RAMANUJAN GRAPHS

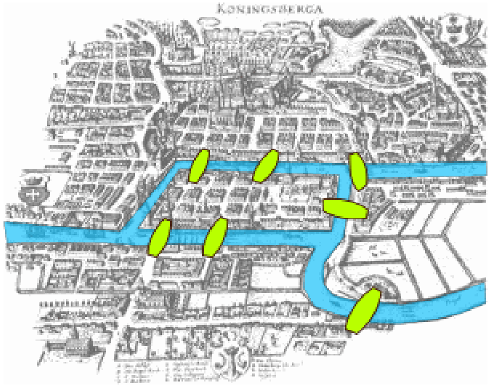
ETHAN YAN

1. Abstract

This paper will assume basic knowledge of graph theory and dive into expander graphs first, which gives motivation for Ramanujan graphs. Then, it will proceed to discuss explicit constructions of Ramanujan graphs as well as the applications of them to the real world.

2. Introduction

One of the most famous (and possibly the first) problems in graph theory is the Bridges of Königsberg (shown below). Leonhard Euler was believed to attempt finding a path that crosses through each edge exactly once (also known as an Euler path) , but he later proved that it was impossible. This was one of the first applications of graph theory.



Euler noted that, when the bridges were represented with edges and pieces of land vertices, each of the vertices had an odd degree. Vertices with an odd degree have a unique property: They have to be either a starting or ending vertex of an Euler path.

Since this problem, graph theory has evolved into a diverse and complex field of mathematics. Currently, it has many applications in numerous fields, such as computer and traffic networking, logistic optimization (shortest path algorithms), and solving puzzles (through graph coloring).

Much research has been centered on the notion of an ”optimal graph,” the notion of a graph well-suited for a particular task, bringing up the notion of Ramanujan graphs, which I will present in this paper.

Date: June 2024.

Acknowledgements

I would like to thank Simon Rubinstein-Salzedo and Christina Yu for their help in writing this paper.

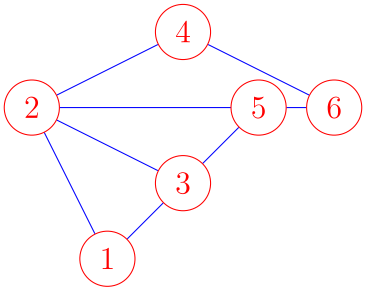
3. Basic Definitions

Definition 3.1. A **node** or **vertex** is a fundamental unit or object in graph theory, often contained in a set of vertices denoted V, and an edge is a connection between two nodes, often contained in a set denoted E. Each element of E is actually a two element subset of V, denoting the two vertices that the edge is connecting.

Definition 3.2. The **degree** of a vertex is the number of edges that are attached to that particular vertex. A regular graph is a graph in which all vertices have the same degree, often denoted a d-regular graph (each vertex has degree d). In this paper, we will primarily be focusing on d-regular graphs, as irregular Ramanujan graphs are tough to construct explicitly.

Definition 3.3. The **diameter** of a graph is the longest path that can be taken between two vertices.

Definition 3.4. The **adjacency matrix** of a graph has the graph's vertices as rows and columns. If there is an edge connecting vertex i to vertex j, then the element at row i and column j will be labelled with a 1. Otherwise, the elements will be labelled with a 0. For example, the following graph:



has the following adjacency matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

4. Expander Graphs

Expander graphs are have two notable properties: that they are sparse and highly connected.

Definition 4.1. A sparse graph contains close to the minimum number of edges possible for a given set of n vertices. In a connected, undirected graph, the minimum number of edges is equal to $n-1$, while the maximum number is $\binom{n}{2} = \frac{n(n-1)}{2}$. In a CS context, even as the total number of vertices approaches infinity, the number of edges in a sparse can be generated in $O(n)$ time.

Definition 4.2. An edge boundary, denoted ∂S, of a set of vertices S is the set of edges attached to both a vertex in S and a vertex in $\overline{S}$.

Definition 4.3. A highly connected graph can be defined in multiple contexts, but the most common one is a bounded Cheeger constant. Also known as the expansion ratio, it is denoted:

$$h(G) = \min_{\{S \mid |S| \leq \frac{n}{2}\}} \frac{|\partial S|}{|S|}.$$

This is also a measure of how easily it is (the minimum number of edges it takes) to sever a graph into two pieces, and, in an expander graph, it is bounded to be at least a certain constant (varies in many cases).

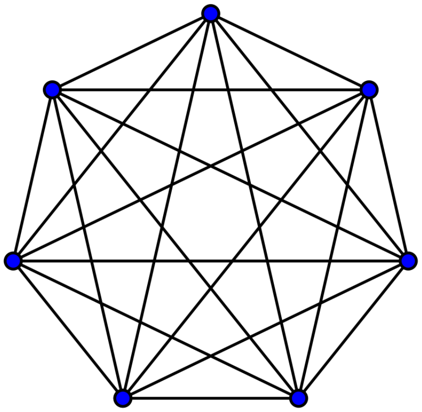


Figure 1. A complete graph

Consider the above two graphs. The complete graph seems like a good contender for an expander graph due to its high connectivity. However, as we take the number of vertices to approach infinity, it becomes clear that the number of edges is far from $O(n)$, meaning that it doesn't satisfy the sparcity requirement.

