Verification of Ramanujan Property for Pair Graphs obtained from Symmetric Groups

Division of Mathematics and Mathematical Science
Department of Computer Science and Engineering
Graduate School of Engineering
Nagoya Institute of Technology
JIANG Zheng(蒋 峥) *

Abstract

A Ramanujan graph is a sparse graph with high connectivity. In other words, it is a graph whose spectral gap is as large as possible. Its concrete construction has so far involved deep mathematical theories such as number theory, representation theory, algebraic geometry, and other fields. In 2016, Cid Reyes-Bustos constructed the pair graph from a pair of a group and its subgroup, and examined the Ramanujan property for the pair graph. In this talk, I will present the results of numerical calculations on pair graphs obtained from pairs of the symmetric group S_n and the alternating group A_n. For $3 \leq n \leq 10$, we discovered many 3-regular Ramanujan graphs.

1 Introduction

Ramanujan graph is a type of sparse graph whose connectivity is very good. In other words, it is such a type of graph with its spectrum gap as large as possible. Let $G = (V, E)$ be a graph, where V is the set of vertices and E is the set of edges. G can be completely represented by its adjacency matrix A algebraically. It is indexed by vertices of G. When G has n vertices, A is an $n \times n$ symmetric matrix whose element A_{xy} is the number of edges between x and y. A has n real eigenvalues and we list them in decreasing order according to multiplicities:

$$\mu_0 \geq \mu_1 \geq ... \geq \mu_{n-1}.$$

If G is connected and k-regular, it is known that

$$k = \mu_0 > \mu_1 \geq ... \geq \mu_{n-1} \geq -k.$$

When G is a bipartite graph, $\mu_{n-1} = -k$. We say that G is a *Ramanujan graph* if $|\mu_i| \leq 2\sqrt{k-1}$ for all $\mu_i \neq \pm k$. When G is bipartite, G is a Ramanujan graph if $\mu_1 \leq 2\sqrt{k-1}$. It is known that a regular graph is Ramanujan if and only if its Ihara zeta function satisfies an analog of the Riemann hypothesis [11].

In 1988, Margulis [7], Lubotzky, Phillips and Sarnak [5] independently gave the explicit construction of Ramanujan graphs for a fixed k and $n \to \infty$ in the case $k-1$ is prime. They constructed Ramanujan graphs as Cayley graphs of certain groups, and to investigate the spectrum, they used different branches of mathematics such as number theory, representation theory and algebraic geometry, cf. [9]. In 1994, Morgenstern [8] extended the result of [5] to the case

*E-mail:jiangzhengszkj@outlook.com

where $k-1$ is a prime power. In 2015, Marcus, Spielman and Srivastava [6] proved that there exist infinite families of regular bipartite Ramanujan graphs of every degree greater than 2. As is well known, expanders (see Definition 2.4 below) have many applications in computer science, and Ramanujan graphs are in some sense the best expanders, so they are also very useful in some situations where expanders are needed. For example, Ramanujan graphs of Pizer has been proposed as a basis for post-quantum elliptic-curve cryptography [3]. Ramanujan graphs can also be used to construct expander codes for good error correcting codes [1]. In addition, Lubetzky and Peres [4] proved that the simple random walk exhibits cutoff phenomenon on all Ramanujan graphs. This result depends strongly on the fact that these graphs are Ramanujan graphs and not just expanders.

Group-subgroup pair graphs were first proposed by Cid Reyes-Bustos [10]. A group-subgroup pair graph is constructed from a group G, a subgroup $H \subset G$, and a subset $S \subset G$. When the group G and its subgroup H are the same group, the definition reduces to that of a Cayley graph. A group-subgroup pair graph can become a Ramanujan graph if it satisfies certain conditions, which will be the core of our study. We see some examples which are the pair graphs constructed from symmetric group S_n and alternating group A_n in [10].

We consider the problem whether the group-subgroup pair graphs obtained from S_n and A_n are Ramanujan graphs or not. It turns out that the case $n=3$ is easy. In the case $n=4$, we compute eigenvalues of the pair graphs for all S with $|S| \leq 4$ and a few S with $|S|=5$. We think our computations have settled the problem for $n=4$, though we have no rigorous proof at present. Because of the increase of both the number of subsets S and vertices of the pair graph $\mathcal{G}(G,H,S)$ when $n \geq 5$, we restrict the form of S, in particular $|S|=3$. We found many examples of 3-regular Ramanujan graphs and we will introduce some of them in this talk.

