CS395T Pseudorandomness and Combinatorial Constructions
Lecture 11, February 20, 2001
Lecturer: Prof. David Zuckerman, Scribe: Ramgopal Mettu

In this lecture, we define and give applications of expander graphs. We discuss the construction of expander graphs and then relate the expansion properties of a graph to the second largest eigenvalue (in absolute value) of the adjacency matrix of that graph.

1 Expander Graphs and their Applications

Let $G = (V, E)$ be a graph with $|V| = n$. For $S \subseteq V$, let $\Gamma(S)$ denote the set of vertices $\{v \mid u \in S \wedge \{u, v\} \in E\}$.

Definition 1 *The* vertex expansion *of G is defined as*

$$min_{S \subseteq V, |S| \leq n/2} \frac{|\Gamma(S) \setminus S|}{|S|}.$$

Let $E(S, \bar{S})$ denote the number of edges between the sets of vertices S and $V \setminus S$.

Definition 2 *The* edge expansion *of G is defined as*

$$min_{S \subseteq V, |S| \leq n/2} \frac{E(S, \bar{S})}{|S|}.$$

Note that for complete graphs, the vertex expansion is $\Theta(1)$. However, the degree is $O(n)$. Our goal will be identify low-degree graphs with large expansion, i.e., graphs where the expansion is $\Omega(1)$ and the degree is $O(1)$. We will call such graphs "expander graphs". Expander graphs have applications in:

- network constructions
- sorting and selection algorithms
- cryptography
- pseudorandomness: amplification of success probability in **BPP** algorithms

More specifically, let us look at the task of amplifying the success probability of a BPP algorithm. Suppose that we have a **BPP** algorithm that uses r random bits to achieve an error of $1/3$. To reduce the error probability to $O(2^{-s})$, we could simply run the algorithm $O(s)$ times and take the majority answer, but this procedure requires $O(rs)$ random bits. Using pairwise independence, we can reduce the number of random bits needed required down to $O(2r)$, but we would need to run the algorithm $\Theta(2^s)$ times to achieve an error probability of $O(2^{-s})$. We saw in a previous lecture that using ideal dispersers (a non-constructive approach) we can achieve this error probability with $s + O(r)$ random bits in polynomial time. Using random walks on expander graphs, we can achieve this error probability using $r + O(s)$ bits.

2 Constructing Expander Graphs

Several well-known types of graphs do not even have constant vertex or edge expansion. For example, a cycle on n vertices has vertex and edge expansion of $4/n$. A 2-dimensional grid ($\sqrt{n}$ by $\sqrt{n}$) has vertex and edge expansion of $\Theta(1/\sqrt{n})$. An ℓ-dimensional hypercube with n vertices has edge expansion 1 (the worst case vertex set is a hypercube of dimension $\ell - 1$). However, the vertex expansion is $\Theta(1/\sqrt{\log n})$ (the worse case vertex set consists of all vertices whose labels have weight less than $\ell/2$).

By the probabilistic method, it is possible to show that graphs of constant degree and constant vertex expansion exist. There also exist explicit constructions. The first construction with an explicitly given constant vertex expansion is due to Gabber and Galil. They define a bipartite graph that is an expander graph as follows. Let $V = A \cup B$, where $|A| = |B| = m^2$, and vertices in A and B are indexed by ordered pairs in $[m] \times [m]$. Then, $\Gamma(\{x, y\}) = \{(x, y), (x, x + y), (x, x + y + 1), (x + y, y), (x + y + 1, y)\}$, where the addition is done modulo m. The degree of this graph is 5, and the vertex expansion for a set of size s is $((2 - \sqrt{3})/4)(1 - s/n)s$.

3 Expansion and Eigenvalues of a Graph

Checking that a graph has a certain vertex or edge expansion is **coNP**-complete, but we can derive bounds on the expansion of a graph by using the second largest (in magnitude) eigenvalue of its adjacency matrix.

Let us fix an d-regular undirected graph G and its adjacency matrix A. Let the eigenvalues of A be $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. It turns out that $\lambda_1 = d$, $\lambda_n \geq -d$, and if G is connected, $\lambda_1 > \lambda_2$. Let $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$.

