Expander Graphs in Computer Science

Introduction to Expander Graphs

He Sun

Max Planck Institute for Informatics

Oct., 19, 2010

Outline

Course Information

- Time: Tuesday 2:00PM - 4:00PM
- Location: Lecture Hall 003, Campus E1. 3
- Credit: 6 ECTS credit points
- Lecturer: He Sun
- Email: hsun@mpi-inf.mpg.de
- Prerequisites: Basic knowledge of Complexity and Probability

Course Information(cont'd)

Grading

- Homework 60% (3 problem sets), Final exam 40% (oral exam)
- You need to collect at least 50% of the homework points to be eligible to take the final exam.

Course Homepage

http://www.mpi-inf.mpg.de/departments/D1/teaching/WS10/EG/WS10.html

Outline

Expander Graphs: Different Definitions

- Combinatorically, expanders are highly connected graphs, and to disconnect a large part of the graph, one has to sever many edges.

Expander Graphs: Different Definitions

- Combinatorically, expanders are highly connected graphs, and to disconnect a large part of the graph, one has to sever many edges.
- Geometrically, every vertex set has a relatively very large boundary.

Expander Graphs: Different Definitions

- Combinatorically, expanders are highly connected graphs, and to disconnect a large part of the graph, one has to sever many edges.
- Geometrically, every vertex set has a relatively very large boundary.
- From the Probabilistic view, expanders are graphs whose behavior is “like” random graphs.

Expander Graphs: Different Definitions

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

Expander Graphs: Different Definitions

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

Vertex Expansion

We consider undirected, regular graphs $G = (V, E)$. G can have self-loops and multi-edges.

For any set $S \subseteq V$, let

$$\Gamma(S) := \{u : v \in S \text{ and } (u, v) \in E\}$$

be the neighboring set of S.

Vertex Expansion

We consider undirected, regular graphs $G = (V, E)$. G can have self-loops and multi-edges.

For any set $S \subseteq V$, let

$$\Gamma(S) := \{u : v \in S \text{ and } (u, v) \in E\}$$

be the neighboring set of S.

Definition

A graph $G = (V, E)$ is said to have vertex expansion (K, A) if

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

Edge Expansion

Let $G = (V, E)$ be an undirected graph. For any set $S \subseteq V$, let

$$\partial S := E(S, \overline{S})$$

be the edge boundary of S.

Definition

The edge expansion of a graph $G = (V, E)$ is

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

Examples:

- If G is a complete graph, then $h(G) = \lceil |V|/2 \rceil$.
- If G is not connected, then $h(G) = 0$.

Definition of Expander Graphs

Definition

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.

Lemma

Any expander graph is a connected graph.

Two General Problems on Expanders

- Existence
  - Probabilistic methods
  - Kolmogorov complexity
- Constructibility
  - Combinatorial methods
  - Algebraic methods
  - ...

Existence of Expander Graphs

Two general problems

- Existence
- Constructibility

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

Theorem

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

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

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

Constructibility of Expander Graphs

Two general problems

- Existence
- Constructibility

Definition

Let $\{G_i\}_i$ 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 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.

Examples

Theorem (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 (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.

Outline

Applications of Expanders

- In Computer Science
  - Derandomization
  - Circuit complexity
  - Error correcting codes
  - Communication networks
  - Approximation algorithms

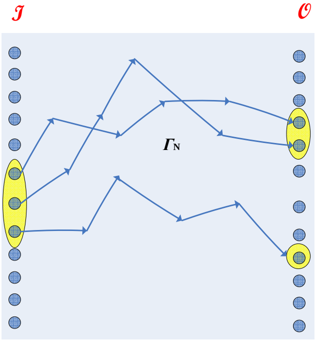
- In Mathematics
  - Graph theory
  - Group theory
  - Number theory
  - Information theory

Three Motivating Problems

1. Super Concentrators
2. Error Correcting Code
3. Deterministic Error Amplification for RP

Super Concentrators

For any integer $N \in \mathbb{N}$, an N-super concentrator Γ_N is a directed graph with input set I and output set O, $|I| = |O| = N$, such that for any subset $S \subseteq I$ and $T \subseteq O$ satisfying $|S| = |T| = k$, there are k vertex-disjoint directed paths in Γ_N from S to T.



