Generalized Group–Subgroup Pair Graphs

Kazufumi Kimoto

Abstract A regular finite graph is called a Ramanujan graph if its zeta function satisfies an analog of the Riemann Hypothesis. Such a graph has a small second eigenvalue so that it is used to construct cryptographic hash functions. Typically, explicit family of Ramanujan graphs are constructed by using Cayley graphs. In the paper, we introduce a generalization of Cayley graphs called generalized group–subgroup pair graphs, which are a generalization of group–subgroup pair graphs defined by Reyes-Bustos. We study basic properties, especially spectra of them.

Keywords Cayley graphs · Spectra of graphs · Group–subgroup pair graphs · Group actions · Homogeneity · Representation theory · Characters

1 Introduction

A k -regular finite graph is called a *Ramanujan graph* if its zeta function satisfies an analog of the *Riemann hypothesis*. This condition is equivalent to say that every nontrivial (i.e. $\neq \pm k$) eigenvalue of the graph is less than or equal to $2\sqrt{k} - 1$. Thus the second largest eigenvalue in absolute value of a Ramanujan graph is small, and this means that it has a large isoperimetric constant (i.e. it is an *expander graph*), so that random walks on such a graph rapidly converge to the uniform distribution as the number of walk steps tends to infinity. Consequently, as an application to cryptography, Ramanujan graphs can be used to construct cryptographic hash functions (see Charles et al. (2009), in which hash functions are constructed from LPS graphs Lubotzky et al. (1988) and Pizer graphs (1990)).

In order to construct (a family of) Ramanujan graphs, the *Cayley graphs* are an important tool; a Cayley graph is a graph whose vertex set is a finite group, and the adjacency of vertices is described in terms of the multiplication of the group. In fact,

K. Kimoto (✉)

Department of Mathematical Sciences, Faculty of Science,
University of the Ryukyus, 1 Senbaru Nishihara, cho Okinawa 903-0213, Japan
e-mail: kimoto@math.u-ryukyu.ac.jp

© The Author(s) 2021

T. Takagi et al. (eds.), *International Symposium on Mathematics, Quantum Theory, and Cryptography*, Mathematics for Industry 33,
https://doi.org/10.1007/978-981-15-5191-8_14

169

most of the known explicit constructions of infinite families of Ramanujan graphs are given as Cayley graphs, and the construction is based on deep results in number theory associated with the group (for instance, the construction of the LPS graphs due to Lubotzky et al. (1988) is based on the Ramanujan–Petersson conjecture on automorphic forms).

Thus it is natural to consider the generalization of Cayley graphs to enlarge the possibility to produce Ramanujan graphs and/or expander families. *Group–subgroup pair graphs* (or pair graph for short) Reyes-Bustos (2016), which are defined for a triplet (G, H, S) of a finite group G , a subgroup $H \subset G$ and a suitable subset $S \subset G$, are one of such attempts. A pair graph is regular in special cases and provides interesting examples of Ramanujan graphs. However, we can construct regular pair graphs only when $[G : H] \leq 2$. The purpose of this paper is to give a generalization of group–subgroup pair graphs, which can provide Ramanujan graph even when $[G : H] > 2$. A generalized pair graph is a graph defined for a pair (G, H) of a group and its subgroup together with a suitable family $\mathcal{S}$ of subsets in G . We study basic properties, especially spectra of them.

Here is the brief description on the organization of the paper: In Sect. 2, we recall basic conventions on graphs. In Sect. 3, we recall the definitions of Cayley graphs and group–subgroup pair graphs, and give several examples of them. In Sect. 4, we introduce the notion of homogeneity of a graph. In Sect. 5, we give a generalization of group–subgroup pair graphs. In Sect. 6, we describe the spectra of generalized group–subgroup pair graphs.

1.1 Conventions

For a matrix A , A^* is the transposed complex conjugate of A , and $\text{Tr}(A)$ is the trace of A . The n by n identity matrix is denoted by I_n .

For a group G , we use the symbol e to indicate the identity element of G . We denote by χ^ρ the *character* of a given representation ρ of G : $\chi^\rho(x) = \text{Tr}(\rho(x))$ for $x \in G$. The *unitary dual* of G (i.e. the set of all equivalence classes of unitary irreducible representations of G) is denoted by $\widehat{G}$. The *dual group* of G is defined to be $G^* = \text{Hom}(G, \mathbb{C}^\times)$. We often identify G^* with the subset

$$\{\pi \in \widehat{G} \mid \deg \pi = 1\} \subset \widehat{G}$$

consisting of 1-dimensional representations of G via the bijection $\pi \mapsto \chi^\pi$. When G is abelian, we have $G^* = \widehat{G}$. We denote by $\mathbf{1}$ the trivial character of G (i.e. $\mathbf{1}(x) = 1$, $x \in G$).

2 Preliminaries

In what follows, a graph is always assumed to be *finite*, *undirected* and *simple* otherwise stated.

Let $X = (V, E)$ be a graph. The number of vertices $|V|$ and edges $|E|$ are called the *order* and *size* of the graph, respectively. We often write $x \sim y$ to indicate that two vertices x and y are adjacent, i.e. $xy \in E$. We denote by $\mathcal{N}(x)$ the *neighborhood* of x : $\mathcal{N}(x) = \{y \in V \mid x \sim y\}$. The *degree* $\deg(x)$ of a vertex x is the number of edges incident to x . If X is simple, then $\deg(x)$ is equal to $|\mathcal{N}(x)|$.

