CS59200-PRS: Pseudorandomness Sep 29, 2025

Lecture 10: Spectral Expansion

Lecturer: Wei Zhan *Scribe: Abhigyan Dutta*

1 Spectral Expansion of Graphs

For undirected d-regular graph $H = (V, E)$ with $|V| = n$, let A be the adjacency matrix of H. The spectrum of $\frac{1}{d}A$ consists of its eigenvalues: $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. The *spectral expansion* of H is defined as $\gamma = 1 - \max\{|\lambda_2|, |\lambda_n|\}$.

Here we list some of the properties of the normalized adjacency matrix $\frac{1}{d}A$ and its spectrum:

1. $\frac{1}{d}A$ is symmetric and doubly stochastic.
2. If $x \in \mathbb{R}^n$ is a distribution over V, then $\frac{1}{d}Ax$ is also a distribution over V. This represents a random step on H: starting from the vertices distributed as x, and take a random neighboring vertex, the resulting distribution is $\frac{1}{d}Ax$
3. If $u = \left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right)^\intercal$, i.e. the uniform distribution over V, then $\frac{1}{d}Au = u$. This can be reduced from the fact that $\frac{1}{d}A$ is doubly stochastic; intuitively, starting from a uniformly random vertex and take a random step will still result in a uniformly random vertex, because of the d-regularity.
4. The spectral radius of $\frac{1}{d}A$, which coincides with its operator ℓ_2-norm $\left\|\frac{1}{d}A\right\|_2$ because of symmetry, is the same as its operator ℓ_1-norm $\left\|\frac{1}{d}A\right\|_1 = 1$, since $\lambda_1 = 1$ with eigenvector u. As a result, $\gamma \in [0, 1]$.

As a result, we can obtain several different formulae that computes γ:

Theorem 1. *We have the following equivalent ways of writing* $1 - \gamma$*:*

$$\begin{aligned} 1 - \gamma &= \max_{x \perp u} \frac{\left\|\frac{1}{d}Ax\right\|_2}{\|x\|_2} = \max_{\sum_i x_i = 0} \frac{\left\|\frac{1}{d}Ax\right\|_2}{\|x\|_2} \\ &= \max_{\sum_i x_i = 1} \frac{\left\|\frac{1}{d}Ax - u\right\|_2}{\|x - u\|_2} = \max_{\textit{distribution } x} \frac{\left\|\frac{1}{d}Ax - u\right\|_2}{\|x - u\|_2} \end{aligned}$$

Proof. The first equality is by the spectral theorem of symmetric matrices, that the eigenspaces of $\frac{1}{d}A$ are orthogonal to each other. The second equality is by the fact $x \perp u$, or $\langle x, u\rangle = 0$, if and only if $\sum_{i=1}^n x_i = 0$. The third equality is due to the fact that every $x \in \mathbb{R}^n$ that $\sum_{i=1}^n x_i = 1$ corresponds to $x' = x - u$ that $\sum_{i=1}^n x'_i = 0$. The final equality is because the set of $(x - u)$ where x is a distribution linearly spans the subspace $\sum_{i=1}^n x_i = 0$. $\square$

The last expression, that $\gamma = 1 - \max \frac{\|\frac{1}{d}Ax-u\|_2}{\|x-u\|_2}$ over distributions x, intuitively suggests how fast you get close to the uniform distribution u starting from an arbitrary distribution x over the vertices and taking one random step in the graph, relative to the distance $\|x-u\|_2$.

1.1 Examples

Example 1 (Complete graph with self loops). We have $A = J$, the matrix with all 1's. Here J is rank-1, so $\gamma = 1 - \max\{|\lambda_2|, |\lambda_n|\} = 1$. Intuitively, taking one step in A will result in equal probability of landing on any vertex, irrespective of where we start.

Example 2 (Complete graph without self loops). We have $A = J - I$, with $d = n-1$. Again, it is easy to check that the spectrum of $\frac{1}{d}A$ is $\left\{1, -\frac{1}{n-1}, -\frac{1}{n-1}, \ldots, -\frac{1}{n-1}\right\}$ giving us $\gamma = \frac{n-2}{n-1} \approx 1$.

Example 3 (Graph is disconnected). Let S be one of the connected components and w.l.o.g assume it to be associated to the first $|S|$ rows and columns of A. Let

$$x = \left(\frac{1}{|S|}, \frac{1}{|S|}, \ldots, \frac{1}{|S|}, 0, 0, \ldots, 0\right)^\intercal$$

then $\frac{1}{d}Ax = x$, implying that $\gamma = 0$ as $\lambda_2 = 1$.

