Chapter 4
Expanders

Angsheng Li

Institute of Software
Chinese Academy of Sciences

Advanced Algorithms
U CAS
13, March, 2016

Outline

1. Backgrounds
2. Eigenvalues
3. Information quickly spreads in expander
4. Combinatorial characterisation
5. Expander $\approx$ pseudo-random generator
6. Algorithm for constructing expanders
7. UPATH is in Logspace

Why expanders?

- Communication networks
- Pseudo random generator
- Randomness
- Derandomisation
- UPATH is Log space
- PCP proof
- PageRank

Conventions

For simplicity, we assume that the graphs allow:

- regular 各顶点度相同的简单无向图
- selfloop
- parallel edges

Theory is possible for general graphs without these assumptions.

Inner product

$\langle u, v \rangle$ 向量

- $\langle xu + yv, w \rangle = x\langle u, w \rangle + y\langle v, w \rangle$
- $\langle v, u \rangle = \overline{\langle u, v \rangle}$, $\bar{z}$ is the complex conjugation of z 复共轭
- For all u, $\langle u, u \rangle \geq 0$, with 0 only if $u = 0$ 两个相同的内积为0
- $\langle u, v \rangle = 0$ means u, v are orthogonal, written $u \perp v$
- If $u^1, u^2, \cdots, u^n$ satisfy $u^i \perp u^j$ for all $i \neq j$, then they are linearly independent. 两两都垂直是线性独立的

Parseval's identity: If $u^1, u^2, \cdots, u^n$ form an orthonormal basis for C^n, then for every v, if $v = \sum_i \alpha_i u^i$, then

$$\langle v, v \rangle = \sum_{i=1}^{n} |\alpha_i|^2. \quad \text{模平方和}$$

Hilbert space: Vector spaces with inner product.

Dot product

- For $u, v \in \mathbb{F}^n$, $u \odot v = \sum_{i=1}^{n} u_i v_i$
- $S \subset \mathbb{F}^n$, $S^{\perp} = \{u : u \perp S\}$ 和S所有向量垂直的所有向量构成的集合
- $u \perp v$, if $u \odot v = 0$, $u \perp S$, if for all $v \in S$, $u \perp v$.
- $\dim(S) + \dim(S^{\perp}) = n$ S的维数和与S垂直的维数和=n
- $u \in \mathbb{F}^n$, $u^{\perp} = \{v : v \perp u\}$, and $\dim(u^{\perp}) = n - 1$.

  对于一个向量，与它垂直的向量的维数为n-1

Random subsum principle

For every nonzero $u \in \mathrm{GF}(2^n)$, 有限域

$$\Pr_{v \in_R \mathrm{GF}(2^n)}[u \odot v = 0] = \frac{1}{2}.$$

要会证

Eigenvectors and eigenvalues

If A is a real, symmetric matrix, for λ and v, if $Av = \lambda v$, then

$$\lambda\langle v, v\rangle = \langle Av, v\rangle = \overline{\langle v, Av\rangle} = \overline{\langle v, \lambda v\rangle} = \bar{\lambda}\langle v, v\rangle$$

$$\Downarrow$$

$$\lambda = \bar{\lambda}$$

λ与它的复共轭相等

so λ is a real.

特征值是实数

Norms

范数

$$||\ ||:\ \mathbb{F}^n \to \mathbb{R}^{\geq 0}$$ 有限域在实数

范数≥0

(i) $||v|| = 0 \iff v = 0$

(ii) $||\alpha v|| = |\alpha| \cdot ||v||$

(iii) $||u + v|| \leq ||u|| + ||v||.$

L_p-norm

L_p-norm of v, $p \geq 1$,

$$||v||_p = (\sum_{i=1}^{n} |v_i|^p)^{1/p}$$

$p = 2$ – the Euclidean norm

$$||v||_2 = (\sum_{i=1}^{n} |v_i|^2)^{1/2}$$

$p = 1$,

$$||v||_1 = \sum_{i=1}^{n} |v_i| \qquad \text{绝对值和}$$

$p = \infty$,

$$||v||_\infty = \max_i |v_i|. \qquad \text{最大的一个}$$

Hölder inequality

For every p, q, if $\frac{1}{p} + \frac{1}{q} = 1$, then

$$\|u\|_p \cdot ||v||_q \geq \sum_{i=1}^{n} |u_i v_i|.$$

$p = q = 2$, Cauch-Schwarz

L_1- and L_2-norms

For every vector $v \in \mathbb{R}^n$,

$$\frac{|v|_1}{\sqrt{n}} \leq ||v||_2 \leq |v|_1.$$

两个范数之间的关系

Adjacent matrix 邻接矩阵

- G: d-regular, n vertices,
- p: a column vector, a distribution over the vertices of G
- A_{ij}: $\frac{n_{ij}}{d}$, where n_{ij} the number of edges between i and j.
- A: the adjacent matrix. It is normalised, symmetric, stochastic 每一行/列 的和都是1
- $q = Ap$: the distribution of a random walk in G from distribution p. 随机游走一步
- $A^l e^i$: the distribution of l-step random walk from node i
- 1: the transpose of $(\frac{1}{n}, \cdots, \frac{1}{n})$, the uniform distribution
- $1^{\perp}$: $\{v : v \perp 1\}$
- $v \perp 1 \iff \sum v_i = 0$.

