Spectral Graph Theory Lecture 5

Cayley Graphs

Daniel A. Spielman September 12, 2018

5.1 Cayley Graphs

Ring graphs and hypercubes are types 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. The set of generators must be closed under inverse. That is, if $s \in S$, then $s^{-1} \in S$. 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 $u + s = v$. The generators of the ring graph are $\{1, -1\}$.

The d-dimensional hypercube, H_d, is a Cayley graph over the additive group $(\mathbf{Z}/2\mathbf{Z})^d$: that is the set of vectors in $\{0,1\}^d$ under addition modulo 2. The generators are given by the vectors in $\{0,1\}^d$ that have a 1 in exactly one position. This set is closed under inverse, because every element of this group is its own inverse.

We require S to be closed under inverse so that the graph is undirected:

$$u + s = v \qquad \Longleftrightarrow \qquad v + (-s) = u.$$

Cayley graphs over Abeliean groups are particularly convenient because we can find an orthonormal basis of eigenvectors without knowing the set of generators. They just depend on the group[1]. Knowing the eigenvectors makes it much easier to compute the eigenvalues. We give the computations of the eigenvectors in sections **??** and A.

We will now examine two exciting types of Cayley graphs: Paley graphs and generalized hypercubes.

5.2 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 $\mathbb{Z}/p$.

[1]More precisely, the characters always form an orthonormal set of eigenvectors, and the characters just depend upon the group. When two different characters have the same eigenvalue, we obtain an eigenspace of dimension greater than 1. These eigenspaces do depend upon the choice of generators.

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 (except that 0 does not have a multiplicative inverse). 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.

The generators of the Paley graphs are the squares modulo p (usually called the *quadratic residues*). That is, the set of numbers s such that there exits an x for which $x^2 \equiv_p s$. Thus, 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 5.2.1. *For every prime p, there exists a number g such that for every number x between 1 and $p-1$, there is a unique i between 1 and $p-1$ such that*

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

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

Corollary 5.2.2. *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

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

5.3 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 $\boldsymbol{L}$ be

the Laplacians matrix of the Paley graph on p vertices. A remarkable feature of Paley graph is that $\boldsymbol{L}^2$ can be written as a linear combination of $\boldsymbol{L}$, $\boldsymbol{J}$ and $\boldsymbol{I}$, where $\boldsymbol{J}$ is the all-1's matrix. We will prove that

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

The proof will be easiest if we express $\boldsymbol{L}$ in terms of a matrix $\boldsymbol{X}$ defined by 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 $\boldsymbol{X}$ by

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

An elementary calculation, which I skip, reveals that

$$\boldsymbol{X} = p\boldsymbol{I} - 2\boldsymbol{L} - \boldsymbol{J}. \tag{5.2}$$

Lemma 5.3.1.

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

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

Proof. The diagonal entries of $\boldsymbol{X}^2$ are the squares of the norms of the columns of $\boldsymbol{X}$. 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 $\boldsymbol{X}$ is symmetric, so the off-diagonal entries are the inner products of columns of $\boldsymbol{X}$. That is,

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

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 $\boldsymbol{X}^2$ is -1. □

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

$$\lambda^2 \boldsymbol{\phi} = \boldsymbol{L}^2 \boldsymbol{\phi} = p\boldsymbol{L}\boldsymbol{\phi} - \frac{p(p-1)}{4}\boldsymbol{I}\boldsymbol{\phi} == (p\lambda - p(p-1)/4)\boldsymbol{\phi}.$$

So, we find

$$\lambda^2 + p\lambda - \frac{p(p-1)}{4} = 0.$$

This gives

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

This tells us at least two interesting things:

1. The Paley graph is (up to a very small order term) a $1+\sqrt{1/p}$ approximation of the complete graph.
2. Payley graphs have only two nonzero eigenvalues. This places them within the special family of Strongly Regular Graphs, that we will study later in the semester.

