MODULAR FORMS AND RAMANUJAN GRAPHS

Honours Year Project - Introductory Talk

Khor Shi-Jie, supervised by Prof Gan Wee Teck

March 9, 2016

National University of Singapore

Agenda

Modular Forms and Ramanujan Graphs

- Expander Graphs
- Ramanujan Graphs
- Construction of Ramanujan Graphs
  - Cayley Graphs
  - Quarternion Algebra
  - The Modular Group
- Directions of Research

EXPANDER GRAPHS

Graphs

We will begin with preliminary definitions.

We will begin with preliminary definitions.

Definition (Graph)

A graph is an ordered pair $X = (V, E)$ where V is the set of vertices and E is the set of edges.

Graphs

We will begin with preliminary definitions.

Definition (Graph)

A graph is an ordered pair $X = (V, E)$ where V is the set of vertices and E is the set of edges.

Definition (Path)

A path in graph X is a finite sequence of vertices $v_1, v_2, \cdots, v_k$ such that $\{v_i, v_{i+1}\}$ is an edge.

Graphs

We will begin with preliminary definitions.

Definition (Graph)

A graph is an ordered pair $X = (V, E)$ where V is the set of vertices and E is the set of edges.

Definition (Path)

A path in graph X is a finite sequence of vertices $v_1, v_2, \cdots, v_k$ such that $\{v_i, v_{i+1}\}$ is an edge.

Definition (Connectivity)

A graph X is connected if every two vertices can be joined by a path.

How Connected is a Graph?

We want a notion to **measure connectivity** in a graph.

How Connected is a Graph?

We want a notion to **measure connectivity** in a graph.

In other words, we want to have a quantity to classify whether a graph is highly connected or not.

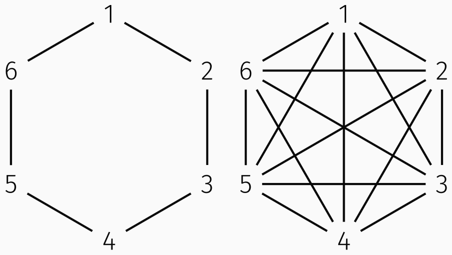


Figure: Which is the more connected graph?

Boundary of Vertices

Definition (Boundary of Vertices)

Given $F \subseteq V$, define the boundary of F to be the set of edges connecting from F to $V - F$. We denote the set as ∂F.

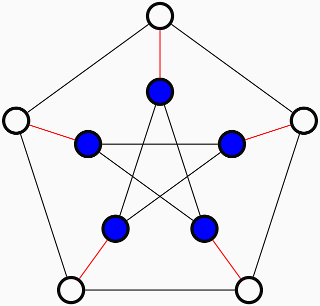


Figure: Take the blue nodes as F, then ∂F are labeled by the red edges.

Expanding Constant

Definition (Expanding Constant)

The expanding constant of graph X is defined to be

$$h(X) := \inf\left\{\frac{\partial F}{\min\{|F|, |V-F|\}} : F \subseteq V,\ 0 < |F| < \infty\right\}$$

Expanding Constant

Definition (Expanding Constant)

The expanding constant of graph X is defined to be

$$h(X) := \inf\left\{\frac{\partial F}{\min\{|F|, |V - F|\}} : F \subseteq V,\ 0 < |F| < \infty\right\}$$

Note that if X is a finite graph, we have

$$h(X) = \min\left\{\frac{\partial F}{|F|} : F \subseteq V,\ |F| \leq \frac{|V|}{2}\right\}$$

The **complete graph** K_n is a graph with n vertices in which every vertex is connected to every other vertex.

If $|F| = l$, then $|V - F| = n - l$ and hence $|\partial F| = l(n - l)$.

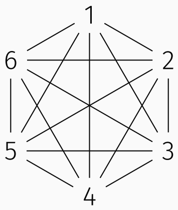


Figure: The complete graph K_6.

