## 18. Random walks on finite groups II

April 22. Transcribed by Hang Du. Used with permission.

**Setup**:

- Let $G$ be a finite group.
- $\mu : G \to \mathbb{R}$ is a probability measure on $G$, i.e., $\mu(g) \geq 0, \sum_{g\in G} \mu(g) = 1$.
- Starting with $g_0 \in G$, let $h_t \in G, t = 1, 2, \dots$ be sampled according to $\mu$, and define the random walk on $G$ by $g_t = g_{t-1} \cdot h_t, t = 1, 2, \dots$.

**Question**: how evenly distributed is $g_K$ on $G$ for large $K$?

To state our question more precisely, we introduce some definitions. For two functions $f_1, f_2 : G \to \mathbb{C}$, define

$$f_1 * f_2(g) = \sum_{g_1,\cdot g_2=g} f_1(g_1)f_2(g_2)\,, \quad \forall g \in G\,.$$

Define the operator $T_\mu : \ell^2(G) \to \ell^2(G)$ by $T_\mu f = f * \mu$. It is straightforward to check that for any $K$, $T_\mu^K \delta_{g_0}$ is the distribution of $g_K$ defined as above. Our main question is to estimate

$$\|T_\mu^K \delta_{g_0} - \tfrac{1}{|G|}\mathbf{1}\|_{\ell^2(G)}$$

for large $K \in \mathbb{N}$.

We start with some easy observations.

**Lemma 18.1.** *$T_\mu \mathbf{1} = \mathbf{1}$, and $\|T_\mu f\|_{\ell^2(G)} \leq \|f\|_{\ell^2(G)}, \forall f \in \ell^2(G)$.*

*Proof.* The first claim can be checked straightforwardly. For the second claim, we define the right shift operator $R_g : \ell^2(G) \to \ell^2(G)$ by

$$R_g f(h) = f(f \cdot g^{-1})\,, \quad \forall f \in \ell^2(G), g, h \in G\,.$$

It is easy to check that $R_g : \ell^2(G) \to \ell^2(G)$ is an isometry, and it holds that

$$T_\mu f = f * \mu = \sum_{g\in G} \mu(g) R_g f\,, \quad \forall f \in \ell^2(G)\,.$$

Therefore, it follows from the triangle inequality that

$$\|T_\mu f\|_{\ell^2(G)} \leq \sum_{g\in G} \mu(g)\|R_g f\|_{\ell^2(G)} = \|f\|_{\ell^2(G)}\,. \qquad \square$$

Denote $\ell^2(G)_0$ as the orthogonal complement of the constant functions in $\ell^2(G)$. One can verify that $T_\mu$ maps $\ell^2(G)_0$ to itself. Denote by $\sigma_1(T_\mu)$ the largest singular value of the operator $T_\mu : \ell^2(G)_0 \to \ell^2(G)_0$.

**Lemma 18.2.** *For any $K \in \mathbb{N}$, it holds that*

$$\|T_\mu^K \delta_{g_0} - \tfrac{1}{|G|}\mathbf{1}\|_{\ell^2(G)} \leq \sigma_1(T_\mu)^K\,.$$

*Proof.* Write $\delta_{g_0} = \frac{1}{|G|}\mathbf{1} + (\delta_{g_0})_h$, where $(\delta_{g_0})_h = \delta_{g_0} - \frac{1}{|G|}\mathbf{1} \in \ell^2(G)_0$. We have for any $K \in \mathbb{N}$, $T_\mu^K \delta_{g_0} = \frac{1}{|G|}\mathbf{1} + T_\mu^K (\delta_{g_0})_h$, and thus

$$\|T_\mu^K \delta_{g_0} - \tfrac{1}{|G|}\mathbf{1}\|_{\ell^2(G)} \le \|T_\mu^K (\delta_{g_0})_h\|_{\ell^2(G)} \le \sigma_1(T_\mu)^K \|(\delta_{g_0})_h\|_{\ell^2(G)} \le \sigma_1(T_\mu)^K . \qquad \square$$

For a subset $A$ of $G$, we denote $\mu_A = \frac{1}{|A|}\mathbf{1}_A$ and abbreviate $T_{\mu_A}$ as $T_A$. Of particular interest of us is the following concrete example: let $G = \mathrm{SL}_2(\mathbb{F}_p)$ where $p$ is a large prime and

$$A_{\mathrm{sel}} = \left\{ \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{F}_p) .$$

We will focus on the following theorem of Selberg.