5.4 Generalizing Hypercubes

To generalize the hypercube, we will consider this same group, but with a general set of generators. We will call then $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k$, and remember that each is a vector in $\{0,1\}^d$, modulo 2.

Let G be the Cayley graph with these generators. To be concrete, I set $V = \{0,1\}^d$, and note that G has edge set

$$\left\{(\boldsymbol{x}, \boldsymbol{x} + \boldsymbol{g}_j) : \boldsymbol{x} \in V, 1 \leq j \leq k\right\}.$$

Using the analysis of products of graphs, we can derive a set of eigenvectors of H_d. We will now verify that these are eigenvectors for all generalized hypercubes. Knowing these will make it easy to describe the eigenvalues.

For each $\boldsymbol{b} \in \{0,1\}^d$, define the function $\boldsymbol{\psi_b}$ from V to the reals given by

$$\boldsymbol{\psi_b}(\boldsymbol{x}) = (-1)^{\boldsymbol{b}^T \boldsymbol{x}}.$$

When I write $\boldsymbol{b}^T\boldsymbol{x}$, you might wonder if I mean to take the sum over the reals or modulo 2. As both $\boldsymbol{b}$ and $\boldsymbol{x}$ are $\{0,1\}$-vectors, you get the same answer either way you do it.

While it is natural to think of $\boldsymbol{b}$ as being a vertex, that is the wrong perspective. Instead, you should think of $\boldsymbol{b}$ as indexing a Fourier coefficient (if you don't know what a Fourier coefficient is, just don't think of it as a vertex).

The eigenvectors and eigenvalues of the graph are determined by the following theorem. As this graph is k-regular, the eigenvectors of the adjacency and Laplacian matrices will be the same.

Lemma 5.4.1. *For each $\boldsymbol{b} \in \{0,1\}^d$ the vector $\boldsymbol{\psi_b}$ is a Laplacian matrix eigenvector with eigenvalue*

$$k - \sum_{i=1}^{k} (-1)^{\boldsymbol{b}^T \boldsymbol{g}_i}.$$

Proof. We begin by observing that

$$\boldsymbol{\psi_b}(\boldsymbol{x}+\boldsymbol{y}) = (-1)^{\boldsymbol{b}^T(\boldsymbol{x}+\boldsymbol{y})} = (-1)^{\boldsymbol{b}^T\boldsymbol{x}}(-1)^{\boldsymbol{b}^T\boldsymbol{y}} = \boldsymbol{\psi_b}(\boldsymbol{x})\boldsymbol{\psi_b}(\boldsymbol{y}).$$

Let $\boldsymbol{L}$ be the Laplacian matrix of the graph. For any vector $\boldsymbol{\psi_b}$ for $\boldsymbol{b} \in \{0,1\}^d$ and any vertex $\boldsymbol{x} \in V$, we compute

$$\begin{aligned}
(\boldsymbol{L}\boldsymbol{\psi_b})(\boldsymbol{x}) &= k\boldsymbol{\psi_b}(\boldsymbol{x}) - \sum_{i=1}^{k} \boldsymbol{\psi_b}(\boldsymbol{x}+\boldsymbol{g}_i) \\
&= k\boldsymbol{\psi_b}(\boldsymbol{x}) - \sum_{i=1}^{k} \boldsymbol{\psi_b}(\boldsymbol{x})\boldsymbol{\psi_b}(\boldsymbol{g}_i) \\
&= \boldsymbol{\psi_b}(\boldsymbol{x}) \left(k - \sum_{i=1}^{k} \boldsymbol{\psi_b}(\boldsymbol{g}_i) \right).
\end{aligned}$$

So, $\boldsymbol{\psi_b}$ is an eigenvector of eigenvalue

$$k - \sum_{i=1}^{k} \boldsymbol{\psi_b}(\boldsymbol{g}_i) = k - \sum_{i=1}^{k} (-1)^{\boldsymbol{b}^T \boldsymbol{g}_i}.$$

□

5.5 A random set of generators

We will now show that if we choose the set of generators uniformly at random, for k some constant multiple of the dimension, then we obtain a graph that is a good approximation of the complete graph. That is, all the eigenvalues of the Laplacian will be close to k. I will set $k = cd$, for some $c > 1$. Think of $c = 2$, $c = 10$, or $c = 1 + \epsilon$.

