RIMS Kôkyûroku Bessatsu
B90 (2022), 153–167

Generalized LPS Ramanujan graphs

By

Hyungrok Jo*

Abstract

We show how to construct generalized LPS Ramanujan graphs (LPS-type graphs), and prove their Ramanujan-ness on the limited case. This work is originally based on "Ramanujan graphs for post-quantum cryptography" in the proceedings of MQC 2019.

This article is basically a résumé of "Ramanujan graphs for post-quantum cryptography" [22] by Jo, Sugiyama and Yamasaki in 2019, which proposed a generalized version of explicit constructions of Lubotzky, Phillips and Sarnak's Ramanujan graphs. Most of contents are contained in [22], and the proof of the Ramanujan-ness are fully discussed with Sugiyama and Yamasaki. This work is motivated from an analysis on cryptographic hash functions, suggested by Charles, Goren, and Lauter [2, 3]. They proposed hash functions based on Cayley-type Ramanujan graphs [25] and supersingular isogeny-type Ramanujan graphs [37, 32, 36, 3, 8]. Especially, in a case of Cayley-type Ramanujan graphs, Lubotzky, Phillips and Sarnak (in short, LPS) [25] suggested Cayley graphs over the projective group with respect to well-chosen generating sets. In our work, we showed how to construct LPS-type graphs and proved the Ramanujan-ness when "$P = 13$", which means the case of a definite quaternion algebra ramified precisely at 13 and ∞.

In this article, we give a more detailed proof of the case when "$P = 13$", and explore the other possibility of Ramanujan graphs in the manner of LPS and Chiu's construction. This article is organized as follows: The first section gives a brief overview of

Received December 31, 2020. Revised April 16, 2021.
2020 Mathematics Subject Classification(s): Primary 05C25; Secondary 11R52
Key Words: *Ramanujan graph, expander graph, LPS Ramanujan graph*
Supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University. This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan.

*Yokohama National University, Institute of Advanced Sciences, 79-5 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa, Japan.
e-mail: `jo-hyungrok-xz@ynu.ac.jp`

theory of expander graphs. The second section provides some preliminaries on quaternion algebras for describing our expecting graphs. In the third section the procedure to construct LPS-type graphs is presented and the Ramanujan-ness when "$P = 13$" is shown. In the final section we discuss difficulties to prove the other cases (when $P = 2, 3, 5, 7$) and some open problems on these extensions with numerical results.

§ 1. A family of expander

An expander graph has been widely studied in many kinds of research areas. Especially, in computer science, because of its sparsity and strong connectivity, it is well used for designing communication networks. The quality of networks on expander graphs can be measured by their expanding ratios [43, 17].

Throughout this article, we assume that all graphs are k-regular, finite, undirected, simple (i.e., no loops nor multi-edges) and connected. Suppose that $X = (V, E)$ is a k-regular graph, composed of a vertex set $V = V(X)$ with n vertices and an edge set $E = E(X)$. For a subset T of V, the *boundary* ∂T of T is defined as

$$\partial T = \{(x, y) \in E \mid x \in T \text{ and } y \in V \setminus T\},$$

where $V \setminus T$ is the complement of T in V. The *expanding constant* $h(X)$ of X, which is defined as below, is a discrete analogue of the *Cheeger constant* in differential geometry [26]:

$$h(X) = \min_{\substack{T \subset V \\ 0 < |T| \leq n/2}} \frac{|\partial T|}{|T|}.$$

We give the definition of *expander graphs*.

Definition 1.1. A family of k-regular graphs $(X_j)_{j \geq 1}$ such that $|V(X_j)| \to +\infty$ as $j \to +\infty$ is called an *expander family* if there is an $\epsilon > 0$ such that the expanding constant $h(X_j)$ satisfies $h(X_j) \geq \epsilon$ for all j.

For exploring the algebraic aspects of graphs, the *adjacency matrix* A of a graph X plays an important role; it is a square matrix indexed by pairs of vertices u, v whose (u, v)-entry $A_{u,v}$ is the number of edges between u and v. Since we assume that X has n vertices, A is an n-by-n symmetric $(0, 1)$-matrix without diagonal entries (i.e., $A_{u,u} = 0$). For such a graph X, the adjacency matrix A of X has the spectrum $k = \lambda_0 > \lambda_1 \geq \cdots \geq \lambda_{n-1}$. It is known [1, 12] that

$$\frac{k - \lambda_1}{2} \leq h(X) \leq \sqrt{2k(k - \lambda_1)}.$$

If the spectral gap $k - \lambda_1$ is larger, the quality of the network of X is getting better as well. However, it is shown by Alon-Boppana as follows that it cannot be too large.

Theorem 1.2. *Let $(X_j)_{j\geq 1}$ be a family of k-regular graphs with $|V(X_j)| \to +\infty$ as $j \to +\infty$. Then*

$$\liminf_{j\to+\infty} \lambda_1(X_j) \geq 2\sqrt{k-1}.$$

This fact motivates the definition of a *Ramanujan graph.*

Definition 1.3. A k-regular graph X is *Ramanujan* if, for every member λ of the spectrum of the adjacency matrix of X other than $\pm k$, one has $|\lambda| \leq 2\sqrt{k-1}$. We call $2\sqrt{k-1}$ the *Ramanujan bound* (RB).

For a more detailed exposition of the theory, refer to [7, 26, 43]. In the literature, there are a few explicit constructions of infinite families of Ramanujan graphs:

(1) When $k-1$ is a prime congruent to 1 modulo 4, Lubotzky, Phillips, and Sarnak [25] and Margulis [28] derived explicit constructions of infinite families of Ramanujan graphs independently.

(2) When $k = 3$, Chiu [4] derived explicit constructions of cubic Ramanujan graphs in 1992.

(3) When $k - 1$ is a prime power, Morgenstern [33] derived explicit constructions of infinite families of Ramanujan graphs in 1994.

(4) Pizer [37] derived explicit constructions of Ramanujan graphs by using Brandt matrix associated to a special order of a certain level, which can be seen as the adjacency matrix of an expecting graph in 1990.

From (1) to (4), the explicit construction turns out to be a consequence of the Ramanujan conjecture for eigenvalues of certain Hecke operators. Refer to [26, 40] for kind explications of theory. Moreover, in 2015, Marcus, Spielman, and Srivastava [29] showed the existence of an infinite family of bipartite k-regular Ramanujan graphs for any $k \geq 3$.