**Theorem 18.3.** *There exists a universal constant $c > 0$ such that, for every $p$, $\sigma_1(T_{A_{\mathrm{sel}}}) \le 1 - c$.*

In general, for a pair $(G, A)$ where $A$ is a subset of the group $G$, we are interested in $\sigma_1(T_A)$. This is not only because it is related to the mixing of random walks on $G$ with steps in $A$ (see Lemma 18.2), but also because the spectral gap $1 - \sigma_1(T_A)$ reflects a certain expansion property of the corresponding Cayley graph.

More precisely, for $A \subset G$ that is symmetric and generates $G$, we define $\mathrm{C}(G, A)$ as the graph with vertices corresponding to the elements of $G$, and with edges $(g_1, g_2) \in E$ if there exists $a \in A$ such that $g_2 = g_1 \cdot a$. Note that $A$ generates $G$, which implies that $\mathrm{C}(G, A)$ is connected. Moreover, for a subset $S \subset G$, we denote $E(S, S^c)$ as the set of edges $(g_1, g_2) \in E$ such that $g_1 \in S$ and $g_2 \in S^c$.

**Lemma 18.4.** *For any $S \subset G$, it holds that*

$$|E(S, S^c)| \ge (1 - \sigma_1(T_A)) \frac{|A||S||S^c|}{|G|} .$$

*Proof.* It is straightforward to check that

$$\begin{aligned} |E(S, S^c)| &= |A| \langle T_A \mathbf{1}_S, \mathbf{1}_{S^c} \rangle \\ &= |A| \langle \tfrac{|S|}{|G|}\mathbf{1}, \tfrac{|S^c|}{|G|}\mathbf{1} \rangle + |A| \langle T_A (\mathbf{1}_S)_h, (\mathbf{1}_{S^c})_h \rangle \\ &\ge \frac{|A||S||S^c|}{|G|} - \sigma_1(T_A) \|(\mathbf{1}_S)_h\|_{\ell^2(G)} \|(\mathbf{1}_{S^c})_h\|_{\ell^2(G)} \\ &\ge (1 - \sigma_1(T_A)) \frac{|A||S||S^c|}{|G|} . \end{aligned} \qquad \square$$

Combining Lemma 18.2 with Theorem 18.3, we obtain that for any $S \subset G = \mathrm{SL}_2(\mathbb{F}_p)$ with $|S| \le \frac{|G|}{2}$, in the graph $\mathrm{C}(\mathrm{SL}_2(\mathbb{F}_p), A_{\mathrm{sel}})$,

$$E(S, S^c) \ge \frac{c|A||S|}{2} .$$

For a large graph $H = (V, E)$, we say $H$ is an expander graph, if there exists a universal constant $c > 0$ such that for any $S \subset V$ with $S \leq \frac{|V|}{2}$, $E(S, S^c) \geq \frac{c|E||S|}{|V|}$. The above result indicates that $\mathrm{C}(\mathrm{SL}_2(\mathbb{F}_p), A_{\mathrm{sel}})$ is a sparse expander graph (here sparse means that the graph has average degree $O(1)$). While Selberg did not state his theorem exactly in the form above, his work is in a sense the first proof of the existence of sparse expander graphs. In what follows we fix a large prime number $p$ and let $G = \mathrm{SL}_2(\mathbb{F}_p)$. We now discuss the proof of Theorem 18.3. We will not give a complete proof, but we will discuss some of the ideas in the proof, following the approach developed by Sarnak-Xue in the early 1990s.