For $\boldsymbol{b} \in \{0,1\}^d$ but not all zero, and for $\boldsymbol{g}$ chosen uniformly at random from $\{0,1\}^d$, $\boldsymbol{b}^T\boldsymbol{g}$ modulo 2 is uniformly distributed in $\{0,1\}$, and so

$$(-1)^{\boldsymbol{b}^T\boldsymbol{g}}$$

is uniformly distributed in ± 1. So, if we pick $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k$ independently and uniformly from $\{0,1\}^d$, the eigenvalue corresponding to the eigenvector $\boldsymbol{\psi_b}$ is

$$\lambda_{\boldsymbol{b}} \stackrel{\text{def}}{=} k - \sum_{i=1}^{k} (-1)^{\boldsymbol{b}^T \boldsymbol{g}_i}.$$

The right-hand part is a sum of independent, uniformly chosen ± 1 random variables. So, we know it is concentrated around 0, and thus $\lambda_{\boldsymbol{b}}$ will be concentrated around k. To determine how concentrated the sum actually is, we use a Chernoff bound. There are many forms of Chernoff bounds. I will not use the strongest, but settle for one which is simple and which gives results that are qualitatively correct.

Theorem 5.5.1. *Let $x_1, \ldots, x_k$ be independent ± 1 random variables. Then, for all $t > 0$,*

$$Pr\left[\left|\sum_i x_i\right| \geq t\right] \leq 2e^{-t^2/2k}.$$

This becomes very small when t is a constant fraction of k. In fact, it becomes so small that it is unlikely that any eigenvalue deviates from k by more than t.

Theorem 5.5.2. *With high probability, all of the nonzero eigenvalues of the generalized hypercube differ from k by at most*

$$k\sqrt{\frac{2}{c}},$$

where $k = cd$.

Proof. Let $t = k\sqrt{2/c}$. Then, for every nonzero $\boldsymbol{b}$,

$$\Pr\left[|k - \lambda_{\boldsymbol{b}}| \geq t\right] \leq 2e^{-t^2/2k} \leq 2e^{-k/c} = 2e^{-d}.$$

Now, the probability that there is some $\boldsymbol{b}$ for which $\lambda_{\boldsymbol{b}}$ violates these bounds is at most the sum of these terms:

$$\Pr\left[\exists \boldsymbol{b} : |k - \lambda_{\boldsymbol{b}}| \geq t\right] \leq \sum_{\boldsymbol{b} \in \{0,1\}^d, \boldsymbol{b} \neq 0^d} \Pr\left[|k - \lambda_{\boldsymbol{b}}| \geq t\right] \leq (2^d - 1)2e^{-d},$$

which is always less than 1 and goes to zero exponentially quickly as d grows. □

I initially suggested thinking of $c = 2$ or $c = 10$. The above bound works for $c = 10$. To get a useful bound for $c = 2$, we need to sharpen the analysis. A naive sharpening will work down to $c = 2 \ln 2$. To go lower than that, you need a stronger Chernoff bound.

5.6 Conclusion

We have now seen that a random generalized hypercube of degree k probably has all non-zero Laplacian eigenvalues between

$$k(1 - \sqrt{2/c}) \quad \text{and} \quad k(1 + \sqrt{2/c}).$$

If we let n be the number of vertices, and we now multiply the weight of every edge by n/k, we obtain a graph with all nonzero Laplacian eigenvalues between

$$n(1 - \sqrt{2/c}) \quad \text{and} \quad n(1 + \sqrt{2/c}).$$

Thus, this is essentially a $1 + \sqrt{2/c}$ approximation of the complete graph on n vertices. But, the degree of every vertex is only $c \log_2 n$. Expanders are infinite families of graphs that are constant-factor approximations of complete graphs, but with constant degrees.

