Expander Graphs in Computer Science **WS 2010/2011**

Lecture 1: Introduction

Lecturer: He Sun

---

1 Definitions

Over the past decades expanders play an important role in derandomization, network design, error-correcting codes and so on. Informally expanders are regular graphs with low degree and high connectivity and we can use different ways to define expanders.

1. **Combinatorically**, expanders are highly connected graphs, and to disconnect a large part of the graph, one has to sever many edges.
2. **Geometrically**, every vertex set has a relatively very large boundary.
3. From the **Probabilistic** view, expanders are graphs whose behavior is "like" random graphs.
4. **Algebraically**, expanders are the real-symmetric matrix whose first positive eigenvalue of the Laplace operator is bounded away from zero.

Before showing the equivalence between combinatorial and algebraical definitions, let us present the combinatorial definition at first. For any d-degree graph $G = (V, E)$, we use $\Gamma(v)$ to represent the set of neighbors of v, i.e.,

$$\Gamma(v) = \{u | (u, v) \in E\}.$$

For any subset $S \subseteq V$, let $\Gamma(S) = \cup_{v \in S} \Gamma(v)$ and $\Gamma'(S) = \Gamma(S) \cup S$. Furthermore, for any set $S \subseteq V$ we define $\partial S := E(S, \overline{S})$.

Definition 1.1 (vertex expansion) *A graph G with n vertices is said to have vertex expansion (K, A) if*

$$|\Gamma(S)| \geq A \cdot |S|, \forall S \subseteq V : |S| \leq K.$$

When $K = n/2$, for simplicity we call G an A-expander.

Informally expanders are graphs with the property that every subsets (under some constraint on the their size) has many neighborhoods.

Definition 1.2 (edge expansion) *The edge expansion of a graph $G = (V, E)$ is defined by*

$$h(G) := \min_{S : |S| \leq |V|/2} \frac{|\partial S|}{|S|}.$$

To explain edge expansion, let us see two examples. (1) If G is non-connected, we choose one connected-component as S and we know that $E(S, \overline{S}) = 0$. Therefore $h(G) = 0$. (2) If G is a complete graph K_n, then $E(S, \overline{S}) = |S| \cdot (n - |S|)$ and $h(G) = \lceil n/2 \rceil$.

Definition 1.3 *Let $d \in \mathbb{N}$. A sequence of d-regular graphs $\{G_i\}_{i\in\mathbb{N}}$ of size increasing with i is a family of expanders if there is $\epsilon > 0$ such that $h(G_i) \geq \epsilon$ for all i.*

Usually, when speaking of an expander G_i, we actually mean a family of graphs $\{G_i\}_{i\in\mathbb{N}}$, where each graph in $\{G_i\}_{i\in\mathbb{N}}$ is d-regular and has the same expansion coefficient.

Proposition 1.4 *Any expander graph is a connected graph.*

2 Existence and Constructibility

Expander graphs have two seemingly contradictory properties: low degree and high connectivity. Two general problems for expanders are *existence* and *constructibility*. Between these two problems, existence proof of a certain family of expanders is easier and, as a black-block, the existence of such kind of expanders can be used to show the existence of other combinatorial objects. On the other hand, many applications of expanders really need explicit constructions and they proved much harder to find. We will show some constructions in this course, but they do not always match the bounds given by probabilistic methods.

2.1 Existence

Let $\mathcal{G}_{d,N}$ be the set of bipartite graphs with bipartite sets L, R of size N and left degree d.

Theorem 1.5 *For any d, there exists an $\alpha(d) > 0$, such that for all N*

$$\Pr[G \text{ is an } (\alpha N, d-2)\text{-expander}] \geq 1/2,$$

where G is chosen uniformly from $\mathcal{G}_{d,N}$.

Proof: Define

$$p_k := \Pr\left[\exists S \subseteq L : |S| = k, |\Gamma(S)| < (d-2)|S|\right].$$

So G is not an $(\alpha N, d-2)$-expander iff $\sum_k p_k > 0$.

Assume that there is a set S of size K and $|\Gamma(S)| < (d-2)|S|$. Then there are at least $2k$ repeats among all the neighbors of vertices in S. We calculate the probability

$$\Pr[\text{at least } 2k \text{ repeats among all the neighbors of vertices in } S] \leq \binom{dk}{2k}\left(\frac{dk}{N}\right)^{2k}.$$

Therefore

$$\begin{aligned} p_k &\leq \binom{N}{k}\binom{dk}{2k}\left(\frac{dk}{N}\right)^{2k} \\ &\leq \left(\frac{N\mathrm{e}}{k}\right)^k \cdot \left(\frac{dk\mathrm{e}}{2k}\right)^{2k} \cdot \left(\frac{dk}{N}\right)^{2k} \\ &= \left(\frac{cd^4k}{N}\right)^k \end{aligned}$$

where $c = e^3$. By setting $\alpha = 1/(cd^4)$ and $k \leq \alpha N$, we know that $p_k \leq 4^{-k}$ and

$$\Pr[G \text{ is not an } (\alpha N, d-2)\text{-expander}] \leq \sum_{k=1}^{\alpha N} p_k \leq \sum_{k=1}^{\alpha N} 4^{-k} \leq 1/2.$$

■

Theorem 1.6 *For any fixed $d \geq 3$, a random d-regular graph is a $(\Omega(N), d - 1.01)$-expander with high probability (as $N \to \infty$, the probability goes to 1).*

2.2 Constructibility

Definition 1.7 *Let $\{G_i\}_{i\in\mathbb{N}}$ be a family of expander graphs where G_i is a d-regular graph on n_i vertices and the integers $\{n_i\}$ are increasing, but not too fast.(e.g. $n_{i+1} \leq n_i^2$ will do)*

