Master thesis

Cayley-type graphs for group-subgroup pairs

Cid Reyes Bustos

Supervisor: Prof. Masato Wakayama

Graduate School of Mathematics
Kyushu University

July 31, 2015

Abstract

In this thesis we introduce a new type of graph for group-subgroup pairs (G, H) and subsets $S \subset G$ that naturally extends Cayley graphs. We show the elementary properties of such graphs, including connectedness, degree and partition structure, and vertex-transitivity, relating these properties with those of the underlying group-subgroup pair. A subset of the spectrum of these graphs, that includes the largest eigenvalue, can be determined from the properties of the group, subgroup and subset. We also present a sufficient condition on the group-subgroup pair (G, H) and the size of S that results on bipartite Ramanujan graphs. Among these Ramanujan graphs, there are some that cannot be obtained as Cayley graphs. As another application, we propose the use of group-subgroup pair graphs to model linear error-correcting codes.

Contents

Introduction

The simplicity of the definition of a graph is the main reason graph theory has found applications in many areas of mathematics. It is just a graphical representation of the relations on a set. The properties of graphs have been studied from different points of view: combinatorial, algebraic and topological, among others.

Regular graphs are of central importance in graph theory and applications. A regular graph is one whose vertices have the same degree, that is, every vertex has the same number of adjacent vertices. Regular graphs have many symmetries, in other words, they have a rich group of graph automorphisms. For instance, for regular graphs we can find groups of automorphisms that act transitively on the vertices, this means that we can think of a regular graph as a homogenous space for a certain group. On the other hand, one can start with a group and a subset of the group and obtain the associated Cayley graph, which is also a regular graph.

In this work, we introduce a Cayley-type graph for a group and subgroup pair and subset, which we call the *group-subgroup pair graph*. The motivation for the definition comes from a recent paper [6] on the extension of the group determinant for group-subgroup pairs using the wreath determinant arising from the invariant theory of the α-determinant [8]. This contruction of wreath determinant suggests a natural definition of the group-subgroup pair graph, a note on the connection between the two concepts is provided in Appendix A.

The resulting group-subgroup pair graph is not a regular graph, but rather a multi-regular graph. The degree of the vertices depends on the cosets of the subgroup. The results on vertex structure of the group-subgroup pair graphs are given in in Section 2.1. The conditions for the connectedness of the graph and for it to be bipartite are described in Section 2.3, along with other basic properties. Additionally, we present in Section 2.4 structure theorems for connected group-subgroup pair graphs. In the simplest case, the pair-graph is isomorphic to a factor graph of the barycentric division of a Cayley graph. The structural properties of graphs according to the choice of subset S and the index of the subgroup are shown in Figure 0.1.

For group-subgroup pair graphs, there is a subset of the spectrum of the graph that is apparent from the properties of the group, subgroup and generating set. This corresponds to the trivial eigenvalues of regular graphs and to the zero eigenvalue with prescribed minimal multiplicity. The description of these apparent eigenvalues and their eigenfunctions is given in Section 2.5.

We present several applications: to the construction of Ramanujan graphs, to the design of linear error-correcting codes and the computation of eigenvalues

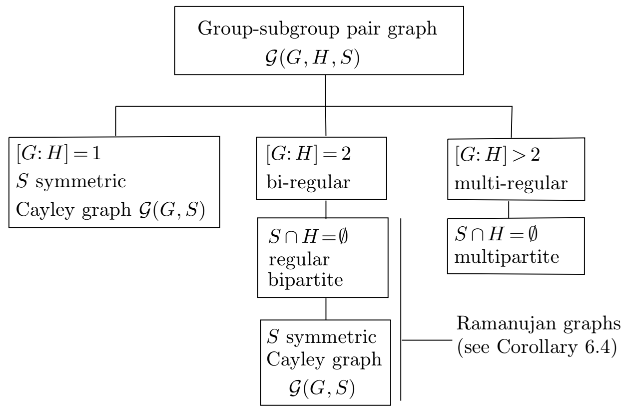

Figure 0.1: Families of group-subgroup pair graphs.

