Algebraic Graphs

Lecturer: Daniel A. Spielman November 14, 2004

12.1 Algebraic Graphs

In this lecture, we will study graphs naturally defined on $\{0,1\}^d$. We will begin with the hypercube, and then examine its generalizations. By using error-correcting codes to define these graphs, we will show how to construct log-degree expander graphs.

We will end the class with an introduction to strongly regular graphs.

12.2 Hypercubes

Let's begin by computing the eigenvalues and eigenvectors of the hypercube. The hypercube, H_d, is the graph with vertex set $\{1,0\}^d$ in which two vertices are connected if they differ in exactly one component. We'll compute the eigenvectors and eigenvalues of A_d, the adjacency matrix of H_d.

I should warn you that I will describe these vertices in two ways. Often, I will describe a vertex by a vector in $\{0,1\}^d$. Other times, I will use the set for which this is the characteristic vector. In this case, vertices are subsets of $\{1,\dots,d\}$.

Actually, I'll tell you what the eigenvectors are. For each $I \subseteq \{1,\dots,n\}$, we have an eigenvector χ_i. For each vertex of H_d, which we identify with a $J \subseteq \{1,\dots,n\}$,

$$\chi_I(J) = (-1)^{|I \cap J|}.$$

Let's now verify that each vector χ_I is an eigenvector. Formally, we have

$$(A_d \chi_I)(J) = \sum_{1 \leq i \leq n} (-1)^{|I \cap (J \oplus \{i\})|}.$$

Now, if $i \in I$, then whether or not $i \in J$, we have

$$(-1)^{|I \cap (J \oplus \{i\})|} = -(-1)^{|I \cap J|},$$

and if $i \notin I$, then

$$(-1)^{|I \cap (J \oplus \{i\})|} = (-1)^{|I \cap J|}.$$

So,

$$(A_d \chi_I)(J) = ((n - |I|) - |I|)(-1)^{|I \cap (J|} = (n - 2\,|I|)(-1)^{|I \cap (J|},$$

and we see that χ_I is an eigenvector with eigenvalue $n - 2\,|I|$.

It remains to verify that these are the only eigenvectors. We can see this by showing that each of these eigenvectors are orthogonal, and verifying that we have as many as there are vertices in the graph. To see that they are orthogonal, we compute for $I \neq J$,

$$\begin{aligned}
\sum_K \chi_I(K)\chi_J(K) &= \sum_K (-1)^{|I \cap K|}(-1)^{|J \cap K|} \\
&= \sum_K (-1)^{|(I \oplus J) \cap K|} \\
&= \sum_K \chi_{(I \oplus J)} \\
&= 0,
\end{aligned}$$

if $I \oplus J \neq \emptyset$. This last calculation is obvious, and I leave it as an exercise.

12.3 Cayley Graphs of $\{0,1\}^d$

We will now generalize the previous construction. The graphs we build will have vertex set $V = \{0,1\}^d$. Their edges will be determined by a set $\mathcal{S} \subset V$. The edge set will be

$$E = \{(I, I \oplus S) : I \in V, S \in \mathcal{S}\}.$$

The hypercube is obtained by letting $\mathcal{S}$ be the set of vectors with just one 1. The graphs from problem 2 of the first problem set were obtained by letting $\mathcal{S}$ be the set of vectors with one or two 1's. Any graph obtained in this way is called a Cayley graph of $\{0,1\}^d$.

We will now show that the vectors χ_I are eigenvectors of every Cayley graph of $\{0,1\}^d$. In our computation, we will treat I and J as vectors, and so we note

$$(-1)^{|I \cap J|} = \prod_{i=1}^{d} (-1)^{I_i J_i}.$$

We now compute

$$\begin{aligned}
(A\chi_I)(J) &= \sum_{S \in \mathcal{S}} (-1)^{|I \cap (J \oplus S)|} \\
&= \sum_{S \in \mathcal{S}} \prod_{i=1}^{d} (-1)^{I_i(J_i + S_i)}, \\
&= \sum_{S \in \mathcal{S}} \prod_{i=1}^{d} (-1)^{I_i J_i} \prod_{i=1}^{d} (-1)^{I_i S_i} \\
&= \prod_{i=1}^{d} (-1)^{I_i J_i} \sum_{S \in \mathcal{S}} \prod_{i=1}^{d} (-1)^{I_i S_i} \\
&= \chi_I(J) \sum_{S \in \mathcal{S}} \prod_{i=1}^{d} (-1)^{I_i S_i}.
\end{aligned}$$

Thus, χ_I is an eigenvector with eigenvalue

$$\sum_{S \in \mathcal{S}} \prod_{i=1}^{d} (-1)^{I_i S_i} = \sum_{S \in \mathcal{S}} (-1)^{\langle I, S \rangle},$$

where $\langle I, S \rangle$ denotes the inner product of I with S. Note that in this case, it makes no difference if we take the inner product over the Reals or modulo 2.