§ 2. Preliminaries

In this section, we prepare terminologies and basic facts of quaternion algebras [44] and quadratic forms [41]. Throughout this article, we denote by $\mathbb{P}$ the set of all prime numbers. Let F be a field and $F^\times$ its unit group. Let $\mathcal{A} = \mathcal{A}_F$ be a *quaternion algebra* over F, i.e., a central simple algebra of dimension 4 over F. In this article, we always assume that F is not of characteristic 2. Then, there exist $a, b \in F^\times$ such that it can be written as

$$\mathcal{A} = \mathcal{A}_F(a,b) = \{\alpha = x + yi + zj + wk \,|\, x, y, z, w \in F\},$$

where i, j, k satisfy $i^2 = a$, $j^2 = b$ and $ij = -ji = k$ (and hence $k^2 = -ab$). For $\alpha = x + yi + zj + wk \in \mathcal{A}$, its *conjugate*, the *reduced trace* and the *reduced norm* are defined by $\overline{\alpha} = x - yi - zj - wk$, $T(\alpha) = \alpha + \overline{\alpha} = 2x \in F$ and $N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = x^2 - ay^2 - bz^2 + abw^2 \in F$, respectively.

§ 2.1. Quaternion algebras over $\mathbb{F}_q$

Let us fix $q \in \mathbb{P} \setminus \{2\}$. It is known that, for any $a, b \in \mathbb{F}_q^\times$, the quaternion algebra $\mathcal{A} = \mathcal{A}_{\mathbb{F}_q}(a, b)$ is isomorphic to the matrix algebra $\mathrm{M}_2(\mathbb{F}_q)$ of the 2-by-2 matrices over $\mathbb{F}_q$. Let $\left(\frac{\cdot}{\cdot}\right)$ be the Kronecker symbol. When $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$, that is, $\sqrt{a}, \sqrt{-b} \in \mathbb{F}_q$, one has the following isomorphism.

Lemma 2.1. *Assume that* $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$. *Then, the map* $\psi_q : \mathcal{A} \to \mathrm{M}_2(\mathbb{F}_q)$ *defined by*

$$\psi_q(x + yi + zj + wk) = \begin{bmatrix} x + y\sqrt{a} & \sqrt{-b}(z + w\sqrt{a}) \\ -\sqrt{-b}(z - w\sqrt{a}) & x - y\sqrt{a} \end{bmatrix}$$

is an isomorphism satisfying $\det(\psi_q(\alpha)) = N(\alpha)$ *and* $\psi_q(\overline{\alpha}) = \overline{\psi_q(\alpha)}$ *for* $\alpha \in \mathcal{A}$. *Here,* $\overline{\begin{bmatrix} s & t \\ u & v \end{bmatrix}} = \begin{bmatrix} v & -t \\ -u & s \end{bmatrix}$ *for* $\begin{bmatrix} s & t \\ u & v \end{bmatrix} \in \mathrm{M}_2(\mathbb{F}_q)$.

For a ring R, we denote by $R^\times$ the group of units of R. Let $\mathrm{GL}_2(\mathbb{F}_q) = \mathrm{M}_2(\mathbb{F}_q)^\times$ and $\mathrm{SL}_2(\mathbb{F}_q) = \{A \in \mathrm{GL}_2(\mathbb{F}_q) \mid \det A = 1\}$. Moreover, let $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/Z(\mathrm{GL}_2(\mathbb{F}_q))$ and $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/Z(\mathrm{SL}_2(\mathbb{F}_q))$. Here, for a group G, we denote by $Z(G)$ the *center* of G. We can naturally see that $\mathrm{PSL}_2(\mathbb{F}_q)$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ of index 2 because now q is odd. Remark that $|\mathrm{PGL}_2(\mathbb{F}_q)| = q(q^2 - 1)$ and $|\mathrm{PSL}_2(\mathbb{F}_q)| = \frac{q(q^2-1)}{2}$. Since $\mathcal{A} \simeq \mathrm{M}_2(\mathbb{F}_q)$, we have $\mathcal{A}^\times \simeq \mathrm{GL}_2(\mathbb{F}_q)$ via (the restriction of) ψ_q and hence obtain the isomorphism $\beta_q : \mathcal{A}^\times/Z(\mathcal{A}^\times) \to \mathrm{PGL}_2(\mathbb{F}_q)$.

We need the following lemma later.

Lemma 2.2 (Davidoff et al. [7, Chapter 3]). *Assume that* $\left(\frac{a}{q}\right) = \left(\frac{-b}{q}\right) = 1$. *Let* $\alpha \in \mathcal{A}$ *with* $N(\alpha) = p \in \mathbb{P}\setminus\{q\}$, *which implies that* $\alpha \in \mathcal{A}^\times$. *Then,* $\beta_q(\alpha\mathbb{F}_q^\times) \in \mathrm{PSL}_2(\mathbb{F}_q)$ *if and only if* $\left(\frac{p}{q}\right) = 1$.

§ 2.2. Quaternion algebras over $\mathbb{Q}$

Let $a, b \in \mathbb{Z}\setminus\{0\}$ and $\mathcal{A} = \mathcal{A}_{\mathbb{Q}}(a, b)$ be a quaternion algebra over $\mathbb{Q}$. A place v of $\mathbb{Q}$ is said to be *split* in $\mathcal{A}$ if $\mathcal{A}_v := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_v \simeq \mathrm{M}_2(\mathbb{Q}_v)$, where $\mathbb{Q}_v$ is the v-adic completion of $\mathbb{Q}$ and is said to be *ramified* if $\mathcal{A}_v$ is a division algebra. We denote by $\mathrm{Ram}(\mathcal{A})$ the set of all places which are ramified in $\mathcal{A}$. Notice that $\mathrm{Ram}(\mathcal{A})$ is a finite set, has an even cardinality, and determines an isomorphism class of quaternion algebras over $\mathbb{Q}$. The product of all primes (= finite places) in $\mathrm{Ram}(\mathcal{A})$ is called the *discriminant* of $\mathcal{A}$ and is denoted by $\mathfrak{D}$. From now on, we assume that $\mathcal{A}$ is definite, that is, the infinite place ∞ is ramified in $\mathcal{A}$, whence there are an odd number of primes which are ramified in $\mathcal{A}$. Notice that $\mathcal{A} = \mathcal{A}_{\mathbb{Q}}(a, b)$ is definite if and only if $a < 0$ and $b < 0$.

