LUBOTZKY-PHILLIPS-SARNAK RAMANUJAN GRAPHS AND COLLISION RESISTANT HASHING

RUBY ZHANG

Abstract. Hash functions underpin modern communication by providing an efficient method of encrypting messages and detecting data corruption. Popular hash functions such as SHA-1 have in recent years been found vulnerable to attack, motivating the development of more collision-resistant hash functions. Several new theoretical approaches to hashing use random walks on Ramanujan graphs, a type of expander graph with unique eigenvalue characteristics that deem it well-suited to constructing collision-resistant hash functions. This paper is an expository study of these new efforts through the lens of spectral graph theory, since it turns out that the suitability of a family of graphs for cryptographic hashing can be determined from the spectral properties of the family. Finally, we describe Lubotzky-Phillips-Sarnak's explicit construction of an infinite family of Ramanujan graphs, focusing specifically on the non-bipartite case.

Contents

1. Introduction

A hash function whose hash values are uniformly distributed decreases the chance of collision, a key characteristic of an effective hash. This paper explores hash functions that utilize random walks on graphs with the set of vertices corresponding to hash values. Exploring graphs with random walks that approach uniform distribution uncovers interesting connections between these graphs and their spectral properties.

Sections 2 and 3 will introduce basic concepts and definitions regarding probability distributions and spectral graph theory, respectively. In Section 4, we will prove the expander mixing lemma and rapid mixing of random walks (based on the exposition of [7]), which subsequently imply that an effective regular graph for hashing has a minimized λ_2 (the second largest eigenvalue of the graph's adjacency matrix). Section 5

Date: August 29, 2016.

introduces Ramanujan graphs, a special family of expander graphs with a minimal λ_2, after first showing Cheeger's inequality and the Alon-Boppana bound on λ_2 for an infinite family of d-regular graphs based on Nilli's version of Alon-Boppana in [4]. The paper will conclude with an explicit construction of an infinite family of Ramanujan graphs by Lubotzky-Phillips-Sarnak [3] which uses properties of prime numbers and projective linear groups. Although a proof that the LPS construction is Ramanujan will not be shown (one can refer to [6]), a lower bound on the girth of the non-bipartite case will be shown using a similar approach seen in [2].

2. Hash Functions and Collision

Definition 2.1. A *hash function* is a mathematical algorithm that maps inputs of an arbitrary size to output values of a small and constant size in a given finite range.

Definition 2.2. An algorithm is solvable in *polynomial time* if the number of steps required to complete the algorithm with an input of size n is $O(n^k)$ for some $k \in \mathbb{N}$. If the algorithm takes longer than polynomial time, then it is solvable in *non-polynomial time*. An example of a non-polynomial time problem is prime factorization.

Definition 2.3. A *collision* is when two inputs hash to the same output value. An optimal hash function is *collision resistant*, in other words, it is computationally difficult (it takes non-polynomial time) to find inputs that collide.

Definition 2.4. A *Markov chain* is a stochastic process (time sequence representing the evolution of a system) involving a set of states, denoted by Ω, and transitions from one state to the next that depend only on the current state and not previous events. A stochastic process of n steps is represented by the sequence $(X_1, X_2, ..., X_n)$, where $X_t \in \Omega$ is the state of the system at time t.

Definition 2.5. A *probability distribution* is a set of non-negative numbers that add up to one and correspond to the states of a stochastic process. It is represented by a vector $q_t = (q_1, q_2, ..., q_n)$ such that $q_i = \mathbb{P}(X_t = i)$ for state i at time t. A *uniform distribution* is when all states have equal probability, represented by $\mu = (\frac{1}{n}, \frac{1}{n}, ..., \frac{1}{n})$. A *step* is the evolution of the system from $t = i$ to $t = i + 1$ based on q_i.

Proposition 2.6. *Let the range of possible hash values represent the states in a probability distribution. Then the uniform distribution minimizes the probability of collision.*

Proof. Let us suppose that $q_t = (q_1, q_2, ..., q_n)$. Given two inputs, the probability that both map to state j at time t is given by q_j^2. Then over all states, the total probability of collision is $\sum_{i=1}^{n} q_i^2$. Using the Cauchy-Schwarz inequality, we have that:

$$\begin{aligned} n(\sum_{i=1}^{n} q_i^2) &\geq (\sum_{i=1}^{n} q_i)^2 \\ n(\sum_{i=1}^{n} q_i^2) &\geq 1^2 \\ \sum_{i=1}^{n} q_i^2 &\geq \frac{1}{n} = \sum_{i=1}^{n} (\frac{1}{n})^2 \end{aligned} \tag{2.7}$$

Therefore, the probability of collision is minimized when $q_t = \mu$. □

From this, it can be seen that a good hash function should reach uniform distribution in the minimum number of steps possible.

3. Expander Graphs and Cayley Graphs

Definition 3.1. A *graph* $G = (V, E)$ is defined as a set of vertices, V, and edges, E, such that $E = \{(u, v)|u, v \in V\}$. A vertex u is a *neighbor* of vertex v if $(u, v) \in E$. A graph is d-regular if all vertices in V have d neighbors. A *cycle* is a sequence of vertices that start and end at the same vertex, and each two consecutive vertices are neighbors. The *girth* of a graph is the length of its shortest cycle. If there are no cycles, then the girth is infinity. The *distance* between two vertices, $\text{dist}(u, v)$, is the minimum length of the paths connecting u and v. The *diameter* of a graph is the maximum distance between any two points: $\text{diam}(G) = \max\{\text{dist}(u, v)|u, v \in V\}$.

