integers up to x is asymptotic to $x/\zeta(2)$.

In order to define general zeta functions in the function field setting, we need to extend the definition of primes by considering all valuations, not only those associated with prime ideals of $\mathbb{F}_q(X)$, i.e. we need to include "the prime at ∞". Let K be a function field over $\mathbb{F}_q$, which is a field containing $\mathbb{F}_q$ and an element x transcendental over $\mathbb{F}_q$ such that $K/\mathbb{F}_q(x)$ is a finite extension. We will also denote $k = \mathbb{F}_q(X)$. A prime in K is by definition a discrete valuation ring R with maximal ideal P such that $\mathbb{F}_q \subseteq R$, and the quotient field of R is K. We refer to such a prime by P, where P is the maximal ideal in R, and by ord_P the discrete valuation associated to P. Also, $\deg P$ is the dimension of R/P over $\mathbb{F}_q$ (which can be shown to be finite). We denote by $\mathcal{S}_K$ the set of primes of K. We refer the reader to [Ros02, Chapter 5] for all the details.

Example: Let $k = \mathbb{F}_q(X)$, and denote $A = \mathbb{F}_q[X]$. Then, each irreducible monic polynomial P give a valuation ring, namely A_P, the localization of $A = \mathbb{F}_q[X]$ at P. A_P is a discrete valuation ring, and we also use P to denote the maximal ideal in A_P. This gives raise to a prime of $\mathbb{F}_q(X)$ as define above, of degree $\deg P$. There is only one more prime of the function field $\mathbb{F}_q(X)$, associated with the ring $A' = \mathbb{F}_q[X^{-1}]$ with prime ideal P' generated by X^{-1}. The localization of A' at P' is a discrete valuation ring which defines a prime of $\mathbb{F}_q(X)$ called the prime at infinity, denoted ∞. We can check that $\deg \infty = 1$.

Let K be a function field, and let $\mathcal{D}_K$ be the group of divisors of K, which is the free abelian group generated by the primes. We denote this group additively, so a typical divisor is a finite sum

$$D = \sum_P a(P)P,$$

where P are primes of K. The degree of such a divisor is $\deg D = \sum_P a(P)\deg(P)$, and the norm of D is $|D| = q^{\deg D}$. A divisor D is said to be effective if $a(P) \geq 0$ for all P. We denote this by $D \geq 0$.

Definition 3.3. *Let K be a function field over $\mathbb{F}_q(X)$. The zeta function of K, $\zeta_K(s)$, is defined by*

$$\zeta_K(s) = \sum_{\substack{D \in \mathcal{D}_K \\ D \geq 0}} |D|^{-s} = \prod_{P \in \mathcal{S}_K} \left(1 - |P|^{-s}\right)^{-1},$$

where the sum runs over all divisors $D \in \mathcal{D}_K$, and the product over all primes $P \in \mathcal{S}_K$.

Example 1: If $K = \mathbb{F}_q(X)$, show that

$$\zeta_K(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}.$$

This is the completed zeta function of $\zeta_q(s)$, which did not include the prime at ∞.

Example 2: Let $K = \mathbb{F}_q(X)(\sqrt{D(X)})$ where D is a square-free polynomial of degree d. As in the number field setting, let χ_K is the character associated with the quadratic field $\mathbb{F}_q[X](\sqrt{D})$, i.e. for each prime P of $\mathbb{F}_q(X)$,

$$\chi_K(P) = \begin{cases} 1 & P \text{ splits in } K \\ -1 & P \text{ is inert in } K \\ 0 & P \text{ ramifies in } K. \end{cases}$$

such that

$$\begin{aligned} \frac{\zeta_K(s)}{\zeta_k(s)} &= \prod_{\substack{P \in \mathcal{S}_k \\ P \text{ is inert}}} \frac{\left(1-|P|^{-2s}\right)^{-1}}{\left(1-|P|^{-s}\right)^{-1}} \prod_{\substack{P \in \mathcal{S}_k \\ P \text{ splits}}} \frac{\left(1-|P|^{-s}\right)^{-2}}{\left(1-|P|^{-s}\right)^{-1}} \prod_{\substack{P \in \mathcal{S}_k \\ P \text{ ramifies}}} \frac{\left(1-|P|^{-s}\right)^{-1}}{\left(1-|P|^{-s}\right)^{-1}} \\ &= \prod_{\substack{P \in \mathcal{S}_k \\ P \text{ is inert}}} \left(1+|P|^{-s}\right)^{-1} \prod_{\substack{P \in \mathcal{S}_k \\ P \text{ splits}}} \left(1-|P|^{-s}\right)^{-1} \prod_{\substack{P \in \mathcal{S}_k \\ P \text{ ramifies}}} 1 \\ &= \prod_{P \in \mathcal{S}_k} \left(1-\chi_K(P)|P|^{-s}\right)^{-1} \end{aligned}$$

For the finite primes $P \in \mathcal{S}_k$, i.e. the irreducible polynomials of $\mathbb{F}_q[X]$, the character χ_K is the quadratic Dirichlet character to the modulus D, i.e. the quadratic residue symbol

$$\chi_D(F) = \left(\frac{D}{F}\right).$$

For a general reference on Dirichlet characters over function fields, and in particular quadratic residue symbols, see [Ros02, Chapter 4]. Let χ be any Dirichlet character. Then, the L-function of χ is defined by

$$L(s,\chi) = \sum_{\substack{F \in \mathbb{F}_q[X] \\ F \text{ monic}}} \frac{\chi(F)}{|F|^s}.$$

It converges absolutely for $\mathrm{Re}(s) > 1$, and we have the product decomposition

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

where the product is over monic irreducible polynomials of $\mathbb{F}_q[X]$.

For the prime at infinity in $\mathcal{S}_k$, we have that

$$\begin{cases} \infty \text{ ramifies in } K & \deg D \text{ odd} \\ \infty \text{ splits in } K & \deg D \text{ even, } \operatorname{sgn} \mathrm{D} = 1 \\ \infty \text{ is inert in } K & \deg D \text{ even, } \operatorname{sgn} \mathrm{D} = \text{-1} \end{cases} \tag{16}$$

where for $D = \sum_{n=0}^{\deg D} a_n X^n \in \mathbb{F}_q[X]$, we define $\operatorname{sgn} D$ to be 1 if $a_{\deg D}$ is a square in $\mathbb{F}_q^*$ and -1 otherwise.

Putting everything together, we have that for D monic and square-free, and $K = k(\sqrt{D})$, that

$$\frac{\zeta_K(s)}{\zeta_k(s)} = (1 - q^{-s})^{-\lambda_D} L(s, \chi_D)$$

where $L(s, \chi_D)$ is the Dirichlet L-function associated with the quadratic residue symbol $\chi_D(F) = \left(\frac{D}{F}\right)$, and

$$\lambda_D = \begin{cases} 1 & \deg D \text{ even} \\ 0 & \deg D \text{ odd.} \end{cases}$$

Proposition 3.4. [Ros02, Proposition 4.3] *Let χ be a non-trivial Dirichlet character to the modulus M. Then, $L(s, \chi)$ is a polynomial in q^{-s} of degree at most* $\deg M - 1$.

Proof. Define

$$A(n, \chi) = \sum_{\substack{\deg F = n \\ F \text{ monic}}} \chi(F).$$

Then,

$$L(s, \chi) = \sum_{n=0}^{\infty} A(n, \chi) q^{-ns},$$

and it follows from the orthogonality relation of characters that $A(n, \chi) = 0$ for $n \geq \deg M$. □

So, it follows from Proposition 3.4 that for $K = \mathbb{F}_q(X)(\sqrt{D})$, $\zeta_K(s)/\zeta_k(s)$ is a polynomial in q^{-s}. We will see that this is true in general.

Example 3: Let ℓ be a prime, and we assume that $q \equiv 1 \mod \ell$. Let $D(X) \in \mathbb{F}_q[X]$ be a monic ℓth-power free polynomial, and let

$$\chi_{D,\ell}(F) = \left(\frac{D}{F}\right)_{\ell}$$

be the ℓth-power residue symbol. It is a character of order ℓ to the modulus D. See [Mor91] for more details on ℓth-power residue symbols. Then, for $K = k(\sqrt[\ell]{D})$, we have

$$\frac{\zeta_K(s)}{\zeta_k(s)} = \left(1 - q^{-s}\right)^{-\lambda_D} \prod_{j=1}^{\ell-1} L(s, \chi_{D,\ell}^j),$$

where the $L(s, \chi_{D,\ell}^j)$ are the Dirichlet L-functions with character $\chi_{D,\ell}^j$ for $j = 1, \ldots, \ell - 1$, and

$$\lambda_D = \begin{cases} \ell - 1 & \deg D \equiv 0 \mod \ell \\ 0 & \deg D \not\equiv 0 \mod \ell \end{cases}$$

(we recall that $D(X)$ is monic). Then, $\frac{\zeta_K(s)}{\zeta_k(s)}$ is also a polynomial in that case by Proposition 3.4. The general case is proven in Rosen, by using the Riemann-Roch theorem [Ros02, Theorem 5.4] to get a closed formula for the number of effective divisors of degree n, for $n > 2g - 2$, where g is the genus of the function field K. The Riemann-Roch theorem also defines the genus, which is a key invariant of the function field K.

Theorem 3.5. [Ros02, Theorem 5.9] *Let K be a function field over $\mathbb{F}_q$ of genus g. Then*

$$\zeta_K(s) = \frac{P_K(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

where $P_K(u)$ is a polynomial of degree $2g$ in $\mathbb{Z}[u]$.

Proof. Let $b_n = b_n(K)$ be the number of effective divisors of degree n in $\mathcal{D}_K$. Assume that for $n > 2g-2$, we have

$$b_n = h_K \, \frac{q^{n-g+1}-1}{q-1}$$

(see [Ros02, Chapter 5] for a proof of that). Using the change of variable $u = q^{-s}$ and defining $Z_K(u) = \zeta_K(s)$, we have

$$Z_K(u) \;=\; \sum_{n=0}^{2g} b_n u^n + \frac{h_K}{q-1}\left(\frac{q^g}{1-qu} - \frac{1}{1-u}\right) u^{2g-1},$$

and we deduce that

$$Z_K(u) = \frac{P_K(u)}{(1-u)(1-qu)},$$

with $P_K(u) \in \mathbb{Z}[u]$. □

Then, the Riemann hypothesis for $\zeta_K(s) = Z_K(q^{-s})$ translates into the statement that the inverse roots of $P_K(q^{-s})$ have absolute value $\sqrt{q}$ writing

$$P_K(u) = \prod_{j=1}^{\deg P_K} (1 - u\pi_j(K)).$$

Indeed,

$$\zeta_K(s) = 0 \iff P_K(q^{-s}) = 0 \iff q^{-s} = \pi_j(K)^{-1}, \quad \text{for some } j = 1, \ldots, \deg P_K.$$

Then, if $\mathrm{Re}(s) = 1/2$, we have

$$\pi_j(K)^{-1} = q^{-1/2} q^{-i\mathrm{Im}(s)} \iff |\pi_j(K)| = q^{1/2}, \;\; j = 1, \ldots, \deg P_K.$$

The Riemann hypothesis for function fields was first proven by Weil. There are now several proofs of this deep and beautiful theorem, two of them due to Weil in the 1940s and 1950s. A more elementary proof due to Stepanov and Bombieri was developed in the 1970s. An overview of Bombieri's proof and complete references are given in [Ros02].

Theorem 3.6. *(The Riemann Hypothesis for Function Fields) Let K be a function field over $\mathbb{F}_q$. Then, all the roots of $\zeta_K(s)$ lie on the line $Re(s) = 1/2$. Equivalently, the inverse roots of $P_K(u)$ have absolute value $\sqrt{q}$.*

Using the Riemann Hypothesis, we can prove the Prime number theorem for general function fields.

Theorem 3.7. *(Prime number theorem for function fields) Let*

$$a_N(K) := \#\left\{P \in \mathcal{S}_K \mid \deg P = N\right\}.$$

Then,

$$a_N(K) = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Proof. See [Ros02, Theorem 5.12]. □

We now wish to derive another expression for the zeta function of a function field K. As above, it is convenient to work with the variable $u = q^{-s}$ and we define $Z_K(u)$ by

$$\zeta_K(s) = Z_K(u).$$

Then, using the Euler product, we have

$$Z_K(u) = \prod_{d=1}^{\infty} (1-u^d)^{-a_d(K)},$$

where $a_d(K)$ is the number of primes in $\mathcal{S}_K$ of degree d, and taking the logarithm on both sides, and using the power series $-\log(1-u) = \sum_{m=1}^{\infty} \frac{u^m}{m}$, we get

$$\log Z_K(u) = \sum_{m=1}^{\infty} \frac{N_m(K)}{m} u^m \iff Z_K(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m(K)}{m} u^m\right), \tag{17}$$

where

$$N_m(K) = \sum_{d|m} d\, a_d(K).$$

Also, it follows from Theorem 3.5 that

$$N_m(K) = q^m + 1 - \sum_{j=1}^{2g} \pi_j(K)^m,$$

by taking logarithms on both sides of

$$Z_K(u) = \frac{P_K(u)}{(1-u)(1-qu)},$$

and writing $P_K(u) = \prod_{j=1}^{2g} (1 - \pi_j(K)u)$.

By studying constant field extensions of $\mathbb{F}_q[X]$, it is shown in Rosen that

Theorem 3.8. [Ros02, Proposition 8.18] *$N_m(K)$ is the number of prime divisors of degree 1 in the function field $K_m = \mathbb{F}_{q^m} K$.*

We now want to change the point of view, and see $Z_K(u)$ as the zeta function of a curve over $\mathbb{F}_q$. We first recall that there is an equivalence of categories between smooth projective curves over $\mathbb{F}_q$ and function fields over $\mathbb{F}_q$ (see for example [Sil09, Chapter 2] for details). Let $C/\mathbb{F}_q$ be a smooth projective curve over $\mathbb{F}_q$, and to simplify the exposition , suppose that C has an affine plane model $F(X,Y) = 0$, where $F(X,Y) \in \mathbb{F}_q[X,Y]$ is an irreducible polynomial. We define the coordinate ring of C as $\mathbb{F}_q[X,Y]/(F(X,Y))$ and the function field of C, denoted $K(C)$, as the ring of fractions of $K[X,Y]/(F(X,Y))$. This creates an equivalence of categories between the set of smooth plane curves over $\mathbb{F}_q$, and functions fields over $\mathbb{F}_q$. The corresponding maps are surjective morphisms of curves defined over $\mathbb{F}_q$, and function field injections preserving $\mathbb{F}_q$. For example, $k = \mathbb{F}_q(X)$ is the function field $\mathbb{P}^1(\mathbb{F}_q)$, $K = \mathbb{F}_q(X)(\sqrt{D(X)})$ is the function field of the hyperelliptic curve with plane model $C : Y^2 = D(X)$, and $K = \mathbb{F}_q(X)(\sqrt[\ell]{D(X)})$ is the function field of the cyclic ℓ-cover with plane model $C : Y^\ell = D(X)$.

Then, fix a curve C over $\mathbb{F}_q$, and let K be its function field (which is a function field over $\mathbb{F}_q$). It is not difficult to see that primes in $\mathcal{S}_K$ must correspond to Galois orbits of points on C. For example, for the function field $k = \mathbb{F}_q(X)$, the finite primes are in one-to-one correspondence with irreducible polynomials in $\mathbb{F}_q[X]$ which are in one-to-one correspondence with $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbits of points in $\mathbb{A}^1(\overline{\mathbb{F}}_q)$ (the Galois orbit associated to a given irreducible polynomial in $P(X) \in \mathbb{F}_q[X]$ is of course the set of roots of $P(X)$.) The degree of the polynomial is then the number of elements in the orbit. With this example in mind, it is natural to think that the set of primes of degree 1 in the function field $K_m = \mathbb{F}_{q^m} K$ must correspond to the points of C defined over $\mathbb{F}_{q^m}$. This gives the following beautiful theorem.

Theorem 3.9. *Let C be a smooth and projective curve of genus g over $\mathbb{F}_q$, and define*

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

Let K be the function field of C. Then,

$$Z_K(u) = Z_C(u).$$

Proof. This follows from the discussion above and (17). □

We can then restate the result of this section in terms of zeta functions of curves over finite fields, which is the way they were stated (and proven) by Weil. For the generalisation to zeta functions of general varieties over finite fields, the Riemann Hypothesis was proven by Deligne.

Theorem 3.10. *(Weil's Theorem) Let C be a smooth and projective curve of genus g over $\mathbb{F}_q$. Let*

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

Then, the zeta function $Z_C(u)$ has the following properties

Rationality:

$$Z_C(u) \quad = \quad \frac{P_C(u)}{(1-u)(1-qu)}$$

where $P_C(u)$ is a polynomial of degree $2g$ in $\mathbb{Z}[u]$.

Functional Equation:

$$Z_C(1/qu) = \pm q^{1-g}T^{2-2g}Z_C(u).$$

Riemann Hypothesis:

$$P_C(u) = \prod_{j=1}^{2g}(1-u\alpha_j(C)), \quad |\alpha_j(C)| = \sqrt{q},$$

i.e. the roots of $P_C(u)$ which are $\alpha_j(C)^{-1}$, $i = 1, \ldots, 2g$, have absolute value $1/\sqrt{q}$.

We conclude this section with the statement of the analogue of the Wiener-Ikehara Tauberian Theorem for the case of function fields, which can be used to estimate arithmetic functions of a function field K over $k = \mathbb{F}_q(T)$. This includes classical arithmetic functions as square-free effective divisors, sum of divisors [Ros02, Chapter 17], and counting functions and estimates for the number of points for components of moduli spaces of curves over finite fields as cyclic ℓ-covers [BDFL10b], ordinary Artin-Schreier curves [BDFL], or cyclic extensions of $k = \mathbb{F}_q[X]$ with prescribed ramification (see Section 4.5).