A *lattice* $\mathcal{I} \subset \mathcal{A}$ is a free $\mathbb{Z}$-submodule of $\mathcal{A}$ of rank 4. A lattice $\mathcal{O} \subset \mathcal{A}$ is called an *order* if it is a ring with unity. In particular, it is called *maximal* if it is not properly contained in any other order. Notice that, if $\mathcal{O}$ is an order of $\mathcal{A}$, then $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is an order of $\mathcal{A}_p$ for $p \in \mathbb{P}$. Here, $\mathbb{Z}_p$ is the ring of p-adic integers. Let $\mathcal{O}$ be an order of $\mathcal{A}$. We call a lattice $\mathcal{I}$ of $\mathcal{A}$ a *left* (resp. *right*) *$\mathcal{O}$-ideal* if $\mathcal{O}_L(\mathcal{I}) = \mathcal{O}$ (resp. $\mathcal{O}_R(\mathcal{I}) = \mathcal{O}$), where $\mathcal{O}_L(\mathcal{I}) = \{\alpha \in \mathcal{A} \,|\, \alpha\mathcal{I} \subset \mathcal{I}\}$ (resp. $\mathcal{O}_R(\mathcal{I}) = \{\alpha \in \mathcal{A} \,|\, \mathcal{I}\alpha \subset \mathcal{I}\}$). We say that two left (resp. right) $\mathcal{O}$-ideals $\mathcal{I}$ and $\mathcal{J}$ are equivalent if there exists $\alpha \in \mathcal{A}^{\times}$ such that $\mathcal{I} = \mathcal{J}\alpha$ (resp. $\mathcal{I} = \alpha\mathcal{J}$). This is an equivalence relation. We denote by $H(\mathcal{O})$ the number of equivalence classes of left (or right) $\mathcal{O}$-ideals, which is shown to be finite, independent of left or right. We call $H(\mathcal{O})$ the *class number* of $\mathcal{O}$. We remark that the class number is finite and independent of orders $\mathcal{O}$.

§ 2.3. Quadratic form

We briefly recall the notion and terminologies of quadratic forms in a special case (see [41]). Let m be a positive integer. A symmetric matrix $A = [a_{ij}] \in \mathrm{M}_{2m}(\mathbb{Z})$ is called *even* if every diagonal entry a_{ii} is even for every $1 \leq i \leq 2m$. With such a matrix, we associate the quadratic form

$$Q(\mathbf{v}) = \frac{1}{2}{}^t\mathbf{v}A\mathbf{v} = \frac{1}{2}\sum_{i=1}^{2m} a_{ii}x_i^2 + \sum_{1\leq i<j\leq 2m} a_{ij}x_ix_j,$$

where $\mathbf{v} = {}^t[x_1, \ldots, x_{2m}]$. We call Q and A *primitive* when the greatest common divisor of all entries of A is 1. We assume that the quadratic form Q is primitive. Let $\det A$ be the determinant of A; one calls $\Delta := (-1)^m \det A$ the *discriminant* of Q. If A_{ij} is the cofactor of a_{ij} in A, then $A^{-1} = \bigl(\frac{A_{ij}}{\det A}\bigr)$. The *level* of Q is defined as the smallest positive integer N such that $NA^{-1} = \frac{N}{\det A}(A_{ij})$ is an even matrix.

For a positive definite quadratic form Q of level N, define the theta series by

$$\Theta_Q(z) = \sum_{\mathbf{v}\in\mathbb{Z}^{2m}} e^{2\pi i Q(\mathbf{v})z} = \sum_{n=0}^{\infty} r_Q(n)e^{2\pi i n z},$$

where, for $n \in \mathbb{Z}_{\geq 0}$, $r_Q(n) = |\{\mathbf{v} \in \mathbb{Z}^{2m} \mid n = Q(\mathbf{v})\}|$. From [41, Chapter IX, Theorems 4, 5], we know that $\Theta_Q(z)$ is a non-cuspidal holomorphic modular form of weight m and of level N with nebentypus χ. Namely, for all $\begin{bmatrix} a\,b \\ c\,d \end{bmatrix} \in \Gamma_0(N) =$

$\left\{ \begin{bmatrix} a\, b \\ c\, d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod N \right\}$, it holds that

$$\Theta_Q\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^m \Theta_Q(z),$$

where χ is a character modulo N defined by $\chi(d) = (\frac{(-1)^m \det A}{d})$ if $d > 0$ and $\chi(d) = (-1)^m \chi(-d)$ if $d < 0$. We also know that $\Theta_Q(z)$ is absolutely and locally uniformly convergent for $z \in \mathbb{C}$ with $\mathrm{Im}(z) > 0$, by [41, Chapter IX, §1.1].

§ 3. The families of LPS-type graphs

We used a variation of Chiu's approach [4]. Since the Hamilton's quaternion algebra $\mathcal{A}_{\mathbb{Q}}(-1,-1)$ is not split at 2, LPS construction is invalid for the prime 2. Thus, Chiu chose the maximal order of $\mathcal{A}_{\mathbb{Q}}(-13,-2)$ which is definite and with class number 1. Successfully, Chiu constructed a cubic Ramanujan graphs (i.e., 3-regular graphs).

First, since our graph is also constructed as a Cayley graph, we give the definition of Cayley graphs. Let G be a group and S a generating set, which is symmetric (i.e. $S = S^{-1}$) and does not contain the identity of G. A *Cayley graph* over G with respect to S is a $|S|$-regular graph with a vertex set V and an edge set E, where $V = G$ and E consists of $(g_1, g_2) \in G \times G$ such that $g_1 = g_2 s$ for some $s \in S$.

Theorem 3.1 (Eichler [14]). *Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{Q}$ and h the class number of $\mathcal{A}$. Then, we have*

$$h = \frac{1}{12}\prod_{\substack{P\in\mathbb{P}\\ P|\mathfrak{D}}}(P-1) + \frac{1}{4}\prod_{\substack{P\in\mathbb{P}\\ P|\mathfrak{D}}}\left(1-\left(\frac{-4}{P}\right)\right) + \frac{1}{3}\prod_{\substack{P\in\mathbb{P}\\ P|\mathfrak{D}}}\left(1-\left(\frac{-3}{P}\right)\right),$$

where $\mathfrak{D}$ is the discriminant of $\mathcal{A}$.