of graphs with particular structure. A Ramanujan graph is a k-regular graph that satisfies

$$|\mu| \leqslant 2\sqrt{k-1},$$

where μ is any nontrivial eigenvalue. This formulation is equivalent to the "Graph Theoretical Riemann Hypothesis" for the Ihara zeta function associated to the graph, as first explained by Sunada in [16]. Ramanujan graphs are the expander graphs that are optimal from the spectral point of view. The original construction of families of Ramanujan graphs was presented by Lubotzky, Phillips and Sarnak in [11] and independently by Margulis in [14]. In Section 3.1 we show that regular group-subgroup pair graphs satisfying

$$|S| \geqslant |H| + 2 - 2\sqrt{|H|},$$

are Ramanujan graphs. In particular, using this result we can obtain bipartite Ramanujan graphs that do not arise as Cayley graphs for the given group.

The second application is to the design of linear codes. Coding theory studies the problem of reliably communicating information over a noisy channel. This is done by adding redundancy to messages to generate codewords, which are later decoded. When a linear transformation is used to generate codewords, the codes are called linear. Linear codes can be represented by means of a bipartite graph, the Tanner graph of the code. Conversely, a bipartite graph may be used to model linear codes. We propose the use of group-subgroup pair graphs for the modeling of linear codes due to their structural properties. Some of the basic ideas are sketched in Section 3.2. The final application is the computation of the full spectrum of generalized cycle graphs, using the structure theorems for group-subgroup pair graphs and the representation theory of the subgroup H.

The contents of this work are based on the preprint article [15].

Chapter 1

Preliminaries

In this section we introduce the preliminary results and notations necessary for the rest of the text.

1.1 Graph theory

A finite *graph* $\mathcal{G}$ is a pair (V, E) consisting of a finite set of vertices V and a relation given by $E \subseteq V \times V$. We will consider only graphs where the relation is symmetric, in this case we write $x \sim y$ when $(x, y) \in E$ and we say that the vertices x and y are adjacent and that the graph $\mathcal{G}$ is *undirected.* If the relation is not reflexive, $x \nsim x$ for any vertex x, we say that the graph contains no loops.

The *degree* of a vertex x is defined as the cardinality of the set

$$\{(x, y) \in E \mid y \in V\}.$$

A graph $\mathcal{G}$ consisting of vertices of uniform degree k is called a *k-regular graph.* A *path* is a finite sequence $x_0, x_1, \ldots, x_n$ of vertices such that $x_i \sim x_{i+1}$ for $i \in \{1, 2, \ldots, n-1\}$, if $x_0 = x_n$ the path is called a *cycle.* A *connected* graph $\mathcal{G}$ is one where any two vertices x, y have a path $x_0, x_1, \ldots, x_n$ with $x_0 = x$ and $x_n = y$. If we make the convention that a vertex x has a path $x_0 = x$ connecting it with itself, the relation of having a path is an equivalence relation on the vertices of the graph. The resulting equivalence classes are the *connected components* of the graph and the graph is connected when it only has one connected component.

A *bipartite graph* is a graph $\mathcal{G}$ along with a function $b : V \to \{0, 1\}$ such that the image E' under b of the relation E is not reflexive. In other words, there is a partition of the vertices $V = V_1 \dot{\cup} V_2$ $\mathcal{G}$ such that any two vertices in the same set are not adjacent.

The space $\mathcal{L}(\mathcal{G})$ consists of functions $f : V \to \mathbb{C}$, if the graph is not finite additional convergence conditions may be imposed to the functions in that space. Associated to a graph $\mathcal{G}$ there is an *adjacency operator* A acting on $\mathcal{L}(\mathcal{G})$ described by

$$Af(x) = \sum_{x \sim y} f(y).$$

The matrix representation $\mathbf{A}$ of the adjacency operator A is called the *adjacency matrix* of the graph.