Theorem 3.11. *Let K be a function field over $k = \mathbb{F}_q(X)$, and let $f : \mathcal{D}_K^+ \to \mathbb{C}$ be a function from the effective divisors of K to the complex numbers. Let*

$$\zeta_f(s) = \sum_{D \in \mathcal{D}_K^+} \frac{f(D)}{|D|^s}$$

be the Dirichlet series associated to f, and suppose that $\zeta_f(s)$ converges absolutely for $Re(s) > 1$ and is holomorphic on

$$\left\{ s \in \mathbb{C} \mid -\frac{\pi i}{\log q} \leq Im(s) < \frac{\pi i}{\log q}, \;\; Re(s) = 1 \right\},$$

except for a simple pole at $s = 1$ with residue α. Then, there is a $\delta < 1$ such that

$$\sum_{\deg D = N} f(D) = \alpha \log(q)\, q^N + O\left(q^{\delta N}\right).$$

If $\zeta_f(s) - \alpha/(s-1)$ is holomorphic in $Re(s) \geq \delta'$, then the error term can be replaced by $O\left(q^{\delta' N}\right)$.

4. Number of points in families of curves as a sum of random variables

4.1. **Introduction.** As a first statistics, we study the fluctuations in the number of points in a family of curves over $\mathbb{F}_q$ of genus g. For any curve of genus g, it follows from Theorem 3.10 that the number of points is given by

$$\#C(\mathbb{F}_q) - (q+1) = \sum_{j=1}^{2g} \alpha_j(C) = q^{1/2} \operatorname{tr} \Theta_C,$$

where C is the $2g \times 2g$ matrix with eigenvalues $q^{-1/2}\alpha_j(C) = e^{i\theta_j(C)}$, $j = 1, \dots, 2g$.

When the genus is fixed and q tends to infinity, $q^{-1/2}\left(\#C(\mathbb{F}_q) - (q+1)\right) = \operatorname{tr} \Theta_C$ is distributed as the trace of matrices in a symmetry group $M(2g)$ determined by the monodromy group of the family, for natural families $\mathcal{F}(g,q)$ of curves of genus g over $\mathbb{F}_q$ where Deligne's equidistribution theorem and its generalisations hold. For example, $\mathcal{F}(g,q)$ could be a moduli space, or an irreducible component in a moduli space, or a stratum in a natural stratification of a moduli space (as the p-rank stratification, where p is the characteristic of q).

In general, let $M(2g) \subseteq U(2g)$, which is a probability space under the Haar probability measure. For any continuous function F on the set of conjugacy classes of $M(2g)$, let

$$\langle F(U) \rangle_{M(2g)} = \int_{M(2g)} F(U)\, d\mathrm{Haar}(U).$$

Let $\mathcal{F} = \mathcal{F}(g,q)$ be a natural family of curves of genus g over $\mathbb{F}_q$ with symmetry type $M(2g)$. Then, for any function F evaluated on the zeroes (the eigenangles) of C, we expect to have as $q \to \infty$

$$\lim_{q\to\infty} \langle F(\Theta_C) \rangle_{\mathcal{F}(g,q)} \quad = \quad \lim_{q\to\infty} \frac{\sum_{C\in\mathcal{F}(g,q)} F(\Theta_C)}{\#\mathcal{F}(g,q)} = \langle F(U) \rangle_{M(2g)} = \int_{M(2g)} F(U)\, d\mathrm{Haar}(U).$$

We study in this section the other type of distribution over a family $\mathcal{F}(g,q)$, when q is fixed and g tends to infinity. We will find that we can describe the distribution of $\#C(\mathbb{F}_q)$ (or $\#C(\mathbb{F}_q) - (q+1)$, or $\operatorname{tr} \Theta_C = q^{-1/2}\left(\#C(\mathbb{F}_q) - (q+1)\right)$) by a natural probabilistic model, in terms of a sum of $q+1$ independent identically distributed random variables. The random variables are different for each family, as computing the average number of points for each family leads to a different sieving depending on the geometry of each family. We will consider in this section the following families of curves over $\mathbb{F}_q$:

- Hyperelliptic curves, which amount to sieve to count square-free polynomials of degree d (taking prescribed value);
- Cyclic trigonal curves, which amount to sieve to count cube-free polynomials $F = F_1 F_2^2$ where $\deg F_1 = d_1$, $\deg F_2 = d_2$.
- Cyclic covers of order ℓ: which amount to sieve to count ℓ-power free polynomials $F = F_1 F_2^2 \dots F_{\ell-1}^{\ell-1}$ where $\deg F_1 = d_1, \dots, \deg F_{\ell-1} = d_{\ell-1}$.
- Trigonal curves, which amount to count cubic extensions of $\mathbb{F}_q(X)$ with prescribed ramification at given primes of $\mathcal{S}_k$.
- Smooth plane curves, which amount to sieve homogeneous polynomials of degree d to count those whose the first order partial derivatives do not vanish simultaneously.

Finally, when both g and q tends to infinity, it can be shown that in all those families, $\operatorname{tr} \Theta_C$ has a Gaussian value distribution with mean zero and variance unity when C varies over the curves in each family mentioned above. This can be thought as the limiting process of both distributions (for q fixed or for g fixed), which is a standard Gaussian in both cases.

4.2. **The distribution of the number of points.** We state in this section results expressing the distribution of $\#C(\mathbb{F}_q)$ as a sum of random variables, when $C \in \mathcal{F}(g,q)$ for several families $\mathcal{F}(g,q)$ and $g \to \infty$.

4.2.1. Let $\mathcal{H}_g$ be the moduli space of hyperelliptic curves of genus g. Then

$$\lim_{g\to\infty} \frac{\#\{C \in \mathcal{H}_g : \#C(F_q) = m\}}{\#\mathcal{H}_g} = \text{Prob}\left(\sum_{i=1}^{q+1} X_i = m\right),$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{q}{2(q+1)} \\ 1 & \text{with probability } \frac{1}{q+1} \\ 2 & \text{with probability } \frac{q}{2(q+1)} \end{cases}$$

Notice that the mean value of each random variables is 1, and then the mean value of the sum is $q+1$. The statistics for the number of *affine* points on hyperelliptic curves are computed in[KR09], and the geometric version of their theorem (counting also the points at infinity, and running over all curves in the moduli space with the appropriate weights) are deduced from their result in [BDFL10b].

4.2.2. The generalisation of the results of Kurlberg and Rudnick to general ℓ-covers with a model $Y^\ell = F(X)$ were considered in [BDFL10b, BDFL11]. In that case, the moduli space of cyclic covers of genus g breaks in irreducible components $\mathcal{H}^{(d_1,d_2)}$ according to the number of simple roots and double roots of the cube-free polynomial $F(X)$ (then, the genus is not determined by the degree of $F(X)$ in this case). More details on the moduli space of general ℓ-covers are given in Section 4.4. The statistics for each component $\mathcal{H}^{(d_1,d_2)}$ of the moduli space were considered in [BDFL10b, BDFL11], and

$$\lim_{d_1,d_2\to\infty} \frac{\#\{C \in \mathcal{H}^{(d_1,d_2)} : \#C(F_q) = m\}}{\#\mathcal{H}^{(d_1,d_2)}} = \text{Prob}\left(\sum_{i=1}^{q+1} X_i = m\right),$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{2q}{3(q+2)} \\ 1 & \text{with probability } \frac{2}{q+2} \\ 3 & \text{with probability } \frac{q}{3(q+2)} \end{cases}$$

Notice that the mean value of each random variables is 1, and then the mean value of the sum is $q+1$. In a similar way, for each irreducible component $\mathcal{H}^{(d_1,\dots,d_{\ell-1})}$ of the moduli space of cyclic ℓ-covers $Y^\ell = F(X)$, it is shown in [BDFL10b, BDFL11] that

$$\lim_{d_1,\dots,d_{\ell-1}\to\infty} \frac{\#\{C \in \mathcal{H}^{(d_1,\dots,d_{\ell-1})} : \#C(F_q) = m\}}{\#\mathcal{H}^{(d_1,\dots,d_{\ell-1})}} = \text{Prob}\left(\sum_{i=1}^{q+1} X_i = m\right),$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{(\ell-1)q}{\ell(q+\ell-1)} \\ 1 & \text{with probability } \frac{\ell-1}{q+\ell-1} \\ \ell & \text{with probability } \frac{q}{\ell(q+\ell-1)} \end{cases}$$

Notice that the mean value of each random variables is 1, and then the mean value of the sum is $q+1$.

For the case of cyclic trigonal curves, and general ℓ-covers, different limiting distributions can be obtained when taking different invariants going to infinity, as in [Xio10a, CWZ] (where ℓ can be taken as any integer co-prime to q in [CWZ], and not necessarily a prime). Let $\mathcal{F}_d$ denote the set of ℓ-th power free degree d polynomials in $\mathbb{F}_q[X]$. For each such polynomial f, let C_f be the curve with affine model $C_f : Y^\ell = f(X)$, and let $\#C_f(\mathbb{F}_q)_{\text{aff}}$ be the number of affine points on C_f. Then, for example for $\ell = 3$, both authors show (with different techniques) that

$$\lim_{d\to\infty} \frac{\#\{f \in \mathcal{F}_d : \#C_f(\mathbb{F}_q)_{\text{aff}} = m\}}{\#\mathcal{F}_d} = \text{Prob}\left(\sum_{i=1}^{q} X_i = m\right),$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{2}{3(q^{-2}+q^{-1}+1)} \\ 1 & \text{with probability } \frac{q^{-2}+q^{-1}}{q^{-2}+q^{-1}+1} \\ 3 & \text{with probability } \frac{1}{3(q^{-2}+q^{-1}+1)} \end{cases}$$

There are q random variables in that case, and not $q+1$, because we consider the distribution for the number of affine points (not including the points at ∞). Notice that the mean value of each random variables is 1, and then the mean value of the sum is q.

We will revisit ℓ-covers from a third point of view in Section 4.5, and present another way to get statistics for the distribution of points in this family.

4.2.3. The case of general trigonal curves, i.e. smooth curves of genus g with a map to $\mathbb{P}^1$ of degree 3, was considered by [Woo12]. Let $\mathcal{T}_g$ be the set of those curves. We remark that the cyclic trigonal curves do not influence those statistics, as the number of such cyclic trigonal curves of genus g is bounded $\underline{o}(\#\mathcal{T}_g)$. It is proven in [Woo12] that

$$\lim_{g\to\infty} \frac{\#\{C \in \mathcal{T}_g : \#C(F_q) = m\}}{\#\mathcal{T}_g} = \text{Prob}\left(\sum_{i=1}^{q+1} X_i = m\right),$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{2q^2}{6q^2+6q+6)} \\ 1 & \text{with probability } \frac{3q^2+6}{6q^2+6q+6} \\ 2 & \text{with probability } \frac{6q}{6q^2+6q+6} \\ 3 & \text{with probability } \frac{q^2}{6q^2+6q+6} \end{cases}$$

Notice that the mean value of each random variables is $1 + \frac{6q}{6q^2+6q+6}$, and then the mean value of the sum is $q + 2 - \frac{1}{q^2+q+1}$.

4.2.4. The fluctuations in the number of points on smooth projective plane curves over a finite field $\mathbb{F}_q$ were considered in [BDFL10a]. Let S_d be the set of homogeneous polynomials $F(X,Y,Z)$ of degree d over $\mathbb{F}_q$, and let $S_d^{\text{ns}} \subseteq S_d$ be the subset of polynomials corresponding to smooth (or nonsingular) curves $C_F : F(X,Y,Z) = 0$. The genus of C_F is $(d-1)(d-2)/2$. Then,

$$\lim_{d\to\infty} \frac{\#\left\{F \in S_d^{\text{ns}} : \#C_F(\mathbb{F}_q) = m\right\}}{\#S_d^{\text{ns}}} = \text{Prob}\left(X_1 + \cdots + X_{q^2+q+1} = m\right),$$

where $X_1, \ldots, X_{q^2+q+1}$ are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{q^2}{q^2+q+1} \\ 1 & \text{with probability } \frac{q+1}{q^2+q+1} \end{cases}$$

Notice that the mean value of each random variables is $\frac{q+1}{q^2+q+1}$, and then the mean value of the sum is $q+1$.

The main tool to count the number of points on smooth plane curves is a sieving process due to Poonen [Poo04] which allows to count the number of polynomials in S_d which give rise to smooth curves C_F, and the number of smooth curves C_F which pass through a fixed set of points of $\mathbb{P}^2(\mathbb{F}_q)$. For more details, we refer the reader to [Poo04, BDFL10a].

The distribution of points in other families of smooth curves was studied in [EW12, BK12].

In the rest of this section, we explain how to prove such results, stressing how the geometry and sieving give raise to the independent random variables in each the different cases.

4.3. **Hyperelliptic curves.** We first concentrate on the case of hyperelliptic curves. Let $\widehat{\mathcal{F}}_d$ be the set of square-free polynomails of degree d (not necessarily monic), and consider the hyperelliptic curve with affine model

$$C_F : Y^2 = F(X), \quad F(X) \in \hat{\mathcal{F}}_d.$$

Such models give a curve of genus d if and only if $d = 2g+1$ or $d = 2g+2$. Also, we remark that by running over all $F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$, one counts every point in the moduli space $\mathcal{H}_g$ exactly $q(q^2-1)$ times (as usual, points in the moduli space are counted with weight $1/|\mathrm{Aut}(C)|$.)

For any $x \in \mathbb{F}_q$, let

$$\chi_2(x) = \begin{cases} 1 & x \in \mathbb{F}_q^2, x \neq 0 \\ -1 & x \notin \mathbb{F}_q^2 \\ 0 & x = 0. \end{cases}$$

Then,

$$\#C_F(\mathbb{F}_q) \quad = \quad \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} 1 + \chi_2(F(x)) = q + 1 + \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_2(F(x)),$$

where the value of F at infinity is given by the value of $X^{2g+1}F(1/X)$ at zero according to (16). We then have to consider the average of

$$\widehat{S}_2(F) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_2(F(x))$$

as F varies over the polynomials in $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$.

Fix $x_1, \dots, x_{q+1}$ an enumeration of the points on $\mathbb{P}^1(\mathbb{F}_q)$ such that x_{q+1} denotes the point at infinity. Then

$$\chi_2(F(x_{q+1})) = \begin{cases} 0 & \text{if } F \in \widehat{\mathcal{F}}_{2g+1}, \\ 1 & \text{if } F \in \widehat{\mathcal{F}}_{2g+2}, \text{ and the leading coefficient is a square in } \mathbb{F}_q, \\ -1 & \text{if } F \in \widehat{\mathcal{F}}_{2g+2}, \text{ and the leading coefficient is not a square in } \mathbb{F}_q. \end{cases}$$

Pick $(\varepsilon_1, \dots, \varepsilon_{q+1}) \in \{0, \pm 1\}^{q+1}$. Denote m the number of zeros in this $(q+1)$-tuple. We evaluate the probability that the character χ_2 takes exactly these values as F ranges over $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$.

Proposition 4.1. *Let $(\varepsilon_1, \dots, \varepsilon_{q+1}) \in \{0, \pm 1\}^{q+1}$, and let m denote the number of zeros in this $(q+1)$-tuple. Then, as $g \to \infty$,*

$$\frac{|\{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_2(F(x_i)) = \varepsilon_i, 1 \leq i \leq q+1\}|}{|\widehat{\mathcal{F}}_{2g+1}| + |\widehat{\mathcal{F}}_{2g+2}|} \sim \frac{2^{m-q-1}q^{-m}}{(1+q^{-1})^{q+1}}.$$

This follows from the results of Kurlberg and Rudnick [KR09] who considered the variation of the number of *affine* points on hyperelliptic curves. Then distribution in this case is given by a sum of q random variables, and Proposition 4.1 is a geometric restatement of the results of [KR09] when we show that the point at ∞ gives raise to an additional independent random variable with the same distribution. Then, the probability of hitting a certain $(q+1)$-tuple does not depend on the entry at the point we designated as the point at infinity, and that point behaves the same as the affine points, which is exactly what one would expect from a geometric standpoint.