From **Theorem 3.1**, we know the fact that $h = 1 \iff \mathfrak{D} = 2, 3, 5, 7, 13$. Now we recall a useful tool to refine the p-norm set.

Theorem 3.2 (Eichler [15]). *Let $\mathcal{A}$ be a definite quaternion algebra over $\mathbb{Q}$ of class number 1 and $p \in \mathbb{P}$ such that $\mathcal{A}$ is unramified at p. Then, for any maximal order $\mathcal{O}$ of $\mathcal{A}$ and $k \in \mathbb{N}$, we have*

$$|\{\alpha \in \mathcal{O} \mid N(\alpha) = p^k\}/\mathcal{O}^\times| = p^k + p^{k-1} + \cdots + p + 1.$$

By Ibukiyama's construction [19], it gives an explicit way to construct maximal orders of definite quaternion algebras over $\mathbb{Q}$ ramified at given primes.

Proposition 3.3 (Ibukiyama [19]). *Let r be an odd positive integer and $P_1, P_2, \dots, P_r$ distinct prime numbers. Set $M = P_1 P_2 \cdots P_r$. Take a prime number Q such that $Q \equiv 3 \pmod 8$ and $(\frac{-Q}{P_i}) = -1$ for all i except for i with $P_i = 2$. Moreover, take an integer T such that $T^2 \equiv -M \pmod Q$. Then, $\mathcal{A}_{\mathbb{Q}}(-M,-Q)$ is a definite quaternion algebra which is ramified only at $\infty, P_1, P_2, \dots, P_r$. Moreover, let*

$$\omega_1 = \frac{1+j}{2}, \quad \omega_2 = \frac{i+k}{2} \quad \textit{and} \quad \omega_3 = \frac{Tj+k}{Q}.$$

Then, $\mathcal{O}_{-M,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ is a maximal order of $\mathcal{A}_{\mathbb{Q}}(-M,-Q)$.

From **Theorem 3.2** and **Proposition 3.3**, we find a refined p-norm set in a maximal order in a definite quaternion algebra of class number 1. The main procedure will be shown as described in [22, Section 3].

1. We fix a $p \in \mathbb{P}$ and take $P \in \{2, 3, 5, 7, 13\}$ such that P is not equal to p.
2. Using Proposition 3.3, we take a prime Q satisfying
$$Q \equiv 3 \pmod 8, \left(\frac{-Q}{P}\right) = -1 \text{ unless } P = 2$$
and an integer T satisfying $T^2 \equiv -P \pmod Q$. Then we have a definite quaternion algebra $\mathcal{A}_{\mathbb{Q}}(-P,-Q)$ (i.e., $i^2 = -P, j^2 = -Q, ij = -ji = k$) and its maximal order $\mathcal{O} = \mathcal{O}_{-P,-Q} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ with class number 1, where
$$\omega_1 = \frac{1+j}{2}, \ \omega_2 = \frac{i+k}{2} \text{ and } \omega_3 = \frac{Tj+k}{Q}.$$
3. Using Theorem 3.2, we find a suitable complete representative of $\{\alpha \in \mathcal{O} \mid N(\alpha) = p\}/\mathcal{O}^\times$ where $\mathcal{O}^\times = \{\alpha \in \mathcal{O} \mid N(\alpha) = 1\}$.
4. Define S by the suitable complete representative. Then $|S|$ is exactly equal to $p+1$, which follows by the class number 1 condition [4, Proposition 3.4].
5. Take a $q \in \mathbb{P} \setminus \{2\}$ satisfying q is not equal to p and $\left(\frac{-P}{q}\right) = \left(\frac{Q}{q}\right) = \left(\frac{p}{q}\right) = 1$.
6. Via the isomorphism ψ_q in Lemma 2.1 and using Lemma 2.2, we realize S as a subset of $\mathrm{PSL}_2(\mathbb{F}_q)$. Write S for the subset.
7. We construct a Cayley graph $X_{P,Q}^{(p,q)} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S)$.

§ 3.1. The Ramanujan-ness of graphs $X_{P,Q}^{(p,q)}$ when $P = 13$

In this subsection, we recall that our constructed graph, say $X_{P,Q}^{(p,q)}$, is Ramanujan when $P = 13$ in [22, Section 3.1]. Let $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3$ be the maximal order we constructed as our recipe for a fixed p, P, Q, T. Then, $\mathcal{O}$ has the class number 1. We take a complete representative

$$S = \{\alpha_1, \ldots, \alpha_s\} \cup \{\bar{\alpha}_1, \ldots, \bar{\alpha}_s\} \cup \{\beta_1, \ldots, \beta_t\}$$

of $\{\alpha \in \mathcal{O} \mid N(\alpha) = p\}/\mathcal{O}^\times$ so that $\bar{\beta}_j = \epsilon_j \beta_j$ for some $\epsilon_j \in \mathcal{O}^\times$ for every j. In this case, $p+1 = 2s+t$. In the same way as [5, Theorem 4.8] and [25, Lemma 3.1], we have the following:

Lemma 3.4. *Any $\alpha \in \mathcal{O}$ with $N(\alpha) = p^k$ for some $k \in \mathbb{N}$ is uniquely decomposed into the product*

$$\alpha = \epsilon p^r R(\alpha_1, \ldots, \alpha_s, \bar{\alpha}_1, \ldots, \bar{\alpha}_s, \beta_1, \ldots, \beta_t),$$

where $\epsilon \in \mathcal{O}^\times$, $r \in \mathbb{N}$ and $R(\alpha_1, \ldots, \alpha_s, \bar{\alpha}_1, \ldots, \bar{\alpha}_s, \beta_1, \ldots, \beta_t)$ is a reduced word of $\alpha_1, \ldots, \alpha_s, \bar{\alpha}_1, \ldots, \bar{\alpha}_s, \beta_1, \ldots, \beta_t$ with length $m = k - 2r$.

Proof. The proof is given by induction on k, following [5, Theorem 4.8]. The cases $k = 0, 1$ are clear. For any $k \geq 2$, we assume the assertion for any k' such that $k' \leq k-1$. Let α be an element of $\mathcal{O}$ with $N(\alpha) = p^k$. By the class number 1 condition, we have $\beta \in \mathcal{O}$ such that $\mathcal{O}\alpha + \mathcal{O}p = \mathcal{O}\beta$. As there is $q \in \mathcal{O}$ such that $p = q\beta$, $N(\beta)$ divides p^2, which leads us $N(\beta) = 1, p, p^2$.

