CS395T Pseudorandomness and Combinatorial Constructions
Lecture 13, February 27, 2001
Lecturer: Prof. David Zuckerman, Scribe: Peiyush Jain

1 Lower Bounds on Expansion

In this lecture we will consider certain graphs and prove lower bounds on their expansion.

2 Vertex Transitive Graphs

Definition 1 *Let $G(V, E)$ be a graph. An automorphism of G is a function $\varphi : V \to V$ such that $\{v, w\} \in E \Leftrightarrow \{\varphi(v), \varphi(w)\} \in E$*

Definition 2 *G is a vertex transitive graph if $\forall v, w \in V$ there is an automorphism φ such that $\varphi(v) = w$.*

Examples of vertex transitive graphs include cycles, 2-d torii and hybercubes.
We will prove lower bounds on the vertex expansion of such graphs.

For any set $S \subset V$ define $\partial S = \Gamma(S)\backslash S$. (i.e Neigbours of S not in S).
Then, vertex expansion of $G = min_{S \subset V_{|S| \leq |V|/2}}(\frac{|\partial S|}{|S|})$

Idea : We will implicitly give a set of paths from S to $\bar{S}$ and show

- that there are many paths,
- for any $v \in \partial S$, not many paths pass through v.

Hence we conclude that ∂S is large.

Theorem 1 *(Babai-Szegedy, Aldous) The vertex expansion of a vertex transitive graph $G(V, E)$ is at least $\frac{1}{diam(G)+1}$, where $diam(G)$ is the diameter of G.*

Proof:
Choose x, y uniformly at random from V. Let P be a random shortest path between x and y. Let D be the expected length of P. Since G is a vertex transitive graph, each vertex is equally likely to occur on P.
Therefore, for any $z \in V$,

$$\Pr[P \text{ passes through } z] = \frac{D+1}{|V|}$$

Thus,

$$\Pr[P \text{ passes through } \partial S] \leq \frac{|\partial S|(D+1)}{|V|}$$

For any $S \subset V$, define $\mu(S) = \frac{|S|}{|V|}$. Now,

$$\Pr[P \text{ passes through } \partial S] \geq \Pr[(x \in S \wedge y \in \bar{S}) \vee (x \in \bar{S} \wedge y \in S)]$$

The right hand side of the above inequality is $2\mu(S)\mu(\bar{S})$. Therefore we have that,

$$2\mu(S)\mu(\bar{S}) \leq \Pr[\ P \text{ passes through } \partial S] \leq \frac{|\partial S|(D+1)}{|V|} = \mu(\partial S)(D+1)$$

Note that $\frac{|\partial S|}{|S|} = \frac{\mu(\partial S)}{\mu(S)}$. From the above inequality we have that, if $|S| \leq |V|/2$,

$$\frac{\mu(\partial S)}{\mu(S)} \geq \frac{2\mu(\bar{S})}{D+1} \geq \frac{1}{D+1}$$

Since $D \leq diam(G)$, we have the result. $\square$

3 Expansion and Girth

We present another approach (due to Alon) to get good expanders.

Definition 3 *The girth of a graph $G(V, E)$ is the length of the smallest cycle in G.*

A fact about the girth of a graph :

Theorem 2 *A graph on n vertices with average degree d, contains a cycle of size $\leq 2\lceil \log_{d-1} n \rceil$.*

We show this for d-regular graphs.

Proof:
Start at a vertex v and form the tree of height $h = \lceil \log_{d-1} n \rceil$ with root v and its $d-1$ neighbours N, neighbours of N and so on.
Now, the number of vertices in a tree of height h is $1 + d + d(d-1) + ... + d(d-1)^{h-1} > (d-1)^h \geq n$.
Therefore, two of the vertices are same, so there is a cycle of size $\leq 2h$. $\square$

Suppose G is a D-regular graph on N vertices with girth $\geq \alpha \log_{D-1} N$.
We show that for small enough sets S of vertices of G, we have large expansion. The idea is to show that, if many edges lay in S then a cycle of smaller size exists.

