1 Intro

- In this talk I will discuss the main results of a paper of Faifman and Rudnick, "Statistics of the Zeros of Zeta Functions in Families of Hyperelliptic Curves over a Finite Field" – specifically, that in the limit of large genus g over a fixed finite field, a particular parameter associated to a randomly-chosen hyperelliptic curve of genus g will be uniformly distributed.
- In this talk, q will always be odd.
- To explain in more detail I first need some definitions.
- If C is a projective variety of genus g defined over $\mathbb{F}_q$, the zeta function of C is defined as $Z_C(u) = \exp(\sum_{n=1}^{\infty} N_n \cdot \frac{u^n}{n})$ for $|u| < 1/q$, where N_n is the number of points on C in the extension field $\mathbb{F}_{q^n}/\mathbb{F}_q$ of degree n.
- It is known that the zeta function for arbitrary projective curves has the form $Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)}$ for some polynomial $P_C(u) \in \mathbb{Z}[u]$ of degree $2g$, with $P(0) = 1$ and satisfying $P_C(u) = (qu^2)^g \cdot P_C(\frac{1}{qu})$. Furthermore, the Riemann hypothesis for curves states that all of the zeros of $P_C(u)$ lie on the circle $|u| = q^{-1/2}$. (Indeed all this is true more generally for arbitrary projective varieties – not just curves – by the Weil Conjectures.)
- Moreover, in the case of curves, there exists a unitary symplectic matrix $\Theta_C \in \mathrm{USp}(2g)$ defined up to conjugacy, with $P_C(u) = \det(I - u\sqrt{q} \cdot \Theta_C)$. Recall that the elements of $\mathrm{USp}(2g)$ are complex-valued, are $2g \times 2g$, unitary, and satisfy $\Theta_C^T \cdot \Omega \cdot \Theta_C = \Omega$ where $\Omega = \begin{bmatrix} 0 & -I_g \\ I_g & 0 \end{bmatrix}$ where I_g is the identity matrix. (Instead of Ω one can choose some other invertible skew-symmetric matrix which will then be conjugate to Ω.) Symplectic matrices have determinant 1 and have characteristic polynomials which are reciprocal; the given condition on $P_C(u)$ is essentially the statement that P_C is the characteristic polynomial of Θ_C, modified to account for the fact that $P_C(u)$ itself is not quite a reciprocal polynomial.
- The fact that Θ_C is actually unitary implies that its $2g$ eigenvalues all have absolute value 1 – write them as $e^{2i\pi\theta_{C,j}}$ for $j = 1, 2, \cdots, 2g$, for some "angles" $\theta_{C,j}$, $1 \le j \le 2g$.
- The goal of this talk is to study the distribution of these angles as we draw the curve C at random from the family of hyperelliptic curves of genus g defined over $\mathbb{F}_q$ for q odd. We denote this family as $H_{2g+2,q}$ and observe that it is the set of curves having an affine equation of the form $y^2 = Q(x)$ where $Q \in \mathbb{F}_q[x]$ is monic, squarefree, and of degree $2g+2$. (Its function field is $\mathbb{F}_q(x, \sqrt{Q(x)})$ and is called a real quadratic function field, in analogy to a real quadratic extension of a number field. For completeness, the analogue to an imaginary quadratic extension occurs when the degree of Q is odd and this can only occur under particular conditions.)
- The measure we will take on $H_{2g+2,q}$ is just the uniform probability measure, since the set is finite. The statistic we will analyze is the counting function of the angles: for an interval $I = [-\frac{\beta}{2}, \frac{\beta}{2}]$ which can vary with g and with q, let
$$N_I(C) = \#\{j : \theta_{j,C} \in I\}$$
(We may assume the interval I to be symmetric about 0 because of the functional equation for P_C.) The main theorem of this paper is that for fixed I, as $g \to \infty$ we have that
$$N_I(C) \sim 2g\,|I|$$
and moreover, it turns out that the variations in $N_I(C)$ are Gaussian, with variance $\frac{2}{\pi^2 \ln(\ln(2g\,|I|))}$.