$\lambda(A)$

Define

$$\lambda(A) = \lambda(G) = \max\{||Av||_2 : \ ||v||_2 = 1, v \perp 1\}.$$

Suppose that

$$\lambda_1, \lambda_2, \cdots, \lambda_n$$ 所有特征值≤1

are the eigenvalues of A with orthogonal eigenvectors

$$v^1, v^2, \cdots, v^n$$

respectively.
Let $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_n|$.

$|\lambda_i| \leq 1$

For λ and v such that $Av = \lambda v$. Then $\lambda = \frac{\langle v, Av \rangle}{\langle v, v \rangle}$.
By definition,

$$\langle v, Av \rangle = \sum_{i=1}^{n} a_{ii} v_i^2 + 2 \sum_{i<j, i \sim j} a_{ij} v_i v_j$$

有边才有Aij

For $i < j$, $i \sim j$:

$$a_{ij}(v_i - v_j)^2 = a_{ij} v_i^2 - 2 a_{ij} v_i v_j + a_{ij} v_j^2$$

Summing up all such i, j's:

$$\sum_{i=1}^{n} (1 - a_{ii}) v_i^2 - 2 \sum_{i<j, i \sim j} a_{ij} v_i v_j$$

Proof - I

$$\langle v, Av \rangle = \sum_{i=1}^{n} a_{ii} v_i^2 + \sum_{i=1}^{n} (1 - a_{ii}) v_i^2 = \sum_{i<j, i\sim j} a_{ij} (v_i - v_j)^2$$

$$= \sum_{i=1}^{n} v_i^2 - \sum_{i<j, i\sim j} a_{ij} (v_i - v_j)^2 \qquad (1)$$

Therefore

$$-1 \leq \lambda \leq 1.$$

By definition,

$$A1 = 1$$ 1是uniform的分布

So $\lambda_1 = 1$, and 1 is the eigenvector of $\lambda_1 = 1$.
By the choice of the eigenvectors, $1^{\perp} = \text{Span}\{v^2, \cdots, v^n\}$.

Proof - II

Given v, with $v \perp 1$, $||v||_2 = 1$.
Let $v = \alpha_2 v^2 + \cdots + \alpha_n v^n$ with $\alpha_2^2 + \cdots + \alpha_n^2 = 1$.

$$Av = \alpha_2 Av^2 + \cdots + \alpha_n Av^n = \alpha_2 \lambda_2 v^2 + \cdots + \alpha_n \lambda_n v^n$$

$$||Av||_2^2 = \alpha_2^2 \lambda_2^2 + \cdots + \alpha_n^2 \lambda_n^2$$

Since $\lambda_2^2 \geq \cdots \geq \lambda_n^2$,

$$\max ||Av||_2^2 = \lambda_2^2.$$

Therefore

$$\lambda = \lambda(G) = |\lambda_2|.$$

Spectral gap

信息传播：少量几步就可以很快传播到网络中

We call $1 - \lambda(G)$ the *spectral gap of G*.

Lemma

Let G be an n-vertex regular graph and p a probability distribution over G's vertices. Then,

$$||A^l p - 1||_2 \leq \lambda^l.$$

从任何一个分部开始，在A中做l步随机游走，

Proofs consist of the following items:

1) By definition of $\lambda = \lambda(G)$, for every $v \perp 1$,

$$||Av||_2 \leq \lambda ||v||_2.$$

几乎是Unifrom

少量几步随机游走，得到的分部和均匀分部类似

最大的

任何一个和1垂直的v作用在A上，Av的范数就收缩λ倍

Proofs - I

Av也和1垂直

2) If $v \perp 1$, then so is Av.

A是对称，转置不变

$$\langle 1, Av \rangle = \langle A^{\mathrm{T}} 1, v \rangle = \langle 1, v \rangle = 0.$$

Note $A = A^{\mathrm{T}}$, and $A1 = 1$.

3) $A : \ 1^{\perp} \to 1^{\perp}$, and

A shrinks each $v \in 1^{\perp}$ by at least λ factor in L_2 norm.