In general,

$$h(K_n) = n - \left\lfloor \frac{n}{2} \right\rfloor$$

Examples

The **cycle** C_n is a graph with n vertices in which the entire graph is a cycle (circuit).

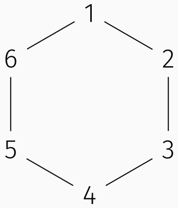


Figure: The cycle C_6.

It is obvious that

$$h(K_n) = \frac{2}{\lfloor \frac{n}{2} \rfloor}.$$

k-Regular Graphs

Definition

A k-regular graph is a graph in which the degree (i.e. number of edges incident to the vertex) of each vertex is equal to k.

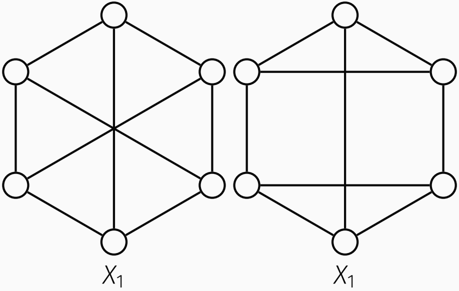


Figure: $h(X_1) = \frac{5}{3}, h(X_2) = 1$.

Family of Expanders

Definition

Fix a $k \in \mathbb{N}$. Let $(X_n)_{n \geq 1}$ be a sequence of finite, connected k-regular graphs $X_n = (V_n, E_n)$ indexed by $m \in \mathbb{N}$. $(X_n)_{n \geq 1}$ is known as a family of expanders if

1. $|V_n| \to +\infty$ when $n \to \infty$.
2. There exists $\epsilon > 0$ such that $h(X_n) \geq \epsilon$ for all $n \in \mathbb{N}$.

Family of Expanders

Definition

Fix a $k \in \mathbb{N}$. Let $(X_n)_{n\geq 1}$ be a sequence of finite, connected k-regular graphs $X_n = (V_n, E_n)$ indexed by $m \in \mathbb{N}$. $(X_n)_{n\geq 1}$ is known as a family of expanders if

1. $|V_n| \to +\infty$ when $n \to \infty$.
2. There exists $\epsilon > 0$ such that $h(X_n) \geq \epsilon$ for all $n \in \mathbb{N}$.

We require each graph in the family of expanders to be k-regular so that the number of edges grows linearly with respect to the number of vertices.

Question: Is $(K_n)_{n\geq 1}$ a family of expanders? Is $(C_n)_{n\geq 1}$ a family of expanders?

Family of Expanders

Main Problem of Study:
Provide explicit construction of a family of expanders.

Family of Expanders

Main Problem of Study:
Provide explicit construction of a family of expanders.

This is an important problem, as expander graphs can be applied in

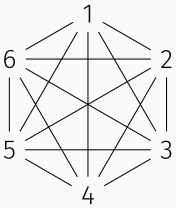
- constructing good pseudorandom number generators,
- derandomizing a probabilistic algorithm,
- constructing error correcting codes,
- or in building probabilistically checkable proofs.

RAMANUJAN GRAPHS

Adjacency Matrix

Definition (Adjacency Matrix)

The adjacency matrix A of a graph $X = (V, E)$ is a matrix indexed by the vertices of X such that A_{xy} is the number of edges between x and y in X.



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

Figure: Adjacency matrix for K_6.

Eigenvalues of Graph

Note that A is a $n \times n$ symmetric matrix (where $n = |V|$).

Eigenvalues of Graph

Note that A is a $n \times n$ symmetric matrix (where $n = |V|$).

Hence, A has n real eigenvalues. We will list the eigenvalues in decreasing order (note that the eigenvalues are listed with multiplicity):

$$k = \mu_0 \geq \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{n-1}$$

Eigenvalues of Graph

Note that A is a $n \times n$ symmetric matrix (where $n = |V|$).

