**CMPT 881: Pseudorandomness** Prof. Valentine Kabanets

# Lecture 8: Spectral Expansion II

*September 30, 2004* *Scribe: Arash Rafiey*

## 1 Two Notions of Spectral Expansion

Let $G$ be a $d$-regular graph on $n$ vertices with normalized adjacency matrix $A$. Let $1 = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ eigenvalues of $G$.

a ) $\lambda_2(G) = max_{i \geq 2}\{|\lambda_i|\}$

b ) $\lambda_2(G) = max_{i \geq 2}\{\lambda_i\}$

If $\lambda_2 \ll 1$ we have an expander. We prove this next.

**Definition 1** *Let $G = (V, E)$. For $B, C \subset V$, let $e(B, C)$ be the number of ordered pairs $(u, v)$ where $u \in B$ and $v \in C$, and $(u, v) \in E$. If $B, C$ are disjoint then $e(B, C)$ is the number of edges between $B$ and $C$.*

**Theorem 2** *Let $G = (V, E)$ be a $d$-regular graph on $n$ vertices, with normalized adjacency matrix $A$. Let $\lambda$ be the second largest eigenvalue of $A$. Then for every partition of $V$ into two disjoint sets $B, C$*
$\frac{e(B,C)}{nd} \geq (1 - \lambda)\mu(B)\mu(C)$*, where* $\mu(B) = \frac{|B|}{n}$ *and* $\mu(C) = \frac{|C|}{n}$.

**Remark** Here is an interpretation of Theorem 2. Consider the following two random experiments. Experiment 1: pick a random vertex $u \in V$ of the graph $G$, and then pick one of its $d$ neighbors $v$, uniformly at random. Experiment 2: pick a random vertex $u \in V$ and then pick a random vertex $v \in V$. What is the probability of picking an ordered pair $(u, v)$ such that $u \in B$ and $v \in C$? For Experiment 1, it is $\frac{e(B,C)}{nd}$; for experiment 2, it is $\mu(B)\mu(C)$. So, Theorem 2 says that, for an expander graph $G$, Experiment 1 results in a pair from $B \times C$ with a probability that is a constant fraction (depending on $\lambda$) of the probability of picking such a pair in Experiment 2. For expander graphs where we have a bound on $\lambda_2(G)$ rather than just $\lambda_2$, we can prove that the probability of getting a pair from $B \times C$ in Experiment 1 is close to that in Experiment 2 — see the Expander Mixing Lemma below (Lemma 5).

**Claim 3** *For any real vector $x = (x_1, x_2, \ldots, x_n)$ and any graph $G$ of order $n$ (without self-loops[1]),* $((I - A)x, x) = \frac{1}{d}\sum_{(i,j)\in E}(x_i - x_j)^2$.

[1] The result is true for arbitrary graph. However, for the sake of simplicity, we prove it only for the case of loopless graphs.

**Proof:**

$$((I-A)x,x) = (x,x) - (Ax,x) = \sum_{i=1}^{i=n} x_i^2 - \frac{2}{d}\sum_{(i,j)\in E}(x_i x_j) =$$

$$\frac{1}{d}\sum_{(i,j)\in E}(x_i^2 + x_j^2) - \frac{2}{d}\sum_{(i,j)\in E} x_i x_j = \frac{1}{d}[\sum_{(i,j)\in E}(x_i - x_j)^2].$$

■

**Proof of Theorem 2:** Let $n = |V|, b = |B|, c = |C| = n - b$.
Define $x = (x_1, x_2, \ldots, x_n)$ by

$$x_i = \begin{cases} -c & \text{if } i \in B \\ b & \text{if } i \in C \end{cases}.$$

Observe that the eigenvalues of the matrix $I - A$ are $0 = 1 - \lambda_1, 1 - \lambda_2, \ldots, 1 - \lambda_n$. So $1 - \lambda$ is the second *smallest* eigenvalue of $I - A$. By Rayleigh's Theorem we have

$$1 - \lambda = min_{y \perp u} \frac{((I-A)y,y)}{\|y\|^2} \le \frac{((I-A)x,x)}{\|x\|^2},$$

where for the last inequality we used the fact that $x \perp u$ by the definition of $x$. By Claim 3, we have $((I-A)x,x) = \frac{n^2}{d} e(B,C)$. Hence

$$((I-A)x,x) \ge (1-\lambda)\|x\|^2 = (1-\lambda)bcn.$$

Therefore $e(B,C) \ge (1-\lambda)\frac{bcnd}{n^2}$ i.e. $\frac{e(B,C)}{nd} \ge (1-\lambda)\mu(B)\mu(C)$. ■

**Corollary 4** *If $\lambda$ is the second largest eigenvalue of a d-regular graph $G$ on $n$ vertices, then $\forall S \subset V$ where $|S| \le \frac{n}{2}$, we have $|N(S) - S| \ge \frac{(1-\lambda)}{2}|S|$.*

**Proof:** By Theorem 2, $e(S,\bar{S}) \ge (1-\lambda)|S||\bar{S}|\frac{d}{n} \ge (1-\lambda)|S|\frac{d}{n}\frac{n}{2} = \frac{(1-\lambda)d|S|}{2}$. Also number of vertices in $\bar{S}$ that have neighbor in $S$ is at least $\frac{e(S,\bar{S})}{d}$. ■

By adding self-loops, we can get a $(d+1)$-regular graph such that $\forall S$, $|S| \le \frac{n}{2}$, $|N(S)| \ge (1 + \frac{1-\lambda}{2})|S|$.