We call X a k -*regular* graph if $\deg(x) = k$ for every $x \in V$. We introduce two generalizations of this notion for later use. Suppose that V has a partition $V = V_1 \sqcup \dots \sqcup V_m$.

(1) If the degree is constant on each subset V_i , say d_i , then we call X a $(d_1, \dots, d_m)$ -*regular* graph.

(2) If

$$d_{ij} := |\{y \in V_j \mid x \sim y\}| \quad (x \in V_i)$$

depends only on i and j , then we say X is a D -*regular* graph, where $D = (d_{ij})_{1 \leq i, j \leq m}$. Notice that if

$$\sum_{i=1}^m d_{ir} = \sum_{j=1}^m d_{rj} =: d_r \quad (r = 1, \dots, m),$$

then X is $(d_1, \dots, d_m)$ -regular ($\deg(x) = d_i$ for any $x \in V_i$).

Numbering the vertices, say $V = \{v_1, \dots, v_N\}$ ($N = |V|$), we define the *adjacency matrix* $\mathcal{A} = \mathcal{A}_X$ of X by

$$\mathcal{A} = (a_{ij})_{1 \leq i, j \leq N}, \quad a_{ij} = \begin{cases} 1 & v_i \sim v_j, \\ 0 & \text{otherwise.} \end{cases}$$

$\mathcal{A}$ depends on the choice of numbering of V , however, it is uniquely determined up to conjugation by permutation matrices. An eigenvalue of $\mathcal{A}$ is called an eigenvalue of the graph X . We denote by $\text{Spec}(X)$ the multiset consisting of eigenvalues of X . If X is k -regular, then k is the largest eigenvalue of X , and every eigenvalue of X lies in the interval $[-k, k]$. We put

$$\lambda(X) := \max \{|\lambda| \mid \lambda \in \text{Spec}(X), \lambda \neq \pm k\}.$$

X is called a *Ramanujan graph* if

$$\lambda(X) \leq 2\sqrt{k-1}.$$

Remark 1 This condition $\lambda(X) \leq 2\sqrt{k-1}$ is equivalent to the analog of the Riemann hypothesis

$$\zeta_X(q^{-s})^{-1} = 0 \quad (q = k-1) \implies \operatorname{Re}(s) = \frac{1}{2}$$

for the Ihara zeta function

$$\zeta_X(u) = \prod_{[P]} (1 - u^{v(P)})^{-1}$$

of X , where $[P]$ runs over all the “primes” in X , and $v(P)$ is the “length” of P . See, for example, Terras (2011) for detail.

Remark 2 It is known that the second largest eigenvalue λ_1 of X satisfies

$$\lambda_1 > 2\sqrt{k-1} - \frac{2\sqrt{k-1}-1}{m}$$

when $\operatorname{diam}(X) \geq 2m+2 \geq 4$, where $\operatorname{diam}(X)$ denotes the diameter of X Nilli (1991).

Remark 3 The notion of Ramanujan graphs is extended to non-regular graphs in several cases. For instance, a (p, q) -regular bipartite graph X is called *Ramanujan bigraph* if

$$\left| \sqrt{p-1} - \sqrt{q-1} \right| \leq \lambda(X) \leq \sqrt{p-1} + \sqrt{q-1}.$$

See, for example, Feng and Li (1996), Hashimoto (1989).

Example 1 The cycle graph C_n of order n is a 2-regular graph, and its eigenvalues are given by $2 \cos \frac{2j\pi}{n}$ ($j = 0, 1, \dots, n-1$), which are all less than or equal to $2 = 2\sqrt{2-1}$. Hence C_n is Ramanujan for any $n \geq 3$.

3 Cayley Graphs and Group–Subgroup Pair Graphs

We briefly recall the basics of the Cayley graphs and group–subgroup pair graphs. We refer to Fulton and Harris (1991) for basic facts on representation theory.

3.1 Cayley Graphs

Definition 1 Let G be a group and $S \subset G$ be a symmetric generating set, that is, $S^{-1} = S$ and $\langle S \rangle = G$. The *Cayley graph* $\operatorname{Cay}(G, S)$ is a graph whose vertex set is G and two vertices $x, y \in G$ are adjacent if and only if $y = xs$ for some $s \in S$.

Let $\mathcal{R}$ be the *left regular representation* of G , which is the permutation representation induced from the left translation. Explicitly, if we index the elements in G as $G = \{g_1, \dots, g_N\}$ ($N = |G|$), then $\mathcal{R}(g)$ ($g \in G$) can be realized as a matrix whose (i, j) -entry is $\delta(g_i^{-1}gg_j)$, where $\delta(x)$ is 1 if $x = e$ and 0 otherwise. Then the adjacency matrix $\mathcal{A}$ of $\text{Cay}(G, S)$ is given by

$$\mathcal{A} = \sum_{s \in S} \mathcal{R}(s).$$

Since the irreducible decomposition of $\mathcal{R}$ is given by

$$\mathcal{R} \sim \bigoplus_{\pi \in \widehat{G}} \pi^{\oplus \deg \pi},$$

there exists a certain unitary matrix U such that

$$U^* \mathcal{R}(g) U = \bigoplus_{\pi \in \widehat{G}} \pi(g)^{\oplus \deg \pi}.$$