Hence, A has n real eigenvalues. We will list the eigenvalues in decreasing order (note that the eigenvalues are listed with multiplicity):

$$k = \mu_0 \geq \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{n-1}$$

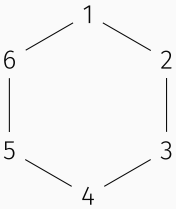
Proposition

Let X be a finite k-regular graph with n vertices. Then

1. $\mu_0 = k$;
2. $|\mu_i| \leq k$ for $1 \leq i \leq n-1$;
3. μ_0 has multiplicity 1 if and only if X is connected.

Examples

The cycle C_6 has the following adjacency matrix



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

Figure: Adjacency matrix for K_6.

The eigenvalues are $\mu_0 = 2, \mu_1 = \mu_2 = 1, \mu_3 = \mu_4 = -1, \mu_5 = -2$.

The following result bounds the expander constant of a graph X.

Theorem (Isoperimetric Inequality)

Let X be a finite, connected, k-regular graph. Then

$$\frac{k-\mu_1}{2} \leq h(X) \leq \sqrt{2k(k-\mu_1)}$$

Estimation of $h(X)$

The following result bounds the expander constant of a graph X.

Theorem (Isoperimetric Inequality)

Let X be a finite, connected, k-regular graph. Then

$$\frac{k-\mu_1}{2} \leq h(X) \leq \sqrt{2k(k-\mu_1)}$$

$k-\mu_1$ is known as the **spectral gap.**

Family of Expanders

Rephrased Problem

Fix a $k \in \mathbb{N}$. Find a sequence $(X_n)_{n\geq 1}$ of finite, connected k-regular graphs $X_n = (V_n, E_n)$ indexed by $m \in \mathbb{N}$. $(X_n)_{n\geq 1}$ where

1. $|V_n| \to +\infty$ when $n \to \infty$.
2. There exists $\epsilon > 0$ such that $\boldsymbol{k - \mu_1(X_n)} \geq \epsilon$ for all $n \in \mathbb{N}$.

To have a good family of expanders, note that our spectral gap has to be as large as possible!

Bounds on the Spectral Gap

How large can the spectral gap be?

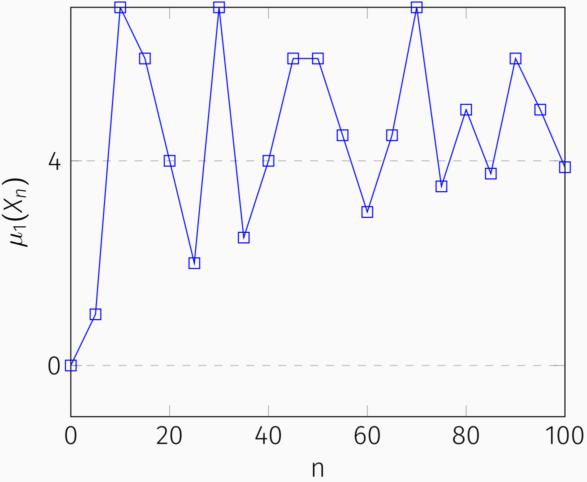
Theorem (Alon and Boppana)

Let $(X_n)_{n\geq 1}$ be a sequence of finite, connected, k-regular graphs with $|V_n| \to +\infty$ as $n \to +\infty$. Then

$$\liminf_{n\to+\infty} \mu_1(X_n) \geq 2\sqrt{k-1}$$

Bounds of Eigenvalues

How can we interpret the result? (Assume $k = 5$)



Ramanujan Graph

Definition (Ramanujan Graph)

A finite, connected, k-regular graph X is a Ramanujan graph if every non-trivial eigenvalue μ of X satisfy $|\mu| \leq 2\sqrt{k-1}$.

Ramanujan Graph

Definition (Ramanujan Graph)

A finite, connected, k-regular graph X is a Ramanujan graph if every non-trivial eigenvalue μ of X satisfy $|\mu| \leq 2\sqrt{k-1}$.

Note that a family of Ramanujan graph $(X_n)_{n\geq 1}$ in which $|V_n| \to +\infty$ for $n \to +\infty$ will attain equality in Alon and Boppana's bound.