2 Ramanujan Graph

All graphs will be supposed to have no loops. Assume that G is a finite graph with n vertices, then the adjacency matrix A is an $n \times n$ symmetric matrix, so all the eigenvalues are real and we list them in decreasing order:

$$\mu_0 \geq \mu_1 \geq \dots \geq \mu_{n-1}.$$

We call the set of the eigenvalues the *spectrum* of G. Note that μ_0 is a simple eigenvalue with multiplicity 1 if and only if $\mu_0 > \mu_1$. A function $f : V \to \mathbb{C}$ can be thought of as a vector in $\mathbb{C}^n$ on which the adjacency matrix acts in the following way:

$$Af = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{i1} & A_{i2} & \dots & A_{in} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} f(v_1) \\ f(v_2) \\ \vdots \\ f(v_n) \end{pmatrix}.$$

Proposition 2.1. *If $G=(V,E)$ is a finite k-regular graph with n vertices, we have:*

(a) $\mu_0 = k$*;*

(b) $|\mu_i| \leq k$ *for* $1 \leq i \leq n-1$*;*

(c) *The multiplicity of* μ_0 *is* 1 *if and only if* G *is connected.*

Proposition 2.2 ([2, Proposition 1.1.4])**.** *Let G be a connected, k-regular graph on n vertices. The following conditions are equivalent:*

(i) *G is bipartite;*

(ii) *the spectrum of G is symmetric about* 0*;*

(iii) $\mu_{n-1} = -k$.

Let $G = (V, E)$ be a graph. For $F \subseteq V$, we define the boundary ∂F of F to be the set of edges with one extremity in F and the other in $V - F$. That is to say, ∂F is the set of edges connecting F to $V - F$. Note that $\partial F = \partial(V - F)$.

Definition 2.3. *We define the expanding constant of a graph G as*

$$h(G) = \inf\{\frac{|\partial F|}{\min\{|F|, |V - F|\}} : F \subseteq V, 0 < |F| < +\infty\}.$$

If G is finite with n vertices, equation (2.3) also can be rephrased as:

$$h(G) = \min\{\frac{|\partial F|}{|F|} : F \subseteq V, 0<|F| \leq \frac{n}{2}\}.$$

Definition 2.4. *Let* $(G_m)_{m\geq 1}$ *be a family of finite k-regular connected graphs with* $|V_m| \to +\infty$ *when* $m \to +\infty$. *We say that* $(G_m)_{m\geq 1}$ *is a family of expanders if there exists* $\epsilon>0$ *such that* $h(G_m) \geq \epsilon$ *for each* $m \geq 1$.

Theorem 2.5 ([2, Theorem 1.2.3])**.** *Let* $G = (V, E)$ *be a finite, connected, k-regular graph with no loops, and* μ_1 *be the first nontrivial eigenvalue of G. We get:*

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

From Definition 2.4 and Theorem 2.5, we deduce the following:

Corollary 2.6. *Let* $(G_m)_{m\geq 1}$ *be a family of finite connected k-regular graphs with no loops, such that* $|V_m| \to +\infty$ *when* $m \to +\infty$. *The family* $(G_m)_{m\geq 1}$ *is a family of expanders if and only if there exists* $\epsilon>0$ *such that* $k - \mu_1(G_m) \geq \epsilon$ *for each* $m \geq 1$.

Remark 2.7. *From Definition 2.4 and Corollary 2.6, we know that the bigger the spectral gap, the better "the quality" of the expander.*

The quality of a family of expanders can be represented by a lower bound on the spectral gap from Corollary 2.6. But it also cannot be too large.

