Honors 1: Undergraduate Math Lab*

Peter Sarnak†, Steven Miller‡, Alex Barnett§

October 23rd, 2002

Courant Institute of Mathematical Sciences
New York University
New York, NY

Abstract

More on Graphs, Kloosterman, and the Third Problem on the Randomness of $x \mapsto \overline{x}$ mod p. Review of projective geometry and fractional linear transformations. Lecture by Peter Sarnak; notes by Steven Miller.

1 Kloosterman Sums

Recall

$$S(a,b,p) \ = \ \sum_{x \bmod p}^{*} e\Big(\frac{ax+b\overline{x}}{p}\Big), \tag{1}$$

where $\sum^*$ means sum over all x relatively prime to p, and $\overline{x} \equiv x^{-1} \bmod p$.

Theorem 1.1 (Weil). *For p an odd prime and $a, b \in \mathbb{Z}$,*

$$|S(a,b,p)| \ \leq \ 2\sqrt{p}. \tag{2}$$

*Homepage: `http://www.math.nyu.edu/~millerj/`
†E-mail: `sarnak@math.princeton.edu`
‡E-mail: `millerj@cims.nyu.edu` or `sjmiller@math.princeton.edu`
§E-mail: `barnett@nmr.mgh.harvard.edu`

The above captures the randomness. We add $p-1$ numbers of modulus 1, and we see square-root cancellation. Weil's Theorem says the cancellation is "like" random numbers. Recall when we added ± 1, we expected to observe a sum around $\sqrt{N}$ if we had N summands.

2 Projective Geometry

Consider the map

$$\begin{aligned} \mathbb{C} &\rightarrow \mathbb{C} \cup \{\infty\} \\ z &\mapsto \frac{az+b}{cz+d}. \end{aligned} \tag{3}$$

We define the above as the action of the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{4}$$

on z.

$\mathbb{P}^1(\mathbb{R})$ is identified with the perimeter of a circle, with antipodal points (points on a diagonal, separated by π radians) identified.

3 Example

Definition 3.1 **($\mathbb{P}^1(\mathbb{F}_p)$).** $\mathbb{P}^1(\mathbb{F}_p)$ *is the projective line,*

$$\mathbb{P}^1(\mathbb{F}_p) = \{0, 1, \ldots, \infty\}. \tag{5}$$

We construct a 3-regular graph G_p on $p+1$ vertices as follows:

1. Join x to $x+1$ mod p.
2. Join x to $x-1$ mod p.
3. Join x to $-\overline{x}$ mod p,

where $\frac{1}{\infty} = 0$.

Form the adjacency matrix of the above graph. Is there a spectral graph?

Theorem 3.2. *There is a spectral gap!*

$$\lambda_1(G_p) \;\leq\; 2.99. \tag{6}$$

These graphs are not *Ramanujan in general.*

We can look at the three maps as matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \tag{7}$$

Exercise 3.3. $(ST)^3 = \pm I$.

Exercise 3.4. *Show the three maps we used to create G_p can be given by*

1. $x \to Tx$ *(corresponding to $x \to x+1$),*
2. $x \to T^{-1}x$ *(corresponding to $x \to x-1$),*
3. $x \to Sx$ *(corresponding to $x \to -\overline{x}$.*

4 Stereographic Projections and Fractional Linear Transformations

What are the analytic, $1-1$ invertible maps from $\mathbb{C} \to \mathbb{C}$? What if we include ∞.

First, one might ask what is ∞?

Take a sphere, call the north pole N. Consider the infinite plane $z = 0$.

To each point P on the sphere, draw the line from N to P, and write down the point of intersection on the plane $z = 0$. Call this map S (stereographic projection; preserves angles), and call the sphere $S^2 = \mathbb{P}^1$.

Thus,

$$S(P) \in \mathbb{C},\; S(\infty) \leftrightarrow N,\; S^2 \cong \mathbb{C} \cup \{\infty\}. \tag{8}$$

Recall GL_2 are the 2×2 matrices with non-zero determinant. $SL_2(\mathbb{C})$ is the group of 2×2 matrices with determinant 1.

Fractional Linear Transformation: $z \mapsto \frac{az+b}{cz+d}$.

If we have two linear transformations

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \; \delta = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \tag{9}$$

then

$$\gamma(\delta z) \;=\; (\gamma\delta)z, \tag{10}$$

where $(\gamma\delta)$ is usual matrix multiplication.

5 More Kesten

Let Γ be a group generated by

$$A_1,\; A_1^{-1},\; A_2,\; A_2^{-1},\; \dots\;,\; A_k,\; A_k^{-1}. \tag{11}$$

We make a $2k$-regular graph by joining x and y with an edge $(x \sim y)$ if and only if $x = A_j^{\pm 1} y$ for some j.

Define, for $f : \Gamma \to \mathbb{C}$,

$$Bf(x) \;=\; \sum_{x \sim y} f(y). \tag{12}$$

To make the sum make sense if we have infinitely many vertices we require $f \in l^2(\Gamma)$, the space of functions g where $\sum |g(\gamma)|^2 < \infty$.

One could ask about the spectrum of B on this space. The HW problem was on a k-regular tree. Make words using the generators. Have the notion of a free group: no relation (ie, no word is the identity word) except the trivial ones $(A_i A_i^{-1} = I)$.

$$\Gamma \;=\; \langle A_1, A_2, \dots, A_k \rangle. \tag{13}$$

Definition 5.1 (Free Group). Γ *is a free group if the only relations in* Γ *giving the identity are the obvious ones (ie, the only word in* $A_1, \dots, A_k$ *that is the identity word is words of the form* $A_k^{-1} A_i A_i^{-1} A_j^{-1} A_j A_k$*, and so on).*

The graph we just spoke about, $G(\Gamma)$ on A_1, A_1^{-1} up to A_k, A_k^{-1} is a $2k$-regular tree if and only if Γ is a free group on $A_1, \dots, A_k$. This is called a Cayley Graph (relative to the given generators).