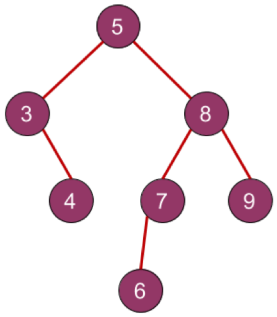


Figure 2. A tree

Conversely, if we consider the case of a tree, it seems like the perfect candidate for sparcity. However, as we take the number of vertices to be approaching infinity, the Cheeger constant becomes very small. (The limiting group is the group of nodes $\{6, 7, 8, 9\}$)

As seen from the above two examples, the two goals of sparcity and high connectivity are hard to satisfy at once, causing expander graphs to be hard to explicitly construct as the number of vertices approaches infinity. This motivates us to take a spectral graph theory route to further analyze these graphs involving concepts such as the spectrum of the graph and adjacency matrices, as will be discussed in the following sections.

Remark 4.4. Expander graphs have many notable applications, such as in data and road networks. In these scenarios, the networks often require high connectivity, but the analogs of edges have heavy costs tied to them, bringing up the importance of a sparse graph.

5. Properties of Adjacency Matrices

Now, we will consider notable properties of the adjacency matrix of a d-regular graph.

Definition 5.1. An **eigenvector** of a matrix is a vector whose direction is unchanged after a matrix transformation.

Definition 5.2. An **eigenvalue** of a matrix is the scalar that gets multiplied to an eigenvector during a matrix transformation.

If the matrix A has an eigenvector $\mathbf{v}$ and an eigenvalue λ, then the following equation is satisfied:

$$A\mathbf{v} = \lambda\mathbf{v}$$

It turns out that the first eigenvalue of an adjacency matrix of a d regular graph is d, with a corresponding eigenvector of all ones. This is because all rows and columns of the adjacency matrix contain exactly d ones, which means multiplying the matrix by the eigenvector will return a vector filled with ds.

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Figure 3. The adjacency matrix of a 6-vertex, 3-regular graph.

Definition 5.3. The **spectrum** of a matrix is the set of eigenvalues of that matrix, where $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \dots \lambda_n$.

Definition 5.4. A **spectral gap** is defined to be the quantity $d - \lambda_2$, where d is the degree of a graph and λ_2 is the second eigenvalue.

Theorem 5.5 (Cheeger Inequalities). *Given a d-regular graph,*

$$\frac{d - \lambda_2}{2} \geq h(G) \geq \sqrt{2d(d - \lambda_2)}.$$

[2]

From this, we can see that a large spectral gap implies a good expander, and a good expander implies a large spectral gap.

6. Bound on Spectral Gap

Now, we must look at how large the spectral gap can actually get, which means we must investigate the upper bound on λ_2.

Theorem 6.1 (Alon-Boppana Bound). *For d-regular graph G with adjacency matrix A with eigenvalues $\lambda_1, \lambda_2, \dots \lambda_n$ and diameter m,*

$$\lambda_2 \geq 2\sqrt{d-1} - \frac{2\sqrt{d-1}}{\lfloor m/2 \rfloor}.$$

This theorem upper bounds how large the spectral gap can get, which offers insight into why expander graphs are especially difficult to construct. The proof of the full theorem is beyond the scope of this paper, but we will see a proof of a less restrictive form of the bound [12]:

Theorem 6.2 (Alon-Boppana Bound Simplified). *For d-regular graph G with adjacency matrix A with eigenvalues $\lambda_1, \lambda_2, \dots \lambda_n$,*

$$\lambda_2 \geq 2\sqrt{d-1} - o(1).$$

Proof. For our proof, we will use a trace argument to upper bound the trace of an adjacency matrix raised to the $2k$ power to that of the infinite d-regular tree. We then utilize the Catalan numbers and approximation to get our bound.

First, we can utilize the trace of the matrix, or the sum of the diagonal entries. From the definition of the determinant of a matrix and Vieta's formulas, we can determine that the trace is also equal to the sum of the eigenvalues, the roots of the characteristic polynomial of the adjacency matrix.

It turns out that the eigenvalues of a matrix raised to the kth power are eigenvalues of the original matrix raised to the power k.

From here, we let $\lambda = max(|\lambda_2|, |\lambda_n|)$.

Then,

$$Tr(A^{2k}) = \sum_{i=1}^{n} \lambda_i^{2k} \leq d^{2k} + (n-1)\lambda^{2k}.$$

The first term in the right hand side comes from the fact that the first eigenvalue of a d-regular graph is d, and the second comes from our definition of λ.

Lemma 6.3. *The sum of the diagonal entries of A^k represents the number of closed paths of length k in A.*

Proof. We can use induction to prove this lemma. By definition, $A_{i,j}$ is the number of paths of length 1 from node i to node j. Assume that $A_{i,j}$ is the number of paths of length $k-1$ from node i to node j. Then,

$$A^{k-1} \cdot A = A^k$$

$$A^k_{i,j} = A^{k-1}_{i,1}A_{1,j} + A^{k-1}_{i,2}A_{2,j} + \ldots + A^{k-1}_{i,n}A_{n,j} = \sum_{x=1}^{n} A^{k-1}_{i,x}A_{x,j}.$$

Each product in the above sum is nonzero if and only if i and j are both connected to node x. By the principle of mathematical induction, $A^k_{i,j}$ = the number of paths of length k from i to j. Hence, our proposed statement is proven. ■

We then notice that, by Lemma 4.3,

$$Tr(A^{2k}) = (\text{\# of closed paths of length } 2k \text{ in } G) \geq n \cdot (\text{\# closed paths of length } 2k \text{ in an infinite } d \text{ regular tree })."$$

To see this, we note how when making a closed path in a tree, we can only increase or decrease the distance to the starting node by 1, due to the fact that there are no cycles. This limits the number of choices to make compared to a random d-regular graph G, where cycles are permitted.

