Spectral Graph Theory Lecture 5

Rings, Paths, and Paley Graphs

Daniel A. Spielman September 12, 2012

5.1 About these notes

These notes are not necessarily an accurate representation of what happened in class. The notes written before class say what I think I should say. The notes written after class way what I wish I said.

All statements in these notes that can be made mathematically rigorous should be taken with a grain of salt and a shot of Tequila.

5.2 Overview

This lecture is devoted to an examination of some special graphs and their eigenvalues.

5.3 The Ring Graph

The ring graph on n vertices, R_n, may be viewed as having a vertex set corresponding to the integers modulo n. In this case, we view the vertices as the numbers 0 through $n-1$, with edges $(i, i+1)$, computed modulo n.

Lemma 5.3.1. *The Laplacian of R_n has eigenvectors*

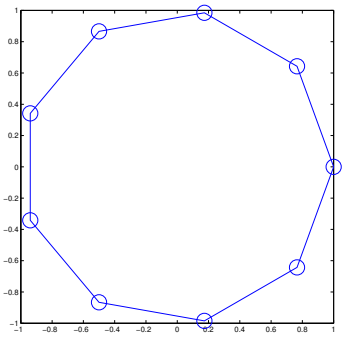
$$\boldsymbol{x}_k(u) = \cos(2\pi ku/n), \text{ and}$$
$$\boldsymbol{y}_k(u) = \sin(2\pi ku/n),$$

for $0 \leq k \leq n/2$, ignoring $\boldsymbol{y}_0$ which is the all-zero vector, and for even n ignoring $\boldsymbol{y}_{n/2}$ for the same reason. Eigenvectors $\boldsymbol{x}_k$ and $\boldsymbol{y}_k$ have eigenvalue $2 - 2\cos(2\pi k/n)$.

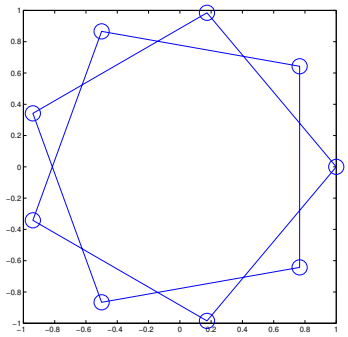
Note that $\boldsymbol{x}_0$ is the all-ones vector. When n is even, we only have $\boldsymbol{x}_{n/2}$, which alternates ± 1.

Proof. We will first see that $\boldsymbol{x}_1$ and $\boldsymbol{y}_1$ are eigenvectors by drawing the ring graph on the unit circle in the natural way: plot vertex u at point $(\cos(2\pi u/n), \sin(2\pi u/n))$.

You can see that the average of the neighbors of a vertex is a vector pointing in the same direction as the vector associated with that vertex. This should make it obvious that both the x and y coordinates in this figure are eigenvectors of the same eigenvalue. The same holds for all k.



(a) The ring graph on 9 vertices.



(b) The eigenvectors for $k = 2$.

Figure 5.1:

Alternatively, we can verify that these are eigenvectors by a simple computation.

$$\begin{aligned}
\left(L_{R_n}\boldsymbol{x}_k\right)(u) &= 2\boldsymbol{x}_k(u) - \boldsymbol{x}_k(u+1) - \boldsymbol{x}_k(u-1) \\
&= 2\cos(2\pi ku/n) - \cos(2\pi k(u+1)/n) - \cos(2\pi k(u-1)/n) \\
&= 2\cos(2\pi ku/n) - \cos(2\pi ku/n)\cos(2\pi k/n) + \sin(2\pi ku/n)\sin(2\pi k/n) \\
&\qquad\qquad - \cos(2\pi ku/n)\cos(2\pi k/n) - \sin(2\pi ku/n)\sin(2\pi k/n) \\
&= 2\cos(2\pi ku/n) - \cos(2\pi ku/n)\cos(2\pi k/n) - \cos(2\pi ku/n)\cos(2\pi k/n) \\
&= (2 - 2\cos(2\pi k/n))\cos(2\pi ku/n) \\
&= (2 - \cos(2\pi k/n))\boldsymbol{x}_k(u).
\end{aligned}$$

The computation for $\boldsymbol{y}_k$ follows similarly. □

5.4 The Path Graph

We will derive the eigenvalues and eigenvectors of the path graph from those of the ring graph. To begin, I will number the vertices of the ring a little differently, as in Figure 5.2.

