Point count statistics for families of curves over finite fields

Pär Kurlberg

Department of Matematics
Royal Institute of Technology (KTH)
Stockholm, Sweden
kurlberg@math.kth.se

Exponential Sums over Finite Fields and Applications
ETH Zürich
Nov 1, 2010

Points on curves over finite fields

Notation:

- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: finite field with p elements, p prime.
- Want to consider **families** of smooth curves $\{C_f\}_f$ defined over $\mathbb{F}_p$. Example:
  - Hyperelliptic curves: $f \in \mathbb{F}_p[X]$ ranges over monic polynomials with distinct roots, say of degree $2g+1$.

$$C_f = \{x, y \in \overline{\mathbb{F}_p} : y^2 = f(x)\} \cup \{\text{point at } \infty\}$$

- Will study the set of $\mathbb{F}_p$-points on the curves, e.g.,

$$C_f(\mathbb{F}_p) := \{x, y \in \mathbb{F}_p : y^2 = f(x)\} \cup \{\text{point at } \infty\}$$

Riemann hypothesis for curves

Basic questions:

- How large/small is $|C_f(\mathbb{F}_p)|$?
- How does $|C_f(\mathbb{F}_p)|$ vary when we vary f?

Theorem (A. Weil — "RH for curves")

Let C be a smooth curve, defined over $\mathbb{F}_p$ and of genus g. Then

$$\big||C(\mathbb{F}_p)| - (p+1)\big| \leq 2g\sqrt{p}$$

- Thus: for g fixed, $p \to \infty$, $|C(\mathbb{F}_p)| \sim p$.
- BUT: what about fluctuations around $p+1$? In particular, what if p fixed and $g \to \infty$?

Fluctations when $g = 1$ (elliptic curves)

- When $g = 1$, hyperelliptics become family of *elliptic curves*. With $C_f = \{x, y : y^2 = f(x)\}$ and

$$\mathcal{F}_p := \{f(X) \in \mathbb{F}_p[X] : \ f \text{ monic, } \deg(f) = 3,\ (f, f') = 1\}$$

  wish to consider the family $\{C_f\}_{f \in \mathcal{F}_p}$.
- By the Hasse/Weil bounds, $\big||C_f(\mathbb{F}_p)| - (p+1)\big| \leq 2\sqrt{p}$, write **fluctuations** as:

$$a_{p,f} := p + 1 - |C_f(\mathbb{F}_p)|$$

- How does $a_{p,f}$ vary when we vary f? Normalize to get rid of p-dependency: consider $a_{p,f}/\sqrt{p} \in [-2, 2]$.

Fluctuations via Haar measure on compact Lie groups

- Fact ("vertical Sato-Tate distribution"): as $p \to \infty$,

$$\frac{|\{f \in \mathcal{F}_p : a_{p,f}/\sqrt{p} \in [t_1, t_2]\}|}{|\mathcal{F}_p|} \simeq \frac{1}{2\pi} \int_{t_1}^{t_2} \sqrt{4 - x^2}\, dx$$

- Where does semicircle come from? "Miracle":

$$\mu_{\text{Haar}}(\{g \in SU_2(\mathbb{C}) : \text{Trace}(g) \in [t_1, t_2]\}) = \frac{1}{2\pi} \int_{t_1}^{t_2} \sqrt{4 - x^2}\, dx$$

- Why $SU_2(\mathbb{C})$? Can write

$$a_{p,f}/\sqrt{p} = \text{Trace}(U_{p,f})$$

  where $U_{p,f} \in SU_2(\mathbb{C})$.
- Distribution of normalized fluctuations "comes from" distribution of $\text{Trace}(U_{p,f})$.
- By Deligne's equidistribution theorem, $\{U_{p,f}\}_{f \in \mathcal{F}}$ become equidistributed[1] in $SU_2(\mathbb{C})$ when $p \to \infty$.

[1] Really should phrase this in terms of conjugacy classes in $SU_2(\mathbb{C})$.

