Expander Graphs and Their Applications (VIII)

Yijia Chen
Shanghai Jiaotong University

Last Lecture

The Zig-Zag Theorem

Theorem

If G is an (n, m, α)-graph and H an (m, d, β)-graph. Then $G \textcircled{z} H$ is an $(nm, d^2, \varphi(\alpha, \beta))$-graph, where

$$\varphi(\alpha, \beta) = \frac{1}{2}(1 - \beta^2)\alpha + \frac{1}{2}\sqrt{(1 - \beta^2)^2\alpha^2 + 4\beta^2}.$$

Corollary

If G is an (n, m, α)-graph and H an (m, d, β)-graph. Then

$$1 - \hat{\lambda}(G \textcircled{z} H) \geq \frac{1}{2}(1 - \beta^2)(1 - \alpha)$$

Lower Bound of $d - \lambda$ in Arbitrary Graphs

Theorem

Let G be a connected, d-regular, and non-bipartite graph with n vertices. Then

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

Reingold's Algorithm for Graph Reachability Problem

Theorem (Omer Reingold, 2005)

There is an algorithm that solves the reachability problem on any graph $G = (V, E)$ using space $O(\log |V|)$.

Let H be a $(d^{16}, d, 1/2)$-graph for some constant $d \in \mathbb{N}$.

Input: A d^{16}-regular graph G with $n := |V(G)|$ and two vertices $s, t \in V(G)$.
Output: Is there a path between s and t in G?

1. Choose some $\ell = O(\log n)$ such that

$$\left(1 - \frac{1}{d^{16} n^2}\right)^{2^\ell} \leq \frac{1}{2}.$$

2. $G_0 \leftarrow G$.
3. **for** $i = 1$ **to** ℓ **do** $G_i \leftarrow (G_{i-1} \circledz H)^8$.
4. Check if s and t are connected in G_ℓ.

The Analysis of Reingold's Algorithm

For all $i \in [\ell]$ and every *connected component* C of G, we define

$$C_0 := C \quad \text{and} \quad C_i := (C_{i-1} \textcircled{z} H)^8$$

It is easy to see

$$G_i := \bigcup_{\substack{C \text{ a connected} \\ \text{component of } G}} C_i$$

Proposition

$$\hat{\lambda}(C_i) \leq \max\left\{\hat{\lambda}^2(C_{i-1}), \frac{1}{2}\right\}.$$

The Analysis of Reingold's Algorithm (cont'd)

Proposition *For every connected component C of G and all $i \in [\ell]$*

$$\hat{\lambda}(C_i) \leq \max\left\{\hat{\lambda}^2(C_{i-1}), \frac{1}{2}\right\}.$$

Corollary

For every connected component C of G

$$\hat{\lambda}(C_\ell) \leq \frac{1}{2}.$$

The Base Graphs

Recall:

1. In the inductive construction of expander graph family using the zig-zag product, we start with a $(d^4, d, 1/4)$-graph.

2. In Reingold's algorithm, we start with a $(d^{16}, d, 1/2)$-graph.

In the following, we

- provide some *explicit construction*,
- and prove their existence by the *probabilistic method*.

Graph Squaring

Recall:
Let G be a graph with adjacency matrix A, and let $i \in \mathbb{N}$. Then, G^i is the ith power of G whose adjacency matrix is A^i.

Theorem

If G is an (n, d, α)-graph, then G^i is an (n, d^i, λ^i)-graph.

Tensor Product

Let $\vec{u} \in \mathbb{R}^{n_1}$ and $\vec{v} \in \mathbb{R}^{n_2}$. Then their tensor product is

$$\vec{u} \otimes \vec{v} \in \mathbb{R}^{n_1 \cdot n_2}$$

whose (i, j)th entry is $u_i \cdot v_j$ for every $i \in [n_1]$ and $j \in [n_2]$.

Let A be an $n_1 \times n_1$ matrix and B an $n_2 \times n_2$ matrix, then their tensor product $A \otimes B$ is an $n_1 \cdot n_2 \times n_1 \cdot n_2$ matrix such that for every $(i_1, j_1), (i_2, j_2) \in [n_1] \times [n_2]$

$$(A \otimes B)_{(i_1, j_1),(i_2, j_2)} = A_{i_1, i_2} \cdot B_{j_1, j_2}.$$

Lemma

$(A \otimes B)(\vec{u} \otimes \vec{v}) = (A\vec{u}) \otimes (B\vec{v})$.

Eigenvalues and Eigenvectors of Tensor Product

Theorem

If α is an eigenvalue for A with corresponding eigenvector $\vec{u}$, and β is an eigenvalue for B with corresponding eigenvector $\vec{v}$, then $\alpha \cdot \beta$ is an eigenvalue for $A \otimes B$ with corresponding eigenvector $\vec{u} \otimes \vec{v}$.