Example 4 (Graph is bipartite). Let H be bipartite over S, S' and w.l.o.g assume S to be associated to the first $|S|$ rows and columns of A. Let

$$x = \left(\frac{1}{|S|}, \frac{1}{|S|}, \cdots, \frac{1}{|S|}, \frac{-1}{|S'|}, \frac{-1}{|S'|}, \cdots, \frac{-1}{|S'|}\right)^\intercal$$

then $\frac{1}{d}Ax = -x$ giving us $\lambda_n = -1$, implying $\gamma = 0$.

2 Spectral Expansion Implies Vertex Expansion

Recall a graph H is α-vertex expanding if,

$$|N(S) \setminus S| \geq \alpha |S|, \quad \forall S \subset V, |S| \leq \frac{n}{2}$$

Theorem 2. *If a graph H has γ spectral expansion then it also has γ vertex expansion.*

Proof. Given a subset of vertices $S \subset V, |S| \leq \frac{n}{2}$ and assume w.l.o.g these are the first $|S|$ vertices in adjacency matrix A. Let $x = \left(\frac{1}{|S|}, \frac{1}{|S|}, \cdots, \frac{1}{|S|}, 0, 0, \cdots, 0\right)^\intercal$ and u be the uniform distribution vector. Since $\langle x, u\rangle = 1/n$ for every distribution x, we have

$$\|x-u\|_2 = \sqrt{\langle x, x\rangle - 2\langle x, u\rangle + \langle u, u\rangle} = \sqrt{\frac{1}{|S|} - \frac{1}{n}}.$$

Since $\frac{1}{d}Ax$ is supported on $N(S)$, $\left\|\frac{1}{d}Ax\right\|_2^2 \geq \frac{1}{|N(S)|}\left|\frac{1}{d}Ax\right|_1^2 = \frac{1}{|N(S)|}$. So similarly we have

$$\left\|\frac{1}{d}Ax - u\right\|_2 = \sqrt{\left\langle \frac{1}{d}Ax, \frac{1}{d}Ax \right\rangle - \frac{1}{n}} \geq \sqrt{\frac{1}{|N(S)|} - \frac{1}{n}}.$$

By the formulation of spectral expansion in Theorem 1 we have $\left\|\frac{1}{d}Ax - u\right\|_2 \leq (1-\gamma)\left\|x - u\right\|_2$, and thus

$$\sqrt{\frac{1}{|N(S)|} - \frac{1}{n}} \leq (1-\gamma)\sqrt{\frac{1}{|S|} - \frac{1}{n}}.$$

Solving $|N(S)|$ gives us

$$\frac{|N(S)|}{|S|} \geq \frac{1}{1 - (2\gamma - \gamma^2)\left(1 - \frac{|S|}{n}\right)} \geq \frac{1}{1 - \gamma + \frac{1}{2}\gamma^2} \geq 1 + \gamma,$$

since $|S|/n \leq 1/2$ and $(1 - \gamma + \frac{1}{2}\gamma^2)(1+\gamma) = 1 - \frac{1}{2}(\gamma^2 - \gamma^3) \leq 1$. Therefore $|N(S) \setminus S| \geq |N(S)| - |S| \geq \gamma|S|$. $\square$

3 Spectral Expansion Implies Edge Expansion

Recall a d-regular graph H is α-edge expanding if,

$$e(S, \overline{S}) \geq \alpha d|S|, \quad \forall S \subset V, |S| \leq \frac{n}{2}, \quad \overline{S} = V \setminus S$$

where $e(S, S') = \#\{(i,j) \in E \mid i \in S, j \in S'\}$.

Theorem 3. *If a graph H has γ spectral expansion then it also has $\gamma/2$ edge expansion.*

Proof. Given a subset of vertices $S \subset V, |S| \leq \frac{n}{2}$ and assume w.l.o.g these are the first $|S|$ vertices of the adjacency matrix A. Let $x = \left(\frac{1}{|S|}, \frac{1}{|S|}, \cdots, \frac{1}{|S|}, 0, 0, \cdots, 0\right)^\intercal$. We can represent the number edges $e(S, S')$ with the adjacency matrix as

$$e(S, S') = \mathbb{1}_S^\intercal A \mathbb{1}_{S'} \tag{1}$$

where $\mathbb{1}_S$ and $\mathbb{1}_{S'}$ are the indicator vectors of sets S and S' respectively. Notice that $\mathbb{1}_S =$