Lemma 3.2. *For a d-regular (connected) graph G with a fixed d, $\lim_{n\to\infty} \text{diam}(G) = \infty$.*

Proof. Suppose $\text{diam}(G) = \text{dist}(u, v) = m$. Since the graph is d-regular, there are d possible next steps at every vertex starting from vertex u. Then the number of walks from u of length m is $\leq d^m$ and all walks from u have $\leq m + 1$ vertices. Since the graph is connected, all verticies can be traversed from u and $n \leq (m + 1)(d^m)$. If d is fixed, then $\lim_{n\to\infty} m = \infty$. □

Lemma 3.3. *For a graph G, $\text{girth}(G) \leq 2\,\text{diam}(G) + 1$.*

Proof. Let $\text{girth}(G) = g, \text{diam}(G) = m$ and assume that $g \geq 2m + 2$. Let $v_1, v_2, ..., v_g$ denote the vertices of a cycle of length g. Then there exists v_n such that, in the cycle, $\text{dist}(v_1, v_n) = m+1$ since if $\text{dist}(v_1, v_n) \leq m$ then $g \leq 2m + 2$. But since $\text{diam}(G) = m$ there must exist a path such that $\text{dist}(v_1, v_n) \leq m$. Then there exist a cycle with length $\leq 2m + 1$, yielding a contradiction. □

Definition 3.4. The *adjacency matrix* of G is $A_G \in M_n(\mathbb{R})$, with $(a_{ij}) = 1$ for $(i, j) \in E$ and 0 otherwise. Note that for vector $x = (x_1, ..., x_n)$, if the value of x_i is assigned to vertex i, then the value of $(A_G x)_i$ is the sum of the values of all the neighbors of vertex i.

Lemma 3.5. *Let the eigenvalues of A_G be $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ for a d-regular graph G. Then $\lambda_1 = d$ and $|\lambda_i| \leq d$ for all i.*

Proof. Note that $\lambda = d$ is an eigenvalue of A_G corresponding to $J = (1, ..., 1)$, the all ones vector. Suppose there exists eigenvalue λ_0 to eigenvector $\nu_0 = (\nu_1, ..., \nu_n)$ such that $\lambda_0 > d$. Let $\nu_j = \max\{\nu_i \mid i \in \mathbb{N}\}$, the maximum component of ν_0. Then every component of the vector $A_G\nu_0$ is less than $d\nu_j$. However, $\lambda\nu_j$ is greater than $d\nu_j$, yielding a contradiction. Thus $\lambda_i \leq d$, for all i. Similarly, assume that the smallest eigenvalue λ_n to eigenvector $\mu_0 = (\mu_1, ..., \mu_n)$ is such that $|\lambda_n| > d$. The same contradiction follows if we consider component $\mu_j = \max\{|\mu_i| \mid i \in \mathbb{N}\}$ since every component of vector $A_G\mu_0$ is less than $|d\mu_j|$. □

Definition 3.6. The Euclidean norm of a vector $x = (x_1, ..., x_n)$ is $\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}$. The induced norm of an $n \times n$ matrix A is $\|A\| = \sup_{x\neq 0} \frac{\|Ax\|}{\|x\|}$. Only the Euclidean vector norm and induced matrix norm will be used in this paper.

Lemma 3.7. *For square matrices A and B, $\|AB\| \leq \|A\|\|B\|$. The induced matrix norm is submultiplicative.*

Proof. By definition $\|Ax\| \leq \|A\|\|x\|$, thus $\|AB\| = \frac{\|ABx\|}{\|x\|} \leq \frac{\|A\|\|Bx\|}{\|x\|} \leq \frac{\|A\|\|B\|\|x\|}{\|x\|} = \|A\|\|B\|$. □

Remark 3.8. In addition, note that $\|A + B\| = \frac{\|Ax+Bx\|}{\|x\|} \leq \frac{\|Ax\|}{\|x\|} + \frac{\|Bx\|}{\|x\|} = \|A\| + \|B\|$.

Definition 3.9. For a regular graph with eigenvalues $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$, λ_2 is the *nontrivial eigenvalue*.

Definition 3.10. For $S, T \subseteq V$, let $E(S, T)$ denote all edges $(u, v) \in E$ such that $u \in S$ and $v \in T$. Let $\overline{S}$, the *complement* of S, refer to the set of all edges in E that are not in S. A (n, d, δ)-*expander graph* with *edge expansion constant* δ is a n vertex, d-regular graph such that for all $S \subset V$ and $|S| \leq \frac{|V|}{2}$,

$$\delta = \min \frac{|E(S, \overline{S})|}{|S|} \tag{3.11}$$

Corollary 3.12. *For any graph,* $0 \leq \delta \leq deg_{\max}$.

Proof. δ must be nonnegative. Take $S = \{v_1\}$, then $\frac{|E(S,\overline{S})|}{|S|} = deg(v_1) \leq deg_{\max}$. □

For example, in the case of a disjoint graph, the edge expansion constant would be 0.

Definition 3.13. A *Cayley graph* consists of a group G and symmetric subset S of G (if $a \in S$, then $a^{-1} \in S$). The elements of G correspond to vertices, and there exists an edge between $u, v \in G$ if uv^{-1} or $vu^{-1} \in S$, hence the symmetry of S.

Example 3.14. A C_n graph (cycle with n vertices) is a Cayley graph of the group $\mathbb{Z}_n$ mod n and generator set $S = \{1, -1\}$. Note that $-1 \equiv n - 1 \bmod n$, the common notation.

4. Random Walks and Rapid Mixing

Definition 4.1. A *random walk* on a graph $G(V, E)$ is a finite Markov chain where $\Omega = V$. Transition probabilities of moving from vertex i to vertex j, $p_{ij} = \mathbb{P}(X_{t+1} = j | X_t = i)$, are given by the transition matrix $T_G = (p_{ij})$. There is an equal chance of moving to any neighbors of vertex i in a given step.
For a d-regular graph, the transition matrix is thus given by the normalized adjacency matrix: $T_G = \frac{1}{d} A_G$.

Theorem 4.2. *[Expander Mixing Lemma] For all $S, T \subseteq V$, of a d-regular non-bipartite graph G with eigenvalues $d = \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$ of A_G, we have that:*

$$|(|E(S,T)| - \frac{d|S||T|}{n})| \leq \lambda_2 \sqrt{|S||T|} \tag{4.3}$$

Proof. Define the vector $\chi_S = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$ by letting

$$s_i = \begin{cases} 1 & \text{if } i \in S, \\ 0 & \text{otherwise} \end{cases}$$