Proposition 4.2. [KR09, Proposition 6] *Let $\mathcal{F}_d$ be the number of monic square-free polynomials of degree d. Let $x_1, \dots, x_{\ell+m} \in \mathbb{F}_q$ be distinct elements, let $a_1, \dots, a_\ell \in \mathbb{F}_q^*$, and let $a_{\ell+1} = \cdots = a_{\ell+m} = 0$. Then*

$$|\{F \in \mathcal{F}_d : F(x_i) = a_i, 1 \leq i \leq m+\ell\}| = \frac{(1-q^{-1})^m q^{d-(m+\ell)}}{\zeta_q(2)(1-q^{-2})^{m+\ell}} \left(1 + O\left(q^{(3m+2\ell-d)/2}\right)\right).$$

and

$$\frac{|\{F \in \mathcal{F}_d : F(x_i) = a_i, 1 \leq i \leq m+\ell\}|}{|\mathcal{F}_d|} = \frac{(1-q^{-1})^m q^{-(m+\ell)}}{(1-q^{-2})^{m+\ell}} \left(1 + O\left(q^{(3m+2\ell-d)/2}\right)\right).$$

Proof. For $d > \ell + m$, the number of polynomials of degree d taking prescribed values at $\ell + m$ points is exactly $q^{d-\ell-m}$. We then have to sieve to get the count for the number of *square-free* polynomials of degree d. □

We now evaluate the probability that the character χ_2 takes the values prescribed by $(\varepsilon_1, \dots, \varepsilon_{q+1})$ as F ranges over $\widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2}$, i.e. we show that Proposition 4.2 imply Proposition 4.1. We first suppose that $\varepsilon_{q+1} = 0$. The numbers of zeros among $\varepsilon_1, \dots, \varepsilon_q$ is now $m-1$. Since there are no polynomials in $\widehat{\mathcal{F}}_{2g+2}$ with $\chi_2(F(x_{q+1})) = 0$, only $\widehat{\mathcal{F}}_{2g+1}$ contributes. There are $q-1$ possibilities for the leading coefficient of such a polynomial and thus

$$\begin{aligned}&|\{F \in \widehat{\mathcal{F}}_{2g+1} \cup \widehat{\mathcal{F}}_{2g+2} : \chi_2(F(x_i)) = \varepsilon_i, 1 \le i \le q+1\}| \\ &= \sum_{\alpha \in \mathbb{F}_q^*} |\{F \in \mathcal{F}_{2g+1} : \chi_2(F(x_i)) = \varepsilon_i \chi_2(\alpha), 1 \le i \le q\}|.\end{aligned}$$

Taking into account that there are $\frac{q-1}{2}$ squares in $\mathbb{F}_q^*$ and the same number of non-squares, and using Proposition 4.2, the above expression is

$$\sim (q-1)\left(\frac{q-1}{2}\right)^{q-m+1} \frac{(1-q^{-1})^m q^{2g+1-q}}{(1-q^{-2})^q} = \frac{2^{m-1-q}(1-q^{-1})^{q+2} q^{2g+3-m}}{(1-q^{-2})^q}. \tag{18}$$

With Lemma 3.2, we compute

$$|\widehat{\mathcal{F}}_{2g+1}| + |\widehat{\mathcal{F}}_{2g+2}| = q^{2g+3}(1-q^{-1})(1-q^{-2}), \tag{19}$$

and dividing (18) by (19) we get Proposition 4.1. The cases where $\varepsilon_{q+1} = \pm 1$ are similar. The result then follows by summing over all $(q+1)$-tuples $(\varepsilon_1, \dots, \varepsilon_{q+1})$ such that $\varepsilon_1 + \dots + \varepsilon_{q+1} = t$ (see section 4.4 for this part of the argument). For all the details, we refer the readers to [BDFL10b, Section 6].

4.4. **Cyclic trigonal curves, and general ℓ-covers.** We first look at the case of cyclic trigonal curves. We assume that $q \equiv 1 (\mathrm{mod}\ 3)$. Let C be a cyclic trigonal curve over $\mathbb{F}_q$, i.e. a cyclic cover of order 3 of $\mathbb{P}^1$ defined over $\mathbb{F}_q$. Then, C has an affine model $Y^3 = F(X)$, where $F(X)$ is a cube-free polynomial in $\mathbb{F}_q[X]$. We write $F(X) = F_1(X)F_2(X)^2$, with F_1 and F_2 relatively prime, square-free, $\deg F_1 = d_1$, $\deg F_2 = d_2$ and $d = \deg F = d_1 + 2d_2$. Then, the curve C_F has genus g if and only if $d_1 + 2d_2 \equiv 0 \pmod 3$ and $g = d_1 + d_2 - 2$, or $d_1 + 2d_2 \equiv 1$ or $2 \pmod 3$ and $g = d_1 + d_2 - 1$. Over $\overline{\mathbb{F}}_q$, one can reparametrize and choose an affine model for any cyclic trigonal curve with $d_1 + 2d_2 \equiv 0 \,(\mathrm{mod}\, 3)$. Furthermore, the moduli space $\mathcal{H}_{g,3}$ of cyclic trigonal curves of fixed genus g splits into irreducible subspaces indexed by pairs of nonnegative integers d_1, d_2 with the property that $d_1 + 2d_2 \equiv 0 \,(\mathrm{mod}\, 3)$, and the moduli space can be written as a disjoint union over its connected components

$$\mathcal{H}_{g,3} = \bigcup_{\substack{d_1+2d_2 \equiv 0 \pmod 3, \\ g = d_1+d_2-2}} \mathcal{H}^{(d_1,d_2)}, \tag{20}$$

where each component $\mathcal{H}^{(d_1,d_2)}$ is irreducible. The components can also be described by their signature (r, s). We refer the reader to [AP07] for the details.

Let $\mathcal{F}_{(d_1,d_2)}$ be the set of polynomials $F = F_1 F_2^2$ such that F_1, F_2 are monic, square-free and co-prime, with $\deg F_1 = d_1, \deg F_2 = d_2$. One can prove that

Theorem 4.3. [BDFL10b, Theorem 3.1]. *Let $\rho \in \mathbb{C}$ be a primitive third root of unity. Let $x_1, \dots, x_q$ be the elements of $\mathbb{F}_q$ and let $\varepsilon_1, \dots, \varepsilon_q \in \{0, 1, \rho, \rho^2\}$. Let m be the number of values of ε_i which are 0. Then*

$$\left|\mathcal{F}_{(d_1,d_2)}\right| = \frac{K q^{d_1+d_2}}{\zeta_q(2)^2},$$

$$\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \ : \ \chi_3(F(x_i)) = \varepsilon_i, \ 1 \le i \le q\right\}\right| = \frac{K q^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{2}{q+2}\right)^m \left(\frac{q}{3(q+2)}\right)^{q-m}$$

and

$$\frac{\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \ : \ \chi_3(F(x_i)) = \varepsilon_i, \ 1 \le i \le q\right\}\right|}{\left|\mathcal{F}_{(d_1,d_2)}\right|} = \left(\frac{2}{q+2}\right)^m \left(\frac{q}{3(q+2)}\right)^{q-m}$$

where K is the constant

$$K = \prod_P \left(1 - \frac{1}{(|P|+1)^2}\right).$$

Then, Theorem 4.3 is the analogue of Proposition 4.2 for the cyclic trigonal curves. It is also obtained by sieving to count the polynomials in $\mathcal{F}_{(d_1,d_2)}$ taking prescribed values. This involves the use of the Tauberian Theorem for function fields [Ros02, Theorem 17.1]. The distribution for the number of *affine points* can then be deduced from Theorem 4.3, and again we can include the point at infinity. We have that

$$\#C_F(\mathbb{F}_q) - (q+1) \quad = \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_3(F(x)) + \overline{\chi_3(F(x))} = \widehat{S}_3(F) + \overline{\widehat{S}_3(F)},$$

where

$$\widehat{S}_3(F) = \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_3(F(x)).$$

Let $\hat{\mathcal{F}}_{(d_1,d_2)}$ to be the set of polynomials $F = \alpha F_1 F_2^2$ where $\alpha \in \mathbb{F}_q^*$, and $F_1F_2^2 \in \mathcal{F}_{(d_1,d_2)}$, and $\widehat{\mathcal{F}}_{[d_1,d_2]} = \hat{\mathcal{F}}_{(d_1,d_2)} \cup \hat{\mathcal{F}}_{(d_1-1,d_2)} \cup \hat{\mathcal{F}}_{(d_1,d_2-1)}$. Then, running over the curves C is the irreducible component $\mathcal{H}^{(d_1,d_2)}$ of the moduli space is that same as running over the models $C_F : Y^3 = F(X)$ where $F(X) \in \widehat{\mathcal{F}}_{[d_1,d_2]}$, and it follows from Theorem 4.3 that

$$\begin{aligned}\frac{|\{F\in\widehat{\mathcal{F}}_{[d_1,d_2]} \ : \ \widehat{S}_3(F)=t\}|}{|\widehat{\mathcal{F}}_{[d_1,d_2]}|} &= \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_{q+1})\\ \varepsilon_1+\cdots+\varepsilon_{q+1}=t}} \frac{|\{F\in\widehat{\mathcal{F}}_{[d_1,d_2]} \ : \ \chi_3(F(x_i))=\varepsilon_i, 1\le i\le q+1\}|}{|\widehat{\mathcal{F}}_{[d_1,d_2]}|}\\ &\sim \sum_{\substack{(\varepsilon_1,\dots,\varepsilon_{q+1})\\ \varepsilon_1+\cdots+\varepsilon_{q+1}=t}} \left(\frac{2}{q+2}\right)^m \left(\frac{q}{3(q+2)}\right)^{q+1-m} = \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = t\right)\end{aligned}$$

where $X_1,\dots,X_{q+1}$ $q+1$ are i.i.d. random variables that take the value 0 with probability $2/(q+2)$ and $1,\rho,\rho^2$ each with probability $q/(3(q+2))$. We then get the result stated in Section 4.2 for the distribution of $\#C(\mathbb{F}_q)-(q+1)$ using the $q+1$ i.i.d. random variables $1+X_i+\overline{X_i}$.

4.5. **Cyclic ℓ-covers revisited.** There is another approach that can be used to study the distribution of the number of points over $\mathbb{F}_q$ on cyclic ℓ-covers $C : Y^\ell = f(X)$: we can count the number of function fields $K = k(C)$ of those curves with prescribed ramification at the primes of degree 1. This idea was previously used by [Woo12] to study the distribution of the number of points on the family of all trigonal curves as explained in the next subsection. In the case of the cyclic trigonal curves, the function fields $k(C)$ are abelian extensions of $k = \mathbb{F}_q(X)$ with cyclic Galois group of order ℓ (we always assume that ℓ divides $q-1$), and the number of such extensions of a given genus can be counted using class field theory transferring the work of Wood [Woo12] from number fields to function fields.

The relation between the point counting on the curves C and the extensions $k(C)$ ramifying at given primes follows easily from the equality of the zeta functions $Z_C(u)$ and $\zeta_{k(C)}(u)$ (Theorem 3.9). For each prime $P \in \mathcal{S}_k$ (including the prime at ∞), let $e(P)$ be the ramification degree, $f(P)$ the inertial degree and $r(P)$ the number of primes above P in the extension $K = k(C)$. Then,

$$Z_C(u) = \exp\left(\sum_{n=0}^{\infty} \#C(\mathbb{F}_{q^n})\frac{u^n}{n}\right) = Z_{k(C)}(u) = \prod_{P\in\mathcal{S}_k}\left(1-u^{\deg P f(P)}\right)^{-r(p)},$$

and taking logarithm on both sides, we get

$$\sum_{n=0}^{\infty} \#C(\mathbb{F}_{q^n})\frac{u^n}{n} = \sum_{P\in\mathcal{S}_k}\sum_{m=1}^{\infty} r(P)\frac{u^{mf(P)\deg P}}{m}.$$

Equating the coefficients of u^n on both sides gives

$$\#C(\mathbb{F}_{q^n}) = \sum_{f(P)\deg P \mid n} r(P) f(P) \deg P. \tag{21}$$

In particular, for $C_\ell : Y^\ell = F(X)$, $K = k(C_\ell)$ and $n = 1$, we have

$$\begin{aligned} \#C_\ell(\mathbb{F}_q) &= \ell \,\#\{P \in \mathcal{S}_k \,:\, \deg P = 1 \text{ and } P \text{ splits in } k(C)\} \\ &\quad +\#\{P \in \mathcal{S}_k \,:\, \deg P = 1 \text{ and } P \text{ ramifies in } k(C)\}. \end{aligned} \tag{22}$$

Let $E_\ell(k,g)$ be the number of cyclic extensions of degree ℓ over $k = \mathbb{F}_q(X)$ with genus g, and for any set of primes of degree one $\mathcal{P} = \{P_1, \dots, P_m\} \subseteq \mathcal{S}_k$, and a choice of $\epsilon_i \in \{0, 1, \ell\}$ for $1 \le i \le m$, let $E_\ell(k, g, \mathcal{P}, \mathcal{E})$ be the number of fields K in $E_\ell(k,g)$ such that P_i ramifies in K if $\epsilon_i = 1$, P_i splits in K if $\epsilon_i = \ell$ and P_i is inert in K if $\epsilon_i = 0$. If one can show that for $g \to \infty$ the densities are

$$\frac{\#E_\ell(k,g,\mathcal{P},\mathcal{E})}{\#E(k,g)} \sim \prod_{i=1}^{m} f_0(q)^{m_0} f_1(q)^{m_1} f_2(q)^{m_2}, \tag{23}$$

where m_0 is the number of $\epsilon_i = 0$ (and similarly for m_1, m_2), then we have by taking the average of (22) over $\mathcal{H}_{g,\ell}$ on both side, and using $\mathcal{P} = \{P_1, \dots, P_{q+1}\}$ to be the set of all primes of degree 1, that

$$\lim_{g\to\infty} \frac{\#\{C \in \mathcal{H}_{g,\ell} \,:\, \#C(\mathbb{F}_q) = m\}}{\#\mathcal{H}_{g,\ell}} = \sum_{\epsilon_1+\cdots+\epsilon_{q+1}=m} \prod_{i=1}^{m} f_0(q)^{m_0} f_1(q)^{m_1} f_3(q)^{m_3},$$

and the number of points on cyclic ℓ-covers $C \in \mathcal{H}_{g,\ell}$ is distributed as a sum of $q+1$ i.i..d. random variables taking the value i with probability $f_i(q)$ for $i = 0, 1, 3$. In some work in progress generalising the work of [Woo12] to functions fields, we computed the densities (23) for $\ell = 3$ and $\mathcal{P}$ any finite set of primes of $\mathcal{S}_k$ with prescribed splitting conditions at each prime. It follows that

$$\lim_{g\to\infty} \frac{\#\{C \in \mathcal{H}_{g,3} \,:\, \#C(\mathbb{F}_q) = m\}}{\#\mathcal{H}_{g,3}} = \sum_{\epsilon_1+\cdots+\epsilon_{q+1}=m} \prod_{i=1}^{m} \left(\frac{2q}{3(q+2)}\right)^{m_0} \left(\frac{2}{q+2}\right)^{m_1} \left(\frac{q}{3(q+2)}\right)^{m_3}.$$

Then, the number of points on the whole moduli space $\mathcal{H}_{g,3}$ is distributed as a sum of $q+1$ i.i.d., which are the same i.i.d. occurring for the number of points on the components $\mathcal{H}^{(d_1,d_2)}$ when $d_1, d_2 \to \infty$. This seems to indicate that the estimates for the components $\mathcal{H}^{(d_1,d_2)}$ could hold under the weaker condition $d_1 + d_2 \to \infty$. Indeed, replacing the main term of the estimates for $\left|\mathcal{H}^{(d_1,d_2)}\right|$ from [BDFL10b], and the estimate for $|\mathcal{H}_{g,3}|$ following by counting all cyclic cubic extensions of genus g in (20), we get that the count agree, and

$$|\mathcal{H}_{g,3}| = \sum_{\substack{d_1+d_2=g+2 \\ d_1+2d_2\equiv 0 \bmod 3}} |\mathcal{H}^{(d_1,d_2)}|.$$

4.6. **Trigonal curves.** The distribution for the number of points on general trigonal curve (i.e. when $k(C)$ is not a Galois extension) was studied by Wood [Woo12] by relating the number of points with the densities of general cubic extensions of $k = \mathbb{F}_q(X)$ with prescribed ramification. The number of such extensions was counted by Datskovsky and Wright [DW86, DW88] who generalized the results of Davenport and Heilbronn [DH69, DH71] on densities of discriminants of cubic extensions with certain splitting conditions to the case where the base field k is any global field of characteristic not 2 or 3, not necessarily the field of rationals. There densities were computed by Datskovsky and Wright using properties of Shintani zeta functions, but the authors did not provide estimates for the error terms. Recently, Zhao [Zha] has shown that the densities of cubic function fields with prescribed splitting conditions can be determined with a novel geometric approach. Zhao obtained a negative secondary term in this setting (as in the number field setting), and also provided bounds for the error terms. The error terms are not needed to relate the distribution of the number of points to a sum of $q+1$ random variables as done in [Woo12], but are necessary to show that the fluctuations of the number of points around the mean give raise to a standard Gaussian as shown recently by [TX14].

Let C be a smooth curve of genus g with $\pi : C \to \mathbb{P}^1$ of degree 3, and let K be the function field of C. Then, K/k is a cubic extension, and by the equivalence of categories explained in Section 3, every geometric cubic extension of k corresponds to such a curve C. By the Hurwitz formula [Ros02, Chapter 7],

$$\deg \mathrm{Disc}(K/k) = 2g + 4.$$

It is known by [DW88, Theorem I.1] that the number of all such cubic extensions of $k = \mathbb{F}_q(X)$ is asymptotic to q^{2g+4}, and that the number of cyclic extensions is $O\left(gq^{g+2}\right)$ [Wri89, Theorem I.3]. Then, the cyclic extensions do not influence the statistics, and it suffices to consider the set

$$E(k,g) := \{K \ : \ K/k \text{ is a non-cyclic cubic extension and } \deg \mathrm{Disc}(K/k) = 2g+4\}.$$

It follows from the explicit formulas of Proposition 5.5 with $n = 1$ that

$$\begin{aligned} \#C(\mathbb{F}_q) - (q+1) = \quad & 2\,\#\{P \in \mathcal{S}_k \ : \ \deg P = 1 \text{ and } P \text{ splits completely in } K\} \\ & - \#\left\{P \in \mathcal{S}_k \ : \ \deg P = 1 \text{ and } P = P_1P_2^2 \text{ in } K\right\} \\ & + \#\{P \in \mathcal{S}_k \ : \ \deg P = 1 \text{ and } P = P_1 \text{ in } K\}. \end{aligned} \tag{24}$$

Then, reversing the order of summation

$$\langle \#C(\mathbb{F}_q) - (q+1)\rangle_{E(k,g)} \quad = \quad \sum_{\deg P = 1} 2\frac{\#E_{111}(k,g,P)}{\#E(k,g)} + \frac{\#E_{11^2}(k,g,P)}{\#E(k,g)} - \frac{\#E_3(k,g,P)}{\#E(k,g)}, \tag{25}$$

where $E_{111}(k,g,P)$ (respectively $E_{11^2}(k,g,P)$ and $E_3(k,g,P)$) is the number of non-cyclic cubic extensions K with $\deg \mathrm{Disc}(K/k) = 2g+4$ and such that P is totally split in K (respectively $P = P_1P_2^2$, and P is inert).