Ramanujan Graph

Definition (Ramanujan Graph)

A finite, connected, k-regular graph X is a Ramanujan graph if every non-trivial eigenvalue μ of X satisfy $|\mu| \leq 2\sqrt{k-1}$.

Note that a family of Ramanujan graph $(X_n)_{n\geq 1}$ in which $|V_n| \to +\infty$ for $n \to +\infty$ will attain equality in Alon and Boppana's bound.

Hence, a family of Ramanujan graph is **optimal from the spectral point of view.**

CONSTRUCTION OF RAMANUJAN GRAPH

The Name "Ramanujan"

Works of Srinivasa Ramanujan mainly centers around number theory. It is surprising to apply his result in the realm of graph theory.

[1] We have $\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots$ where $q = e^{2\pi i z}$.

The Name "Ramanujan"

Works of Srinivasa Ramanujan mainly centers around number theory. It is surprising to apply his result in the realm of graph theory. Turns out that the construction of Ramanujan graphs often invoke the Ramanujan conjecture.

[1] We have $\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots$ where $q = e^{2\pi i z}$.

The Name "Ramanujan"

Works of Srinivasa Ramanujan mainly centers around number theory. It is surprising to apply his result in the realm of graph theory. Turns out that the construction of Ramanujan graphs often invoke the Ramanujan conjecture.

Theorem (Ramanujan-Petersson conjecture)

Define the Ramanujan's τ function to be the Fourier coefficients of the cusp form $\Delta(z)$[1] *of weight 12. Then*

$$|\tau(p)| \leq 2p^{\frac{11}{2}}$$

[1]We have $\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots$ where $q = e^{2\pi i z}$.

Cayley Graphs

We need to find a good source of family of graphs.

We need to find a good source of family of graphs.

Definition (Cayley Graph)

Let G be a group. Choose $S \subseteq G$ such that S is symmetric, i.e. $S = S^{-1}$.

The Cayley graph $\mathcal{G}(G, S)$ is defined with the following vertex set and edge set:

$$
\begin{aligned}
V &= G \\
E &= \{\{x, y\} : x, y \in G, \exists s \in S : y = xs\}
\end{aligned}
$$

Examples of Cayley Graphs

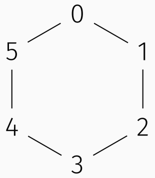


Figure: $G = \mathbb{Z}_6, S = \{-1, 1\}$.

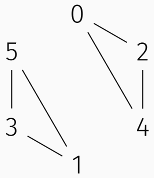


Figure: $G = \mathbb{Z}_6, S = \{-2, 2\}$.

Examples of Cayley Graphs

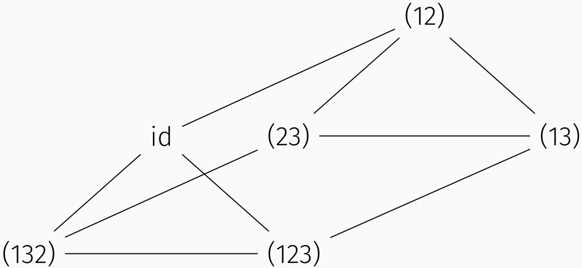


Figure: $G = \mathrm{Sym}_3, S = \{(123), (132), (12)\}$.

What should the choice of G and S be to generate a family of Ramanujan graphs?

[2] Denote $GL_2(K)$ as the group of invertible 2×2 matrices with entries in K, and $SL_2(K)$ as the subgroup of $GL_2(K)$ of matrices with determinant equals to 1.

Modular Group

What should the choice of G and S be to generate a family of Ramanujan graphs? Since the Ramanujan conjecture is related to modular forms, it is no surprise that G is chosen to be the modular group.

[2] Denote $GL_2(K)$ as the group of invertible 2×2 matrices with entries in K, and $SL_2(K)$ as the subgroup of $GL_2(K)$ of matrices with determinant equals to 1.