When $N(\beta) = 1$, β is a unit. Then, take $x, y \in \mathcal{O}$ satisfying $x\alpha + yp = \beta$. By taking the reduced norm and mod p reduction, $N(x)N(\alpha) \equiv 1 \pmod{p}$, which contradicts to the fact that p divides $N(\alpha)$.

When $N(\beta) = p$, there are $j \in \{1, \ldots, s\}$ and $\epsilon \in \mathcal{O}^\times$ such that $\beta = \epsilon\alpha_j$. Since we can take $\gamma \in \mathcal{O}$ such that $\alpha = \gamma\beta$ and $N(\gamma\epsilon) = p^{k-1}$, we have a factorization of α.

When $N(\beta) = p^2$, q must be a unit because of $p^2 = N(q)p^2$. As we see $\mathcal{O}\alpha + \mathcal{O}p = \mathcal{O}\beta$, α is divisible by p. By $N(p^{-1}\alpha) = p^{k-2}$, we have a factorization. From the consideration above, we are done.

We assume $\mathcal{O}$ is maximal. Then, the number of representations of decompositions of α is given by

$$\#\mathcal{O}^\times \{ \sum_{0 \leq r < k/2} (p+1)p^{k-2r-1} + \delta(k)\} = \#\mathcal{O}^\times \times \frac{p^{k+1}-1}{p-1},$$

where $\delta(k) = 1$ if k is even, and 0 otherwise. It is exactly equal to the number of solutions $\alpha \in \mathcal{O}$ of $N(\alpha) = p^k$. □

The unit group $\mathcal{O}^\times$ is $\{\pm 1\}$ only when $P = 13$. In that case, we can prove the Ramanujan property of our graph $X_{P,Q}^{(p,q)}$ in the same way as [25]. For the variable

$v = (x, y, z, w)$, we set

$$\begin{aligned} Q_q(v) =& x^2 + qxy + q^2\left(\frac{1+Q}{4}\right)y^2 + q^2Tyz \\ &+ q^2P\left(\frac{1+Q}{4}\right)z^2 + q^2Pzw + q^2\left(\frac{P+T^2}{Q}\right)w^2. \end{aligned}$$

It is a positive definite quadratic form of order 4 corresponding to the reduced norm on $\mathcal{O}$. Let A_q be the symmetric matrix such that $Q_q(v) = \frac{1}{2}{}^t vA_qv$, i.e.,

$$A_q = \begin{bmatrix} 2 & q & 0 & 0 \\ q & \frac{q^2(1+Q)}{2} & 0 & q^2T \\ 0 & 0 & \frac{q^2P(1+Q)}{2} & q^2P \\ 0 & q^2T & q^2P & 2q^2\frac{P+T^2}{Q} \end{bmatrix}.$$

Hence, A_q is an even matrix, i.e., $A_q \in \mathrm{M}_4(\mathbb{Z})$ and every diagonal component is contained in $2\mathbb{Z}$.

Lemma 3.5. *The level N of Q_q is equal to Pq^2.*

Proof. For the sake of simplicity, write A for A_q. A direct computation yields $D(A) = P^2q^6$ and

$$\gcd(A_{ij}, \frac{1}{2}A_{ii})_{1\le i,j\le 4} = Pq^4,$$

where A_{ij} is the (i, j)-cofactor of A. Hence we have the assertion by [41, Chapter IX, Theorem 1]. We give the expression of A^{-1}:

$$A^{-1} = \frac{1}{P^2q^6}\begin{bmatrix} q^6\frac{1+Q}{2}P(\frac{P+T^2}{Q}) & -q^5P\left(\frac{P+T^2}{Q}+T^2\right) & -q^5PT & q^5PT\frac{1+Q}{2} \\ -q^5P\left(\frac{P+T^2}{Q}+T^2\right) & 2q^4P(\frac{P+T^2}{Q}+T^2) & 2q^4PT & -q^4PT(1+Q) \\ -q^5PT & 2q^4PT & 2q^4P & -PQq^4 \\ q^5PT\frac{1+Q}{2} & -q^4PT(1+Q) & -PQq^4 & q^4PQ\frac{(1+Q)}{2} \end{bmatrix}.$$

□

Set $r_{Q_q}(n) := |\{\alpha \in \mathcal{O} \mid N(\alpha) = n\}/\mathcal{O}^\times|$ for $n \in \mathbb{N}$. Then, the theta series is given by

$$\Theta_{Q_q}(z) := \sum_{n=0}^{\infty} r_{Q_q}(n)e^{2\pi inz} = \sum_{v\in\mathbb{Z}^4} e^{2\pi iQ_q(v)z}$$

for $z \in \mathbb{C}$ with $\mathrm{Im}(z) > 0$.

Proposition 3.6. *The theta series $\Theta_{Q_q}(z)$ is a holomorphic modular form of weight 2 on $\Gamma_0(Pq^2)$ with trivial nebentypus.*

Proof. By [41, Chapter IX, Theorem 4], Θ_{Q_q} is a holomorphic modular form of weight 2 on $\Gamma(Pq^2)$. Furthermore, by [41, Chapter IX, Theorem 5] for $\mathbf{h} = \mathbf{0}$, the function Θ_{Q_q} satisfies the relation

$$\Theta_{Q_q}(\gamma z) = \chi(d)(cz+d)^2\Theta_{Q_q}(z), \qquad \forall\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(Pq^2),$$

where χ is the even Dirichlet character modulo N determined by the Jacobi symbol: $\chi(d) = (\frac{P^2q^6}{d})$. As our χ is the trivial character, we are done. □

