Statistics for traces of cyclic trigonal curves over finite fields

Matilde N. Lalín

University of Alberta
mlalin@math.ualberta.ca
http://www.math.ualberta.ca/~mlalin

joint with A. Bucur, C. David, B. Feigon

2009 CMS Winter meeting – Number Theory special session

December 6, 2009

Zeta functions of curves over finite fields

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

$$Z_C(T) = \exp\left(\sum_{n=1}^{\infty} N_n(C)\frac{T^n}{n}\right), \quad |T| < 1/q,$$

$$N_n(C) = |C(\mathbb{F}_{q^n})|.$$

Weil conjectures

$$Z_C(T) = \frac{P_C(T)}{(1-T)(1-qT)} \qquad \textbf{(Rationality)}$$

$$P_C(T) \in \mathbb{Z}[T], \quad \deg P_C = 2g,$$

and

$$P_C(T) = \prod_{j=1}^{2g}(1 - T\alpha_{j,C}), \quad |\alpha_{j,C}| = \sqrt{q}. \qquad \textbf{(Riemann Hypothesis)}$$

Counting points and the zeroes of $Z_C(T)$

$$Z_C(T) = \exp\left(\sum_{n=1}^{\infty} N_n(C)\frac{T^n}{n}\right) = \frac{\prod_{j=1}^{2g}(1 - T\alpha_{j,C})}{(1-T)(1-qT)},$$

Taking logarithms on both sides,

$$\begin{aligned} N_1(C) &= q + 1 - \sum_{j=1}^{2g} \alpha_{j,C} \\ &= q + 1 - \mathrm{Tr}(\mathrm{Frob}_C). \end{aligned}$$

Distribution of $\mathrm{Tr}(\mathrm{Frob}_C)$ for $q \to \infty$

Writing $\alpha_{j,C} = \sqrt{q}\, e^{2\pi i \theta_{j,C}}$,

$$P_C(T) = \prod_{i=1}^{2g} (1 - T\sqrt{q}\, e^{2\pi i \theta_{j,C}}) = \det\left(I - T\sqrt{q}\Theta_c\right)$$

where Θ_C is a unitary symplectic matrix in $\mathrm{USp}(2g)$ (defined up to conjugation) with eigenvalues $e^{2\pi i \theta_{j,C}}$.

When g is fixed and $q \to \infty$, Katz and Sarnak showed that the roots $\theta_{j,C}$ are distributed as the eigenvalues of matrices in $\mathrm{USp}(2g)$.

Then, $\mathrm{Tr}(\mathrm{Frob}_C)/\sqrt{q}$ is distributed as the trace of a random matrix in $\mathrm{USp}(2g)$ of $2g \times 2g$ as $q \to \infty$.

Hyperelliptic curves

$$C_F : Y^2 = F(X)$$

$F(X)$ is a square-free polynomial of degree $d \geq 3$.

This is a curve of genus $g = \left[\frac{d-1}{2}\right]$.

We want to study the variation of

$$\mathrm{Tr}(\mathrm{Frob}_{C_F}) = \sum_{i=1}^{2g} \alpha_{j,C_F}$$

as C_F varies over the family of hyperelliptic curves where $F(X)$ has degree $2g+1$ or $2g+2$.

Hyperelliptic Curves

By counting the number of points of $Y^2 = F(X)$ over $\mathbb{P}^1(\mathbb{F}_q)$, we can write

$$N_1(C_F) = q + 1 - \mathrm{Tr}(\mathrm{Frob}_{C_F}) \quad = \quad \sum_{x \in \mathbb{F}_q} [1 + \chi_2(F(x))] + N_\infty(C_F)$$

where χ_2 is the quadratic character of $\mathbb{F}_q^*$, and

$$N_\infty(C_F) = \begin{cases} 1 & \deg F \text{ odd,} \\ 2 & \deg F \text{ even, leading coeff of } F \in \mathbb{F}_q^2, \\ 0 & \deg F \text{ even, leading coeff of } F \notin \mathbb{F}_q^2. \end{cases}$$

is the number of points at infinity.