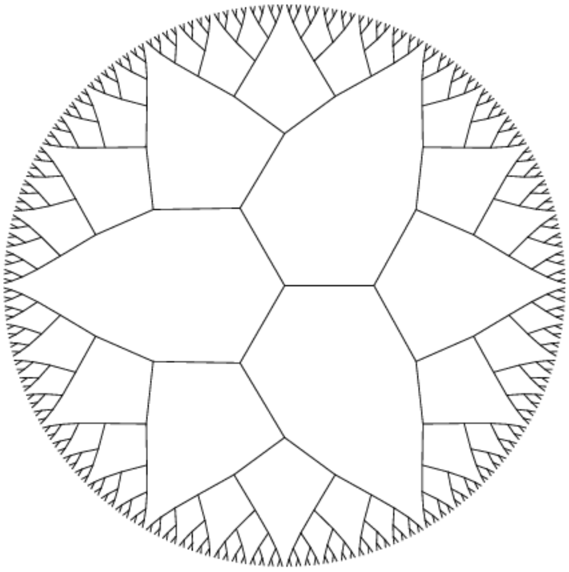


Figure 4. An infinite 3-regular tree

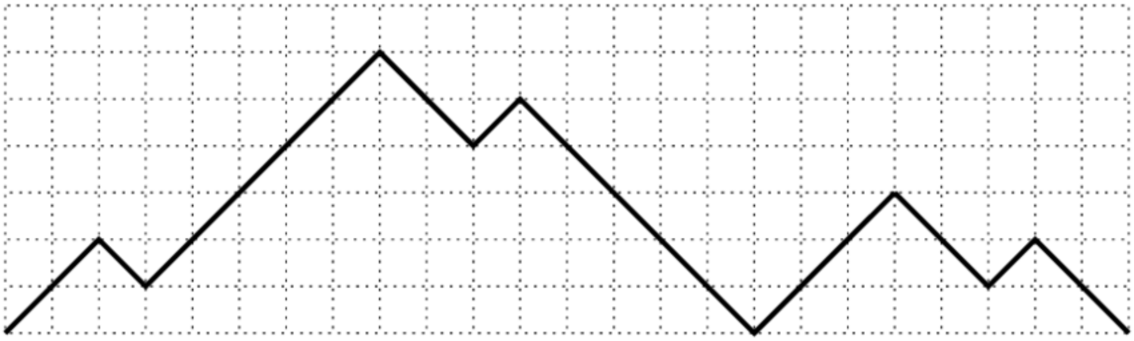


Figure 5. A Dyck path of length 24.

To count the number of possible closed paths in an infinite d-regular tree (above is an infinite 3-regular tree), we note how the fact that we can only increase or decrease the distance by 1 makes the closed walk a Dyck path. Therefore, the number of paths would correspond to the kth Catalan number. Moreover, from each choice, we have $d-1$ edges to pick from (as the tree is d-regular). Hence, we get

$$d^{2k} + (n-1)\lambda^{2k} \geq n \cdot \frac{1}{k+1}\binom{2k}{k}(d-1)^k.$$

Moving around the terms and dividing by $n-1$ from both sides, we get

$$\lambda^{2k} \geq \frac{n}{n-1}\left(\frac{1}{k+1}\binom{2k}{k}(d-1)^k\right) - \frac{d^{2k}}{n-1}.$$

.

After taking the $\frac{1}{2k}$th power of the inequality and utilizing some approximation, we get

$$\lambda \geq 2\sqrt{d-1} - o(1).$$

. ■

7. Ramanujan Graphs

Definition 7.1. A **Ramanujan graph** has $\lambda(G) \leq 2\sqrt{d-1}$. This relationship implies that Ramanujan graphs have small second eigenvalues, making them incredibly good expander graphs. [10]

An example of a Ramanujan graph is the complete graph K_{d+1} (with degree $d+1$). The spectrum of the graph is $d, -1, -1, \ldots, -1$, and $\lambda(K_{d+1}) = 1$, making the graph Ramanujan for $d > 1$.

Theorem 7.2 (Alon's Conjecture)**.** *Incidentally, for every $\epsilon > 0$ and random (n, d) graph G, $Pr(\lambda(G) \leq 2\sqrt{d-1} + \epsilon) = 1 - o_n(1)$, where $\lim_{n->\infty} o_n(1) = 0$.*

In other words, every d-regular graph has a high probability that it is weakly Ramanujan [5] [8].

7.1. LPS Construction of Ramanujan Graph.

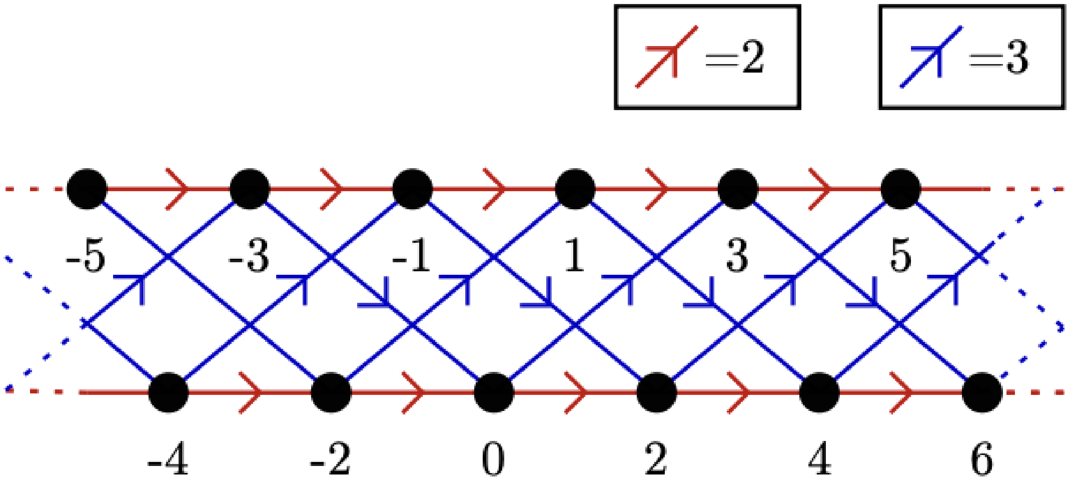
Theorem 7.3 (Theorem proposed by Lubotzky, Phillips, and Sarnak)**.** *For every prime number p, Infinite sequences of Ramanujan graphs exist for $d = p + 1$. [3]*

Definition 7.4. A **generating set** of a group is a subset of the group such that any element within a group can be constructed through the operation defined by the group applied to elements of the generating set and their inverses.