We know that random regular graphs are probably expanders. If we want explicit constructions, we need to go to non-Abelian groups.

Explicit constructions that achieve bounds approaching those of random generalized hypercubes come from error-correcting codes.

Explicit constructions allow us to use these graphs in applications that require us to implicitly deal with a very large graph. A few weeks from now, we will see how to use such graphs to construct pseudo-random generators.

5.7 Non-Abelian Groups

In the homework, you will show that it is impossible to make constant-degree expander graphs from Cayley graphs of Abelian groups. The best expanders are constructed from Cayley graphs of 2-by-2 matrix groups. In particular, the Ramanujan expanders of Margulis [Mar88] and Lubotzky, Phillips and Sarnak [LPS88] are Cayley graphs over the Projective Special Linear Groups $\mathrm{PSL}(2, p)$, where p is a prime. These are the 2-by-2 matrices modulo p with determinant 1, in which we identify A with $-A$.

They provided a very concrete set of generators. For a prime q modulo to 1 modulo 4, it is known that there are $p + 1$ solutions to the equation

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = p,$$

where a_1 is odd and a_2, a_3 and a_4 are even. We obtain a generator for each such solution of the form:

$$\frac{1}{\sqrt{p}} \begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix},$$

where i is an integer that satisfies $i^2 = -1$ modulo p.

Even more explicit constructions, which do not require solving equations, may be found in [ABN+92].

A Eigenvectors of Cayley Graphs of Abelian Groups

The wonderful thing about Cayley graphs of Abelian groups is that we can construct an orthornormal basis of eigenvectors for these graphs without even knowing the set of generators S. That is, the eigenvectors only depend upon the group. Related results also hold for Cayley graphs of arbitrary groups, and are related to representations of the groups. See [Bab79] for details.

As Cayley graphs are regular, it won't matter which matrix we consider. For simplicity, we will consider adjacency matrices.

Let n be an integer and let G be a Cayley graph on $\mathbf{Z}/n$ with generator set S. When $S = \{\pm 1\}$, we get the ring graphs. For general S, I think of these as generalized Ring graphs. Let's first see that they have the same eigenvectors as the Ring graphs.

Recall that we proved that the vectors $\boldsymbol{x}_k$ and $\boldsymbol{y}_k$ were eigenvectors of the ring graphs, where

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

for $1 \le k \le n/2$.

Let's just do the computation for the $\boldsymbol{x}_k$, as the $\boldsymbol{y}_k$ are similar. For every u modulo n, we have

$$\begin{aligned}(A\boldsymbol{x}_k)(u) &= \sum_{g\in S} \boldsymbol{x}_k(u+g)\\ &= \frac{1}{2}\left(\sum_{g\in S} \boldsymbol{x}_k(u+g) + \boldsymbol{x}_k(u-g)\right)\\ &= \frac{1}{2}\left(\sum_{g\in S} \sin(2\pi k(u+g)/n) + \sin(2\pi k(u-g)/n)\right)\\ &= \frac{1}{2}\left(\sum_{g\in S} 2\sin(2\pi ku/n)\cos(2\pi kg/n)\right)\\ &= \sin(2\pi ku/n)\sum_{g\in S}\cos(2\pi kg/n)\\ &= \boldsymbol{x}_k(u)\sum_{g\in S}\cos(2\pi kg/n).\end{aligned}$$

So, the corresponding eigenvalue is

$$\sum_{g\in S}\cos(2\pi kg/n).$$

References

[ABN+92] Noga Alon, Jehoshua Bruck, Joseph Naor, Moni Naor, and Ron M. Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38(2):509–516, March 1992.

[Bab79] László Babai. Spectra of cayley graphs. *Journal of Combinatorial Theory, Series B*, pages 180–189, 1979.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[Mar88] G. A. Margulis. Explicit group theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problems of Information Transmission*, 24(1):39–46, July 1988.