Hyperelliptic Curves

$$-\operatorname{Tr}(\operatorname{Frob}_{C_F}) = \sum_{x\in\mathbb{F}_q} \chi_2(F(x)) + (N_\infty(C_F) - 1) = \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_2(F(x)).$$

One can study the variation of

$$S_2(F) = \sum_{x\in\mathbb{F}_q} \chi_2(F(x))$$

over the family of hyperelliptic curves and translate it into a variation for $\operatorname{Tr}(\operatorname{Frob}_{C_F})$.

This amounts to evaluate the probability that a random square-free polynomial $F(x)$ of degree d takes a prescribed set of values $F(x_1) = a_1, \dots, F(x_{q+1}) = a_{q+1}$ for the distinct elements of $\mathbb{P}^1(\mathbb{F}_q)$.

Distribution of $\mathrm{Tr}(\mathrm{Frob}_{C_F})$ for $g \to \infty$

When q is fixed and $g \to \infty$, Kurlberg and Rudnick showed that $S_2(F)$ is distributed as a sum of q independent identically distributed (i.i.d.) trinomial variables $\{X_i\}_{i=1}^q$ taking values $0, \pm 1$ with probabilities $1/(q+1)$, $1/2(1+q^{-1})$ and $1/2(1+q^{-1})$ respectively.

Theorem (Kurlberg and Rudnick)

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

$$\begin{aligned}\lim_{d\to\infty} \mathrm{Prob}\left(S_2(F)=s\right) &= \lim_{d\to\infty} \frac{|\{F \in \mathcal{F}_d \;:\; S_2(F)=s\}|}{|\mathcal{F}_d|} \\ &= \mathrm{Prob}\left(X_1+\cdots+X_q=s\right).\end{aligned}$$

Distribution of $\mathrm{Tr}(\mathrm{Frob}_{C_F})$ for $g \to \infty$

This result may be formulated directly in terms of the genus g.

Theorem

The distribution of the trace of the Frobenius endomorphism associated to C as C ranges over the moduli space $\mathcal{H}_g$ of hyperelliptic curves of genus g defined over $\mathbb{F}_q$, with q fixed and $g \to \infty$, is that of the sum of $X_1, \dots, X_{q+1}$:

$$\frac{|\{C \in \mathcal{H}_g : \mathrm{Tr}(\mathrm{Frob}_C) = -s\}|'}{|\mathcal{H}_g|'} = \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = s\right)\left(1 + O\left(q^{(3q-2-2g)/2}\right)\right)$$

By comparing moments of the previous distributions,

Theorem (Kurlberg and Rudnick)

When q, g tend to infinity, the limiting distribution of the normalized trace

$$\mathrm{Tr}(\mathrm{Frob}_C)/\sqrt{q+1}$$

is a standard Gaussian with mean zero and variance one.

Cyclic Trigonal Curves

Let $q \equiv 1 \pmod 3$. Consider the family of curves

$$C_F \ : \ Y^3 = F(X)$$

where $F(X) \in \mathbb{F}_q[X]$ is cube-free of degree d.

We write

$$F(X) = aF_1(X)F_2^2(X)$$

where F_1 and F_2 are monic square-free polynomials of degree d_1 and d_2 respectively, $(F_1, F_2) = 1$.

Then, $d = d_1 + 2d_2$, and the genus is

$$g = \begin{cases} d_1 + d_2 - 2 & \text{if } d = d_1 + 2d_2 \equiv 0 \pmod 3, \\ d_1 + d_2 - 1 & \text{if } d = d_1 + 2d_2 \not\equiv 0 \pmod 3. \end{cases}$$

Moduli Space of Cyclic Trigonal Curves

The moduli space $\mathcal{H}_{g,3}$ of cyclic trigonal curves of genus g parametrizes the cyclic trigonal curves of genus g up to isomorphism.

It splits into irreducible components $\mathcal{H}^{(d_1,d_2)}$ for pairs (d_1, d_2) such that

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

The union is disjoint.

