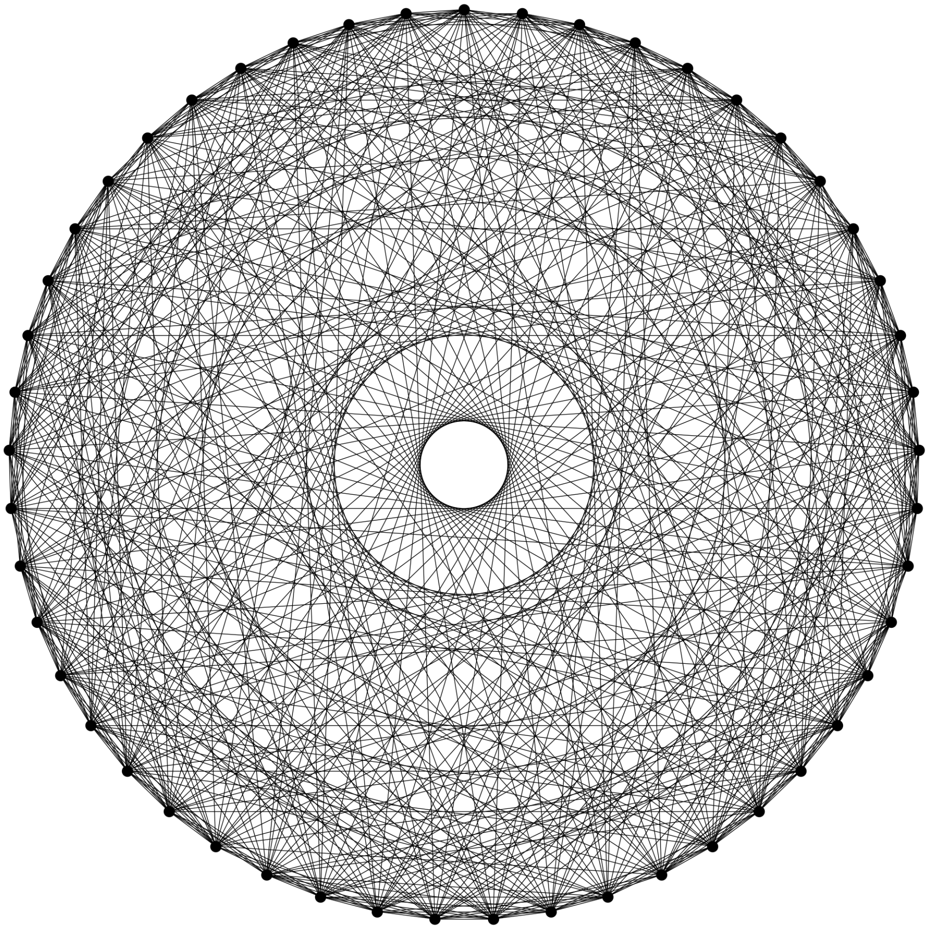
Infinite Families of Ramanujan Graphs

An Open Problem in Graph Theory

Shai Levin

October 2021

This report serves as a brief summary on an open problem in spectral graph theory. Namely, the existence of infinite families of non-bipartite d-regular Ramanujan graphs for each d. This problem has been solved for $d = q + 1$ for prime powers q, but remains open for other cases. We discuss the constructions used in the special cases, and modern approaches to solving the open problem using covering graphs.



The Paley graph of order 49, a Ramanujan graph.

Introduction

Ramanujan graphs arise from the field of *spectral* graph theory, the study of the properties of the matrices associated to a graph - such as the adjacency matrix. Ramanujan graphs are a nearly optimal case of something known as an *expander* graph, and satisfy a number of extremal combinatorial properties. In loose terms, graphs which have relatively few edges but remain 'strongly' connected. These graphs largely appear as algebraic constructions from number theory, algebraic geometry and representation theory. In this report, we shall discuss the existence of infinite families of Ramanujan graphs - an open problem in spectral graph theory - and what makes this problem important.

History and Applications

Ramanujan graphs were first named in a paper of Alexander Lubotzky [1] in 1988. In his paper, Lubotzky constructs families of Ramanujan graphs using the Ramanujan conjecture. This is a prized conjecture of Srinivasa Ramanujan, a prolific Indian mathematician of the early 20th century, known for his substantial contributions to analysis and number theory, despite his limited mathematical education. Lubotzky introduced the open problem of constructing Ramanujan graphs in his 1988 paper. Morgenstern, a student of Lubotzky, provided a construction of prime power families in 1993 [2].