**Lemma 5 (Expander-Mixing Lemma)** *Let $G$ be a d-regular graph with $\lambda_2(G) \le \lambda$. Then $\forall S, T \subset V$, $|\frac{e(S,T)}{nd} - \mu(S)\mu(T)| \le \lambda\sqrt{\mu(S)\mu(T)}$.*

**Proof:** Let $\sigma = (\sigma_1, \ldots, \sigma_n)$ be the characteristic vector for $S$, where

$$\sigma_i = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{if } i \notin S \end{cases}.$$

Similarly, let $\tau$ be the characteristic vector for $T$. Let $A$ be the normalized adjacency matrix of $G$. Observe that $e(S,T) = \sum_{\text{ordered pairs } (i,j)\in E} \sigma_i \tau_j = \sigma(dA)\tau$. Let $\alpha = \mu(S)$ and $\beta = \mu(T)$.

Write $\sigma = \sigma^{\|} + \sigma^{\perp}$, where $\sigma$ is parallel to $u$ and $\sigma^{\perp}$ is orthogonal to $u$. So $\sigma = c.u$ where $c = \frac{(\sigma,u)}{\|u\|^2} = \frac{|S|.\frac{1}{n}}{\frac{1}{n}} = |S| = \alpha n$. Similarly for $\tau^{\|} = \beta n.u$. Now,

$$\begin{aligned}\frac{e(S,T)}{dn} &= \frac{1}{n}[\sigma A \tau] \\ &= \frac{1}{n}[(\sigma^{\|} + \sigma^{\perp})A(\tau^{\|} + \tau^{\perp}] \\ &= \frac{1}{n}[\sigma^{\|}A\tau^{\|} + \sigma^{\|}A\tau^{\perp} + \sigma^{\perp}A\tau^{\|} + \sigma^{\perp}A\tau^{\perp}] \\ &= \frac{1}{n}[\alpha n.uA\beta n.u + \sigma^{\perp}A\tau^{\perp}] = \alpha\beta + \frac{1}{n}\sigma^{\perp}A\tau^{\perp}.\end{aligned}$$

Note that $\sigma^{\perp}A\tau^{\|} = \sigma^{\|}A\tau^{\perp} = 0$. Therefore

$$|\frac{e(S,T)}{dn} - \alpha\beta| = \frac{1}{n}\sigma^{\perp}A\tau^{\perp} \leq \frac{1}{n}\|\sigma^{\perp}\|\|A\tau^{\perp}\| \leq \frac{1}{n}\|\sigma^{\perp}\|\lambda\|\tau^{\perp}\| \leq \frac{\lambda}{n}\|\sigma\|\|\tau\| = \frac{\lambda}{n}\sqrt{\alpha n\beta n} = \lambda\sqrt{\alpha\beta}.$$

So we have $|\frac{e(S,T)}{dn} - \alpha\beta| \leq \lambda\sqrt{\alpha\beta}$. ■

**Remark** The Expander Mixing Lemma shows that a $d$-regular expander graph $G = (V, E)$ on $n$ vertices, with a bound on $\lambda_2(G) \leq \lambda$, can be used to sample from the direct product $V \times V$ in a way that is more randomness efficient than the obvious sampling from $V$ two times independently. Namely, it says that, for *any* sets $S, T \subseteq V$, if we take a random vertex $u \in V$ and then take its random neighbor $v$, we get $(u, v) \in S \times T$ with about the same probability as we would when sampling $u \in V$ and $v \in V$ independently. Thus, instead of spending $2 \log n$ random bits, we can spend only $\log n + \log d$ random bits.

## 2 Random Walks on Expanders

Suppose $A$ is a randomized algorithms with error probability $\epsilon$ using $m$ random bits. By running $A$ $t$ times, we can reduce the error exponentially, but we should use $mt$ random bits. By walking randomly on an expander graph $G$ with parameters $(2^m, d, \lambda)$ (here $2^m$ is number of vertices, $d$ is degree, $\lambda$ is spectral expansion factor), we can reduce the number of random bits to $m + O(t)$. We start in a uniformly chosen vertex $v$ and walk randomly in $G$ for $t$ steps, using the labels of the vertices encountered in the walk as a random strings for $A$. Note that for finding a random neighbor we need to use $\log d$ bits, which is a constant. The following table summarize the above observation.

| Random Algorithm | 1-sided error probability | random bits |
|---|---|---|
| $A$ | $\frac{1}{10}$ | $m$ |
| Repeat $A$, $t$ times | $\leq 2^{-t}$ | $tm$ |
| Random walk on $(2^m, d, \frac{1}{40})$ | $\leq 2^{-t}$ | $m + O(t)$ |