It follows that

$$U^* \mathcal{A} U = \bigoplus_{\pi \in \widehat{G}} \left(\sum_{s \in S} \pi(s) \right)^{\oplus \deg \pi},$$

and hence the characteristic polynomial of the adjacency matrix $\mathcal{A}$ is written as

$$\det(x I_N - \mathcal{A}) = \prod_{\pi \in \widehat{G}} \det \left(x I_{\deg \pi} - \sum_{s \in S} \pi(s) \right)^{\deg \pi}.$$

When G is abelian, every irreducible representation of G is 1-dimensional and we have

$$\text{Spec}(\text{Cay}(G, S)) = \left\{ \sum_{s \in S} \varphi(s) \mid \varphi \in G^* \right\}.$$

Example 2 Let $G = D_n = \langle s, t \rangle$ be the dihedral group of degree $2n$ ($s^n = t^2 = e$, $tst = s^{-1}$). Take a symmetric generating subset $S = \{s, s^{-1}, t\}$. Then the Cayley graph $\text{Cay}(G, S)$ is a 3-regular graph which is isomorphic to the Cartesian product of the path graph P_1 of length 1 and the cycle graph C_n of length n (Fig. 1). The following are the pictures of $\text{Cay}(G, S)$ for $n = 5, 6, 7, 8$:

The eigenvalues of $\text{Cay}(G, S)$ are given by

$$2 \cos \frac{2j\pi}{n} \pm 1 \quad (j = 0, 1, \dots, n-1).$$

We see that $\text{Cay}(G, S)$ is no longer Ramanujan if $2 \cos \frac{2\pi}{n} + 1 > 2\sqrt{2}$ or $n \geq 16$.

Fig. 1 $\text{Cay}(D_n, S)$ for $n = 5, 6, 7, 8$

3.2 Group–Subgroup Pair Graphs

Definition 2 (Reyes-Bustos (2016)) Let G be a group, H a subgroup of G and $S \subset G$ such that $S_0 = S \cap H$ is symmetric (i.e. $S_0^{-1} = S_0$). The *group–subgroup pair graph* (or *pair graph* for short) $\mathcal{G}(G, H, S)$ is a graph whose vertex set is G and two vertices $x, y \in G$ are adjacent if and only if there exist $h \in H$ and $s \in S$ such that $\{x, y\} = \{h, hs\}$.

Remark 4 If $G = H = \langle S \rangle$, then $\mathcal{G}(G, G, S) = \text{Cay}(G, S)$. If $[G : H] = 2$ and $S_0 = \emptyset$, then $\mathcal{G}(G, H, S)$ is bipartite.

Example 3 If $H = \{e\}$ and $S = G \setminus \{e\}$, then $\mathcal{G}(G, H, S)$ is the *star graph* $K_{1,k}$ (with $|G| = k + 1$). For instance, the pair graph for $G = \mathbb{Z}_8 = \mathbb{Z}/8\mathbb{Z}$, $H = \{0\}$ and $S = \mathbb{Z}_8 \setminus \{0\}$ is

Here we summarize several elementary facts on pair graphs (see Reyes-Bustos (2016) for the proof). Assume that H is a subgroup of G with index $k + 1$ and order n . Put $N = |G| = (k + 1)n$ for short. Fix a set $\{x_0 = e, x_1, x_2, \dots, x_k\}$ of representatives of the right cosets in G modulo H :

$$G = \bigsqcup_{i=0}^k V_i, \quad V_i := Hx_i,$$

and put $S_i = Hx_i \cap S$. We also put $d_i = |S_i|$ and $d = |S|$. We denote by $\mathcal{A}$ the adjacency matrix for $\mathcal{G}(G, H, S)$, and by λ_i ($i = 0, 1, \dots, N - 1$) the eigenvalues of $\mathcal{G}(G, H, S)$ which are ordered in decreasing order: $\lambda_0 \geq \lambda_1 \geq \dots \geq \lambda_{N-1}$.

- We have

$$\deg(v) = \begin{cases} d & v \in V_0 = H, \\ d_i & v \in V_i \quad (i = 1, \dots, k). \end{cases}$$

In particular, $\mathcal{G}(G, H, S)$ is regular if and only if $k = 0$ or $k = 1$ and $S_0 = \emptyset$.

- $\mathcal{G}(G, H, S)$ is a D -regular graph for

$$D = \begin{pmatrix} d_0 & d_1 & \dots & d_k \\ d_1 & & & \\ \vdots & & O & \\ d_k & & & \end{pmatrix}.$$

- $\mathcal{G}(G, H, S)$ is bipartite if and only if $S_0 = \emptyset$. The bipartition of G is then given by V_0 and $\bigcup_{i=1}^k V_i$.
- $\mathcal{G}(G, H, S)$ is connected if and only if $S_i \neq \emptyset$ for all $i \geq 1$ and $S_0 \cup \bigcup_{i=1}^k S_i S_i^{-1}$ generates H (Theorem 3.3 in Reyes-Bustos (2016)).
- $\mathcal{G}(G, H, S)$ has eigenvalues (called *trivial eigenvalues*; see Theorem 5.1 in Reyes-Bustos (2016))

$$\mu_{\pm} = \frac{1}{2} \left(d_0 \pm (d_0^2 + 4 \sum_{i=1}^k d_i^2)^{1/2} \right).$$

μ_+ is the largest eigenvalue, and it is simple if $\mathcal{G}(G, H, S)$ is connected. For any eigenvalue λ of $\mathcal{G}(G, H, S)$ other than $\pm \lambda_0$, we have $|\lambda| < \lambda_0$.