Since the rise of computing, Ramanujan graphs have become an object of great interest. These graphs have a wide variety of application in error-correction codes, network reliability, and cryptography. We illustrate their expansion property like so: on a Ramanujan graph, take random walks of fixed length from a given vertex. The probability distribution measuring end vertices of the random walks will quickly converge to the uniform distribution on the vertex set. Guaranteeing short paths is desirable in designing communication networks, but in cryptographic applications, we are interested in a further implication of this property - while short paths exist, they are hard to find. The hardness of path finding on Ramanujan graphs is applicable to cryptographic hash functions. Schemes based on a particular Ramanujan graph exploit this [3]. While most research of these graphs come from the early 1990s, the current search for quantum computer resistant cryptographic protocols has enriched their study once more.

Isogeny based cryptography is one of the most promising candidates in post-quantum cryptography. These schemes are based on isogenies - the morphisms/maps between particular algebraic geometric structures known as elliptic curves. They can be described in graph theoretical terms by forming graphs with elliptic curves as vertices and isogenies between them as edges. Most variants rely on the hardness of the *isogeny path finding problem*. Loosely stated, that finding paths on a particular component of this graph is hard. This component is Ramanujan, as proven by Pizer in 1990 [4], and the hardness of this more algebraic problem is closely related to the hardness of path finding on Ramanujan graphs.

Background: Expanders and Ramanujan Graphs

We shall briefly go over the definitions and properties of these graphs, obtained from a survey of Hoory et al [5]. Expanders may be defined in a number of ways. We will define the expansion ratio, and then briefly the algebraic properties of expanders.

Let G be a graph. We refer to the vertex set of G as $V(G)$ and the edge set of G as $E(G)$. G is called d-regular if for all $v \in V(G)$, the degree of v is d.

Definition 1 (Expansion Ratio)**.** Let G be an undirected, d-regular graph. Let $S \subseteq V(G)$, then $\bar{S}$ is the set of vertices of G not in S, and $(S, \bar{S})$ is a partitioning of G. Let $E(S, \bar{S}) = \{(u, v) \in E(G) : u \in S, v \in \bar{S}\}$. That is, the edges of G between S and $\bar{S}$. We define the *expansion ratio* of G as

$$h(G) = \min_{\{S \subseteq V(G), |S| \leq \frac{|V(G)|}{2}\}} \frac{|E(S, \bar{S})|}{|S|}$$

All connected d-regular graphs are expanders. However, informally speaking, the best expander graphs are graphs with lowest possible vertex degree while maintaining a high expansion ratio. We shall see that Ramanujan graphs are such a graph. Typically the expansion ratio is considered over a family $\mathcal{G}_d$ of d-regular graphs, where for any $n \in \mathbb{Z}^+$, $G \in \mathcal{G}_d$ is a d-regular graph on n vertices. We fix d and see a bound for $h(G)$ for all $G \in \mathcal{G}_d$. In practice, as n gets large, $h(G)$ becomes hard to compute, so expanders are typically defined by way of graph spectrum.

Definition 2 (Graph Spectrum)**.** Let G be a graph on n vertices. We define $A = A(G)$ to be the *adjacency matrix* of G, an $n \times n$ matrix whose (u, v) entry is the number of edges between vertices u and v. Since A is symmetric, and real, it has n real eigenvalues, denoted as λ_i for $1 \leq i \leq n$ where

$$d \geq \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n \geq -d.$$

These eigenvalues are known as the *spectrum* of G, and are studied in spectral graph theory. For instance, here are some properties we can determine from the spectrum of a graph G [5, 2.3]:

- G is connected if and only if $\lambda_1 > \lambda_2$
- G is bipartite if and only if $\lambda_1 = -\lambda_n$
- If G is d-regular, then $\lambda_1 = d$.

Definition 3 (Expander Graph, Spectral Gap)**.** A connected, d-regular graph is an expander graph, with spectrum $\lambda_1 \geq ... \geq \lambda_n$. We define the *spectral gap* as $d - \lambda_2$. The spectral gap provides an estimation of the expansion ratio, because of the following bound [5, Thm. 2.4]:

$$\frac{1}{2}(d - \lambda_2) \leq h(G) \leq \sqrt{2d(d - \lambda_2)}$$

An important property of expander graphs is given below.

