CMPT 881: Pseudorandomness	Prof. Valentine Kabanets
Lecture 10: Some Constructions of Expander Graphs	
October 7, 2004	*Scribe: Leila Kalantari*

1 Ramanujan Graphs (Lubotzky, Phillips & Sarnak, and Margulis)

1.1 Some Bounds on Spectral Expansion

Theorem 1 *(Alon, Boppana) For an infinite family of d-regular graphs G, $\lambda_2(G) \geq \frac{2\sqrt{d-1}}{d} - o(1)$, where $o(1) \to 0$ as $|V| \to \infty$.*

Theorem 2 *(Friedman '02) For any constant d and $\epsilon > 0$, a random d-regular graph has $\lambda_2(G) \leq \frac{2\sqrt{d-1}}{d} + \epsilon$, with probability $\geq 1 - n^{-\Omega(\sqrt{d})}$.*

Ramanujan d-regular graphs are those graphs G for which $\lambda_2(G) \leq \frac{2\sqrt{d-1}}{d}$. Explicit constructions of such graphs are known. In the next section we give one such construction due to Lubotzky, Phillips, and Sarnak.

1.2 Construction of Ramanujan Graphs

Let p and q be two prime numbers such that $p \equiv 1 \mod 4$, $q \equiv 1 \mod 4$ and $q \geq 2\sqrt{p}$. Let

$$\begin{aligned} S = &\{(a_0, a_1, a_2, a_3) | a_i \in \mathbb{Z}_p, a_0 > 1, \quad a_0 \text{ is odd}, \\ & a_1, a_2, a_3 \text{ are even, and} \\ & a_0^2 + a_1^2 + a_2^2 + a_3^2 = p\} \end{aligned}$$

By Number Theory, it can be shown that $|S| = p + 1$. It can also be shown that there is an i such that $i^2 \equiv -1 \mod q$. Then define for every $\alpha = (a_0, a_1, a_2, a_3) \in S$, the matrix $\tilde{\alpha} \equiv \begin{bmatrix} a_0+ia_1 & a_2+ia_3 \\ -a_2+ia_3 & a_0-ia_1 \end{bmatrix}$ mod q. Note that $\det(\tilde{\alpha}) \equiv p \mod q$.

Definition 3 *The group $PGL(2, \mathbb{Z}_q)$ is the quotient group of all 2x2 invertible matrices over $\mathbb{Z}_q$ modulo $\{\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}, \lambda \neq 0\}$.*

Definition 4 *The group $PSL(2, \mathbb{Z}_q)$ is the quotient group of all 2x2 matrices over $\mathbb{Z}_q$ with determinant 1, modulo $\{I, -I\}$ where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.*

Define $G = (V, E)$, where $V = PGL(2, \mathbb{Z}_q)$, and $E = \{(A, B) | \exists \alpha \in S \;\; s.t. \;\; B = A\tilde{\alpha}\}$. The degree of G is $p + 1$. The number of vertices is $\approx q^3$. This graph is Ramanujan, i.e., $|\lambda_2| \leq \frac{2\sqrt{p}}{p+1}$.

1. When p is a non-square modulo q, then the Ramanujan graph constructed above is bipartite.

2. When p is a square modulo q, then by letting $V = PSL(2, \mathbb{Z}_q)$, we obtain a non-bipartite Ramanujan graph.

The expansion for these Ramanujan graphs is $\frac{d}{2}$, where d is the degree of the graph. This is still far from non-constructive bounds of expansion, like $d - 1.01$.

Open Problem 5 *Construct an explicit d-regular graph for some d, with expansion $d - \theta(1)$.*

It is known how to construct (unbalanced) bipartite expander graphs with expansion $(1-\epsilon)d$ for a given $\epsilon > 0$ [Capalbo, Reingold, Vadhan, & Wigderson], but it is still open how to construct *non-bipartite* expanders with such an expansion factor.

2 Zig-Zag Expanders (Reingold, Vadhan, Wigderson '02)

2.1 Idea

Start with a "constant-size" expander H. By applying certain operations on the graph, turn H into an expander of "large" size. The operation will increase the number of vertices, but keep the degree constant, and keep the spectral expansion bounded away from 1.
Recall our notation: (n, d, λ)-graph is a d-regular multigraph on n vertices, with spectral expansion λ, i.e., $\max_{i>1} |\lambda_i| \leq \lambda$.

We will use the following operations:

- Squaring: $G \longrightarrow G^2$
- Tensor product: $G_1, G_2 \longrightarrow G_1 \otimes G_2$
- Zig-zag product: $G, H \longrightarrow G ⓩ H$

2.2 Squaring

Definition 6 *For a multigraph $G = (V, E)$, define $G^2 = (V, E')$ where $E' = \{(x, y) | \exists z \in V, (x, z), (z, y) \in E\}$ (there is a path of length exactly 2 between x and y in G).*

Lemma 7 *Let G be an (n, d, λ)-graph. Then G^2 is an (n, d^2, λ^2)-graph.*

Note that Squaring improves spectral gap, worsens degree and does not affect the size of the graph.