- This is a similar sort of analysis to that of Selberg, who analyzed the behavior of the number of zeros $N(t)$ of the Riemann zeta function $\zeta(s)$ up to a given height t on the critical line $\mathrm{Re}(z) = \frac{1}{2}$. By the Riemann-von Mangoldt formula it was known that $N(t) = \frac{t}{2\pi} \cdot \ln(\frac{t}{2\pi e}) + O(\ln(t))$, and this was subsequently improved to $N(t) = \frac{t}{2\pi} \cdot \ln(\frac{t}{2\pi e}) + \frac{7}{8} + S(t) + O(\frac{1}{t})$ where $S(t) = \frac{1}{\pi} \arg(\zeta(\frac{1}{2} + it))$. Selberg analyzed the behavior of $S(t)$, for t chosen uniformly in $[0, T]$, and showed that its variance was $\frac{1}{2\pi^2} \ln(\ln(t))$ and that the moments of $\frac{S(t)}{\sqrt{\frac{1}{2\pi^2} \ln(\ln(t))}}$ were those of a standard Gaussian distribution.

- Katz and Sarnak showed that for fixed genus, the conjugacy classes of Θ_C become uniformly distributed in $\mathrm{USp}(2g)$ in the limit of $q \to \infty$, so in particular the statistics of N_I will be the same as those for the corresponding angle-counting function $\hat{N}_I$ for a randomly-chosen matrix of $\mathrm{USp}(2g)$. In the limit of large matrix size, the statistics of $\hat{N}_I$ (along with many other statistics) are known to have a Gaussian distribution; in particular, when averaged over $\mathrm{USp}(2g)$, the expected value of $\hat{N}_I$ is $2g\,|I|$, with variance $\frac{2}{\pi^2 \ln(\ln(2g\,|I|))}$, and such that the normalized value has a normal Gaussian distribution. In fact this result still holds even if the size of the interval shrinks, provided that the expected number of angles $2g\,|I|$ still goes to infinity. To summarize, Katz and Sarnak showed that

$$\lim_{g\to\infty} \left(\lim_{q\to\infty} \mathrm{Prob}_{H_{2g+2,j}} \left(a < \frac{N_I(C) - 2g\,|I|}{\sqrt{\frac{2}{\pi^2} \ln(\ln(2g\,|I|))}} < b \right) \right) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-x^2/2} dx.$$

- This paper shows the result still holds even if we fix the size of the field – i.e., if we remove the limit as $q \to \infty$ – which was central to Katz and Sarnak's proof.

- For the remainder of this talk I will focus on proving the statement that the angles are uniformly distributed, as the evaluation of the asymptotics on the higher moments uses essentially the same method albeit with more involved computations. We prove the result in two main steps: First, we show that the polynomial $P_C(u)$, the numerator of the zeta function for C, is the L-function for the quadratic character associated to $\mathbb{F}_q[x]$ and use this to derive an explicit formula for the sum of the values of an arbitrary trigonometric polynomial at the points $\theta_{C,j}$, $1 \le j \le 2g$. Second, we approximate our counting function $N_I(x)$ with Beurling-Selberg trigonometric polynomials, and then apply the explicit formula to deduce the results.

2 Dirichlet Characters on Function Fields

2.1 General Theory

- We first need some background on Dirichlet characters and L-functions on function fields. (If you are interested in learning more about this, you might want to read Rosen's book "Number Theory in Function Fields", which starts from elementary principles.)

- For $f \in \mathbb{F}_q[x]$ we define the norm of f as $||f|| = q^{\deg(f)}$. The zeta function of the rational function field is $\zeta_q(s) = \sum_{f \text{ monic}} ||f||^{-s}$ for $\mathrm{Re}(s) > 1$; its Euler product expansion is $\zeta_q(s) = \prod_{P \text{ monic irred}} (1 - ||P||^{-s})^{-1} = \prod_P (1 - u^{\deg(P)})^{-1}$ where the product is over irreducible monic polynomials P ("primes") in $\mathbb{F}_q[x]$; the second form is in terms of the variable $u = q^{-s}$. Directly from the sum we see that $Z(u) = \frac{1}{1 - qu}$.

- Given a monic polynomial $Q \in \mathbb{F}_q[x]$, we define a Dirichlet character modulo Q as a group homomorphism $\chi : (\mathbb{F}_q[x]/(Q))^\times \to \mathbb{C}^\times$. Such a character is primitive if it is not induced by any proper divisor of Q – i.e., if there is no $\tilde{Q}|Q$ and character $\tilde{\chi}$ mod $\tilde{Q}$ for which $\chi(n) = \tilde{\chi}(n)$ for all n with $\gcd(n, Q) = 1$.

