COUNTING POINTS ON CURVES OVER FINITE FIELDS

ALINA BUCUR

Let $C/\mathbb{F}_q$ be a curve. The zeta function of C is

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

By the Weil conjectures, we know this can be written as $\frac{P_C(T)}{(1-T)(1-qT)}$, where $\deg P_C(T) = 2g$, with g the genus of C.

Write

$$P_C(T) = \prod_{j=1}^{2g} (1 - T\alpha_j(C)) \in \mathbb{Z}[T].$$

The numbers α_j are the eigenvalues of the Frobenius endomorphism. The number of $\mathbb{F}_q$-points on the curve is $\#C(\mathbb{F}_q) = q + 1 - \mathrm{tr}(\mathrm{Frob}_C)$.

Deligne proved that the distribution of eigenvalues of Frobenius approaches the distribution of eigenvalues of a random matrix in $USp(2g)$. Katz-Sarnak showed that this situation was generic, in that hyperelliptic curves are generic in the moduli space of curves of genus g.

1. Arithmetic situation

Take a curve $C/\mathbb{Q}$ of genus 2 and consider its reductions modulo p as $p \to \infty$. Now the Katz-Sarnak prediction is that the distribution of eigenvalues of Frobenius approaches the distribution of eigenvalues of random matrices in USp(4).

(cf talk of Drew Sutherland next week – also, pictures of exceptional distributions on `math.mit.edu/~drew`)

2. Discrete probabilistic situation

Fix $\mathbb{F}_q$, genus $\to \infty$.

Kurlberg-Rudnick consider hyperelliptic curves. The trace of Frobenius is distributed as the sum of $q+1$ i.i.d. random variables taking 0 with probability $\frac{1}{q+1}$ and ± 1 each with probability $\frac{q}{2(q+1)}$.

This was generalized by B-David-Feigon-Lalín: looked at p-fold covers of $\mathbb{P}^1$. The trace of $\mathrm{Frob}_C \mid_{H^1_{\chi_p}}$ is distributed as the sum of $X_0 + \cdots X_q$, where X_i are i.i.d. random variables, taking value 0 with probability $\frac{p-1}{q+p-1}$ and value a pth root of unity with probability $\frac{q}{p(q+p-1)}$.

2.1. Plane curves.

What if we try to do this for plane curves?

We recall the following theorem of Poonen:

Theorem 2.1 (Bertini with Taylor conditions)**.** *Let X be a quasi-projective subscheme of $\mathbb{P}^n$ over $\mathbb{F}_q$, Z finite subscheme of $\mathbb{P}^n$ such that $U = X \setminus (X \cap Z)$ is smooth of dimension m. Fix $T \subset H^0(Z, \mathcal{O}_Z)$. Given a homogeneous polynomial f of degree d, let $f|_Z$ denote the element of $H^0(Z, \mathcal{O}_Z)$ that on each connected component Z_i equals the restriction of $x_j^{-d} f$ to Z_i, where $j = j(i)$ is the smallest integer $0 \le j \le n$ such that the coordinate x_j is invertible on Z_i. Then*

$$\frac{\#\{f \in S_d; H_f \cap U \text{ smooth, } f|_Z \in T\}}{\#S_d} \to \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \zeta_U(m+1)^{-1} \text{ as } d \to \infty.$$

How we use it: let $X = \mathbb{P}^2$. We want to sort through smooth curves and reproduce the earlier p-fold cover situation, where each thing gave one condition, i.e., one random variable. So each point in $\mathbb{P}^2$ is going to impose a condition. We also choose Z to be an $\mathfrak{m}_P^2$-neighborhood for each point $P \in \mathbb{P}^2(\mathbb{F}_q)$ (this means that we look at the value of F and its first order derivatives at each point). Thus

$$H^0(Z, \mathcal{O}_Z) = \prod_{P \in \mathbb{P}^2(\mathbb{F}_q)} \mathcal{O}_P/\mathfrak{m}_P^2.$$

Strategy: the probability that H_f is smooth at a closed point P of the subscheme U is given by

$$1 - q^{-3 \deg P}.$$

If conditions were independent, we would get that the probability that H_f is smooth was

$$\prod_{P \text{ closed point of } U} (1 - q^{-3 \deg P}) = \frac{1}{\zeta_U(3)}.$$

The proof of Poonen's result is a sieving argument that separately treats the closed points of X of low, medium, and high degree (as a function of d).

So to adapt Poonen's result to our case, the strategy is to work through his proof and extract the error terms.

We sieve the closed points of X into 3 categories:

- points of low degree
- points of medium degree
- points of high degree

We show that the last two things are small (via Bézout, Weil bounds, etc. to bound contribution of these last two parts). For high degree, separate variables by writing $f = f_0 + x_1^p f_1 + x_2^p f_2$ and taking partial derivatives, and use this to say something about the contributions.

This gives the following theorem:

Theorem 2.2. *Let $X_1, \dots, X_{q^2+q+1}$ be q^2+q+1 i.i.d. Bernoulli random variables taking the value 1 with probability $\frac{q+1}{q^2+q+1}$ and the value 0 with probability $\frac{q^2}{q^2+q+1}$. Then, for $0 \le t \le q^2+q+1$,*

$$\begin{aligned} \frac{\#\{F \in S_d^{\mathrm{ns}}; \#C_F(\mathbb{F}_q) = t\}}{\#S_d^{\mathrm{ns}}} &= \mathrm{Prob}\left(X_1 + \cdots + X_{q^2+q+1} = t\right) \\ &\times \left(1 + O\left(q^t\left(d^{-1/3} + (d-1)^2 q^{-\min\left(\left\lfloor \frac{d}{p}\right\rfloor + 1, \frac{d}{3}\right)} + d q^{-\left\lfloor \frac{d-1}{p}\right\rfloor - 1}\right)\right)\right). \end{aligned}$$

Note that the average number of points is $q+1$.

2.2. **Complete intersections.** B-Kedlaya: what happens if you redo Poonen's sieving argument with H_F a complete intersection? This shows that the average being $q+1$ is a fluke.

Suppose we take two hypersurfaces $H_{f_1} \cap H_{f_2}$ in $\mathbb{P}^3$. The average number of points is

$$q + 1 - \frac{q^{-2}(1+q^{-1})}{1+q^{-2}-q^{-5}} < q+1.$$

So the expected value of the trace of Frobenius is not 0.