Similarly, we will have the vector χ_T. Since A_G is a real symmetric matrix with eigenvalue d and eigenvector J (the all ones vector), then it can be assigned an orthonormal eigenbasis with $b = (b_1, b_2, ..., b_n)$ such that $b_1 = \frac{1}{\sqrt{n}} J$. Then let $\chi_S = \sum_{i=1}^n \alpha_i b_i$ and $\chi_T = \sum_{i=1}^n \beta_i b_i$. Since b is an orthonormal eigenbasis, $\langle \chi_S, \chi_S \rangle = \sum_{i=1}^n \alpha_i^2$ and $\langle \chi_T, \chi_T \rangle = \sum_{i=1}^n \beta_i^2$. We also have that $\alpha_1 = \langle \chi_S, b_1 \rangle = \frac{|S|}{\sqrt{n}}$ and $\beta_1 = \langle \chi_T, b_1 \rangle = \frac{|T|}{\sqrt{n}}$. We then have that

$$
\begin{aligned}
|E(S,T)| &= \langle \chi_S, A_G \chi_T \rangle \\
&= \langle \sum_{i=1}^{n} \alpha_i b_i, A_G \sum_{i=1}^{n} \beta_i b_i \rangle \\
&= \langle \sum_{i=1}^{n} \alpha_i b_i, \sum_{i=1}^{n} \beta_i \lambda_i b_i \rangle \\
&= \sum_{i=1}^{n} \alpha_i \lambda_i \beta_i \\
&= \alpha_1 \lambda_1 \beta_1 + \sum_{i=2}^{n} \alpha_i \lambda_i \beta_i \\
|(|E(S,T)| - \frac{d|S||T|}{n})| &= |\alpha_1 \lambda_1 \beta_1 + \sum_{i=2}^{n} \alpha_i \lambda_i \beta_i - d \frac{|S|}{\sqrt{n}} \frac{|T|}{\sqrt{n}}| \qquad (4.4) \\
&= |\sum_{i=2}^{n} \alpha_i \lambda_i \beta_i| \\
&\leq \lambda_2 \sum_{i=2}^{n} |\alpha_i \beta_i| \\
&\leq \lambda_2 \sqrt{\sum_{i=2}^{n} |\alpha_i|^2 \sum_{i=2}^{n} |\beta_i|^2} \qquad \text{via the Cauchy-Schwarz inequality} \\
&\leq \lambda_2 \sqrt{\langle \chi_S, \chi_S \rangle \langle \chi_T, \chi_T \rangle} \\
&= \lambda_2 \sqrt{|S||T|}
\end{aligned}
$$

□

Theorem 4.5. *[Rapid Mixing of Random Walks] For a d-regular graph with n vertices and normalized adjacency matrix T_G, at the k^{th} step from the starting point ν_0 with initial probability distribution $q_0 = (q_1, ..., q_n)$, we have that:*

$$
\|(T_G)^k q_0 - \mu\| \leq (\frac{\lambda_2}{d})^k \qquad (4.6)
$$

Proof. Note that since $0 \leq q_i \leq 1$, then $q_i^2 \leq q_i$. Therefore, $\|q_0\| = \sqrt{\sum_{i=1}^{n} q_i^2} \leq \sqrt{\sum_{i=1}^{n} q_i} = 1$.
Assign the orthonormal eigenbasis with $b = (b_1, b_2, ...b_n)$ such that $b_1 = \frac{1}{\sqrt{n}} J$. Let $q_0 = \sum_{i=1}^{n} \alpha_i b_i$. Note

that $\alpha_1 = \langle q_0, b_1 \rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} q_i = \frac{1}{\sqrt{n}}$. Since $T_G = \frac{1}{d} A_G$, we have that

$$\begin{aligned} \|(T_G)^k q_0 - \mu\| &= \|(\frac{1}{d} A_G)^k \sum_{i=1}^{n} \alpha_i b_i - \mu\| \\ &= \|(\frac{1}{d})^k d^k \frac{1}{\sqrt{n}} b_1 + (\frac{1}{d})^k (\sum_{i=2}^{n} \alpha_i \lambda_i^k b_i) - \mu\| \\ &= \|\mu + (\frac{1}{d})^k (\sum_{i=2}^{n} \alpha_i \lambda_i^k b_i) - \mu\| \\ &\leq (\frac{\lambda_2}{d})^k \|\sum_{i=2}^{n} \alpha_i b_i\| \\ &\leq (\frac{\lambda_2}{d})^k \|q_0\| \\ &\leq (\frac{\lambda_2}{d})^k \end{aligned} \tag{4.7}$$

□

Corollary 4.8. *A d-regular graph with n vertices reaches uniform distribution in logarithm time.*

Proof. Since $\lambda_2 < d$, then $\alpha = \frac{\lambda_2}{d} < 1$. Suppose we have any $0 < \varepsilon < \alpha$ such that $\|(T_G)^k q_0 - \mu\| \leq \varepsilon$. Then we have that

$$\begin{aligned} \|(T_G)^k q_0 - \mu\| \leq (\frac{\lambda_2}{d})^k &\leq \varepsilon \\ k \log \frac{\lambda_2}{d} &\leq \log \varepsilon \\ k &\leq \log_\alpha \varepsilon \end{aligned} \tag{4.9}$$

□

Both theorem 4.2 and theorem 4.5 imply the same conclusion: a graph with a minimized nontrivial eigenvalue reaches uniform distribution faster. For a random, uniformly distributed d-regular graph with n vertices, the number of expected edges between any subsets of vertices is $\frac{d|S||T|}{n}$. Therefore, a smaller λ_2 minimizes the distance of a d-regular graph with n vertices from a random, uniform distribution according to theorem 4.2. For ε close to zero, k is minimized when α is minimized, in other words, if λ_2 is minimized according to theorem 4.5. In the next section, we will see that a minimized nontrivial eigenvalue also results in a stronger expander graph (a larger expansion constant) due to a higher lower and upper bound. Therefore, expander graphs quickly mix and approach uniform distribution, which is characteristic of a good hash function.

5. Ramanujan Graphs

The expansion constant is also known as the Cheeger constant, and Cheeger's inequality places lower and upper bounds on the expansion constant in terms of the nontrivial eigenvalue. Though the upper bound is $\delta \leq \sqrt{2d(d - \lambda_2)}$, we will show the slightly weaker result:

Theorem 5.1. *[Cheeger's Inequality] For a d-regular graph $G(V, E)$, the edge expansion constant has the following bound:*

$$\frac{d - \lambda_2}{2} \leq \delta \leq 2\sqrt{d(d - \lambda_2)} \tag{5.2}$$

Proof. Let us first prove the lower bound using the following proposition.