1. *The family is called **Mildly Explicit** if there is an algorithm that generates the j-th graph in the family $\{G_i\}_{i\in\mathbb{N}}$ in time polynomial in j.*
2. *The family is called **Very Explicit** if there is an algorithm that on input of an integer i, a vertex $v \in V(G_i)$ and $k \in \{1, \cdots, d\}$ computes the k-th neighbor of the vertex v in the graph G_i. The algorithm's running time should be polynomial in its input length.*

Theorem 1.8 (Margulis, 1973) *Fix a positive integer M and let $[M] = \{1, 2, \cdots, M\}$. Define the bipartite graph $G = (V, E)$ as follows. Let $V = [M]^2 \cup [M]^2$, where vertices in the first partite set as denoted $(x, y)_1$ and vertices in the second partite set are denoted $(x, y)_2$. From each vertex $(x, y)_1$, put in edges*

$$(x, y)_2, (x, x + y)_2, (x, x + y + 1)_2, (x + y, y)_2, (x + y + 1, y)_2,$$

where all arithmetic is done modulo M. Then G is an expander.

Theorem 1.9 (Jimbo and Maruoka, 1987) *Let $G = (L \cup R, E)$ be the graph described above, then $\forall X \subset L$, $|\Gamma(X)| \geq |X|(1 + d_0|\overline{X}|/n)$, where $d_0 = (2 - \sqrt{3})/4$ is the optimal constant.*

3 Applications

3.1 Super concentrators

Let $G = (V, E)$ be a directed graph and let I and O be two subsets of V with n vertices, each called the input and the output sets respectively. We call G a *super concentrator* if for every k and every $S \subseteq I, T \subseteq O$ with $|S| = |T| = k$, there exist k vertex disjoint paths in G from S to T. The density of a super concentrator is defined by $\text{Den}(G) = \frac{|E[G]|}{n}$.

Proposed by Valiant, super concentrators have many applications in computer science and communication networks. Valiant conjectured that any super concentrator with n inputs must have $\gg n$ edges. However, Valiant himself disproved this conjecture and presented super concentrators with $O(n)$ edges. The main problems in this topic include:

- Prove the existence of super concentrators with low density. It was known that there exists a super concentrator with density 28, whose proof is based on Kolmogorov complexity.

- Give an explicit construction of super concentrators. Gabber and Galil presented the first explicit construction of super concentrators with density about 270, and so far the best known result is 44 (SODA 2003).

- Prove the lower bound of $\mathrm{Den}(G)$. The best known lower bound is $(5 - o(1))$, proved by Lev and Valiant.

Now we show that super concentrators with constant density can be constructed from constant degree expanders.

Lemma 1.10 *Assume that $\{G_i\}_{i\in\mathbb{N}}$ is a family of bipartite expanders with bipartite sets L, R with $|R| = \alpha|L|, 1/2 < \alpha < 1$ and left degree d. Moreover each graph in $\{G_i\}_{i\in\mathbb{N}}$ has vertex expansion ≥ 1. Then there is a super concentrator with density $\frac{1+2d}{1-\alpha}$.*

3.2 Saving Random Bits

For several problems, expander graphs provide an efficient way to derandomize complexity classes. For example, Reingold used expander graphs to derandomize the complexity class SL, which was open for many years. On the other hand, expanders are used to save random bits and reduce the randomness complexity in randomized algorithms. Here we consider the complexity class RP.

Definition 1.11 *The complexity class* RP *is the class of all languages L for which there exists a probabilistic polynomial-time Turing machine M such that*

$$m \in L \Longrightarrow \Pr[M(x) = 1] \geq \frac{3}{4}$$

$$m \notin L \Longrightarrow \Pr[M(x) = 1] = 0$$

Fix any RP language L and let $r(|x|)$ be the number of random bits used for the RP machine M. To decrease the error probability to δ, a basic approach is to use the Chernoff bound. We run M $O(\log \frac{1}{\delta})$ independent trials and take the average value. But the number of random bits used is $O(r \log \frac{1}{\delta})$.

Now we discuss how to use expanders to decrease the error probability to $\frac{1}{\mathrm{poly}(|r|)}$ with no extra random bits. At first we assume that there is an explicit family of expanders $\mathcal{G} = \{G_i\}_{i\in\mathbb{N}}$ with vertex expansion A where $N = |V[G]| = 2^r$. Our algorithm is as follows:

Input: x.
Choose a parameter c such that $1/(4A^c) < \delta$ and let $v \sim_u V[G]$;
Run $M(x, y_i)$ for all strings y_i where $\mathrm{dist}(v, y_i) \leq c$;
if $\wedge_i M(x, y_i) = 0$ **then**
  return 0
else
  return 1
end

Algorithm 1: Algorithm for Saving Random Bits

Assume that $L \in$ RP. For any $x \in L$, define $Bad_x = \{y | M(x, y) = 0\}$ and $B = \{v | \Gamma'_c(v) \subseteq Bad_x\}$. Then Algorithm 1 outputs 0 iff $v \in B$. By definition, $\forall 1 \leq i \leq c-1$, we have $\Gamma'_i(B) \leq \Gamma'_{i+1}(B) \subseteq Bad_x$. Since $L \in$ RP, we get $|Bad_x| \leq N/4$. On the other hand $|\Gamma'_c(B)| \geq A^c|B|$. Therefore $A^c|B| \leq |\Gamma'_c(B)| \leq |Bad_x| \leq N/4$ and the error probability of Algorithm 1 is bounded by $|B|/N \leq 1/(4A^c) \leq \delta$.