Let 1 denote the all 1s vector of length n. For a subset S of V, let 1_S denote the bit vector representation of S with respect to V. Let $E(S, U)$ denote the number of edges between sets S and U that are contained in V. We will place bounds on $E(S, \bar{S})$ to get a bound on the edge expansion of G.

Fix S and U and let $|S| = s$ and let $|U| = u$. Note that $E(S, U)$ is exactly $1_S^T \cdot A \cdot 1_U$. We can rewrite 1_S (resp., 1_U) as $1 \cdot \frac{s}{n} + v_S$ (resp., $1 \cdot \frac{u}{n} + v_U$) where v_S (resp., v_U) is a vector chosen to be orthogonal to 1. By observing that for any vector v, if v is orthogonal to 1, then Av is orthogonal to 1, we see that $E(S, U)$ equals

$$\begin{aligned} \left(1\frac{s}{n} + v_S\right)^T A \left(1\frac{u}{n} + v_U\right) &= \frac{su}{n^2} 1^T A 1 + \frac{s}{n} 1^T A v_U + v_S^T A \left(\frac{u}{n} 1\right) + v_S^T A v_U \\ &= \frac{su}{n^2}(dn) + v_S^T A v_U. \end{aligned}$$

Now, by rearranging, we get that $|E(S, U) - \frac{dsu}{n}| = |v_S^T A v_U|$, which in turn is at most $\|v_S\| \cdot \|Av_U\|$, where $\|\cdot\|$ is the L_2 norm. Since $\|Av_U\|_2$ is at most $\lambda \|v_U\|$, we get that $|E(S, U) - \frac{dsu}{n}| \leq \lambda \|v_S\| \|v_U\|$. Now, by definition, $\|v_S\|^2 = \|1_S\|^2 - \|\frac{s}{n} 1\|^2$ and $\|v_U\|^2 = \|1_U\|^2 - \|\frac{u}{n} 1\|^2$. Thus, $\|v_S\|^2 = s(n - s)/n$ and $\|v_U\|^2 = u(n - u)/n$. This gives us that

$$|E(S, U) - \frac{dsu}{n}| \leq \lambda \sqrt{su(1 - s/n)(1 - u/n)} \leq \lambda \sqrt{su}.$$

Then the edge expansion of the set S is at least $(d - \lambda)(n - s)/n$. To obtain a bound on the edge expansion of G, we notice that over all sets S such that $|S| \leq n/2$, $(d - \lambda)(n - s)/n$ is at least $(d - \lambda)/2$. For the vertex expansion, we can observe that it is always at least $1/d$ times the edge expansion since G is d-regular. Thus, the vertex expansion of G is at least $(1 - \lambda/d)/2$.

3.1 A Lower Bound for λ

Since we've determined lower bounds on the edge and vertex expansion of a graph in terms of the degree and second largest eigenvalue, it would be useful to derive a lower bound the second largest eigenvalue in terms of the degree.

Definition 3 *The* trace *of an n by n matrix M, denoted $tr(M)$, is defined as $\sum_{i=1}^{n} M_{ii}$.*

First, we can observe that for any i, $1 \leq i \leq n$, $\sum_{j=1}^{n} A_{ij} A_{ji} = \sum_{j=1}^{n} A_{ij}^2 = d$ (this sum counts the number of cycles of length 2). This gives that the $tr(A^2) = nd$.

If we decompose A into $U^T \Lambda U$, where U is unitary and Λ has the eigenvalues of A on the diagonal, we get that $tr(A^2) = tr(U^T \Lambda^2 U)$. One property of the trace is that for any matrices M and M', $tr(MM') = tr(M'M)$. Thus,

$$\begin{aligned} tr(U^T \Lambda^2 U) &= tr(\Lambda^2 U U^T) \\ &= tr(\Lambda^2) \\ &= \sum_{i=1}^{n} \lambda_i^2 \\ &\leq d^2 + (n-1)\lambda. \end{aligned}$$

We then get that $nd \leq d^2 + (n-1)\lambda$, which by rearranging yields that $\lambda \geq \sqrt{d(n-d)/(n-1)}$. That is, $\lambda = \Omega(\sqrt{d})$.