We now state the result of Zhao about the densities of cubic fields with certain splitting conditions.The work of Zhao is still in preparation, and he should had more specific values for the error term in the final preprint.

Theorem 4.4. [Zha] *For any finite set of primes $\mathcal{S}_k$, and any set of splitting conditions at the primes of $\mathcal{S}_k$, define $E(k,g,\mathcal{S})$ to be the subset of $E(k,g)$ consisting of the cubic extensions satisfying those splitting conditions. Then, as $g \to \infty$*

$$\frac{\#E(k,g,\mathcal{S})}{\#E(k,g)} = \prod_{P \in \mathcal{S}} c_P + O\left(q^{-\delta g} \prod_{P \in \mathcal{S}} |P|^A\right),$$

where $\delta, A > 0$ are fixed constants, and where

$$c_P\left(1 + |P|^{-1} + |P|^{-2}\right) = \begin{cases} 1/6 & \text{for } P \text{ totally split in } K \\ 1/2 & \text{for } P \text{ partially split in } K \\ 1/3 & \text{for } P \text{ inert } K \\ |P|^{-1} & \text{for } P \text{ partially ramified in } K \\ |P|^{-2} & \text{for } P \text{ totally ramified in } K. \end{cases}$$

Using the results of Theorem 4.4 in (25), we get that

$$\langle \#C(\mathbb{F}_q) - (q+1)\rangle_{E(k,g)} = \frac{q^2(q+1)}{q^2+q+1}\left(\frac{2}{6} - \frac{1}{3} + \frac{1}{q}\right) = q + 2 - \frac{1}{q^2+q+1}.$$

It also follows from (25) that

$$\lim_{g\to\infty} \frac{\#\{C \in \mathcal{T}_g \ : \ \#C(\mathbb{F}_q) - (q+1) = m\}}{\#\mathcal{T}_g} = \sum_{\substack{(\varepsilon_1,\ldots,\varepsilon_{q+1}) \in \{0,\pm 1,2\}^{q+1} \\ \sum_{j=1}^{q+1} \epsilon_j = m}} \frac{\#E(k,g,\mathcal{S}(\varepsilon_1,\ldots,\epsilon_{q+1}))}{\#E(K,g)}$$

where $\mathcal{S}(\varepsilon_1,\ldots,\varepsilon_{q+1})$ is the set of primes $P_1,\ldots,P_{q+1}$ of degree 1 with the splitting conditions

$$\begin{cases} P_i \text{ totally split in } K & \text{if } \varepsilon_i = 2 \\ P_i \text{ partially ramified in } K & \text{if } \varepsilon_i = 1 \\ P_i \text{ inert } K & \text{if } \varepsilon_i = -1 \\ P_i \text{ partially split, or totally ramified} & \text{if } \varepsilon_i = 0 \end{cases}$$

Let m_{111} (respectively m_{11^2}, m_3) be the number of j such that $\epsilon_j = 2$ (respectively $\epsilon_j = -1$, $\epsilon_j = 1$), and $m = (q+1) - m_{111} - m_{11^2} - m_3$. This gives the result quoted in Section 4.2 for the distribution of $\#C(\mathbb{F}_q)$ (the random variables are $1 + X_i$, $j = 1,\ldots,q+1$, where X_i are the random variables for $\#C(\mathbb{F}_q) - (q+1)$).

5. Explicit formulas for curves over finite fields

We give in this section some instances of the explicit formulas relating sum over the zeroes of L-functions to the coefficients of the L-functions. For the case of curves over finite fields, the L-functions are polynomials with finitely many zeroes, and the explicit formulas are much simpler than in the number field case.

5.1. **Hyperelliptic curves.** Let C_D be the hyperelliptic curves

$$C_D : Y^2 = D(X)$$

where $D(X)$ is a square-free monic polynomial of positive degree d. Then, C_D is a smooth curve of genus $g_D = \lfloor (\deg D - 1)/2 \rfloor$ with zeta function

$$Z_{C_D}(u) = \frac{P_{C_D}(u)}{(1-u)(1-qu)}.$$

As showed in Section 3, we have that

$$P_{C_D}(u) = \prod_{j=1}^{2g_D} (1 - \alpha_j(D)u) = (1-u)^{-\lambda_D} L(u, \chi_D), \tag{26}$$

where

$$\lambda_D = \begin{cases} 1 & \text{if } \deg D \text{ is even} \\ 0 & \text{if } \deg D \text{ is odd.} \end{cases}$$

and $L(s, \chi_D)$ is the Dirichlet L-function associated with the quadratic residue symbol

$$\chi_D(F) = \left(\frac{D}{F}\right).$$

We write $\alpha_j(D) = \sqrt{q}e^{i\theta_j(D)}$, and we denote by Θ_D the $2g_D \times 2g_D$ diagonal matrix with eigenvalues $e^{i\theta_j(D)}, j = 1, \dots, 2g_D$.

Proposition 5.1. [Rud10, Section 2.5] *Let n be an integer. For $F \in \mathbb{F}_q[X]$, we define*

$$\Lambda(F) = \begin{cases} \deg P & \text{if } F = P^k; \\ 0 & \text{otherwise} \end{cases}. \tag{27}$$

Then

$$\operatorname{tr} \Theta_D^n = \sum_{j=1}^{2g_D} e^{in\theta_j(D)} = -q^{-|n|/2} \left(\lambda_D + \sum_{\deg F = |n|} \Lambda(F)\chi_D(F) \right)$$

Proof. Let n be a positive integer. Then, by logarithmic derivative on both sides of (26), we get

$$-u\frac{d}{du} \sum_P \log\left(1 - \chi_D(P)u^{\deg P}\right) = u\frac{d}{du}\left(\lambda_D \log(1-u) + \sum_{j=1}^{2g_D} \log(1 - \alpha_j(D)u) \right)$$

$$\iff \quad \sum_P \frac{\deg P \chi_D(P) u^{\deg P}}{1 - \chi_D(P)u^{\deg P}} = \frac{-u\lambda_D}{1-u} + \sum_{j=1}^{2g_D} \frac{-\alpha_j(D)u}{1 - \alpha_j(D)u}$$

$$\iff \quad \sum_P \deg P \sum_{n=1}^{\infty} \chi_D(P)^n u^{n \deg P} = -\lambda_D \sum_{n=1}^{\infty} u^n - \sum_{j=1}^{2g_D} \alpha_j(D)^n u^n,$$

and equating the coefficients of u^n, we get that

$$-q^{n/2} \operatorname{tr} \Theta_D^n = -\sum_{j=1}^{2g_D} \alpha_j(D)^n = \sum_{\deg P | n} \deg P \; \chi_D(P)^{n/\deg P} + \lambda_D,$$

where we can rewrite

$$\sum_{\deg P | n} \deg P \; \chi_D(P)^{n/\deg P} = \sum_{\deg F = n} \Lambda(F)\chi_D(F).$$

Taking the complex conjugate, we also get the result for negative integers, since χ_D is a real character. □

5.2. **Cyclic ℓ-covers.** Let ℓ be a prime (including $\ell = 2$ unless mentioned) such that $\ell \mid q-1$. Let $Q(x)$ be a ℓth-power free polynomial of degree d. Then,

$$C_Q : Y^\ell = Q(X)$$

is a smooth projective curve of genus g (the formula for the genus of C_Q is given in Section 4). As we showed in Section 3, the zeta function of C_Q writes as

$$Z_{C_Q}(u) = \frac{P_{C_Q}(u)}{(1-u)(1-qu)},$$

where

$$P_{C_Q}(u) = \prod_{j=1}^{2g_Q} \left(1 - q^{1/2} e^{i\theta_j(Q)}\right) = (1-u)^{-\lambda_Q} \prod_{i=1}^{\ell-1} L(s, \chi_Q^j), \tag{28}$$

where χ_Q is the ℓth-power residue symbol

$$\chi_Q(F) = \left(\frac{Q}{F}\right)_\ell,$$

and

$$\lambda_Q = \begin{cases} \ell - 1 & \deg D \equiv 0 \mod \ell \\ 0 & \deg Q \not\equiv 0 \mod \ell \end{cases}$$

Proposition 5.2. [Xio10b] *Let n be an integer. Then*

$$\operatorname{tr} \Theta_Q^n = \sum_{j=1}^{2g_Q} e^{in\theta_j(Q)} = -q^{-|n|/2} \left(\lambda_Q + \sum_{\deg P \mid n} \deg P \sum_{j=1}^{\ell-1} \left(\frac{Q}{P}\right)_\ell^{jn/\deg P} \right).$$

Proof. The proof is exactly the same as the proof for hyperelliptic curves. Also, using the notation defined in Proposition 5.1, we can rewrite the above as

$$\operatorname{tr} \Theta_Q^n = \sum_{j=1}^{2g_Q} e^{in\theta_j(Q)} = -q^{-|n|/2} \left(\lambda_Q + \sum_{\deg F = |n|} \Lambda(F) \sum_{j=1}^{\ell-1} \left(\frac{Q}{F}\right)_\ell^{\pm j} \right),$$

where the power of the ℓ-residue symbol is j if $n > 0$, and $-j$ is $n < 0$. □

5.3. **Artin-Schreier curves.** We now consider the family of Artin-Schreier curves. Artin-Schreier curves represent a special family because they have no analogue over number fields, and their zeta function writes in a natural way with additive characters of $\mathbb{F}_p$, not multiplicative characters. Fix a finite field $\mathbb{F}_q$ of odd characteristic p. An Artin-Schreier curve over $\mathbb{F}_q$ is a smooth curve with an affine model

$$Y^p - Y = f(X),$$

where $f(X) \in \mathbb{F}_q(X)$ is a rational function. A formula for the genus of C, and details about the geometry of Artin-Schreier curves, are given in Section 6.3.

Let $N_C(\mathbb{F}_{q^k})$ be the number of points on C over $\mathbb{F}_{q^k}$ and $N_C(\mathbb{F}_{q^k}, \alpha)$ be the number of points on C over $\mathbb{F}_{q^k}$ in the fiber above $\alpha \in \mathbb{F}_{q^k}$. Then, if follows from Hilbert's Theorem 90 that

$$N_C(\mathbb{F}_{q^k}, \alpha) = \begin{cases} 1 & f(\alpha) = \infty \\ p & f(\alpha) \in \mathbb{F}_{q^k}, \operatorname{tr}_k f(\alpha) = 0 \\ 0 & f(\alpha) \in \mathbb{F}_{q^k}, \operatorname{tr}_k f(\alpha) \neq 0 \end{cases}$$

where $\operatorname{tr}_k : \mathbb{F}_{q^k} \to \mathbb{F}_p$ is the trace down to $\mathbb{F}_p$.

Then, writing the number of points of $C(\mathbb{F}_{q^k})$ with the additive characters of $\mathbb{F}_p$, we get that

$$N_C(\mathbb{F}_{q^k}) \quad = \quad \sum_{\substack{\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k}) \\ f(\alpha) \neq \infty}} \sum_{\psi} \psi(\operatorname{tr}_k f(\alpha)) + \sum_{\substack{\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k}) \\ f(\alpha) = \infty}} 1.$$

For each fixed non-trivial additive character of $\mathbb{F}_p$, we define

$$S_k(f,\psi) = \sum_{\substack{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})\\ f(\alpha)\neq\infty}} \psi(\mathrm{tr}_k\, f(\alpha))$$

and

$$L(f,u,\psi) = \exp\left(\sum_{k=1}^{\infty} S_k(f,\psi)\frac{u^k}{k}\right).$$

We first show that the zeta function $Z_C(u)$ can be written in terms of the L-functions $L(f,u,\psi)$.

Proposition 5.3. *Let C be the Artin-Schreier curve with affine equation $C: Y^p - Y = f(X)$, for some rational function $f(X)\in\mathbb{F}_q(X)$, with zeta function*

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)} = \frac{\prod_{j=1}^{2g}(1-u\alpha_j(C))}{(1-u)(1-qu)}.$$

Then,

$$P_C(u) = \prod_{\psi\neq 1} L(f,u,\psi).$$

Proof. We have that

$$\begin{aligned} Z_C(u) &= \exp\left(\sum_{k=1}^{\infty}\sum_{\substack{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})\\ f(\alpha)\neq\infty}}\sum_{\psi}\psi(\mathrm{tr}_k\, f(\alpha))\frac{u^k}{k} + \sum_{\substack{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})\\ f(\alpha)=\infty}}\frac{u^k}{k}\right)\\ &= \prod_{\psi\neq 1}\exp\left(\sum_{k=1}^{\infty}\sum_{\substack{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})\\ f(\alpha)\neq\infty}}\psi(\mathrm{tr}_k\, f(\alpha))\frac{u^k}{k}\right)\times\exp\left(\sum_{k=1}^{\infty}\sum_{\substack{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})\\ f(\alpha)\neq\infty}}\frac{u^k}{k} + \sum_{\substack{\alpha\in\mathbb{P}^1(\mathbb{F}_{q^k})\\ f(\alpha)=\infty}}\frac{u^k}{k}\right)\\ &= \prod_{\psi\neq 1} L(f,u,\psi)\times\exp\left(\sum_{k=1}^{\infty}(q^k+1)\frac{u^k}{k}\right) = \frac{\prod_{\psi\neq 1}L(f,u,\psi)}{(1-u)(1-qu)}, \end{aligned}$$

and

$$P_C(u) = \prod_{j=1}^{2g}(1-u\alpha_j(C)) = \prod_{\psi\neq 1} L(f,u,\psi).$$

□

Writing

$$L(u,f,\psi) = \prod_{j=1}^{2g/(p-1)}\left(1-\alpha_j(f,\psi)\right),$$

where $\alpha_j(f,\psi) = \sqrt{q}e^{i\theta_j(f,\psi)}$, we now write an explicit formula for

$$\mathrm{tr}\,\Theta_{f,\psi}^n = \sum_{j=1}^{2g/(p-1)} e^{in\theta_j(f,\psi)}.$$

Lemma 5.4. *Let $C: Y^p - Y = f(X)$ be an Artin-Schreier curve and ψ be a non-trivial additive character of $\mathbb{F}_p$. Then,*

$$\mathrm{tr}\,\Theta_{f,\psi}^n = \sum_{j=1}^{2g/(p-1)} e^{in\theta_j(f,\psi)} = \begin{cases} -\dfrac{S_n(f,\psi)}{q^{n/2}} & \text{for } n>0;\\ -\dfrac{S_{|n|}(f,\psi^{-1})}{q^{|n|/2}} & \text{for } n<0; \end{cases} \tag{29}$$

Proof. Recall from above that

$$L(u,f,\psi)=\exp\left(\sum_{n=1}^{\infty}S_n(f,\psi)\frac{u^n}{n}\right)=\prod_{j=1}^{2g/(p-1)}(1-\alpha_j(f,\psi)u). \tag{30}$$

Taking logarithmic derivatives, we have

$$\frac{d}{du}\sum_{j=1}^{2g/(p-1)}\log(1-\alpha_j(f,\psi)u)=\frac{d}{du}\sum_{n=1}^{\infty}S_n(f,\psi)\frac{u^n}{n}.$$

Multiplying both sides by u, we get

$$\sum_{j=1}^{2g/(p-1)}\frac{-\alpha_j(f,\psi)u}{1-\alpha_j(f,\psi)u}=\sum_{n=1}^{\infty}S_n(f,\psi)u^n,$$

that is,

$$-\sum_{j=1}^{2g/(p-1)}\sum_{n=1}^{\infty}(\alpha_j(f,\psi)u)^n=\sum_{n=1}^{\infty}S_n(f,\psi)u^n.$$

Comparing coefficients,

$$-\sum_{j=1}^{2g/(p-1)}(\alpha_j(f,\psi))^n=S_n(f,\psi).$$

Thus, for $n>0$, we get

$$-\sum_{j=1}^{2g/(p-1)}e^{in\theta_j(f,\psi)}=\frac{S_n(f,\psi)}{q^{n/2}}. \tag{31}$$

For $n<0$, taking complex conjugates, we have by (30) and (31)

$$\begin{aligned}-\sum_{j=1}^{2g/(p-1)}e^{in\theta_j(f,\psi)} &= -\overline{\sum_{j=1}^{2g/(p-1)}e^{i|n|\theta_j(f,\psi)}}=-\overline{\sum_{j=1}^{2g/(p-1)}\frac{\alpha_j(f,\psi)^{|n|}}{q^{|n|/2}}}\\ &= \frac{\overline{S_{|n|}(f,\psi)}}{q^{|n|/2}}=\frac{S_{|n|}(f,\overline{\psi})}{q^{|n|/2}}=\frac{S_{|n|}(f,\psi^{-1})}{q^{|n|/2}}.\end{aligned}$$

□

5.4. **Trigonal curves.** Let K/k be a cubic extension, i.e. K is a function field over $\mathbb{F}_q$ of degree 3. By definition, the zeta function of K writes as

$$\zeta_K(s)=\prod_{v\in\mathcal{S}_K}(1-|v|^{-s})^{-1},$$

where $\mathcal{S}_K$ is the set of primes of K. We can rewrite $\zeta_K(s)$ a a product over the primes $P\in\mathcal{S}_k$ by considering their splitting behavior in K. Since K/k is a cubic extension, there are 5 cases, namely: $P=v_1v_2v_3$ (i.e. P is totally split), or $P=v_1v_2$ (i.e. P is partially split), or $P=v_1v_2^2$ (i.e. P is partially ramified), or $P=v_1^3$ (i.e. P is totally ramified), or $P=v_1$ (i.e. P is inert). We write $\mathcal{S}_k$ as the disjoint union of the sets $\mathcal{S}_{111},\mathcal{S}_{12},\mathcal{S}_{11^2},\mathcal{S}_{1^3}$ and $\mathcal{S}_3$ according to the 5 cases above. Then, by definition of $\zeta_K(s)$, we have for $\mathrm{Re}(s)>1$, that

$$\frac{\zeta_K(s)}{\zeta_k(s)}=\prod_{P\in\mathcal{S}_{111}}\left(1-|P|^{-s}\right)^{-2}\prod_{P\in\mathcal{S}_{12}}\left(1-|P|^{-2s}\right)^{-1}\prod_{P\in\mathcal{S}_{11^2}}\left(1-|P|^{-s}\right)^{-1}\prod_{P\in\mathcal{S}_3}\left(1-|P|^{-3s}\right)^{-1}(1-|P|^{-s}).$$

Then, it follows from Theorem 3.9 that for $u=q^{-s}$,

$$\frac{\zeta_K(s)}{\zeta_k(s)}=P_C(u)=\prod_{j=1}^{2g}\left(1-\sqrt{q}\,u\,e^{i\theta_j(C)}\right), \tag{32}$$

where C is the smooth curve of genus g with function field K. We can then use the zeta function of K to write the sum of powers of the roots of $P_C(u)$ (and then the number of points of C over extensions of $\mathbb{F}_q$).