**$\ell^2$-bound**. We claim the following $\ell^2$-estimate of $\sigma_1(T_\mu)$.

**Theorem 18.5.** *There exists a universal constant $C > 0$ such that*

$$\sigma_1(T_\mu)^2 \leq Cp^2 \|\mu\|^2_{\ell^2(G)}\,.$$

We begin with a lemma on non-trivial representations of $G = \mathrm{SL}_2(\mathbb{F}_p)$.

**Lemma 18.6.** *Let $\rho : G \to \mathrm{U}(d)$ be a non-trivial representation of $G$, then $d \geq \frac{p-1}{2}$.*

*Proof.* Consider the following two elements in $G$:

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad v = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

It is easy to check that $u, v$ generates $G$. Since $\rho$ is non-trivial, without loss of generality we may assume that $\rho(u) \neq I_d$. Note that

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & a^2 \\ 0 & 1 \end{pmatrix}, \quad \forall a \in \mathbb{F}_p^*\,.$$

This implies that $u$ is conjugate to $u^{a^2}$ for any $a \in \mathbb{F}_p^*$. Let $\Lambda$ be the multi-set of eigenvalues of $\rho(u)$, we have $\Lambda = \Lambda^{a^2}, \forall a \in \mathbb{F}_p^*$. On the other hand, since $u^p = 1$, we have $\Lambda \subset \{z \in \mathbb{C}, z^p = 1\}$. Moreover, one can check that $\Lambda \neq \{1, \ldots, 1\}$, as this would imply that $\rho(u)^p \neq I_d$ (unless $\rho(u) = I_d$). Consequently, we can pick $\lambda \in \Lambda$ such that $\lambda \neq 1$. Then, the $\frac{p-1}{2}$ distinct elements $\lambda^{a^2}, a \in \mathbb{F}_p^*$ all lie in $\Lambda$. We conclude that $d \geq |\Lambda| \geq \frac{p-1}{2}$, as desired. □

The above lemma says that any non-trivial representation of $G = \mathrm{SL}_2(\mathbb{F}_p)$ has dimension at least of order $p$. This lower bound is order tight: consider the subgroup $U$ of $G$:

$$U = \left\{ \begin{pmatrix} a & t \\ 0 & a^{-1} \end{pmatrix}, a \in \mathbb{F}_p^*, t \in \mathbb{F}_p \right\},$$

which has size of order $p^2$. We have $G$ acts on $G/U$ induces a non-trivial representation with dimension of order $p$.

Before proving Theorem 18.5, we first introduce some notations. For $\mu : G \to \mathbb{R}$, define $\mu^*(g) = \mu(g^{-1}), \forall g \in G$. One can check that $T_\mu^*$, the adjoint of $T_\mu$, equals $T_{\mu^*}$. Moreover, $T_\mu T_\mu^* = T_\mu T_{\mu^*} = T_{\mu * \mu^*}$. Denote $\nu = \mu * \mu^*$.

*Proof of Theorem 18.5.* Let $V \subset \ell^2(G)_0$ be the eigenspace of $T_\nu = T_\mu T_\mu^*$ that corresponds to the eigenvalue $\lambda_1(T_\nu) = \sigma_1(T_\mu)^2$. Consider the left shift operator $L_g : \ell^2(G) \to \ell^2(G)$ defined by $L_g f(h) = f(g^{-1}h), \forall f \in \ell^2(G), g, h \in G$. It is straightforward to check that $L_g$ commutes with $T_\nu$, and thus $L_g$ maps $V$ to itself. Since $V$ does not contain any constant function, $L_g$ induces a non-trivial representation of $G$ on $V$. By Lemma 18.6, we have $\dim(V) \geq \frac{p-1}{2}$, and thus $\lambda_1(T_\nu)$ has multiplicity at least $\frac{p-1}{2}$. Therefore, by the trace formula we have

$$\begin{aligned}\frac{p-1}{2}\sigma_1(T_\mu)^2 &= \frac{p-1}{2}\lambda_1(T_\mu) \leq \sum_i \lambda_i(T_\nu) = \mathrm{Tr}(T_\nu) \\ &= \mathrm{Tr}(T_\mu T_\mu^*) = \sum_{g_1,g_2 \in G} T_{\mu,g_1,g_2}^2 = |G| \sum_{g \in G} \mu(g)^2 = |G| \|\mu\|_{\ell^2(G)}^2 .\end{aligned}$$

