Lecture 11

Expander Graphs

In this lecture we will study expansion properties of finite graphs. Throughout, $G = (V, E)$ will be a graph with vertex set V, and edge set E. Moreover, we assume that G is d-regular, i.e., every vertex in G has degree d, and we let n denote the size of V: $n := |V|$.

11.1. Edge and Vertex Expansion

For two subsets S and T of the set of vertices of G we denote by $E(S, T)$ the set of edges with one endpoint in S and one endpoint in T:

$$E(S, T) = \{(u, v) \in E \mid u \in S, v \in T\}.$$

In particular, $E(S, S)$ is the set of edges that connect vertices in S to vertices in S. Denoting by $\overline{S}$ the complement of S in V, we denote by ∂S the set $E(S, \overline{S})$ and call it the boundary of S. The vertex expansion of the graph G is defined as

$$h(G) := \min_{1 \le |S| \le n/2} \frac{|\partial S|}{|S|},$$

The vertex expansion thus measures the *minimal flow* of any subset of vertices to its complement.

For nonempty S, the set $\Gamma(S)$ denotes the set of vertices in $\overline{S}$ that are connected to a vertex in S. In other words,

$$\Gamma(S) = \{u \in \overline{S} \mid \exists v \in S: \quad (u, v) \in E\}.$$

The vertex expansion of the graph G is defined as

$$\mu(G) := \min_{1 \le |S| \le n/2} \frac{|\Gamma(S)|}{|S|}.$$

The vertex expansion measures by how much any set of vertices in G expands. Sometimes, we would like to limit the size of the sets S under consideration. We therefore define the α-expansion of G as

$$\mu_\alpha(G) := \min_{1 \le |S| \le \alpha n} \frac{|\Gamma(S)|}{|S|},$$

so that $\mu(G) = \mu_{1/2}(G)$. Note that $\mu_\alpha(G) \ge \mu_{1/2}(G)$ if $\alpha \le 1/2$, and that

$$\mu(G) \ge \frac{h(G)}{d}, \tag{11.1}$$

since G is d-regular.

For various applications, in particular in coding theory, it is desirable to construct sequences of d-regular graphs with small d which have large edge and vertex expansion.

Lecture and scribes by Amin Shokrollahi

11.2. Random Graphs

Theorem 11.1. *Let G be a random d-regular graph on n vertices, and β be a constant with $1 \le \beta < d-1$. Then, there exists effectively computable constants $\alpha = \alpha(\beta)$ and $p = p(\beta)$ such that the probability that $\mu_\alpha(G) \ge \beta$ is at least p.*

Proof. Let G be sampled uniformly from the set of d-regular graphs on n vertices. For subsets S and T of the vertex set of G with $|S| = s$ and $|T| = \beta s$, let $\tau(S,T)$ denote the event that all the neighbors of the vertices in S are contained in T. The event $\mu_\alpha(G) \le \beta$ is then the union of the events $\tau(S,T)$, where S runs over all nonempty subsets of size $\le \alpha n$ and T runs over all nonempty subsets of size $\beta|S|$ of the vertex set of G. Therefore, by the union bound

$$\Pr[\mu_\alpha(G) > \beta] \ge 1 - \sum_{\substack{0<|S|\le\alpha n\\ 0<|T|\le\beta|S|}} \Pr[\tau(S,T)].$$

Since $\Pr[\tau(S,T)] = (|T|/n)^{d|S|}$, we have

$$\begin{aligned}\Pr[\mu_\alpha(G) > \beta] &\ge 1 - \sum_{\substack{0<|S|\le\alpha n\\ 0<|T|\le\beta|S|}} \Pr[\tau(S,T)]\\ &\ge 1 - \sum_{s=1}^{\alpha n} \left(\frac{\beta s}{n}\right)^{ds} \binom{n}{s}\binom{n}{\beta s}.\end{aligned}$$