Let $\mathcal{G} = (V, E)$ be a graph, the *barycentric division* $\mathcal{G}^{(2)}$ of the graph $\mathcal{G}$ is the graph with set of vertices $V \cup E$ and in which two vertices $x \in V$, $(y, z) \in E$ are adjacent if $x = y$ or $x = z$. These are the only edges of the graph, therefore the sets V and E are a bipartition of $\mathcal{G}^{(2)}$.

The spectrum of a graph

The *spectrum* $\text{Spec}(\mathcal{G})$ of a graph $\mathcal{G}$ is just the spectrum of the associated adjacency operator A. The spectrum of a graph reflects certain combinatorial properties of the graph. The results of this section will be stated without proof, but the proofs can be found in any standard text such as [1] or [9].

Proposition 1.1.1. *Let $\mathcal{G}$ be a simple graph without loops. Then the following are equivalent:*

1. *$\mathcal{G}$ is a bipartite graph.*
2. *There are no cycles of odd length in $\mathcal{G}$.*
3. *$\text{Spec}\,\mathcal{G}$ is symmetric about 0.*

We denote by $\rho(\mathcal{G})$ the spectral radius of the graph $\mathcal{G}$. The following results relate the spectral radius of a graph with various combinatorial properties.

Proposition 1.1.2. *If the graph $\mathcal{G}$ is k-regular, then*

$$\rho(\mathcal{G}) = k$$

The eigenvalue k of a k-regular graph $\mathcal{G}$ is usually called the *trivial eigenvalue* of the graph. If the graph is bipartite, then $-k$ is also called trivial eigenvalue.

Proposition 1.1.3. *The graph $\mathcal{G}$ is connected if and only if the multiplicity of $\rho(\mathcal{G})$ is one. If the graph is k-regular, the multiplicity of $\rho(\mathcal{G}) = k$ is the number of connected components of $\mathcal{G}$.*

A graph is called *vertex transitive* when for any pair of different vertices x and y there is graph automorphism φ such that $\varphi(x) = y$.

1.2 Cayley graphs

A Cayley graph is graph constructed from a group G and where the relation between vertices is obtained from a *generating set* S using the group operation. The graphs were introduced by Arthur Cayley in 1878 [2].

A subset S of a group G is said to be symmetric if it contains the inverse of all of its elements, that is, if $S = S^{-1}$.

Definition 1.2.1. *Let G and $S \subseteq G$ a symmetric subset. A **Cayley graph** $\mathcal{G}(G, S)$ is a graph with set of vertices G and where $g, h \in G$ are adjacent if there is an element $s \in S$ such that*

$$h = gs.$$

In the notation of the previous section, $g \sim h$ if $g^{-1}h \in S$. There is no generally accepted notation for Cayley graphs, and sometimes the notation $\mathrm{Cay}(G,S)$ is used, also sometimes the generating set is called Cayley set.

It can be seen from the definition that a Cayley graph $\mathcal{G}(G,S)$ is regular, and the degree of its vertices is the cardinality of the generating set S.

Proposition 1.2.2. *A Cayley graph $\mathcal{G}(G,S)$ is connected if and only if*

$$\langle S \rangle = G.$$

When the graph is not connected, the connected components are given by left cosets of $\langle S \rangle$.

In other words, the graph is connected if the generating set S generates the group G. The group G naturally acts on itself via left translations, therefore this extends to a graph bijection that preserves the edges. It is clearly a graph automorphism. Moreover, since we can find one such automorphism that takes any vertex into any other, we have:

Proposition 1.2.3. *A Cayley graph $\mathcal{G}(G,S)$ is vertex transitive.*

In his 1878 article, Arthur Cayley introduces the graph as a mean of representing a group and gives the example with the symmetric group of 4 letters. In that article, the role of the generating set S above is taken by a minimal set of generator of the group G. With respect to the paths (routes) in the graph he writes:

> "We hence see that a route applied in succession to the whole series of initial points or letters $abcdefghijkl$, gives a new arrangement of these letters, wherein no one of them occupies its original place; a route is thus, in effect, a substitution. Moreover, we may regard as distinct routes, those which lead from a to a, to b, to c, ... to l,respectively."