Since $|G| \sim p^3$, the desired result follows. □

As a corollary, we see that for any set $A \subset G$ with $|A| \geq 2Cp^2$, it holds that $\sigma_1(T_A)^2 \leq Cp^2 \|\mu_A\|_{\ell^2(G)}^2 \leq 1/2$. Note that for $U$ the subgroup of $G$ defined as above, we have $|U| \sim p^2$ and $\sigma_1(T_U) = 1$. This example also shows that the result of Theorem 18.5 is order-tight.

We say $\mu$ is symmetric if $\mu = \mu^*$ (i.e. $\mu(g) = \mu(g^{-1})$). When $\mu$ is symmetric, we have $T_\mu$ is self-adjoint and thus $\sigma_1(T_\mu)^K = \lambda_1(T_\mu)^K = \lambda_1(T_\mu^K) = \lambda_1(T_{\mu^{*K}}) = \sigma_1(T_{\mu^{*K}})$. Applying Theorem 18.5, we obtain that for any $K \in \mathbb{N}$, it holds that

$$\sigma_1(T_{A_{\mathrm{sel}}})^K \leq Cp^2 \|\mu_{A_{\mathrm{sel}}}^{*K}\|_{\ell^2(G)}^2 .$$

Our plan is to pick $K = C_0 \log p$ for some universal constant $C_0 > 0$, and show that $\|\mu_{A_{\mathrm{se;}}}^{*K}\|_{|ell^2(G)}^2 \leq p^{-2.1}$. This would imply that $\sigma_1(T_{A_{\mathrm{sel}}}) \leq 1 - c$ for some universal $c = c(C, C_0) > 0$.

**Lifting to** $\mathrm{SL}_2(\mathbb{Z})$. Consider the projection $\pi_p : \mathbb{Z} \to \mathbb{F}_p$, which induces a group homomorphism $\Pi_p : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_p)$. Let $M$ be a probability measure on $\mathrm{SL}_2(\mathbb{Z})$ and we let $\mu = \Pi_p(M)$ be its push-forward onto $\mathrm{SL}_2(\mathbb{F}_p)$. It holds that $\Pi_p(M^{*K}) = \mu^{*K}$ for any $K \in \mathbb{N}$. Therefore, to understand $\mu_{A_{\mathrm{sel}}}^{*K}$ for large $K \in \mathbb{N}$, we may try to first understand $M_{A_{\mathrm{sel}}}^{*K}$, where $M_{A_{\mathrm{sel}}} = \frac{1}{4}\mathbf{1}_{A_{\mathrm{sel}}}$, and then understand how it projects onto $\mathrm{SL}_2(\mathbb{F}_p)$.

**Some good features about** $\mathrm{SL}_2(\mathbb{Z})$:

(1) $\mathrm{SL}_2(\mathbb{Z})$ is virtually free, meaning that it has a finite index free subgroup.
(2a) $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$ closely related to Lie groups.

(2b) $\mathrm{SL}_2(\mathbb{Z})$ acts nicely on the $\mathbb{H}^2$ hyperbolic plane.

**Intuition about convolution on** $\mathrm{SL}_2(\mathbb{Z})$: As a warm-up, consider the convolution on $\mathbb{Z}$. Let $\mu = \frac{1}{2}(\delta_1+\delta_{-1})$. By the central limit theorem, $\mu^K$ can be approximated by Gaussian, which intimately relates to the heat kernel on $\mathbb{R}$. In light of this, we might hope that for a probability measure $M$ on $\mathrm{SL}_2(\mathbb{Z})$, there is some central limit theorem for matrices, and the convolution $M^{*K}$ would be related to the "heat kernel" on $\mathrm{SL}_2(\mathbb{R})$.