What should the choice of G and S be to generate a family of Ramanujan graphs? Since the Ramanujan conjecture is related to modular forms, it is no surprise that G is chosen to be the modular group.

Definition (Modular Group on Field K)

Suppose K is a field. We define $PSL_2(K)$, the modular group on the field K, to be [2]

$$PSL_2(K) = SL_2(K) \Big/ \left\{ \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix} : \epsilon = \pm 1 \right\}$$

[2] Denote $GL_2(K)$ as the group of invertible 2×2 matrices with entries in K, and $SL_2(K)$ as the subgroup of $GL_2(K)$ of matrices with determinant equals to 1.

Modular Group

We will simply denote $PSL_2(q)$ to be the modular group over the finite field of order q where q is a prime.

Proposition

1. $|PSL_2(q)| = \begin{cases} q(q^2-1) \text{ if } q \text{ is even} \\ \frac{q(q^2-1)}{2} \text{ otherwise} \end{cases}$
2. $|PSL_2(K)|$ is simple for $|K| \geq 4$.

Hamilton Quarternion Algebra

How should we choose the symmetric set for our Cayley graph?

Hamilton Quarternion Algebra

How should we choose the symmetric set for our Cayley graph?

Definition (Hamilton Quarternion Algebra)

The Hamilton quarternion algebra over a ring R, denoted by $\mathbb{H}(R)$, is a unital, associative algebra satisfying the following properties:

1. $\mathbb{H}(R)$ is a free R-module over the symbols $1, i, j, k$. Hence,

$$\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$$

2. 1 is the multiplicative identity.
3. $i^2 = j^2 = k^2 = -1$.
4. $ij = -ji = k; jk = -kj = i; ki = -ik = j$.

Integer Quarternions $\mathbb{H}(\mathbb{Z})$

Given a Hamilton quarternion algebra $\mathbb{H}(R)$, define the norm $N : \mathbb{H}(R) \to R$ by

$$N(a_0 + a_1 i + a_2 j + a_3 k) = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

We would like to investigate the irreducible elements in $\mathbb{H}(\mathbb{Z})$.

Integer Quarternions $\mathbb{H}(\mathbb{Z})$

Given a Hamilton quarternion algebra $\mathbb{H}(R)$, define the norm $N : \mathbb{H}(R) \to R$ by

$$N(a_0 + a_1 i + a_2 j + a_3 k) = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

We would like to investigate the irreducible elements in $\mathbb{H}(\mathbb{Z})$.

Proposition

$\delta \in \mathbb{H}(\mathbb{Z})$ is irreducible in $\mathbb{H}(\mathbb{Z})$ if and only if $N(\delta)$ is prime in $\mathbb{Z}$.

Sum of Four Squares

Using the multiplicativity of N and the previous proposition, we can easily conclude the following classical result

Theorem

Every natural number is a sum of four squares.

Sum of Four Squares

Using the multiplicativity of N and the previous proposition, we can easily conclude the following classical result

Theorem

Every natural number is a sum of four squares.

There is a stronger version of the above theorem proven by Jacobi.

Theorem

Let n be an odd positive integer. Then the number of ways to write n as a sum of four squares is $8\sum_{d|n} d$.

Distinguished Solutions

Note that if $\delta \in \mathbb{H}(\mathbb{Z})$ satisfy $N(\delta) = p$ [3], then for each $\epsilon \in \{\pm 1, \pm i, \pm j, \pm k\}$, we have $N(\epsilon\delta) = p$.

[3] In other words, the coefficients of δ presents a way to write p as a sum of four squares

Distinguished Solutions

Note that if $\delta \in \mathbb{H}(\mathbb{Z})$ satisfy $N(\delta) = p$ [3], then for each $\epsilon \in \{\pm 1, \pm i, \pm j, \pm k\}$, we have $N(\epsilon\delta) = p$.

Out of these 8 quarternions, we want to choose one of them and call it a **distinguished solution**.