Definition 7.5. A **Cayley Graph** $\Gamma = \Gamma(G, S)$ is constructed by:

- A vertex set G
- Each edge $s \in S$ assigned a color s belonging to the generating set.
- There is an edge of color s connecting g and gs, where gs represents the operation of the group applied between g and s.

Remark 7.6. It is possible for a Cayley Graph to have a double edge if s is its own inverse.



In the Cayley graph above, the red arrows represent the generator of 2 and the blue arrows represent the generator of 3. Together, they make up the generating set of $\{2, 3\}$. Using the group uoperation of edition, these two generators can generate the vertex set of all the integers.

Definition 7.7. An integer q is a quadratic residue of p if $(\exists x)(x^2 \equiv q \mod p)$.

Definition 7.8. The Legendre symbol, denoted $(\frac{q}{p})$ satisfies the following:

(1) If $(\frac{q}{p}) = 1$, then q is a quadratic residue of p.
(2) If $(\frac{q}{p}) = -1$, then q is a quadratic nonresidue of p.

Lemma 7.9. *Let a and x be integers, and let p be an odd prime such that $p \nmid a$. Then, $x^2 \equiv a \mod p$ has either none or two incongruent solutions modulo p.*

Lemma 7.10. *Every odd prime p has $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues.*

Proof. Suppose that p has k incongruent quadratic residues. By Lemma 5.9, each one of them has 2 solutions, meaning that there are $2k$ solutions total. The set of least positive residues 1 through $p-1$ make up a solution set, so $2k = p - 1$, which means that $k = \frac{p-1}{2}$. From here, we get that there are $\frac{p-1}{2}$ quadratic nonresidues as well, completing our proof. ■

Theorem 7.11 (Wilson's Theorem). *For any prime p, $(p-1)! \equiv -1 \pmod p$.*

Proof. Any number other than numbers that are $1 \pmod p$ or $-1 \pmod p$ has a unique modular inverse. Hence, we can say that $(p-1)! \equiv (p-1) \cdot 1 \pmod p \equiv -1 \pmod p$, as we can pair up all of the numbers other than $p-1$ and 1. ■

Theorem 7.12. *For an odd prime p, there exists an integer i such that $i^2 \equiv 1 \pmod 4$.*

Proof. By Wilson's Theorem, since $p-1$ divides 4,$(p-1)! \equiv ((\frac{p-1}{2})!)^2(-1)^{\frac{p-1}{2}} \equiv ((\frac{p-1}{2})!)^2 \equiv -1 \pmod 4$ The value of $((\frac{p-1}{2})!)^2$ can serve as our i. ■

Definition 7.13. The **center** of a group G, often denoted $Z(G)$ is the set of elements within G such that the commutative property is preserved. In other words $Z(G) = \{z \in G | \forall g \in G, zg = gz\}$

Definition 7.14 (Prime Fields)**.** Prime fields, often denoted to be $\mathbb{F}_p$, are finite fields (finite set on which the operations are defined and satisfy basic rules) in which all the elements are integers $\pmod p$

Definition 7.15. We consider $GL(n, \mathbb{F}_p)$ to be the group of all $n \times n$ invertible matrices over $\mathbb{F}_p$. Its projective group is known as $PGL(n, \mathbb{F}_{|}) = GL(n, \mathbb{F}_p/Z(G)$, where $Z(G)$ is the group of identity matrices multiplied by a certain constant λ. Because of this, all matrices that are scalar multiples of each other are in the same equivalence class in the projective group. Moreover, the special linear group $SL(n, \mathbb{F}_p)$ consists of all matrices that are part of $GL(n, \mathbb{F}_p)$ that have determinant 1. Its projective group, $PSL(n, \mathbb{F}_p)$, has $Z(G)$ consisting of the positive and negative identity matrices.

It turns out that there are $p(p^2-1)$ elements in $PGL(2, \mathbb{F}_p)$ and $\frac{p(p^2-1)}{2}$ in $PSL(2, \mathbb{F}_p)$

The Construction:

Let p and q be two distinct primes, both $1 \pmod 4$ and i an integer such that $i^2 \equiv -1 \pmod p$. There are a total of $8(q+1)$ 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 the others are even. Associate with each set of solutions the following:

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

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

- if $(\frac{q}{p}) = -1$, then the Cayley graph of $PGL(2, \mathbb{F}_{|})$ with generating set S generates a bipartite Ramanujan graph with $p(p^2-1)$ vertices
- if $(\frac{q}{p}) = 1$,, the Cayley graph of $PSL(2, \mathbb{F}_p)$ will generate a non-bipartite Ramanujan graph with $\frac{p(p^2-1)}{2}$ vertices.

It turns out that the eigenvalue bound is $2\sqrt{q}$.