Consider the "ball" in $\mathrm{SL}_2(\mathbb{R})$ with radius $T$, defined as follows:

$$B_T := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : a^2+b^2+c^2+d^2 \le T^2 \right\}.$$

Moreover, we denote $B_T(\mathbb{Z}) := B_T \cap \mathrm{SL}_2(\mathbb{Z})$.

**Lemma 18.7.** *For $T$ large, we have $|B_T(\mathbb{Z})| \approx T^2$.*

*Proof sketch.* We need to count the solutions of $ad-bc=1, a,b,c,d \in \mathbb{Z}, a^2+b^2+c^2+d^2 \le T^2$. For a typical pair $(a,d) \in [-T,T]^2$, the number of pairs $(b,c) \in [-T,T]^2$ such that $bc = ad-1$ is at least 1, and at most $T^{o(1)}$. This suggests $|B_T(\mathbb{Z})| \approx T^2$. □

Vague statement: for large $K$, $M^{*K}$ is roughly equally distributed on $B_T(\mathbb{Z})$, where $T \sim \exp(c(M)\cdot K)$.

Let us see how a statement of this form about random walks on $SL_2(\mathbb{Z})$ leads to a spectral gap in $SL_2(\mathbb{F}_p)$.

**Lemma 18.8.** *If $\mu$ is symmetric, then $\|\mu^{*K}\|^2_{\ell^2(G)} = \mu^{*2K}(I)$, where $I \in G$ is the identity element.*

*Proof.* By definition we have

$$\|\mu^{*K}\|^2_{\ell^2(G)} = \sum_{g\in G} \mu^{*K}(g)^2 = \sum_{g\in G} \mu^{*K}(g)\mu^{*K}(g^{-1}) = \mu^{*2K}(I). \qquad \square$$

This leads us to examine $\|\mu_{A_{\mathrm{sel}}}^{*K}\|^2_{\ell^2(G)} = \mu_{A_{\mathrm{sel}}}^{*2K}(I)$, where $I \in SL_2(\mathbb{F}_p)$ is the identity. We can relate this to a measure on $SL_2(\mathbb{Z})$. To set this up, let $\Gamma_p \subset \mathrm{SL}_2(\mathbb{Z})$ be the pre-image of $I \in \mathrm{SL}_2(\mathbb{F}_p)$ under $\Pi_p$, i.e.,

$$\Gamma_p := \left\{ a,b,c,d \in \mathbb{Z}, ad-bc=1, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod p \right\}$$

Now we have

$$\|\mu_{A_{\mathrm{sel}}}^{*K}\|^2_{\ell^2(G)} = \mu_{A_{\mathrm{sel}}}^{*2K}(I_2) = \Pi_p(M_{\mathrm{sel}}^{*2K}(I)),$$

and by the vague statement, we expect

$$\Pi_p(M_{\mathrm{sel}}^{*2K}(I_2)) \approx \frac{|\Gamma_p \cap B_T(\mathbb{Z})|}{|B_T(\mathbb{Z})|}$$

where $T \sim \log p$. Since $\mathrm{SL}_2(\mathbb{F}_p)$ has size of order $p^3$, it is natural to expect that for large $T$, $\Gamma_p \cap B_T(\mathbb{Z})$ occupies nearly a $p^{-3}$-fraction in $B_T(\mathbb{Z})$. The following lemma shows that this is indeed the case.