Cyclic Trigonal Curves

By counting the number of points of $C_F : Y^3 = F(X)$ over $\mathbb{P}^1(\mathbb{F}_q)$, we can write

$$\begin{aligned} & q + 1 - \mathrm{Tr}(\mathrm{Frob}_C |_{H^1_{\chi_3}}) - \mathrm{Tr}(\mathrm{Frob}_C |_{H^1_{\overline{\chi_3}}}) \\ = & \sum_{x \in \mathbb{F}_q} [1 + \chi_3(F(x)) + \overline{\chi_3(F(x))}] + N_\infty(C_F) \end{aligned}$$

χ_3 is the cubic character of $\mathbb{F}_q^*$ given by

$$\chi_3(x) \equiv x^{(q-1)/3} \pmod q$$

taking values in $\{1, \omega, \omega^2\}$ where ω is a third root of unity, and

$$N_\infty(C_F) = \begin{cases} 1 & \deg F \not\equiv 0 \pmod 3, \\ 0 & \deg F \equiv 0 \pmod 3 \quad \text{lead coeff } F \notin \mathbb{F}_q^3, \\ 1 & \deg F \equiv 0 \pmod 3 \quad \text{lead coeff } F \in \mathbb{F}_q^3 \quad q \equiv -1 \pmod 3, \\ 3 & \deg F \equiv 0 \pmod 3 \quad \text{lead coeff } F \in \mathbb{F}_q^3 \quad q \equiv 1 \pmod 3. \end{cases}$$

Cyclic Trigonal Curves

Then we study the variation of

$$-\operatorname{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_3}}) \;=\; \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_3(F(x)),$$

where F runs over a family of irreducible components of the moduli space of cyclic trigonal curves of genus g with the property that $g \to \infty$.

Trace on cyclic trigonal curves

Theorem (BDFL)

If q is fixed and $d_1, d_2 \to \infty$, the distribution of the trace of the Frobenius endomorphism associated to C as C ranges over $\mathcal{H}^{(d_1,d_2)}$ is that of the sum of $q+1$ i.i.d. random variables $X_1, \ldots, X_{q+1}$, where each X_i takes the value 0 with probability $2/(q+2)$ and $1, \omega, \omega^2$ each with probability $q/(3(q+2))$. More precisely, for any $s \in \mathbb{Z}[\omega] \subset \mathbb{C}$ with $|s| \leq q+1$, we have for any $1 > \varepsilon > 0$,

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,d_2)} : \mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_3}}) = -s\right\}\right|'}{\left|\mathcal{H}^{(d_1,d_2)}\right|'} = \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = s\right) \times \left(1 + O\left(q^{-(1-\varepsilon)d_2+q} + q^{-(d_1-3q)/2}\right)\right).$$

When $q, d_1, d_2 \to \infty$

Theorem (BDFL)

For any positive integers j and k, let $M_{j,k}(q,(d_1,d_2))$ be the moments

$$\frac{1}{\left|\mathcal{H}^{(d_1,d_2)}\right|'} \sideset{}{'}\sum_{C\in\mathcal{H}^{(d_1,d_2)}} \left(\frac{-\operatorname{Tr}(\operatorname{Frob}_C|_{H^1_{\chi_3}})}{\sqrt{q+1}}\right)^j \left(\frac{-\operatorname{Tr}(\operatorname{Frob}_C|_{H^1_{\overline{\chi}_3}})}{\sqrt{q+1}}\right)^k.$$

Let ε and $X_1,\dots,X_{q+1}$ be as before. Then

$$M_{j,k}(q,(d_1,d_2)) = \mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1}X_i\right)^j\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q+1}\overline{X_i}\right)^k\right) \times\left(1+O\left(q^{-(1-\varepsilon)d_2+\varepsilon(j+k)}+q^{-d_1/2+j+k}\right)\right).$$

When $q, d_1, d_2 \to \infty$

Corollary (BDFL)

When q, d_1, d_2 tend to infinity, the limiting distribution of the normalized trace

$$\mathrm{Tr}(\mathrm{Frob}_C |_{H^1_{\chi_3}})/\sqrt{q+1}$$

is a complex Gaussian with mean zero and variance one.