Morgernstern later generalized a construction for degree $d = p^k + 1$, where p is a prime and k a positive integer. However, an open problem in the field of Ramanujan graphs is if

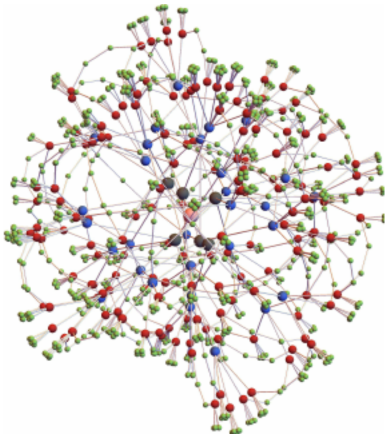


Figure 6. A 6-regular, 12180 vertex LPS Graph

we can construct arbitrarily large Ramanujan graphs for any degree d. The current smallest value for d that cannot satisfy this yet is $d = 7$.

8. Bipartite Ramanujan Graphs

Definition 8.1. A **bipartite** graph is a graph in which all the vertices can be divided into two disjoint sets such that all the edges connect a vertex in one set to a vertex in the other disjoint set.

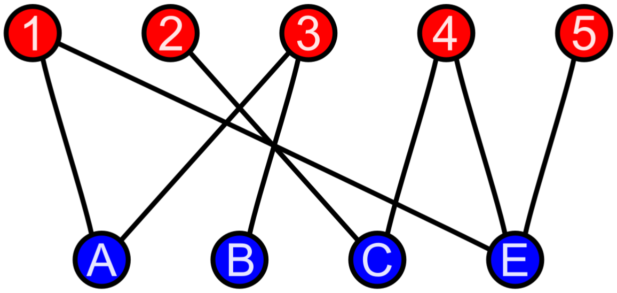


Figure 7. A bipartite graph.

It turns out that we can construct infinitely many d-regular bipartite Ramanujan graphs through a process called a 2-lift [13] [1] [4].

Definition 8.2. A 2-lift is a process that takes a graph and duplicates its vertices to construct a new graph. The process is as follows:

(1) Duplicate the graph (all edges and vertices)

(2) For each pair of vertices connected by an edge $\{v_1, v_2\}$, either leave them as is or cross them over. That is, if $\{v_1', v_2'\}$ are the duplicate vertices, then the edges will either remain as is or connect v_1 to v_2' and v_2 to v_1'.

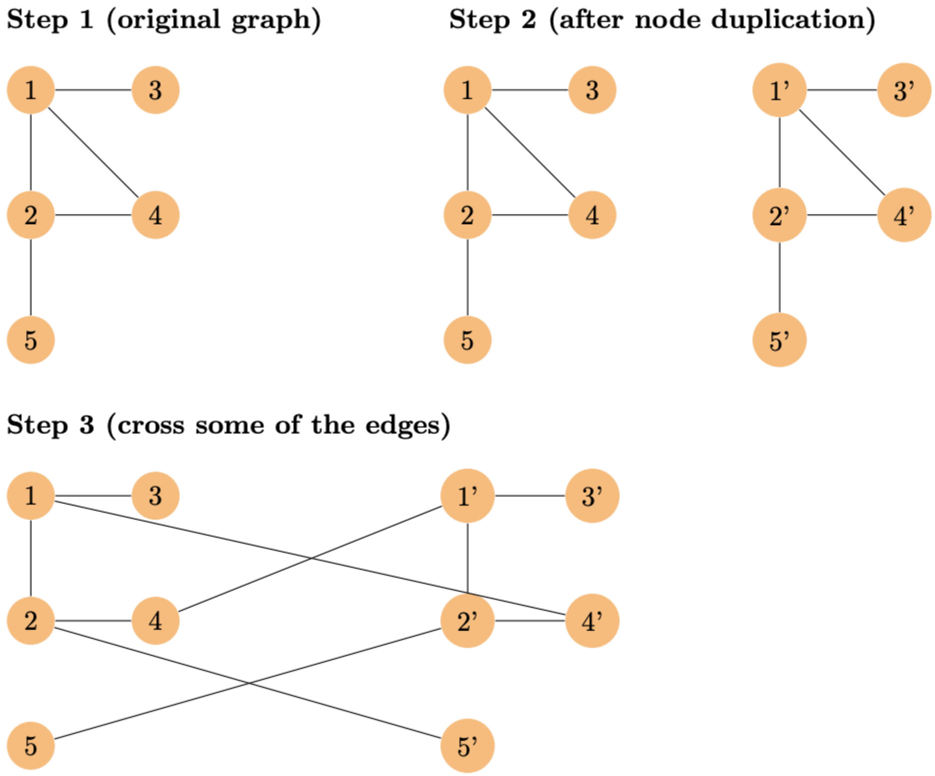

Step 1 (original graph)
Step 2 (after node duplication)
Step 3 (cross some of the edges)
1
3
2
4
5
1'
3'
2'
4'
5'

Figure 8. A 2-lift process.

We can now denote the original graph as G and the resulting graph G'. Suppose that the adjacency matrix of G looked like the following:

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Then, instead of creating a whole new separate $2n \times 2n$ matrix for G', we can instead replace 1 values with -1 values in the above adjacency matrix if the edges crossed over. An example of such a matrix would look like this:

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 & -1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & -1 & 0 & 0 \end{pmatrix}$$

We call this matrix the **signed matrix** of G', A_s Although it is not immediately obvious why we would do this, as we will soon see, the signed matrix has some unique relations with the eigenvalues of G'.

Lemma 8.3. *The eigenvalues of G' are the union of the eigenvalues of A and the eigenvalues of A_s, counting multiplicities.*

Proof. We can define two more matrices, A_1 and A_2 such that they satisfy the following:

$$(A_1)_{ij} = \begin{cases} x & \text{if } A_{ij} = 1 \text{ and } (A_s)_{ij} = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$(A_2)_{ij} = \begin{cases} x & \text{if } A_{ij} = 1 \text{ and } (A_s)_{ij} = -1 \\ 0 & \text{otherwise} \end{cases}$$

Because A_1 only has a 1 if a specific edge did not cross during the 2-lift and A_2 only has a 1 if a specific edge did cross, $A = A_1 + A_2$, where A was the original matrix of G. Utilizing similar reasoning, $A_s = A_1 - A_2$. Moreover, we have

$$A' = \begin{bmatrix} A_1 & A_2 \\ A_2 & A_1 \end{bmatrix}.$$

To understand why this is true, note that the A_1 matrices, which are in the top left corner and bottom right corner, represent all of the edges that connect vertices within the original and duplicated graphs, respectively. Conversely, the A_2 graphs represent all of the crossed over edges.