Theorem 2.8 ([2, Theorem 1.3.1])**.** *Let* $(G_m)_{m\geq 1}$ *be the same as Corollary 2.6. Then,*

$$\liminf_{m\to+\infty} \mu_1(G_m) \geq 2\sqrt{k - 1}.$$

Definition 2.9. *A finite connected k-regular graph G is a Ramanujan graph if* $|\mu| \leq 2\sqrt{k - 1}$ *for any nontrivial eigenvalue* μ *of G.*

Example 2.10. *The Petersen graph is an undirected graph with* 10 *vertices and* 15 *edges that is as shown in Figure 1. It is* 3*-regular and its spectrum is* $\{3, 1, 1, 1, 1, 1, -2, -2, -2, -2\}$. *It obviously satisfies the condition in Definition 2.9, so that it is a Ramanujan graph.*

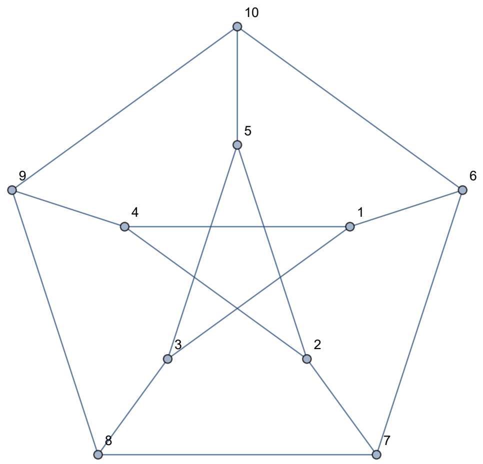

Figure 1: Petersen graph

3 Group-subgroup Pair Graphs

Definition 3.1 (Cf. [10])**.** *Let G be a group, H be a subgroup of G and S be a subset of G such that $S \cap H$ is a symmetric subset of H. Then the group-subgroup pair graph $\mathcal{G}(G, H, S)$ is defined as the undirected graph with vertices G and its edges*

$$\{(h, hs); h \in H, s \in S\}.$$

We use the short term "pair graph" instead of "group-subgroup pair graph".

We need some notations.

(i) For a group G, a subgroup H and a subset S of G, we denote

$$S_H := S \cap H,$$
$$S_O := S - H.$$

(ii) If H is a subgroup of index $k+1$ of G, we consider a set of representatives of the cosets $\{x_0 = e, x_1, ..., x_k\}$. Then, a partition of S_O is given by the sets

$$S_i := S \cap Hx_i, \quad i \in \{1, ..., k\}.$$

For a general pair graph, when the generating subset S is empty, it still satisfies the conditions of Definition 3.1. Then the resulting pair graph $\mathcal{G}(G, H, S)$ is trivial, i.e, it has no edge.

Example 3.2. *Let $G = \mathbb{Z}/12\mathbb{Z}$,$H = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, and $S = \{\bar{1}, \bar{2}, \bar{4}, \bar{8}\}$. The corresponding pair graph is drawn in Figure 2.*

Proposition 3.3. *The pair-graph $\mathcal{G}(G, H, S)$ contains no isolated vertices if and only if S contains a representative for each coset of H in G other than $He = H$.*

Proposition 3.4. *All the vertices in the same coset have the same degree in a pair graph $\mathcal{G}(G, H, S)$. The degree of vertices in H is $|S|$ and the degree of the vertices in the coset Hx other than H is $|S \cap Hx|$.*

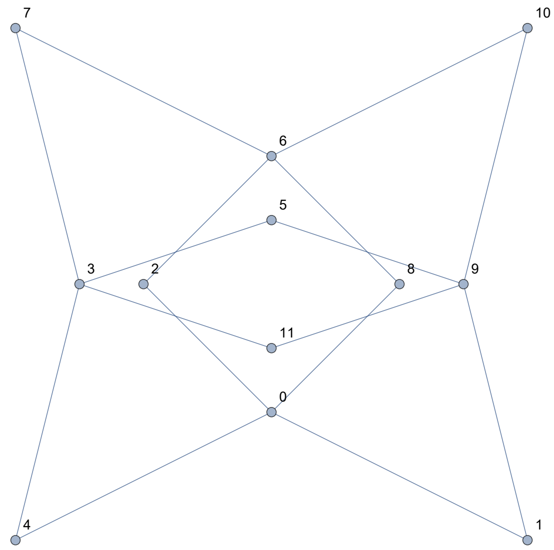

Figure 2: $\mathcal{G}(G, H, S)$

Corollary 3.5. *Let G be a group, H be a subgroup with index $[G:H] = k+1$, S be a subset of G such that S_H is symmetric. Then for $h \in H$, we have*

$$\deg(h) \geq \sum_{i=1}^{k} \deg(x_i).$$

When S_H is empty, the equality is satisfied. Particularly, a nontrivial pair graph is regular if and only if $S_H = \emptyset$ and $[G:H] = 2$, or $[G:H] = 1$.

