CS761 Derandomization and Pseudorandomness

2022-23 Sem I

Lecture 9: 05-09-2022

Scribe: Amit Rajaraman Lecturer: Rohit Gurjar

Definition 9.1. A graph G is said to be an (n, d, λ) -expander if

- |V(G)| = n,
- G is d-regular, and
- λ is the second largest eigenvalue $\lambda(G)$ of G in absolute value.

Definition 9.2 (Spectral expanders). A sequence $\{G_n\}_{n\geq 0}$ of d-regular graphs is said to be a spectral expander family if for some $\lambda < 1$, $\lambda(G_n) \leq \lambda$ for all n.

We saw last lecture that random walks on expander graphs converge to the uniform distribution in $O(\log n)$ steps.

This means that there are only $d^{O(\log n)} = \mathsf{poly}(n)$ paths to explore. Therefore, there is a *deterministic* polynomial time algorithm to determine connectivity of expander graphs.

Definition 9.3 (Sparsity). Given a d-regular graph G, define the sparsity

$$h(G) = \min_{\substack{S \subseteq V \\ |S| \le (n/2)}} \frac{|E(S, \overline{S})|}{d|S|}.$$

It is evident that $h(G) \leq 1$. Some definitions use $|E(S, \overline{S})|/|S|$ in the definition of sparsity instead.

It is natural to see that h(G) measures (in some sense) how well-connected a graph is. If it is low, there is some "bottleneck" in the graph where the random walk can get stuck – a set of high measure with very few outgoing edges.

Definition 9.4 (Combinatorial expanders). A sequence $\{G_n\}_{n\geq 0}$ of d-regular graphs is said to be a combinatorial expander family if for some h>0, $h(G_n)\geq h$ for all n.

Theorem 9.5 (Cheeger's Inequality). For any graph G with second eigenvalue λ_2 and sparsity h,

$$\frac{1-\lambda_2}{2} \le h \le \sqrt{2(1-\lambda_2)}.$$

In particular, spectral expanders are combinatorial expanders and vice-versa.

Markov chain Monte Carlo methods find many uses nowadays in problems such as sampling random spanning trees, random independent sets etc. The idea in these is that we start with an arbitrary spanning tree (say), and then randomly move to a "neighbouring" spanning tree – add a random edge not in the spanning tree and remove a random edge from the cycle thus formed. After sufficiently many steps, we are at a(n almost) uniformly random spanning tree. This massive graph composed of spanning trees as vertices ends up being an expander! Because the graph of spanning trees has only exponentially many vertices, we get a polynomial time algorithm to randomly sample spanning trees.

Cheeger's inequality is also seen to be asymptotically tight by the following examples:

- The *n*-cycle C_n . It has sparsity $h(C_n) = 2/n$, and $\lambda(C_n) = \cos(2\pi/n) \approx 1 (2\pi/n)^2$.
- The hypercube graph H_n , with vertex set $\{0,1\}^n$ and edge between two vertices iff they differ at precisely one coordinate. It has sparsity $h(H_n) = 1/n$, and $\lambda(H_n) = 1 \frac{1}{n}$.

What guarantee do we even have that expanders exist? It turns out that a random d-regular graph is a (combinatorial) expander with high probability!

However, how do we construct expander graphs? Our goal is to use expander graphs to reduce randomness in algorithms, so it does not make sense to construct them using the above random argument. We also want the algorithm itself to run in polylog time – this requirement makes sense in light of our remarks towards the end of Lecture 6.

Let p be a prime and consider the 3-regular graph over \mathbb{F}_p^* , where each x is adjacent to $x+1, x-1, x^{-1}$. This graph is an expander; however, the proof of this is not very straightforward and we omit it.

Theorem 9.6 (Expander Mixing Lemma). Let G be a (n, d, λ) -expander. Then, for any $S, T \subseteq V$,

$$\left| E(S,T) - \frac{d}{n} |S| |T| \right| \le d\lambda \sqrt{|S| |T|}.$$

If G were a random graph, then the expected number of edges between S, T is precisely (d/n)|S||T| – of the d|S| edges out of S, we expect a |T|/n fraction to be incident on T.

Proof. Let M be the transition matrix of the random walk on G; it is equal to (1/d) times the adjacency matrix of G. For any set X, let $\mathbf{1}_X$ be the indicator vector of X, with 1s at vertices in X and 0 elsewhere. Observe that

$$\frac{1}{d}E(S,T) = \mathbf{1}_S^{\top} M \mathbf{1}_T.$$

Now, we have $M = \sum_i \lambda_i u_i u_i^{\top}$ using the spectral theorem, where $(u_i)_{i=1}^n$ are orthonormal eigenvectors of M with corresponding real eigenvalues $(\lambda_i)_{i=1}^n$. Note in particular that $\lambda_1 = 1$ and u_1 is the vector with all coordinates having value $1/\sqrt{n}$.