4) By 3), A^l shrinks each $v \in 1^{\perp}$ by at least λ^l factor, giving

$$\lambda(A^l) \leq \lambda^l.$$

Proofs - II

和1平行+和1垂直

5) Let $p = \alpha 1 + p'$, $p' \perp 1$, Since $p' \perp 1$, $\sum p'_i = 0$.
But $\sum p_i = 1$, so $\alpha = 1$.

$$A^l p = A^l(1 + p') = A^l 1 + A^l p' = 1 + A^l p'.$$

要会证

$$\begin{aligned} ||A^l p - 1||_2 &= ||A^l p'||_2 \\ &\leq ||A^l||_2 \cdot ||p'||_2 \\ &\leq \lambda^l \cdot ||p'||_2 \\ &\leq \lambda^l \cdot ||p||_2 \\ &\leq \lambda^l \cdot |p|_1 = \lambda^l. \end{aligned}$$

The third inequality uses $||p||_2^2 = ||1||_2^2 + ||p'||_2^2$.

Log space algorithm for connectivity in expanders

如果特征值小于1，随机游走l步即可得到均匀分布

Suppose that λ is a constant significantly smaller than 1.
By the lemma above, let $l = O(\log n)$.
Then $\lambda^l \approx 0$. Therefore

随机游走l步后,走匀,走到哪的概率都一样

$$A^l p \approx 1.$$

均匀分布

也就是说走l步后哪都可以走到

This means that for any two nodes i, j, the distance between i and j is within $O(\log n)$.
According to this property, we are able to design a log space algorithm to decide, for any two vertices, whether or not, they are connected.

λ < 1时，走log n 步就可以判断i和j是不是联通

The algorithm simply enumerates all the paths from i of length $O(\log n)$, to see if there is a path passes j. The enumeration of all the paths can be done in log space.

Randomized log space for connectivity

Lemma 任意图

If G is a regular connected graph with selfloop at each vertex, then 要求联通

$$\lambda(G) \leq 1 - \frac{1}{4dn^2}.$$

d regular

regular：每个定点有d个邻居

Let $u \perp 1$, $||u||_2 = 1$.
We show that $||Au||_2 \leq 1 - \frac{1}{4dn^2}$.
Let $v = Au$. It suffices to show that $1 - ||v||_2^2 \geq \frac{1}{2dn^2}$.
Since $||u||_2 = 1$,

$$1 - ||v||_2^2 = ||u||_2^2 - ||v||_2^2.$$

Considering $\sum_{i,j} A_{ij}(u_i - v_j)^2$, we have

Proofs - I

$$\begin{aligned}
\sum_{i,j} A_{ij}(u_i - v_j)^2 &= \sum_{i,j} A_{ij}u_i^2 - 2\sum_{i,j} A_{ij}u_i v_j + \sum_{i,j} A_{ij}v_j^2 \\
&= \sum_{i=1}^{n} u_i^2 - 2\langle Au, v\rangle + \sum_{j=1}^{n} v_j^2 \\
&= ||u||_2^2 - 2\langle Au, v\rangle + ||v||_2^2 \\
&= ||u||_2^2 - 2||v||_2^2 + ||v||_2^2 \\
&= ||u||_2^2 - ||v||_2^2 = 1 - ||v||_2^2. \qquad (2)
\end{aligned}$$

Therefore, we only need to prove

$$\sum_{i,j} A_{ij}(u_i - v_j)^2 \geq \epsilon = \frac{1}{2dn^2}.$$

Proofs - II

By the choice of u, $\sum u_i = 0$, and $\sum u_i^2 = 1$. So there exist i, j such that $u_i u_j < 0$.

Since $||u||_2 = 1$, the average of u_i^2 is $\frac{1}{n}$, and the average of $|u_i|$ is $\frac{1}{\sqrt{n}}$. 1范数和2范数的关系

Let i nd j be such that $u_i > 0$, $u_j < 0$, and

$$u_i - u_j \geq \frac{1}{\sqrt{n}}.$$

(Such i, j are guaranteed to exist, as above)

Proofs - III

Because G is connected, there is a path P between i and j.
Suppose that the path P is labelled by $1, 2, \cdots D+1$.
Then:

$$\begin{aligned}
\frac{1}{\sqrt{n}} &\leq u_1 - u_{D+1} \\
&= (u_1 - v_1) + (v_1 - u_2) + (u_2 - v_2) + \cdots + (v_D - u_{D+1}) \\
&\leq |u_1 - v_1| + |v_1 - u_2| + \cdots + |v_D - u_{D+1}| \\
&\leq \sqrt{(u_1 - v_1)^2 + (v_1 - u_2)^2 + \cdots + (v_D - u_{D+1})^2} \cdot \sqrt{2D+1}.
\end{aligned}$$