This is, of course, the statement of the vertex transitivity of the graph.

One of the most important properties of Cayley graphs is that for abelian groups we can compute the eigenvalues using representation theory.

Theorem 1.2.4. *Let G be an abelian group. Then the eigenvalues of the Cayley graph $\mathcal{G}(G,S)$ are given by*

$$\lambda_i = \sum_{s \in S} \chi_i(s),$$

where χ_i are the irreducible characters of G.

There are several proofs of this result, for a proof using the Fourier transform, the reader is referred to [17].

Chapter 2

Group-subgroup pair graphs

The aim of this work is to introduce a new type of graph, constructed from a group G, a subgroup $H \subseteq G$, and a subset $S \subseteq G$, that is a generalization of Cayley graphs, study its structural properties and present some applications.

2.1 Definition and basic properties

Definition 2.1.1. *Let G be a group, H a subgroup of G and $S \subseteq G$ a subset such that $S \cap H$ is a symmetric subset of G. The **Group-Subgroup Pair Graph** $\mathcal{G}(G, H, S)$ is the undirected graph with vertices G and simple edges given by*

$$(h, hs) \qquad \forall h \in H, \quad \forall s \in S.$$

*We use the term **pair-graph** as a synonymous for group-subgroup pair-graph.*

In terms of relations, we see that a pair $(h, g) \in H \times G$ or $(g, h) \in G \times H$ is an edge if and only if $h^{-1}g \in S$. On the other hand, pairs (g, g') with $g, g' \notin H$ are not edges. When the group and the subgroup coincide the definition reduces to that of a Cayley graph.

With the exception of Section 2.3 all groups are assumed to be finite, and e always represents the identity of a given group G. The notation $[k]$ is used for the set $\{1, 2, \ldots, k\}$ for $k \in \mathbb{N}$. For a given group G, subgroup H and symmetric subset S we denote by S_H and S_O the subsets of G given by

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

Additionally, if H is a subgroup of index $k+1$ of G, we will frequently consider a set of representatives of the cosets, denoted by

$$\{x_0 = e, x_1, \ldots, x_k\},$$

and a partition of S_O given by sets

$$S_i := S \cap Hx_i,$$

for $0 \neq i \in [k]$.

It follows directly from Definition 2.1.1 that the pair graph $\mathcal{G}(G,H,S)$ contains the Cayley graph $\mathcal{G}(H,S_H)$ as a subgraph. Therefore, the class of Cayley graphs is contained in the class of group-subgroup pair graphs. When the generating subset S is empty, we say that the resulting pair-graph $\mathcal{G}(G,H,S)$ is *trivial*.

Example 2.1.2. Let $G = \mathbb{Z}/12\mathbb{Z}$, $H = \{\bar{0},\bar{3},\bar{6},\bar{9}\}$, and $S = \{\bar{2},\bar{4},\bar{5},\bar{7},\bar{8}\}$. The corresponding pair-graph $\mathcal{G}(G,H,S)$ is shown on Figure 2.1.

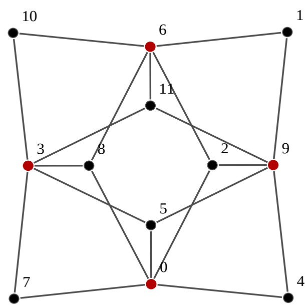

Figure 2.1: The pair-graph $\mathcal{G}(\mathbb{Z}/12\mathbb{Z},H,S)$.

We list some facts that follow from the definition that are used frequently in the paper.

- All the vertices in S are adjacent to the identity $e \in H$.
- A vertex $x \in G - H$ is incident to the edge (x, xs^{-1}) for any $s \in Hx \cap S_O$.
- Two vertices $x, y \in G - H$ are not adjacent.
- If (x,y) is an edge, then (hx,hy) is also an edge of the graph, for any $h \in H$.

