So you think you can count?

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, A. Cojocaru, C. David, B. Feigon

February 19 , 2009

Diophantine equations and zeta functions

$$2x^2 - 1 = 0 \qquad x \in \mathbb{Z}$$

No solutions!!!
($2x^2$ is always even and 1 is odd.)

We are looking at "odd" and "even" numbers instead of integers (reduction modulo $p = 2$).

Local solutions = solutions modulo p, and in $\mathbb{R}$.

Global solutions = solutions in $\mathbb{Z}$

global solutions $\Rightarrow$ local solutions

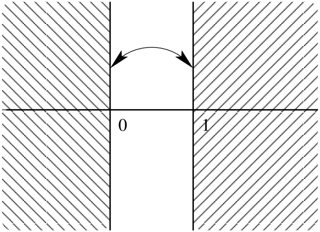
local solutions $\not\Rightarrow$ global solutions

The Riemann Zeta function

Local info $\rightsquigarrow$ zeta functions

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

Analytic continuation to $\mathbb{C}$, simple pole at $s = 1$.



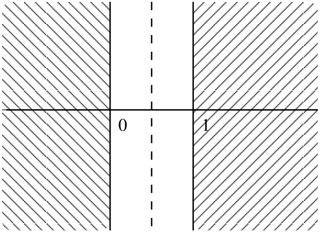
$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s)$$

The Riemann Zeta function

Trivial zeros: $-2, -4, -6, \ldots$

Nontrivial zeros: $\rho = \beta + i\gamma$, $0 < \beta < 1$.

Riemann Hypothesis: Nontrivial zeros are on the line $\mathrm{Re}(s) = \frac{1}{2}$.



$\zeta(s)$ and Random Matrix Theory

Hilbert and Pólya's question:

$\frac{1}{2} + i\gamma$ zero of $\zeta(s)$,

Does $\gamma \in$ set of eigenvalues of a Hermitian operator?

If yes, γ is real $\Rightarrow$ Riemann Hypothesis!!!

Riemann-Von Mangoldt formula:

$$\begin{aligned} N(T) &= \#\{\rho=\beta+i\gamma\ :\ \beta\in(0,1), \quad 0<\gamma\le T\} \\ &= \frac{T}{2\pi}\log\frac{T}{2\pi e}+O(\log T) \end{aligned}$$

Average gap between zeroes at height T is $2\pi/\log T$.

Montgomery's Pair Correlation conjecture, 1974

$$\frac{|\{(\gamma,\gamma')\in[0,T]\ :\ \frac{2\pi\alpha}{\log T}<\gamma-\gamma'<\frac{2\pi\beta}{\log T}\}|}{N(T)}\sim\int_\alpha^\beta 1-\left(\frac{\sin\pi u}{\pi u}\right)^2du$$

The pair correlation of eigenvalues of large random Hermitian matrices with a Gaussian measure is also $1-\left(\frac{sin\pi u}{\pi u}\right)^2$.

$\zeta(s)$ and Random Matrix Theory

New philosophy to study the Riemann zeta function:

$$\begin{aligned} \text{zeroes of } \zeta(s) &\quad\leftrightarrow\quad \text{eigenvalues of random matrices} \\ \zeta(s) &\quad\leftrightarrow\quad \text{characteristic polynomial of random matrices} \end{aligned}$$

The relation between $\zeta(s)$ and RMT is purely conjectural.

Zeta functions of curves and Random Matrix theory

Zeta functions of curves over finite fields, the zeros are the reciprocal of eigenvalues of Frobenius acting on the first cohomology (with ℓ-adic coefficients) of the curve.

Katz and Sarnak (1999) used this spectral interpretation to prove that the zeros of zeta functions of curves in various families were distributed as eigenvalues of random matrices in the monodromy group associated to the family as q tends to ∞.