- To a Dirichlet character mod Q we form the L-function

$$L(u,\chi) = \prod_P (1-\chi(P)\cdot u^{\deg(P)})^{-1} = \sum_f \chi(f)\cdot u^{\deg(f)}$$

which converges for $|u| < 1/q$, where P runs over all monic irreducibles and f runs over all monics. If χ is nontrivial then it is not hard to see that $\sum_{\deg(f)=n}\chi(f) = 0$ for $n \geq \deg(Q)$, and therefore the L-function is actually a polynomial, of degree at most $\deg(Q)-1$.

- We say a character is "even" if $\chi(c) = 1$ for all $c \in \mathbb{F}_q^\times$ (this is analogous to the condition $\chi(-1) = 1$ for ordinary Dirichlet characters). For even characters the L-function will have a trivial zero at $u = 1$ and so (for primitive characters of positive degree) we define the "completed" L-function

$$L^*(u,\chi) = (1-\lambda_\infty(\chi)u)^{-1}\cdot L(u,\chi)$$

where $\lambda_\infty(\chi)$ is 1 if $\chi$is even and 0 if χ is not. The completed L-function is a polynomial of degree $D = \deg(Q) - 1 - \lambda_\infty(x)$ and satisfies the functional equation $L^*(u,\chi) = \epsilon(\chi)\cdot(q^{1/2}u)^D \cdot L^*(\frac{1}{qu},\chi^{-1})$ where $\epsilon(\chi)$ is some complex number of absolute value 1.

- We can factor $L^*(u,\chi) = \prod_{j=1}^{D}(1-\alpha_{j,\chi}u)$ in terms of its inverse zeros $\alpha_{j,\chi}$; the Riemann hypothesis (proved by Weil) in this setting states that all $\alpha_{j,\chi}$ have absolute value $q^{1/2}$, so we can write $\alpha_{j,\chi} = q^{1/2}\cdot e^{2\pi i\theta_{j,\chi}}$ for some phases $\theta_{j,\chi} \in \mathbb{R}/\mathbb{Z}$.

2.2 Quadratic Dirichlet Characters

- Let $P(x) \in \mathbb{F}_q[x]$ be monic and irreducible, and $f \in \mathbb{F}_q[x]$ relatively prime to P. We define the quadratic residue symbol $\left(\frac{f}{P}\right) \in \{\pm 1\}$via

$$\left(\frac{f}{P}\right) \equiv f^{\frac{||P||-1}{2}} \bmod P$$

(Recall $||P|| = q^{\deg(P)}$.)

- We generalize to the Jacobi symbol in the usual way – namely, for arbitrary monic Q we define the Jacobi symbol $\left(\frac{f}{Q}\right)$ by writing $Q = \prod_i P_i$ as a product of monic irreducibles and setting $\left(\frac{f}{Q}\right) = \prod_i \left(\frac{f}{P_i}\right)$ if f and P are coprime, and 0 otherwise. If $f = c$ is a scalar (i.e., element of $\mathbb{F}_q^*$) then we set $\left(\frac{c}{Q}\right) = c^{\frac{q-1}{2}\deg(Q)}$.

- We recover quadratic reciprocity for these Jacobi symbols – if A, B are monic and relatively prime then $\left(\frac{A}{B}\right) = \left(\frac{B}{A}\right)\cdot(-1)^{\frac{q-1}{2}\deg(A)\cdot\deg(B)} = \left(\frac{B}{A}\right)\cdot(-1)^{\frac{||A||-1}{2}\cdot\frac{||B||-1}{2}}$. (If they are not relatively prime then it's still true as both sides are zero.)

- If $Q \in \mathbb{F}_q[x]$ is squarefree then we define the quadratic character $\chi_Q(f) = \left(\frac{Q}{f}\right)$. If $\deg(Q)$ is even then this character is primitive mod Q. Also observe that χ_Q is an even character (i.e., trivial on scalars) if and only if $\deg(Q)$ is even.

- The reason we need all of this background is because the polynomial $P_C(u)$ in the numerator of the zeta function of the hyperelliptic curve $y^2 = Q(x)$ is equal to the completed Dirichlet L-function $L^*(u,\chi_Q)$ associated with the quadratic character χ_Q.