It should be clear by now that re-naming the vertices does not change the eigenvalues of the graphs and merely permutes the eigenvectors appropriately. To see this in a mathematically formal way, observe that any permutation can be represented by a permutation matrix Π. That is, a matrix that is all zeros except for exactly one 1 in each row and column. Permutation matrices are orthonormal, so $\Pi\Pi^T = I$. If we permute the vertices according to the permutation encoded by Π, we must permute the rows and columns of the corresponding matrix. That is, we multiply by Π^T on the left and by Π on the right. So, what I said at the beginning of the paragraph amounts to

$$\boldsymbol{L}\boldsymbol{\psi} = \lambda\boldsymbol{\psi} \qquad \Longleftrightarrow \qquad (\Pi^T\boldsymbol{L}\Pi)(\Pi^T\boldsymbol{\psi}) = \lambda(\Pi^T\boldsymbol{\psi}).$$

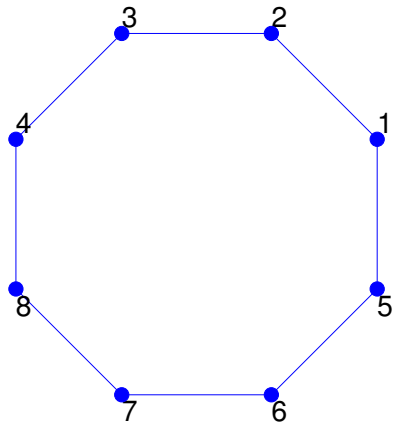


Figure 5.2: The ring on 8 vertices, numbered differently

Lemma 5.4.1. *Let $P_n = (V, E)$ where $V = \{1, \ldots, n\}$ and $E = \{(i, i+1) : 1 \leq i < n\}$. The Laplacian of P_n has the same eigenvalues as R_{2n}, namely $2(1 - \cos(\pi k/n))$, and eigenvectors*

$$\boldsymbol{v}_k(u) = \cos(\pi k u/n - \pi k/2n).$$

for $0 \leq k < n$

Proof. We derive the eigenvectors and eigenvalues by treating P_n as a quotient of R_{2n}: we will identify vertex u of P_n with vertices u and $u + n$ of R_{2n} (under the new numbering of R_{2n}). These are pairs of vertices that are above each other in the figure that I drew.

Let $\boldsymbol{I}_n$ be the n-dimensional identity matrix. You should check that

$$\begin{pmatrix} \boldsymbol{I}_n & \boldsymbol{I}_n \end{pmatrix} \boldsymbol{L}_{R_{2n}} \begin{pmatrix} \boldsymbol{I}_n \\ \boldsymbol{I}_n \end{pmatrix} = 2\boldsymbol{L}_{P_n}.$$

If there is an eigenvector $\boldsymbol{\psi}$ of R_{2n} with eigenvalue λ for which $\boldsymbol{\psi}(u) = \boldsymbol{\psi}(u + n)$ for $1 \leq u \leq n$, then the above equation gives us a way to turn this into an eigenvector of P_n: Let $\boldsymbol{\phi} \in \mathbb{R}^n$ be the vector for which

$$\boldsymbol{\phi}(u) = \boldsymbol{\psi}(u), \text{for } 1 \leq u \leq n.$$

Then,

$$\begin{pmatrix} \boldsymbol{I}_n \\ \boldsymbol{I}_n \end{pmatrix} \boldsymbol{\phi} = \boldsymbol{\psi}, \quad \boldsymbol{L}_{R_{2n}} \begin{pmatrix} \boldsymbol{I}_n \\ \boldsymbol{I}_n \end{pmatrix} \boldsymbol{\psi} = \lambda \boldsymbol{\psi}, \quad \text{and} \quad \begin{pmatrix} \boldsymbol{I}_n & \boldsymbol{I}_n \end{pmatrix} \boldsymbol{L}_{R_{2n}} \begin{pmatrix} \boldsymbol{I}_n \\ \boldsymbol{I}_n \end{pmatrix} \boldsymbol{\psi} = 2\lambda \boldsymbol{\phi}.$$

So, if we can find such a vector $\boldsymbol{\psi}$, then the corresponding $\boldsymbol{\phi}$ is an eigenvector of P_n of eigenvalue λ.

As you've probably guessed, we can find such vectors $\boldsymbol{\psi}$. I've drawn one in Figure 5.2. For each of the two-dimensional eigenspaces of R_{2n}, we get one such a vector. These provide eigenvectors of eigenvalue

$$2(1 - \cos(\pi k/n)),$$

for $1 \leq k < n$. Thus, we now know $n-1$ distinct eigenvalues. The last, of course, is zero. □

5.5 Cayley Graphs

The ring graph is a type of Cayley graph. In general, the vertices of a Cayley graph are the elements of some group Γ. In the case of the ring, the group is the set of integers modulo n. The edges of a Cayley graph are specified by a set $S \subset \Gamma$, which are called the *generators* of the Cayley graph. Vertices $u, v \in \Gamma$ are connected by an edge if there is an $s \in S$ such that

$$u \circ s = v,$$

where $\circ$ is the group operation. In the case of Abelian groups, like the integers modulo n, this would usually be written $u + s = v$. To guarantee that the graph is undirected, we must insist that the inverse of every $s \in S$ also appear in S. In the case of the ring graph, the generators are $\{1, -1\}$.