Proposition 5.3. *For all $v \perp J$ and d-regular graphs, $\frac{\langle v^T A_G v\rangle}{\|v\|^2} \leq \lambda_2$.*

Proof. Let $b = (\frac{1}{\sqrt{n}}J, b_2, b_3, ...b_n)$ be the orthonormal eigenbasis of A_G, which is possible since A_G is a real symmetric matrix with $\lambda_1 = d$ and corresponding eigenvector J. Then $v \perp J$ can be written as $v = \sum_{i=2}^{n} \alpha_i b_i$. Thus we have that $\frac{\langle v^T A_G v\rangle}{\|v\|^2} = \frac{\sum_{i=2}^{n} \alpha_i^2 \lambda_i}{\sum_{i=2}^{n} \alpha_i^2} \leq \lambda_2$ since $\lambda_2 \geq \lambda_3 \geq ... \geq \lambda_n$. □

Let $S \subset V$ such that $\delta = \frac{|E(S,\overline{S})|}{|S|}$. Take vector μ such that $\mu_i = -|\overline{S}|$ if $i \in S$ and $\mu_i = |S|$ if $i \in \overline{S}$. Note that $\langle \mu, J\rangle = |S||\overline{S}| - |\overline{S}||S| = 0$.
Then we have that $\|\mu\|^2 = |S||\overline{S}|^2 + |\overline{S}||S|^2 = |S||\overline{S}|(|S| + |\overline{S}|) = |S||\overline{S}|n$.
In addition, we also have $A_G\mu = \begin{pmatrix} |S|E(\overline{S},\{1\}) - |\overline{S}|E(S,\{1\}) \\ \vdots \\ |S|E(\overline{S},\{n\}) - |\overline{S}|E(S,\{n\}) \end{pmatrix}$.
Since the graph is d-regular and each edge consists of two vertices, then $d|S| = 2E(S) + E(S,\overline{S})$ and $d|\overline{S}| = 2E(\overline{S}) + E(S,\overline{S})$. Thus,

$$\begin{aligned} \langle \mu, A_G\mu\rangle &= |S|(\sum_{i\in\overline{S}} |S|E(\overline{S},\{i\}) - |\overline{S}|E(S,\{i\})) - |\overline{S}|(\sum_{i\in S} |S|E(\overline{S},\{i\}) - |\overline{S}|E(S,\{i\})) \\ &= 2|S|^2E(\overline{S}) - 2|S||\overline{S}|E(S,\overline{S}) + 2|\overline{S}|^2E(S) \\ &= |S|^2(d|\overline{S}| - E(S,\overline{S})) - 2|S||\overline{S}|E(S,\overline{S}) + |\overline{S}|^2(d|S| - E(S,\overline{S})) \\ &= d|S||\overline{S}|(|S| + |\overline{S}|) - E(S,\overline{S})(|S| + |\overline{S}|)^2 \\ &= nd|S||\overline{S}| - n^2E(S,\overline{S}) \end{aligned} \tag{5.4}$$

Therefore, we have that $\frac{\langle \mu, A_G\mu\rangle}{\|\mu\|^2} = d - \frac{nE(S,\overline{S})}{|S||\overline{S}|} \geq d - \frac{n}{|\overline{S}|}\delta \geq d - 2\delta$ since $|\overline{S}| \geq \frac{n}{2}$. From the proposition, we have that $\lambda_2 \geq \frac{\langle \mu, A_G\mu\rangle}{\|\mu\|^2} \geq d - 2\delta$, thus, $\frac{d-\lambda_2}{2} \leq \delta$.

Now we will prove the upper bound on the expansion constant, the harder side of the inequality. We will prove several propositions first which we use to prove the final inequality.

Proposition 5.5. *For a vector x, $\sum_{\{u,v\}\in E}(x_u - x_v)^2 = dx^Tx - x^TA_Gx$.*

Proof.

$$\begin{aligned} \sum_{\{u,v\}\in E} (x_u - x_v)^2 &= \sum_{\{u,v\}\in E} (x_u^2 + x_v^2) - \sum_{\{u,v\}\in E} 2x_ux_v \\ &= d\sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} x_i(\sum_{i\sim j} x_j) \\ &= dx^Tx - \sum_{i=1}^{n} x_i(A_Gx)_i \\ &= dx^Tx - x^TA_Gx \end{aligned} \tag{5.6}$$

□

Remark 5.7. Note that $\sum_{\{u,v\}\in E}(x_u - x_v)^2 \geq 0$, thus $dx^Tx \geq x^TA_Gx$.

Let $R_L(x) = \frac{\sum_{\{u,v\}\in E}(x_u - x_v)^2}{\sum_{u\in V} x_u}$ for the remainder of the paper.

Lemma 5.8. *For an eigenvector x of λ_2, let $x^J = x + \alpha J$ for any $\alpha \in \mathbb{R}$. Then $R_L(x) \geq R_L(x^J)$.*

Proof. Since A_G is a real symmetric matrix, it is possible to find an orthogonal eigenbasis b such that $b_1 = J$. Then we have that $\langle x, J\rangle = \sum_{u\in V} x_u = 0$.

We have the following two observations for the numerator:

$$\begin{aligned}\sum_{\{u,v\}\in E} (x_u^J - x_v^J)^2 &= \sum_{\{u,v\}\in E} ((x_u+\alpha) - (x_v+\alpha))^2 \\ &= \sum_{\{u,v\}\in E} (x_u - x_v)^2\end{aligned} \tag{5.9}$$

and for the denominator:

$$\begin{aligned}\sum_{u\in V} x_u^J &= \sum_{u\in V} (x_u+\alpha)^2 \\ &= \sum_{u\in V} x_u^2 + \alpha^2 + 2\alpha \sum_{u\in V} x_u \\ &\geq \sum_{u\in V} x_u^2\end{aligned} \tag{5.10}$$

Since the numerator stays the same and the denominator increases, $\frac{\sum_{\{u,v\}\in E}(x_u-x_v)^2}{\sum_{u\in V} x_u} \geq \frac{\sum_{\{u,v\}\in E}(x_u^J-x_v^J)^2}{\sum_{u\in V} x_u^J}$ for any choice of α. □

Lemma 5.11. *For a vector x, let vector $y_i = \max\{x_i, 0\}$ and vector $z_i = \min\{x_i, 0\}$. Then $R_L(y) \leq 2R_L(x)$ or $R_L(z) \leq 2R_L(x)$.*

Proof. Since the square of a number is always positive, evidently $\sum_{\{u,v\}\in E}(x_u - x_v)^2 \geq \sum_{\{u,v\}\in E}(y_u - y_v)^2$ and $\sum_{\{u,v\}\in E}(x_u - x_v)^2 \geq \sum_{\{u,v\}\in E}(z_u - z_v)^2$.