Riemann Zeta function over $\mathbb{F}_q(X)$

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
$\lvert n\rvert = n$	$\leftrightarrow$	$\lvert F(X)\rvert = q^{\deg F}$

$$\zeta_I(s,\mathbb{F}_q(X)) = \sum_{\substack{F\,\in\,\mathbb{F}_q[X]\\ F\ \text{monic}}} \frac{1}{|F|^s} = \prod_P \left(1-\frac{1}{|P|^s}\right)^{-1}$$

Riemann Zeta function over $\mathbb{F}_q(X)$

$$\zeta_I(s,\mathbb{F}_q(X)) = \sum_{\substack{F\,\in\,\mathbb{F}_q[X]\\ F\ \text{monic}}} \frac{1}{|F|^s} = \prod_P \left(1-\frac{1}{|P|^s}\right)^{-1}$$

Since there are q^d monic polynomials of degree d,

$$\zeta_I(s,\mathbb{F}_q(X)) = \sum_{d\geq 0} \frac{q^d}{q^{ds}} = (1-q^{1-s})^{-1}.$$

The Riemann Hypothesis is then trivially true since $\zeta_I(s,\mathbb{F}_q(X))$ has no zeros!

Zeta functions over general function fields

Let K be a function field over $\mathbb{F}_q$.

We will consider two cases

$$\begin{aligned} K &= \mathbb{F}_q(X)\left(\sqrt{D}\right), \quad D \in \mathbb{F}_q[X] \\ K &= \mathbb{F}_q(X)\left(\sqrt[3]{D}\right), \quad D \in \mathbb{F}_q[X],\ q \equiv 1 \mod 3. \end{aligned}$$

Then,

$$\zeta(s,K) = \prod_{\mathfrak{P}} \left(1 - \frac{1}{|\mathfrak{P}|^s}\right)^{-1} = \zeta_I(s,K)\zeta_\infty(s,K).$$

Zeta functions over general function fields

When one considers all primes (finite and infinite),

$$\zeta(s, \mathbb{F}_q(X)) = (1 - q^{1-s})^{-1}(1 - q^{-s})^{-1}.$$

We now consider $\zeta(s, K)$ as the zeta function of a curve over the finite field $\mathbb{F}_q$.

Zeta functions of functions fields		Zeta functions of curves over finite fields
$K = \mathbb{F}_q(X)(\sqrt{D})$	$\leftrightarrow$	$C : Y^2 = D(X)$
$K = \mathbb{F}_q(X)(\sqrt[3]{D})$	$\leftrightarrow$	$C : Y^3 = D(X)$

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

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

Rationality and Riemann Hypothesis

Let K be the function field of the curve C. Then,

$$\zeta(s,K)=Z_C(q^{-s})=\frac{P_C(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

Taking $C=\mathbb{P}^1$, we have

$$Z_{\mathbb{P}^1}(T)=\frac{1}{(1-T)(1-qT)} \text{ and } Z_{\mathbb{P}^1}(q^{-s})=\zeta(s,\mathbb{F}_q(X)).$$

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

$$q^{-s}=\alpha_{j,C}^{-1} \iff s=\log_q \alpha_{j,C},$$

and the real part of the zeroes of $\zeta(s,K)$ is $1/2$.

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,

$$N_1(C) = q + 1 - \sum_{j=1}^{2g} \alpha_{j,C} = q + 1 - S(F).$$

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 the trace

$$S(F) = \sum_{i=1}^{2g} \alpha_{j,C}$$

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

Distribution of $S(F)$ 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 θ_{j,C_F} are distributed as the eigenvalues of matrices in $\mathrm{USp}(2g)$.

Then, $S(F)/\sqrt{q}$ is distributed as the trace of a random matrix in $\mathrm{USp}(2g)$ of $2g \times 2g$.

Distribution of $S(F)$ 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,

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

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 $X_1, \dots, X_{q+1}$:

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

Overview of the proof

Let

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

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

$$q + 1 - S(F) \ = \ \sum_{x \in \mathbb{F}_q} [1 + \chi_2(F(x))] + N_\infty(C_F)$$

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

$$N_\infty(C_F) = \begin{cases} 1 & \deg F \text{ odd}, \\ 2 & \deg F \text{ even, leading coeff of } F \in \mathbb{F}_q^2, \\ 0 & \deg F \text{ even, leading coeff of } F \not\in \mathbb{F}_q^2. \end{cases}$$

Overview of the proof

Then,

$$-S(F) = \sum_{x\in\mathbb{F}_q} \chi_2(F(x)) + (N_\infty(C_F) - 1) = \sum_{x\in\mathbb{P}^1(\mathbb{F}_q)} \chi_2(F(x)),$$

and one studies the variation of

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

over the family of hyperelliptic curves.