3 The Explicit Formula

- Now we will return closer to our original problem. For the approximation theory later we will need to evaluate trigonometric polynomials at the points θ_{j,χ_Q}, the phases of the normalized inverse-zeros of the L-function of the character χ_Q, the quadratic character associated to Q. Conveniently, there is a general, explicit formula for evaluation at the phases $\theta_{j,\chi}$ for any character χ.

- Lemma 2.2: Let $h(\theta) = \sum_{|k|\leq K} \hat{h}(k) \cdot e(k\theta)$ be an arbitrary real-valued, even trigonometric polynomial – i.e., with $h(-\theta) = h(\theta) = \overline{h(\theta)}$. Then for any primitive character χ we have

$$\sum_{j=1}^{D} h(\theta_{j,\chi}) = D\cdot\int_0^1 h(\theta)d\theta + \lambda_\infty(\chi)\frac{1}{\pi i}\int_0^1 h(\theta)\frac{d}{d\theta}\left[\ln(1-\frac{e^{2i\pi\theta}}{\sqrt{q}}\right]d\theta - \sum_f \hat{h}(\deg(f))\cdot\frac{\Lambda(f)}{||f||^{1/2}}(\chi(f)+\overline{\chi(f)})$$

  where $\Lambda(f) = \deg(P)$ if $f = P^k$ is a prime power and is 0 otherwise.

  – Proof: By computing the logarithmic derivative $u\cdot\dfrac{L'}{L}$ in two different ways, one via the Euler product and the other by the product in terms of the inverse zeroes, we get an identity

$$-\sum_{j=1}^{D}\alpha_{j,\chi}^n = \sum_{\deg(f)=n}\Lambda(f)\chi(f) + \lambda_\infty(\chi)$$

  which we can write in terms of the phases as

$$-\sum_{j=1}^{D} e^{2\pi i n\theta_{j,\chi}} = \frac{\lambda_\infty(\chi)}{q^{|n|/2}} + \sum_{\deg(f)=|n|}\frac{\Lambda(f)}{||f||^{1/2}}\cdot\begin{cases}\overline{\chi(f)}, & n<0\\ \chi(f), & n>0\end{cases}$$

  Now if $h(\theta)$ is real and even then so are its Fourier coefficients so writing out the Fourier expansion and then applying the result above gives

$$\begin{aligned}\sum_{j=1}^{D} h(\theta_j) &= D\cdot\hat{h}(0) + \sum_j\sum_{k=1}^{K}\hat{h}(k)\cdot[e(k\theta_j)+e(-k\theta_j)]\\ &= D\int_0^1 h(\theta)d\theta - 2\lambda_\infty\sum_{k=1}^{K}\frac{\hat{h}(k)}{q^{k/2}} - \sum_f\hat{h}(\deg(f))\frac{\Lambda(f)}{||f||^{1/2}}(\chi(f)+\overline{\chi(f)})\end{aligned}$$

  and finally since h is real-valued we can rewrite the middle term as

$$\sum_{k=1}^{K}\frac{\hat{h}(k)}{q^{k/2}} = \int_0^1 h(\theta)\cdot\frac{q^{-1/2}e^{2\pi i\theta}}{1-q^{-1/2}e^{2\pi i\theta}} = \frac{1}{2\pi i}\int_0^1 h(\theta)\cdot\frac{d}{d\theta}\left[\ln(1-\frac{1}{1-e^{2\pi i\theta}q^{-1/2}})\right]d\theta$$

  which gives the result.

- In the particular case where $\chi = \chi_Q$ is the quadratic character corresponding to a squarefree polynomial Q of degree $2g+2$ we get $\lambda_\infty = 1$, $D = 2g$, and so the formula is

$$\sum_{j=1}^{2g} h(\theta_{j,Q}) = 2g\int_0^1 h(\theta)d\theta + \frac{1}{\pi i}\int_0^1 h(\theta)\cdot\frac{d}{d\theta}\left[\ln(1-\frac{e^{2i\pi\theta}}{\sqrt{q}}\right]d\theta - 2\sum_f\hat{h}(\deg(f))\cdot\frac{\Lambda(f)}{||f||^{1/2}}\chi_Q(f)$$