Generalized Sato-Tate distribution

What about families of hyperelliptic curves? Let

$$\mathcal{F}_p := \{f(X) \in \mathbb{F}_p[X] : \ f \text{ monic}, \deg(f) = 2g+1, (f, f') = 1\}$$

For $f \in \mathcal{F}_p$, let $C_f = \{y^2 = f(x)\}$, and let $a_{p,f} = p + 1 - |C_f(\mathbb{F}_p)|$.
Let

$$USp(2g) := U(2g) \cap Sp(2g).$$

Turns out that $a_{p,f}/\sqrt{p} = \text{Trace}(U_{p,f})$ where $U_{p,f} \in USp(2g)$.

Theorem (Katz-Sarnak)

As $p \to \infty$, $\{U_{p,f}\}_{f \in \mathcal{F}}$ becomes equidistributed in $USp(2g)$. In particular,

$$\frac{|\{f \in \mathcal{F}_p : a_{p,f}/\sqrt{p} \in [t_1, t_2]\}|}{|\mathcal{F}_p|} \simeq \mu_{Haar}(\{h \in USp(2g) : \text{Trace}(h) \in [t_1, t_2]\})$$

Large genus limit

What is distribution of $\{\text{Trace}(h)\}_{h \in USp_{2g}(\mathbb{C})}$ when $g \to \infty$?

Theorem (Diaconis-Shahshahani)

As $g \to \infty$, the distribution of $\{\text{Trace}(h)\}_{h \in USp_{2g}(\mathbb{C})}$ becomes **Gaussian**. *I.e., given an compact interval $I \subset \mathbb{R}$,*

$$\lim_{g \to \infty} \mu_{Haar}(\{h \in USp(2g) : \text{Trace}(h) \in I\}) = \frac{1}{\sqrt{2\pi}} \int_I e^{-x^2/2} \, dx$$

Remarks:

- If $h \in USp(2g)$, then $\text{Trace}(h) = \sum_{i=1}^{2g} \lambda_i$, and $|\lambda_i| = 1$.
- One thus *might* expect $\text{Trace}(h)$ being of size $\sim \sqrt{2g}$ (cf. random walk). **BUT**: eigenvalues of typical elements in $USp(2g)$ are very regularly spaced; get *massive* cancellation (like summing roots of unity).
- Gaussian "without" CLT — we don't divide by $\sqrt{2g}$. (!)

Point count statistics in large genus limit

Katz-Sarnak plus Diaconis-Shahshahani: point count fluctuations (normalized by $\sqrt{p}$) is **Gaussian** for family of hyperelliptics *provided* we take limits in the order

$$\lim_{g\to\infty}(\lim_{p\to\infty}\ldots)$$

Remarks:

- K-S plus D-S gives Gaussian point counts for other families, e.g., family of all genus g curves. (Via $M_{g,n}$.)
- M. Larsen (unpublished) obtained Gaussian moments for hyperelliptics of the form $y^2 = \prod_{i=1}^{d}(x-\alpha_i)$, $\alpha_i \in \mathbb{F}_p$.

What about other limits?

- $\lim_{p,g\to\infty}$ in arbitrary way?
- What about p fixed??

Warmup problem for p fixed

- "Toy model" family (non-smooth!):

$$\mathcal{F} = \mathcal{F}_p := \{f \in \mathbb{F}_p : f \text{ monic and } \deg(f) = d\}$$

  and, as $d \to \infty$, consider $C_f : y^2 = f(x)$.
- "Coin flip model" for $|C_f(\mathbb{F}_p)|$: define independent random variables $\{X_i\}_{i=1}^p$ where

$$X_i = \begin{cases} 0 & \text{with prob. } 1/p \\ 1 & \text{with prob. } (p-1)/2p \\ -1 & \text{with prob. } (p-1)/2p \end{cases}$$

- Claim: if $d \geq p$, then the fluctuations of

$$\{|C_f(\mathbb{F}_p)|\}_{f \in \mathcal{F}} \quad \text{and} \quad \sum_{i=1}^{p} X_i$$

  have the same distribution.

