

Lecture 3

Instructor: Salil Vadhan

Scribe: Abhishek Sharma

1 Recap / Correction from Last Time

Complete graphs without self-loops

1. The Laplacian matrix of a complete graph has eigenvalues $\lambda_2 = \lambda_3 = \dots = \lambda_n = n - d + 1$
2. Largest possible value of $\lambda_2/d = n/(n - 1)$.

Proof. Let L be the Laplacian of any d -regular graph.

$$d \cdot n = \text{Tr}(L) = \sum_{i=1}^n \lambda_i \geq (n - 1)\lambda_2$$

$$\implies \frac{n}{n - 1} \geq \frac{\lambda_2}{d}$$

□

This means that *asymptotically*, $\lambda_2/d \rightarrow 1$, but it can take a higher value (it is 2 for $n = 2$).

3. Largest possible value of $\lambda_n/d = 2$ (we will see this in more detail in a later class; it is achieved in any connected bipartite graph).

2 Diagonalization on \mathbb{C}

Theorem 1 (Spectral Theorem on \mathbb{R}). *Let $M \in \mathbb{R}^{n \times n}$ ($n \times n$ real matrices), then the following are equivalent (TFAE):*

1. *There exists an orthonormal basis $v_1, \dots, v_n \in \mathbb{R}^n$ of **real** eigenvectors of M*
2. *$M = V\Lambda V^T$ for **orthogonal** matrix $V \in \mathbb{R}^{n \times n}$ and diagonal $\Lambda \in \mathbb{R}^{n \times n}$*
3. *M is symmetric*

But what are the complex analogues of the above objects?

- For $z = x + iy \in \mathbb{C}$, $z^* = x - iy$
- For $v \in \mathbb{C}^n$, $M \in \mathbb{C}^{n \times n}$, v^* , M^* are called *conjugate transposes*
- $\|v\| = \sqrt{v^*v}$ (norm), $\langle v, w \rangle = v^*w$ (inner product)
- Orthonormal basis of $\mathbb{C}^{n \times n}$: $v_1, \dots, v_n \in \mathbb{C}^n$ s.t. $\langle v_i, v_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$
- Unitary matrix $V \in \mathbb{C}^{n \times n}$: $V^*V = I$
- M is Hermitian if $M^* = M$

Theorem 2. For $M \in \mathbb{C}^{n \times n}$, the following are equivalent:

1. There exists orthonormal basis $v_1, \dots, v_n \in \mathbb{C}^n$ of **complex** eigenvectors of M
2. $M = V^* \Lambda V$ for unitary V and diagonal Λ
3. M is normal: $M^* M = M M^*$. Note: This is a more general condition than M being Hermitian or symmetric (even for real matrices).

3 Groups

Definition 3 (Group). A group is a set Γ with a binary operation \circ such that:

1. $\forall x, y, z \in \Gamma, (x \circ y) \circ z = x \circ (y \circ z)$ (associativity)
2. $\exists e \in \Gamma$ s.t. $\forall x \in \Gamma, e \circ x = x \circ e = x$ (identity)
3. $\forall x \in \Gamma, \exists y \in \Gamma, x \circ y = y \circ x = e$ (inverses)

Definition 4 (Abelian Group). A group (Γ, \circ) is abelian if $\forall x, y \in \Gamma: x \circ y = y \circ x$ (commutativity).

Examples of groups

1. $(\mathbb{R}, +)$ - addition on the set of real numbers
2. $(\mathbb{R}^{n \times n}, +)$ - addition of the set of real, square matrices
3. $(\mathbb{Z}, +)$ - addition of the set of integers
4. $\mathbb{Z}_n = (\{0, \dots, n-1\}, + \text{ mod } n) \cong \mathbb{Z}/n\mathbb{Z}$ - integers "modulo" equivalence relation ($a \equiv b$ if $n|a-b$; ' \cong ': 'congruent to')
5. $(\{0, 1\}^d, \text{bitwise } \oplus) \cong (\mathbb{Z}/2\mathbb{Z})^d$ - bitwise xor on the d -dimensional hypercube
6. Every finite abelian group is $\cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$
7. $\mathbb{R}^* = (\mathbb{R} - \{0\}, \times), \mathbb{C}^* = (\mathbb{C} - \{0\}, \times)$
8. $S^1 = (\{z \in \mathbb{C} : |z| = 1\}, \times)$ (where inverse of $z = z^*$)
9. $(n \times n$ invertible real matrices, \times) - nonabelian when $n > 1$
10. $(n \times n$ unitary complex matrices, \times) - nonabelian when $n > 1$

4 General Cayley Digraphs

Definition 5 (Cayley Digraph). For a finite group $(\Gamma, +)$ and a subset $S \subseteq \Gamma$, $\text{Cay}(\Gamma, S)$ is the $|S|$ -regular digraph with

- vertex set: Γ
- edges: $\{(x, x+s) : s \in S\}$

It is connected iff S "generates" Γ .