This amounts to evaluate the probability that a random monic square-free polynomial $F(x)$ of degree d takes a prescribed set of values $F(x_1) = a_1, \dots, F(x_m) = a_m$ for $x_1, \dots, x_m$ distinct elements of $\mathbb{F}_q$.

Cyclic Trigonal Curves

Let $q \equiv 1 \mod 3$. 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

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

Moduli Space

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

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

Several ways to take $g \to \infty$.

Trace on 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

$$q + 1 - S(F) \quad = \quad \sum_{x \in \mathbb{F}_q} [1 + \chi_3(F(x)) + \overline{\chi_3(F(x))}] + N_\infty(C_F)$$

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

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

taking values in $\left\{1, \rho, \rho^2\right\}$ where ρ is a third root of unity, and

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

Trace on cyclic trigonal curves

Then we study the variation of

$$-S(F) \;=\; \sum_{x\in\mathbb{F}_q} \chi_3(F(x)) + \overline{\chi_3(F(x))} + (N_\infty(C_F) - 1)\,,$$

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

Let

$$\mathcal{F}_{(d_1,d_2)} = \left\{ F = F_1F_2^2 \;:\; F_1 \in \mathcal{F}_{d_1}, F_2 \in \mathcal{F}_{d_2}, (F_1,F_2)=1 \right\}$$
$$\widehat{\mathcal{F}}_{(d_1,d_2)} = \left\{ F = aF_1F_2^2 \;:\; F_1 \in \mathcal{F}_{d_1}, F_2 \in \mathcal{F}_{d_2}, (F_1,F_2)=1 \right\}$$

Then

$$|\widehat{\mathcal{F}}_{(d_1,d_2)}| = (q-1)^2|\mathcal{F}_{(d_1,d_2)}|.$$

The component $\mathcal{H}^{(d,0)}$

Theorem

When C_F ranges over $\mathcal{H}^{(d,0)}$ and $d \to \infty$, the trace

$$-S(F) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_3(F(x)) + \overline{\chi_3(F(x))}$$

is distributed as the sum of $2q+2$ random variables

$$X_1 + X_2 + \cdots + X_{q+1} + \overline{X_1} + \cdots + \overline{X_{q+1}}$$

where the X_i are independent identically distributed random variables taking value 0 with probability $1/(q+1)$, and any of the value $1, \rho, \rho^2$, with probability $1/3(1+q^{-1})$.

The component $\mathcal{H}^{(d,0)}$

Let $x_1, \dots, x_{\ell+m}$ be distinct points of $\mathbb{F}_q$, $a_1, \dots, a_\ell \in \mathbb{F}_q^*$ and $a_{\ell+1}, \dots, a_{\ell+m} = 0$. For q fixed and $d \to \infty$,

$$|\{F \in \mathcal{F}_{(d,0)} : F(x_i) = a_i \ : \ 1 \leq i \leq m + \ell\}| \sim \frac{(1-q^{-1})^m q^{d-\ell-m}}{\zeta_q(2)(1-q^{-2})^{m+\ell}}.$$

We can now evaluate

$$\frac{\left|\left\{F \in \widehat{\mathcal{F}}_{(d,0)} \cup \widehat{\mathcal{F}}_{(d-1,0)} \ : \ \chi_3(F(x_i)) = \varepsilon_i \ : \ 1 \leq i \leq q+1\right\}\right|}{|\widehat{\mathcal{F}}_{(d,0)}| + |\widehat{\mathcal{F}}_{(d-1,0)}|}$$

where $\varepsilon_i \in \left\{0, 1, \rho, \rho^2\right\}$ for $1 \leq i \leq q+1$ with m ε_i's of value 0.
If $\varepsilon_i = 0$, then $F(x_i)$ must be 0.
If $\varepsilon_i = 1$, then $F(x_i)$ must be one of the $(q-1)/3$ non-zero cubes in $\mathbb{F}_q$, and similarly for $\varepsilon_i = \rho, \rho^2$.