- When $[G : H] = 2$, $\mathcal{G}(G, H, S)$ is Ramanujan if $|S| \geq n + 2 - 2\sqrt{n}$.

When the subgroup H is *abelian*, the eigenvalues of $\mathcal{G}(G, H, S)$ can be expressed in terms of *group characters* of H as follows.

Theorem 1 (Kimoto, 2018, Theorem 3) *If H is abelian, then the eigenvalues of $\mathcal{G}(G, H, S)$ are given by*

$$\lambda_{\varphi, \pm} = \frac{1}{2} \left(\sum_{h \in H_0} \varphi(h) \pm \left(\left(\sum_{h \in H_0} \varphi(h) \right)^2 + 4 \sum_{j=1}^k \left| \sum_{h \in H_j} \varphi(h) \right|^2 \right)^{1/2} \right) \quad (\varphi \in H^*)$$

and zeros whose multiplicity is at least $(k-1)n$. Here $H_i := S_i x_i^{-1} \subset H$.

4 Homogeneity

We introduce a simple notion concerning the symmetry of a graph. Let $X = (V, E)$ be a graph. Assume that a group G acts on V . We say that X is G -homogeneous if $x \sim y$ implies $gx \sim gy$ for any $g \in G$. This is equivalent to say that G is embedded in the graph automorphism group $\text{Aut}(X)$ of the graph X . We see that $\mathcal{N}(gx) = g\mathcal{N}(x)$ and hence $\deg(x) = \deg(gx)$ for any $x \in V$ and $g \in G$. In particular, if $G \curvearrowright V$ is transitive (i.e. for any $x, y \in V$, we can find $g \in G$ such that $y = gx$), then X is regular.

Remark 5 X is $\text{Aut}(X)$ -homogeneous.

Remark 6 A G -homogeneous graph X is vertex-transitive (i.e. for any $x, y \in V$, there exists a graph isomorphism f such that $y = f(x)$) if $G \curvearrowright V$ is transitive.

Example 4 A Cayley graph $X = \text{Cay}(G, S)$ is G -homogeneous by the natural left translation $(g, x) \mapsto gx$. X is $G \times G$ -homogeneous via $((g_1, g_2), x) \mapsto g_1 x g_2^{-1}$ if and only if S is *normal* or G -conjugate invariant (i.e. $g S g^{-1} = S$ for all $g \in G$) or S is a union of several conjugacy classes of G . In such a case, we have

$$\det(x I_N - \mathcal{A}) = \prod_{\pi \in \widehat{G}} \left(x - \frac{1}{\deg \pi} \sum_{s \in S} \chi^\pi(s) \right)^{(\deg \pi)^2}$$

by Schur's lemma since $\sum_{s \in S} \pi(s)$ commutes with every $\pi(g)$ ($g \in G$) for each $\pi \in \widehat{G}$. Here χ^π is the character of π .

Example 5 A pair graph $X = \mathcal{G}(G, H, S)$ is H -homogeneous.

Proposition 1 Let $X = (V, E)$ be a graph with a group action $G \curvearrowright V$ which is free (i.e. stabilizer of any $v \in V$ is trivial) and transitive. Then $X \cong \text{Cay}(G, S)$ for a certain $S \subset G$.

Proof We have $\mathcal{N}(gv) = g\mathcal{N}(v)$ for each $g \in G$ and $s \in S$. There exists $S \subset G$ such that $\mathcal{N}(v) = \{sv \mid s \in S\}$. It is straightforward to check that $X \cong \text{Cay}(G, S)$. $\square$

We roughly observe that the spectra $\text{Spec}(X)$ of a graph X tends to be simple if X is equipped with a large symmetry. Pair graphs can be regarded as a class of graphs which have weakened but nontrivial symmetry (or homogeneity) compared to Cayley graphs.

In the following section, we introduce a generalization of pair graphs, which are free but non-transitive H -homogeneous graphs.

5 Generalized Group–Subgroup Pair Graph

5.1 Definition

Let G be a finite group and H its subgroup of index $k + 1$. For later use, we put $N = |G|, n = |H|$ (hence we have $N = (k + 1)n$). Fix a collection of representatives $\{x_0 = e, x_1, \dots, x_k\}$ of $H \backslash G$ and put $V_i = Hx_i$ ($i = 0, 1, \dots, k$). Let $\mathcal{S} = \{S_{ij}\}_{i,j=0}^k$ be a family of subsets in G such that

- (1) $S_{ij} \subset V_i^{-1}V_j = x_i^{-1}Hx_j$,
- (2) $e \notin S_{ij}$,
- (3) $S_{ij}^{-1} = S_{ji}$.

For two vertices $x, y \in G$, we connect these two by an edge if and only if $y = xs$ for some $s \in S_{ij}$ when $x \in V_i$ and $y \in V_j$ ($i, j = 0, 1, \dots, k$). We denote this graph by $\mathcal{G}(G, H, \mathcal{S})$, and call such a graph a *generalized group-subgroup pair graph*, or simply *generalized pair graph*. Put

$$D = \begin{pmatrix} d_{00} & d_{01} & \dots & d_{0k} \\ d_{10} & d_{11} & \dots & d_{1k} \\ \vdots & \vdots & \ddots & \vdots \\ d_{k0} & d_{k1} & \dots & d_{kk} \end{pmatrix}$$

with $d_{ij} = |S_{ij}|$. Notice that D is symmetric. We also put

$$d_s = \sum_{j=0}^k d_{sj} = \sum_{i=0}^k d_{is} \quad (s = 0, 1, \dots, k).$$

Then $\mathcal{G}(G, H, \mathcal{S})$ is a D -regular and $(d_0, d_1, \dots, d_k)$ -regular graph. Thus, if every row sum and column sum of D is equal to d , then $\mathcal{G}(G, H, \mathcal{S})$ is d -regular. By the definition, we readily see that the following lemma holds.