Theorem

Let A be an $n_2 \times n_2$ matrix with eigenvalues $\alpha_1, \ldots, \alpha_{n_1}$ and corresponding orthogonal eigenvectors $\vec{u}_1, \ldots, \vec{u}_{n_1}$. And let B be an $n_2 \times n_2$ matrix with eigenvalues $\beta_1, \ldots, \beta_{n_2}$ and corresponding orthogonal eigenvectors $\vec{v}_1, \ldots, \vec{v}_{n_2}$. Then $A \otimes B$ has eigenvalue

$$\alpha_1 \cdot \beta_1, \alpha_2 \cdot \beta_1, \ldots, \alpha_{n_1} \cdot \beta_1, \alpha_1 \cdot \beta_2, \ldots, \alpha_{n_1} \cdot \beta_{n_2}$$

with corresponding orthogonal eigenvectors

$$\vec{u}_1 \otimes \vec{v}_1, \vec{u}_2 \otimes \vec{v}_1, \ldots, \vec{u}_{n_1} \otimes \vec{v}_1, \vec{u}_1 \otimes \vec{v}_2, \ldots, \vec{u}_{n_1} \otimes \vec{v}_{n_2}.$$

Graph Tensoring

Let G, H be two graphs with adjacency matrices A and B, respectively. Then, their tensor product $G \otimes H$ is the graph whose adjacency matrix is $A \otimes B$.

Theorem

If G_i is an (n_i, d_i, α_i) graph for $i = 1, 2$, then $G_1 \otimes G_2$ is an

$$(n_1 \cdot n_2, d_1 \cdot d_2, \max\{\alpha_1, \alpha_2\})\text{-graph}.$$

Proof.

$$\begin{aligned}\hat{\lambda}(G_1 \otimes G_2) &= \max\left\{\left|\hat{\lambda}_i(G_1) \cdot \hat{\lambda}_j(G_2)\right| \mid i \in [n_1], j \in [n_2], \text{ and } (i \neq 1 \text{ or } j \neq 1)\right\} \\ &= \max\left\{\hat{\lambda}(G_1), \hat{\lambda}(G_2)\right\}.\end{aligned}$$

□

The Affine Plane

Let $q := p^t$ where p is a prime and $t \in \mathbb{N}$. And let $\mathbb{F}_q$ be the *finite field of size* q.

Then AP_q is a graph with vertex set $\mathbb{F}_q^2$ and edge set

$$\{\text{an edge between } (a, b) \text{ and } (c, d) \mid a, b, c, d \in \mathbb{F}_q \text{ and } ac = b + d\}.$$

Equivalently, we connect the vertex (a, b) to all points on the line

$$L_{a,b} := \{(x, y) \mid y = ax - b\}.$$

The Affine Plane (cont'd)

Lemma
AP_q is a $(q^2, q, 1/\sqrt{q})$-graph.

Proof. Let M be the $q^2 \times q^2$ normalized adjacency matrix of AP_q. The entry of M^2 in row (a, b) and column (a', b') is exactly the number of common neighbors of (a, b) and (a', b') *divided by q^2*, i.e.,

$$\left|L_{a,b} \cap L_{a',b'}\right|/q^2.$$

.

- If $a \neq a'$, then $|L_{a,b} \cap L_{a',b'}| = 1$.
- If $a = a'$ and $b \neq b'$, then $|L_{a,b} \cap L_{a',b'}| = 0$
- If $a = a'$ and $b = b'$, then $|L_{a,b} \cap L_{a',b'}| = q$

Proof (cont'd)

Let I_q be the $q \times q$ identity matrix and J_q the $q \times q$ all-one matrix.

$$M^2 = \frac{1}{q^2}\begin{pmatrix} qI_q & J_q & \dots & J_q \\ J_q & qI_q & \dots & J_q \\ \vdots & & \ddots & J_q \\ J_q & J_q & \dots & qI_q \end{pmatrix} = \frac{1}{q^2}\Big(I_q \otimes qI_q + (J_q - I_q) \otimes J_q\Big)$$

J_q has eigenvalues q (multiplicity 1) and 0 (multiplicity $q-1$). Therefore, $(J_q - I_q) \otimes J_q$ has

eigenvalue	$(q-1)q$	$-q$	0
multiplicity	1	$q-1$	$(q-1)q$

By adding $I_q \otimes qI_q$ and dividing by q^2, we get for M^2

eigenvalue	1	0	$1/q$
multiplicity	1	$q-1$	$(q-1)q$

Thus $\lambda(M) = 1/\sqrt{q}$. □

Let

$$AP_q^1 := AP_q \otimes AP_q$$
$$AP_q^{i+1} := AP_q^i \textcircled{z} AP_q.$$

Theorem
AP_q^i is an $(q^{2(i+1)}, q^2, i/\sqrt{q})$-graph.