Recall $P = 13$. Let Λ' be the set of all $\alpha \in \mathcal{O}$ such that $N(\alpha) = p^k$ for some $k \in \mathbb{N}$. We define an equivalence relation on Λ so that $\alpha \sim \beta$ means $\alpha = \epsilon p^n \beta$ for some $\epsilon \in \mathcal{O}^\times$ and $n \in \mathbb{Z}$. Since $\mathcal{O}^\times = \{\pm 1\}$ holds, the quotient set

$$\Lambda := \Lambda'/\sim\, = \{[\alpha] \mid \alpha \in \Lambda'\} \tag{3.1}$$

has a natural group structure by $[\alpha][\beta] = [\alpha\beta]$. By Lemma 3.4, it is generated by S, a complete representative of $\{\alpha \in \mathcal{O} \mid N(\alpha) = p\}/\mathcal{O}^\times$, and $\mathrm{Cay}(\Lambda, S)$ is a $(p+1)$-regular tree. The homomorphism $\Lambda \to \mathrm{PSL}_2(\mathbb{F}_q)$ as a restriction of ψ_q of Lemma 2.1 induces $\Lambda/\Lambda(q) \to \mathrm{PSL}_2(\mathbb{F}_q)$ with $\Lambda(q) = \ker(\psi_q|_\Lambda)$. This homomorphism $\Lambda/\Lambda(q) \to \mathrm{PSL}_2(\mathbb{F}_q)$ is surjective as in theory of quadratic diophantine equations applied to the quadratic form Q_q (cf. [25, p.267], [27]). Then $X_{13,Q}^{(p,q)} = \mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), S)$ is identified with $\Lambda/\Lambda(q)$ as a graph.

Let $\lambda_0 = p+1 > \lambda_1 \geq \cdots \geq \lambda_{n-1}$ be the spectrum of the adjacency matrix of $X_{13,Q}^{(p,q)}$. Here, $n = |X_{13,Q}^{(p,q)}| = |\mathrm{PSL}_2(\mathbb{F}_q)| = \frac{q(q^2-1)}{2}$. Then, for proving Ramanujan-ness, we have only to show $\theta_j \in \mathbb{R}$ for all $j \in \{1, \ldots, n-1\}$, where $\theta_j \in \mathbb{C}$ is taken so that $\lambda_j = 2\sqrt{p}\cos\theta_j$ for each $j \in \{0, \ldots, n-1\}$. By the trace formula for a regular graph as in [25, p.270–272 and p.274, Remark 2], we have the expression

$$r_{Q_q}(p^k) = \frac{2p^{k/2}}{n}\sum_{j=0}^{n-1}\frac{\sin(k+1)\theta_j}{\sin\theta_j}.$$

Recall that this is the p^kth Fourier coefficient of the modular form Θ_{Q_q}. Since the theta series is a sum of a linear combination of cuspidal Hecke eigenforms and that of Eisenstein series of weight 2 and level $\Gamma_0(Pq^2)$, We may take the cuspidal modular form f_1 and the non-cuspidal modular form f_2 so that $\Theta_{Q_q} = f_1 + f_2$. Let $a(m)$ and $C(m)$ be the mth Fourier coefficients of f_1 and of f_2 at the cusp ∞ for $m \in \mathbb{N}$, respectively. Then, $r_{Q_q}(p^k)$ has the following expression:

$$C(p^k) + a(p^k) = r_{Q_q}(p^k) = \frac{2p^{k/2}}{n}\sum_{j=0}^{n-1}\frac{\sin(k+1)\theta_j}{\sin\theta_j}.$$

By Deligne's bound as a resolution of the Ramanujan-Petersson conjecture ([9, 10]), we have $|a(p^k)| = O_\epsilon(p^{k(1/2+\epsilon)})$. By properties of Fourier coefficients of Eisenstein series,

$C(m)$ can be described as $C(m) = \sum_{d|m} F(d)$ for a periodic function $F : \mathbb{N} \to \mathbb{C}$ (cf. [25, p.272]). By $(\frac{p}{q}) = 1$ and $\theta_0 = i \log \sqrt{p}$, we have

$$C(p^k) = \frac{2}{n}\frac{p^{k+1}-1}{p-1} - a(p^k) + o(p^k) = \frac{2}{n}\frac{p^{k+1}-1}{p-1} + o(p^k).$$

By the Deligne bound of $a(p^k)$ and [25, Lemma 4.4], we have $C(p^k) = \frac{2}{n}\frac{p^{k+1}-1}{p-1}$ because of $(\frac{p}{q}) = 1$. As a consequence, for any $\epsilon > 0$,

$$\frac{2}{n}\sum_{j=1}^{n-1}\frac{\sin(k+1)\theta_j}{\sin\theta_j} = \frac{1}{p^{k/2}}O_\epsilon(p^{k(1/2+\epsilon)}) = O_\epsilon(p^{k\epsilon}),$$

which leads us that every θ_j for $j = 1, \ldots, n-1$ is real. Therefore, we obtain $|\lambda_j| \leq 2\sqrt{p}$ for all $j = 1, \ldots, n-1$, which proves the Ramanujan-ness of $X_{13,Q}^{(p,q)}$.

§ 4. Numerical results and open problems

In Table 1, we present some numerical results which show the Ramanujan-ness of our graphs. Indeed, we showed in the previous section that our LPS-type graphs are Ramanujan when $P = 13$, which is the only choice of $P \in \{2, 3, 5, 7, 13\}$ such that $\mathcal{O}^\times$ is equal to $\{\pm 1\}$. Unfortunately, for the cases of $P \in \{2, 3, 5, 7\}$, we are unable to prove or disprove the Ramanujan-ness of our graphs. The main reason why the existing procedure is not applied happens in (3.1). For the cases of $P \in \{2, 3, 5, 7\}$, elements of the unit group does not commute with other elements of $\mathcal{O}$.

Table 1: Numerical results on the Ramanujan-ness of LPS-type graphs $X = X_{P,Q}^{(p,q)}$

p	Parameters (P, Q, q, T)	$\lambda_1(X)$	$2\sqrt{p}$ (RB)	$\lvert V(X)\rvert$
2	$(13, 11, 7, 3)$	2.7253	2.8284	168
3	$(2, 3, 11, 1)$	3.3322	3.4641	660
5	$(2, 3, 11, 1)$	4.4718	4.4721	660
7	$(5, 67, 3, 14)$	3	5.2915	12
11	$(13, 11, 7, 3)$	6	6.6332	660

* It is implemented by Magma and MATLAB.