Lemma 1 $\mathcal{G}(G, H, \mathcal{S})$ is H -homogeneous, that is, $x \sim y$ implies $hx \sim hy$ for any $x, y \in G$ and $h \in H$.

When $k = 1$ or $[G : H] = 2$, H is normal and $G/H \cong \mathbb{Z}/2\mathbb{Z}$, and hence it follows that

$$S_{00}, S_{11} \subset V_0, \quad S_{01}, S_{10} \subset V_1.$$

In this case, $\mathcal{G}(G, H, \mathcal{S})$ is (d_0, d_1) -biregular, and it is regular if $|S_{00}| = |S_{11}|$.

Remark 7 When $S_{ii} = \emptyset$ ($i = 0, 1, \dots, k$), then $\mathcal{G}(G, H, \mathcal{S})$ is a *multi-partite graph*.

5.2 Examples

Example 6 Let $X = (V, E)$ be a graph of order $k + 1$ with $V = \{0, 1, \dots, k\}$, and $A = (a_{ij})_{0 \leq i, j \leq k}$ be its adjacency matrix. Take a group $G = \{x_0, x_1, \dots, x_k\}$ of order $k + 1$, and put $H = \{e\}$ and

$$S_{ij} = \begin{cases} \emptyset & a_{ij} = 0, \\ \{x_i^{-1}x_j\} & a_{ij} = 1. \end{cases}$$

Then $\mathcal{G}(G, H, \mathcal{S}) \cong X$. Thus any finite graph is captured in the framework of generalized pair graphs (with trivial symmetry).

Example 7 Let G be a finite group, H its subgroup of index $k + 1$ and $S \subset G$ a subset such that $S \cap H$ is symmetric. Fix a collection of representatives $\{x_0 = e, x_1, \dots, x_k\}$ of $H \backslash G$ and put $V_i = Hx_i$ ($i = 0, 1, \dots, k$). Define

$$S_{0i} = S \cap V_i, \quad S_{i0} = S_{0i}^{-1} \quad (i = 0, 1, \dots, k), \\ S_{ij} = \emptyset \quad (i \neq 0, j \neq 0).$$

Then $\mathcal{G}(G, H, S)$ is reduced to the original group-subgroup pair graph $\mathcal{G}(G, H, S)$.

Example 8 Let $G = D_n = \langle s, t \rangle$ be the dihedral group of degree $2n$. We take $H = \langle s \rangle$ and $x_0 = e, x_1 = t$. Put

$$S_{00} = \{s, s^{-1}\}, \quad S_{01} = S_{10} = \{t\}, \quad S_{11} = \{s^2, s^{-2}\}.$$

Then $\mathcal{G}(G, H, S)$ is a $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ -regular graph (and hence it is 3-regular). The following are the pictures of $\mathcal{G}(G, H, S)$ for $n = 5, 6, 7, 8$ (Fig. 2): when $n = 5$, $\mathcal{G}(G, H, S)$ is isomorphic to the Petersen graph (the leftmost one in the picture above). These four examples are Ramanujan graphs:

$$\det(xI - \mathcal{A}) = \begin{cases} (x-3)(x-1)^5(x+2)^4 & n=5, \\ (x-3)(x-1)x^2(x+2)^2(x^2-5)(x^2-2)^2 & n=6, \\ (x-3)(x-1)(x^6+2x^5-6x^4-10x^3+10x^2+11x-1)^2 & n=7, \\ (x-3)(x-1)(x^2-5)(x^2+2x-1)^2(x^4-4x^2+1)^2 & n=8 \end{cases}$$

and

$$\lambda(X) \approx \begin{cases} 2 & n=5, \\ 2.2361 & n=6, \\ 2.3319 & n=7, \\ 2.4142 & n=8, \end{cases}$$

which are less than $2\sqrt{2} \approx 2.8284$. In general, the eigenvalues of $\mathcal{G}(G, H, S)$ are given by

$$\cos \frac{2\pi j}{n} + \cos \frac{4\pi j}{n} \pm \sqrt{\left(\cos \frac{2\pi j}{n} - \cos \frac{4\pi j}{n}\right)^2 + 1} \quad (j = 0, 1, \dots, n-1).$$

$\mathcal{G}(G, H, S)$ is Ramanujan whenever $n \leq 23$, and is not Ramanujan when $n \geq 24$.

