18.317 Combinatorics, Probability, and Computations on Groups	5 November 2001

Lecture 22

Lecturer: Igor Pak — *Scribe: Nate Ackerman*

Theorem 1 (This is a special case of the theorem from last class.)
Suppose $\Gamma = \Gamma(G, S)$, υ = *set of paths in* Γ, *and* $\gamma = \{\gamma_x\colon$ *path from id to* $x\}$. *Also suppose that* $\pi, \widetilde{\pi}$ *are symmetric,* $s \subseteq$ *support*(π), *diam* $\upsilon = \max_x |\gamma_x| = d$ *and* $\mu_s(x)$ = *number of generators* s *in* $\gamma_x = s_{i_1} s_{i_2} \cdots$.

Then $\mathcal{E}_\pi(\varphi, \varphi) \geq (1/|A|) \cdot \mathcal{E}_{\widetilde{\pi}}(\varphi, \varphi)$ *where* $A = d \cdot \max_{s \in S}(\max_{x \in G} \mu_s(x))/\pi(s)$.

We shall prove the following important corollary from the Theorem.

Lemma 2 *Suppose* $\mathcal{E}_{\widetilde{\pi}}(\varphi, \varphi) \leq A \cdot \mathcal{E}_\pi(\varphi, \varphi)\ \forall \varphi$. *Then*

$$1 - \widetilde{\lambda}_i \leq A(1 - \lambda_i),$$

where λ_i *are the eigenvalues of* M_π.

For every probability distribution π, consider the matrix

$$M_\pi = (a_{xy})_{|G| \times |G|}, a_{xy} = \pi(x^{-1}y)$$

Here it is important π is symmetric so all eigenvectors are real: $1 = \lambda_0 \geq \lambda_1 \geq \cdots \geq -1$.

Recall that $\mathcal{E}_\pi(\varphi, \varphi) = \langle (I - P_\pi)\varphi, \varphi \rangle$, where P_π is exactly convolution with π. Then M_π is then exactly the matrix of that operation.
Consider the scalar product of a function and an operator on that function.

Lets call this operation $Q = I - P_\pi$.

Lemma 3 *For every symmetric operator* Q,

$$\min_\varphi \frac{\langle Q\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle}$$

is equal to the smallest eigenvalue of Q.

Proof: To see this let us look at it the other way. We see easily from linear algebra that $\max_\varphi \langle Q\varphi, \varphi \rangle / \langle \varphi, \varphi \rangle$ is just the maximal eigenvalue of Q. Similarly

$$\min_\varphi \frac{\langle Q\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} = \min_{\varphi\colon\, \Sigma\varphi = 0} \frac{\langle Q\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} = \lambda_1$$

∎

We just need one more well known result from linear algebra to complete the proof of Lemma 2.

Theorem 4 (min-max principle)
Let Q be a symmetric linear operator on V with eigenvalues $q_0 \leq q_1 \leq \cdots \leq q_n$. Let $m(W) = \min\{\langle Qf, f\rangle / \langle f, f\rangle : f \in W \subseteq V\}$. Then

$$q_i = \max\{m(W) : dim(W) = i\}$$

This follows when you consider vector spaces generated by first i eigenvectors.

This is all we need to complete the proof of Lemma 2. Indeed, Theorem 4 implies: $1 - \widetilde{\lambda_i} \leq A(1 - \lambda_i)$. Therefore $\lambda_1 \leq 1 - (1 - \widetilde{\lambda_1})/A$

Let $\widetilde{\pi} = U(G) =$ uniform distribution on the group, and let $\pi = U(S)$ be a uniform distribution on the generating set. Assume our generating set is the whole group ($S = G$). Then the transition matrix $M_{\widetilde{\pi}}$ is given by

$$\frac{1}{|G|}\begin{pmatrix} 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

This matrix has an eigenvalue of 1. But, because it also has rank 1, we know that all remaining eigenvalues are 0. Thus, $\lambda_0 = 1$, $\lambda_i = 0$, and therefore $\widetilde{\lambda_1} = 0$. Finally, we conclude $\lambda_1 \leq 1 - 1/A$
Recall that

$$A = d \cdot \max_{s \in S} \max_{g \in G} \frac{\mu_s(x)}{\pi(s)},$$

where $d = \text{diameter}(\gamma)$, and $\pi(s) = 1/|S|$ since π is the uniform distribution. Therefore,

$$A = d \cdot |S| \cdot \max_{s \in S} N_\gamma(S, G),$$

and we obtain:

Theorem 5 *Let G be a finite group, let $S = S^{-1}$ be a symmetric generating set, and let $\Gamma = \Gamma(G, S)$ be a Cayley graph with diameter d. Then*

$$\lambda_1 \leq 1 - \frac{1}{A} \leq 1 - \frac{1}{d \cdot |S| \cdot N_\gamma} \leq 1 - \frac{1}{d^2\,|S|},$$

where $N_\gamma = \max_{s \in S} N_\gamma(S, G)$.