Note that $\sum_{u\in V} x_u^2 = \sum_{u\in V} y_u^2 + \sum_{u\in V} z_u^2$. If $\sum_{u\in V} y_u^2 \geq \frac{\sum_{u\in V} x_u^2}{2}$, then $R_L(y) \leq 2R_L(x)$. Otherwise, $\sum_{u\in V} z_u^2 \geq \frac{\sum_{u\in V} x_u^2}{2}$ and $R_L(z) \leq 2R_L(x)$. □

Remark 5.12. Let x be an eigenvector of A_G. Then $-x$ is also an eigenvector to the same eigenvalue.

Let x be an eigenvector of λ_2 and $\alpha \in \mathbb{R}$ such that the median of $x^J = x + \alpha J$ is 0. Let vector $y_i = \max\{x_i^J, 0\}$. We can assume that $R_L(y) \leq 2R_L(x)$ since $-x$ can be used if otherwise. Furthermore, note that there are $\leq \frac{n}{2}$ positive terms.

Proposition 5.13. $d - \lambda_2 \geq \frac{(\sum_{\{u,v\}\in E} |x_u^2 - x_v^2|)^2}{4d(y^T y)^2}$.

Proof.

$$
\begin{aligned}
d - \lambda_2 &= \frac{dx^T x - x^T A_G x}{x^T x} \qquad \text{since } x \text{ is an eigenvector} \\
&\geq R_L(x^J) \\
&\geq \frac{dy^T y - y^T A_G y}{2y^T y} \\
&= \frac{\sum_{\{u,v\}\in E}(y_u - y_v)^2}{2y^T y} \\
&= \frac{(\sum_{\{u,v\}\in E}(y_u - y_v)^2)(\sum_{\{u,v\}\in E}(y_u + y_v)^2)}{2y^T y(\sum_{\{u,v\}\in E}(y_u + y_v)^2)} \qquad (5.14) \\
&\geq \frac{(\sum_{\{u,v\}\in E}|y_u^2 - y_v^2|)^2}{2y^T y(dy^T y + y^T A_G y)} \qquad \text{via the Cauchy-Schwartz Inequality} \\
&\geq \frac{(\sum_{\{u,v\}\in E}|y_u^2 - y_v^2|)^2}{2y^T y(2dy^T y)} \qquad \text{using 5.7} \\
&= \frac{(\sum_{\{u,v\}\in E}|y_u^2 - y_v^2|)^2}{4d(y^T y)^2}
\end{aligned}
$$

□

Proposition 5.15. $\sum_{\{u,v\}\in E}|y_u^2 - y_v^2| \geq \delta y^T y$.

Proof. Order the vertices so that $y_1 \geq y_2 \geq ... \geq y_n$. Let $q = \max\{k|y_k > 0\}$. Then we have that

$$
\begin{aligned}
\sum_{\{u,v\}\in E}|y_u^2 - y_v^2| &= \sum_{u=1}^{q}\sum_{\substack{u\sim v \\ v>u}} y_u^2 - y_v^2 \\
&= \sum_{u=1}^{q}\sum_{\substack{u\sim v \\ v>u}}\sum_{k=u}^{v-1}(y_k^2 - y_{k+1}^2) \qquad \text{via a telescoping series} \\
&= \sum_{k=1}^{q}\sum_{u\leq k}\sum_{\substack{v>k \\ v\sim u}}(y_k^2 - y_{k+1}^2) \qquad (5.16) \\
&= \sum_{k=1}^{q}(y_k^2 - y_{k+1}^2)|E(S_k, \overline{S}_k)| \qquad \text{for } S_k = \{1, ..., k\} \\
&\geq \sum_{k=1}^{q}\delta k(y_k^2 - y_{k+1}^2) \qquad \text{since } |S_k|\delta \leq |E(S_k, \overline{S}_k)| \\
&= \delta\sum_{k=1} qy_k^2 \\
&= \delta y^T y
\end{aligned}
$$

□

Substituting 5.15 into 5.13, we have that $d - \lambda_2 \geq \frac{(\sum_{\{u,v\}\in E}|y_u^2 - y_v^2|)^2}{4d(y^T y)^2} \geq \frac{(\delta y^T y)^2}{4d(y^T y)^2} = \frac{\delta^2}{4d}$. Therefore, we have that $\delta \leq 2\sqrt{d(d - \lambda_2)}$.

□

Cheeger's inequality shows the direct bounds placed on the expansion constant by the nontrivial eigenvalue. A smaller λ_2 results in a higher lower and upper bound on δ, resulting in a larger expansion constant. Then working towards the goal of a collision-resistant hash function, it is optimal to construct a family of graphs with a minimal λ_2. Alon-Boppana indeed does place a lower bound on λ_2 for an infinite family of d-regular graphs.

Theorem 5.17. *[Alon-Boppana] Given a d-regular graph G with n vertices, the following limit is placed on the largest nontrivial eigenvalue:*

$$\lim_{n\to\infty} \lambda_2 \geq 2\sqrt{d-1} \tag{5.18}$$

Proof. Let $\operatorname{diam}(G) = \operatorname{dist}(u,v) \geq 2b+2$, for some b, and u' be a neighbor of u. For a vertex $i \in V, \operatorname{dist}(i,\{u,u'\}) = \min\{\operatorname{dist}(i,u), \operatorname{dist}(i,u')\}$. Construct the vector $\alpha \in \mathbb{R}^n$ such that $\alpha_i = \frac{1}{(\sqrt{d-1})^t}$ if $t = \operatorname{dist}(i,\{u,u'\}) < b$ and $\alpha_i = 0$ otherwise. Let $S_i = \{j \mid i \sim j, \alpha_j < \alpha_i\}$. Since it is a d-regular graph, then $|S_i| \leq d-1$ as every vertex has at most $d-1$ neighbors at a distance of $\frac{1}{(\sqrt{d-1})^{t+1}}$ from $\{u,u'\}$ (thus a smaller α_j value) as at least one of its neighbors must be traversed to reach u or u'. Let $L_t = \{i \in V \mid \operatorname{dist}(i,\{u,u'\}) = t\}$. From 5.5 we have that