Proof:

- Recall Legendre symbol

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x = \square \text{ in } \mathbb{F}_p,\ x \neq 0, \\ -1 & \text{if } x \neq \square \text{ in } \mathbb{F}_p, \\ 0 & \text{if } x = 0. \end{cases}$$

- Since $|\{y : y^2 = f(x)\}| = 1 + \left(\frac{f(x)}{p}\right)$, we get

$$|C_f(\mathbb{F}_p)| = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{f(x)}{p}\right)\right) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)$$

  so fluctuations given by $\sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)$.
- Result now follows immediately from:
  - the linear evaluation map $f \to (f(1), f(2), \ldots, f(p))$ is surjective if $d \geq p$.
  - Number of nonzero squares: $(p-1)/2$. Number of nonsquares: $(p-1)/2$. Number of zero elements: 1.

Back to hyperelliptics

- For smoothness, need $(f', f) = 1$, i.e., f must be square free; let $\mathcal{F} := \{f \in \mathbb{F}_p[X] : f$ squarefree and monic, $\deg(f) = d\}$.
- Again, seems reasonable to expect that point count fluctuations for $|C_f(\mathbb{F}_p)|$, $f \in \mathcal{F}$ should be same as $\sum_{i=1}^{p} X_i$
- Surprise (!?): Basically correct, but must adjust coin flip model: define independent random variables $\{Y_i\}_{i=1}^{p}$ where

$$Y_i = \begin{cases} 0 & \text{with prob. } \frac{1}{p+1} \\ \pm 1, & \text{each with prob. } \frac{1}{2(1+1/p)} \end{cases}$$

Theorem (K.-Rudnick)

$$\frac{|\{f \in \mathcal{F} : |C_f(\mathbb{F}_p)| - (p+1) = n\}|}{|\mathcal{F}|} = \mathrm{Prob}(\sum_{i=1}^{p} Y_i = n)\cdot(1+O(p^{(3p-d)/2}$$

Why correction? $f(x) = 0$ a little less likely if f square free.

Gaussian by letting $p, d \to \infty$

Flipping many coins should give Gaussian:

- If p large, $\sum_{i=1}^{p} Y_i$ behaves as the sum of p fair coin flips (with ± 1 on each side.)
- Hence $a_{p,f} = |C_f(\mathbb{F}_p)| - (p+1)$ has zero mean, variance p.
- In particular, if $p, d \to \infty$ s.t. $d - 3p \to \infty$, get *Gaussian* distribution (with mean zero, variance one) for $a_{p,f}/\sqrt{p}$.

Is $d - 3p$, $p \to \infty$ needed? No!

Theorem (K.-Rudnick)

$\{a_{p,f}/\sqrt{p}\}_{f \in \mathcal{F}}$ has Gaussian moments as long as $p, d \to \infty$.

Rough idea of proofs: use sieve to pick out square free polynomials, use surjectivity of evaluation map "on remainder".

What about p fixed?

Random matrix theory must fail if p fixed and $g \to \infty$

- Recall Weil bounds etc:

$$|C_f(\mathbb{F}_p)| = p + 1 - a_{p,f} = p + 1 - p^{1/2} \cdot \mathrm{Trace}(U_{p,f})$$

- Expect: for C_f in "nice" family of genus g curves, $\{U_{p,f}\}_f$ equidistribute in some compact Lie group of $2g \times 2g$-matrices. (True for $p \to \infty$.)
- In particular, $\mathrm{Trace}(U_{p,f}) \simeq 2g$ can/should happen if random matrix model also correct when p fixed.
- BUT: if this happens when $g \to \infty$ and p fixed, positivity is violated(!!):

$$0 \leq |C_f(\mathbb{F}_p)| = p + 1 - a_{p,f} \simeq p + 1 - p^{1/2} \cdot 2g$$

Mystery: how adjust random matrix model when p fixed? Possible to get Gaussian even if p fixed?