2.3 Zig-Zag Product

We will define zig-zag product later in the course.

Lemma 8 (Zig-Zag Lemma) *Let G be an (n_1, d_1, λ_1)-graph, and let H be an (d_1, d_2, λ_2)-graph. Then $G ⓩ H$ is an $(n_1 d_1, d_2^2, f(\lambda_1, \lambda_2))$-graph, where $f(\lambda_1, \lambda_2) \leq \lambda_1 + \lambda_2 + \lambda_2^2$.*

Note: Think of H as a "small" graph and of G as a "large" graph. Then $G ⓩ H$ is a "bigger" graph such that

1. degree of $G ⓩ H$ is a d_2^2, i.e., smaller than d_1.
2. If λ_1 and λ_2 are sufficiently small, then $G ⓩ H$ is an expander.

2.4 Zig-Zag Construction: First Attempt

Let H be a (d^4, d, λ_0)-graph for $\lambda_0 \leq \frac{1}{5}$. Define the sequence of graphs G_t, for $t = 1, 2, \ldots$ as follows:

$G_1 = H^2$,

$G_{t+1} = G_t^2 ⓩ H$.

Claim 9 *Degree of G_t is d^2; its number of vertices is d^{4t}, and its spectral expansion is $\leq \frac{2}{5}$.*

> **Proof of claim:** By induction.
> Base Case: for $t = 1$, the proof is easy.
> Inductive Step: suppose G_t is an (d^{4t}, d^2, λ)-graph, with $\lambda \leq \frac{2}{5}$. Then G_{t+1} is $(d^{4t}d^4, d^2, f(\lambda^2, \lambda_0))$-graph, where $f(\lambda^2, \lambda_0) \leq \lambda^2 + \lambda_0 + \lambda_0^2 \leq \frac{4}{25} + \frac{1}{5} + \frac{1}{25} = \frac{2}{5}$. □

How explicit is our construction? Let N_t denote the number of vertices in G_t. Recall that $N_t = d^{4t}$. Let time(G_t) be the number of operations to compute one neighbor of a given vertex in G_t. We have time$(G_{t+1}) \approx 2$time(G_t). This implies that time$(G_t) \approx 2^t = \text{poly}(N_t)$.

We use the tensor product operation to make our expander construction more explicit, i.e, reducing time(G_t) from poly(N_t) to polylog(N_t).

2.5 Tensor Product

Definition 10 (Tensor Operation on Graphs) *For regular graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, define $G_1 \otimes G_2 = (V, E)$, where $V = V_1 \times V_2$, $E = \{((u_1, u_2), (v_1, v_2)) | (u_1, v_1) \in E_1, (u_2, v_2) \in E_2\}$.*

Definition 11 (Tensor Operation on Vectors) *For every $x = (x_i) \in \mathbb{R}^n$ and $y = (y_i) \in \mathbb{R}^m$, their tensor product is $z = x \otimes y \in \mathbb{R}^{nm}$, where $z_{i,j} = x_i y_i$. Equivalently, we can say if $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_m)$ then $z = (x_1.y, x_2.y, \ldots, x_n.y)$.*

Definition 12 (Tensor Operation on Matrices) *For every matrix $A = (a_{i,j}) \in \mathbb{R}^{nxn}$ and matrix $B = (b_{i,j}) \in \mathbb{R}^{mxm}$, their tensor product is $A \otimes B = (c_{i,j}) \in \mathbb{R}^{nmxnm}$, where $c_{ii',jj'} = a_{i,j} b_{i',j'}$. Equivalently, we can write*

$$A \otimes B = \begin{pmatrix} a_{1,1}.B & a_{1,2}.B & \ldots & a_{1,n}.B \\ \vdots & \vdots & \vdots\,\vdots\,\vdots & \vdots \\ a_{n,1}.B & a_{n,2}.B & \ldots & a_{n,n}.B \end{pmatrix}.$$

Exercises 13 *(Properties of the tensor product)*

1. *For probability distributions* $x \in \mathbb{R}^n$ *and* $y \in \mathbb{R}^m$, $x \otimes y$ *is a probability distribution on* $[n] \times [m]$ *(where* $[n] = \{1, 2, \ldots, n\}$*).*

2. *If* A_1 *and* A_2 *are normalized adjacency matrices of graphs* G_1 *and* G_2 *respectively, then* $A_1 \otimes A_2$ *is the normalized adjacency matrix of* $G_1 \otimes G_2$.

3. *For every* $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{m \times m}$, $x \in \mathbb{R}^n$, *and* $y \in \mathbb{R}^m$, $(A \otimes B)(x \otimes y) = (Ax) \otimes (By)$.