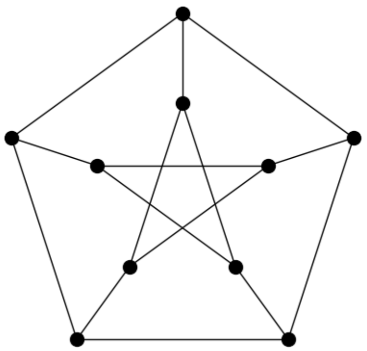


Figure 1: The Petersen graph, a Ramanujan graph.

Lemma 1 (Expander Mixing Lemma)**.** *Let G be a d-regular graph with n vertices. We define $\lambda(G)$ where*

$$\lambda(G) = max(|\lambda_2|, ..., |\lambda_n|).$$

That is, the absolute largest eigenvalue that is not $\lambda_1 = d$. then for all $S, T \subseteq V(G)$:

$$|E(S,T)| - \frac{d|S||T|}{n} \leq \lambda(G)\sqrt{|S||T|}$$

Proof. See [5, Lemma 2.5] □

The left hand side of this equation measures the deviation between two quantities: $|E(S,T)|$, the number of edges between the two vertex sets; and the expected number of edges between S and T in a random graph of edge density d/n. In layman's terms, this lemma implies the following:

- Edges of an expander graph are evenly distributed in the graph.
- The distribution of end vertices of random walks quickly converge to a uniform distribution. If a graph has n vertices, it converges in $O(\log n)$ steps. The rate of this convergence is known as the *mixing* property of a graph.

What makes this property interesting? Consider a naive protocol on a graph G, where Alice shares a (public) vertex v with her friend, Bob. She then constructs a random walk on G of a fixed length, starting at v. At each step, she picks an adjacent vertex with equal likelihood to add to her path. She stops once her walk reaches n edges, and keeps it secret. Now, suppose Bob wanted to guess the endpoint of the random walk. For each vertex u in G, the attacker calculates the probability of ending a walk at u. If this probability distribution is not uniform, he may pick the vertices of highest probability first. This, in practice, means Bob may need to make fewer guesses than if the distribution was uniform.

Note that the smaller our value of $\lambda(G)$, the better *mixing* properties G has. Stated below is a lower bound for $\lambda(G)$:

Theorem 1 (Alon-Boppana)**.** *A d-regular graph on n vertices satisfies:*

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

for $\epsilon > 0$ where $\epsilon \to 0$ as $n \to \infty$ for a fixed d.

There is a particular class of expander graph that exhibits a tight upper bound for $\lambda(G)$.

Definition 4 (Ramanujan Graph)**.** An d-regular expander graph is a *Ramanujan graph* if

$$\lambda(G) \leq 2\sqrt{d-1}.$$

This is almost the tightest possible bound for $\lambda(G)$ and as a consequence, Ramanujan graphs are essentially optimal expander graphs.

The Open Problem

Now that we have defined Ramanujan graphs, we shall state the open problem. Unfortunately it turns out that, in general, Ramanujan graphs are difficult to construct. Note that the problem excludes bipartite graphs, of which construction is straightforward, but of limited application. [6]

Open Problem 1. *There exists infinitely many non-bipartite d-regular Ramanujan graphs for $d \geq 3$.*

We are interested in finding families of these graphs, and as such, solutions to cases of this open problem have used constructive proofs. Suppose for any d, we knew an infinite family of Ramanujan graphs existed, then we could use such constructions to derive graphs that suit applications in, for instance, cryptography.

Now, the conjecture has been proved for some cases. In his foundational paper on Ramanujan graphs, Lubotzky used the Ramanujan conjecture to construct infinite families of $(p+1)$-regular Ramanujan graphs where p is prime [1]. Later, Morgenstern extended this result to prime powers, so the conjecture is proved when p is a prime power. Morgensterns construction is a remarkable example of using algebraic number theory to derive a result in the seemingly unrelated field of graph theory.

Proposition 1. *There exists an infinitely many $(q+1)$-regular Ramanujan graphs, for prime powers q.*

Proof. See [2, Thm. 5.13]. □

The problem remains open for non prime powers, in fact, it has yet to be proved for $d = 7$, the minimal example such that $d - 1$ is not a prime power. One might wonder what proportion of d-regular graphs of n vertices are Ramanujan. Friedman showed that, surprisingly, almost all d-regular graphs are Ramanujan. However, it is not what proportion are Ramanujan [7].