Example 9 Let $G = D_n$ be the dihedral group of degree $2n$, and we take $H = \langle s \rangle$ and $x_0 = e, x_1 = t$. Put

Fig. 2 $\mathcal{G}(G, H, \mathcal{S})$ for $n = 5, 6, 7, 8$

$$S_{00} = \{s, s^{-1}\}, \quad S_{01} = S_{10} = \{st, s^{-1}t\}, \quad S_{11} = \{s^2, s^{-2}\}.$$

Then $\mathcal{G}(G, H, \mathcal{S})$ is a $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$ -regular graph (and hence it is 4-regular). The following are the pictures of $\mathcal{G}(G, H, \mathcal{S})$ for $n = 5, 6, 7, 8$ (Fig. 3): these four examples are Ramanujan graphs:

$$\det(xI - \mathcal{A}) = \begin{cases} x(x-4)(x^4 + 2x^3 - 4x^2 - 5x + 5)^2 & n = 5, \\ x^3(x-4)(x+2)^2(x^2-8)(x^2-2)^2 & n = 6, \\ x(x-4)(x^6 + 2x^5 - 8x^4 - 15x^3 + 14x^2 + 28x + 7)^2 & n = 7, \\ x^3(x-4)(x+2)^2(x^2-8)(x^4 - 6x^2 + 4)^2 & n = 8 \end{cases}$$

and

$$\lambda(X) \approx \begin{cases} 2.4667 & n = 5, \\ 2.8284 & n = 6, \\ 2.6377 & n = 7, \\ 2.8284 & n = 8, \end{cases}$$

which are less than $2\sqrt{3} \approx 3.4641$. In general, the eigenvalues of $\mathcal{G}(G, H, \mathcal{S})$ are given by

$$\cos \frac{2\pi j}{n} + \cos \frac{4\pi j}{n} \pm \sqrt{\left(\cos \frac{2\pi j}{n} - \cos \frac{4\pi j}{n}\right)^2 + 4 \cos^2 \frac{2\pi j}{n}} \quad (j = 0, 1, \dots, n-1).$$

$\mathcal{G}(G, H, \mathcal{S})$ is Ramanujan whenever $n \leq 15$, and is not Ramanujan when $n \geq 16$.

In general, when $[G : H] = 2$, take $S_{00} \subset H = Hx_0$ such that $S_{00}^{-1} = S_{00}$ and $S_{01} \subset Hx_1$. We also take a nontrivial group automorphism f of H . Put $S_{11} = f(S_{00})$ and $S_{10} = S_{01}^{-1}$. Then we get a regular graph $\mathcal{G}(G, H, \mathcal{S})$.

Fig. 3 $\mathcal{G}(G, H, \mathcal{S})$ for $n = 5, 6, 7, 8$

6 Spectra of $\mathcal{G}(G, H, \mathcal{S})$

6.1 Adjacency Matrix of $\mathcal{G}(G, H, \mathcal{S})$

Let $\mathcal{A}$ be the adjacency matrix of $\mathcal{G}(G, H, \mathcal{S})$. For a concrete description of $\mathcal{A}$, we write $H = \{h_0, \dots, h_{n-1}\}$ with $h_0 = e$, and put $g_{ni+j} = h_j x_i$ for $i = 0, \dots, k$ and $j = 0, \dots, n-1$. Thus we have $G = \{g_0, g_1, \dots, g_{N-1}\}$. Then $\mathcal{A}$ is of the form

$$\mathcal{A} = \begin{pmatrix} \mathcal{A}_{00} & \mathcal{A}_{01} & \dots & \mathcal{A}_{0k} \\ \mathcal{A}_{10} & \mathcal{A}_{11} & \dots & \mathcal{A}_{1k} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{A}_{k0} & \mathcal{A}_{k1} & \dots & \mathcal{A}_{kk} \end{pmatrix},$$

where each block $\mathcal{A}_{pq}$ ($0 \leq p, q \leq k$) is given by

$$(\mathcal{A}_{pq})_{ij} = \begin{cases} 1 & h_i^{-1} h_j \in H_{pq} := x_p S_{pq} x_q^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

We notice that we can express each $\mathcal{A}_{pq}$ as

$$\mathcal{A}_{pq} = \sum_{s \in H_{pq}} \mathcal{R}_H(s),$$

where $\mathcal{R}_H$ is the left regular representation of H .

6.2 When H is abelian

If H is *abelian*, then $\mathcal{R}_H$ is a direct sum of all inequivalent 1-dimensional (irreducible) representations of H , that is, there exists a certain unitary matrix U such that

$$U^* \mathcal{R}_H(h) U \sim \bigoplus_{\varphi \in H^*} \varphi(h).$$

Hence

$$U^* \mathcal{A}_{pq} U = \sum_{s \in H_{pq}} \bigoplus_{\varphi \in H^*} \varphi(s).$$

Since $\{U^* \mathcal{A}_{pq} U\}_{p,q}$ commutes with each other, we have the following theorem.

Theorem 2 Assume that H is an abelian subgroup of G . The adjacency matrix $\mathcal{A}$ of the generalized pair graph $\mathcal{G}(G, H, \mathcal{S})$ is given by

$$\det(x I_N - \mathcal{A}) = \prod_{\varphi \in H^*} \det(x I_{k+1} - \mathcal{A}_\varphi),$$

where $\mathcal{A}_\varphi$ with $\varphi \in H^*$ is given by

$$\mathcal{A}_\varphi = \left(\sum_{s \in H_{ij}} \varphi(s) \right)_{0 \leq i, j \leq k}.$$

Remark 8 When $H = \{e\}$, we see that $H^* = \{\mathbf{1}\}$ and $\mathcal{A}_1 = \mathcal{A}$. Thus the theorem above is trivial.

Remark 9 Notice that $\mathcal{A}_1 = D$. It follows that the eigenvalues of D are also eigenvalues of $\mathcal{G}(G, H, \mathcal{S})$ if H is abelian. It is natural to ask the relation between $\text{Spec}(\mathcal{A})$ and $\text{Spec}(D)$ when H is non-abelian. We leave this as a future problem.