Lemma 3.6. *Let G be a group, H be a subgroup and S be a subset of G with $S_H = \emptyset$. The vertices of H are in the same connected component of $\mathcal{G}(G, H, S)$ if and only if $\langle H \cap (SS^{-1}) \rangle = H$.*

Proposition 3.7. *Let G be a group, H be a subgroup and S be a subset of G with $S_H = \emptyset$. The necessary and sufficient conditions for a pair graph to be connected are:*

(*a*) $\langle H \cap (SS^{-1}) \rangle = H$,

(*b*) *S contains representatives of all the cosets of H other than H.*

We need to introduce a notation before the next theorem:

$$\widetilde{S_O} = \langle H \cap (S_O S_O^{-1}) \rangle.$$

Theorem 3.8 ([10, Theorem 4.5])**.** *A pair graph $\mathcal{G}(G, H, S)$ is bipartite if there exists a group homomorphism $\chi : H \to \{-1, 1\}$ such that $\chi(S_H) = \{-1\}$ and $\chi(\widetilde{S_O}) = \{1\}$. The converse holds when the pair graph is connected.*

Theorem 3.9 ([10, Corollary 6.4])**.** *A nontrivial connected k-regular pair graph $\mathcal{G}(G, H, S)$ with $|G| = 2n$ and $[G:H] = 2$ is a Ramanujan graph if*

$$k = |S| \geq n + 2 - 2\sqrt{n}.$$

4 Results

We choose the symmetric group S_n as G and the alternating group A_n for its subgroup as H of pair graph $\mathcal{G}(G,H,S)$. In this case, $[G:H]=2$, so if we take $S\subset G-H$, then by Corollary 3.5, $\mathcal{G}(G,H,S)$ is k-regular where $k=|S|$, and $\mathcal{G}(G,H,S)$ is bipartite since $\chi=1$ satisfies the condition in Theorem 3.8. We consider whether such a graph satisfies the conditions for being a Ramanujan graph.

Example 4.1 ([10, Example 6.5])**.** *Let $G=S_4, S=A_4$. Take*

$$S=\{(1,2),(1,3),(1,4),(2,4),(3,4),(1,3,2,4),(1,4,2,3),(1,4,3,2)\},$$

so that $|S|=8$ and it satisfies the bound of Theorem 3.9 (in this case, $n=12$), so the corresponding pair graph $\mathcal{G}(S_4,A_4,S)$ is a Ramanujan graph. Its spectrum is $\{\pm 8, \pm\sqrt{7}\times 2, \pm\sqrt{3}\times 6, 0\times 6\}$.

The 4-regular pair graph generated by $S'=\{(2,3),(1,2,3,4),(1,2,4,3),(1,3,4,2)\}$ is also a Ramanujan graph. Therefore, the result of Theorem 3.9 is not a necessary condition.

Let us consider the case $G=S_3, H=A_3$. From Theorem 3.9, we know $\mathcal{G}(S_3,A_3,S)$ is a Ramanujan graph if $|S|\geq 3+2-2\sqrt{3}\approx 1.54$. When $|S|\leq 1$, the pair graph is disconnected. So we have nothing to do any more.

We proceed to the case $n\geq 4$.

Proposition 4.2. *Let $n\geq 4, S\subset S_n-A_n$. If $|S|\leq 2$, the pair graph $\mathcal{G}(S_n,A_n,S)$ is disconnected.*

So we assume $|S|\geq 3$ in the following.

We consider the case $G=S_4, H=A_4$. From Theorem 3.9, we know that the pair graph $\mathcal{G}(S_4,A_4,S)$ is a Ramanujan graph if $|S|\geq 12+2-2\sqrt{12}\approx 7.07$. So we just need to investigate the cases where $3\leq|S|\leq 7$. Firstly, let $|S|=3$, the number of such subsets is 220. Among the corresponding pair graphs, 28 are disconnected and 192 are Ramanujan graphs. Secondly, let $|S|=4$, the number of such subsets is 495. Only in the 3 cases

$$\begin{aligned}
S&=\{(1,2),(3,4),(1,3,2,4),(1,4,2,3)\},\\
S&=\{(1,3),(2,4),(1,2,3,4),(1,4,3,2)\},\\
S&=\{(1,4),(2,3),(1,2,4,3),(1,3,4,2)\},
\end{aligned}$$

the corresponding pair graphs are disconnected. For each of these cases, we verified by computation that if we add an arbitrary element in $G-H-S$ to S, then the pair graph becomes a Ramanujan graph. In general, we suspect that if $\mathcal{G}(G,H,S)$ is a Ramanujan graph, then $\mathcal{G}(G,H,S')$ is also a Ramanujan graph for any $S'\supset S$. So we stop our computations in the case $G=S_4, H=A_4$.