Many of the most interesting graphs are Cayley graphs. We have seen at least one other: the hybercube.

5.6 Paley Graphs

The Paley graph are Cayley graphs over the group of integer modulo a prime, p, where p is equivalent to 1 modulo 4. Such a group is often written $\mathbb{Z}/p$.

I should begin by reminding you a little about the integers modulo p. The first thing to remember is that the integers modulo p are actually a field, written $\mathbb{F}_p$. That is, they are closed under both addition and multiplication (completely obvious), have identity elements under addition and multiplication (0 and 1), and have inverses under addition and multiplication. It is obvious that the integers have inverses under addition: $-x$ modulo p plus x modulo p equals 0. It is a little less obvious that the integers modulo p have inverses under multiplication. That is, for every $x \neq 0$, there is a y such that $xy = 1$ modulo p. When we write $1/x$, we mean this element y. I'll quickly explain to some of you why these inveses exist. Recall that the greatest common divisor of p and a number x that is not divisible by p is equal to 1. If we use the extended version of Euclid's algorithm to compute the gcd of x and p, we obtain an a and b such that

$$ax + bp = 1 \implies ax \equiv_p 1.$$

The generators of the Paley graphs are the *quadratic residues* modulo p. That is, the set of numbers s such that there exits an x for which $x^2 \equiv_p s$. That is, the vertex set is $\{0, \ldots, p-1\}$, and there is an edge between vertices u and v if $u - v$ is a square modulo p. I should now prove that $-s$ is a quadratic residue if and only if s is. This will hold provided that p is equivalent to 1 modulo 4. To prove that, I need to tell you one more thing about the integers modulo p: their multiplicative group is cyclic.

Fact 5.6.1. *For every prime p, there exists a number g such that for every number x between 1 and $p-1$, there is an i between 1 and $p-1$ such that*

$$x \equiv g^i \mod p.$$

In particular, $g^{p-1} \equiv 1$.

Corollary 5.6.2. *If p is a prime equivalent to 1 modulo 4, then -1 is a square modulo p.*

Proof. We know that 4 divides $p-1$. Let $s = g^{(p-1)/4}$. I claim that $s^2 = -1$. This will follow from $s^4 = 1$.

To see this, consider the equation

$$x^2 - 1 \equiv 0 \mod p.$$

As the numbers modulo p are a field, it can have at most 2 solutions. Moreover, we already know two solutions, $x = 1$ and $x = -1$. As $s^4 = 1$, we know that s^2 must be one of 1 or -1. However, it cannot be the case that $s^2 = 1$, because then the powers of g would begin repeating after the $(p-1)/2$ power, and thus could not represent every number modulo p. □

We now understand a lot about the squares modulo p (formally called *quadratic residues*). The squares are exactly the elements g^i where i is even. As $g^i g^j = g^{i+j}$, the fact that -1 is a square implies that s is a square if and only if $-s$ is a square. So, S is closed under negation, and the Cayley graph of $\mathbb{Z}/p$ with generator set S is in fact a graph. As $|S| = (p-1)/2$, it is regular of degree

$$d = \frac{p-1}{2}.$$

5.7 Eigenvalues of the Paley Graphs

It will prove simpler to compute the eigenvalues of the adjacency matrix of the Paley Graphs. Since these graphs are regular, this will immediately tell us the eigenvalues of the Laplacian. Let $\boldsymbol{A}$ be the adjacency matrix of the Paley graph on p vertices. We will prove that

$$\boldsymbol{A}^2 = \frac{p-1}{4}(\boldsymbol{I} + \boldsymbol{J}) - \boldsymbol{A}, \tag{5.1}$$

where $\boldsymbol{J}$ is the all-1's matrix. This gives us a quadratic equation that every eigenvalue other than d must obey. Let $\boldsymbol{\phi}$ be an eigenvector of $\boldsymbol{A}$ of eigenvalue $\mu \neq 0$. As $\boldsymbol{\phi}$ is orthogonal to the all-1s vector, $\boldsymbol{J}\boldsymbol{\phi} = \boldsymbol{0}$. So,

$$\mu^2\boldsymbol{\phi} = \boldsymbol{A}^2\boldsymbol{\phi} = \frac{p-1}{4}\boldsymbol{I}\boldsymbol{\phi} - \boldsymbol{A}\boldsymbol{\phi} = (\frac{p-1}{4} - \mu)\boldsymbol{\phi}.$$