We now use the estimate $\binom{n}{k} \le (n\mathrm{e}/k)^k$ to obtain

$$\begin{aligned}\Pr[\mu_\alpha(G) > \beta] &\ge 1 - \sum_{s=1}^{\alpha n} \left(\frac{\beta s}{n}\right)^{ds} \binom{n}{s}\binom{n}{\beta s}\\ &\ge 1 - \sum_{s=1}^{\alpha n} \left(\frac{\beta s}{n}\right)^{ds} \left(\frac{n\mathrm{e}}{s}\right)^{s} \left(\frac{n\mathrm{e}}{\beta s}\right)^{\beta s}\\ &= 1 - \sum_{s=1}^{\alpha n} \left(\frac{s}{n}\right)^{(d-\beta-1)s} \gamma^s,\end{aligned}$$

where $\gamma = \beta^{d-\beta}\mathrm{e}^{1+\beta}$. Noting that $s/n \le \alpha$, we further obtain

$$\Pr[\mu_\alpha(G) > \beta] \ge 1 - \sum_{s=1}^{\alpha n} \left(\alpha^{d-\beta-1}\gamma\right)^s.$$

If $\alpha^{d-\beta-1}\gamma < 1/2$, then

$$1 - \sum_{s=1}^{\alpha n} \left(\alpha^{d-\beta-1}\gamma\right)^s \ge 1 - \frac{\alpha^{d-\beta-1}\gamma}{1-\alpha^{d-\beta-1}\gamma} =: p > 0.$$

It therefore suffices to have

$$\alpha < \left(\frac{1}{2\gamma}\right)^{\frac{1}{d-\beta-1}}.$$

For $\beta < d-1$ the right hand side of the above inequality is positive, and this gives us the desired upper bound for α. □

Unfortunately, the performance of random graphs cannot be quite matched with explicitly constructed graphs, in the sense that the latter type does not exhibit as much an expansion as random graphs. (Or, at least, they cannot provably match the expansion of random graphs.)

How could we find a bound on the expansion of a given graph? Clearly, computing the expansion of all subsets of vertices is not an efficient method. Instead, we can use techniques from linear algebra, as described in the next section.

11.3. Elements of Spectral Graph Theory

Let A denote the adjacency matrix of G. It is an $n \times n$ matrix which is symmetric and in which all rows and all columns sum up to d. We denote by L the matrix A/d. Then L is doubly stochastic, i.e., the sum of each row and each column of L is 1.

Since L is symmetric, all its eigenvalues are real. Let $\lambda_{n-1} \leq \lambda_{n-2} \leq \cdots \leq \lambda_1 \leq \lambda_0$ denote the n eigenvalues of L, sorted in descending order. Then we have

Proposition 11.2. *The following assertions hold for the eigenvalues of L:*

(1) *The largest eigenvalue of L is* 1*, i.e.,* $\lambda_0 = 1$.

(2) $|\lambda_{n-1}| \leq 1$.

(3) $\lambda_{n-1} = -1$ *if and only if G is bipartite.*

(4) $\lambda_1 = 1$ *if and only if G is not connected.*

(5) *If G is bipartite, then the eigenvalues are symmetric around* 0.

Proof. We will only prove (1), and leave the proofs of the other assertions to the reader. Let $||\cdot||_1$ denote the 1-norm on $\mathbb{R}^n$, i.e., $||x||_1 = \sum_{i=1}^n |x_i|$. It suffices to show that for all x we have $||Lx||_1 \leq ||x||_1$. Index the coordinates of x by the vertices $v \in V$, so that $x = (x_v \mid v \in V)$ (we assume a fixed ordering on V). Then $(Lx)_v = \sum_{u\sim v} x_u/d$, where $u \sim v$ is a short-hand notation for $(u, v) \in E$. We therefore have

$$\begin{aligned} ||Lx||_1 &= \frac{1}{d}\sum_{v\in V}|\sum_{u\sim v} x_u| \\ &\leq \frac{1}{d}\sum_{(u,v)\in E}|x_u| \\ &= \sum_{u\in V}|x_u| \\ &= ||x||_1. \end{aligned}$$

This concludes the proof. □

Since L is symmetric, all the eigenspaces of L are one-dimensional, and the space $\mathbb{R}^n$ can be decomposed into these eigenspaces. Moreover, these eigenspaces are mutually orthogonal with respect to the standard scalar product, denoted $\langle \cdot, \cdot, \rangle$.