$|S|x$, while $\mathbb{1}_{\overline{S}} = nu - |S|x$. Hence we can write,

$$
\begin{aligned}
e(S, \overline{S}) &= (|S|x)^\intercal A\,(nu - |S|x) \\
&= nd|S|x^\intercal u - |S|^2 x^\intercal Ax \\
&= d|S| - |S|^2 x^\intercal Ax \\
&= d|S| - |S|^2 (x-u)^\intercal A(x-u) - |S|^2\left(u^\intercal Ax + x^\intercal Au - u^\intercal Au\right) \\
&= d|S| - |S|^2 (x-u)^\intercal A(x-u) - \frac{d}{n}|S|^2 \\
&\geq d|S| - d|S|^2 \left\|x-u\right\|_2 \left\|\frac{1}{d}A(x-u)\right\|_2 - \frac{d}{n}|S|^2 \\
&\geq d|S| - (1-\gamma)d|S|^2 \left\|x-u\right\|_2^2 - \frac{d}{n}|S|^2 \\
&= d|S| - (1-\gamma)d|S|^2 \left(\frac{1}{|S|} - \frac{1}{n}\right) - \frac{d}{n}|S|^2 \\
&= \gamma\left(d|S| - \frac{d}{n}|S|^2\right).
\end{aligned}
$$

Here we used several times the fact that $\frac{1}{d}Au = u$ and $\langle x, u\rangle = \frac{1}{n}$. The inequalities are because of Cauchy-Schwarz, and the formulation of spectral expansion in Theorem 1. Finally, because $|S| \leq n/2$, we conclude that $e(S, \overline{S}) \geq \frac{1}{2}\gamma d|S|$. $\square$

4 Expander Mixing Lemma

Recall a d-regular graph $H = (V, E)$ on n vertices is ε-mxing if,

$$
\left|\frac{e(S, S')}{dn} - \frac{|S||S'|}{n^2}\right| \leq \varepsilon, \quad \forall S, S' \subseteq V
$$

Theorem 4 (Expander mixing lemma)**.** *If a graph H has $(1-\lambda)$ spectral expansion then it is λ-mixing.*

Proof. Given two subset of vertices $S, S' \subseteq V$ and assume w.l.o.g S consists of the first $|S|$ vertices while S' consists of the last $|S'|$ vertices. Let $x = \left(\frac{1}{|S|}, \frac{1}{|S|}, \cdots, \frac{1}{|S|}, 0, 0, \cdots, 0\right)^\intercal$ and $y = \left(0, 0, \cdots, \frac{1}{|S'|}, \frac{1}{|S'|}, \cdots, \frac{1}{|S'|}\right)^\intercal$.

From earlier Equation 1 we have $e(S, S') = |S||S'|x^\intercal Ay$. We also have

$$
x^T Ay = (x-u)^\intercal A(y-u) + u^\intercal Ay + x^\intercal Au - u^\intercal Au = (x-u)^\intercal A(y-u) + \frac{d}{n}
$$

where the second equality follows by noting that $\frac{1}{d}x^\intercal A u = x^\intercal u = \frac{1}{n}$. Using the above we get,

$$\begin{aligned}
\left|\frac{e(S,S')}{dn} - \frac{|S||S'|}{n^2}\right| &= \frac{|S||S'|}{nd}\left|(x-u)^\intercal A(y-u)\right| \\
&\le \frac{|S||S'|}{n}\cdot \|x-u\|_2 \cdot (1-\gamma)\,\|y-u\|_2 \\
&= (1-\gamma)\frac{|S||S'|}{n}\sqrt{\frac{1}{|S|}-\frac{1}{n}}\sqrt{\frac{1}{|S'|}-\frac{1}{n}} \\
&= (1-\gamma)\sqrt{\frac{|S|}{n}\cdot\frac{n-|S|}{n}\cdot\frac{|S'|}{n}\cdot\frac{n-|S'|}{n}} \le (1-\gamma).
\end{aligned}$$

Here the third to last inequality follows from Cauchy-Schwarz and Theorem 1. ☐

Often when we use Theorem 4 we use the bound $(1-\gamma)\sqrt{\frac{|S|}{n}\cdot\frac{n-|S|}{n}\cdot\frac{|S'|}{n}\cdot\frac{n-|S'|}{n}}$ directly, which is dubbed the strongest form of the expander mixing lemma. Some intermediate bounds that are easy to use include $(1-\gamma)\sqrt{\frac{|S|}{n}\cdot\frac{|S'|}{n}}$; and when $S' = S$ or $S' = \overline{S}$ we get $(1-\gamma)\frac{|S|}{n}\cdot\frac{|\overline{S}|}{n}$.