Choosing some sufficiently large q, we can get a $(d^4, d, 1/4)$-graph or a $(d^{16}, d, 1/2)$ graph.

The Probabilistic Method

Main Theorem

Theorem

There exists a constant $c > 0$ *such that for all sufficiently large* $n \in \mathbb{N}$ *three exists an* n*-vertex, 3-regular graphs with* $h(G) \geq c$.

Random Perfect Matching

Definition

Let G be a graph. A matching M of G is a subset of $E(G)$ (without selfloop) such that *every vertex appears in at most one edge of the subset.* M is a perfect matching of G if every vertex is incident to one edge in M.

Let $k \in \mathbb{N}$ and $V := [2k]$. Consider the following random process $\mathbb{P}(k)$:

1. $S \leftarrow V$ and $E \leftarrow \emptyset$.
2. **while** $S \neq \emptyset$ **do**
3. Choose a pair $(u, v) \in S^2$ uniformly at random.
4. $S \leftarrow S \setminus \{u, v\}$ and $E \leftarrow E \cup \{$an edge between u and $v\}$.
5. Output E.

$\mathbb{P}(k)$ is a random perfect matching on $[2k]$.

Random d-Regular Graph

Let $k, d \in \mathbb{N}$ and consider the random process $\mathbb{R}_d(k)$.

1. $V \leftarrow [2k]$ and $E \leftarrow \emptyset$.
2. **for** $\ell = 1$ **to** d **do**
3. $\quad E \leftarrow E \cup \mathbb{P}(k)$
4. Output (V, E).

$\mathbb{R}_d(k)$ is a d-regular graph on vertices $[2k]$.

An Important Warning: $\mathbb{R}_d(k)$ is not uniformly distributed over all d-regular graphs on vertices $[2k]$.

Main Theorem (Restated)

Theorem

There exists a constant $c > 0$ such that for all sufficiently large $k \in \mathbb{N}$

$$\Pr\left[h(\mathbb{R}_3(k)) \geq c\right] > 0$$

Proof.

Consider the event

$E :=$ there exists a subset $S \subseteq V$ with $|S| \leq k = |V|/2$ and $|\partial S| \leq c \cdot |S|$.

By *the union bound*

$$\Pr[E] \leq \sum_{|S| \leq k} \Pr\left[|\partial S| \leq c \cdot |S|\right].$$

Then, it is easy to verify that

$$\Pr[E] \leq \sum_{|S| \leq k} \sum_{\substack{|S'| = c|S|, \\ S \cap S' = \emptyset}} \left[\Gamma(S) \subseteq S'\right]$$

where $\Gamma(S) := \{v \mid v \notin S \text{ and there is an edge between } v \text{ and } S\}$.

$$\begin{aligned}\Pr[E] &\leq \sum_{i \in [k]} \binom{2k}{i} \binom{2k - i}{c \cdot i} \Pr\left[\Gamma([i]) \subseteq [i + c \cdot i]\right] \\ &\leq \sum_{i \in [k]} \binom{2k}{i} \binom{2k}{c \cdot i} \Pr\left[\Gamma([i]) \subseteq [i + c \cdot i]\right].\end{aligned}$$

Proof. (cont'd)

Now we aim to bound $\Pr\left[\Gamma([i]) \subseteq [i + c \cdot i]\right]$ *from above:*

Recall G is the union of three perfect matchings. In one (random) perfect matching $\mathbb{P}(k)$, the probability that all vertices in $[i]$ are matched to vertices in $[i + c \cdot i]$ is bounded by

$$\prod_{j=1}^{\lceil i/2 \rceil} \frac{i + c \cdot i - 2j + 1}{2k - 2j + 1}.$$

Then

$$\begin{aligned}
\prod_{j=1}^{\lceil i/2 \rceil} \frac{i + c \cdot i - 2j + 1}{2k - 2j + 1} &\leq \prod_{j=0}^{\lceil i/2 \rceil - 1} \frac{i + c \cdot i - 2j}{2k - 2j} \\
&= \frac{2^{\lceil i/2 \rceil} \cdot \prod_{j=0}^{\lceil i/2 \rceil - 1} \left(\lceil (i + c \cdot i)/2 \rceil - j \right)}{2^{\lceil i/2 \rceil} \cdot \prod_{j=0}^{\lceil i/2 \rceil - 1} (k - j)} \\
&= \binom{\lceil (i + c \cdot i)/2 \rceil}{\lceil i/2 \rceil} \Big/ \binom{k}{\lceil i/2 \rceil}
\end{aligned}$$