We will use the following notation. First, we index the eigenvalues of L by the vertices of G. In this notation the eigenvalues of L are λ_v, $v \in V$. Next, we denote by f_v, $v \in V$, eigenvectors for these eigenvalues. We also assume that these eigenvectors are normalized, i.e., $||f_v||_2 = \sqrt{\langle f_v, f_v\rangle} = 1$. By a slight abuse of notation, we denote by f_1 the eigenvector for eigenvalue 1. Note that $f_1 = \mathbf{1}/\sqrt{n}$, where $\mathbf{1}$ is the vector all of whose entries are 1. We will sometimes also abuse notation and talk about the *eigenvlaues of G* which are to be meant as the eigenvalues of L.

The edge and vertex expansion of G can be related to its second largest eigenvalue, denoted $\lambda(G)$:

$$\lambda(G) = \max_{1\leq i\leq n-1} |\lambda_i|.$$

Proposition 11.3. *If G is connected and not bipartite, then we have for all* $x \in \mathbb{R}^n$ *such that* $x \perp \mathbf{1}$*:*

$$1 - \lambda(G) \leq \frac{|\langle x, (I-L)x\rangle|}{\langle x, x\rangle}.$$

Proof. If x is orthogonal to $\mathbf{1}$, then

$$x = \sum_{v\neq 1} x_v f_v.$$

It follows that $|\langle x, (I-L)x\rangle| = |\sum_{v\neq 1} x_v^2(1-\lambda_v)| \geq \sum_{v\neq 1} x_v^2(1-\lambda(G)) = \langle x, x\rangle(1-\lambda(G))$, and we are done. □

Theorem 11.4. *Let* $\lambda := \lambda(G)$*. Then we have*

$$h(G) \geq \frac{d}{2}(1-\lambda).$$

Proof. Let $S \subseteq V$ be such that $|\partial S|/|S| = h(G)$. Clearly, S and $\overline{S}$ are not empty, where $\overline{S}$ denotes the complement of S in V. Further, let x be a vector that takes the value $1/|S|$ on S and $-1/|\overline{S}|$ on $\overline{S}$. We will index the positions of x with the elements of V, and thus $x = (x_v \mid v \in V)$, so that $x_v = 1/|S|$ of $v \in S$ and $x_u = 1/|\overline{S}|$ if $u \in \overline{S}$. Note that x is orthogonal to $\mathbf{1}$.

We will show that

$$\frac{2h(G)}{d} \geq \frac{|\langle x, (I-L)x\rangle|}{\langle x, x\rangle}.$$

Using Proposition 11.3, this proves the theorem. To this end, note that

$$\langle x, (I-L)x\rangle = \frac{1}{d} \sum_{\substack{u,v\in V\\(u,v)\in E}} x_u(x_u - x_v).$$

If u and v are both in S of both in $\overline{S}$, then $x_u - x_v = 0$. If $u \in S$ and $v \in \overline{S}$, then $x_u(x_u - x_v) = \frac{1}{|S|}\left(\frac{1}{|S|} + \frac{1}{|\overline{S}|}\right)$, and if $u \in \overline{S}$ and $v \in S$, then $x_u(x_u - x_v) = \frac{1}{|\overline{S}|}\left(\frac{1}{|S|} + \frac{1}{|\overline{S}|}\right)$. Thus,

$$\langle x, (I-L)x\rangle = \frac{1}{d}|E(S,\overline{S})|\left(\frac{1}{|S|} + \frac{1}{|\overline{S}|}\right)^2,$$

where $E(S,\overline{S})$ is the number of edges in E with exactly one endpoint in S, and hence $h(G) = |E(S,\overline{S})|/|S|$. On the other hand, $\langle x, x\rangle = \left(\frac{1}{|S|} + \frac{1}{|\overline{S}|}\right)$, so that

$$\frac{|\langle x, (I-L)x\rangle|}{\langle x, x\rangle} = \frac{|E(S,\overline{S})|}{d}\left(\frac{1}{|S|} + \frac{1}{|\overline{S}|}\right) \leq \frac{2|E(S,\overline{S})|}{|S|d} = \frac{2h(G)}{d},$$

which completes the proof. □

The following result follows immediately from (11.1).