Proposition 2. *Given a d-regular graph G on n vertices, we have that*

$$\lambda(G) \leq 2\sqrt{d-1} + \epsilon,$$

for $\epsilon > 0$ where $\epsilon \to 0$ as $n \to \infty$.

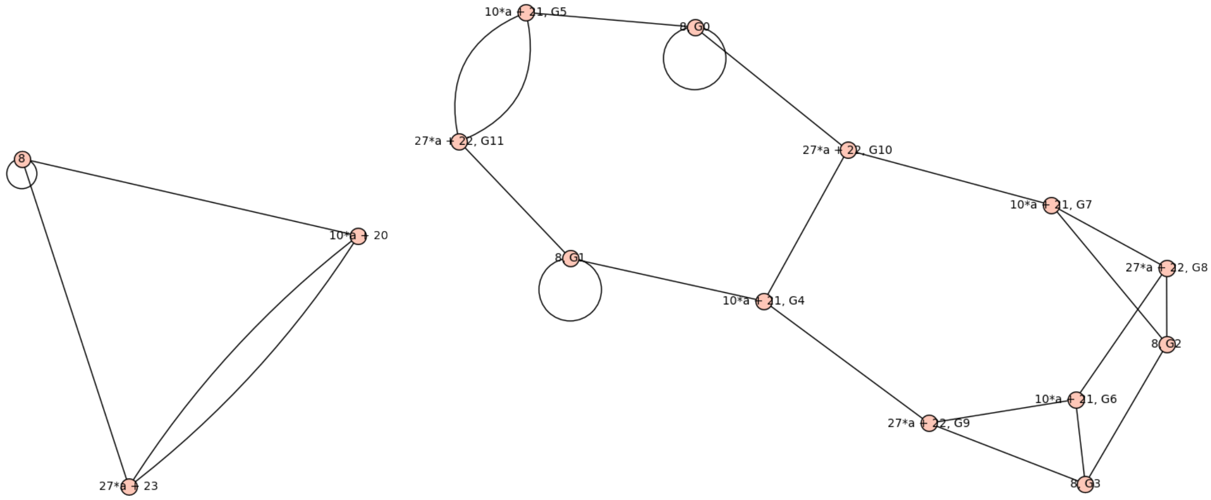


Figure 2: **Left:** the supersingular 2-isogeny graph on $\mathbb{F}_{37^2}$. **Right:** a corresponding covering graph, with a covering map is given by $f(j,k) = j$ for a vertex label (j,k).

Variations on the Open Problem

It is possible to construct infinite families of Ramanujan graphs using covering graphs. As such, some variation on the open problem exists - relating to the spectrum of the lift of a graph. Warning: there is no connection between covering graphs and vertex or edge coverings.

Definition 5. Let $G = (V_1, E_1), C = (V_2, E_2)$ be graphs. We say that C is a *covering graph*, or a *lift* of G is there exists a *covering map* from C to G. $f : V_2 \to V_1$ is a covering map from C to G if:

(i) f is surjective.

(ii) f is a *local isomorphism*. That is, for each $v \in V_2$, the edges of $f(v)$ in G are in one-to-one correspondence with the edges of v in C. Stated otherwise, the adjacent vertices of v in C and the adjacent vertices of $f(v)$ in G are in bijection.

We say that C is an *n-lift* of G if for all $v \in V_1$, $|f^{-1}(v)| = n$.

A lift of a d-regular graph will necessarily be d-regular. There has been some research into the properties of lifts of Ramanujan graphs by Bilu and Linial and (a similarly named) Lubetzky [8]. Lubetzsky showed that a typical n-lift of a Ramanujan graph is nearly Ramanujan. Now, if we could find a way to construct lifts of a Ramanujan graph that are also Ramanujan, we might have a good way to prove Open Problem 1. Bilu and Linial established the following conjecture in 2006 [9].

Open Problem 2. *Let G be a d-regular Ramanujan graph. For some $\ell > 1$, there exists a Ramanujan ℓ-lift of G. [5, Conjecture 6.8]*

This conjecture has been used for alternative constructions to the special cases of the open problem. For instance, the zig-zag product [10]. Solving this problem in the general case would provide a means to construct infinite families of Ramanujan graphs for any d. A similar method was exploited by Hall, Puder and Sawain to construct rich families of bipartite Ramanujan graphs [11]. Such a construction could indeed be a method to solve the open cases of Open Problem 1.

