

## Lecture 9: Expander Graphs

October 5, 2004

Scribe: Leila Kalantari

## 1 Random Walks on Expanders and Error Reduction for BPP

**Notation:** For any vector  $v$ , the  $l_1$ -norm of  $v$  is  $\|v\|_1 = \sum_{i=1}^v |v_i|$  where  $v = (v_1, \dots, v_n)$ .

Define  $P$  to be the projection matrix for the set  $B \subseteq V$ , where  $|V| = n$ , i.e.,

$$P = \begin{pmatrix} p_1 & 0 & 0 & 0 & \dots & 0 \\ 0 & p_2 & 0 & 0 & \dots & 0 \\ 0 & 0 & p_3 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & p_n \end{pmatrix}$$

where

$$p_i = \begin{cases} 1 & \text{if } i \in B, \\ 0 & \text{if } i \notin B \end{cases}$$

and  $i \in [n]$ .

**Theorem 1 (Hitting Property of Expander Graphs)** *Let  $G$  be any  $d$ -regular expander on  $n$  vertices, with  $\lambda_2(G) \leq \lambda$ . Let  $B \subseteq V$  be any subset of vertices of density  $\beta = \frac{|B|}{n}$ . Then the probability that a random walk on a graph  $G$  starting from uniformly random vertex, will stay inside  $B$  for  $t$  steps of the random walk is  $\leq (\lambda + \beta)^t$ .*

**Claim 2**  $\|(PA)^t Pu\|_1$  is the probability that a  $t$ -step random walk, starting from a uniformly random vertex, never leaves  $B$ .

**Lemma 3** *For any non-negative vector,  $\|PAPv\| \leq (\lambda + \beta)\|v\|$*

**Proof of Theorem 1:**

Using Claim 2, we need to show that  $\|(PA)^t Pu\|_1 \leq (\lambda + \beta)^t$ . We proceed to show this using Lemma 3. We have

$$\|(PA)^t pu\|_1 = \|(PAP) \dots (PAP)u\|_1 = \|(PAP)^t u\|_1.$$

Note that  $PP = P$  because projecting once, projecting one more time does not change anything.

By Cauchy-Schwarz, we can write

$$\|(PAP)^t u\|_1 \leq \sqrt{n} \|(PAP)^t u\| \leq \sqrt{n}(\lambda + \beta)^t \|u\| = (\lambda + \beta)^t,$$

completing the proof of the theorem. ■

**Proof of Lemma 3:**

**Idea:** Projection matrix  $P$  will shrink the uniform component of a vector. Matrix  $A$  will shrink the orthogonal to uniform component. Therefore, together they shrink the entire vector.

Let  $y = Pv$ . Write  $y = y^{\parallel} + y^{\perp}$ , where, as usual,  $y^{\parallel}$  is the component of  $y$  that is parallel to the uniform distribution  $u$ , and  $y^{\perp}$  is the component of  $y$  that is orthogonal to  $u$ . We have

$$\begin{aligned} \|PAy\| &\leq \|PAy^{\parallel}\| + \|PAy^{\perp}\| \\ &\leq \|Py^{\parallel}\| + \|Ay^{\perp}\|. \end{aligned} \tag{1}$$

We have  $\|Ay^{\perp}\| \leq \lambda\|y^{\perp}\| \leq \lambda\|y\|$ . Now for  $\|Py^{\parallel}\|$ , we have  $y^{\parallel} = cu$ , for some scalar  $c$ .

$$c = \frac{(y, u)}{\|u\|^2} = \frac{\frac{1}{n} \sum y_i}{\frac{1}{n}} = \sum y_i.$$

Hence,  $y^{\parallel} = (\sum y_i)u$ . This implies

$$\|Py^{\parallel}\| = \sqrt{\beta n \left( \frac{\sum y_i}{n} \right)^2} = \sqrt{\beta} \|y^{\parallel}\|.$$

By Cauchy-Schwarz,  $\sum y_i \leq \|y\| \sqrt{\beta n}$ . Therefore,

$$\|y^{\parallel}\| = \left( \sum y_i \right) \|u\| \leq \frac{\|y\| \sqrt{\beta n} \sqrt{\beta}}{\sqrt{n}}.$$

Continuing with inequalities (1), we have

$$\leq \beta \|y\| + \lambda \|y\| \leq (\beta + \lambda) \|v\|,$$

completing the proof of the lemma. ■

How pseudorandom numbers generated by a random walk on an expander graph can be used to simulate a **BPP**-type algorithm?

Let  $G = (V, E)$  be an expander graph. Pick a random vertex  $v_0 \in V$  uniformly and at random; collect vertex labels  $v_0, v_1, \dots, v_t$  over a random walk with length  $t$  on  $G$  starting from a uniformly random vertex  $v_0$ .

**Theorem 4** *Let  $B_0, B_1, \dots, B_t \subseteq V$  be subsets of densities  $\beta_i$ , then*

$$\Pr \left[ \bigwedge_{i=0}^t [v_i \in B_i] \right] \leq \prod_{i=0}^{t-1} \left( \sqrt{\beta_i \beta_{i+1}} + \lambda \right).$$

**Exercise 5** *For a randomized algorithm  $A$  that on input  $x$  uses random strings of length equal to length of the vertex labels of  $G$ , show that*

$$\Pr \left[ \bigwedge_{i=0}^t \text{maj } A(x, v_i) \text{ is wrong} \right] \leq 2^{-\Omega(t)}.$$

## 2 Some Known Expander Constructions

(1) (Margulis '73) (Gaber & Galil '80)

Define  $G = (V_m, E)$ , where  $V_m = \mathbb{Z}_m \times \mathbb{Z}_m$ ,  $E = \{(\bar{v}, \bar{w}) | \bar{v} \in V_m, \bar{w} \in \{T_1\bar{v}, T_2\bar{v}, T_3\bar{v}, T_4\bar{v}\}\}$ ,  $T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ ,  $T_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ ,  $T_3 = T_1^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ ,  $T_4 = T_2^{-1} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$ . Graph  $G$  is a Cayley graph of degree 4. Its spectral expansion is some constant less than 1. (2) (Lubotzky, Phillips & Sarnak '88)

Define  $G = (V_p, E)$  where, for a prime  $p$ ,  $V_p = \mathbb{Z}_p \cup \{\infty\}$ ,  $\infty$  is a special symbol called infinity, and  $E = \{(x, y) | x \in V_p, y \in \{x + 1, x - 1, \frac{1}{x}\}\}$ . Graph  $G$  is a Cayley graph of degree 3, with spectral expansion bounded by some constant less than 1.