4 Beurling-Selberg Functions + Approximation

- Let $I = \left[-\frac{\beta}{2}, \frac{\beta}{2}\right]$ be an interval of length $0 < \beta < 1$, and let $K \geq 1$ be an integer. The Beurling-Selberg polynomials $I_K^{\pm}$ are trigonometric polynomials approximating the indicator function 1_I on the interval I with the following properties:
  - The $I_K^{\pm}$ have degree $\leq K$.
  - They satisfy $I_K^- \leq 1_I \leq I_K^+$.
  - The integral is close to the length of the interval: $\int_0^1 I_K^{\pm}(x)dx = \int_0^1 1_I dx \pm \frac{1}{K+1}$
  - The $I_K^{\pm}$ are even. (Follows because the interval is symmetric about 0.)
  - In particular, the nonzero Fourier coefficients satisfy $\left|\hat{I}_K^{\pm}(k) - \hat{1}_I(k)\right| \leq \frac{1}{K+1}$ and so in particular $\left|\hat{I}_K^{\pm}(k)\right| \leq \frac{1}{K+1} + \min(\beta, \frac{\pi}{|k|})$, for $0 < |k| \leq K$.

5 Counting Functions

- Now we will apply the results we have obtained about these Beurling-Selberg polynomials to our advantage by using the "explicit formula" expansion.
- So for χ_Q the quadratic Dirichlet character associated to the polynomial Q, recall that $N_I(\chi)$ denotes the number of angles θ_{j,χ_Q} of the L-function $L^*(u, \chi_Q)$ in the interval $I = \left[-\frac{\beta}{2}, \frac{\beta}{2}\right]$.
- Now define $N_K^{\pm}(\chi_Q) = \sum_{j=1}^{D} I_K^{\pm}(\theta_{j,\chi_Q})$, where here K is allowed to depend on $\deg(Q)$. This will be our smooth approximation to the counting function $N_I(\chi_Q)$.
- In particular we note that $N_K^-(\chi_Q) \leq N_I(\chi_Q) \leq N_K^+(\chi_Q)$.
- The idea is to show that we can pick a K that makes the two smooth counting functions behave asymptotically well, hence allowing us to show something about the discrete function $N_I(\chi_Q)$. To do this we will use the Beurling-Selberg polynomials to approximate the characteristic function on the interval I as inputs into the "explicit formula".
- Prop 5.1: For any fixed symmetric interval I, we have that $N_I(Q) = 2g\,|I| + O(\frac{g}{\ln(g)})$. In particular the angles θ_{j,χ_Q} become asymptotically uniformly-distributed.
  - Proof: Since $N_K^-(\chi_Q) \leq N_I(\chi_Q) \leq N_K^+(\chi_Q)$ it suffices to show that the two smooth counting functions satisfy $N_K^{\pm}(Q) = 2g\,|I| + O(\frac{g}{\ln(g)})$ for judicious K.
  - Using the explicit formula on the trigonometric polynomials $I_K^{\pm}(\theta)$ we obtain

$$N_K^{\pm}(\chi_Q) = D(\beta \pm \frac{1}{K+1}) + \frac{1}{\pi i}\int_0^1 I_K^{\pm}(\theta)\frac{d}{d\theta}\left[\ln(1 - \frac{e^{2\pi i\theta}}{\sqrt{q}})\right]d\theta + S_K^{\pm}(\chi)$$

  where $S_K^{\pm}(\chi_Q) = -2\sum_{\deg(f)\leq K} \hat{I}_K^{\pm}(\deg(f))\frac{\Lambda(f)}{||f||^{1/2}}\chi_Q(f)$, the sum taken over prime powers $f \in \mathbb{F}_q[x]$ of degree at most K.