Example 2.1.3. Let $K = \mathbb{F}_{7^2}$, the finite field of 7^2 elements, and $H = \mathbb{F}_7$ the prime field of K considered as a subgroup of the additive group K. Then K is the direct sum of seven copies of H. Let φ be the norm map of K as a field extension of H, then if $S = \varphi^{-1}(\{\bar{5},\bar{6}\})$, we obtain the pair-graph $\mathcal{G}(K,H,S)$ shown in Figure 2.2. The pair-graph $\mathcal{G}(\mathbb{F}_{7^2},\mathbb{F}_7,S)$ contains vertices of degree 2, 4 and 16.

Note that the graphs of the above examples are not Cayley graphs for any group, specifically, none of the graphs above are regular.

Remark 2.1.4. We briefly mention another generalization of Cayley graphs for group G and subgroup H, the *Schreier Coset Graph.* For a symmetric subset S of G, the Schreier coset graph is defined as the graph with the set $H\backslash G$ of cosets as vertices and where two cosets Hx and Hy are adjacent when there is an $s \in S$ such that

$$Hxs = Hy.$$

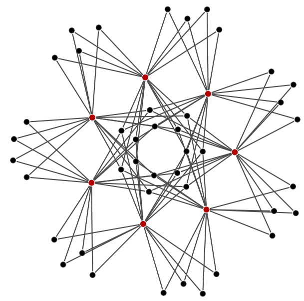

Figure 2.2: The pair-graph $\mathcal{G}(\mathbb{F}_{7^2}, \mathbb{F}_7, S)$.

A Schreier Coset graph can have multiples edges and loops (even when $e \notin S$). The Schreier coset graphs have been used for coset enumeration techniques, a detailed exposition can be found in [3]. For a given group G, the Schreier Coset graph is a Cayley graph when $H = \{e\}$, whereas the group-subgroup pair graph is a Cayley graph when $H = G$.

Degree structure of group-subgroup pair graphs

An isolated vertex is one that is not connected to any other vertex. In contrast with Cayley graphs, group-subgroup pair graphs may contain isolated vertices even when the generating subset is not empty. The following result characterizes the presence of isolated vertices in group-subgroup pair graphs.

Proposition 2.1.5. *i) 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 on G other than $He = H$.*

ii) The vertices H are isolated in $\mathcal{G}(G, H, S)$ if and only if S is the empty set.

Proof. Suppose S contains a representative for each coset other than H, then take $x \in G - H$, and $s \in S$ the representative of Hx, then there is $h \in H$ such that $hs = x$, and therefore x is connected to h. Conversely, if there are no isolated vertices, by the definition we must have $HS_O = G - H$. The second statement follows directly from the definition. □

Example 2.1.6. Let G be any group of order n and $H = \{e\}$. The pair-graph $\mathcal{G}(G, H, S)$ with $S = G - H$ contains no isolated vertices. In fact, $\mathcal{G}(G, H, S)$ is a T_{n-1} *star graph*, as shown in Figure 2.3.

A graph in which all the vertices have the same degree is called a *regular graph*. More precisely, if all the vertices have degree k the graph is called *k-regular graph*. An important property of a Cayley graph $\mathcal{G}(G, S)$ is that it is $|S|$-regular. Example 2.1.2 shows that this is not true in general for group-subgroup pair graphs, but there is still uniformity on the degree of the vertices within each coset.

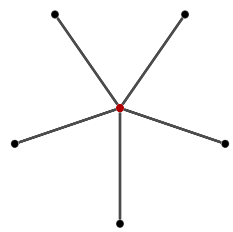

Figure 2.3: The pair-graph $\mathcal{G}(G, \{e\}, S)$ with $|G| = 6$ and $S = G - \{e\}$.