Now, we can define the action of vector concatenation. In this process, $[v_1, v_2]$ represents copying v_2 onto the end of v_1. We can also confirm, by definition of matrix-vector multiplication, that if v is an eigenvector of A, then $[v, v]$ is an eigenvector of A' with the same eigenvalue. Similarly, we can confirm that if u is an eigenvector of A_s, then $[u, -u]$ is an eigenvector of A' with the same eigenvalue.

From here, we utilize the fact that the eigenvectors of symmetric matrices are orthogonal. Since the relationship that $v_1 \perp v_2$ implies that $[v_1, v_1] \perp [v_2, v_2]$ (because the dot product remains to be 0 and, for the same reason, the relationship that $u_1 \perp u_2$ implies that $[u_1, -u_1] \perp [u_2, -u_2]$, we can say that all pairs of $[v, v]$ (where v is an eigenvector of A are orthogonal, and all pairs of $[u, -u]$ (where u is an eigenvector of A_s are orthogonal as well. Moreover, if we take the dot product of any $[v, v]$ and any $[u, -u]$, we get that $[v, v] \cdot [u, -u] = v \cdot u + v \cdot (-u) = 0$. Hence, all eigenvectors in A' are pairwise orthogonal.

Since A and A_s both have n orthogonal eigenvectors and A' has $2n$ orthogonal eigenvectors, we have proven our lemma.

■

As for constructing bipartite Ramanujan graphs from 2-lifts, we know that all complete d-regular bipartite Ramanujan graphs $K_{d,d}$ are Ramanujan due to the fact that the nontrivial eigenvalues are all 0 (the trivial ones being d and $-d$). We must look at the 2^m possible 2-lifts of the graph in order to determine if we can utilize a 2-lift to preserve the Ramanujan property of the bipartite graph. By the previous theorem we have proved, this boils down to checking whether the eigenvalues of A_s fall within the Ramanujan bound. As for the other two properties of being d-regular and bipartite, a 2-lift will preserve them due to how it is creating a duplicate of the current graph. In order to analyze the eigenvalues of the signed adjacency matrix, we must take a look at another concept: the matching polynomial.

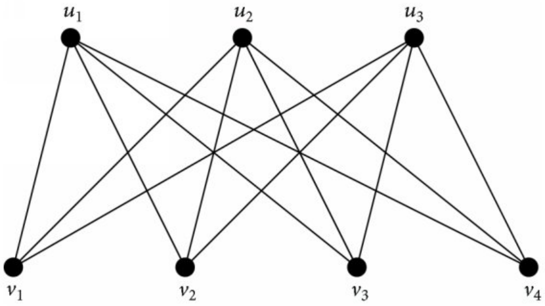
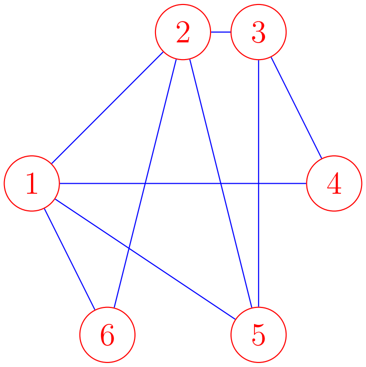


Figure 9. An example of a complete bipartite graph.

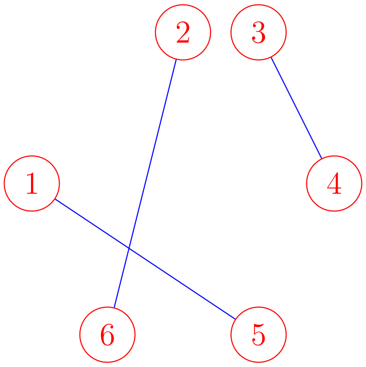
Definition 8.4. For a graph G, a graph matching is a certain subset of the edge set E of G such that no two of the edges share the same vertex.

For a graph with n vertex, the graph matching can contain a maximum of $\frac{n}{2}$ edges (due to the fact that any more edges will lead to intersecting vertices.

As an example, consider the following graph:



A possible graph matching could be the following:



Definition 8.5. The matching polynomial for G, where $m_i(G)$ represents the number of graph matchings possible for a certain number of edges i and $m_0(G) = 1$, is defined as

$$\mu_G(x) = \sum_{i \geq 0} x^{n-2i}(-1)im_i(G).$$

Note how when i surpasses $\frac{n}{2}$, $m_i(G)$ becomes 0.

We can utilize the matching polynomial through the following relation, where $A_s(x)$ is the characteristic polynomial of A_s and $\mathbb{E}_s$ represents the expected value :

$$\mathbb{E}_s[A_s(x)] = \mu_G(x).$$

From here, the problem boils down to bounding the roots of the matching polynomial.