Because of the increase of both the number of subsets S and vertices of the pair graph $\mathcal{G}(G,H,S)$ when $n\geq 5$, we must restrict ourselves to treat the cases where S is of certain form. Specifically, we assume that S consists of 2 cycles of length 4 and another *fixed cycle* $(1,2,...,n)$ (resp. $(1,2,...,n-1)$) when n is even (resp. odd). We give some examples when $5\leq n\leq 9$. Note that the corresponding pair graphs are 3-regular and $2\sqrt{3-1}=2.82842\ldots$. The numerical values of the second largest eigenvalues μ_1 are approximate values.

- $n=5,\ S=\{(1,3,2,5),(2,3,5,4),(1,2,3,4)\},\ \mu_1=2.73205.$
- $n=6,\ S=\{(1,4,3,6),(3,4,6,5),(1,2,3,4,5,6)\},\ \mu_1=2.72069.$
- $n=7,\ S=\{(1,7,3,2),(4,5,7,6),(1,2,3,4,5,6)\},\ \mu_1=2.80175.$

- $n = 8,\ S = \{(1,6,4,2),(5,6,8,7),(1,2,3,4,5,6,7,8)\},\ \mu_1 = 2.81106.$
- $n = 9,\ S = \{(1,5,2,9),(6,7,9,8),(1,2,3,4,5,6,7,8)\},\ \mu_1 = 2.82777.$

When $n = 10$, we could not find Ramanujan graphs according to the previous rules of S. Incidentally, we succeeded in finding 2 Ramanujan graphs when

$$S = \{(1,9,2,3),(6,7,9,8),(1,2,3,4,5,6,7,8,9,10)\},\ \mu_1 = 2.82838$$

and

$$S = \{(3,4,7,5),(6,7,9,8),(1,2,3,4,5,6,7,8,9,10)\},\ \mu_1 = 2.82633.$$

References

[1] Asherov, R.; Dinur, I. Bipartite Unique Neighbour Expanders via Ramanujan Graphs. Entropy 2024, 26, 348. `https://doi.org/10.3390/e26040348`

[2] G. P. Davidoff, P. C. Sarnak and A. J. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London Mathematical Society Student Texts, 55, Cambridge Univ. Press, Cambridge, 2003; MR1989434

[3] K. Eisenträger et al., Supersingular isogeny graphs and endomorphism rings: reductions and solutions, in *Advances in cryptology—EUROCRYPT 2018. Part III*, 329–368, Lecture Notes in Comput. Sci., 10822, Springer, Cham, ; MR3794837

[4] E. Lubetzky and A. Sly, Explicit expanders with cutoff phenomena, Electron. J. Probab. **16** (2011), no. 15, 419–435; MR2774096

[5] A. Lubotzky, R. S. Phillips and P. C. Sarnak, Ramanujan graphs, Combinatorica **8** (1988), no. 3, 261–277; MR0963118

[6] A. W. Marcus, D. A. Spielman and N. Srivastava, Interlacing families I: Bipartite Ramanujan graphs of all degrees, Ann. of Math. (2) **182** (2015), no. 1, 307–325; MR3374962

[7] G. A. Margulis, Problems Inform. Transmission **24** (1988), no. 1, 39–46; translated from Problemy Peredachi Informatsii **24** (1988), no. 1, 51–60; MR0939574

[8] M. Morgenstern, Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q, J. Combin. Theory Ser. B **62** (1994), no. 1, 44–62; MR1290630

[9] M. R. Murty, Ramanujan graphs, J. Ramanujan Math. Soc. **18** (2003), no. 1, 33–52; MR1966527

[10] C. Reyes-Bustos, Cayley-type graphs for group-subgroup pairs, Linear Algebra Appl. **488** (2016), 320–349; MR3419789

[11] A. A. Terras, *Zeta functions of graphs*, Cambridge Studies in Advanced Mathematics, 128, Cambridge Univ. Press, Cambridge, 2011; MR2768284