[3] In other words, the coefficients of δ presents a way to write p as a sum of four squares

Distinguished Solutions

Note that if $\delta \in \mathbb{H}(\mathbb{Z})$ satisfy $N(\delta) = p$ [3], then for each $\epsilon \in \{\pm 1, \pm i, \pm j, \pm k\}$, we have $N(\epsilon\delta) = p$.

Out of these 8 quarternions, we want to choose one of them and call it a **distinguished solution**.

If $p \equiv 1 \pmod 4$, then exactly one out of the four coordinates must be odd. We will choose the solution in which the real part is odd and positive to be the distinguished solution.

If $p \equiv 3 \pmod 4$, then exactly one out of the four coordinate must be even, and we will make a similar choice above.

[3] In other words, the coefficients of δ presents a way to write p as a sum of four squares

Distinguished Solutions

Suppose $p = 5$, we have the following solutions to the four square problem:

(1, -2, 0, 0)	(1, 0, -2, 0)	(1, 0, 0, -2)	(1, 0, 0, 2)	(1, 0, 2, 0)	(1, 2, 0, 0)
$(-1, 2, 0, 0)$	$(-1, 0, 2, 0)$	$(-1, 0, 0, 2)$	$(-1, 0, 0, -2)$	$(-1, 0, -2, 0)$	$(-1, -2, 0, 0)$
$(2, 1, 0, 0)$	$(0, 1, 0, 0)$	$(0, 1, -2, 0)$	$(0, 1, 2, 0)$	$(0, 1, 0, 0)$	$(-2, 1, 0, 0)$
$(-2, -1, 0, 0)$	$(0, -1, 0, 0)$	$(0, -1, 2, 0)$	$(0, -1, -2, 0)$	$(0, -1, 0, 0)$	$(2, -1, 0, 0)$
$(0, 0, 1, -2)$	$(2, 0, 1, 0)$	$(0, 2, 1, 0)$	$(0, -2, 1, 0)$	$(-2, 0, 1, 0)$	$(0, 0, 1, 2)$
$(0, 0, -1, 2)$	$(-2, 0, -1, 0)$	$(0, -2, -1, 0)$	$(0, 2, -1, 0)$	$(2, 0, -1, 0)$	$(0, 0, -1, -2)$
$(0, 0, 2, 1)$	$(0, -2, 0, 1)$	$(2, 0, 0, 1)$	$(-2, 0, 0, 1)$	$(0, 2, 0, -1)$	$(0, 0, -2, 1)$
$(0, 0, -2, -1)$	$(0, 2, 0, -1)$	$(-2, 0, 0, -1)$	$(2, 0, 0, -1)$	$(0, -2, 0, 1)$	$(0, 0, 2, -1)$

The set of distinguished solutions is denoted as S_p[4].

[4] Note that we may refer to S_p as a subset in $\mathbb{H}(\mathbb{Z})$ or as an integer 4-tuple interchangeably.

Embedding Quarternions into Matrices

Note that our distinguished set is a subset of the quarternion, yet we stated previously that we would like to choose $PSL_2(q)$ as the base group for our Cayley Graph.

Embedding Quarternions into Matrices

Note that our distinguished set is a subset of the quarternion, yet we stated previously that we would like to choose $PSL_2(q)$ as the base group for our Cayley Graph. First, we consider the reduction modulo q,

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{Z}_q).$$

We would like to find a way to embed $\mathbb{H}(\mathbb{Z}_q)$ into $M_2(\mathbb{Z}_q)$.

Embedding Quarternions into Matrices

Proposition

If K is a field not of characteristic 2, suppose there exists $x, y \in K$ such that $x^2 + y^2 + 1 = 0$. Then $\mathbb{H}(K)$ is isomorphic to $M_2(K)$, the two-by-two matrices over K.

Embedding Quarternions into Matrices

Proposition

If K is a field not of characteristic 2, suppose there exists $x, y \in K$ such that $x^2 + y^2 + 1 = 0$. Then $\mathbb{H}(K)$ is isomorphic to $M_2(K)$, the two-by-two matrices over K.