**Lemma 18.9.** *For $T > p^2$, it holds that $|\Gamma_p \cap B_T(\mathbb{Z})| \lessapprox p^{-3}T^2$.*

*Proof.* For any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_p$, we have $p \mid b, p \mid c$, and thus $p^2 \mid bc = ad - 1$. Meanwhile, we have $p \mid a-1, p \mid d-1$, which implies $p^2 \mid (a-1)(d-1) = ad-a-d+1$. Altogether we conclude that $p^2 \mid a+d-2$. In light of this, we see that for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_p \cap B_T(\mathbb{Z})$, $a \in [-T, T]$ has at most $O(p^{-1}T)$ choices, and given $a$, $d$ satisfies $d \equiv -2-a \pmod{p^2}$ has at most $O(p^{-2}T)$ choices (here we use the fact that $T > p^2$). Finally, given $a, d$, $b, c$ satisfies $bc = ad - 1$ has at most $T^{o(1)}$ choices. Combining things together, we obtain the desired bound. □

*Proof sketch for Theorem 18.3.* Assuming the vague statement about random walks on $SL_2(\mathbb{Z})$ we can now assemble our ingredients to give a proof sketch of Selberg's theorem.

We pick $K$ such that $T \sim \exp(c(M_{\mathrm{sel}})K) \sim p^{1.1}$, and thus $K \leq C_0 \log p$ for a universal constant $C_0 > 0$. By the vague statement and Lemmas 18.8, 18.9, we have

$$\|\mu_{A_{\mathrm{sel}}}^{*K}\|_{\ell^2(G)}^2 \lessapprox \frac{|\Gamma_p \cap B_T(\mathbb{Z})|}{|B_T(\mathbb{Z})|} \lessapprox \frac{p^{-3}T^2}{T^2} = p^{-3}.$$

Applying Theorem 18.5, we obtain that $\sigma_1(T_{A_{\mathrm{sel}}})^K \lessapprox p^{-1}$. This yields that $\sigma_1(T_{A_{\mathrm{sel}}}) \leq 1 - c$ for some universal constant $c > 0$. □

**Connection to hyperbolic geometry**

Selberg's theorem is closely connected to hyperbolic geometry. In fact, Selberg's original theorem was about the eigenvalues of the Laplacian on certain hyperbolic manifolds. The hyperbolic manifold perspective also gives a nice approach to the vague statement in the proof sketch above. In this short section, we briefly introduce these ideas.

Recall that $\mathrm{SL}_2(\mathbb{Z})$ acts isometrically on $\mathbb{H}^2$. Let $X(p) = \mathbb{H}^2/\Gamma_p$. If $p$ is large, then the action is properly discontinuous, and so $X(p)$ is a hyperbolic surface. It is a complete surface with finite area and with some cusps. Note that $X(p)$ is a cover of $X(1)$, and the group of deck tranform of $X(p)$ is $\mathrm{SL}_2(\mathbb{F}_p)$. So the "large scale geometry" of $X(p)$ is closely related to the geometry of the Cayley graph of $SL_2(\mathbb{F}_p)$ with generators $A$, where $A$ is the reduction mod $p$ of some set of generators of $SL_2(\mathbb{Z})$. For instance, we could take $A = A_{sel}$.

Consider the spectrum of the Laplacian of $X(p)$. We have 0 lies in the spectrum, but above 0 there is a gap. Denote $\lambda_1(X(p))$ the smallest positive eigenvalue of

the Laplacian of $X(p)$. Selberg proved that $\lambda_1(X(p)) \geq \frac{3}{16}$ and conjectured that $\lambda_1(X(p)) \geq \frac{1}{4} - o(1)$. Because of the close connection between the geometry of $X(p)$ and the geometry of the Cayley graph of $SL_2(\mathbb{F}_p)$, it is not too hard to show that a lower bound for $\lambda_1(X(p))$ is equivalent to an upper bound for $\sigma_1(T_A)$, with $A$ as above.

The proof we sketched above can be translated into hyperbolic geometry using the heat kernel. The heat kernel describes a diffusion process on a Riemannian manifold, and it is a continuous analogue of a random walk. The heat kernel on a Riemannian manifold is written as $H_t(x, y)$, where $t$ represents time, and $x, y$ live in the Riemannian manifold. The probabilistic interpretation is that $H_t(x, y)dvol_y$ is the probability distribution for the position of a particle that started at $x$ and then diffused for time $t$.