Lemma 8.6. *Denote G with vertex i removed as the graph $G \backslash i$. Then,*

$$\mu_G(x) = x\mu_{G\backslash i}(x) - \sum_{\{i,j\} \in E} \mu_{G\backslash i \backslash j}(x).$$

Proof. Since the number of k-size graph matchings over G that do not involve the vertex i is $m_k(G\backslash i)$. Moreover, the number of matchings over G that do involve the vertex i is $\sum_{\{i,j\} \in E} m_{k-1}(G\backslash i \backslash j)$. Now, by definition,

$$m_k(G) = m_k(G\backslash i) + \sum_{\{i,j\} \in E} m_{k-1}(G\backslash i \backslash j)$$

Plugging this into the equation of the definition of $\mu_G(x)$ and performing some manipulation, we can get the statement we wanted to prove. ■

Lemma 8.7. *Suppose that $\delta \geq d > 1$. If deg$(i) < \delta$, then*

$$x > 2\sqrt{\delta - 1} \Rightarrow \frac{\mu_G(x)}{\mu_{G\backslash i}(x)} > \sqrt{\delta - 1}$$

Proof. We can prove this utilizing the principle of mathematical induction (over the number of vertices n. We can start with the base case of $n = 1$. Then, there are no edges, so we have that $\mu G(x) = x$ because there is one matching with no edges. We also have that $\mu G\backslash i(x) = 1$. The lemma does hold in this case due to the fact that

$$x > 2\sqrt{\delta - 1} \Rightarrow \frac{\mu_G(x)}{\mu_{G\backslash i}(x)} = x > 2\sqrt{\delta - 1} > \sqrt{\delta - 1}.$$

To proceed, we assume at the lemma holds for the case of $n = k$ vertices. By Lemma 6.6, we can say that:

$$\mu_G(x) = x\mu_{G\backslash i}(x) - \sum_{\{i,j\}\in E} \mu_{G\backslash i\backslash j}(x).$$

After plugging in our assumption for x and utilizing the fact that the lemma is satisfied for $n = k$, we get the following:

$$\frac{\mu_G(x)}{\mu_{G\backslash i}(x)} > 2\sqrt{\delta - 1} - \frac{1}{\sqrt{\delta - 1}} \sum_{\{i,j\}\in E} 1 = 2\sqrt{\delta - 1} - \frac{deg(i)}{\sqrt{\delta - 1}}.$$

From here, we remember how we made the assumption that $deg(i) < \delta$. This gives us the following: $\frac{\mu_G(x)}{\mu_{G\backslash i}(x)} > 2\sqrt{\delta - 1} - \frac{\delta - 1}{\sqrt{\delta - 1}} = \sqrt{\delta - 1}$. This proves the lemma for $n = k + 1$. By the principle of mathematical induction, our lemma is proven. ■

Theorem 8.8. *All real roots of* $\mu_G(x)$ *lie in the interval* $[-2\sqrt{d - 1}, 2\sqrt{d - 1}]$.

Proof. We can use the two lemmas above to prove this theorem. It suffices to show that there are no roots for $x > 2\sqrt{d - 1}$ We again utilize the principle of mathematical induction. For the base case, the $n = 1$ graph has $\mu_G(x) = x$, and the zero (which is 0), is within the desired interval. Thus, the base case is proven. Now we move on to the case of $n = k$.

From Lemma 6.6, we get that

$$\frac{\mu_G(x)}{\mu_{G\backslash i}(x)} = x - \sum_{\{i,j\}\in E} \frac{\mu_{G\backslash i\backslash j}(x)}{\mu_{G\backslash i}(x)}$$

Substituting in our assumption for x, we get

$$\frac{\mu_G(x)}{\mu_{G\backslash i}(x)} > 2\sqrt{d - 1} - \sum_{\{i,j\}\in E} \frac{\mu_{G\backslash i\backslash j}(x)}{\mu_{G\backslash i}(x)}.$$

Now we must consider two cases to prove this, case one being if there are no edges between i and j in G. This brings the the equation of

$$\frac{\mu_G(x)}{\mu_{G\backslash i}(x)} > 2\sqrt{d - 1}.$$

By the induction assumption, $\mu_{G\setminus i}(x)$ has no zeroes for $x > 2\sqrt{d-1}$. This implies that $\mu_G(x)$ has no zeroes for $x > 2\sqrt{d-1}$ as well because if that were so, the left hand side would be 0, violating the inequality.

Now we must consider case two: if there is an edge between i and j. Now, we have the following relation:

$$deg_{G\setminus i}(j) \leq d-1 < d.$$

This is because one of the edges that was connected to vertex j is removed alongside vertex i. We can utilize Lemma 6.7 to simplify this equation:

$$\frac{\mu_G(x)}{\mu_{G\setminus i}(x)} = x - \sum_{\{i,j\}\in E} \frac{\mu_{G\setminus i\setminus j}(x)}{\mu_{G\setminus i}(x)}$$

To this equation:

$$\frac{\mu_G(x)}{\mu_{G\setminus i}(x)} = x - \sum_{\{i,j\}\in E} \frac{1}{\sqrt{d-1}}.$$

This gives us the following:

$$\frac{\mu_G(x)}{\mu_{G\setminus i}(x)} > 2\sqrt{d-1} - \frac{deg_G(i)}{\sqrt{d-1}} \geq 2\sqrt{d-1} - \frac{d}{\sqrt{d-1}}.$$

Now, we take the following derivative:

$$\frac{d}{dt}(2\sqrt{d-1} - \frac{d}{\sqrt{d-1}}) = \frac{d}{2(d-1)^{\frac{3}{2}}}$$

We note that the derivative is always greater than 0 when $d \geq 2$. Hence, we get that $\frac{\mu_G(x)}{\mu_{G\setminus i}(x)} > 0$ whenever $x > 2\sqrt{d-1}$ We can now make the same argument we made during the proof of the base case: Since the denominator is never zero, we get that the numerator is never zero in order to ensure that the LHS remains positive. Hence, our theorem is proven. ■

Now, we run into some trouble. Although it would seem like we are finished with proving the existence of infinitely bipartite Ramanujan graphs, we utilized the concept of expected value on our characteristic polynomial of A_s. It turns out that the maximum root of all the polynomials in the characteristic polynomial can actually be above the maximum root of the expected characteristic polynomial. Hence, we must introduce a new concept: interlacing families.

