Chapter 7

Cayley Graphs

7.1 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 7.4 and 7.8.

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

[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.

7.2 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 $\mathbb{Z}/p$.

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 $\{0, \dots, p-1\}$, 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 7.2.1. *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 7.2.2. *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

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

7.3 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

$$\boldsymbol{L}^2 = p\boldsymbol{L} + \frac{p-1}{4}\boldsymbol{J} - \frac{p(p-1)}{4}\boldsymbol{I}. \tag{7.1}$$

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

$$\boldsymbol{X} = p\boldsymbol{I} - 2\boldsymbol{L} - \boldsymbol{J}. \tag{7.2}$$

Lemma 7.3.1.

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

When combined with (7.2), this lemma immediately implies (7.1).

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, $\boldsymbol{J}\boldsymbol{\phi} = \boldsymbol{0}$. 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.

7.4 Generalizing Hypercubes

To generalize the hypercube, we will consider Cayley graphs over the same group, but with more generators. Recall that we view the vertex set as the vectors in $\{0,1\}^d$, modulo 2. Each generator, $\boldsymbol{g}_1, \dots, \boldsymbol{g}_k$, is in the same group.

Let G be the Cayley graph with these generators. To be concrete, 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 derived 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 $\boldsymbol{\psi}_{\boldsymbol{b}}$ from V to the reals given by

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

When we write $\boldsymbol{b}^T \boldsymbol{x}$, you might wonder if we 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).