Applications

1. Complexity Theory
2. Network Design
3. Matrix Theory
4. ......

Progress in the Past 30 Years

The density of a super concentrator Γ_N is

$$\frac{\#\text{ of edges in }\Gamma_N}{N}.$$

Table: Explicit construction of super concentrator

Authors	Density	Year	Conf./Jour.
Valiant	238	1975	STOC
Gabber	271.8	1981	JCSS
Shamir	118	1984	STACS
Alon	60	1987	JACM
Alon	$44 + o(1)$	2003	SODA

Note: Alon's construction in 2003 is feasible only if $N \geq 262,080$.

Existence: Super concentrators with density 28 exists.

Lower Bound of the Density[Valiant, 1983]: $5 - o(1)$.

Expanders Used in Super Concentrators

Lemma

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*

$$\frac{1+2d}{1-\alpha}.$$

Error Correcting Codes

Let $\mathcal{C} \subseteq \{0,1\}^n$ be a dictionary. The rate and normalized distance are

$$R := \frac{\log |\mathcal{C}|}{n} \quad \delta := \frac{\min_{c_1 \neq c_2 \in \mathcal{C}} d_H(c_1, c_2)}{n}$$

Problem: Is it possible to design arbitrarily large dictionaries $\{\mathcal{C}_k\}$ of size $|\mathcal{C}_k| = 2^k$, with $R(\mathcal{C}_k) \geq R_0$ and $\delta(\mathcal{C}_k) \geq \delta_0$ for some absolute constant $R_0, \delta_0 > 0$? Moreover, can we make these code explicit and efficiently encodable and decodable?

Saving Random Bits for RP

Definition (RP)

The complexity class RP is the class of all languages L for which there exists a probabilistic polynomial-time Turning machine M, such that

$$x \in L \Rightarrow \Pr[M(x) = 1] \geq 3/4$$

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

Independent V.S. Dependent Sampling

No.	# of random bits	Methods	Error Prob.
1	r	Def. of RP	$1/4$
2	$O(r \log \frac{1}{\delta})$	Chernoff Bound	δ
3	r	Expander Graph	$\frac{1}{\mathrm{poly}(r)}$

Algorithm for Saving Random Bits

Lemma

There is an algorithm A^*, such that for the given vertex v and index $i \in \{1, \cdots, d\}$, Algorithm A^* can output the i-th neighbor of v with time complexity $\text{poly}(|v|, |i|)$.

Algorithm Description M^*

1. Run the original RP algorithm M for all strings y lying within a ball of radius c around $v, v \sim_u V$.
2. If for all these y, $M(x, y) = 0$, reject x.
3. If $M(x, y) = 1$ for any y, accept x.

Note: Algorithm M^* uses an $(N/2, A)$-expander, where $N = 2^r$. The parameter c is satisfying $1/4A^c < \delta$.

Algorithm for Saving Random Bits (cont'd)

For any language $L \in RP$ and $x \in L$, define

$$Bad_x = \{y | M(x,y) = 0\} \quad B = \{v | \Gamma'_c(v) \subseteq Bad_x\}$$

So $M^*(x,v) = 0$ if and only if $v \in B$.

By definition of RP, $|Bad_x| \leq N/4, N = 2^r$, and

$$\Gamma'_i(B) \subseteq \Gamma'_{i+1}(B) \subseteq Bad_x, \forall 1 \leq i \leq c-1,$$

therefore $|\Gamma'_c(B)| \geq A^c|B|$ and $N/4 \geq |Bad_x| \geq |\Gamma'_c(B)| \geq A^c|B|$. Thus

$$\Pr\left[M^*(x) = 0\right] = \frac{|B|}{N} \leq \frac{1}{4A^c} < \delta.$$

$\square$