Proposition 5.5. [TX14, Proposition 3] *For each integer $n \geq 1$, we have*

$$-q^{n/2}\sum_{j=1}^{2g} e^{in\theta_j(C)} = \sum_{\substack{P\in S_{111}\\ \deg P|n}} 2\deg P + \sum_{\substack{P\in S_{12}\\ \deg P|n/2}} 2\deg P + \sum_{\substack{P\in S_{11^2}\\ \deg P|n}} \deg P + \sum_{\substack{P\in S_3\\ \deg P|n/3}} \deg P - \sum_{\substack{P\in S_3\\ \deg P|n}} \deg P.$$

Proof. The result follows by taking the logarithmic derivative on both sides of (32) with respect to s, and the expression for $\zeta_K(s)/\zeta_k(s)$ as an Euler product. □

6. Average number of points over $\mathbb{F}_{q^n}$

We now consider the average number of points of curves C over $\mathbb{F}_{q^n}$ when C varies over various families of curves defined over $\mathbb{F}_q$. If C is a curve over $\mathbb{F}_q$ with zeta function

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)} = \frac{\prod_{j=1}^{2g}\left(1-\sqrt{q}e^{i\theta_j(C)}\right)}{1-u)(1-qu)},$$

and Θ_C is the diagonal matrix with entries $e^{i\theta_j(C)}$, then

$$\#C(\mathbb{F}_{q^n}) - (q^n+1) = -q^{n/2}\operatorname{tr}\Theta_C.$$

6.1. **Hyperelliptic curves in the q-limit for fixed g.** Let $\mathcal{H}_g$ be the moduli space of hyperelliptic curves of genus g. For each $C \in \mathcal{H}_g$, let Θ_C be the diagonal matrix with entries $e^{i\theta_j(C)}$. Then, Θ_C is a $2g \times 2g$ unitary symplectic matrix in $\mathrm{USp}(2g)$. When g is fixed and $q \to \infty$, Katz and Sarnak [KS99a] showed that the Frobenius classes Θ_C become equidistributed in in the unitary symplectic group $USp(2g)$.

Theorem 6.1. *(Equidistribution Theorem for hyperelliptic curves) Let $\mathcal{H}_g(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-isomorphism classes of hyperelliptic curves of genus g over $\mathbb{F}_q$, and let f be any continuous class function on $USp(2g)$. Then*

$$\lim_{q\to\infty}\langle f(\Theta_C)\rangle := \lim_{q\to\infty}\frac{\sum'_{C\in\mathcal{H}_g(\mathbb{F}_q)} f(\Theta_C)}{\sum'_{C\in\mathcal{H}_g(\mathbb{F}_q)} 1} = \int_{USp(2g)} f(A)dA,$$

where $\sum'$ means that every curve should be weighted by $\frac{1}{\#Aut(C/\mathbb{F}_q)}$.

Then, this gives the distribution of the average number of points of C over $\mathbb{F}_{q^n}$ since

$$\#C(F_{q^n}) - (q^n+1) = -q^{n/2}\operatorname{tr}\Theta_C^n.$$

Corollary 6.2. *When g is fixed and q tends to infinity, the normalised power of traces $\operatorname{tr}\Theta_C^n = \sum_{j=1}^{2g} e^{2\pi i\theta_j(C)}$ are distributed over the family of hyperelliptic curves C as the power of trace $\operatorname{tr}U^n$ of a random matrix U in the group $USp(2g)$ of $2g\times 2g$ unitary symplectic matrices, i.e.*

$$\lim_{q\to\infty}\langle \operatorname{tr}\Theta_C^n\rangle = \int_{USp(2g)} \operatorname{tr}(U^n)\, dU.$$

We can then identify the limiting distribution which depends only on random matrix theory. In particular, it is shown in [DS94] that the average of the traces of powers averaged over $\mathrm{USp}(2g)$ is given by

$$\int_{\mathrm{USp}(2g)} \operatorname{tr}(U^n)\, dU = \begin{cases} 2g & n=0 \\ -\eta_n & 1\le|n|\le 2g \\ 0 & |n|>2g \end{cases}, \tag{33}$$

where

$$\eta_n = \begin{cases} 1 & n \text{ even} \\ 0 & n \text{ odd.} \end{cases} \tag{34}$$

We remark that for $g=1$ (i.e. the case of elliptic curves), the distribution at the q-limit given by Theorem 6.1 was proven by Birch [Bir68] for q prime, and by Deligne [Del80] for all q. For the context of elliptic curves, the Haar measure on $\mathrm{USp}(2)$ is also called the Sato-Tate measure. Let p be a prime and let E be an elliptic curve over $\mathbb{F}_p$. Then, Θ_E is the matrix with diagonal entries $e^{i\theta_p(E)}, e^{-i\theta_p(E)}$ for some unique angle $\theta_p(E)\in[0,\pi]$, and Birch showed that

$$\lim_{p\to\infty}\operatorname{Prob}\left(a\le\theta_p(E)\le b\right) = \frac{1}{\pi}\int_a^b \sin^2\theta\, d\theta,$$

using the Eichler-Selberg's trace formula.

We follow here Birch's proof to give a formula for the average number of points $\#E(\mathbb{F}_{p^n})$, when E varies over all elliptic curves defined over $\mathbb{F}_p$, at the limit when $p\to\infty$, as outlined in [BG01]. For any function F on $\mathrm{USp}(2)$ invariant by conjugation, we let $\sum'_{\tilde{E}/\mathbb{F}_p} F(\Theta_E)$ denote the sum is over representatives $\tilde{E}$ of

the $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ weighted by $2/\#\mathrm{Aut}(E)$. Then, $\sum_{\tilde{E}/\mathbb{F}_p}' 1 = 2p$, and we define the average over elliptic curve over $\mathbb{F}_p$ as

$$\langle F(\Theta_E)\rangle_p := \frac{1}{2p}\sum_{\tilde{E}/\mathbb{F}_p}' F(\Theta_E).$$

We write $\alpha_p(E) = \sqrt{p}\, e^{i\theta_p(E)}$. Then,

$$p^{n/2}\,\mathrm{tr}\,\Theta_E^n = \alpha_p(E)^n + \overline{\alpha_p(E)}^n, \quad \text{and} \quad \#E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha_p(E)^n + \overline{\alpha_p(E)}^n).$$

Selberg's trace formula [Sel65] implies that for all even integers $n \geq 0$

$$\sigma_n(T_p) + 1 = -\frac{1}{2}\sum_{\tilde{E}/\mathbb{F}_p}' \frac{\alpha_p(E)^{n-1} - \overline{\alpha_p(E)}^{n-1}}{\alpha_p(E) - \overline{\alpha_p(E)}}$$

where $\sigma_n(T_p)$ is the trace of the Hecke operator T_p acting on the cusp forms of weight n in $\mathrm{SL}_2(\mathbb{Z})$ for $n \geq 4$. We also have that $\sigma_0(T_p) = 0$ and $\sigma_2(T_p) = -p - 1$ which follows from $\sum_{\tilde{E}/\mathbb{F}_p}' 1 = 2p$. Since

$$\frac{\alpha_p(E)^{n+1} - \overline{\alpha_p(E)}^{n+1}}{\alpha_p(E) - \overline{\alpha_p(E)}} - p\frac{\alpha_p(E)^{n-1} - \overline{\alpha_p(E)}^{n-1}}{\alpha_p(E) - \overline{\alpha_p(E)}} = \alpha_p(E)^k + \overline{\alpha_p(E)}^n,$$

we deduce that for even $n \geq 2$

$$\left\langle \mathrm{tr}\, p^{n/2}\,\Theta_E^n \right\rangle_p := \frac{\sum_{\tilde{E}/\mathbb{F}_p}' \alpha_p(E)^n + \overline{\alpha_p(E)}^n}{\sum_{\tilde{E}/\mathbb{F}_p}' 1} = \sigma_n(T_p) + 1 - \frac{1}{p}\left(\sigma_{n+2}(T_p) + 1\right). \tag{35}$$

Since $\sigma_n(T_p) = 0$ for $n = 4, 6, 8, 10, 14$ and $\sigma_{12}(T_p) = \tau(p)$, the Ramanujan's τ-function, we have that the first few values of

$$\langle \#E(\mathbb{F}_{p^n}) - (p^n + 1)\rangle_p = \left\langle p^{n/2}\,\mathrm{tr}\,\Theta_E^n \right\rangle_p$$

are given by

$$\begin{aligned}
\left\langle \#E(\mathbb{F}_{p^2}) - (p^2+1)\right\rangle_p &= p + 1/p \\
\left\langle \#E(\mathbb{F}_{p^n}) - (p^n+1)\right\rangle_p &= -1 + 1/p \quad \text{for } n = 4, 6, 8 \\
\left\langle \#E(\mathbb{F}_{p^{10}}) - (p^{10}+1)\right\rangle_p &= -1 + \frac{\tau(p)+1}{p} \\
\left\langle \#E(\mathbb{F}_{p^{12}}) - (p^{12}+1)\right\rangle_p &= -1 - \tau(p) + \frac{1}{p}.
\end{aligned}$$

For general n, using Deligne's bound [Del71, Del74]

$$\sigma_n(T_p) = O\left(p^{(n-1)/2+\varepsilon}\right),$$

we have from (35) that

$$\langle \#E(\mathbb{F}_{p^n}) - (p^n + 1)\rangle_p = O\left(p^{(n-1)/2+\varepsilon}\right).$$

Working similarly, Birch proved that the matrices Θ_E, as E varies over elliptic curves over $\mathbb{F}_p$, are distributed according to the Sato-Tate measure by computing all the moments

$$\left\langle \left(\frac{\alpha_p(E) + \overline{\alpha_p(E)}}{2\sqrt{p}}\right)^{2n} \right\rangle_p,$$

and comparing with the analogous moments for the Sato-Tate distribution, i.e. checking that

$$\left\langle \left(\frac{\alpha_p(E) + \overline{\alpha_p(E)}}{2\sqrt{p}}\right)^{2n} \right\rangle_p \sim \begin{cases} \frac{2R!}{R!(R+1)!}p^R & n = 2R \\ 0 & k = 2R+1, \end{cases}$$

as $p \to \infty$ [Bir68, Theorem 1]. We remark that the fact that the odd moments are zero follows from symmetry. Indeed, suppose that $p > 5$, so every curve has a model $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$. If $E : y^2 = x^3 + ax + b$ has $p + 1 - a_p(E)$ points over $\mathbb{F}_p$, then $E_d : dy^2 = x^3 + ax + b$ has $p + 1 - \left(\frac{d}{p}\right) a_E(p)$ points over $\mathbb{F}_p$, and the distribution of

$$\operatorname{tr} \Theta_p(E) = \frac{a_p(E)}{2\sqrt{p}}$$

is symmetric, so the odd moments are 0.

6.2. **Hyperelliptic curves in the g-limit for q fixed.** This section describes the results of [Rud10] where the author computes the distribution of $\operatorname{tr} \Theta_C^n$ where C varies over hyperelliptic curves of genus g, for q fixed and $g \to \infty$.

Consider the space $\mathcal{H}_{2g+1}$ of hyperelliptic curves over $\mathbb{F}_q$ given by

$$C_D \ : \ Y^2 = D(X)$$

where $D(X)$ is a square-free, monic polynomial of degree $2g+1$. The curve C_D is then non-singular and has genus g. For any function f on $\mathcal{H}_{2g+1}$, we define

$$\langle F \rangle := \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{D \in \mathcal{H}_{2g+1}} f(D).$$

We saw in the precedent section the distribution of $\langle \operatorname{tr} \Theta_D^n \rangle$ at the q-limit. Without taking the q-limit, it can be proven that

Theorem 6.3. [Rud10, Theorem 1] *For all $n > 0$, we have*

$$\langle \operatorname{tr} \Theta_D^n \rangle = \begin{cases} -\eta_n & 1 \le n < 2g \\ -1 - \frac{1}{q-1} & n = 2g \\ 0 & n > 2g \end{cases} + \eta_n \frac{1}{q^{n/2}} \sum_{\deg P \mid \frac{n}{2}} \frac{\deg P}{|P| + 1} + O_q\left(nq^{n/2-2g} + gq^{-g}\right),$$

where the sum is over all irreducible polynomials P, and where $|P| := q^{\deg P}$, and η_n is defined by (34).

Corollary 6.4. *If $3 \log_q g < n < 4g - 5 \log_q g$, but $n \neq 2g$, then*

$$\langle \operatorname{tr} \Theta_D^n \rangle = \int_{USp(2g)} \operatorname{tr} U^n \, dU + \underline{o}\left(\frac{1}{g}\right).$$

This fits the random matrix model for n large enough (with respect to g), but we get deviations for small values of n, for instance

$$\left\langle \operatorname{tr} \Theta_D^2 \right\rangle \sim \int_{\mathrm{USp}(2g)} \operatorname{tr} U^2 \, du + \frac{1}{q+1}.$$

Also, for $n = 2g$, when q is fixed and $g \to \infty$, we have

$$\left\langle \operatorname{tr} \Theta_D^{2g} \right\rangle \sim \int_{\mathrm{USp}(2g)} \operatorname{tr} U^{2g} \, du - \frac{1}{q-1}.$$

We remark that there is a "bias" in the number of points over $\mathbb{F}_{q^n}$ for n even when C varies over hyperelliptic curves defined over $\mathbb{F}_q$, as it follows from Corollary 6.4 that the average number of point is

$$\langle \#C(\mathbb{F}_{q^n}) \rangle = \left\langle q^n + 1 - q^{n/2} \operatorname{tr} \Theta_C^n \right\rangle \sim \begin{cases} q^n + \underline{o}(q^{n/2}) & n \text{ odd} \\ q^n + q^{n/2} + \underline{o}(q^{n/2}) & n \text{ even}, \end{cases}$$

when $g \to \infty$, and $3 \log_q g < n < 4g - 5 \log_q g$. This was observed by Brock and Granville [BG01], and the bias is because the family of hyperelliptic curves has unitary symplectic symmetries, and the average of traces of powers averaged over $\mathrm{USp}(2g)$ has a "bias" as it can be seen in (33). This bias is then a feature of the statistics at the q-limit, but it also shows without taking the q-limit when n is large enough with respect to the genus of the family, as proven by Theorem 6.3. See also [BG01, Corollary 6.1].

We now outline some details of the proof of Theorem 6.3 as given in [Rud10]. Using the explicit formula of Proposition 5.1, one has to compute the average

$$\left\langle \sum_{\deg F=n} \Lambda(F)\chi_D(F) \right\rangle$$

over the family of hyperelliptic curves $C_D : Y^2 = D(X)$ of genus g. One treats separately the contributions coming from F prime, F a square, and F an odd power greater than 1 of a prime. The contribution from the squares on average over the family can be shown to be

$$-1 + O\left(\frac{n}{q^{n/2}}\right) + O(q^{-2g}) = -\eta_n \left(1 + \underline{o}\frac{1}{g}\right),$$

when $n \gg \log_q(g)$. This explains the bias (as there is no contribution from the squares if $n = \deg F$ is odd). To analyze the contribution of the primes, we are led to consider the double character sums

$$S(\beta; n) := \sum_{\substack{\deg P=n \\ P \text{ prime}}} \sum_{\substack{\deg B=\beta \\ B \text{ monic}}} \left(\frac{B}{P}\right),$$

and we write the contribution coming from the primes as

$$\frac{-n}{(q-1)q^{2g+n/2}} \sum_{\substack{\beta+2\alpha=2g+1 \\ \alpha,\beta\geq 0}} \sigma_n(\alpha) S(\beta; n).$$

For $n \leq g$, the contribution is bounded by gq^{-g} which goes to 0 as $g \to \infty$. For $g < n < 2g$, $S(g \pm 1; n) = 0$, and there is no contribution. For $n = 2g$, we get a contribution of

$$\frac{1}{q-1} + O\left(gq^{-g}\right).$$

For $2g < n$, we get a contribution of

$$\eta_n \left(1 + O\left(gq^{-g}\right)\right) + O\left(nq^{n/2-2g}\right),$$

and we get an estimate when $2g < n < 4g - 4\log_q g$. Finally, we show that the contribution from the higher prime powers is bounded, and we get the result.