Curiously there is a way to construct lifts on the supersingular isogeny graph, the Ramanujan graph used in isogeny based cryptography [12][13]. These graphs are $q+1$-regular for a prime power q . It is conjectured these lifts are Ramanujan, and it could provide another alternative construction to Morgenstern's. There could also be a way to extend this construction to non-prime powers. See Figure 3 for this particular construction. Note that both graphs are Ramanujan.

Conclusion

Ramanujan graphs provide a good source of pseudo-randomness in computing due to their strong mixing property. They also act as a potential candidate for a cryptographic primitive, and are strongly related to the hard problem used in isogeny based cryptography. Becoming a subject of interest with the the search for post quantum cryptographic protocols, we may yet see progress on this open problem over the next decade. There are already contributions to finding these infinite families of Ramanujan graphs, with Lubotzky and Morgenstern proving the cases of prime powers, and later researches proving the conjecture for bipartite graphs of any regularity [6]. Constructions with covering graphs of Ramanujan graphs, such as the supersingular isogeny graph, could prove key to solving the remaining cases of this open problem.

References

[1] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," *Combinatorica*, vol. 8, no. 3, pp. 261–277, Sep. 1988. [Online]. Available: https://doi.org/10.1007/BF02126799

[2] M. Morgenstern, "Existence and Explicit Constructions of q + 1 Regular Ramanujan Graphs for Every Prime Power q," *Journal of Combinatorial Theory, Series B*, vol. 62, no. 1, pp. 44–62, Sep. 1994. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0095895684710549

[3] A. Costache, B. Feigon, K. Lauter, M. Massierer, and A. Puskás, "Ramanujan Graphs in Cryptography," in *Research Directions in Number Theory*, J. S. Balakrishnan, A. Folsom, M. Lalín, and M. Manes, Eds. Cham: Springer International Publishing, 2019, vol. 19, pp. 1–40, series Title: Association for Women in Mathematics Series. [Online]. Available: http://link.springer.com/10.1007/978-3-030-19478-9_1

[4] A. K. Pizer, "Ramanujan graphs and Hecke operators," *Bulletin of the American Mathematical Society*, vol. 23, no. 1, pp. 127–137, 1990. [Online]. Available: https://www.ams.org/bull/1990-23-01/S0273-0979-1990-15918-X/

[5] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications," *Bulletin of the American Mathematical Society*, vol. 43, no. 04, pp. 439–562, Aug. 2006. [Online]. Available: http://www.ams.org/journal-getitem?pii=S0273-0979-06-01126-8

[6] A. W. Marcus, N. Srivastava, and D. A. Spielman, "Interlacing Families IV: Bipartite Ramanujan Graphs of All Sizes," *arXiv:1505.08010 [math]*, May 2015, arXiv: 1505.08010. [Online]. Available: http://arxiv.org/abs/1505.08010

[7] J. Friedman, "A proof of Alon's second eigenvalue conjecture and related problems," *Memoirs of the American Mathematical Society*, vol. 195, no. 910, pp. 0–0, 2008. [Online]. Available: http://www.ams.org/memo/0910

[8] E. Lubetzky, B. Sudakov, and V. Vu, "Spectra of lifted Ramanujan graphs," *Advances in Mathematics*, vol. 227, no. 4, pp. 1612–1645, Jul. 2011. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0001870811001010

[9] Y. Bilu and N. Linial, "Lifts, Discrepancy and Nearly Optimal Spectral Gap*," *Combinatorica*, vol. 26, no. 5, pp. 495–519, Oct. 2006. [Online]. Available: http://link.springer.com/10.1007/s00493-006-0029-7

[10] O. Reingold, S. Vadhan, and A. Wigderson, "Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors," in *Proceedings 41st Annual Symposium on Foundations of Computer Science*, Nov. 2000, pp. 3–13, iSSN: 0272-5428.

[11] C. Hall, D. Puder, and W. F. Sawin, "Ramanujan Coverings of Graphs," *Advances in Mathematics*, vol. 323, pp. 367–410, Jan. 2018, arXiv: 1506.02335. [Online]. Available: http://arxiv.org/abs/1506.02335

[12] M. Roda, "Supersingular isogeny graphs with level N structure and path problems on ordinary isogeny graphs," 2019, publisher: McGill University.

[13] S. Levin, "Lifted elliptic curve isogeny graphs," 2021, honours thesis.