– Now, because $\left|\hat{I}_K^{\pm}(k) - \hat{1}_I(k)\right| \leq \frac{1}{K+1}$ we can use this to approximate the middle term (the integral) and see that

$$\begin{aligned}\frac{1}{\pi i}\int_0^1 I_K^{\pm}(\theta)\frac{d}{d\theta}\left[\ln(1-\frac{e^{2\pi i\theta}}{\sqrt{q}}\right]d\theta &= \frac{1}{\pi i}\int_{-\beta/2}^{\beta/2}\frac{d}{d\theta}\left[\ln(1-\frac{e^{2\pi i\theta}}{\sqrt{q}})\right]d\theta + O(\frac{1}{K}) \\ &= \frac{2}{\pi}\arg(1-\frac{e^{2\pi i\theta}}{\sqrt{q}}) + O(\frac{1}{K})\end{aligned}$$

– We can also bound the $S_K^{\pm}(\chi_Q)$ term by observing that $\hat{I_K}^{\pm}(\deg(f))\cdot\Lambda(f) = O(1)$ since $\left|\hat{I}_K^{\pm}(k)\right| \leq \frac{1}{K+1} + \min(\beta, \frac{\pi}{|k|})$, for $0 < |k| \leq K$. Therefore we get $S_K^{\pm}(\chi_Q) = O(1)\cdot\sum_{\deg(f)\leq K}||f||^{-1/2} = O(q^{K/2})$.

– Combining all of the estimates yields $N_K^{\pm}(\chi_Q) = 2g\,|I| + O(\frac{g}{K}) + O(1) + O(q^{K/2})$. Finally, taking $K \approx \log_q(g/\ln(g))$ gives the desired asymptotic estimate.

6 Higher Moments (sketch)

- I will briefly sketch the results needed to establish that the higher moments of the counting function are Gaussian.
- Step 1: Define the auxiliary function $T_K^{\pm}(\chi_Q) = -2\sum_{P \text{ prime}}\frac{\hat{I}_K^{\pm}(\deg(P))\cdot\deg(P)}{||P||^{1/2}}\cdot\chi_Q(P)$, which approximates the terms $S_K^{\pm}(\chi_Q) = -2\sum_{\deg(f)\leq K}\hat{I}_K^{\pm}(\deg(f))\frac{\Lambda(f)}{||f||^{1/2}}\chi_Q(f)$. (The difference being that T is a sum over all primes, while S is only a sum over primes of bounded degree.)
- Step 2: Show that $\left\langle\left|T_K^{\pm}\right|^2\right\rangle \sim \frac{2}{\pi^2}\ln(\beta g)$, and that $\left\langle\left|T_K^{+} - T_K^{-}\right|^2\right\rangle = \left\langle\left|S_K^{+} - T_K^{+}\right|^2\right\rangle = \left\langle\left|S_K^{-} - T_K^{-}\right|^2\right\rangle = O(1)$ provided that $K \approx g/\ln(\ln(g\beta))$ with $g \to \infty$ and $\beta g \to \infty$. The proofs of these statements are mostly an application of some straightforward bounds along with some diagonal/off-diagonal counting arguments.
- Step 3: Show that the higher moments of $T_K^{\pm}$ are Gaussian: specifically, that $\left|\left\langle(T_K^{\pm})^{2r-1}\right\rangle\right| = o(1)$ and that $\left|\left\langle(T_K^{\pm})^{2r}\right\rangle\right| = \frac{(2r)!}{r!\cdot\pi^{2r}}\ln^r(\beta K) + O(\ln^{r-1}(\beta K))$. (The proofs here again involve similar diagonal/off-diagonal analysis.) Conclude that $T_K^{\pm}/\sqrt{\frac{2}{\pi^2}\ln(g\beta)}$ has a standard Gaussian limiting distribution.
- Step 4: Show that $\left\langle\left|\frac{S_I - T_K^{\pm}}{\sqrt{\frac{2}{\pi^2}\log(g\beta)}}\right|^2\right\rangle \to 0$ as $g \to \infty$ and $g\beta \to \infty$ with $K \approx g/\ln(\ln(g\beta))$, where $S_I = N_I - 2g\,|I| - \frac{2}{\pi}\arg(1-\frac{e^{i\pi|I|}}{\sqrt{q}})$. Apply step 2, the triangle inequality, and the fact that $S_K^{\pm}$ closely approximates S_I – this follows from what we did much earlier – to see that $S_I/\sqrt{\frac{2}{\pi^2}\log(\beta g)}$ has a standard Gaussian distribution as claimed. (Finally note that the arg term is irrelevant.)

7 Other Stuff I Cut Out For Being Irrelevant

- Lemma 2.1: If χ is a nontrivial Dirichlet character modulo f, then for $n < \deg(f)$,

$$\left| \sum_{\deg(B)=n} \chi(B) \right| \leq \binom{\deg(f)-1}{n} \cdot q^{n/2}$$

[Note that for $n \geq \deg(f)$ the character sum vanishes.]