Proofs - IV

Since $A_{ii}, A_{ii+1} \geq \frac{1}{d}$,

$$\begin{aligned} & \sum_{i,j} A_{ij}(u_i - v_j)^2 \\ \geq & \frac{1}{d} \cdot [(u_1 - v_1)^2 + (v_1 - u_2)^2 + \cdots + (v_D - u_{D+1})^2] \\ \geq & \frac{1}{dn(2D+1)} \\ \geq & \frac{1}{2dn^2}. \end{aligned}$$

Random walk lemma

对于 d-regular 图，走 n2logn步到达均匀分布，很难枚举出来

Lemma

Let G be a d-regular n-vertex graph with all vertices having a selfloop. Let s be a vertex in G. Let $l > \Omega(dn^2 \log n)$, and X_l be the distribution of the vertex of the lth step in a random walk from s. Then for every t,

$$\Pr[X_l = t] > \frac{1}{2n}.$$

走一步后，只记住当前的路径

Proofs 不讲了

By the previous lemma,

$$||A^l p - 1||_2 \leq (1 - \frac{1}{4dn^2})^{\Omega(dn^2 \log n)} < \frac{1}{n^\alpha}$$

for some constant α.
Choose α such that for $q = A^l p$,

$$|q - 1|_1 < \frac{1}{n^2}.$$

Therefore, the probability that $X_l = t$ is at least

$$\frac{1}{n} - \frac{1}{n^2} \geq \frac{1}{2n}.$$

Run the l-step random walks for $O(n \log n)$ many times, almost surely, every vertex is visited.
This gives a randomized log space algorithm to decide the connectivity of two vertices.

(n, d, λ)-expander graph

Definition

It is an n-vertex, d-regular graph G, satisfying $\lambda(G) \leq \lambda$ for some $\lambda < 1$.

A family of graphs $\{G_n\}$ is an expander family, if there exist d, $\lambda < 1$ such that for every n, G_n is an (n, d, λ)-expander graph.

(n, d, ρ)-combinatorial edge expander

For every S, $|S| \leq \frac{n}{2}$,

$$|E(S, \bar{S})| \geq \rho \cdot d \cdot |S|.$$

S出去的边数

Theorem

For each $\epsilon > 0$, there is $d = d(\epsilon)$ and N such that for all $n > N$, there is an $(n, d, \frac{1}{2} - \epsilon)$-edge expander.

从任何一个子集合出去都有半个边和外面的相连

Probabilistic argument.

Random graphs are expanders with high probability.

Characterisation

Theorem

1) *If G is (n, d, λ)-expander, then it is $(n, d, \frac{1-\lambda}{2})$-edge expander.*
2) *If G is (n, d, ρ)-edge expander, then*

$$\lambda(G) \leq 1 - \frac{\rho^2}{2}.$$

Furthermore, if G has all self loops, it is $(n, d, 1-\epsilon)$-expander, $\epsilon = \min\{\frac{2}{d}, \frac{\rho^2}{2}\}$.

Algebraic expander implies combinatorial edge expansion

Lemma

Let G be an (n, d, λ)-expander. $S \subset V$, $T = \overline{S}$. Then:

$$|E(S,T)| \geq (1-\lambda)\frac{d|S| \cdot |T|}{|S| + |T|}.$$

Define $x \in \mathbb{R}^n$ by
$x_i = |T|$, if $i \in S$, and $-|S|$, otherwise.
Then:

$$||x||_2^2 = |S| \cdot |T|^2 + |T| \cdot |S|^2 = |S| \cdot |T| \cdot (|S| + |T|).$$

$x \perp 1$, since $\sum x_i = 0$.
Set $Z = \sum_{i,j} A_{ij}(x_i - x_j)^2$.
If i, j are all in S or T, $x_i - x_j$, and if i, j are in the cut, then $(x_i - x_j)^2 = (|S| + |T|)^2$.

Proof - I

Therefore,

$$Z = \frac{2}{d} \cdot |E(S,T)| \cdot (|S| + |T|)^2.$$

On the other hand,

$$\begin{aligned} Z &= \sum_{i,j} A_{ij}(x_i - x_j)^2 \\ &= \sum_{i,j} A_{ij}x_i^2 - 2\sum_{i,j} A_{ij}x_i x_j + \sum_{i,j} A_{ij}x_j^2 \\ &= 2||x||_2^2 - 2\langle x, Ax\rangle. \end{aligned}$$

Proof - II

Therefore

$$\frac{1}{d} \cdot |E(S,T)|(|S| + |T|)^2 = ||x||_2^2 - \langle x, Ax \rangle.$$

Since $x \perp 1$,
(i) $\|Ax\|_2 \leq \lambda \|x\|_2$
(ii) $\langle x, Ax \rangle \leq \|x\|_2 \cdot \|Ax\|_2$.
Finally,

$$|E(S,T)| \geq (1-\lambda)\frac{d|S| \cdot |T|}{|S| + |T|}.$$

Expander mixing lemma

Lemma

Let $G = (V, E)$ be an (n, d, λ)-expander. Let $X, Y \subseteq V$. Then:

$$\left| |E(X, Y)| - \frac{d}{n}|X| \cdot |Y| \right| \leq \lambda d \cdot \sqrt{|X| \cdot |Y|}.$$