So, we find

$$\mu^2 + \mu - \frac{p-1}{4} = 0.$$

This gives

$$\mu = \frac{1}{2}\left(-1 \pm \sqrt{p}\right).$$

Let's prove it. It will be easiest to think in terms of the *quadratic character*:

$$\chi(x) = \begin{cases} 1 & \text{if } x \text{ is a quadratic residue modulo } p \\ 0 & \text{if } x = 0, \text{ and} \\ -1 & \text{otherwise.} \end{cases}$$

This is called a character because it satisfies $\chi(xy) = \chi(x)\chi(y)$. We will use this to define a matrix $\boldsymbol{M}$ by

$$\boldsymbol{M}(u, v) = \chi(u - v).$$

Note that

$$\boldsymbol{A} = \frac{1}{2}\left(\boldsymbol{M} + \boldsymbol{J} - \boldsymbol{I}\right). \tag{5.2}$$

Lemma 5.7.1.

$$\boldsymbol{M}^2 = p\boldsymbol{I} - \boldsymbol{J}.$$

When combined with (5.2), this lemma immediately implies (5.1).

Proof. The diagonal entries of $\boldsymbol{M}^2$ are the squares of the norms of the columns of $\boldsymbol{M}$. As each contains $(p-1)/2$ entries that are 1, $(p-1)/2$ entries that are -1, and one entry that is 0, its squared norm is $p - 1$.

To handle the off-diagonal entries, we observe that $\boldsymbol{M}$ is symmetric, so the off-diagonal entries are the inner products of columns of $\boldsymbol{M}$. That is,

$$\boldsymbol{M}(u, v) = \sum_x \chi(u - x)\chi(v - x) = \sum_y \chi(y)\chi((v - u) + y),$$

where we have set $y = u - x$. For convenience, set $w = v - u$, so we can write this more simply. As we are considering a non-diagonal entry, $w \neq 0$. The term in the sum for $y = 0$ is zero. When $y \neq 0$, $\chi(y) \in \pm 1$, so

$$\chi(y)\chi(w + y) = \chi(w + y)/\chi(y) = \chi(w/y + 1).$$

Now, as y varies over $\{1, \ldots, p-1\}$, w/y varies over all of $\{1, \ldots, p-1\}$. So, $w/y - 1$ varies over all elements other than 1. This means that

$$\sum_y \chi(y)\chi((v - u) + y), = \left(\sum_{z=0}^{p-1} \chi(z)\right) - \chi(1) = 0 - 1 = -1.$$

So, every off-diagonal entry in $\boldsymbol{M}$ is -1. □

5.8 Implications

Let's see what the eigenvalues of $\boldsymbol{A}$ tell us about the graph. First, let's examine Hoffman's bound on the size of the largest independent set. If G is a Paley graph and S is an independent set,

Hoffman's bound tells us that

$$\begin{aligned}|S| &\leq n\frac{-\mu_n}{d-\mu_n}\\ &= p\frac{(\sqrt{p}+1)/2}{(p-1)/2+(\sqrt{p}+1)/2}\\ &= p\frac{\sqrt{p}+1}{p+\sqrt{p}}\\ &= \sqrt{p}.\end{aligned}$$

Until recently, there were no significantly better upper bounds on the sizes of independent sets in any explicitly constructed graphs whose degree was half its number of vertices.

In Lecture 2, we proved that for every subset of vertices S,

$$|\partial(S)| \geq \lambda_2 |S| (|V| - |S|)/n.$$

For a Paley graph, we have

$$\lambda_2 = d - \mu_2 = \frac{p-1}{2} - \frac{1}{2}(\sqrt{p}-1).$$

For now, I just want to point out that this number is very close to d, which is close to $p/2$. To interpret the lower bound we obtain on the size of the boundary of S, consider how many edges we would expect to find on the boundary of S if we chose a graph uniformly at random, with every edge appearing with probability $1/2$. There are $|S|\,|V-S|$ edges that could possibly appear on the boundary, and we would expect half of them to appear in a random graph. So, the number of edges on the boundary of every set in a Paley graph is at least a number just slightly lower than what we could expect to find in a random graph. This is one of the reasons that Paley graphs have been called quasi-random graphs [**?**].

5.9 Acknowledgment

I thank Zeyuan Allen Zhu for pointing out a mistake in my 2009 lecture notes on the path graph.