  - Proof: Compare coefficients of the series expansion of the L-function $L(u,\chi)$ to the coefficients of the expansion of the product in terms of its inverse zeroes to see that

$$\sum_{\deg(B)=n} \chi(B) \quad = \quad (-1)^n \cdot \sum_{\substack{S \subset \{1,\cdots,\deg(f)-1\} \\ \#(S)=n}} \prod_{j \in S} \alpha_j = \sigma_n(\alpha_1, \cdots, \alpha_{\deg(f)-1})$$

and then observe that each of the $\binom{\deg(f)-1}{n}$ terms in the sum on the RHS is bounded by $(\sqrt{q})^n$.

- Lemma 3.1: If $f \in \mathbb{F}_q[x]$ is not a square then $\langle \chi_Q(f) \rangle \leq \dfrac{2^{\deg(f)-1}}{(1-q^{-1})q^{g+1}}$.

  - Proof: We use the Mobius function to kill the non-squarefree polynomials, so we can write

$$\begin{aligned}
\left| \sum_{Q \in H_{2g+2,q}} \chi_Q(f) \right| &= \left| \sum_{\deg(Q)=2g+2} \sum_{A^2|Q} \mu(A) \cdot \left(\frac{Q}{f}\right) \right| \\
&= \left| \sum_{\deg(A) \leq g+1} \mu(A) \cdot \left(\frac{A}{f}\right)^2 \cdot \sum_{\deg(B)=2g+2-2\deg(A)} \left(\frac{B}{f}\right) \right| \\
&\leq \sum_{g+q-\frac{\deg(f)}{2} \leq \deg(A) \leq g+1} \left| \binom{\deg(f)-1}{2g+2-2\deg(A)} q^{g+1-\deg(A)} \right| \\
&\leq q^{g+1} \cdot 2^{\deg(f)-1}
\end{aligned}$$

where we applied the triangle inequality and the bound (2.1) on the sum over the nontrivial character $\left(\dfrac{B}{f}\right)$ in the third step along with noting that the inner sum was zero of the degree of B was larger than the degree of f, and summed the binomial coefficients in the last step. Dividing by $\#(H_{2g+2,q}) = q^{2g+2}(1-q^{-1})$ gives the result.

- The previous lemma gives a bound for when f is not a square; we now need the case when f is a square.

- Lemma 3.2: If $P_1, \cdots, P_k$ are prime polynomials, then $\left\langle \chi_Q(\prod_j P_j^2) \right\rangle = 1 + O\left(\sum_j ||P_j||^{-1}\right)$.

  - Proof: Clearly we have $\chi_Q(\prod_j P_j^2) = 1$ except when one of the P_j divides Q, in which case it is 0. So we need to count how many squarefree Q of degree $2g+2$ are divisible by at least one P_j. Clearly this will be bounded by the number of arbitrary monic Q of degree $2g+2$ divisible by at least one P_j, and this is clearly at most $\sum_j \dfrac{q^{2g+2}}{||P_j||}$. Since $H_{2g+2,q} = q^{2g+2}(1-q^{-1})$ we see that $1 - (1-q^{-1})^{-1} \cdot \left(\sum_j ||P_j||^{-1}\right) \leq \left\langle \chi_q(\prod_j P_j^2) \right\rangle \leq 1$ whence the result.

- For a polynomial $Q \in \mathbb{F}_q[x]$ of positive degree, define $\eta(Q) = \sum_{P|Q} ||P||^{-1}$, where the sum is over primes P dividing Q.

- Lemma 3.3: The mean values of η and η^2 are uniformly bounded – explicitly, they satisfy $\langle \eta \rangle \leq (1-q^{-1})^{-2}$ and $\langle \eta^2 \rangle \leq (1-q^{-1})^{-3} + (1-q^{-1})^{-1}(1-q^{-2})^{-1}$.