Intuition: Expander $\approx$ Pseudorandom

Proof - I

Define $\psi_X(x) = \sqrt{d}$, if $x \in X$, and 0, otherwise.
Then:

$$\psi_X A \psi_Y^{\mathrm{T}} = e(X, Y) = |E(X, Y)|.$$

Let $\phi_1, \phi_2, \cdots, \phi_n$ be the orthonormal eigenvectors of A.
Suppose that

$$\psi_X = a_1\phi_1 + a_2\phi_2 + \cdots + a_n\phi_n$$

$$\psi_Y = b_1\phi_1 + b_2\phi_2 + \cdots + b_n\phi_n.$$

Then $\phi_1 = \sqrt{n}1$, $a_1 = \frac{\sqrt{d}}{\sqrt{n}}|X|$, and $b_1 = \frac{\sqrt{d}}{\sqrt{n}}|Y|$.

Proof - II

$$
\begin{aligned}
|e(X,Y) - a_1 b_1| &= \left| \sum_{i=2}^{n} a_i b_i \lambda_i \right| \\
&\leq \lambda(G) |\sum_{i=2}^{n} a_i b_b| \\
&\leq \lambda(G) \sqrt{\sum_{i=2}^{n} a_i^2 \cdot \sum_{i=2}^{n} b_i^2}. \qquad (3)
\end{aligned}
$$

By definition,

$$
\sum_{i=1}^{n} a_i^2 = \|\psi_X\|_2^2 = d \cdot |X|.
$$

Proof - III

Giving

$$\sqrt{\sum_{i=1}^{n} a_i^2} = \sqrt{d \cdot |X|}.$$

Therefore,

$$\left| e(X,Y) - \frac{d \cdot |X| \cdot |Y|}{n} \right| \leq \lambda(G)\sqrt{d|X|} \cdot \sqrt{d|Y|} = \lambda d \sqrt{|X| \cdot |Y|}.$$

X到Y的边数

Combinatorial edge expansion implies algebraic expander

Let $G = (V, E)$ be n-vertex, d degree such that for any $S \subset V$ of size $\leq \frac{n}{2}$, $e(S, \overline{S}) \geq \rho d|S|$. 出去的边>

We will show that $\lambda(G) \leq 1 - \frac{\rho^2}{2}$.

Let A be the matrix of G, and λ be the second largest absolute eigenvalue of A.

Then there exists a u such that

(i) $u \perp 1$

(ii) $Au = \lambda u$.

Proof - I

Let $v_i = u_i$, if $u_i > 0$, and 0 otherwise.
Let $w_i = u_i$ if $u_i < 0$, and 0, otherwise.
Then $u = v + w$. Since $u \perp 1$, $v, w \neq 0$.
Suppose WLOG that the number of i's such that $v_i \neq 0$ is at most $\frac{n}{2}$.
Set $Z = \sum_{i,j} A_{ij} \left| v_i^2 - v_j^2 \right|$.
We will prove

(1) $Z \geq 2\rho \|v\|_2^2$.

(2) $Z \leq \sqrt{8(1-\lambda)} \|v\|_2^2$.

The result follows.

For (1)

Suppose $v_1 \geq v_2 \geq \cdots \geq v_n$. So $v_i = 0$ for $i > \frac{n}{2}$.
For $i < j$:

$$v_i^2 - v_j^2 = \sum_{k=i}^{j-1} (v_k^2 - v_{k+1}^2).$$

By the assumption of v_i's,

$$Z = \sum_{i,j} A_{ij} \left| v_i^2 - v_j^2 \right| = 2 \sum_{i<j} A_{ij} \sum_{k=i}^{j-1} (v_k^2 - v_{k+1}^2).$$

For fixed k, for every edge $i \sim j$ with $i \leq k < j$, the term $v_k^2 - v_{k+1}^2$ appears once.