Binary Entropy

Definition

The binary entropy function $H_2 : (0, 1) \longrightarrow \mathbb{R}$ is defined by

$$H_2(p) = -p \log_2 p - (1 - p) \log_2(1 - p).$$

Lemma

For $p \in (0, 1)$ *and* $n \in \mathbb{N}$

$$\binom{n}{\lceil p \cdot n \rceil} \approx 2^{H(p) \cdot n}.$$

Proof. (cont'd)

We have seen

$$\begin{aligned}
&\Pr\left[\text{there exists an } S \subseteq V \text{ with } |S| \le k \text{ and } |\partial S| \le c \cdot |S|\right] \\
&\le \sum_{i \in [k]} \binom{2k}{i} \binom{2k}{c \cdot i} \Pr\left[\Gamma([i]) \subseteq [i + c \cdot i]\right] \\
&\le \sum_{i \in [k]} \binom{2k}{i} \binom{2k}{c \cdot i} \binom{\lceil (i + c \cdot i)/2 \rceil}{\lceil i/2 \rceil}^3 \Big/ \binom{k}{\lceil i/2 \rceil}^3
\end{aligned}$$

Then

$$\begin{aligned}
&\log_2 \left(\binom{2k}{i} \binom{2k}{c \cdot i} \binom{\lceil (i + c \cdot i)/2 \rceil}{\lceil i/2 \rceil}^3 \Big/ \binom{k}{\lceil i/2 \rceil}^3 \right) \\
&\approx H_2(i/2k) \cdot 2k + H_2(c \cdot i/2k) \cdot 2k \\
&\quad + 3 \cdot H_2(i/(i + c \cdot i)) \cdot (i + c \cdot i)/2 - 3H_2(i/2k) \cdot k \\
&= -\left(H_2(i/2k) - 2H_2(c \cdot i/2k)\right) \cdot k + 3 \cdot H_2(1/(1 + c)) \cdot (i + c \cdot i)/2.
\end{aligned}$$

Binary Entropy (cont'd)

Lemma

Let $p \in (0, 1/2)$ *and* $\varepsilon \in (0, 1/2)$*. Then*

$$H_2(\varepsilon \cdot p) \leq \delta \cdot H_2(p)$$

for $\delta := -4 \cdot \varepsilon \cdot \log \varepsilon$*.*

Proof.

$$\begin{aligned}
H_2(\varepsilon \cdot p) &= -\varepsilon \cdot p \cdot \log(\varepsilon \cdot p) - (1 - \varepsilon \cdot p) \log(1 - \varepsilon \cdot p) \\
&\leq -2 \cdot \varepsilon \cdot p \cdot \log(\varepsilon \cdot p) \\
&\leq 4 \cdot \varepsilon \cdot p \cdot \log \varepsilon \cdot \log p \\
&\leq -4 \cdot \varepsilon \cdot \log \varepsilon \cdot H_2(p).
\end{aligned}$$

□

Proof. (cont'd)

For $c \in (0, 1/2)$, recall

$$\log_2 \left(\binom{2k}{i} \binom{2k}{c \cdot i} \binom{\lceil (i + c \cdot i)/2 \rceil}{\lceil i/2 \rceil}^3 \Big/ \binom{k}{\lceil i/2 \rceil}^3 \right)$$
$$\approx - \big(H_2(i/2k) - 2H_2(c \cdot i/2k) \big) \cdot k + 3 \cdot H_2(1/(1+c)) \cdot (i + c \cdot i)/2$$
$$\leq - (1 - c') \cdot H_2(i/2k) \cdot k + c' \cdot i,$$

for $c' := \max \big\{ -8 \cdot c \cdot \log c, 3 \cdot H_2(1/(1+c)) \cdot (1+c)/2 \big\}$.
Now

$$\Pr \big[\text{there exists an } S \subseteq V \text{ with } |S| \leq k \text{ and } |\partial S| \leq c \cdot |S| \big]$$
$$\leq \sum_{i \in [k]} \binom{2k}{i} \binom{2k}{c \cdot i} \binom{\lceil (i + c \cdot i)/2 \rceil}{\lceil i/2 \rceil}^3 \Big/ \binom{k}{\lceil i/2 \rceil}^3$$
$$\leq \sum_{i \in [k]} 2^{-(1-c')H_2(i/2k) \cdot k + c' \cdot i} < 1$$

for some appropriate c (independent of k). □