  - Proof: For the sum of $\eta(Q)$ we need equivalently count, for each prime P, how many Q are divisible by P – this gives

$$\begin{aligned}
\sum \eta(Q) &= \sum_{Q \in H_{2g+2,q}} \sum_{P|Q} ||P||^{-1} \\
&= \sum_{\deg(P) \leq 2g+2} ||P||^{-1} \cdot \#(Q \in H_{2g+2,q} : P|Q) \\
&\leq \sum_{\deg(P) \leq 2g+2} ||P||^{-1} \cdot \frac{q^{2g+2}}{||P||} \\
&\leq q^{2g+2} \cdot \sum_{k=0}^{\infty} q^{-k} \\
&= q^{2g+2}(1-q^{-1})^{-1}
\end{aligned}$$

    and hence the average value is bounded by $(1-q^{-1})^{-2}$.
    [Remark: There was an error in the paper here; it incorrectly gave the bound obtained this way as 1.]

    For the second moment, expand out the square in $\sum_Q \left(\sum_{P|Q} ||P||^{-1} \right)^2$ as $\sum_Q \sum_{P_1} \sum_{P_2} ||P_1||^{-1} \cdot ||P_2||^{-1}$ and split into diagonal and off-diagonal terms. For the off-diagonal, observe that if P_1 and P_2 both divide Q then if Q is squarefree then Q is divisible by $P_1 P_2$. Then we are reduced to a count essentially the same as before: $\sum n^2(Q) \leq \sum_{P_1} \sum_{P_2} \frac{q^{2g+2}}{||P_1||^2 ||P_2||^2} \leq q^{2g+2}(1-q^{-1})^{-2}$.

    For the diagonal, we have $\sum_Q \sum_{P|Q} ||P||^{-2} \leq \sum_{\deg(P) \leq 2g+2} ||P||^{-2} \cdot \frac{q^{2g+2}}{||P||} \leq q^{2g+2}(1-q^{-2})^{-1}$ and therefore after combining the two we get the bound $\langle \eta^2 \rangle \leq (1-q^{-1})^{-3} + (1+q^{-1})^{-1}(1-q^2)^{-1}$.
    [Remark: There was another error here; the authors mistakenly omitted the diagonal terms.]

- Prop 4.1: Let $K \geq 1$ be an integer for which $K\beta > 1$. Then

$$\begin{aligned}
\sum_{n \geq 1} \hat{I}_K^{\pm}(2n) &= O(1) \\
\sum_{n \geq 1} n \hat{I}_K^{\pm}(2n)^2 &= \frac{1}{2\pi^2} \ln(K\beta) + O(1)
\end{aligned}$$

  where the implied constants are independent of K and β.

  - Proof: By the inequality on the Fourier coefficients we have $\hat{I}_K^{\pm}(2n) = \frac{\sin(2\pi n\beta)}{2\pi n} + O(\frac{1}{K})$. Now it is a simple matter to sum over n; for $n < 1/\beta$ one can use $\sin(2\pi n\beta) < 2\pi n\beta$ to obtain a bound of 2π on that piece of the sum. For $1/\beta < n < K$ one can use summation by parts; each partial sum $\sum \sin(2\pi n\beta)$ is $O(\frac{1}{\beta})$, so

$$\sum_{1/\beta < n < K/2} \frac{\sin(2\pi n\beta)}{2\pi n} << \frac{1}{\beta K} + 1 + \frac{1}{\beta} \int_{1/\beta}^{K} \frac{1}{t^2} dt = O(1)$$

    yielding the first result.

– For the second part, use again the inequality on the Fourier coefficients to write

$$\sum_{n\geq 1} n\hat{I}_K^{\pm}(n)^2 = \frac{1}{\pi^2}\sum_{n\leq K}\frac{\sin(\pi n\beta)^2}{n} + O(1)$$

and again split the sum into the two parts $[1, 1/\beta]$ and $[1/\beta, K]$. The first interval is easy with $\sin(\pi n\beta) \leq \pi n\beta$ again, giving $O(1)$, while on the second interval we can use $\sin^2(y) = \frac{1}{2}(1 - \cos(2y))$ and summation by parts once again. The cosine portion of the sum gives a bounded contribution, while the constant piece is trivial to evaluate as giving $\frac{1}{2\pi^2}\cdot\ln(K\beta) + O(1)$, hence result again.

8 Now What?

- The general form of the argument could fairly easily be generalized to broader families of curves, if there were a similar connection to be made through Dirichlet L-functions on function fields. The fact that χ_Q was quadratic was not particularly central to the proof. I believe this is the topic of Thursday's lecture.