Proof - I

Therefore,

$$
\begin{aligned}
Z &= 2\sum_{i<j} A_{ij} \cdot e(\{1,2,\cdots,k\},\{k+1,\cdots,n\}) \cdot (v_k^2 - v_{k+1}^2) \\
&= \frac{2}{d}\sum_{k=1}^{n/2} e(\{1,2,\cdots,k\},\{k+1,\cdots,n\})(v_k^2 - v_{k+1}^2) \\
&\geq \frac{2}{d}\sum_{k=1}^{n/2} \rho \cdot d \cdot k \cdot (v_k^2 - v_{k+1}^2) \\
&= 2\rho\sum_{k=1}^{n/2} k(v_k^2 - v_{k+1}^2) = 2\rho\|v\|_2^2. \qquad (4)
\end{aligned}
$$

For (2)

$$Z \leq \sqrt{8(1-\lambda)} \cdot \|v\|_2^2$$

Recall $Au = \lambda u$, $u = v + w$, $u \perp 1$, $v \perp w$.

$$\langle Av, v\rangle + \langle Aw, v\rangle = \langle Au, v\rangle = \langle \lambda(v+w), v\rangle = \lambda\|v\|_2^2$$

Since $\langle Aw, v\rangle < 0$, $\frac{\langle Av,v\rangle}{\langle v,v\rangle} \geq \lambda$.
Therefore

$$\begin{aligned} & 1-\lambda \\ \geq\ & 1 - \frac{\langle Av, v\rangle}{\|v\|_2^2} = \frac{\|v\|_2^2 - \langle Av, v\rangle}{\|v\|_2^2} \\ =\ & \frac{\sum_{i,j} A_{ij}(v_i - v_j)^2}{2\|v\|_2^2}. \end{aligned} \tag{5}$$

Proof - II

Note $Z = \sum_{i,j} A_{ij}(v_i - v_j)^2 = 2\|v\|_2^2 - 2\langle Av, v\rangle$.

Cauch-Schwarz: $\langle x, y\rangle \leq \|x\|_2 \cdot \|y\|_2$.

Let $x_{ij} = \sqrt{A_{ij}}(v_i - v_j)$, $y_{ij} = \sqrt{A_{ij}}(v_i - v_j)$.

$$
\begin{aligned}
&(\sum_{i,j} A_{ij}(v_i - v_j)^2) \cdot (\sum_{i,j} A_{ij}(v_i + v_j)^2) \\
&\geq (\sum_{i,j} A_{ij}(v_i - v_j) \cdot (v_i + v_j))^2 = Z^2. \qquad (6)
\end{aligned}
$$

Proof - III

$$
\begin{aligned}
& 2\|v\|_2^2 \sum_{i,j} A_{ij}(v_i + v_j)^2 \\
= \quad & 2\|v\|_2^2 (\sum A_{ij} v_i^2 + 2 \sum A_{ij} v_i v_j + \sum A_{ij} v_j^2) \\
= \quad & 2\|v\|_2^2 (2\|v\|_2^2 + 2\langle Av, v\rangle). \qquad (7)
\end{aligned}
$$

Noting
(i) $\|Av\|_2 \leq \|v\|_2$
(ii) $\langle Av, v\rangle \leq \|Av\|_2 \cdot \|v|_2 \leq \|v\|_2^2$.
Finally, $1 - \lambda \geq \frac{Z^2}{8\|v\|_2^4}$, giving

$$Z \leq \sqrt{8(1-\lambda)} \cdot \|v\|_2^2.$$

Spectral norm

矩阵的范数

For every matrix A, define the *spectral norm* of A, written $\|A\|$, as follows:

$$\begin{aligned} \|A\| &= \max\{\|Av\|_2 : \|v\|_2 = 1\} \\ &= \max\{\frac{\|Av\|_2}{\|v\|_2}\}. \end{aligned} \tag{8}$$

Proposition For any matrices A, B,
(1) $\|A+B\| \leq \|A\| + \|B\|$, and
(2) $\|AB\| \leq \|A\| \cdot \|B\|$.

Extracting randomness from expander

Theorem

Let A be the adjacency matrix of an (n, d, λ)-expander graph G. Let J be the $n \times n$ matrix such that $J_{ij} = \frac{1}{n}$ for all i, j. Then

$$A = (1 - \lambda)J + \lambda C$$

随机矩阵+小于等于1的

for some C with $\|C\| \leq 1$.

Intuition A uniformly random distribution can be extracted from an expander. If λ is small, then G is largely a random graph.

Proof - I

Solving C, we have

$$C = \frac{1}{\lambda}(A - (1-\lambda)J).$$

We prove $\|C\| \leq 1$, that is, for every v, $\|Cv\|_2 \leq \|v\|_2$.
Fix v.
Set
$v = u + w$, $u = \alpha 1$, $w \perp 1$. 分解为平行1和垂直1的
We have
(1) $Cu = u$, easy
(2) For $w' = Aw$,

$$Cw = \frac{1}{\lambda}w'$$

Because: $w \perp 1$, so $\sum w_i = 0$, and hence $Jw = 0$.