Main step in the proof

$$\mathcal{F}_{(d_1,d_2)} = \{F = F_1F_2^2 : F_1, F_2 \text{ monic, square-free and coprime,} \\ \deg F_1 = d_1, \deg F_2 = d_2\}$$

Proposition

Let $0 \le \ell \le q$, let $x_1, \ldots, x_\ell$ be distinct elements of $\mathbb{F}_q$, and $a_1, \ldots, a_\ell \in \mathbb{F}_q^*$. Then for any $1 > \varepsilon > 0$, we have

$$\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} : F(x_i) = a_i, 1 \le i \le \ell\right\}\right| = \frac{Kq^{d_1+d_2}}{\zeta_q(2)^2}\left(\frac{q}{(q+2)(q-1)}\right)^\ell \\ \times \left(1 + O\left(q^{-(1-\varepsilon)d_2+\varepsilon\ell} + q^{-d_1/2+\ell}\right)\right)$$

$$K = \prod_{P \text{ monic irreducible}} \left(1 - \frac{1}{(|P|+1)^2}\right).$$

We prove

$$\left|\left\{F \in \mathcal{F}_{(d_1,d_2)} \ : \ F(x_i) = a_i, \ 1 \leq i \leq \ell\right\}\right| = \frac{q^{d_1-\ell}}{\zeta_q(2)(1-q^{-2})^{\ell}} \sum_{\deg F = d_2} b(F) + O\left(q^{d_2+d_1/2}\right),$$

where for any polynomial F,

$$b(F) = \begin{cases} \mu^2(F)\prod_{P|F}(1+|P|^{-1})^{-1} & F(x_i) \neq 0, 1 \leq i \leq \ell. \\ 0 & \text{otherwise.} \end{cases}$$

To evaluate $\sum_{\deg F=d_2} b(F)$, we consider the Dirichlet series

$$G(s)=\sum_F \frac{b(F)}{|F|^s}=\prod_{\substack{P\\ P(x_i)\neq 0, 1\leq i\leq \ell}}\left(1+\frac{1}{|P|^s}\cdot\frac{|P|}{|P|+1}\right)$$

$$=\frac{\zeta_q(s)}{\zeta_q(2s)}H(s)\left(1+\frac{1}{q^{s-1}(q+1)}\right)^{-\ell},$$

where

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

and apply a function field version of the Wiener-Ikehara Tauberian Theorem, we get that

$$\sum_{\deg F=d_2} b(F)=\frac{K}{\zeta_q(2)}\left(\frac{q+1}{q+2}\right)^{\ell}q^{d_2}+O(q^{\varepsilon(d_2+\ell)}).$$

General result for p-fold covers of $\mathbb{P}^1(\mathbb{F}_q)$.

$$Y^p = F(X)$$

Theorem (BDFL)

Let $X_1, \dots, X_{q+1}$ be complex i.i.d. random variables taking the value 0 with probability $(p-1)/(q+p-1)$ and each of the p-th roots of unity in $\mathbb{C}$ with probability $q/(p(q+p-1))$. As $d_1, \dots, d_{p-1} \to \infty$,

$$\frac{\left|\left\{C \in \mathcal{H}^{(d_1,\dots,d_{p-1})} : \mathrm{Tr}(\mathrm{Frob}_C\,|_{H^1_{\chi_p}}) = -s\right\}\right|'}{\left|\mathcal{H}^{(d_1,\dots,d_{p-1})}\right|'} = \mathrm{Prob}\left(\sum_{i=1}^{q+1} X_i = s\right)$$

$$\times\left(1 + O\left(q^{\varepsilon(d_2+\cdots+d_{p-1})+q}\left(q^{-d_2}+\cdots+q^{-d_{p-1}}\right)+q^{-(d_1-3q)/2}\right)\right)$$

for any $s \in \mathbb{C}$, $|s| \le q+1$ and $0 > \varepsilon > 1$.

Theorem (BDFL)

As $q, d_1, \dots, d_{p-1} \to \infty$,

$$\mathrm{Tr}(\mathrm{Frob}_C \,|_{H^1_{\chi_p}})/\sqrt{q+1}$$

has a complex Gaussian distribution with mean 0 *and variance* 1 *as* C *varies in* $\mathcal{H}^{(d_1,\dots,d_{p-1})}(\mathbb{F}_q)$.