Theorem 5.2 (Kesten). *The spectrum of B when Γ is free on k generators is*

$$\text{spectrum}(B) \ = \ \Big[-2\sqrt{2k-1}, 2\sqrt{2k-1}\Big]. \tag{14}$$

Further, Γ is free on $A_1, \dots, A_k$ if and only if

$$\text{spectrum}(B) \ \subset \ \Big[-2\sqrt{2k-1}, 2\sqrt{2k-1}\Big]. \tag{15}$$

Thus, the spectrum contains a point outside *this interval if and only if Γ is not free.*

Finally, $2k$ is in the spectrum if and only if Γ is amenable (for example, abelian).

Corollary 5.3. *Our graphs G_p cannot be Ramanujan, as there* is *a relation among the generators, namely $(ST)^3 = \pm I$.*

6 $\mathbf{SL}_2(\mathbb{Z})$

Definition 6.1 ($\mathbf{SL}_2(\mathbb{Z})$). *$SL_2(\mathbb{Z})$ is the group of 2×2 matrices with unit determinant and integer coefficients.*

Exercise 6.2. *Consider the matrices*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \tag{16}$$

Show these three matrices generate $SL_2(\mathbb{Z})$; as $(ST)^3 = \pm I$, this shows $SL_2(\mathbb{Z})$ is not a free group.

Where should $\mathrm{SL}_2(\mathbb{Z})$ act? Lubotsky: you don't understand a group until it acts on something you know. Galois had groups acting on roots of polynomials (permuting roots).

What does $\mathrm{SL}_2(\mathbb{Z})$ act on? It does act on the sphere, but it is too big a space. We want to study the smallest space where it acts reasonably.

Look at $\mathrm{SL}_2(\mathbb{R})$, the group of 2×2 matrices with determinant 1 and real entries. Let z be in the upper half plane, so $z = x + iy$, $y > 0$. Then

$$z \ \mapsto \ \frac{az+b}{cz+d}, \ \mathrm{Im}\Big(\frac{az+b}{cz+d}\Big) \ > \ 0. \tag{17}$$

A similar statement holds for z in the lower half plane. Thus, $\mathrm{SL}_2(\mathbb{R})$ maps the upper (lower) half plane to itself.

By shifting by an integer, we can bring any $x \in \mathbb{R}$ to $x' \in [0, 1)$.

Gauss was the first to draw the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ acting on the upper half plane:

Draw a circle of radius 1 with center 0; draw vertical lines at $x = \pm\frac{1}{2}$, going from the point on the circle to infinity. The region formed is called the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane. This means that any z in the upper half plane can be brought into this region.

7 Is $x \to \overline{x}$ mod p Random?

7.1 First Test

Question 7.1. *To what extent is / how random is $x \to \overline{x}$ mod p?*

There are p numbers.

If look at all numbers $1 \leq x \leq p - 1$, we get all the numbers back (in some new order). We can look at a long segment (on what scale?), say

$$\sqrt{p} \ \leq x \leq 2\sqrt{p}. \tag{18}$$

Now $\overline{x}$ will be all over $[1, p-1]$. This generates $\sqrt{p}$ numbers between 1 and $p-1$. The average spacing is is approximately $\frac{p-1}{\sqrt{p} \approx \sqrt{p}}$. How are numbers spaced?

First, we need to write them in increasing order

$$1 \leq a_1 \ < \ a_2 \ < \ \cdots \ < a_l \ \leq p - 1. \tag{19}$$

Let us denote the nearest neighbor spacings by $\Delta_1 = a_2 - a_1$, $\Delta_2 = a_3 - a_2$ and so on. Let

$$\delta_j = \frac{\Delta_j}{\sqrt{p}}. \tag{20}$$

Note the δ_js have unit mean spacing.

Conjecture 7.2 (Naive Conjecture). *We expect the spacings to follow Poissonian Statistics. Explicitly, the distribution of spacings we see here should be the same as that from choosing $\sqrt{p}$ numbers independently from the uniform distribution on $[0, 1)$.*

7.2 Second Test

Question 7.3 (Jim Propp). *Does $x \to \overline{x}$ behave like a random permutation of order 2?*

What is the distribution of the longest increasing sub-sequence?

Given a permutation of $1, 2, \ldots, N$, we have $i \mapsto \sigma(i)$. Permutations are often denoted by

$$\begin{pmatrix} 1 & 2 & \cdots & N \\ \sigma(1) & \sigma(2) & & \sigma(N) \end{pmatrix} \tag{21}$$

Look at the distribution of the longest increasing sub-sequence about the mean. Normalized appropriately, what does it look like?

7.3 Third Test: Hooley's R^*

$$\sum_{x=A}^{A+N} e\left(\frac{\overline{x}}{p}\right), \tag{22}$$

where $1 \leq A \leq A + N \leq p - 1$.

When we add numbers of modulus one, we expect square-root cancellation.

Then

Conjecture 7.4 (Hooley's R^*). *For every $\epsilon > 0$,*

$$\left| \sum_{x=A}^{A+N} e\left(\frac{\overline{x}}{p}\right) \right| \ll_\epsilon N^{\frac{1}{2}} p^\epsilon. \tag{23}$$

Note $\ll_\epsilon$ means the left hand side is less than c_ϵ times the right hand side (for some c_ϵ ¿ 0).

Note there is no dependence on A – the only dependence is on the size of summation N and the prime p.

If $N > \sqrt{p}$, the above can be proven. by Weil's bound.