Proof - II

(3) $Cv = C(u + w) = u + \frac{1}{\lambda}w'$
(4)

$$\|Cv\|_2^2 = \|u\|_2^2 + \|\frac{1}{\lambda}w'\|_2^2 = \|u\|_2^2 + \frac{1}{\lambda^2} \cdot \|Aw\|_2^2$$
$$\leq \|u\|_2^2 + \frac{1}{\lambda^2} \cdot \lambda^2 \cdot \|w\|_w\|_2^2 = \|v\|_2^2. \quad (9)$$

Intuition of expanders

- Expander is basically a random graph
- The nice properties of expander graphs can be achieved simply by randomness
- Randomness plays an essential role for expanders:
- Information quickly spreads in expander graphs
- Viruses quickly infect the whole expander graphs
  (Here there is a dilemma to achieve both security and quick spreading of information in communication networks. Expanders may not be the best model for communication networks.

快速传播的通讯网络同样具有安全性的问题

如何做到有安全性又快速传播

Expander walk theorem

对于一个小集合B，走了k步后还在B中的概率非常小

走几步之后不会在小圈子里转，一定会跑出去

Theorem

Let G be an (n, d, λ)-expander graph. Let $\mathcal{B}$ be a set of $[n]$ of size $\leq \beta n$, $0 < \beta < 1$. Let $X_1, X_2, \cdots, X_k$ be a random walk in G from X_1, where X_1 is randomly and uniformly chosen. Then:

$$\Pr[(\forall i \in [k])[X_i \in \mathcal{B}]] \leq ((1-\lambda)\sqrt{\beta} + \lambda)^{k-1}.$$

网络的设计，可以设计一个小圈，不容易走出来（安全性）

Proof - I

For each i, $1 \leq i \leq k$, let
B_i: the event $X_i \in \mathcal{B}$.
Then:

$$\begin{aligned} & \Pr[\wedge_{i=1}^{k} B_i] \\ = \quad & \Pr[B_1] \cdot \Pr[B_2|B_1] \cdot \cdots \cdot \Pr[B_k \,|B_1, \cdots, B_{k-1}]. \end{aligned} \tag{10}$$

Define B to be a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^n$ that keeps the values indexed in $\mathcal{B}$. That is, for $(u_1, u_2, \cdots, u_n)$, the $(Bu)_i$ is u_i, if $i \in \mathcal{B}$, and 0 otherwise.

Proof - II

For every probability vector p,
(i) Bp is the vector whose coordinates sum to the probability that a vertex i is chosen according to p, is in $\mathcal{B}$.
(ii) The normalised Bp is the distribution of p conditioned to the event that the vertex is in $\mathcal{B}$.

Proof - III

Let p^i be the distribution of X_i conditioned on the events $B_1, \cdots, B_i$. Then:

$$p^1 = \frac{1}{\Pr[B_1]} \cdot B1$$

$$p^2 = \frac{1}{\Pr[B_2|B_1]\Pr[B_1]} BAB1$$

$$p^i = \frac{1}{\Pr[B_i\ |B_{i-1}, \cdots B_1] \cdots \Pr[B_1]} (BA)^{i-1} B1.$$

Hence,

$$\Pr[B_1] \cdots \Pr[B_k|B_{k-1} \cdots B_1] p^k = (BA)^{k-1} B1.$$

Proof - IV

$$\Pr[\wedge_{i=1}^{k} B_i] = \Pr[B_1] \cdots \Pr[B_k | B_{k-1} \cdots B_1] = |(BA)^{k-1} B1|_1.$$

Let $A = (1-\lambda)J + \lambda C$.
Then $BA = (1-\lambda)BJ + \lambda BC$.
Noting:
(i) $\|B1\|_2 \leq \sqrt{\beta}\|1\|_2$
(ii) $\|BJ\| \leq \sqrt{\beta}$, $\|B\| \leq 1$, $\|BC\| \leq 1$.
(iii) $\|BA\| \leq (1-\lambda)\sqrt{\beta} + \lambda$
Therefore,

$$\begin{aligned} |(BA)^{k-1} B1|_1 &\leq \|(BA)^{k-1} B1\|_2 \cdot \sqrt{n} \\ &\leq ((1-\lambda)\sqrt{\beta} + \lambda)^{k-1}. \end{aligned} \tag{11}$$

Rotation map

Given a d-regular graph G, n个节点

$$\widehat{G}: [n] \times [d] \to [n] \times [d]$$ 构造另一个图

$\widehat{G}(u,i) = (v,j)$ means:
(i) v is the i-th neighbor of u, and
(ii) u is the j-th neighbor of v.
$\widehat{G}$ is log space computed.

目的：把λ变小

log空间的规约

The matrix product

GG' corresponds to AA'

$$\lambda(GG') \leq \lambda(G) \cdot \lambda(G').$$

The tensor product

Graphs G, G'
matrices A, A'
$G \otimes G'$ 图乘积
$A \otimes A'$.

$$\lambda(G \otimes G') \leq \max\{\lambda(G), \lambda(G')\}.$$

Replacement product

Given:
(i) G: n vertices, degree D
(ii) G': D vertices, degree d.
Define the replacement product:

$$A \circ_R A' = \frac{1}{2}\widehat{A} + \frac{1}{2}(I_n \otimes A')$$

$\widehat{A}$ is the matrix of the rotation map of G.