Let $\mathbf{1}_S = \sum_i \alpha_i u_i$ and $\mathbf{1}_T = \sum_i \beta_i u_i$. It is seen that $\alpha_1 = \langle \mathbf{1}_S, u_1 \rangle = |S|/\sqrt{n}$ and $\beta_1 = |T|/\sqrt{n}$. Using orthonormality,

$$\frac{1}{d}E(S,T) = \left(\sum_{i} \alpha_{i} u_{i}^{\top}\right) \left(\sum_{i} \lambda_{i} u_{i} u_{i}^{\top}\right) \left(\sum_{i} \beta_{i} u_{i}\right)
= \left(\sum_{i} \alpha_{i} u_{i}^{\top}\right) \left(\sum_{i} \beta_{i} \lambda_{i} u_{i}\right)
= \sum_{i} \alpha_{i} \beta_{i} \lambda_{i}
= \alpha_{1} \beta_{1} + \sum_{i=2}^{n} \alpha_{i} \beta_{i} \lambda_{i}
= \frac{|S||T|}{n} + \sum_{i=2}^{n} \alpha_{i} \beta_{i} \lambda_{i}.$$

Therefore,

$$\begin{split} \left| E(S,T) - \frac{d}{n} |S| |T| \right| &= d \left| \sum_{i=2}^{n} \alpha_{i} \beta_{i} \lambda_{i} \right| \\ &\leq d\lambda \sum_{i=2}^{n} |\alpha_{i} \beta_{i}| \\ &\leq d\lambda \sqrt{\left(\sum_{i=2}^{n} \alpha_{i}^{2} \right) \left(\sum_{i=2}^{n} \beta_{i}^{2} \right)} \\ &\leq d\lambda \sqrt{\left\| \mathbf{1}_{S} \right\| \left\| \mathbf{1}_{T} \right\|} = d\lambda \sqrt{|S| |T|}. \end{split}$$

We shall now see how to save randomness using expanders.

Let \mathcal{A} be an algorithm that uses k independent random bits. Let G be a $(2^k, d, \lambda)$ -expander. Starting at an arbitrary vertex v_1 , perform a random walk for ℓ steps through vertices $v_1, v_2, \ldots, v_{\ell}$. Run the algorithm on each of these inputs v_1, \ldots, v_{ℓ} (interpreting the 2^k elements of V(G) as length k bit strings.

Recall that if running \mathcal{A} once (using k bits) has error probability β , running the algorithm ℓ times (using $k\ell$ bits) reduces this to an error probability of β^{ℓ} . It turns out that running the algorithm ℓ times in the manner described above (using $O(k + \ell \log d)$ bits) reduces the error probability to $(\beta + \lambda)^{\ell}$! In purely graph theoretic terms, this says the following.

Theorem 9.7. Let G be a (n, d, λ) -expander, and let $B \subseteq V$ be of size βn . Starting at a uniformly random vertex v_1 , consider ℓ steps of the random walk going through vertices v_1, v_2, \ldots, v_ℓ . Then,

$$\Pr\left[all\ v_i\ are\ in\ B\right] \leq (\beta + \lambda)^{\ell}.$$

Proof sketch. Consider the diagonal matrix D with 1s at vertices in B and 0 elsewhere. Let $p^{(0)}$ be the initial (uniform) distribution of v_0 . Observe that the sum of components of $DM^ip^{(0)}$ is precisely the probability that v_i is in B. To bound this, we split a given probability vector into its components along and orthogonal to the uniform distribution. The norm of the second part decreases by λ at every step.

Theorem 9.8 (Alon-Boppana bound). For any (n, d, λ) -expander,

$$\lambda \ge \frac{2\sqrt{d-1}}{d}(1 - o(1)).$$

Definition 9.9 (Ramanujan Graph). A (n,d,λ) -expander is said to be a Ramanujan graph if

$$\lambda \le \frac{2\sqrt{d-1}}{d}.$$

Ramanujan graphs are "ideal" expanders in some sense.

It was proved in 2014 by Adam Marcus, Daniel Spielman, and Nikhil Srivastava that there exist infinite families of bipartite Ramanujan graphs of every degree greater than 2.