6.3. **Artin-Schreier curves.** We compute in this section the average number of points over $\mathbb{F}_{q^n}$ for the ordinary strata of Artin-Scheier curves, as done in [BDFL].

Given a Artin-Schreier curve $C : Y^p - Y = f(X)$ where $f(X) \in \mathbb{F}_q(X)$ is a rational function over a finite field of characteristic $p \geq 3$ which has poles at the projective points $P_1, \ldots, P_{r+1}$ of order $d_1, \ldots, d_{r+1}$ with $p \nmid d_1 \ldots d_{r+1}$, the genus of C is given by

$$g = \left(-2 + \sum_{j=1}^{r+1} e_j\right) \frac{p-1}{2}.$$

Note that we can always make a change a variables to get to the case when $p \nmid d_1 \ldots d_{r+1}$, so this condition does not impose any restriction on the family of curves. Furthermore, the moduli space of Artin-Schreier curves of genus g breaks into strata according to the p-rank of the Jacobian of C. [1] We have that

$$\mathrm{Jac}(C)[p](\mathbb{F}_q) = p^s, \quad \text{where } s = r(p-1) \text{ for some nonnegative integer } r.$$

[1] In the case of an E is an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic p, since the genus of E is 1, the p-rank is either 0 or 1, and it can be read from the Newton polygon of $P_E(u) = u^2 - a_p(E)u + p$. There are only 2 cases here, either one of the slope is 0 and the other one is 1, and E has p-rank 1 (and E is ordinary), or there are two slopes of $1/2$ and E has p-rank 0 (and E is supersingular). For an arbitrary curve C defined over a finite field $\mathbb{F}_q$ of characteristic p, the Newton polygon of $P_C(u)$ has length $2g(C)$ and gets up to height $g(C)$, and the p-rank is the length of the edge of slope 0. Then, C is ordinary if the p-rank is equal to the genus, and C is supersingular if the Newton polygon consists only of the slope $1/2$ that appears with multiplicity $2g(C)$ (i.e. the polygon is a straight line). Both the Newton polygon and the p-rank are isogeny invariants.

If $r = s = 0$, then $f(X)$ has one pole of degree d that can be moved at ∞, and $g = \frac{(d-1)(p-1)}{2}$. The p-rank 0 strata then consists of exactly the curves with affine model $Y^p - Y = f(X)$ with

$$f(X) \in \mathcal{F}_d^0 = \{f(X) \in \mathbb{F}_q[X], \ \deg f = d, a_{kp} = 0\}.$$

Note that our goal is count Artin-Schreier covers up to isomorphism. If $a_{kp} \neq 0$ one can employ a simple change of variables to obtain a model with $f \in \mathcal{F}_d$. Furthermore, this is the only restriction we have to impose in order to make sure we counting each isomorphism class exactly once.

We remark that the p-rank 0 strata contains the supersingular locus (they are usually not equal), but "most of the curves" are in the maximal p-rank stratum. (That is, this stratum is dense in every irreducible component of the moduli space that it meets. Note that usually $\mathcal{AS}_g$ is not irreducible, and the ordinary locus is not usually dense in the whole space.) The maximal p-rank is the same as the ordinary locus, if this locus is nonempty. For the ordinary locus, we must have

$$r(p-1) = g = \left(\sum_{j=1}^{r+1} e_j - 2\right) \frac{p-1}{2} \iff e_j = 2, j = 1, \ldots, r+1,$$

and $g = r(p-1)$. In particular, the ordinary locus exists only when the genus g happens to be even. (If g is odd the maximal p-rank is $g - \frac{p-1}{2}$.) For g even, the ordinary locus consists of the curves $Y^p - Y = f(X)$, where $f(X)$ has $r+1$ simple poles with $r = g/(p-1)$.

Let $\mathcal{F}$ be a family of Artin-Schreier covers defined over $\mathbb{F}_q$ (for example, $\mathcal{F}$ is a stratum of the p-rank stratification). For any $\alpha, \beta \in \mathbb{P}^1(\mathbb{F}_{q^k})$, let

$$\mathcal{F}(\alpha, \beta) = \{f \in \mathcal{F} \ : \ f(\alpha) = \beta\}.$$

Then, it follows from Hilbert's Theorem 90 (see Section 5.3) that the average number of points over the family, which was defined as

$$\left\langle N_C(\mathbb{F}_{q^k}) \right\rangle_{\mathcal{F}} \ := \ \frac{1}{\#\mathcal{F}} \sum_{C \in \mathcal{F}} N_C(\mathbb{F}_{q^k}),$$

is given by

$$\left\langle N_C(\mathbb{F}_{q^k}) \right\rangle_{\mathcal{F}} \ = \ \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_q)} \frac{\#\mathcal{F}(\alpha, \infty)}{\#\mathcal{F}} + \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})} \sum_{\substack{\beta \in \mathbb{F}_{q^k} \\ \mathrm{tr}_k \, \beta = 0}} p \frac{\#\mathcal{F}(\alpha, \beta)}{\#\mathcal{F}}$$

The number of points over $\mathbb{F}_{p^k}$ will behave differently if $p \mid k$ as tr_k will be zero on the whole subfield $\mathbb{F}_{q^{k/p}}$. We want to study that over various families defined in terms of some geometrical invariants. In each case, we need to compute $\#\mathcal{F}(\alpha, \beta)$. and in for $\alpha, \beta \in \mathbb{P}^1(\mathbb{F}_{q^k})$. If $\mathcal{F}$ is the stratum of p-rank 0, then the family is indexed by $f \in \mathcal{F}_d^0$ defined above. The size of the family is $q^{d+1-\lfloor d/p \rfloor}$. In this case, for any $\alpha \in \mathbb{F}_{q^k}$ of degree u and $\beta \in \mathbb{F}_{q^u}$, we have

$$\#\mathcal{F}_d^0(\alpha, \beta) = q^{d+1-\lfloor d/p \rfloor - u}.$$

If $\mathcal{F}$ is the ordinary locus, the family is indexed by the set $\mathcal{F}_d^{\mathrm{ord}}$ of rational functions defined over $\mathbb{F}_q$ with exactly d simple poles. The size of the family is already more complicated, namely

$$\#\mathcal{F}_d^{\mathrm{ord}} = \frac{H(1) q^{2d+2}}{\zeta_q(2)^2} + O\left(q^{(3/2+\varepsilon)d}\right),$$

where

$$H(1) = \prod_P \left(1 + \frac{1}{(|P|+1)(|P|^2-1)}\right),$$

where the product is over monic irreducible polynomials of $\mathbb{F}_q[X]$. This involves the use of the Tauberian Theorem for function fields [Ros02, Theorem 17.1].

As for the size of the fibers, for $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k})$ of degree u and $\beta \in \mathbb{P}^1(\mathbb{F}_{q^u})$, we have [BDFL, Corollary 3.9].

$$\#\mathcal{F}_d^{\mathrm{ord}}(\alpha,\beta) = \begin{cases} \frac{H(1)q^{2d+2-u}(1-q^{-u})}{\zeta_q(2)^2(1+q^{-u}-q^{-2u})} + O\left(q^{(3/2+\varepsilon)d+u}\right) & \beta=\infty, \\ \\ \frac{H(1)q^{2d+2-u}}{\zeta_q(2)^2(1+q^{-u}-q^{-2u})} + O\left(q^{(3/2+\varepsilon)d}\right) & \beta\in\mathbb{F}_{q^u}. \end{cases} \tag{36}$$

It then follows that

Theorem 6.5. *The expected number of $\mathbb{F}_{q^k}$-points on an Artin-Schreier cover defined over $\mathbb{F}_q$ with p-rank equal to 0 is*

$$\begin{cases} q^k+1 & p\nmid k \\ q^k+1+(p-1)q^{k/p} & p\mid k \end{cases}.$$

The expected number of $\mathbb{F}_{q^k}$-points on an ordinary Artin-Schreier cover defined over $\mathbb{F}_q$ is

$$\begin{cases} q^k+1+O\left(q^{(-1/2+\varepsilon)d+2k}\right) & p\nmid k \\ q^k+1+\frac{p-1}{1+q^{-1}-q^{-2}}+\sum_{u|\frac{k}{p}}\frac{p-1}{1+q^{-u}-q^{-2u}}\sum_{v|u}\mu(v)q^{u/v}+O\left(q^{(-1/2+\varepsilon)d+2k}\right) & p\mid k \end{cases}.$$

In particular, the average number of $\mathbb{F}_{q^p}$-points on an ordinary cover is

$$q^p+1+\frac{(p-1)(q+1)}{1+q^{-1}-q^{-2}}+O\left(q^{(-1/2+\varepsilon)d+2p}\right).$$

7. Zeros in intervals

Let C be a curve over $\mathbb{F}_q$ with zeros $\alpha_j(C) = \sqrt{q}e^{2\pi i\theta_j(C)}$, and eigenangles $\theta_1(C), \dots, \theta_{2g}(C)$. For any an interval $\mathcal{I} \subset [-1/2, 1/2)$, we define

$$N_{\mathcal{I}}(C) := \#\{1 \le j \le 2g \ : \ \theta_j(C) \in \mathcal{I}\},$$

and we want to study the distribution of $N_{\mathcal{I}}(C)$ when C varies over the curves in a family $\mathcal{F} = \mathcal{F}(g, q)$. For q large, the distribution is given by distribution of random matrices as usual. Let $M(2g) \subseteq U(2g)$ be a probability space under the Haar measure, $U \in \mathrm{M}(2g)$ with eigenangles $\theta_1(U), \dots, \theta_{2g}(U)$, and set

$$N_{\mathcal{I}}(U) = \#\left\{j \ : \ \theta_j(U) \in \mathcal{I}\right\}.$$

If the family $\mathcal{F}(g, q)$ has symmetry type $M(2g)$, then it follows from the work of Katz and Sarnak that (for example)

$$\lim_{q\to\infty} \frac{\#\left\{C \in \mathcal{F}(g,q) \ : \ N_{\mathcal{I}}(C) = k\right\}}{\#\mathcal{F}(g,q)} = \mathrm{Prob}_{M(2g)}\left(N_{\mathcal{I}}(U) = k\right).$$

It follows from classical results on random matrix theory that the statistics for $N_{\mathcal{I}}(U)$ for $U \in M(2g)$ have Gaussian distribution at the limit for large g in various ensemble of random matrices. In particular, as $g \to \infty$

$$\begin{aligned} \mathbb{E}\left[N_{\mathcal{I}}(U)\right] &\sim 2g|\mathcal{I}| \\ \mathbb{E}\left[\left(N_{\mathcal{I}}(U) - 2g|\mathcal{I}|\right)^2\right] &\sim \frac{2}{\pi^2}\log\left(2g|\mathcal{I}|\right) \end{aligned}$$

and the random variable

$$\frac{N_{\mathcal{I}}(U) - 2g|\mathcal{I}|}{\sqrt{\frac{2}{\pi^2}\log\left(2g|\mathcal{I}|\right)}}$$

has a normal distribution as $g \to \infty$. (The variance might differ slightly for different ensembles of random matrices).

Then, if the family $\mathcal{F}(g, q)$ has symmetry type $M(2g)$, it follows from the work of Katz and Sarnak that

$$\lim_{g\to\infty}\left(\lim_{q\to\infty}\mathrm{Prob}_{\mathbb{F}(g,q)}\left(a < \frac{N_{\mathcal{I}}(C) - 2g|\mathcal{I}|}{\sqrt{\frac{2}{\pi^2}\log\left(2g|\mathcal{I}|\right)}} < b\right)\right) = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-x^2/2}\,dx.$$

We now study this question in the limit when the genus goes to infinity, but without taking the limit when $q \to \infty$ first. It turns out that one can show that the fluctuations of $N_{\mathcal{I}}(C)$ (minus the mean and divided by the standard deviation) are also Gaussian. This holds for intervals of fixed length, and also intervals of size going to 0 as long as $|\mathcal{I}|g \to \infty$ as $g \to \infty$. This question was first addressed by Faifman and Rudnick for hyperelliptic curves [FR10], and then generalised to other families as cyclic ℓ-covers [Xio10b], Artin-Schreier curves of p-rank 0 [Ent12, BDF$^+$12], ordinary Artin-Schreier curves [BDFL] and trigonal curves [TX14]. In all those proofs, the starting point is to use the the Beurling-Selberg polynomials of level K to approximate the characteristic function of the interval $\mathcal{I}$, and the appropriate version of the explicit formulas to relate the sum over zeros to a sum over the coefficients of the zeta function of the curve.

We first review the Beurling-Selberg polynomials. For all details, we refer the reader to [Mon94]. Let $\mathcal{I} = [-\beta/2, \beta/2]$ be a symmetric interval, and for each K, let

$$I_K^{\pm}(x) = \sum_{|k|\le K} c(k)e(kx)$$

be the Berling-Selberg polynomials of degree K. Those are even trigonometric polynomials (i.e. $c(-k) = c(k)$) which approximate very well $\chi_{\mathcal{I}}$, the characteristic function of the interval $\mathcal{I}$. In particular, they approximate $\chi_{\mathcal{I}}(x)$ in a monotone manner

$$I_K^-(x) \le \chi_{\mathcal{I}}(x) \le I_K^+(x),$$

and the integral of $I_K^{\pm}$ is close to the length of the interval $\mathcal{I}$

$$\left|\int_0^1 I_K^{\pm 1}(x) - \int_0^1 \chi_{\mathcal{I}}(x)\,dx\right| \leq \frac{1}{K+1}. \tag{37}$$

We record some useful properties of the Beurling-Selberg polynomials.

Proposition 7.1. *Let $\mathcal{I} = [-\beta/2, \beta/2]$, and let $K \geq 1$ be an integer such that $K\beta > 1$. Let*

$$I_K^{\pm}(x) = \sum_{k \leq K} c(k) e(kx)$$

be the Berling-Selberg polynomials of degree K. Then,

$$\begin{aligned} |c^{\pm}(k)| &\leq \frac{1}{K+1} + \min\left(\beta, \frac{\pi}{|k|}\right), \quad 0 < |k| < K \\ \sum_{k \geq 1} c_K^{\pm}(2k) &= O(1) \\ \sum_{k \geq 1} k c_K^{\pm}(k)^2 &= \frac{1}{2\pi^2}\log(K\beta). \end{aligned}$$

Proof. Those follows by looking comparing the Fourier of $\chi_{\mathcal{I}}(x) = \sum_{k\in\mathbb{Z}} a(k)e(kx)$, where

$$a(k) = \begin{cases} \frac{\sin 2\pi k\beta}{2\pi k} & k \neq 0 \\ 1 & k = 0, \end{cases}$$

and $I_K^{\pm}(x)$ and using (37). □

Let $\mathcal{F}(g,q)$ be a family of curves of genus g over $\mathbb{F}_q$. Using the explicit formulas for this family and the Beurling-Selberg polynomials, we show that the normalised moments of $N_{\mathcal{I}}(C) - 2g|\mathcal{I}|$ match the moments of a Gaussian, i.e.

$$\left\langle \left(\frac{N_{\mathcal{I}}(C) - 2g|\mathcal{I}|}{\sqrt{\frac{1}{\pi^2}\log(2g|\mathcal{I}|)}} \right)^n \right\rangle_{\mathcal{F}_g} \sim \begin{cases} \dfrac{(2\ell)!}{\ell! 2^\ell} & n = 2\ell, \\ 0 & n = 2\ell+1, \end{cases}$$

We give some outline of the proofs in the case of Artin-Schreier curves. We fix an additive character ψ, and we study the distribution of the zeros of the L-functions $L(u, f, \psi)$ attached to the Artin-Schreier curves $Y^p - Y = f(X)$ when f runs into some family $\mathcal{F}_d$ of indexed by the degree d, as $\mathcal{F}_d^{\mathrm{ord}}, \mathcal{F}_d^{\mathrm{full}}$ or any of the family with precribed ramification type as described in Section 6.3. Then, each $L(u, f, \psi)$ has $2g/(p-1)$ zeros, and we denote the angles by $\theta_j(f, \psi)$.

It follows from using the explicit formula of Proposition 5.4 that

$$\sum_{j=1}^{2g/(p-1)} I_K^{\pm}(\theta_j(f,\psi)) - \frac{2g}{p-1} c_K^{\pm}(0) = \sum_{1 \leq k \leq K} \frac{c_K^{\pm}(k) S_K(f,\psi) + c_K^{\pm}(-k) S_k(f, \bar{\psi})}{q^{k/2}}$$

where

$$S_k(f,\psi) = \sum_{\substack{\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k}) \\ f(\alpha) \neq \infty}} \psi(\mathrm{tr}_k\, f(\alpha)),$$

and from the properties of the Beurling-Selberg polynomials, this gives

$$N_{\mathcal{I}}(f,\psi) - \frac{2g}{p-1}|\mathcal{I}| \approx \sum_{1 \leq k \leq K} \frac{c_K^{\pm}(k) S_K(f,\psi) + c_K^{\pm}(-k) S_k(f, \bar{\psi})}{q^{k/2}}$$

Then, to get the mean of $N_{\mathcal{I}}(f,\psi)$ over each family $\mathcal{F}_d$, we need to compute for each $1 \leq k \leq K$

$$\langle S_k(f,\psi)\rangle_{\mathcal{F}_d} = \frac{1}{\#\mathcal{F}_d} \sum_{f \in \mathcal{F}_d} \sum_{\substack{\alpha \in \mathbb{P}^1(\mathbb{F}_{q^k}) \\ f(\alpha) \neq \infty}} \psi(\mathrm{tr}_k\, f(\alpha)).$$

Reversing the sums, this becomes

$$\frac{1}{\#\mathcal{F}_d}\sum_{\alpha\in\mathbb{F}_{q^k}}\sum_{\substack{f\in\mathcal{F}_d\\ f(\alpha)\neq\infty}}\psi(\mathrm{tr}_k\, f(\alpha))=\sum_{\beta\in\mathbb{F}_{q^u}}\psi(\mathrm{tr}_k\,\beta)\frac{\#\mathcal{F}_d(\alpha,\beta)}{\#\mathcal{F}_d}$$

where $\mathcal{F}_d(\alpha,\beta)$ is the number of $f\in\mathcal{F}_d$ such that $f(\alpha)=\beta$.