Corollary 11.5.

$$\mu_{1/2}(G) \geq \frac{1}{2}(1-\lambda).$$

11.4. Example: Eigenvalues of Codes

Let C be an $[n,k,d]_2$-code, and let $\Gamma = (x_1 \mid x_2 \mid \cdots \mid x_n)$ be a generator matrix for C, where $x_i \in \mathbb{F}_2^k$. Let G be the graph $(\mathbb{F}_2^k, E)$, where $E = \{(x, x + x_i) \mid x \in \mathbb{F}_2^k, i = 1,\ldots,n\}$. In other words, the vertices of G are the elements of $\mathbb{F}_2^k$ and two vertices are connected if and only if they differ by one of the x_i's. In this section we determine the eigenvalues of this graph, which we call the *eigenvalues of* C.

The adjacency matrix A of G is a $2^k \times 2^k$-matrix. We index the rows and the columns of this matrix by the elements of $\mathbb{F}_2^k$. Then, at row $u \in \mathbb{F}_2^k$, the matrix has ones only at positions $u + x_1, \ldots, u + x_n$, and otherwise it has zeros.

For $u \in \mathbb{F}_2^k$, let X_u be the vector which at position $v \in \mathbb{F}_2^k$ has value $(-1)^{\langle u,v\rangle}$, where $\langle u, v\rangle = \sum_{i=1}^k u_i v_i$. Then we have

$$\begin{aligned}(A\mathrm{X}_u)_v &= \sum_{i=1}^n (\mathrm{X}_u)_{v+x_i}\\ &= \sum_{i=1}^n (-1)^{\langle u, v+x_i\rangle}\\ &= (-1)^{\langle u,v\rangle}\sum_{i=1}^n (-1)^{\langle u,x_i\rangle}\\ &= \sum_{i=1}^n (-1)^{\langle u,x_i\rangle}(\mathrm{X}_u)_v,\end{aligned}$$

so that X_u is an eigenvector of A with eigenvalue $\theta_u := \sum_{i=1}^n (-1)^{\langle u,x_i\rangle}$. Since the vectors X_u are all different, they form an orthogonal basis of $\mathbb{R}^n$, and the θ_u's form all the eigenvalues of A.

These eigenvalues can be related to the weight distribution of C. Note that $u\Gamma = (\langle u, x_i\rangle \mid i = 1,\ldots,n)$, and hence

$$\sum_{i=1}^{n}(-1)^{\langle u,x_i\rangle} = n - 2\mathrm{wgt}(u\Gamma).$$

If A_w denotes the number of codewords of weight w in C, then the eigenvalues of C are $n - 2w$ and each such eigenvalue has multiplicity A_w. If C contains the all-one codeword, then the second largest eigenvalue of C is -1, and the next eigenvalue is $n - 2d$ where d is the minimum distance of C.

11.5. Families of Expanders

Let α and ε be positive real numbers. A sequence $G_1, G_2, \ldots$ of graphs is called a sequence of (d, α, ε)-expanders if

1. The number of vertices of the graphs goes to infinity,
2. each G_i is d-regular, and
3. $\mu_\alpha(G_i) \geq \varepsilon$ for all i.

From Corollary 11.5 it is clear that to satisfy the third property for some positive ε, it suffices to have $\lambda(G_i) \leq 1-\delta$ for some fixed positive δ.

There are many known sequences of expander graphs. We will introduce some of them in this section, without proving their expansion properties.