(5.19)

$$\begin{aligned}
\alpha^T A\alpha &= d\alpha^T\alpha - \sum_{\{i,j\}\in E} (\alpha_i - \alpha_j)^2 \\
&= d\alpha^T\alpha - \sum_{t<b}\sum_{i\in L_t}\sum_{j\in S_i} (\alpha_i-\alpha_j)^2 \qquad \text{since the neighbors in } S_i \text{ have a distance greater than t from } \{u,u'\} \\
&= d\alpha^T\alpha - \sum_{t<b-1}\sum_{i\in L_t}\sum_{j\in S_i} (\alpha_i-\alpha_j)^2 - \sum i \in L_{b-1} \sum_{j\in S_i} \alpha_i^2 \\
&= d\alpha^T\alpha - \sum_{t<b-1}\sum_{i\in L_t} |S_i|(\alpha_i - \frac{\alpha_i}{\sqrt{d-1}})^2 - \sum_{i\in L_{b-1}} |S_i|\alpha_i^2 \\
&\geq d\alpha^T\alpha - \sum_{t<b-1}\sum_{i\in L_t} (d-1)(\alpha_i - \frac{\alpha_i}{\sqrt{d-1}})^2 - \sum_{i\in L_{b-1}} (d-1)\alpha_i^2 \\
&= d\alpha^T\alpha - \sum_{t<b-1}\sum_{i\in L_t} \alpha_i^2(d-2\sqrt{d-1}) - \sum_{i\in L_{b-1}} (d-1)\alpha_i^2 \\
&= d\alpha^T\alpha - \sum_{t<b}\sum_{i\in L_t} \alpha_i^2(d-2\sqrt{d-1}) + \sum_{i\in L_{b-1}} \alpha_i^2(d-2\sqrt{d-1}) - \sum_{i\in L_{b-1}} (d-1)\alpha_i^2 \\
&= d\alpha^T\alpha - (d-2\sqrt{d-1})\sum_{i\in V}\alpha_i^2 - (2\sqrt{d-1}-1)\frac{|L_{b-1}|}{(d-1)^{b-1}} \\
&= 2\sqrt{d-1}\|\alpha\|^2 - (2\sqrt{d-1}-1)\frac{|L_{b-1}|}{(d-1)^{b-1}} \\
&= 2\sqrt{d-1}\|\alpha\|^2 - (2\sqrt{d-1}-1)\frac{1}{b}\sum_{t=0}^{b-1}\frac{|L_{b-1}|}{(d-1)^{b-1}} \\
&\geq 2\sqrt{d-1}\|\alpha\|^2 - \frac{(2\sqrt{d-1}-1)}{b}\sum_{t=0}^{b-1}\frac{|L_t|}{(d-1)^t} \qquad \text{since } \frac{|L_t|}{(d-1)^t} \leq \frac{|S_{t-1}||L_{t-1}|}{(d-1)^t} \leq \frac{|L_{t-1}|}{(d-1)^{t-1}} \\
&= 2\sqrt{d-1}\|\alpha\|^2 - \frac{(2\sqrt{d-1}-1)}{b}\sum_{i\in V}\alpha_i^2 \\
&= (2\sqrt{d-1} - \frac{2\sqrt{d-1}-1}{b})\|\alpha\|^2
\end{aligned}$$

Construct a similar vector β for $\{v, v'\}$, then we have that $\beta^T A\beta \geq (2\sqrt{d-1} - \frac{2\sqrt{d-1}-1}{b})\|\beta\|^2$. Note that if $\alpha_i \neq 0$ then $\beta_i = 0$ (and vice versa) since if $\text{dist}(i, \{u, u'\}) \leq b-1$ and $\text{dist}(i, \{v, v'\}) \leq b-1$, then there exists a path of distance $\leq 2b$ from u to v, which is not possible. Therefore, $\langle \alpha, \beta \rangle = 0$ and $\alpha \perp \beta$.

Furthermore, note that there cannot be $(i, j) \in E$ such that $\alpha_i \neq 0$ and $\beta_j \neq 0$ since this would mean that a path of length $\leq 2b+1$ from u to v exists, again a contradiction. Then we have that $\alpha^T A\beta = \sum_{i \in V} \sum_{i \sim j} \alpha_i \beta_j = 0$.

Take $\gamma = a\alpha + b\beta$. Since γ is in a two dimensional space, then it can be written as the linear combination of two orthonormal eigenbasis of A_G (that does not include J). Then $\gamma \perp J$ and from 5.3 we have that

$$\begin{aligned} \lambda_2 &\geq \frac{\gamma^T A_G \gamma}{\|\gamma\|^2} \\ &= \frac{a^2 \alpha^T A_G \alpha + b^2 \beta^T A_G \beta}{\|\gamma\|^2} \\ &\geq \frac{(2\sqrt{d-1} - \frac{(2\sqrt{d-1}-1)}{b})(a^2\|\alpha\|^2 + b^2\|\beta\|^2)}{\|\gamma\|^2} \\ &= \frac{(2\sqrt{d-1} - \frac{2\sqrt{d-1}-1}{b})\|\gamma\|^2}{\|\gamma\|^2} = (2\sqrt{d-1} - \frac{2\sqrt{d-1}-1}{b}) \end{aligned} \tag{5.20}$$

Using lemma 3.2, $\lim_{n\to\infty} b = \infty$. Since d is fixed, then $\lim_{n\to\infty} \lambda_2 \geq 2\sqrt{d-1}$. □

This bound on λ_2 inspires the definition of a Ramanujan graph, a family of graphs with the smallest possible nontrivial eigenvalue.

Definition 5.21. A d-regular finite graph is a Ramanujan graph if

$$\lambda_2 \leq 2\sqrt{d-1} \tag{5.22}$$

It can be proved that there exist bipartite Ramanujan graphs of all degrees. However, an explicit construction is much more difficult to obtain.