By (36), for any $\beta,\beta'\in\mathbb{F}_{q^u}$, we have that $\#\mathcal{F}_d(\alpha,\beta)\sim\#\mathcal{F}_d(\alpha,\beta')$, and we expect that the sum above will be 0, because when β runs over the elements of $\mathbb{F}_{q^u}$, $\mathrm{tr}_k\,\beta$ takes every value in $\mathbb{F}_p$ the same number of times, and then

$$\psi(\mathrm{tr}_k\,\beta)=e^{2\pi i\,\mathrm{tr}_k\,\beta/p}$$

takes each pth root of 1 the same number of times. Unless $p\mid k$, and $\alpha\in\mathbb{F}_{q^{k/p}}$: in that case, $\beta=f(\alpha)\in\mathbb{F}_{q^{k/p}}$, and

$$\mathrm{tr}_k\,\beta=p\,\mathrm{tr}_{k/p}\,\beta=0,$$

and $\psi(\mathrm{tr}_k\,\beta)=e\left(\frac{2\pi i\,\mathrm{tr}_k\,\beta}{p}\right)=1$. The bound for $\langle S_k(f,\psi)\rangle_{\mathcal{F}_d}$ can be deduced by summing over all $\alpha\in\mathbb{F}_{q^k}$ which give a contribution, and we get

$$\langle S_k(f,\psi)\rangle_{\mathcal{F}_d}\ll q^{k/p}$$

(dealing appropriately with all the error terms). Then, using the explicit formulas and summing over all $1\le k\le K$, we get

$$\left\langle N_{\mathcal{I}}(f,\psi)-\frac{2g}{p-1}|\mathcal{I}|\right\rangle_{\mathcal{F}_d}\ll 1.$$

Similarly, for the second moments, we have that

$$\left\langle\left(N_{\mathcal{I}}(f,\psi)-\frac{2g}{p-1}|\mathcal{I}|\right)^2\right\rangle_{\mathcal{F}_d}\approx\left\langle\left(\sum_{1\le k\le K}\frac{c_K^{\pm}(k)S_k(f,\psi)+c_K^{\pm}(-k)S_k(f,\bar{\psi})}{q^{k/2}}\right)^2\right\rangle_{\mathcal{F}_d},$$

and we are led to consider averages of the type

$$\left\langle S_{k_1}(f,\psi)S_{k_2}(f,\bar{\psi})\right\rangle_{\mathcal{F}_d},$$

for fixed $1\le k_1,k_2\le K$. We first reverse the sum over $f\in\mathcal{F}_d$ and the sum over $\alpha_1,\alpha_2\in\mathbb{F}_{q^k}$.

Then, for each fixed $\alpha_1,\alpha_2\in\mathbb{F}_{q^{k_1}},\mathbb{F}_{q^{k_2}}$ of degree u_1,u_2, we have the sum

$$\sum_{\substack{f\in\mathcal{F}_d\\ f(\alpha_1)\neq\infty,f(\alpha_2)\neq\infty}}\psi\left(\mathrm{tr}_{k_1}\,f(\alpha_1)-\mathrm{tr}_{k_2}\,f(\alpha_2)\right)=\sum_{\beta_1\in\mathbb{F}_{q^{u_1}},\beta_2\in\mathbb{F}_{q^{u_1}}}\psi\left(\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta_2\right)\frac{\#\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1,\beta_2)}{\#\mathcal{F}_d}$$

where

$$\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1,\beta_2)=\{f\in\mathcal{F}_d\ :\ f(\alpha_1)=\beta_1\ \text{ and }\ f(\alpha_2)=\beta_2\}.$$

Again, by Theorem 36, for any $\beta_1,\beta_1'\in\mathbb{F}_{q^{u_1}},\beta_2,\beta_2'\in\mathbb{F}_{q^{u_2}}$, we have that

$$\#\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1,\beta_2)\sim\#\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1',\beta_2').$$

Then, we expect that

$$\sum_{\beta_1\in\mathbb{F}_{q^{u_1}},\beta_2\in\mathbb{F}_{q^{u_1}}}\psi\left(\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta_2\right)\frac{\#\mathcal{F}_d(\alpha_1,\alpha_2,\beta_1,\beta_2)}{\#\mathcal{F}_d}$$

will be 0, because when β_i runs over $\mathbb{F}_{q^{u_i}}$, $\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta$ takes every value in $\mathbb{F}_p$ the same number of times, and then $\psi\left(\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta_2\right)$ takes each pth root of 1 the same number of times. Unless $p\mid k_i$, and $\alpha_i\in\mathbb{F}_{q^{k_i/p}}$, or α_1 and α_2 are conjugate. In the first case, Then, $\beta_i=f(\alpha_i)\in\mathbb{F}_{q^{k_i/p}}$, and

$$\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta_2=p\,\mathrm{tr}_{k_1/p}\,\beta_1+p\,\mathrm{tr}_{k_2/p}\,\beta_2=0,$$

and $\psi\left(\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta_2\right)=e^0=1$. In the second case, β_1,β_2 are conjugate, $\mathrm{tr}_{k_1}\,\beta_1=\mathrm{tr}_{k_2}\,\beta_2\iff\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta_2=0$, and $\psi\left(\mathrm{tr}_{k_1}\,\beta_1-\mathrm{tr}_{k_2}\,\beta_2\right)$. We then have to count the contributions of the pairs (α_1,α_2) such that $p\mid(k_1,k_2)$, $\alpha_1\in\mathbb{F}_{q^{k_1}}$, $\alpha_2\in\mathbb{F}_{q^{k_2}}$ and α_1,α_2 conjugate of degree $m\mid(k_1,k_2)$. It turns out that the only contributions to the main term of the second moments are those coming from α_1,α_2 conjugate of degree

$k_1 = k_2$, and those can be counted by counting the number of irreducible polynomials of degree k in $\mathbb{F}_q[X]$. By Theorem 3.1 (the prime number theorem for polynomials), there are

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

such pairs, and the contribution from α_1, α_2 conjugate of degree $k_1 = k_2$ is

$$\sum_{k=1}^{K} \widehat{I}_K(k)^2 k \sim \frac{1}{2\pi^2} \log\left(K|\mathcal{I}|\right),$$

by properties of the Beurling-Selberg polynomials.

For the general moments, we had some combinatorics, and we have to count the number of ways to pick pairs of conjugate roots among n elements of $\overline{\mathbb{F}}_q$. We then get that the nth moment

$$\left\langle \left(N_{\mathcal{I}}(f,\psi) - \frac{2g}{p-1}|\mathcal{I}| \right)^n \right\rangle_{\mathcal{F}_d}$$

is asymptotic when $d \to \infty$ to

$$\begin{cases} \dfrac{(2\ell)!}{\ell!(2\pi^2)^\ell} \log^\ell(K|\mathcal{I}|) & n = 2\ell, \\ \\ C\dfrac{(2\ell+1)!}{\ell!(2\pi^2)^\ell} \log^\ell(K|\mathcal{I}|) & n = 2\ell+1, \end{cases},$$

and the (properly normalized) number of zeros with angles in a prescribed intervals has Gaussian distribution. Dealing appropriately with the error terms, we can show that this also holds when $|\mathcal{I}|$ tends to 0 as long as $g|\mathcal{I}| \to \infty$ when $g \to \infty$.

8. One-level density in the function field setting

For a general family of curves $\mathcal{F}(g,q)$, the traces of powers $\operatorname{tr}\Theta_C^n$ determine all linear statistics, such as the number of angles $\theta_j(C)$ lying in an interval $\mathcal{I} \subseteq [-\pi,\pi]$ as we studied in the preceding section, or the one-level density which is a smooth linear statistic. More suprinsingly, they also determine the n-level density, see for example [Hug05].

To define the one-level density in the function field setting, let f be an even test function on the Schwartz space $\mathcal{S}(\mathbb{R})$, and for any $N \geq 1$, we set

$$F(\theta) := \sum_{k\in\mathbb{Z}} f\left(N\left(\frac{\theta}{2\pi} - k\right)\right)$$

which is periodic with period 2π localized in an interval of size approximatively $1/N$ (we recall that the one-level density is the study of the low-lying zeros).

Exercise: The Fourier expansion of F is

$$F(\theta) = \frac{1}{N}\int_{-\infty}^{\infty} f(x)dx + \frac{1}{N}\sum_{n\neq 0} \hat{f}\left(\frac{n}{N}\right) e^{in\theta} \tag{38}$$

(using for example the Poisson summation formula).

For a unitary $N\times N$ matrix U with eigenvalues $e^{i\theta_j}$, $j=1,\dots,N$, we define

$$W_f(U) := \sum_{j=1}^{N} F(\theta_j).$$

Replacing (38) in the definition of W_f, we get

$$W_f(U) = \int_{-\infty}^{\infty} f(x)\, dx + \frac{1}{N}\sum_{n\neq 0} \hat{f}\left(\frac{n}{N}\right) \operatorname{tr} U^n, \tag{39}$$

so we have expressed the one-level density in terms of traces.

Now, suppose that $\mathcal{F}(g,q)$ be a family of curves of genus g with symmetry type $G(N)$, and as usual let

$$\langle W_f\rangle_{\mathcal{F}(g,q)} = \frac{1}{\#\mathcal{F}(g,q)} \sum_{C\in\mathcal{F}(g,q)} W_f(\theta_C).$$

Then, Katz and Sarnak conjectured that

$$\lim_{g\to\infty} \langle W_f\rangle_{\mathcal{F}(g,q)} = \lim_{g\to\infty} \int_{G(2g)} W_f(U)\, dU \tag{40}$$

as $g\to\infty$. Of course, taking the q-limit, it follows from the equidistribution theorem for the given family $\mathcal{F}(g,q)$ that

$$\lim_{q\to\infty} \langle W_f\rangle_{\mathcal{F}(g,q)} = \int_{G(2g)} W_f(U)\, dU. \tag{41}$$

Then, in view of (39), to prove (40), we have to compute the average

$$\langle \operatorname{tr}(\Theta_C^n)\rangle_{\mathcal{F}(g,q)}$$

and compare with

$$\int_{G(2g)} \operatorname{tr}(U^n)\, dU.$$

Then, using the results of Section 6.2, it follows that

Theorem 8.1. [Rud10, Corollay 3] *Let $\mathcal{H}_{2g+1}$ be the family of all hyperelliptic curves with affine equation $Y^2 = Q(X)$, where $Q(X)$ is square-free, monic of degree $2g+1$, and let*

$$\langle W_f\rangle := \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{Q\in\mathcal{H}_{2g+1}} W_f(\Theta_C).$$

If $f \in \mathcal{S}(\mathbb{R})$ is even, with Fourier transform $\hat{f}$ supported in $(-2,2)$, then

$$\langle W_f \rangle = \int_{USp(2g)} W_f(U) dU + \frac{dev(f)}{g} + \underline{o}\left(\frac{1}{g}\right),$$

where

$$dev(f) = \hat{f}(0) \sum_P \frac{\deg P}{|P|^2 - 1} - \hat{f}(1) \frac{1}{q-1}.$$

Proof. Using the Fourier expansion (39) and (33), we compute that

$$\int_{\mathrm{USp}(2g)} W_f(U)\, du = \int_{-\infty}^{\infty} f(x)\, dx - \frac{1}{g} \sum_{1 \le m \le g} \hat{f}\left(\frac{m}{g}\right).$$

Similarly, using the Fourier expansion (39) and Theorem 6.3, we get that

$$\langle W_f \rangle = \int_{-\infty}^{\infty} f(x)\, dx - \frac{1}{g} \sum_{1 \le m \le g} \hat{f}\left(\frac{m}{g}\right) - \frac{1}{q-1}\widehat{f}(1) - \widehat{f}(0) \sum_P \frac{\deg P}{|P|^2 - 1} + \underline{o}\left(\frac{1}{g}\right), \tag{42}$$

provided that the error term of Theorem 6.3 does not contribute: we need $n/2 - 2g < 0 \iff n < 4g$, which is guaranteed since $\widehat{f}\left(\frac{n}{2g}\right) = 0$ when $n/2g \geq 2$. □

Then, for functions f with limited support of the Fourier transform, one has that

$$\lim_{g \to \infty} \langle W_f \rangle_{\mathcal{H}_{2g+1}} = \lim_{g \to \infty} \int_{\mathrm{USp}(2g)} Z_f(U)\, dU = \int_{\mathbb{R}} f(x) \left(1 - \frac{\sin(2\pi x)}{2\pi x}\right) dx,$$

as conjectured by Katz and Sarnak for all functions f. The one-level density (42) for hyperelliptic curves for q fixed is analogous to the number field result, i.e. the one-level density for the non-trivial zeros of $L(s, \chi_d)$ where χ_d varies over the primitive Dirichlet characters as described in Section 2.1, except for the presence of the lower order term $-\hat{f}(1)/(q-1)$ coming from the extra contribution of the moment for $n = 2g$. One believes that this lower term will not appear in the number field setting, but this cannot be proven, as the lower order terms are known only for test functions f with Fourier transform such that $\mathrm{supp}(\hat{f}) \subseteq (-1, 1)$ in this case [Mil08].

For the n-level density, one needs to consider averages of product of traces, as is done in [ERGR13] (see next section). We also refer the reader to [Hug05]. The general expression relating the n-level density to products of traces involves some non-trivial combinatorics, but one can write closed formulas for (small) fixed n.

In order to define the n-level density in the function field setting, let f be a function of n variables in the Schwartz space $\mathcal{S}(\mathbb{R}^n)$. For $\vec{\theta} = (\theta_1, \ldots, \theta_n)$, let

$$\vec{F}(\vec{\theta}) = \sum_{k \in \mathbb{Z}^n} f\left(N\left(\frac{\vec{\theta}}{2\pi} - \vec{k}\right)\right) = \frac{1}{N^n} \sum_{\vec{m} \in \mathbb{Z}^n} \hat{f}(\frac{\vec{m}}{N}) e^{i\vec{m}\cdot\vec{\theta}}.$$

The n-level density of a unitary N by N matrix U with eigenvalues $e^{i\theta_j}$ is then defined as

$$W_f^{(n)}(U) = \sum_{\substack{j_1, \ldots, j_n \\ \text{distinct}}} F(\theta_{j_1}, \ldots, \theta_{j_n}),$$

and this can also be expressed in terms of powers of traces.

Taking for example $n = 2$, using the relation

$$\begin{aligned} \sum_{j \neq k} e^{i(m_1\theta_j + m_2\theta_k)} &= \left(\sum_j e^{im_1\theta_j}\right)\left(\sum_j e^{im_2\theta_k}\right) - \sum_j e^{i(m_1+m_2)\theta_j} \\ &= \operatorname{tr} U^{m_1} \operatorname{tr} U^{m_2} - \operatorname{tr} U^{m_1+m_2}, \end{aligned}$$

we obtain

$$W_f^{(2)}(U) = \frac{1}{N^2} \sum_{\vec{m}} \hat{f}\left(\frac{\vec{m}}{N}\right) \operatorname{tr} U^{m_1} \operatorname{tr} U^{m_2} - \frac{1}{N} \sum_m \frac{1}{N} \sum_{m'} \hat{f}\left(\frac{m', m-m'}{N}\right) \operatorname{tr} U^m. \tag{43}$$

In the case of hyperelliptic curves, the averages

$$\langle \operatorname{tr} U^{m_1} \operatorname{tr} U^{m_2} \rangle_{\mathcal{H}_{2g+1}}$$

are computed in [Rud10], and one can see that they fit the averages

$$\int_{\mathrm{USp}(2g)} \operatorname{tr} U^{m_1} \operatorname{tr} U^{m_2} \, dU,$$

for some range of m_1, m_2, and this can be used to give closed formulas for the two-level density. As for the case $n = 1$, the average of traces do not agree completely with the random matrix model for q small for exceptional values of m_1 and m_2 ($m_1 + m_2 = 2g$, $M_1 = 2g$ and $m_1 - m_2 = 2g$). See also [RG12].

9. n-level density over number fields and function fields

We survey in this section the recent work of Entin, Roditty-Gershon and Rudnick [ERGR13], where the authors show how the equidistribution theorem for hyperelliptic curves can be used to deduce statistics about the corresponding family over number fields, namely the family of quadratic Dirichlet L-functions. The number field situation was explained in Section 2.1, and to prove Theorem 2.6, it remains to show that for all n

$$A(f) = \int_{\mathbb{R}^n} f(x)\, W_{\mathrm{USp}}^{(n)}(x)\, dx,$$

where $A(f)$ is the expression computed by Gao [Gaoa, Gaob] for the family of quadratic Dirichlet L-functions.