Definition 8.9. We can say a polynomial with real roots $\alpha_1, \ldots, \alpha_{n-1}$ and degree $n-1$ interlaces a real-rooted degree n polynomial f with roots $\beta_1, \ldots, \beta_n$ if $\beta_1 \leq \alpha_1 \leq \ldots \leq \alpha_{n-1} \leq \beta n$.

Definition 8.10. If there exists a polynomial that interlaces each of hte polynomials $f_1, f_2, \ldots, f_k$, then we can say that $f_1, \ldots, f_k$ have a common interlacing.

It turns out that all possible characteristic polynomials do have a common interlacing, and there does exist a largest root of a certain polynomial that is the largest real root of the expected polynomial.

We can now proceed on to the proof of existence.

Theorem 8.11. *There exist infinite families of bipartite Ramanujan graphs of all $d \geq 3$.*

Proof. Select a certain degree $d \geq 3$. Then we can start off the 2-lift process with $K_{d,d}$, the complete bipartite graph of degree d, which is Ramanujan. After performing the 2-lift, the new graph is Ramanujan if the eigenvalues of A_s, the signed adjacency matrix, satisfy the Ramanujan bound. There exists a certain polynomial that has its largest root at least the largest root of $\mathbb{E}_s[A_s(x)]$, which equals $\mu_G(x)$. The largest root of the matching polynomial is at most $2\sqrt{d-1}$. Hence, the largest root of $A_s(x)$ is at most $2\sqrt{d-1}$. Because a 2-lift gives yet another bipartite graph, the smallest eigenvalue is $2\sqrt{d-1}$. Thus, we know that the new graph after the 2-lift is still Ramanujan. Hence, by continuing the process, we can generate an infinite family of bipartite Ramanujan graphs of degree d. ■

9. Applications

Because of their connectivity properties, Ramanujan graphs have many applications in fields such as computer science and pure mathematics. We will now explore them in the context of hash functions [7] [6].

Definition 9.1. A **hash function** is a function well studied in cryptography that takes a string of variable length and converts it to a string of fixed length.

Definition 9.2. A **hash collision** is when two messages have the same hash code. This becomes problematic when a collision can easily be artificially generated, which breaks a hash function (as there can be no certainty of the exact message that is stored from a specific hash code).

For the context of Ramanujan graphs, we are concerned with unkeyed hash functions, which do not require a specific key to decode, that are collision resistant.

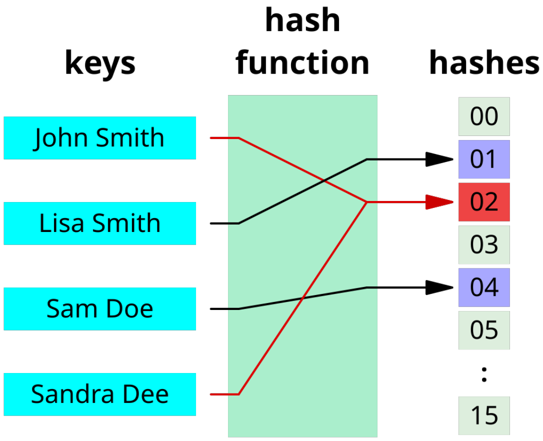


Figure 10. An example of a hash function.

One might wonder how exactly an input is transformed into an output for a hash function. It turns out that the input gives directions for a walk on the Ramanujan graph that is non-backtracking, and the output would be the ending vertex of the walk. Since there isn't any backtracking, for any d-regular graph, there are $d-1$ choices for the next edge to take. To make the right choice, the input message is split into e chunks, where $2^e \leq k-1$, and each succeeding chunk dictates the edge that is taken.

Definition 9.3. A **girth** of a graph is the length of the shortest cycle. It turns out that causing a collision in a hash code generated by a graph boils down to finding the shortest girth.

The girth of the LPS graph is optimal, and it is much larger than the girth of a random d-regular graph (which is already considered to be pretty large and is widely agreed to be hard to find).

References

[1] Bipartite ramanujan graphs. *cs.uwaterloo.ca.*

[2] Cheeger's inequality. *cs.waterloo.edu.*

[3] P. Sarnak A. Lubotzky, R. Phillips. Ramanujan graphs. *Combinatorica*, 1988.

[4] Nikhil Srivastava Adam W. Marcus, Daniel A. Spielman. Interlacing families iv: Bipartite ramanujan graphs of all sizes. *cs.yale.edu*, 2018.

[5] Charles Bordenave. A new proof of friedman's second eigenvalue theorem and its extension to random lifts. *univ-amu.fr*, 2019.

[6] Kristin Lauter Christophe Petit and Jean-Jacques Quisquater. Full cryptanalysis of lps and morgenstern hash functions. *uclouvain.be*, 2008.

[7] Kristin E. Lauter Denis X. Charles, Eyal Z. Goren. Cryptographic hash functions from expander graphs. *math.mcgill.ca*, 2006.

[8] Joel Friedman. A proof of alon's second eigenvalue conjecture and related problems. 2004.

[9] Swastik Kopparty. Expander graphs. *math.rutgers.edu*, 2011.

[10] Ram Murty. Ramanujan graphs. *math.queensu.ca*, 2003.

[11] Richard E. Quandt. Some basic matrix theorems. *math.princeton.edu*.

[12] Luca Trevisan. The alon-boppana theorem. 2014.

[13] Christopher Williamson. Spectral graph theory, expanders, and ramanujan graphs. *sites.math.washington.edu*, 2014.

[11] [9]