The component $\mathcal{H}^{(d,0)}$

This gives

$$\frac{|\{C \in \mathcal{H}^{(d,0)} : \mathrm{Tr}(\mathrm{Frob}_C) = -s\}|}{|\mathcal{H}^{(d,0)}|} \sim \frac{3^{m-1-q} q^{-m}}{(1+q^{-1})^{q+1}}$$

Moreover, let X_i with $i = 1, \dots, q+1$ be i.i.d. random variables taking the value 0 with probability $1/q+1$, and taking the values $1, \rho, \rho^2$ with probability $1/3(1+q^{-1})$. Then

$$\mathrm{Prob}(X_i = \varepsilon_i \ : \ 1 \leq i \leq q+1) = \frac{3^{m-1-q} q^{-m}}{(1+q^{-1})^{q+1}}.$$

The component $\mathcal{H}^{(d,1)}$

Theorem

When C_F ranges over $\mathcal{H}^{(d,1)}$ and $d \to \infty$, the trace

$$-S(F) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_3(F(x)) + \overline{\chi_3(F(x))}$$

is distributed as the sum of $2q+2$ random variables

$$X_1 + X_2 + \cdots + X_{q+1} + \overline{X_1} + \cdots + \overline{X_{q+1}}$$

where the X_i are independent identically distributed random variables taking value 0 with probability $1/(q+1)$, and any of the value $1, \rho, \rho^2$, with probability $1/3(1+q^{-1})$ together with a linear bias towards the number of zero values for $X_1, \dots, X_{q+1}$.

The component $\mathcal{H}^{(d,1)}$

We have an analogous result

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

and

$$\frac{\left|\left\{F \in \widehat{\mathcal{F}}_{(d,1)} \cup \widehat{\mathcal{F}}_{(d-1,1)} \cup \widehat{\mathcal{F}}_{(d,0)} : \chi_3(F(x_i)) = \varepsilon_i \, 1 \leq i \leq q+1\right\}\right|}{|\widehat{\mathcal{F}}_{(d,1)}| + |\widehat{\mathcal{F}}_{(d-1,1)}| + |\widehat{\mathcal{F}}_{(d,0)}|} \\ = \frac{|\{C \in \mathcal{H}^{(d,1)} : \mathrm{Tr}(\mathrm{Frob}_C) = -s\}|}{|\mathcal{H}^{(d,1)}|} \sim \frac{3^{m-1-q}q^{-m}m}{(1+q^{-1})^{q+1}}.$$

In particular, if $m = 0$, the probability that $\chi_3(F(x_i)) = \varepsilon_i$ for $1 \leq i \leq q+1$ is 0 as $F = aF_1(x-\alpha)^2$ always has a 0 over $\mathbb{F}_q$.

The component $\mathcal{H}^{(d,1)}$

Let X be a random variable taking the values $1, \rho, \rho^2$, with probability $1/3(1+q^{-1})$ and 0 with probability $1/(q+1)$.
Let $X_1, \dots, X_{q+1}$ be random variables distributed as X with a linear bias towards m, the number of zero values. Then

$$\mathrm{Prob}\left(X_i = \varepsilon_i \;:\; 1 \leq i \leq q+1\right) = \frac{m}{S}\left(\frac{1}{q+1}\right)^m \left(\frac{q}{3(q+1)}\right)^{q+1-m}$$

where

$$S = \sum_{(\varepsilon_1,\dots,\varepsilon_{q+1})\in\{0,1,\rho,\rho^2\}^{q+1}} m\left(\frac{1}{q+1}\right)^m \left(\frac{q}{3(q+1)}\right)^{q+1-m} = 1.$$