Examples

1. Hypercube: $\Gamma = \{0, 1\}^d$, $S = \{e_1, \dots, e_d\}$
2. Directed n -cycle: $\Gamma = \mathbb{Z}_n$ (which is abelian), $S = \{1\}$
3. Undirected n -cycle: $\Gamma = \mathbb{Z}_n$, $S = \{1, -1\} = \{1, n-1\}$
4. Complete graph (with self-loops): $S = \Gamma$

Weighted Cayley Digraphs

Definition 6 (Weighted Cayley Digraphs). *Given a weight function on the group, $w_0 : \Gamma \rightarrow \mathbb{R}^{\geq 0}$, $\text{Cay}(\Gamma, w_0)$ has:*

- *vertex set:* Γ
- *edge weights:* $w(a, b) = w_0(b - a)$
- *d -regular with $d = \sum_{s \in \Gamma} w_0(s)$*

Note that this definition is more general than the previous one. More specifically, $\text{Cay}(\Gamma, S) = \text{Cay}(\Gamma, \mathbf{1}_S)$, where $\mathbf{1}_S$ is the indicator for set S .

Example: Noisy Hypercube, NH_p for $p \in [0, 1]$

For $s \in \{0, 1\}^d$:

$$\begin{aligned} w(s) &= p^{|s|} \cdot (1-p)^{d-|s|} \\ &= \Pr(s) = \text{Bern}(p)^d \end{aligned}$$

where $|s|$ is the number of 1's in s (which is the 'Hamming weight' of s).

Finite abelian groups

Let Γ be a finite abelian group, $S \subseteq \Gamma$, then:

1. M is the adjacency matrix of $\text{Cay}(\Gamma, S)$
2. $W = M/d$ is the random walk matrix, where $d = |S|$
3. $L = I - W$ is the normalized Laplacian

Claim 7. M (and hence W, L) is normal

Proof. We note that the M is a real matrix, and M^*M, MM^* have nice interpretations themselves (in terms of Cayley graphs):

$$\begin{aligned} M^*M &= M^T M = \text{Cay}(\Gamma, \{s-t : s, t \in S\}) \\ MM^* &= MM^T = \text{Cay}(\Gamma, \{-s+t : s, t \in S\}) \end{aligned}$$

where the sets $\{s-t : s, t \in S\}, \{-s+t : s, t \in S\}$ are with multiplicity. Because the group is abelian, we will have the two sets being the same. ■

In general, for every S, T , $\text{Cay}(\Gamma, S)$ and $\text{Cay}(\Gamma, T)$ commute with each other (i.e. their adjacency matrices commute). This further implies that the adjacency matrices have a common diagonalization, with a common basis for all choices of S, T . The Fourier eigenbasis is that basis, and lets us get an explicit handle on what that basis is.

5 Fourier eigenbasis

Theorem 8. Assume Γ to be abelian. An orthogonal set of **complex** eigenvectors for $\text{Cay}(\Gamma, S)$ (for M, L , and W) is given by the set of characters $\chi : \Gamma \rightarrow \mathbb{C}$, where:

$$\begin{aligned} \chi : \Gamma &\rightarrow S' \subseteq \mathbb{C} \\ \text{s.t. } \forall x, y : \quad \chi(x+y) &= \chi(x)\chi(y) && (\text{homomorphism}) \end{aligned}$$

Examples

1. Characters for $\mathbb{Z}_n = (\{0, \dots, n-1\}, + \text{ mod } n)$: $\chi_r(x) = e^{2\pi i r x / n}$, $r \in \{0, \dots, n-1\}$.

For $n = 4$:

	$\chi(0)$	$\chi(1)$	$\chi(2)$	$\chi(3)$
$r = 0$	1	1	1	1
$r = 1$	1	i	-1	-i
$r = 2$	1	-1	1	-1
$r = 3$	1	-i	-1	i

2. Characters for hypercube $\cong \mathbb{Z}_2^d$:

For $r \in \{0, 1\}^d$:

$$\begin{aligned} \chi_r(x) &= (-1)^{r_1 x_1} (-1)^{r_2 x_2} \dots (-1)^{r_n x_n} \\ &= (-1)^{\langle r, x \rangle} \end{aligned}$$

6 Calculating eigenvalues

$$\begin{aligned} (M\chi)(a) &= \sum_{b \in \Gamma} M(a, b)\chi(b) \\ &= \sum_{b \in \Gamma} w(b, a)\chi(b) \\ &= \sum_{b \in \Gamma} w_0(a-b)\chi(b) \\ &= \sum_{s \in \Gamma} w_0(s)\chi(a-s) \\ &= \sum_{s \in \Gamma} w_0(s)\chi(a)\chi(-s) && (\text{homomorphism}) \\ &= \chi(a) \sum_{s \in \Gamma} w_0(s)\chi(s)^* && \left(= \chi(a) \sum_{s \in \Gamma} \chi(s)^* \text{ for unweighted case} \right) \\ &= \chi(a)\lambda_\chi \end{aligned}$$

Here we find that the eigenvalue corresponding to the eigenvector χ is $\sum_{s \in \Gamma} w_0(s)\chi(s)^*$

7 Exercise for the next class

1. Work out the n eigenvalues of directed n -cycle (Trevisan does undirected n -cycles)
2. Work out the 2^d eigenvalues of the Noisy Hypercube, NH_p (Trevisan does ordinary hypercube)