6. LPS Construction of Ramanujan Graphs

Before describing the LPS construction of Ramanujan graphs, we will first define and review concepts about quadratic residues and linear groups necessary for understanding the LPS construction.

Definition 6.1. The Legendre symbol is denoted as $(\frac{q}{p})$. If $(\frac{q}{p}) = 1$, then $(\exists x)(x \not\equiv 0 \mod p$ and $q \not\equiv x^2 \mod p)$. In other words, q is a *quadratic residue* of p. If $(\frac{q}{p}) = -1$, then $(\forall x)(q \not\equiv x^2 \mod p)$, q is a *nonresidue*.

Theorem 6.2. *For an odd prime p, there are exactly $\frac{p-1}{2}$ quadratic residues and nonresidules modulo p.*

Proof. First, note that $x^2 \equiv p^2 \pm x^2 \mod p$ for all x, thus there are at most only $\frac{p-1}{2}$ possible quadratic residues: $1^2, 2^2, ..., (\frac{p-1}{2})^2$. Suppose that $x^2 \equiv y^2$ for $x, y \in \{1, 2, ..., \frac{p-1}{2}\}$. Then $x^2 - y^2 = (x-y)(x+y) = cp$ for some $c \in \mathbb{N}$. However $(x-y)$ and $(x+y)$ are both less than p. Therefore, there are $\frac{p-1}{2}$ quadratic residues, which means there are $\frac{p-1}{2}$ nonresidues (excluding 0). □

Theorem 6.3. *For an odd prime p, there exists some integer i such that $i^2 \equiv -1 \mod p$ if $p \equiv 1 \mod 4$.*

Proof. Each $a \in \mathbb{F}_p$ has a unique a^{-1} except for $a = \pm 1$ since $a^2 = 1$ so $a = a^{-1} \mod p$. Then by pairing each element of $\mathbb{F}_p$ with its inverse (with the exception of ± 1), $(p-1)! \equiv 1(p-1) \cdot 1 \equiv -1 \mod p$. Since $p \equiv 1 \mod 4, (p-1)! \equiv ((\frac{p-1}{2})!)^2(-1)^{\frac{p-1}{2}} \equiv ((\frac{p-1}{2})!)^2 \equiv -1 \mod p$. □

Definition 6.4. The *center* of a group G, denoted by $Z(G)$, is the set of elements in G that commute with every element of G. In other words, $Z(G) = \{z \in G \mid \forall g \in G, zg = gz\}$.

Definition 6.5. $GL(n, \mathbb{F}_p)$ is the group of all $n \times n$ invertible matrices over the field of integers modulo prime p. Its projective group $PGL(n, \mathbb{F}_p) = GL(n, \mathbb{F}_p)/Z(G)$ with $Z(G) = \{\lambda I \mid \lambda \in \mathbb{F}_p\}$ and I being the identity matrix. Thus all matrices which are scalar multiples of each other belong in the same equivalence class in $PGL(2, \mathbb{F}_p)$. The special linear group $SL(n, \mathbb{F}_p)$ are matrices of $GL(n, \mathbb{F}_p)$ with determinant 1. Therefore, the special projective linear group, $PSL(n, \mathbb{F}_p) = SL(n, \mathbb{F}_p)/Z(G)$ with $Z(G) = \{I, -I\}$, consists of all equivalence classes of $n \times n$ invertible matrices over $\mathbb{F}_p$ with determinant 1 modulo scalars.

Remark 6.6. The inverse of a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the matrix $\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Lemma 6.7. *There are $p(p^2-1)$ elements (equivalence classes) in $PGL(2, \mathbb{F}_p)$.*

Proof. Since all matrices in $GL(2, \mathbb{F}_p)$ are invertible, then they must be nonsingular and have linearly independent columns. Let the columns be non-zero vectors β_1, $\beta_2 \in \mathbb{R}_2$. Therefore, there are $q^2 - 1$ possible vectors for β_1, and since $\beta_2 \neq c\beta_1$, then there are $q^2 - q$ possible vectors for β_2. Since $PGL(2, \mathbb{F}_p)$ is the quotient group of $GL(2, \mathbb{F}_p)$ over all non-zero scalar transformations, then $|PGL(2, \mathbb{F}_p)| = \frac{|GL(2,\mathbb{F}_p)|}{p-1} = p(p^2-1)$. □

Proposition 6.8. *A matrix with a quadratic residue as its determinant represents a class in $PSL(2, \mathbb{F}_p)$.*

Proof. For a matrix $A \in GL(2, \mathbb{F}_p)$, det(A) is either a quadratic residue or a nonresidue. Let us suppose that $\det(A) = x^2$. Note that for a matrix, $\det(cA) = c^2\det(A)$, therefore $c^{-1}A \in SL(2, \mathbb{F}_p)$. Then all scalar multiples of $c^{-1}A$, including A, belong in the same equivalence class.

Now suppose that det(A) is a nonresidue. Since $\det(cA) = c^2\det(A)$, it is impossible to produce a cA with a quadratic residue determinant since det(A) is not a square. □

Corollary 6.9. *There are $\frac{p(p^2-1)}{2}$ elements (or equivalence classes) in $PSL(2, \mathbb{F}_p)$.*

Proof. Since no two elements of $PGL(2, \mathbb{F}_p)$ are scalar multiples of each other and there are equal numbers of quadratic residues and nonresidues using theorem 6.2, then $|PSL(2, \mathbb{F}_p)| = \frac{|PGL(2,\mathbb{F}_p)|}{2} = \frac{p(p^2-1)}{2}$. □

Theorem 6.10. *[Jacobi Four Square] The number of ways to represent any positive integer n as the sum of four squares is $8\sum_{\substack{m|n \\ 4\nmid m}} m$ (8 times the sum of all its divisors which are not divisible by 4).*

Construction 6.11. [Lubotzky-Phillips-Sarnak Ramanujan graph] Let p, q be two distinct primes such that $p, q \equiv 1 \mod 4$ and i an integer satisfying $i^2 \equiv -1 \mod p$ which is possible from theorem 6.3. From theorem 6.10, there are $8(q+1)$ integer solutions to $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = q$. There are $q+1$ solutions such that $\alpha_0 > 1$ and is odd, and $\alpha_1, \alpha_2, \alpha_3$ are even. Associate with each such solution $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ the following matrix:

$$\alpha = \begin{bmatrix} \alpha_0 + i\alpha_1 & \alpha_2 + i\alpha_3 \\ -\alpha_2 + i\alpha_3 & \alpha_0 - i\alpha_1 \end{bmatrix}$$

Note the inverse of the matrix is simply the solution $(\alpha_0, -\alpha_1, -\alpha_2, -\alpha_3)$ corresponding to a factor $\frac{1}{q^2}$, which is 1 in the projective group.