Corollary 6

a) The relaxation time $\tau_1 = 1/(1 - \lambda_1) \leq d \cdot |S| \cdot N_\gamma$.

b) The mixing time of the lazy random walk $\mathcal{W}$ on $\Gamma(G, S)$ satisfies:

$$\tau_3 \leq d \cdot |S| \cdot N_\gamma \log |G| \leq d^2 |S| \log |G|$$

Part b) in the corollary follows from part a) and $\tau_3^* \leq \tau_1 \log |G|$, where * refers to the lazy random walk. Now, let us consider several special cases

<u>Example 1</u> Let $G = \mathbb{Z}_n$, $S = \{\pm 1\}$.
The corollary gives mix $= O(n^2 \log(n))$, which is slightly weaker from the tight bound mix $= O(n^2)$.

Example 2 Let $G = \mathbb{Z}_2^n$, $S = \{(a_1, \cdots, a_n) : a_i = 1$ and the rest are 0, for $1 \leq i \leq n\}$.
To calculate the mixing time we need the diameter (d) and $|S|$. Since d=n, and $|S| = n$, we obtain

$$\tau_3^* \leq d^2|S|\log|G| = O(n^4).$$

On the other hand, a stronger inequality $\tau_3^* \leq d|S|N_\gamma \log|G|$ gives us a better (but still not great) upper bound. Indeed, since $N_\gamma = 1$, we get $\tau_3^* \leq O(n^3)$. This should be compared with $\tau_3^* = O(n\log n)$ we obtained by a stopping times argument.

Example 3 Let $G = S_n$, $R = \{(12)(13)\cdots(1n)\}$ Consider $d = \operatorname{diam}\Gamma(S_n, R))$. The largest distance to identity has a permutation $g = (23)(45)\cdots(2m, 2m+1), n = 2m+1$.
This implies that

$$\operatorname{diam}\Gamma(S_n, R) =\sim 3/2n + O(1).$$

We also have $|S| = n - 1 = O(n)$, and $\log|G| = O(n\log(n))$, so, mix $\leq d^2|R|\log|G| \leq O(n^4\log(n))$.

On the other hand, we know that N_γ is small. In fact, an easy check shows that N_γ is at most 2, and so

$$\text{mix} \leq d\,|R|\,N_\gamma \log|G| = O(n^3\log(n))$$

Recall that by a stopping time argument we obtained a tight upper bound of $O(n\log n)$ in this case.

Example 4 Let $G = S_n$, $R = \{(ij) : 1 \leq i < j \leq n\}$
We can do a similar stopping argument to show that in fact mix= $Cn\log(n)$.
However, the upper bound given by corollary is not nearly that good. We have: $|R| = O(n^2)$, $d = O(n)$, and $N_\gamma = 1$. Therefore, have mix$\leq d\,N_\gamma\,|R|\log|G| = O(n^4\log(n))$.

This is another example of weakness of the bound given by Corollary 6. The larger the generating set, the bigger the bound on the mixing time. This is unfortunate, as the larger the generating set, the smaller the mixing time tends to be.

Multicomodity flows
Imagine we have an industrial structure that looks like a Cayley graph, and each place has to trade commodities with the other places. In particular between any two plans 1 commodity must flow. However, the 1 unit flow along different paths. All that matters is that the sum total of the flow is 1 unit (so the flows look like a probability distribution on the paths between any two sites.)

Let $\gamma = \{\gamma_x =$ flow from id to x in $G\}$. So γ_x can consist of several different paths so long as the flows add to 1.

$N_\gamma = \max_{s\in S}\max_{x\in S}\mu_s(\gamma_x)$ (= expected number of times s occurs in a path from id to x)

Claim Theorem 1 and Corollary 6 remain correct under this generalization.

Corollary 7 *If $\Gamma = \Gamma(G, S)$ is vertex transitive. (e.g. if $H \subseteq$Aut(G) then H acts transitively on S) Then the relaxation time $\tau_1 = O(d^2)$, and the mixing time $\tau_3 = O(d^2\log|G|)$*

Indeed, consider a uniform distribution on all paths giving a shortest decomposition of an element. Then $N_\gamma = d/|S|$, and we have $d|S|N_\gamma = d^2$. In a special case of the Example 4 the corollary gives $O(n^3\log n)$ bound now.