12.4 The Code Connection

This last calculation gives us a convenient way characterize the eigenvalues of the Cayley graph. Let M be the d-by-$|\mathcal{S}|$ matrix whose columns are the vectors in $\mathcal{S}$. If I is a row vector in $\{0,1\}^d$, and we consider the product IM modulo 2, then each entry of IM is $\langle I, S \rangle$ for some $S \in \mathcal{S}$, where here we take the inner product modulo 2. For a vector I in $\{0,1\}^d$, let $|I|$ denote the number of 1s in I–that is, the size of the set. Then,

$$|IM| = \sum_{S \in \mathcal{S}} IS = \sum_{S \in \mathcal{S}} \langle I, S \rangle .$$

Set $k = |S|$, So,

$$2\,|IM| - k = \sum_{S \in \mathcal{S}} (2\,\langle I, S \rangle - 1) = \sum_{S \in \mathcal{S}} (-1)^{\langle I, S \rangle}.$$

This gives us a particularly compact calculation for the eigenvalue of χ_I: it is $2\,|IM| - k$.

Let me now give another interpretation of $|IM|$. In the last two classes, we discussed linear error-correcting codes. The codewords of these were vector spaces in $\{0,1\}^k$. Each such vector space is the row-span of a matrix M. So, if we look at the collection of vectors of the form IM, for $I \in \{0,1\}^d$, we can view them as a code. Recall that the minimum distance between two codewords in a code equals the minimum number of ones in a non-zero codeword, which is

$$\min_{I \neq \mathbf{0}} |IM| .$$

So, let's see what happens if we let M generate a code of rate r that is δ-decodable. The rate is $r = d/k$, and so $k = d/r = \log(n)/r$, where n is the number of vertices in the graph. So, if r is held fixed, we get a family of graphs of degree $k = O(\log n)$. If the code is δ-decodable, then no codeword has less than $2\delta k$ ones, and so

$$\min_{I \neq \mathbf{0}} |IM| \geq 2\delta k.$$

Thus, $\lambda_2 \leq k - 2\delta k$. If δ is also held fixed, then we have

$$\frac{\lambda_2}{k} \leq 1 - 2\delta.$$

As this is a constant less than 1, from any infinite family of codes with fixed r and δ, we obtain an infinite family of expanding graphs.

12.5 Strongly-Regular Graphs

Another interesting family of graphs is the family of strgonly-regular graphs. A strongly-regular graph with parameters (n, k, l, m) is a k-regular graph on n vertices that satisfies

- For all pairs of vertices u and v that are neighbors, u and v have l neighbors in common, and
- for all pairs of vertices u and v that are not neighbors, u and v have m neighbors in common.

The simplest example of such a family comes from the lattice graphs. Let $S = \{1, \ldots, s\}$. The lattice graph with $n = s^2$ vertices has vertex set $V = S \times S$ and edge set

$$\{((a, b), (c, d)) : a = c \text{ or } b = d\}.$$

To see that this is strongly-regular, consider two vertices that are neighbors, say (a, b) and (a, c). Then, the common neighbors of these vertices are exactly those with label (a, d) for $d \notin \{b, c\}$, and so $l = s - 2$. On the other hand, if (a, b) and (c, d) are not neighbors, then their only common neighbors will be (a, d) and (b, c), so $m = 2$.

I will now show you that knowledge of n, k, l and m are all we need to calculate the eigenvalues of this graph. Let J denote the all-1's matrix. Then, we have

$$A^2 = kI + lA + m(J - I - A).$$

Collecting terms, this becomes

$$A^2 = (l - m)A + (k - m)I + mJ.$$

For any eigenvector v other than $\mathbf{1}$ this gives the identity

$$A^2 v - (l - m)Av - (k - m)v = 0,$$

and for λ the corresponding eigenvalue

$$\lambda^2 - (l - m)\lambda - (k - m) = 0.$$

We can now solve for λ by solving this quadratic equation. We find

$$\lambda = \frac{l - m \pm \sqrt{(l - m)^2 + 4(k - m)}}{2}.$$

Perhaps the most remarkable fact here is that, other than k, such graphs have only two eigenvalues.

You may be wondering if there are other families of strongly-regular graphs. In fact there are, and we will see some more next class.