Spectral Graph Theory Lecture 15

Algebraic Constructions of Graphs

Daniel A. Spielman October 17, 2012

15.1 Overview

In this lecture, I will explain how to make graphs from linear error-correcting codes. These will come close to being expanders, except that their degrees are logarithmic rather than constant.

In preparation for constructing expanders in the next lecture, I will show how one can improve the expansion of a graph by squaring it. If there is time, I will say a little about Cayley graphs in general.

15.2 Graphs from Linear Codes

Consider a linear code over $\{0,1\}$ from m bits to n bits. We may assume that such a code is encoded by an n-by-m matrix $\boldsymbol{G}$, and that its codewords are the vectors

$$\boldsymbol{G}\boldsymbol{b},$$

where $\boldsymbol{b} \in \{0,1\}^m$. Let d be the minimum distance of this code (warning: in this section d is not degree). We will use this code to construct an n-regular graph on 2^m vertices with $\lambda_2 = 2d$. The construction will be a generalization of the hypercube, and we in fact obtain the hypercube we set $\boldsymbol{G} = \boldsymbol{I}_m$.

We will take as the vertex set $V = \{0,1\}^m$. Thus, I will also write vertices as vectors, such as $\boldsymbol{x}$ and $\boldsymbol{y}$. Two vertices $\boldsymbol{x}$ and $\boldsymbol{y}$ will be connected by an edge if their sum modulo 2 is a row of $\boldsymbol{G}$.

Let me say that again. Let $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n$ be the rows of $\boldsymbol{G}$. Then, the graph has edge set

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

Of course, this addition is taken modulo 2. You should now verify that if $\boldsymbol{G}$ is the identity matrix, we get the hypercube. In the general case, it is like a hypercube with extra edges.

This graph is a Cayley graph over the additive group $(\mathbf{Z}/2\mathbf{Z})^m$: that is the set of strings in $\{0,1\}^m$ under addition modulo 2. Other Cayley graphs that we have seen in this class include the hypercubes, the ring graphs, and the Payley graphs. In fact, these are all Cayley graphs over Abelian groups. The great thing about Cayley graphs over Abeliean groups is that their eigenvectors are determined just from the group[1]. They do not depend upon the choice of generators. Knowing

[1]More precisely, the characters always form an orthonromal 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.

the eigenvectors makes it much easier to compute the eigenvalues.

15.3 Analyzing the Eigenvectors and Eigenvalues

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

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

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.

Theorem 15.3.1. *For each $\boldsymbol{b} \in \{0,1\}^m$ the vector $\boldsymbol{v_b}$ is a Laplacian matrix eigenvector with eigenvalue*

$$2\left|\boldsymbol{G}\boldsymbol{b}\right|.$$

Recall that $|\boldsymbol{G}\boldsymbol{b}|$ is the Hamming-weight of $\boldsymbol{G}\boldsymbol{b}$. That is, the number of 1s in the vector. This is the number of j for which $\boldsymbol{g}_j^T\boldsymbol{b}$ is 1.

Proof of Theorem 15.3.1. We begin by observing that

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

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

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

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

$$\begin{aligned}
n - \sum_{i=1}^{n} \boldsymbol{v_b}(\boldsymbol{g}_i) &= \sum_{i=1}^{n} (1 - \boldsymbol{v_b}(\boldsymbol{g}_i)) \\
&= 2\left|\boldsymbol{G}\boldsymbol{b}\right|,
\end{aligned}$$

as

$$1 - \boldsymbol{v}_{\boldsymbol{b}}(\boldsymbol{g}_i) = \begin{cases} 2 & \text{if } \boldsymbol{g}_i^T \boldsymbol{b} = 1 \\ 0 & \text{otherwise.} \end{cases}$$

□

So, if d is the minimum weight of a non-zero codeword, then $\lambda_2 = 2d$.

15.4 The Quality of Expanders

Either I defined, or I should have defined, an ϵ-expander to be a d-regular graph G on n vertices such that

$$(1-\epsilon)\frac{d}{n}\boldsymbol{L}_{K_n} \preccurlyeq \boldsymbol{L}_G \preccurlyeq (1+\epsilon)\frac{d}{n}\boldsymbol{L}_{K_n}.$$

That is, it is a graph for which $\lambda_i \in [d-\epsilon d, d+\epsilon d]$ for all $i \geq 2$. This is the definition I will use when I am talking about a single graph. When I talk about a family, ϵ and d should remain constant as n grows. For many of the uses of expanders, our first concern is the value of ϵ. While we would also like for d to be small, it is often a secondary concern.

The construction of the previous section turns an asymptotically good family of error-correcting codes into a family of near-expanders: they can have constant ϵ but the degree grows logarithmically with the number of vertices. Recall that for r and δ such that

$$r + H(\delta) < 1, \quad \text{where } H(\delta) \stackrel{\text{def}}{=} -(\delta \log_2 \delta + (1-\delta)\log_2(1-\delta)),$$

there exist codes of rate r and minimum relative distance at least δ for sufficiently large block lengths n. If we take $\delta = 1/2 - \epsilon/2$, then we obtain a graph on 2^m vertices with degree $n = m/r$ and

$$\lambda_2 \geq 2(1/2 - \epsilon/2)n = (1-\epsilon)n.$$

That is half of what we need for the graph to be an ϵ-expander. We also need an upper bound on the largest eigenvalue. There are a few ways to address this. The first is to observe that we can bound the largest weight of a codeword in the same way that we did the smallest weight, with a negligible loss of rate. In the next lecture, we will see how to make graphs with good largest eigenvalues just from graphs with good smallest eigenvalues.