Gaussian point counts for p fixed

Given a family $\mathcal{F}$ of curves, what is necessary for normalized fluctuations to be Gaussian?
Define the mean and variance of point counts as

$$M := \frac{\sum_{C \in \mathcal{F}} |C(\mathbb{F}_p)|}{|\mathcal{F}|}, \quad V := \frac{\sum_{C \in \mathcal{F}} |C(\mathbb{F}_p)|^2}{|\mathcal{F}|} - M^2,$$

To get Gaussian (with mean zero, variance one), should look at normalized point counts:

$$\frac{|C(\mathbb{F}_p)| - M}{V^{1/2}}$$

Now, since $|C(\mathbb{F}_p)|$ is integer valued, must have $V \to \infty$ for normalized point counts to have a continuous distribution.
Further, $V \to \infty$ and $|C(\mathbb{F}_p)| \geq 0$ implies that we also need $M \to \infty$ (the Gaussian is symmetric!)

Candidates for Gaussian point counts (p fixed)

- Problem with hyperelliptics: $|C_f(\mathbb{F}_p)| \leq 2p + 1$, so $M \to \infty$ impossible no matter how large $\deg(f)$ is.
- Any collection of families of curves C that can be embedded in $\mathbb{P}^n$ suffers same problem: $|C(\mathbb{F}_p)| \leq |\mathbb{P}^n(\mathbb{F}_p)|$ gives upper bound on mean.
- What about all genus g curves $M_g(\mathbb{F}_p)$? Well, not so clear that mean $= \frac{\sum_{C \in M_g} |C(\mathbb{F}_p)|}{|M_g|} \to \infty$ when $g \to \infty$.

Families of curves with many points

- Goal: produce sequence of families of curves (over $\mathbb{F}_p$) such that M, the average point count, tends to infinity (along with the variance.)
- Idea: Given a projective *surface* $X \subset \mathbb{P}^n$ and a degree d homogenuous polynomial $f(X_0, X_1, \ldots, X_n)$ define

  $$C_f := X \cap H_f$$

  where $H_f = \{P \in \mathbb{P}^n : f(P) = 0\}$ is the hypersurface defined by f.
- **If** $|X(\mathbb{F}_p)|$ large, $|C_f(\mathbb{F}_p)|$ might be large for many f.
  - Model for $|C_f(\mathbb{F}_p)|$: toss $|X(\mathbb{F}_p)|$ **unfair** coins, where prob. of success $= 1/p = \mathrm{Prob}(f(P) = 0)$.
- Problem: C_f might not be smooth for all f. Perhaps generic, or "most", f works?

Smooth curves "by definition"

Recall: $X \subset \mathbb{P}^n$ is a surface, $C_f := X \cap H_f$ where H_f is hypersurface.

- Let $S_d \subset \mathbb{F}_p[X_0, \ldots, X_n]$ be the set of degree d homogenuous polynomials in $n+1$ variables.
- Define **smooth** family of curves

$$\mathcal{F}(d) := \{C_f : f \in S_d, \text{ and } C_f \text{ smooth.}\}$$

- Problem: $\mathcal{F}(d)$ might be empty.
- By Poonen's "finite field Bertini", when $d \to \infty$,

$$|\mathcal{F}(d)| = |S(d)|/\zeta_X(3) \cdot (1 + o(1)).$$

  Here $\zeta_X(s)$ is the zeta function of X, i.e.,

$$\zeta_X(s) := \prod_{P \in X,\ P \text{ closed}} (1 - |P|^{-s})^{-1}$$

- Upshot: $|\mathcal{F}(d)| \to \infty$ when $d \to \infty$.

A coin flip model for $(X \cap H_f)(\mathbb{F}_p)$

A slightly more explicit version of Poonen's "finite field Bertini with Taylor coeffecients" gives:

Proposition (K.-Wigman)

As $d \to \infty$,

$$\frac{|\{C \in \mathcal{F}(d) : |C(\mathbb{F}_p)| = s\}|}{|\mathcal{F}(d)|}$$
$$= \binom{|X(\mathbb{F}_p)|}{s} \left(\frac{p+1}{p^2+p+1}\right)^s \left(1 - \frac{p+1}{p^2+p+1}\right)^{|X(\mathbb{F}_p)|-s} \cdot (1+o(1))$$

uniformly *for $0 \le s \le |X(\mathbb{F}_p)|$.*

Note: this is just coin flip model with prob. of success $= \frac{p+1}{p^2+p+1}$.
(But **not** $= 1/p$.)