Theorem 3 *If G is a D-regular graph on N vertices with girth $\geq \alpha \log_{D-1} N$, any set of size at most $N^{\alpha/4}$ has edge expansion $\geq D - 1 - \sqrt{D-1}$.*

Proof:
Let S be a set with $|S| \leq N^{\beta}$.

Let the average degree in S be d_S (i.e there are $\frac{d_S|S|}{2}$ edges within S).
Therefore, there is a cycle of size $\leq 2\log_{d_S-1}|S| \leq 2\beta\log_{d_S-1}N$. Therefore,

$$\alpha\log_{D-1}N \leq 2\beta\log_{d_S-1}N$$

simplifying, we get

$$d_S \leq 1 + (D-1)^{\frac{2\beta}{\alpha}}$$

for $\beta = \alpha/4$ we have that $d_S \leq 1 + \sqrt{D-1}$. Therefore,

$$\text{edge expansion} \geq D - d_S \geq D - 1 - \sqrt{D-1}.$$

□

This is a better bound for small sets than what has been achieved using the 2^{nd} largest eigenvalue. Such graphs with large girth exist and can be efficiently constructed.

4 Cayley Graphs

A Cayley graph consists of a group H and a set $S \subseteq H$ such that $g \in S \Leftrightarrow g^{-1} \in S$.
We construct a graph $G(V,E)$ from H and S by taking $V = H$ and $E = \{\{g, sg\} : g \in H, s \in S\}$.

For example, $H = \mathbb{Z}_m \times \mathbb{Z}_m$ and $S = \{(\pm1, 0), (0, \pm1)\}$ generates a $2-D$ torus.
Other examples include cycles and hypercubes.

A few facts about Cayley graphs:

- Cayley graphs are vertex transitive.
- If H is abelian and $|S| > 2$, then the girth of the graph ≤ 4.

We construct a Cayley Graph of girth $= \Omega(\log|H|)$. From the above, we must use a non-abelian group.

5 A Cayley Graph with Large Girth

This construction is due to Margulis.

Let

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \ B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

Then,

$$A^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, \; B^{-1} = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}$$

It is known that $\{A, B\}$ generates a free subgroup. That is, any pair of reduced words formed from A, B, A^{-1} and B^{-1} are different.
A reduced word is any word in which the words $AA^{-1}, A^{-1}A, BB^{-1}, B^{-1}B$ do not appear.
Now we show a Cayley graph $G(V, E)$ with girth $\Omega(\log |H|)$.

Let H be the group $SL(2, \mathbb{Z}_p)$, which is the set of 2×2 matrices with determinant 1 and entries from $\mathbb{Z}_p$ for prime p. Let $S = \{A, B, A^{-1}, B^{-1}\}$.
Construct the Cayley graph from H and S. This is a 4-regular graph with $(p^2 - 1)p \approx p^3$ vertices.

Theorem 4 *The Cayley graph defined as above has girth $g = \Omega(\log p)$.*

Proof:
Consider a cycle of size $\geq 2l$ passing through $w = I_2$, the identity. Since the cycle is of size $\geq 2l$, we must have a vertex v on the cycle such that the two paths ending on w and v which make up the cycle are of length $\geq l$. These paths correspond to two different reduced words w_1, w_2 formed from $\{A, B, A^{-1}, B^{-1}\}$. We must have that

$$w_1 \equiv w_2 \pmod p$$

and

$$\|w_1 - w_2\| \geq p$$

The inequality follows from the fact that $\{A, B\}$ generates a free subgroup, so $w_1 \neq w_2$ as matrices over $\mathbb{Z}$.
Therefore, $\exists i$ such that $\|w_i\| \geq p/2$. Since each of $\|A\|, \|B\|, \|A^{-1}\|, \|B^{-1}\| \leq 1 + \sqrt{2}$, it follows that

$$l \geq \log_{1+\sqrt{2}} p/2$$

Hence,

$$g = \Omega(\log p) = \Omega(\log |H|)$$

$\square$