Using this set of matrices as the generating set S of a Cayley graph, there is a bipartite and a non-bipartite construction of a $q+1$ regular Ramanujan graph:

Case 1: $(\frac{q}{p}) = -1$
In this case, the Cayley graph of the group $PGL(2, \mathbb{F}_p)$ with generating set S generates a bipartite Ramanujan graph with $p(p^2 - 1)$ vertices.

Case 2: $(\frac{q}{p}) = 1$
In this case, note that $\det(\alpha) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = q = x^2$ in $\mathbb{F}_p$. Since the determinant is a square modulo and all matrices are not scalar multiples of each other, then all elements of S belong in $PSL(2, \mathbb{F}_p)$, which is the group of vertices for the Cayley graph. This generates a non-bipartite Ramanujan graph with $\frac{p(p^2-1)}{2}$ vertices.

The LPS construction generates a connected Ramanujan graph with a nontrivial eigenvalue bound of $2\sqrt{q}$, the proof of which is beyond the scope of this paper [6]. Since a bipartite Ramanujan graph is proven to exist for all degrees [5], particular interest is given to the explicit construction of an infinite family of non-bipartite Ramanujan graphs, which there have been very few of over the years.

Construction 6.12. (LPS Hashing)
Assign an arbitrary ordering to the generators in S. The LPS hash function first converts the input α to a base q number based on a key of the given alphabet. Starting at a vertex, each digit of the resulting number determines which element of $S \backslash g^{-1}$ to multiply by in order to determine the next vertex without backtracking. Note that g is a previous element that was used. The final vertex corresponds to the output of the hash.

Thus, the LPS hash function is a random walk over the graph. Ramanujan graphs, which maximize the expansion constant, are ideal due to the rapidly mixing property as they approach uniform distribution faster. Since outputs are uniformly distributed over the set of hash codes, this minimizes two inputs hashing to the same vertex. Another way to think of collision resistance is using girth. Finding collisions is equivalent to finding cycles in the graph, so a large girth would ensure a smaller probability of collision.

Definition 6.13. A *reduced word* over S is a finite sequence $s_1, ..., s_n$ such that either s_i or $s_i^{-1} \in S$ and $s_{i+1} \neq s_i^{-1}$ for all $i = 1, ..., n$.

Definition 6.14. Let $\phi : PSL(2, \mathbb{F}_p) \to PSL(2, \mathbb{Z})$ such that for $A \in PSL(2, \mathbb{F}_p)$, $a_{ij} \to p + a_{ij}$. Let $\gamma = \sup_{A \in PSL(2, \mathbb{F}_p)} \|\phi(A)\|$, which exists since $\mathbb{F}_p$ is finite.

Proposition 6.15. *For the non-bipartite LPS Ramanujan graph G with n vertices,* $\text{girth}(G) \geq \frac{\log n}{3 \log \gamma}$.

Proof. Let g be the girth of G, S be the generator set of the Cayley graph, and $W \in PSL(2, \mathbb{F}_p)$ correspond to a vertex in a cycle of length g. By the definition of a Cayley graph, $W \cdot s_1 \cdot ... \cdot s_g = W$, thus $s_1 \cdot ... \cdot s_g = I$ is a reduced word over S. Let $W' = \phi(s_1) \cdot ... \cdot \phi(s_g) \equiv I \mod p$. From the submultiplicativity of induced matrix norms, we have that $\|W'\| \leq \prod_{i=1}^{g} \|\phi(s_i)\| \leq \gamma^g$. Since $\phi(s_i) > 0$ for all i and $W' \equiv I \mod p$, then there exists a vector x such that $\|W'x\| \geq (p-1)\|x\|$ and $\|W'\| \geq (p-1)$. Furthermore, $(p-1)^3 \geq \frac{p^2(p-1)}{2}$ for $p \geq 4$, which is true for all non-bipartite constructions. Therefore, $g \geq \frac{\log \|W'\|}{\log \gamma} \geq \frac{\log p-1}{\log \gamma} \geq \frac{\log n}{3 \log \gamma}$. □

Sarnak proves a tighter and more explicit lower bound for the girth of $g \geq 2 \log_q p$, using $q^g = b_0^2 + 4p^2 b_1^2 + 4p^2 b_2^2 + 4q^2 b_3^2$ such that at least one b_1, b_2, b_3 is not zero [6]. From lemma 3.3, we have that $\text{diam}(G) \geq \frac{\log n - 3 \log \gamma}{6 \log \gamma}$, which is also the result of lemma 3.2 and corresponds to the Alon-Boppana bound.

Acknowledgments. It is a pleasure to thank my mentors, Josh Falk and Owen Barrett, for their expertise and guidance throughout the project, which would have been impossible without them. I would also like to thank Professor May for making the REU possible and Professor Babai for the wonderful and thought-provoking lectures.

References

[1] Denis Charles, Kristin Lauter, and Eyal Zvi Goren. Cryptographic Hash Functions from Expander Graphs. *Journal of Cryptology*, 2008. doi: 10.1007/s00145-007-9002-x.

[2] G. A. Margulis. Explicit Constructions of Graphs Without Short Cycles and Low Density Codes, *Combinatorica 2*, **1** (1982) 71-78.

[3] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan Graphs. *Combinatorica 8*, **3** (1988) 261-277.

[4] Mike Krebs, Anthony Shaheen. Expander Families and Cayley Graphs. Oxford University Press. 2011.

[5] Adam W. Marcus, Daniel A. Spielman, Nikhil Srivastava. Interlacing Families I: Bipartite Ramanujan Graphs of All Degrees. Cornell University Library. 2014.

[6] Peter Sarnak. Some Applications of Modular Forms. Cambridge University Press. 1990.

[7] Christopher Williamson. Spectral Graph Theory, Expanders, and Ramanujan Graphs. University of Washington. 2014.