1. Let $V_m := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, and $E_m \subseteq V_m^2$ be such that $((x,y),(z,u)) \in E_m$ if and only if

$$(z,u) \in \{(x+y,y),(x-y,y),(x,y+x),(x,x-y)\}.$$

   Then the sequence of graphs $G_m = (V_m, E_m)$ is an expander sequence of degree 4.

2. Let $V_m := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, and $\sigma_1,\ldots,\sigma_6$ be transformations of V_m into itself defined as

$$\begin{aligned}
\sigma_1(x,y) &= (x, y+2x),\\
\sigma_2(x,y) &= (x, y+2x+1),\\
\sigma_3(x,y) &= (x, y+2x+2),\\
\sigma_4(x,y) &= (x+2y, y),\\
\sigma_5(x,y) &= (x+2y+1, y),\\
\sigma_6(x,y) &= (x+2y+2, y).
\end{aligned}$$

   Let $E_m \subseteq V_m^2$ be such that $(u,v) \in E_m$ if and only if $u = \sigma_i(v)$ of $v = \sigma_i(u)$ for some i. Then the sequence of graphs $G_m = (V_m, E_m)$ is an expander family of degree 12. It can be shown that $\lambda_1(G_m) \geq (2-\sqrt{3})/3$.

3. [Ramanujan graphs] Let p be a prime congruent to 1 modulo 4. Let q be another prime congruent to 1 modulo 4, and u be an integer such that $u^2 \equiv -1 \bmod q$ (such a u always exists). It can be shown that there are exactly $(p+1)$ 4-tuples $v = (a,b,c,d)$ of integers such that $a > 1$, and b,c,d are even. To each such v we associate the matrix

$$\tilde{v} = \begin{pmatrix} a+ub & c+ud \\ -c+ud & a-ub \end{pmatrix} \in \mathrm{GL}(2,\mathbb{F}_q).$$

   These matrices can be seen as distinct matrices in $\mathrm{PGL}(2,\mathbb{F}_q)$, from which we obtain a set S of $(p+1)$ distinct matrices in $\mathrm{PGL}(2,\mathbb{F}_q)$. The Ramanujan graphs $G_{p,q}$ have vertex set $\mathrm{PGL}(2,\mathbb{F}_q)$ and edge set E, where $(x,y) \in E$ if and only if $y = x\tilde{v}$ for some $\tilde{v} \in S$. These graphs are $(p+1)$-regular, and it can be shown that $\lambda(G_{p,q}) = 2\sqrt{p}/(p+1)$.

11.6. A Lower Bound on $\lambda(G)$

What is the minimum value for $\lambda(G)$? We state two results in this direction, of which we prove only one.

Theorem 11.6 (Alon-Boppana)**.** *We have*

$$\liminf_{n\to\infty} \lambda(X_{n,d}) \geq 2\frac{\sqrt{d-1}}{d},$$

where the limit is over all d-regular graphs $X_{n,d}$ with n vertices.

This theorem shows that Ramanujan graphs introduced in the last section are optimal in terms of their eigenvalues. We will not prove this theorem here, but instead show the following weaker version.

Theorem 11.7. *We have*

$$\liminf_{n\to\infty} \lambda(X_{n,d}) \geq \frac{1}{\sqrt{d}}$$

where the limit is over all d-regular graphs $X_{n,d}$ with n vertices.

Proof. Let G be a d-regular graph on n vertices, and A be its adjacency matrix. Let $\mathrm{Tr}(A^2)$ denote the trace of A^2. On the one hand, this is the sum of the diagonal entries of A^2, i.e., $\mathrm{Tr}(A^2) = nd$, since G is d-regular. On the other hand, $\mathrm{Tr}(A^2)$ is the sum of the eigenvalues of A^2, so $\mathrm{Tr}(A^2) = d^2 \sum_{i=0}^{n-1} \lambda_i^2 \leq d^2(1 + (n-1)\lambda^2)$, where $\lambda = \lambda(G)$. This show that

$$\lambda(G) \geq \frac{1}{\sqrt{d}}\sqrt{\frac{n-d}{n-1}}.$$

As n goes to infinity, the right hand side converges to $1/\sqrt{d}$, and we are done. □