Remark 10 When $\mathcal{G}(G, H, \mathcal{S})$ is a pair graph, that is, $\mathcal{A}_{ij} = 0$ if $i \neq 0$ and $j \neq 0$, we have

$$\det(x I_N - \mathcal{A}) = x^{(k-1)n} \det\left(x^2 I_n - x \mathcal{A}_{00} - \sum_{j=1}^k \mathcal{A}_{0j} \mathcal{A}_{j0}\right)$$

without any assumption on H . If H is abelian, then Theorem 1 follows immediately from the equation above.

6.3 Petersen Extension

Let G be a group, H be a subgroup of G with index 2 and $X := \text{Cay}(H, S)$ be a k -regular Cayley graph. Assume that $G = H \cup Hw$ with $w \in G$. Take a group endomorphism $\sigma \in \text{End}(H)$. Notice that $X' := \text{Cay}(H, \sigma(S)) \cong X$ if σ is an *automorphism*. Put

$$S_{00} = S, \quad S_{11} = \sigma(S), \quad S_{01} = \{w\}, \quad S_{10} = \{w^{-1}\}.$$

Fig. 4 $\text{Cay}(H, S)$ and its Petersen extension $\mathcal{G}(G, H, S)$

Then $\tilde{X} = \mathcal{G}(G, H, S)$ is a $(k + 1)$ -regular H -homogeneous graph. We call this the *Petersen extension* of $\text{Cay}(H, S)$. The adjacency matrix $\tilde{\mathcal{A}}$ of $\tilde{X}$ is given by

$$\tilde{\mathcal{A}} = \begin{pmatrix} \mathcal{A} & I_n \\ I_n & \mathcal{A}' \end{pmatrix},$$

where $\mathcal{A}$ and $\mathcal{A}'$ are the adjacency matrices of X and X' , and it follows that

$$\det(x I_{2n} - \tilde{\mathcal{A}}) = \det(x^2 I_n - x(\mathcal{A} + \mathcal{A}') + \mathcal{A}\mathcal{A}' - I_n).$$

Example 10 When $G = D_5 = \langle s, t \rangle$, $H = \langle s \rangle$, $S = \{s, s^{-1}\}$, $w = t$ and $\sigma \in \text{Aut}(H)$ is given by $\sigma(h) = h^2$ ($h \in H$), the Petersen extension $\mathcal{G}(G, H, S)$ of $\text{Cay}(H, S)$ is the *Petersen graph* (Fig. 4).

Remark 11 If σ is the identity map of H (i.e. $X' = X$), then the Petersen extension $\mathcal{G}(G, H, S)$ of $\text{Cay}(H, S)$ is just a Cartesian product of $\text{Cay}(H, S)$ and the path graph $P_1 = \bullet \text{---} \bullet$.

In general, it is not true that the Petersen extension $\tilde{X}$ of $X = \text{Cay}(H, S)$ is Ramanujan when X is Ramanujan. Thus we propose the following problem.

Problem 1 Characterize the quintuple (G, H, S, w, σ) such that both $\text{Cay}(H, S)$ and its Petersen extension with w and σ are Ramanujan.

6.3.1 Examples: Dihedral case

We look at the case where $G = D_n = \langle s, t \rangle$, $H = \langle s \rangle$ and $w = t$, for instance. In this case, an endomorphism σ of H is given by $\sigma(h) = h^l$ for certain $l \in \mathbb{Z}$, and $\sigma \in \text{Aut}(H)$ if and only if $\gcd(n, l) = 1$. We also notice that $wSw^{-1} = tSt = S$ for any symmetric generating subset S of H .

Let $X_{n,l} := \mathcal{G}(G, H, S)$ be the Petersen extension of $\text{Cay}(H, S)$ defined by w and $\sigma : H \ni h \mapsto h^l \in H$. Then, the family $\mathcal{S}$ is given by

$$S_{00} = S, \quad S_{01} = S_{10} = \{t\}, \quad S_{11} = \{s^l \mid s \in S\}.$$

For each character $\varphi \in H^*$, define

$$\alpha_\varphi := \sum_{s \in S} \varphi(s), \quad \beta_\varphi := \sum_{s \in S} \varphi(s^l).$$

By Theorem 2, we see that

$$\det(x I_{2n} - \mathcal{A}) = \prod_{\varphi \in H^*} \det(x I_2 - \mathcal{A}_\varphi), \quad \mathcal{A}_\varphi = \begin{pmatrix} \alpha_\varphi & 1 \\ 1 & \beta_\varphi \end{pmatrix},$$

where $\mathcal{A}$ is the adjacency matrix of $X_{n,l}$. Hence the eigenvalues of $X_{n,l}$ are given by

$$\frac{\alpha_\varphi + \beta_\varphi \pm \sqrt{(\alpha_\varphi - \beta_\varphi)^2 + 4}}{2} \quad (\varphi \in H^*).$$

Example 11 If $n \geq 3$ and $S = \{s, s^{-1}\}$, then

$$\begin{aligned} \alpha_\varphi &= e^{\frac{2\pi i j}{n}} + e^{-\frac{2\pi i j}{n}} = 2 \cos \frac{2\pi j}{n}, \\ \beta_\varphi &= e^{\frac{2l\pi i j}{n}} + e^{-\frac{2l\pi i j}{n}} = 2 \cos \frac{2l\pi j}{n} \end{aligned}$$

for $\varphi \in H^*$ given by $\varphi(s) = e^{\frac{2\pi i j}{n}}$. Thus the eigenvalues of $X_{n,l}$ are calculated as

$$\cos \frac{2\pi j}{n} + \cos \frac{2l\pi j}{n} \pm \sqrt{\left(\cos \frac{2\pi j}{n} - \cos \frac{2l\pi j}{n}\right)^2 + 1} \quad (j = 0, 1, \dots, n-1).$$

We can numerically check that

- (1) if $n \leq 53$ and $n \neq 48$, then there exists l such that $X_{n,l}$ is Ramanujan,
- (2) if $n \geq 54$ or $n = 48$, then $X_{n,l}$ is not Ramanujan for any choice of l .