The component $\mathcal{H}^{(d_1,d_2)}$

$$\widehat{\mathcal{F}}_{(d_1,d_2)} = \bigcup \widehat{\mathcal{F}}^k_{(d_1,d_2)}$$

where for $k \in \mathbb{Z}$ with $0 \leq k \leq d_2$, we define

$$\widehat{\mathcal{F}}^k_{(d_1,d_2)} = \left\{ aF_1F_2^2 \in \mathcal{F}_{(d_1,d_2)} \ : \ F_2 \text{ has } k \text{ roots in } \mathbb{F}_q \right\}.$$

Theorem

$$\frac{\left| \left\{ F \in \widehat{\mathcal{F}}^0_{(d,2)} \cup \widehat{\mathcal{F}}^0_{(d-1,2)} \ : \ \chi_3(F(x_i)) = \varepsilon_i \ 1 \leq i \leq q+1 \right\} \right|}{\left| \widehat{\mathcal{F}}^0_{(d,2)} \right| + \left| \widehat{\mathcal{F}}^0_{(d-1,2)} \right|} \sim \frac{3^{m-1-q} q^{-m}}{(1+q^{-1})^{q+1}}.$$

This is as before the probability for the $q+1$ i.i.d. random variables $X_1, \ldots, X_{q+1}$.

The component $\mathcal{H}^{(d,2)}$

$$\frac{\left|\left\{F \in \widehat{\mathcal{F}}^2_{(d,2)} \cup \widehat{\mathcal{F}}^2_{(d-1,2)} \cup \widehat{\mathcal{F}}^1_{(d,1)} \ : \ \chi_3(F(x_i)) = \varepsilon_i\right\}\right|}{\left|\widehat{\mathcal{F}}^2_{(d,2)}\right| + \left|\widehat{\mathcal{F}}^2_{(d,1)}\right| + \left|\widehat{\mathcal{F}}^1_{(d,1)}\right|} \sim \frac{3^{m-1-q}q^{-m}m(m-1)}{(1+q^{-1})^q}$$

This is

$$\mathrm{Prob}\left(X_i = \varepsilon_i \ : \ 1 \leq i \leq q+1\right)$$

for the $q+1$ i.i.d. random variables $X_1, \dots, X_{q+1}$ with a quadratic bias towards the number of pairs (i,j) with $i \neq j$ and $\varepsilon_i = \varepsilon_j = 0$.

Mixed Probabilities

Then,

$$\frac{\left|\left\{F \in \widehat{\mathcal{F}}_{(d,2)} \cup \widehat{\mathcal{F}}_{(d-1,2)} \cup \widehat{\mathcal{F}}_{(d,1)} \ : \ \chi_3(F(x_i)) = \varepsilon_i\right\}\right|}{\left|\widehat{\mathcal{F}}_{(d,2)}\right| + \left|\widehat{\mathcal{F}}_{(d,1)}\right| + \left|\widehat{\mathcal{F}}_{(d,1)}\right|}$$

$$= \frac{|\{C \in \mathcal{H}^{(d,2)} : \mathrm{Tr}(\mathrm{Frob}_C) = -s\}|}{|\mathcal{H}^{(d,2)}|}$$

is given by a mixed probability involving the cases with $k = 2$ and $k = 0$.

The general case follows similarly.

Theorem

Let $d_2 \geq 0$, and $0 \leq k \leq d_2$. Then, as $d_1 \to \infty$,

$$\frac{\left|\left\{F \in \widehat{\mathcal{F}}^k_{(d_1,d_2)} \cup \widehat{\mathcal{F}}^{k-1}_{(d_1-1,d_2)} \cup \widehat{\mathcal{F}}^k_{(d_1,d_2-1)} \ : \ \chi_3(F(x_i)) = \varepsilon_i\right\}\right|}{\left|\widehat{\mathcal{F}}^k_{(d_1,d_2)}\right| + \left|\widehat{\mathcal{F}}^k_{(d_1-1,d_2)}\right| + \left|\widehat{\mathcal{F}}^{k-1}_{(d_1,d_2-1)}\right|}$$

$$\sim \frac{3^{m-1-q} q^{k-m} \binom{m}{k}}{\binom{q+1}{k}(1+q^{-1})^{q+1-k}}.$$