Proposition 2.1.7. *In a pair-graph $\mathcal{G}(G, H, S)$, all the vertices in the same coset have the same degree. Namely, the vertices in H have degree $|S|$ and for $x \notin H$ the degree of the vertices in the coset Hx is $|S \cap Hx|$.*

Proof. It is clear from the discussion following Example 2.1.2 that any two vertices $x, y \in G - H$ in the same coset Hx have the same degree $|Hx \cap S_O| = |Hy \cap S_O|$. The vertices in H have degree $|S|$ by construction. □

A graph with a partition of the vertices $V_1, V_2, \ldots, V_r$ such that the degree of the vertices on each partition is constant is called a *multi-regular* graph or $p_1, p_2, \ldots, p_r$*-regular* graphs, where p_i is the degree of the vertices on a given partition. The above proposition shows that pair-graphs in general are multi-regular graphs.

Returning to Example 2.1.2, $(H + \bar{1}) \cap S = \{\bar{4}, \bar{7}\}$, $(H + \bar{2}) \cap S = \{\bar{2}, \bar{5}, \bar{8}\}$ and $|S| = 5$. The cardinality of these sets corresponds to the degree of the vertices in the respective cosets and the corresponding pair-graph is then a $2, 3, 5$-regular graph.

Corollary 2.1.8. *Let G be a group, H a subgroup of index $[G : H] = k + 1$ and S a subset of G with S_H symmetric. Then for $h \in H$,*

$$\deg(h) \geqslant \sum_{i=1}^{k} \deg(x_i), \tag{2.1}$$

in $\mathcal{G}(G, H, S)$. The equality holds when S_H is empty. In particular, a nontrivial pair-graph $\mathcal{G}(G, H, S)$ is regular if and only if $S_H = \varnothing$ and $[G : H] = 2$, or when $[G : H] = 1$.

Proof. Since $\deg(h) = |S|$ and $\sum_{i=1}^{k} \deg(x_i) = \sum_{i=1}^{k} |S_i| = |S_O|$ by Proposition 2.1.7, the inequality follows since $|S| \geqslant |S_O|$, and the equality is equivalent to $S_H = \varnothing$. The *if* part of the proof follows directly from the inequality and the definitions. For the *only if* part, consider a j-regular pair-graph $\mathcal{G}(G, H, S)$, then by Proposition 2.1.7, $|S| = j$ and $|Hx \cap S_O| = j$ for $x \notin H$. It follows from inequality (2.1) that $|S_O| = kj = k|S|$ and therefore k is necessarily 0 or 1. If $k = 1$, then $[G : H] = 2$ and $|S_O| = |S|$, so $S = S_O$ and the case $k = 0$ gives $[G : H] = 1$. □

Note that in view of Proposition 2.1.7, we can consider $\deg(Hx)$ as the degree of any of the elements of the coset. In that case, the above identity can be written as

$$\deg(H) \geqslant \sum_i \deg(Hx_i),$$

with equality happening when S_H is empty. The preceding discussion shows that the structure of $H\backslash G$, the set of cosets of H on G, is closely related to the degree structure of the graph, this is also the case for the eigenvalues of the graph, as described in Section 3.1.

Proposition 2.1.9. *Let G be a group, H a subgroup with $[G : H] = 2$, and S a subset of G such that $\mathcal{G}(G, H, S)$ is a nontrivial regular pair-graph. If S is a symmetric set, the pair-graph $\mathcal{G}(G, H, S)$ is a Cayley graph. Namely, $\mathcal{G}(G, H, S) = \mathcal{G}(G, S)$.*

Proof. The conditions imply that $S_O = S$, then by the definition of the pair-graph the edges are given by

$$(h, hs), \forall h \in H, \quad \forall s \in S \qquad \text{and} \qquad (x, xs^{-1}), \forall x \in (G - H), \quad \forall s \in S.$$

Since S is symmetric one can simply write (x, xs), $\forall x \in G$, $\forall s \in S$, which is the definition of Cayley graph. □

Example 2.1.10. If R is a ring we denote by $\mathbb{H}(R)$ the ring of quaternions with coefficients in R. Take p and q odd prime numbers with $q > 2\sqrt{p}$ such that p is not a square modulo q. Consider the set $S_p \subset \mathbb{H}(\mathbb{Z})$ of integer quaternions