We write $H_{t,X(p)}$ for the heat kernel on $X(p)$. We think of $H_{t,X(p)}$ as analogous to $\mu^{*k}$ in the proof sketch above, with $t$ analogous to $k$.

First big step: Prove that $H_{t,X(p)}$ is roughly evenly distributed on $X(p)$. We will discuss the proof of this more below.

In particular, we prove that there is a constant $C_0$ so that if $t = C_0 \log p$ and $x \in X(p)$, and for $t = C_0 \log p$, then

$$\|H_{t,X(p)}(x, y)\|^2_{L^2_y} \leq p^{-2.1}.$$

This is analogous to proving that $\|\mu^{*k}\|^2_{L^2(SL_2(\mathbb{F}_p)} \leq p^{-2.1}$. There is a close connection between the mixing properties of the heat kernel and the eigenvalues of the Laplacian on a Riemannian manifold. This connection is analogous to the trace formula that we used in the finite group setting. On a closed manifold, the formula has a simple form closely parallel to the formulas we used above. If we let $0 = \lambda_0 < \lambda_1 \leq \lambda_2 \leq ...$ be the spectrum of the Laplacian on a compact Riemannian manifold $M$, then we have

$$\sum_j e^{-2t\lambda_j} = \int_M H_{2t}(x, x)dvol = \int_{M\times M} H_t(x, y)^2 dxdy.$$

Since $X(p)$ is not compact, its spectral theory is a little more complicated, but this is a technical detail. This part of the proof is less elementary in the hyperbolic setting than in the finite group setting, but it is basically analogous.

Since $SL_2(\mathbb{F}_p)$ acts isometrically on $X(p)$, each eigenspace is a representation of $SL_2(\mathbb{F}_p)$. The main case is when the representation on the $\lambda_1$ eigenspace is nontrivial. Then it has dimension at least $(p-1)/2$ and so we get

$$\frac{p-1}{2} e^{-2t\lambda_1} \leq \int_{M\times M} H_t(x, y)^2 dxdy.$$

Then the first big step gives us, with $t = C \log p$,

$$\frac{p-1}{2} e^{-2t\lambda_1} \leq \int_{M \times M} H_t(x,y)^2 dx dy \lesssim p^3 p^{-2.1}$$

and so $e^{-2t\lambda_1} \leq p^{-.1}$, and so $\lambda_1 \geq c > 0$ uniformly in $p$.

Now we return to the first big step.

We write $H_{t,X(p)}$ for the heat kernel on $X(p)$ and $H_{t,\mathbb{H}}$ for the heat kernel on the hyperbolic plane. These two heat kernels are closely connected: $H_{t,X(p)}$ is the pushforward of $H_{t,\mathbb{H}}$ by the covering map $\Pi_p : \mathbb{H} \to X(p)$. In other words, if $\Pi_p(\tilde{x}) = x$ and $\Pi_p(\tilde{y} = y)$, then

$$H_{t,X(p)}(x,x) = \sum_{\gamma \in \Gamma_p} H_{t,\mathbb{H}}(\gamma \tilde{x}, \tilde{y}).$$

In particular, to do the first big step, we have to estimate

$$H_{2t,X(p)}(x,x) = \sum_{\gamma \in \Gamma_p} H_{2t,\mathbb{H}}(\gamma \tilde{x}, \tilde{x}).$$

This is analogous to estimate $M^{*k}(\Gamma_p)$ in the proof sketch above. This was a key moment in the proof sketch above where we made a vague statement. This part of the proof is easier in the hyperbolic context because there is a simple explicit formula for $H_{t,\mathbb{H}}$. Using this explicit formula and Lemma 18.9, it is fairly easy to prove the desired bounds for $H_{2t,X(p)}$. So this part of the proof is actually easier in the hyperbolic setting than in the finite group setting.

# 18.156 Projection Theory

Spring 2025