Lemma

If $\lambda(G) \leq 1 - \epsilon$, $\lambda(H) \leq 1 - \delta$, *then*

$$\lambda(G \circ_R H) \leq 1 - \frac{\epsilon\delta^2}{24}.$$

The construction

1. Let H be a $(D = (2d)^{100}, d, 0.01)$-expander, d constant.
2. Let G_1 be a $((2d)^{100}, 2d, \frac{1}{2})$-expander
   G_2 be a $((2d)^{200}, 2d, \frac{1}{2})$-expander.
3. For $k > 2$,

$$G_k = (G_{\lfloor \frac{k-1}{2} \rfloor} \otimes G_{\lceil \frac{k-1}{2} \rceil})^{50} \circ_R H.$$

Theorem

G_k is $((2d)^{100k}, 2d, 1 - \frac{1}{50})$-expander graph.

UPATH is in RL

UPATH: Given an undirected graph G, for given s, t, decide whether or not there is a path from s to t.
Assume G is regular and has self-loop at every vertex.
By the previous theorems, for $l = n^4$, with probability $\geq \frac{2}{3}$, a random walk of length l hits t, if there is a path from s to t.
So
UPATH is in RL, randomised log space.

Connectivity of expander

For regular graphs with self-loop at each vertex, we have:
1) If G is connected and $\lambda(G) < 1$, then the diameter of G is $O(\log n)$.
2) If there is a constant $\lambda < 1$ such that for every connected component H of G, $\lambda(H) \leq \lambda$, then for every H, the diameter of H is $O(\log n)$.
For a graph with property 2), there is a deterministic log space algorithm to decide for given s, t, whether or not there is a path from s to t.

UPATH $\in$ L

Reduction: for a regular graph G,

1) Let G_0 be obtained from G by adding self-loops such that G_0 has degree d^{50} for some constant d.
2) Let H be a $(d^{50}, \frac{d}{2}, 0.01)$-expander.
3) Gor $k \geq 1$,

$$G_k = (G_{k-1} \circ_R H)^{50}.$$

Proof

Lemma

For every $k \geq 0$, every connected component in G_k is an $(d^{50k}n, d^{20}, 1-\epsilon)$-expander, where $\epsilon = \min\{\frac{1}{20}, \frac{1.5^k}{12n^2}\}$, there n is the number of vertices in G.

For $k = 10 \log n$, ϵ is constant.
G_k is computed from G by log space, and the connectivity in G_k is decided in log space.

Conclusions and discussion

1. expander $\approx$ random graph
2. expander can be used to de-randomize
3. information quickly spreads in expander
4. explicit construction of expanders can be used in new algorithms

Open questions

- Resolving the dilemma of expander walk and security of networks
- Is expander an idea model for engineering networks?
- Can we decompose a network similar to that of expanders as random part and the other part? Possible applications?
- Information theoretical characterisation of expander (in progress)
- Super expander? (in progress) 用信息论刻画

Exercises 1

1. Recall the spectral norm of a matrix A, written $\|A\|$ to be the $\|Av\|_2$ for unit v. Let A be symmetric stochastic, i.e., $A = A^{\mathrm{T}}$, and every row and column of A has nonnegative entries summing up to 1. Prove that $\|A\| \leq 1$.
2. Let A, B be symmetric stochastic matrices. Prove that $\lambda(A + B) \leq \lambda(A) + \lambda(B)$.
3. Let A, B be two $n \times n$ matrices.
   (a) Prove that $\|A + B\| \leq \|A\| \cdot \|B\|$.
   (b) Prove that $\|AB\| \leq \|A\| \cdot \|B\|$

Exercises 2

Let G be an (n, d, λ)-expander graph, and $\mathcal{B}$ be a set of vertices of size at most βn for $0 < \beta < 1$. Let $X_1, X_2, \cdots, X_k$ be a random walk of k steps in G from X_1 that is randomly and uniformly chosen.

1. Prove that for every subset $I \subseteq [k]$,

$$\Pr[(\forall i \in I)[X_i \in \mathcal{B}]] \leq (1 - \lambda)\sqrt{\beta} + \lambda)^{|I|-1}.$$

2. Conclude that if $\mathcal{B} < n/100$ and $\lambda < 1/100$, then the probability that there exists a subset $I \subseteq [k]$ such that $|I| > k/10$ and $\forall_{i \leq |I|} X_i \in \mathcal{B}$ is at most $2^{-k/100}$.
3. To show that every BPP algorithm that uses m coins and decides a language L with probability 0.99 into an algorithm B that uses $m + O(k)$ coins and decides the language L with probability $1 - 2^{-k}$.