The isomorphism is induced by $\psi : \mathbb{H}(K) \to M_2(K)$, defined as follows

$$\psi(a_0 + a_1 i + a_2 j + a_3 k) = \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}$$

Proposition

Let q be an odd prime power. Then there exists $x, y \in \mathbb{Z}_q$ such that $x^2 + y^2 + 1 = 0$.

Hence $\mathbb{H}(\mathbb{Z}_q)$ is isomorphic to $M_2(\mathbb{Z}_q)$. We denote the isomorphism by ψ_q.

Embedding S_p into $PSL_2(q)$

Combining the results from the previous slides, we note that

$$(\psi_q \circ \tau_q)(S_p) \subseteq GL_2(q)$$

Note that we omitted the proof that each element in S_p is mapped to an invertible matrix.

Embedding S_p into $PSL_2(q)$

Combining the results from the previous slides, we note that

$$(\psi_q \circ \tau_q)(S_p) \subseteq GL_2(q)$$

Note that we omitted the proof that each element in S_p is mapped to an invertible matrix. Define ϕ to be the projection map from $GL_2(q)$ to $PGL_2(q)$. Then we have

$$(\phi \circ \psi_q \circ \tau_q)(S_p) \subseteq PGL_2(q)$$

We denote $S_{p,q} = (\phi \circ \psi_q \circ \tau_q)(S_p)$.

The Cayley Graph $X^{p,q}$

It can be proven that $S_{p,q} \subseteq PSL_2(q)$ if $\left(\frac{p}{q}\right) = 1$.

When $\left(\frac{p}{q}\right) = 1$, define $X^{p,q} = \mathcal{G}(PSL_2(q), S_{p,q})$.

It can be proven that $S_{p,q} \subseteq PSL_2(q)$ if $\left(\frac{p}{q}\right) = 1$.

When $\left(\frac{p}{q}\right) = 1$, define $X^{p,q} = \mathcal{G}(PSL_2(q), S_{p,q})$.

The central theorem in the research is the following:

Theorem

$X^{p,q}$ is a non-bipartite Ramanujan graph with $\frac{q(q^2-1)}{2}$ vertices.

DIRECTIONS OF RESEARCH

Open Problem

The main objective is to prove that $X^{p,q}$ is a family of Ramanujan graphs.

Open Problem

The main objective is to prove that $X^{p,q}$ is a family of Ramanujan graphs.

Theorem

For the following values of k, there exist infinite families of k -regular Ramanujan graphs:

1. $k = p + 1$, *where p is an odd prime.*
2. $k = 3$.
3. $k = q + 1$, *where q is a prime power.*

Open Problem

The main objective is to prove that $X^{p,q}$ is a family of Ramanujan graphs.

Theorem

For the following values of k, there exist infinite families of k -regular Ramanujan graphs:

1. $k = p + 1$, *where p is an odd prime.*
2. $k = 3$.
3. $k = q + 1$, *where q is a prime power.*

Open Problem: *Is it possible to form Ramanujan graphs of arbitrary degree?*

References I

- G. Davidoff, P. Sarnak, and A. Valette, *Elementary number theory, group theory and ramanujan graphs*, Elementary Number Theory, Group Theory, and Ramanujan Graphs, Cambridge University Press, 2003.
- Shlomo Hoory, Nathan Linial, and Avi Wigderson, *Expander graphs and their applications*, BULL. AMER. MATH. SOC. **43** (2006), no. 4, 439–561.
- A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8**, no. 3, 261–277.
- Alexander Lubotzky, *Expander graphs in pure and applied mathematics*, Bull. Amer. Math. Soc. (N.S, 2012.

References II

- P. Sarnak, *Some applications of modular forms*, Cambridge Studies in Applied Ecology and Resource Management, Cambridge University Press, 1990.
- Jean-Pierre Serre, *A course in arithmetic*, Springer, 1993.

Thank You