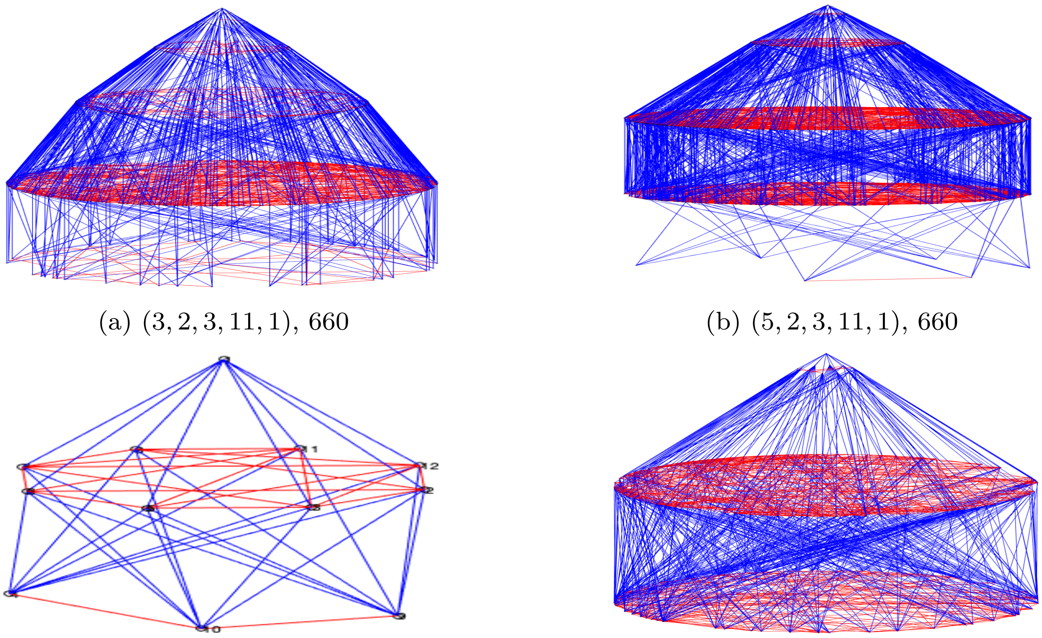
As depicted in the Table 2, we know the group corresponding to each case. For the case $p = 2$, the unit group $\mathcal{O}_{-2,-Q}^\times$ is the binary tetrahedral group, which can be written as the semidirect product $Q \rtimes \mathrm{C}_3$ where Q is the quaternion group consisting of the 8 Lipschitz units and C_3 is the cyclic group of order 3. They used a Lipschitz quaternion order with the unit group Q instead of a Hurwitz quaternion order with

Table 2: The unit group of maximal order $\mathcal{O}_{-P,-Q}$ when $P \in \{2,3,5,7\}$

$\mathcal{O}^{\times}_{-2,-Q}$	E_{24}	Binary tetrahedral group ([double cover of A_4] $\simeq Q \rtimes \mathrm{C}_3$)
$\mathcal{O}^{\times}_{-3,-Q}$	$\mathrm{C}_3 \rtimes \mathrm{C}_4$	Binary dihedral group
$\mathcal{O}^{\times}_{-5,-Q}$	C_6	Cyclic group
$\mathcal{O}^{\times}_{-7,-Q}$	C_4	Cyclic group

Here, Q is the quaternion group of 8 Lipschitz units, i.e., $\{1, \pm i, \pm j, \pm k\}$.

the unit group E_{24} when they constructed a natural group as in (3.1). It guarantees the unique factorization as in **Lemma 3.4**. However, we still do not know how to circumvent the non-commutativity of units and other elements and define the quotient set as in (3.1) which forms a natural group structure.


(a) $(3,2,3,11,1)$, 660

(b) $(5,2,3,11,1)$, 660

(c) $(7,5,67,3,14)$, 12

(d) $(13,5,67,3,14)$, 168

Figure 1: Parameters (p,P,Q,q,T) and $|V(X)|$

Figure 1 presents the visualizations of toy-examples in Table 1. Figures (a), (b), (c), (d) represent the cases when $p = 3, 5, 7, 13$, respectively. The blue line stands for the spanning tree of the graph and the red line stands for the links between vertices within the same tier. (These figures are provided from Vladimir Pelekhaty (Ciera Co.) by MATLAB.)

One of potential way to circumvent is to consider theory of elliptic curves. For example, it is known that every supersingular elliptic curve over an algebraically closed field of characteristic p has a model defined over $\mathbb{F}_{p^2}$ under the Deuring correspondence

Table 3: The order of Aut(E)

# Aut(E)	$j(E)$	char(F)
2	$j(E) \neq 0, 1728$	-
4	$j(E) = 1728$	char$(F) \neq 2, 3$
6	$j(E) = 0$	char$(F) \neq 2, 3$
12	$j(E) = 0 = 1728$	char$(F) = 3$
24	$j(E) = 0 = 1728$	char$(F) = 2$

Here, $j(E)$ is the j-invariant of an elliptic curve E over a field F.

[11]. The set of isomorphism classes of supersingular elliptic curves is one-to-one correspondence with the set of ideal classes of a maximal order of the definite quaternion algebra which is ramified precisely at p and ∞. In §10, Chapter 3 [42], the automorphism group of an elliptic curve is a finite group of order dividing 24. More precisely, we describe it in Table 3. From this, we can check that the cardinality of the automorphism group of an elliptic curve and that of the unit group of a maximal order is identical. It seems better to check the relationships and backgrounds between the unit group of our maximal order and the automorphism group of a certain elliptic curve.

Besides, as argued in §26, Chapter 6 [38], for an order of class number 1, we can obtain a factorization theorem for elements, rather than ideals. It gives us to prove that every positive rational integer is expressible as a sum of four squares with some coefficients. In a sense of it, it is necessary to consider the integral solutions of norm equations of maximal orders as a sum of four squares with some coefficients.

Acknowledgement

The author would like to thank Shingo Sugiyama and Yoshinori Yamasaki for their careful reading and pointing out mistakes and inaccuracies. This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University. This research was in part conducted under a contract of “Research and development on new generation cryptography for secure wireless communication services” among “Research and Development for Expansion of Radio Wave Resources(JPJ000254)”, which was supported by the Ministry of Internal Affairs and Communications, Japan.

References

[1] Alon, N., Milman, V., λ_1, isoperimetric inequalities for graphs, and superconcentrators. J. Comb. Theory. B., **38(1)**, 73–88 (1985)

[2] Charles, D. X., Goren, E. Z., Lauter, K. E., Cryptographic hash functions from expander graphs. J. Cryptology. **22(1)**, 93–113 (2009)

[3] Charles, D. X., Goren, E. Z., Lauter, K. E., Families of Ramanujan graphs and quaternion algebras. Groups and symmetries, **47**, CRM Proc. Lecture Notes, Amer. Math. Soc., Providence, RI, 53–80 (2009).