5 Expander Random Walks

One of the most prominent uses of expander graphs is the random walks. A t-step random walk on a graph $H = (V, E)$ is defined as $v_0 \sim \mathcal{U}(V), v_1 \sim \mathcal{U}(N(v_0)), \ldots, v_t \sim \mathcal{U}(N(v_{t-1}))$, where $\mathcal{U}(N(v))$ denotes uniform random sampling from the neighbors of vertex v.

When H is a complete graph with self-loops, the sequence $(v_0, v_1, \ldots, v_t)$ simply consists of t uniform and independent elements from V. Using expander graphs, we get a sequence of vertices that shares a lot of good properties with the independently uniform sequence, but with significantly less randomness when the degree of the graph is small.

Theorem 5 (Hitting property of expander random walks)**.** *Suppose that H has γ spectral expansion, and $(v_1, \ldots, v_t)$ is a random walk on H. For every $S \subseteq V$ we have*

$$\Pr\left[v_i \notin S, \forall i \in [t]\right] \le \left(1 - \frac{\gamma|S|}{n}\right)^t$$

Proof. Since $(v_1, \ldots, v_t)$ form a Markov chain, we have

$$\begin{aligned}
\Pr\left[v_i \notin S, \forall i \in [t]\right] &= \prod_{i=1}^{t} \Pr\left[v_i \notin S | v_1, \cdots, v_{i-1} \notin S\right] \\
&= \prod_{i=1}^{t} \Pr\left[v_i \notin S | v_{i-1} \notin S\right] = \prod_{i=1}^{t} \frac{\Pr\left[v_i \notin S, v_{i-1} \notin S\right]}{\Pr\left[v_{i-1} \notin S\right]}.
\end{aligned}$$

Each v_i itself is uniformly distributed, and thus $\Pr[v_{i-1} \notin S] = |\overline{S}|/n$. On the other hand, (v_{i-1}, v_i) is a uniformly random edge in H, and thus

$$\Pr[v_i \notin S, v_{i-1} \notin S] = \frac{e(\overline{S}, \overline{S})}{nd} \le \left(\frac{|\overline{S}|}{n}\right)^2 + (1-\gamma)\frac{|S||\overline{S}|}{n^2}$$

by the expander mixing lemma. Plug them in and we have

$$\Pr[v_i \notin S, \forall i \in [t]] \le \prod_{i=1}^{t} \left(\frac{|\overline{S}|}{n} + (1-\gamma)\frac{|S|}{n}\right) = \left(1 - \frac{\gamma|S|}{n}\right)^t. \qquad \square$$

Notice that the above probability is exponentially small in t, similar to the case with independent sequence $v_1, \ldots, v_n$ (for which the probability of not hitting S is $(1-|S|/n)^t$).

The hitting property can be used for derandomizing algorithms with one-sided error. For two-sided error, we can use the following version of Chernoff bound on expander random walks.

Theorem 6 (Expander Chernoff bound)**.** *Suppose that H has γ spectral expansion, and $(v_1, \ldots, v_t)$ is a random walk on H. For every $f : V \to [0,1]$,*

$$\Pr_{v_1,\cdots,v_t}\left[\left|\frac{1}{t}\sum_{i=1}^{t} f(v_i) - \mathop{\mathbb{E}}_{v\sim V}[f(v)]\right| \ge \varepsilon\right] \le 2e^{-\frac{1}{4}\gamma t \varepsilon^2}$$

The proof of Theorem 6 can be found in:

- David Gillman. *A Chernoff Bound for Random Walks on Expander Graphs.*
- Alex Healy. *Randomness-Efficient Sampling within* NC^1*.*

As an application of the expander Chernoff bound, think of the error reduction task we examined in Lecture 3. We have an algorithm $A(x, r)$ with m-bit randomness r that is correct with probability $\frac{1}{2} + \varepsilon$. To reduce the error down to $1/\text{poly}(n)$, we can drawn $r_1, \ldots, r_t$ using a random walk on the expander H with 2^m vertices, constant degree d and constant spectral expansion γ. Theorem 6 implies that $t = O(\varepsilon^{-2} \log n)$ steps suffices, and the number of random bits used to perform the random walk is only $m + t \log d = m + O(\varepsilon^{-2} \log n)$.

Compared to the error reduction with k-wise independence, this has worse dependence on ε but better (in fact, optimal) dependence on m and n.