I also observe that many of the applications of expanders actually only need bounds on λ_2. In the proof of Theorem 10.2.1 and 10.3.1 (numbering as in 2009), we assumed an upper bound on λ_{max} as well. It turns out that an upper bound on λ_{max} is unnecessary for Theorem 10.3.1, and for one side of Theorem 10.2.1.

Before we proceed, let's see how the degree of these graphs scales with ϵ. Using a Taylor expansion, we see that

$$H(1/2 - \epsilon/2) \approx 1 - \frac{\epsilon^2}{2\ln 2}.$$

So, the degree of the corresponding graph would be

$$(2\ln 2)m/\epsilon^2 = (2\ln 2)(\log_2 |V|)/\epsilon^2.$$

Except for the $\log_2 |V|$ term, this is the right rate of growth in ϵ.

15.5 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. For each such solution we obtain a generator 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].

The Ramanujan expanders have all their eigenvalues in the range $[d - 2\sqrt{d-1}, d + 2\sqrt{d-1}]$. So, they are $2\sqrt{d-1}/d$-expanders. In terms of ϵ, this gives

$$d \approx 4/\epsilon^2.$$

Note, again, that this is quadratic in $1/\epsilon^2$.

15.6 Squaring a graph

We can improve the expansion of a graph by squaring it, at the cost of increasing its degree. Given a graph G, we define the graph G^2 to be the graph in which vertices u and v are connected if they are at distance 2 in G. Formally, G^2 should be a weighted graph in which the weight of an edge is the number of such paths. We may form the adjacency matrix of G^2 from the adjacency matrix of G. Let A be the adjacency matrix of G. Then $A^2(u, v)$ is the number of paths of length 2 between u and v in G, and $A^2(v, v)$ is always d. We will eliminate those self-loops. So,

$$A_{G^2} = A_G^2 - dI_n.$$

If G has no cycles of length up to 4, then all of the edges in its square will have weight 1.

Lemma 15.6.1. *Let G be a d-regular graph with Laplacian eigenvalues is $\lambda_1, \ldots, \lambda_n$. Then, G^2 is a $d(d-1)$-regular graph with Laplacian eigenvalues*

$$2d\lambda_i - \lambda_i^2.$$

In particular, the largest Laplacian eigenvalue of G^2 is at most d^2.

Proof. First, let's handle the largest Laplacian eigenvalue. As A_G^2 is positive semi-definite, the smallest eigenvalue of A_{G^2} is at least $-d$, and so the largest Laplacian eigenvalue of G^2 is at most

$$d(d-1) - d = d^2.$$

As for the other eigenvalues, we find that

$$\begin{aligned}
&\lambda_i \text{ is an eigenvalue of } L_G \implies \\
&d - \lambda_i \text{ is an eigenvalue of } A_G \implies \\
&(d-\lambda_i)^2 - d \text{ is an eigenvalue of } A_{G^2} \implies \\
&d(d-1) - (d-\lambda_i)^2 + d \text{ is an eigenvalue of } L_{G^2},
\end{aligned}$$

and

$$d(d-1) - (d-\lambda_i)^2 + d = d^2 - (d-\lambda_i)^2 = 2d\lambda_i - \lambda_i^2.$$

□

Note that if λ_n is large, then the second-smallest eigenvalue of G could be $2d\lambda_n - \lambda_n^2$. For an extreme example, consider the case in which G is bipartite. In this case, $\lambda_n = 2d$, and this becomes an extra eigenvalue of 0 in G^2. The square of a bipartite graph is not a connected graph.

Let's see what the squaring of a graph does to the quality of an expander. To begin, assume that G is an ϵ-expander. So, all of the eigenvalues satisfy $\lambda_i = (1+\alpha)d$, where $|\alpha| \leq \epsilon$. The squaring of the graph then produces an eigenvalue that is equal to

$$\begin{aligned}
2d\lambda_i - \lambda_i^2 &= d^2(2(1+\alpha) - (1+\alpha)^2) \\
&= d^2(2 + 2\alpha - 1 - 2\alpha - \alpha^2) \\
&= d^2(1-\alpha^2).
\end{aligned}$$

So, G^2 is essentially an ϵ^2-expander. In fact, it is slightly better as the ratio of eigenvalue to degree is

$$\frac{d^2(1-\alpha^2)}{d(d-1)}.$$

15.7 Foreshadowing

We also observe that squaring can turn a weak expander into a better expander. As this is in the regime in which ϵ is near 1, we will instead write the condition as

$$\lambda_2 \geq \delta d.$$

Assuming this, squaring the graph gives $\lambda_2(G^2)$ equal to

$$2d\lambda_2 - \lambda_2^2 = d^2(2\delta - \delta^2) \approx 2\delta d^2 \approx 2\delta d(d-1).$$

So, when δ is small the ratio of the second eigenvalue to the degree approximately doubles.

This might not seem so useful, as the degree of the graph squares. But, it is possible to get the same effect while increasing the degree by less. Observe that the square of a graph can be written as a sum of cliques, one on the neighbors of each vertex. We know that we can approximate a clique by an expander, so we will approximate each small clique by a small expander. This is part of the idea behind how we will build expander graphs. This is analogous to how we build expander codes. Where expander codes combined a big graph and a small code, we will combine a big graph with small expanders.

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.

[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.