When n is *odd* and $\gcd(n, l) = 1$ (i.e. $\sigma \in \text{Aut}(H)$), then we see that

- (1) if $n \leq 53$ and $n \neq 45$, then there exists l such that $X_{n,l}$ is Ramanujan,
- (2) if $n \geq 55$ or $n = 45$, then $X_{n,l}$ is not Ramanujan for any choice of l .

Example 12 If $n = 2m \geq 4$ is *even* and $S = \{s, s^m, s^{-1}\}$, then

$$\begin{aligned} \alpha_\varphi &= e^{\frac{2\pi i j}{n}} + e^{\frac{2m\pi i j}{n}} + e^{-\frac{2\pi i j}{n}} = (-1)^j + 2 \cos \frac{2\pi j}{n}, \\ \beta_\varphi &= e^{\frac{2l\pi i j}{n}} + e^{\frac{2lm\pi i j}{n}} + e^{-\frac{2l\pi i j}{n}} = (-1)^{lj} + 2 \cos \frac{2l\pi j}{n} \end{aligned}$$

for $\varphi \in H^*$ given by $\varphi(s) = e^{\frac{2\pi i j}{n}}$. We can numerically check that

- (1) if $m \leq 29$ ($n \leq 58$), then there exists l such that $X_{n,l}$ is Ramanujan,

(2) if $m \geq 30$ ($n \geq 60$), then $X_{n,l}$ is not Ramanujan for any choice of l .

Example 13 If $n \geq 5$ and $S = \{s, s^2, s^{-1}, s^{-2}\}$, then

$$\begin{aligned}\alpha_\varphi &= e^{\frac{2\pi ij}{n}} + e^{\frac{4\pi ij}{n}} + e^{-\frac{2\pi ij}{n}} + e^{-\frac{4\pi ij}{n}} = 2 \cos \frac{2\pi j}{n} + 2 \cos \frac{4\pi j}{n}, \\ \beta_\varphi &= e^{\frac{2\pi ij}{n}} + e^{\frac{4\pi ij}{n}} + e^{-\frac{2\pi ij}{n}} + e^{-\frac{4\pi ij}{n}} = 2 \cos \frac{2\pi j}{n} + 2 \cos \frac{4\pi j}{n}\end{aligned}$$

for $\varphi \in H^*$ given by $\varphi(s) = e^{\frac{2\pi ij}{n}}$. We can numerically check that

- (1) if $n \leq 33$, then there exists l such that $X_{n,l}$ is Ramanujan,
- (2) if $n \geq 34$, then $X_{n,l}$ is not Ramanujan for any choice of l .

Remark 12 In the paper, we discuss the construction of graphs when a finite group G and its subgroup H are given. It would be also interesting to consider the situation where finite groups G, H and an epimorphism $p: G \twoheadrightarrow H$ are given (i.e. H is a quotient group of G).

Acknowledgements This work was supported by JST CREST Grant Number JPMJCR14D6, Japan. The author would like to thank the anonymous reviewer for his/her comments and suggestions.

References

- D. Charles, K. Lauter, E. Goren, Cryptographic hash functions from expander graphs. *J. Cryptol.* **22**, 93–113 (2009)
- K. Feng, W.-C.W. Li, Spectra of hypergraphs and applications. *J. Number Theory* **60**(1), 1–22 (1996)
- W. Fulton, J. Harris, Representation Theory: A First Course. Graduate Texts in Mathematics, vol. 129 (Springer, New York, 1991)
- K. Hashimoto, Zeta functions of finite graphs and representations of p -adic groups. Automorphic forms and geometry of arithmetic varieties. In: *Advanced Studies in Pure Mathematics*, vol. 15 (Academic Press, Boston, MA, 1989), pp. 211–280
- K. Kimoto, Spectra of Group-Subgroup Pair Graphs, in *Mathematical Modelling for Next-Generation Cryptography*, Math. Ind. eds. by T. Takagi et al., vol. 29 (Springer, Singapore, 2018)
- A. Lubotzky, R. Phillips, P. Sarnak, Ramanujan graphs. *Combinatorica* **8**, 261–277 (1988)
- A. Nilli, On the second eigenvalue of a graph. *Discrete Math.* **91**, 207–210 (1991)
- A.K. Pizer, Ramanujan graphs and Hecke operators. *Bull. Am. Math. Soc. (N.S.)* **23**, 127–137 (1990)
- C. Reyes-Bustos, Cayley-type graphs for group-subgroup pairs. *Linear Algebra Appl.* **488**, 320–349 (2016)
- A. Terras, *Zeta Functions of Graphs—A stroll through the Garden* (Cambridge Univ Press, Cambridge, 2011)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.