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k$$

of norm p with $a_0 \geq 0$ such that $\alpha \equiv 1 (\bmod 2)$ or $\alpha \equiv i + j + k (\bmod 2)$. It is known that there are $p + 1$ such integer quaternions. Let $\tau : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$ be the reduction modulo q, ψ be the embedding of $\mathbb{H}(\mathbb{F}_q)$ into $M_2(\mathbb{F}_q)$ and φ the canonical homomorphism of $GL_2(q)$ onto $PGL_2(q)$. Set $S = (\varphi \circ \psi \circ \tau)(S_p)$, then the pair-graph $\mathcal{G}(PGL_2(q), PSL_2(q), S)$ is a connected bipartite $(p + 1)$-regular graph. Moreover, the set S is symmetric and the pair-graph $\mathcal{G}(PGL_2(q), PSL_2(q), S)$ is actually the Ramanujan Cayley graph $X^{p,q}$ of Lubotzky, Phillips and Sarnak [11].

2.2 Connectedness of group-subgroup pair graphs

Connectedness

In this section we discuss the connectedness of group-subgroup pair graphs. Recall that a Cayley graph $\mathcal{G}(G, S)$ is connected if and only if $\langle S \rangle = G$. We begin by considering the case where S_H is empty, in other words, none of the vertices of H are adjacent in $\mathcal{G}(G, H, S)$.

Lemma 2.2.1. *Let G be a group, H a subgroup and $S \subset G$ a subset with $S_H = \varnothing$. The vertices of H in the pair-graph $\mathcal{G}(G, H, S)$ are in the same connected component if and only if $\langle H \cap (SS^{-1}) \rangle = H$.*

Proof. If $\langle H \cap (SS^{-1}) \rangle = H$, then it suffices to prove that the identity e is connected to an arbitrary $h \in H$. For $h \in H$, we have $h = s_1 s_2^{-1} \dots s_{n-1} s_n^{-1}$ with $s_i s_{i+1}^{-1} \in H$, then if we set $h_1 = s_1 s_2^{-1} \dots s_{n-3} s_{n-2}^{-1}$, h_1 is adjacent to $h_1 s_{n-1} = x_1$ and h is adjacent to $h s_n = h_1 s_{n-1} = x_1$ so h_1 is connected to h. By repeating this process we conclude that e is connected to h.

On the other hand, if in the graph $\mathcal{G}(G, H, S)$ all the vertices of H are in the same connected component, any $h \in H$ is connected to $e \in H$. Since there are no direct connections between two elements of H or $G - H$, there must be path from e to h where every even vertex is an element of H, so we have a sequence $h_0 = e, h_1, \dots, h_{n-1}, h_n = h$ of elements of H, where h_i and h_{i+1} are adjacent to $x_i \in G - H$ for $i = 0, 1, 2, \dots, n-1$. That is, we have a sequence of edges $(h_0, x_0), (x_0, h_1) \dots (h_{n-1}, x_{n-1}), (x_{n-1}, h_n)$, as shown in Figure 2.4.

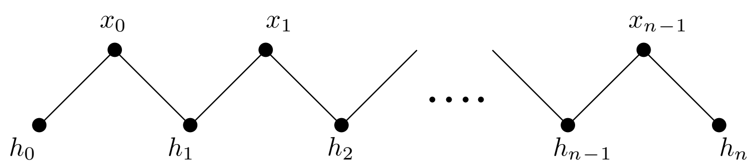

Figure 2.4: The path from h_0 to h_n.