[4] Chiu, P., Cubic Ramanujan graphs. Combinatorica **12(3)**, 275–285 (1992)

[5] Coan, B., Perng, C., Factorization of Hurwitz quaternions, Int. Math. Forum, **7**, (2012), no. 41–44, 2143–2156.

[6] Costache, A., Feigon, B., Lauter, K. E., Massierer, M., Puskás, A., Ramanujan graphs in cryptography. arXiv preprint arXiv:1806.05709 (2018).

[7] Davidoff, G., Sarnak, P., Valette, A., Elementary Number Theory, Group Theory and Ramanujan Graphs. Cambridge University Press (2003).

[8] Déchène, I., Quaternion algebras and the graph method for elliptic curves, Master's Thesis, *Department of Mathematics and Statistics, McGill University, Montreal*, (1998).

[9] Deligne, P., Formes modulaires et représentations l-adiques, Séminaire N. Bourbaki, (1968–1969), exp. n°, 139–172.

[10] Deligne, P., La conjecture de Weil. I, Inst. Hautes Études Sci. Publ. Math., **43**, (1974), 273–307.

[11] Deuring, M., Die typen der multiplikatorenringe elliptischer funktionenkörper, In Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, **14(1)**, Springer-Verlag, (1941), 197–272.

[12] Dodziuk, J., Difference equations, isoperimetric inequality and transience of certain random walks. T. Am. Math. Soc., **284(2)**, (1984), 787–794.

[13] Eichler, M., Zur Zahlentheorie der Quaternionen-Algebren, J. Reine Angew. Math., **195**, (1955), 127–151.

[14] Eichler, M., The basis problem for modular forms and the traces of the Hecke operators. In: Willem Kuyk (eds.) Modular Functions of One Variable, **320**, Springer, Heidelberg, (1973), 75–152.

[15] Eichler, M., Sundaravaradan, S., Lectures on modular correspondences. Tata Institute of Fundamental Research (1956) Available via DIALOG. `http://www.math.tifr.res.in/~publ/ln/tifr09.pdf`

[16] Hirschhorn, M., A simple proof of Jacobi's four-square theorem. P. Am. Math. Soc., **101(3)**, (1987), 436–438.

[17] Hoory, H., Linial, N., Wigderson, A., Expander graphs and their applications. B. Am. Math. Soc., **43(4)**, (2006), 439–561.

[18] Ibukiyama, T., A basis and maximal orders of quaternion algebras over the rational number (In Japanese) , *MSJ, Sugaku*, **24(4)**, (1972), 316–318. `https://core.ac.uk/download/pdf/38181256.pdf`

[19] Ibukiyama, T., On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings. Nagoya. Math. J., **88**, (1982), 181–195.

[20] Ihara, Y., Discrete Subgroups of $\mathrm{PL}(2, \mathfrak{k}_{\mathfrak{p}})$. In Proc. Symp. Pure Math., (1966), 272–278.

[21] Jo, H., Yamasaki, Y., LPS-type Ramanujan graphs. In 2018 International Symposium on Information Theory and Its Applications, ISITA 2018, (2018), 399–403.

[22] Jo, H., Sugiyama, S., Yamasaki, Y., Ramanujan Graphs for Post-Quantum Cryptography, International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry, **33**. Springer, Singapore, (2020), 231–250.

[23] Jo, H., Sugiyama, S., Yamasaki, Y., A general explicit construction of LPS-type Ramanu-

jan graphs, in preparation.

[24] Kirschmer, M., Voight, J., Algorithmic enumeration of ideal classes for quaternion orders. SIAM Journal on Computing, **39(5)**, (2010), 1714–1747.

[25] Lubotzky, A., Phillips, R., Sarnak, P., Ramanujan graphs. Combinatorica **8(3)**, (1988), 261–277.

[26] Lubotzky, A., Discrete groups, expanding graphs and invariant measures. Springer Science Business Media. (1994).

[27] Malishev, A. I., On the representation of integers by positive definite forms (in Russian), Trudy Mat. Inst. Steklov. **65**, (1962), 1–319.

[28] Margulis, G., Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. Probl. Peredachi. Inf., **24(1)**, (1988), 51–60.

[29] Marcus, A. W., Spielman, D. A., Srivastava, N., Interlacing families II: Mixed characteristic polynomials and the Kadison—Singer problem. Ann. of Math. (2015), 327–350.

[30] Meier, J., Groups, graphs and trees; an introduction to the geometry of infinite groups. Cambridge University Press, (2008).

[31] Mestre, J. F., La méthode des graphes. Exemples et applications. In Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata), (1986), 217–242.

[32] Mestre, J. F., Jorza, T. A., The Method of Graphs. Examples and Applications. Notes. (2011).

[33] Morgenstern, M., Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q. Journal of Combinatorial Theory, Series B, **62(1)**, 44–62 (1994)

[34] Pizer, A. K., Type numbers of Eichler orders. J. reine angew. Math., **264**, (1973), 76–102.

[35] Pizer, A. K., On the arithmetic of quaternion algebras. Acta Arithmetica, **31**, (1976), 61–89.

[36] Pizer, A. K., Ramanujan graphs and Hecke operators. B. Am. Math. Soc., **23(1)**, (1990), 127–137.

[37] Pizer, A. K., Ramanujan graphs. AMS/IP Studies in Advanced Mathematics, **7**, (1998), 159–178.

[38] Reiner, I., Maximal orders, London Mathematical Society Monographs New Series, **28**, (1975).

[39] Rosson, H. J., Ellison, B. J., Wilson, J. B., Trees, Hecke operators, and quadratic forms, preprint.
`https://www.math.colostate.edu/~jwilson/math/PrePrintTree.pdf`

[40] Sarnak, P., Some Applications of Modular Forms. Cambridge University Press (1999).

[41] Schoeneberg, B, Elliptic Modular Functions: An Introduction, Springer-Verlag, **203**, (2012).

[42] Silverman, J. H., The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, **106**, Springer-Verlag, (1986).

[43] Terras, A., Zeta functions of graphs; a stroll through the garden, **128**, Cambridge University Press, (2010).

[44] Vignéras, M. F., Arithmétique des algèbres de quaternions, Lecture Notes in Math., **800**, Springer, Berlin, (1980).