Let $\mathcal{F}(2g+1,q)$ be the family of hyperelliptic curves

$$C_D \ : \ Y^2 = D(X),$$

where $D(X) \in \mathbb{F}_q[X]$ is a square-free polynomial with $\deg D = 2g+1$. Then, the zeta functions of the curves C_D correspond to the L-function of the Dirichlet characters χ_D, i.e.

$$Z_{C_D}(u) = \frac{P_{C_D}(u)}{(1-u)(1-qu)} = \frac{L(u,\chi_D)}{(1-u)(1-qu)},$$

where

$$L(u,\chi_D) = \prod_P \left(1-\chi_D(P)u^{\deg P}\right)^{-1},$$

and the product is over monic irreducible polynomials $P(X) \in \mathbb{F}_q[X]$. To define the n-level density for the family $\mathcal{F}(2g+1,q)$, let $f_1,\dots,f_n$ be even test functions on the Schwartz space $\mathcal{S}(\mathbb{R})$, and assume that the Fourier transforms $\hat{f}_j$ are supported in the interval $(-s_j,s_j)$ for $\sum_{j=1}^n |s_j| < 2$. For $C_D \in \mathcal{F}(2g+1,q)$, let $e^{i\theta_j(D)}$, $j = \pm 1,\dots,\pm g$ with $\theta_{-j}(D) = -\theta_j(D)$ be the zeros of $Z_{C_D}(u)$. Let

$$F_k(t) = \sum_{\ell\in\mathbb{Z}} f_k\left(2g\left(\frac{t}{2\pi}+\ell\right)\right)$$

be the associated test function with period 2π, and we denote

$$W^{(n)}(f_1,\dots,f_n;D) = \sum_{\substack{\theta_{j_1},\dots,\theta_{j_n}\\ 1\le|j_k|\le g, j_k\neq\pm j_\ell}} F_1(\theta_{j_1}(D))\dots F_n(\theta_{j_n}(D)).$$

Then, the n-level density over the family $\mathcal{F}(2g+1,q)$ is

$$\left\langle W^{(n)}(f_1,\dots,f_n;D)\right\rangle_{\mathcal{F}(2g+1,q)} := \frac{1}{\#CF(2g+1,q)} \sum_{C_D\in CF(2g+1,q)} W^{(n)}(f_1,\dots,f_n;D).$$

We know that

1. By Theorem 6.1, the statistics on the zeros of the L-functions $L(u,\chi_D)$ as C_D varies over all the hyperelliptic curves in the family $\mathcal{F}(2g+1,q)$ are given by the corresponding statistics on the matrix group $\mathrm{USp}(2g)$, and in particular taking the statistic to be the n-level density, we have

$$\lim_{q\to\infty}\left\langle W^{(n)}(f_1,\dots,f_n;D)\right\rangle_{\mathcal{F}(2g+1,q)} = \int_{\mathrm{USp}(2g)} f(x)\, W_f^{(n)}(U)\, dU. \tag{44}$$

2. If we further take the limit as $g\to\infty$ in (44), we get the scaling density $W_{\mathrm{USp}}^{(n)}$, i.e.

$$\lim_{g\to\infty}\left(\lim_{q\to\infty}\left\langle W^{(n)}(f_1,\dots,f_n;D)\right\rangle_{\mathcal{F}(2g+1,q)}\right) = \int_{\mathbb{R}^n} f(x) W_{\mathrm{USp}}^{(n)}(x)\, dx. \tag{45}$$

To be able to use (44) and (45) above, we first need to compute the n-level density on average over the family of hyperelliptic curves, for q any g finite.

Theorem 9.1. [ERGR13, Theorem 1.2] *Assume that $f(x_1,\dots,x_n)=\prod_{j=1}^n f(x_j)$ and that each $\widehat{f_j}(u_j)$ is supported on the range $|u_j|<s_j$ with $\sum_j s_j<2$. Then,*

$$\left\langle W^{(n)}(f_1,\dots,f_n;D)\right\rangle_{\mathcal{F}(2g+1,q)} = A(f)+O_f\left(\frac{g}{\log g}\right), \tag{46}$$

where the implied constant in independent of q and where $A(f)=A(f_1,\dots,f_n)$ is the combinatorial expression computed in [Gaoa, Gaob].

Then, taking the q-limit on both sides of (46), we get from (44)

$$A(f)+O_f\left(\frac{g}{\log g}\right)=\int_{\mathrm{USp}(2g)} f(x)\,W_f^{(n)}(U)\,dU$$

since the remainder term of (46) is independent of q. Now, by taking the g-limit on both sides, we get by (45) that

$$A(f)=\int_{\mathbb{R}^n} f(x)W_{\mathrm{USp}}^{(n)}(x)\,dx.$$

9.1. **n-level density for Artin-Scheier curves.** For Artin-Schreier curves, the n-level density follows from the work of Entin in [Ent13] where he studied the n-correlation for the p-rank 0 strata of Artin-Schreier curves (and both the n-level density and the n-correlation can be determined from the power of traces).

Let $\mathcal{F}(g,q)$ be a family of Artin-Schreier curves, for example a stratum of the moduli space (see Section 6.3) It was proven by Katz and Sarnak that at the q-limit, the statistics on $\mathcal{F}(g,q)$ will be given by the corresponding statistics on the space of unitary matrices $U(2g)$.

Theorem 9.2. [Kat05, Theorem 3.9.2] *Let g be fixed. Then, as $q\to\infty$, the matrices $\{\Theta_C\}_{C\in\mathcal{F}(g,q)}$ become equidistributed in $U(2g)$ with respect to the Haar measure.*

In particular, for g fixed, we have that

$$\lim_{q\to\infty}\langle \operatorname{tr}\Theta_C^n\rangle=\int_{U(2g)}\operatorname{tr}U^n\,dU=0,\quad n\in\mathbb{Z},n\neq 0. \tag{47}$$

More generally, we have the following result for the average product of powers of traces for eigenvalues of random matrices in $U(N)$.

Theorem 9.3. [DS94] *Let $r_1,\dots,r_n$ be non-zero integers $\sum_{i=1}^n|r_i|\le 2N$. Let $s_1,\dots,s_m$ be the distinct values appearing in the list $|r_i|$, $i=1,\dots,n$, and let a_j (respectively b_j) be the number of times each value s_j (respectively $-s_j$) occurs. Then,*

$$M(r_1,\dots,r_n;N) \;:=\; \int_{U(N)}\prod_{i=1}^n\operatorname{tr}U^{r_i}\,dU=\begin{cases}\prod_{j=1}^m a_j!s_j^{a_j}, & \text{if } a_j=b_j, j=1,\dots,m\\ 0 & \text{otherwise.}\end{cases}$$

This was originally proven by Diaconis and Shahshahani [DS94] using representation theory of unitary matrices. A new proof was given recently by [Ent13] by computing the averages $\prod_{i=1}^n\operatorname{tr}\Theta_C^{r_i}$ over the family of Artin-Schreier curves of p-rank 0, and using the equidistribution theorem of Katz and Sarnak to relate this to the average $M(r_1,\dots,r_n;N)$ over unitary matrices, i.e. using an approach similar to [ERGR13].

Let $\mathcal{F}_d$ be the family of polynomials of degree d, and assume that $(d,p)=1$. Fix a non-trivial additive character ψ of $\mathbb{F}_p$. Let $L(u,f,\psi)$ be the L-functions associated to an Artin-Shreier curve $C_f: Y^p-Y=f(X)$ for some $f\in\mathcal{F}_d$ and to the character ψ (as defined in Section 5.3). Let $e=(d-1)/(p-1)$, and let $\Theta_{f,\psi}$ be the e by e matrix with eigenvalues

$$q^{-1/2}\alpha_j(f,\psi)=e^{i\theta_j(f,\psi)},\quad j=1,\dots,e.$$

Theorem 9.4. [Ent13] *Let $r_1,\dots,r_k,t_1,\dots,t_\ell$ be natural numbers satisfying $\sum r_i=\sum t_j<d$. Let $s_1,\dots,s_m$ be the distinct values appearing in the list $r_1,\dots,r_k$, each appearing a_i times. Then,*

$$\left\langle\prod_{i=1}^k\operatorname{tr}\Theta_{f,\psi}^{r_i}\prod_{i=1}^\ell\operatorname{tr}\Theta_{f,\psi}^{t_j}\right\rangle_{\mathcal{F}_d}=\begin{cases}\prod_{j=1}^m a_j!\prod_{i=1}^k t_i+O\left(q^{-1/2}\right) & \text{if } k=\ell \text{ and the } r_i \text{ and the } t_i \text{ coincide}\\ O(q^{-1/2}) & \text{otherwise}\end{cases}$$

Then, using Katz and Sarnak equidistribution theorem, it follows from Theorem 9.4 that when $q \to \infty$

$$\left\langle \prod_{i=1}^{k} \left| \operatorname{tr} \Theta_{f,\psi}^{r_i} \right|^2 \right\rangle_{\mathcal{F}_d} \sim \int_{U(e)} \left| \operatorname{tr} U^{r_i} \right|^2 \, dU = M(r_1, \dots, r_k, -r_1, \dots, -r_k; e),$$

and the other cases (other choices of r_i) are treated similarly. Finally, deriving the n-correlation (or the n-level density) from the arbitrary moments of traces can be done with Fourier series as explained in Section 8.

References

[AP07] Jeffrey D. Achter and Rachel Pries. The integral monodromy of hyperelliptic and trielliptic curves. *Math. Ann.*, 338(1):187–206, 2007.

[BDF+12] Alina Bucur, Chantal David, Brooke Feigon, Matilde Lalín, and Kaneenika Sinha. Distribution of zeta zeroes of Artin-Schreier covers. *Mathematical Research Letters*, 19(6):1329–1356, 2012.

[BDFL] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Statistics for ordinary Artin-Schreier covers and other p-rank strata. *Transactions of the American Mathematical Society.* (to appear).

[BDFL10a] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Fluctuations in the number of points on smooth plane curves over finite fields. *J. Number Theory*, 130(11):2528–2541, 2010.

[BDFL10b] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Statistics for traces of cyclic trigonal curves over finite fields. *Int. Math. Res. Not. IMRN*, (5):932–967, 2010.

[BDFL11] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín. Biased statistics for traces of cyclic p-fold covers over finite fields. In *WIN—women in numbers*, volume 60 of *Fields Inst. Commun.*, pages 121–143. Amer. Math. Soc., Providence, RI, 2011.

[BG01] Bradley W. Brock and Andrew Granville. More points than expected on curves over finite field extensions. *Finite Fields Appl.*, 7(1):70–91, 2001. Dedicated to Professor Chao Ko on the occasion of his 90th birthday.

[Bir68] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[BK12] Alina Bucur and Kiran S. Kedlaya. The probability that a complete intersection is smooth. *J. Théor. Nombres Bordeaux*, 24(3):541–556, 2012.

[Bru92] Armand Brumer. The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992.

[CFZ08] Brian Conrey, David W. Farmer, and Martin R. Zirnbauer. Autocorrelation of ratios of L-functions. *Commun. Number Theory Phys.*, 2(3):593–636, 2008.

[CWZ] GilYoungl Cheong, Melanie Matchett Wood, and Azeem Zaman. The distribution of points on superelliptic curves over finite fields.

[Del71] Pierre Deligne. Formes modulaires et représentations l-adiques. In *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, volume 175 of *Lecture Notes in Math.*, pages Exp. No. 355, 139–172. Springer, Berlin, 1971.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[Del80] Pierre Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.

[DH69] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. *Bull. London Math. Soc.*, 1:345–348, 1969.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[DHP] Chantal David, Duc Khiem Huynh, and James Parks. One-level density of families of elliptic curves and the ratio conjectures. (preprint).

[DS94] Persi Diaconis and Mehrdad Shahshahani. On the eigenvalues of random matrices. *J. Appl. Probab.*, 31A:49–62, 1994. Studies in applied probability.

[DW86] Boris Datskovsky and David J. Wright. The adelic zeta function associated to the space of binary cubic forms. II. Local theory. *J. Reine Angew. Math.*, 367:27–75, 1986.

[DW88] Boris Datskovsky and David J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math.*, 386:116–138, 1988.

[Ent12] Alexei Entin. On the distribution of zeroes of Artin-Schreier L-functions. *Geom. Funct. Anal.*, 22(5):1322–1360, 2012.

[Ent13] Alexei Entin. Artin-Schreier L-functions and random unitary matrices. 2013. (preprint).

[ERGR13] Alexei Entin, Edva Roditty-Gershon, and Zeév Rudnick. Low-lying zeros of quadratic Dirichlet L-functions, hyperelliptic curves and random matrix theory. *Geom. Funct. Anal.*, 23(4):1230–1261, 2013.

[EW12] Daniel Erman and Melanie Matchett Wood. Semiample bertini theorems over finite fields. 2012. Available at arXiv:1209.5266.

[FR10] Dmitry Faifman and Zeév Rudnick. Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field. *Compos. Math.*, 146(1):81–101, 2010.

[Gaoa] P. Gao. n-level density on the low-lying zeroes of quadratic dirichlet l-functions. Ph. D. Thesis, University of Michigan, 2005.

[Gaob] P. Gao. n-level density on the low-lying zeroes of quadratic dirichlet l-functions. Available at arXiv:0806.4830.

[HB04] D. R. Heath-Brown. The average analytic rank of elliptic curves. *Duke Math. J.*, 122(3):591–623, 2004.

[Hug05] C. P. Hughes. Mock-Gaussian behaviour. In *Recent perspectives in random matrix theory and number theory*, volume 322 of *London Math. Soc. Lecture Note Ser.*, pages 337–355. Cambridge Univ. Press, Cambridge, 2005.

[ILS00] Henryk Iwaniec, Wenzhi Luo, and Peter Sarnak. Low lying zeros of families of L-functions. *Inst. Hautes Études Sci. Publ. Math.*, (91):55–131 (2001), 2000.

[Kat05] Nicholas M. Katz. *Moments, monodromy, and perversity: a Diophantine perspective*, volume 159 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2005.

[KR09] Pär Kurlberg and Zeév Rudnick. The fluctuations in the number of points on a hyperelliptic curve over a finite field. *J. Number Theory*, 129(3):580–587, 2009.

[KS99a] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.

[KS99b] Nicholas M. Katz and Peter Sarnak. Zeroes of zeta functions and symmetry. *Bull. Amer. Math. Soc. (N.S.)*, 36(1):1–26, 1999.

[LM] Jake Levinson and Steven J. Miller. The n-level densities of low-lying zeros of quadratic dirichlet l-functions. (preprint).

[Mes86] Jean-François Mestre. Formules explicites et minorations de conducteurs de variétés algébriques. *Compositio Math.*, 58(2):209–232, 1986.

[Mil04] Steven J. Miller. One- and two-level densities for rational families of elliptic curves: evidence for the underlying group symmetries. *Compos. Math.*, 140(4):952–992, 2004.

[Mil08] Steven J. Miller. A symplectic test of the L-functions ratios conjecture. *Int. Math. Res. Not. IMRN*, (3):Art. ID rnm146, 36, 2008.

[Mon73] H. L. Montgomery. The pair correlation of zeros of the zeta function. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 181–193. Amer. Math. Soc., Providence, R.I., 1973.

[Mon94] Hugh L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[Mor91] Carlos Moreno. *Algebraic curves over finite fields*, volume 97 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1991.

[ÖS93] Ali E. Özlük and C. Snyder. Small zeros of quadratic L-functions. *Bull. Austral. Math. Soc.*, 47(2):307–319, 1993.

[ÖS06] A. E. Özlük and C. Snyder. On the one-level density conjecture for quadratic Dirichlet L-functions. *Canad. J. Math.*, 58(4):843–858, 2006.

[Poo04] Bjorn Poonen. Bertini theorems over finite fields. *Ann. of Math. (2)*, 160(3):1099–1127, 2004.

[RG12] Edva Roditty-Gershon. Statistics for products of traces of high powers of the Frobenius class of hyperelliptic curves. *J. Number Theory*, 132(3):467–484, 2012.

[Riz03] Ottavio G. Rizzo. Average root numbers for a nonconstant family of elliptic curves. *Compositio Math.*, 136(1):1–23, 2003.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[RS96] Zeév Rudnick and Peter Sarnak. Zeros of principal L-functions and random matrix theory. *Duke Math. J.*, 81(2):269–322, 1996. A celebration of John F. Nash, Jr.

[Rub01] Michael Rubinstein. Low-lying zeros of L-functions and random matrix theory. *Duke Math. J.*, 109(1):147–181, 2001.

[Rud10] Zeév Rudnick. Traces of high powers of the Frobenius class in the hyperelliptic ensemble. *Acta Arith.*, 143(1):81–99, 2010.

[Sel65] Atle Selberg. On the estimation of Fourier coefficients of modular forms. In *Proc. Sympos. Pure Math., Vol. VIII*, pages 1–15. Amer. Math. Soc., Providence, R.I., 1965.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[TX14] Frank Thorne and Maosheng Xiong. Distribution of zeta zeroes for cyclic trigonal curves over a finite field. 2014. (preprint).

[Was87] Lawrence C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.*, 48(177):371–384, 1987.

[Woo12] Melanie Matchett Wood. The distribution of the number of points on trigonal curves over $\mathbb{F}_q$. *Int. Math. Res. Not. IMRN*, (23):5444–5456, 2012.

[Wri89] David J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58(1):17–50, 1989.

[Xio10a] Maosheng Xiong. The fluctuations in the number of points on a family of curves over a finite field. *J. Théor. Nombres Bordeaux*, 22(3):755–769, 2010.

[Xio10b] Maosheng Xiong. Statistics of the zeros of zeta functions in a family of curves over a finite field. *Int. Math. Res. Not. IMRN*, (18):3489–3518, 2010.

[You06] Matthew P. Young. Low-lying zeros of families of elliptic curves. *J. Amer. Math. Soc.*, 19(1):205–250, 2006.

[Zha] Yongqiang Zhao. *****. (preprint).