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, $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k$, 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).

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 7.4.1. *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

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

□

7.5 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. This construction comes from the work of Alon and Roichman [AR94]. We 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 $\boldsymbol{\psi}_{\boldsymbol{b}}$ 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. We will not use the strongest, but settle for one which is simple and which gives results that are qualitatively correct.

Theorem 7.5.1. *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 7.5.2. *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. □

We 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.

7.6 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. In Chapter 31, we will see how to use such graphs to construct pseudo-random generators.

7.7 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].

7.8 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

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

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

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

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

So, the corresponding eigenvalue is

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