Making the average point count tend to infinity

- M, the mean point count of $C \in \mathcal{F}(d)$ equals $|X(\mathbb{F}_p)| \cdot \frac{(p+1)}{p^2+p+1} \cdot (1+o(1))$ as $d \to \infty$.
- How ensure $M \to \infty$? Just take **sequence** of surfaces X_i such that $X_i(\mathbb{F}_p) \to \infty$.
- One way to do this: use Ihara (or Tsfasman, Vlăduț, and Zink) construction of tower of modular **curves** $Y_0(l)$, l prime, with many points over $\mathbb{F}_{p^2}$: $Y_0(l)(\mathbb{F}_{p^2}) \geq (p-1)(l+1)/12$. Letting X_i be the restriction of scalars of $Y_0(l_i)(\mathbb{F}_{p^2})$ to $\mathbb{F}_p$, get **surfaces** X_i s.t $X_i(\mathbb{F}_p) \gg l_i$
- Thus, if we let d_i grow fast enough and take $\mathcal{F}_i := \mathcal{F}_i(d_i)$, $\{\mathcal{F}_i\}_{i\geq 1}$ will be sequence of families of smooth curves s.t.
  - $M_i, |\mathcal{F}_i| \to \infty$.
  - Easy to see that $V_i \to \infty$.

Gaussian for p fixed (at last!)

Theorem (K.-Wigman)

There exists a sequence of families $\{\mathcal{F}_i\}_{i=1}^{\infty}$ of smooth curves defined over $\mathbb{F}_p$ with the following properties: $|\mathcal{F}_i|, M_i, V_i$ all tend to infinity, and, for all compact intervals I,

$$\frac{1}{|\mathcal{F}_i|}\left|\left\{C \in \mathcal{F}_i : \frac{|C(\mathbb{F}_p)| - M_i}{V_i^{1/2}} \in I\right\}\right| = \frac{1}{\sqrt{2\pi}} \int_I e^{-x^2/2} dx + o(1),$$

as $i \to \infty$.

Wrong bias

Why do coins have "wrong" bias — why $(p+1)/(p^2+p+1)$ rather than $1/p$?

- We expect that f vanishes at $Q \in X$ with prob. $1/p$.
- However: we conditioned on f so that $C_f = X \cap H_f$ is smooth; this changes things.
- Let $f|_X = A + BT_1 + CT_2 +$ (higher order) in local coords T_1, T_2 at $Q \in X$. (Corresponding to $T_1 = T_2 = 0$.)
- Prob. that C_f smooth at Q (whether $Q \in C_f$ or not): $(p^3-1)/p^3 = (1-p^{-3})$. (Must avoid $A = B = C = 0$.)
- Prob. that C_f smooth at Q **and** $f(Q) = 0$: $(p^2-1)/p^3$. (Must have $A = 0$ and avoid $B = C = 0$.)
- Thus: prob. that $Q \in C_f$ given that C_f smooth

$$= \frac{(p^2-1)/p^3}{(p^3-1)/p^3} = \frac{p+1}{p^2+p+1} \neq 1/p$$

Some related results

- Knizhnerman and Sokolinskii: computed moments of fluctuations for $y^2 = f(x)$ and f ranging over non-square polynomials.
- Bucur, David, Feigon, Lalín:
  - Coin flip model valid for curves of the form $y^l = f(x)$ when $d = \deg(f)$ tends to infinity (l fixed.)
    Get Gaussian distribution if $p, d \to \infty$.
  - Coin flip model also valid for smooth plane curves given by homogenous polynomials $f \in \mathbb{F}_p[X_0, X_1, X_2]$ when $d = \deg(f)$ tends to infinity.
    Get Gaussian distribution if $p, d \to \infty$ **provided** $d > p^{1+\epsilon}$.
- M. Xiong: Similar results for $y^l = f(x)$ where f ranges over degree d families of polynomials — either l-th power free, or irreducible. (Proof uses character sums.)