Then, for $s_i \in S$,

$$\begin{aligned} x_0 &= h_0 s_0 \quad , \quad x_0 = h_1 s_1 \\ x_1 &= h_1 s_2 \quad , \quad x_1 = h_2 s_3 \\ &\vdots \qquad\quad \vdots \\ x_{n-1} &= h_{n-1} s_{2n-2} \quad , \quad x_{n-1} = h_{n-1} s_{2n-1} \end{aligned}$$

thus,

$$\begin{array}{rcl} s_0 = h_0 s_0 = h_1 s_1 & & h_1 = s_0 s_1^{-1} \\ h_1 s_2 = h_2 s_3 & & h_2 = h_1 s_2 s_3^{-1} \\ \vdots & \Rightarrow & \vdots \\ h_{n-1} s_{n-2} = h_n s_{2n-1} & & h = h_{n-1} s_{n-2} s_{n-1}^{-1}, \end{array}$$

it follows that $s_i s_{i+1}^{-1} \in H$ and $h \in \langle H \cap SS^{-1} \rangle$. □

Note that since a group-subgroup pair graph may contain isolated vertices, the condition of the lemma alone is not sufficient for connectedness.

Proposition 2.2.2. *Let G be a group, H a subgroup and $S \subseteq G$ a subset with $S_H = \varnothing$. The pair-graph $\mathcal{G}(G, H, S)$ is connected if and only if*

$$\langle H \cap SS^{-1} \rangle = H$$

and S contains representatives of all the cosets of H other than H.

Proof. The result follows from Lemma 2.2.1, Proposition 2.1.5 and the observation that any vertex $x \in G - H$ must be connected to some $h \in H$ which is in turn connected to the identity $e \in H$. □

For the general result, we introduce the notation

$$\widetilde{S} := H \cap SS^{-1},$$

for a subset S of $G - H$.

Theorem 2.2.3. *A pair-graph $\mathcal{G}(G, H, S)$ is connected if and only if*

$$\langle S_H \cup \widetilde{S_O} \rangle = H$$

and S contains representatives of all the cosets of H other than H.

Proof. First we see that the vertices of H are in the same connected component if and only if $\langle S_H \cup \widetilde{S_O} \rangle = H$. The proof of this fact is the same as that of Lemma 2.2.1 while considering that in the path from $e \in H$ to $h \in H$ there may be edges connecting elements h_1, h_2 from H, in such case we have $h_2 = h_1 s_H$, with $s_H \in S_H$. Then the result follows like in Proposition 2.2.2. □

Example 2.2.4. Let $G = \mathbb{Z}/12\mathbb{Z}$, $H \cong \mathbb{Z}/4\mathbb{Z}$. Set $S = \{\bar{2}, \bar{8}\}$ and $S' = \{\bar{1}, \bar{2}, \bar{6}, \bar{7}, \bar{8}\}$, the corresponding group-subgroup pair graphs are shown in Figure 2.5. Note that $\langle H \cap SS^{-1} \rangle = \{\bar{0}, \bar{6}\}$ and $\langle S'_H \cup \widetilde{S'_O} \rangle = \{\bar{0}, \bar{6}\}$, so neither graph is connected. Moreover, as there are no elements of the coset $H + \bar{4} = \{\bar{1}, \bar{4}, \bar{7}, \overline{10}\}$ on S, all the vertices of that coset are isolated on $\mathcal{G}(G, H, S)$.

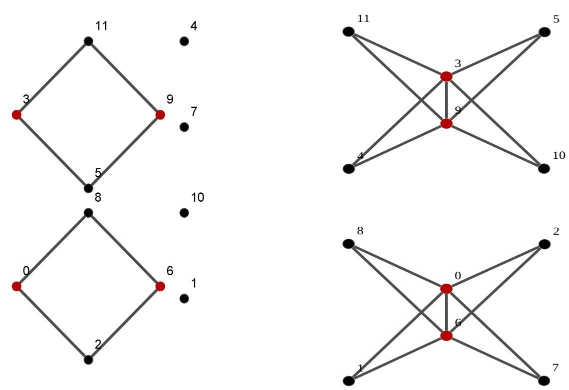

Figure 2.5: The pair-graphs $\mathcal{G}(G, H, S)$ and $\mathcal{G}(G, H, S')$.

Connected Components

If a graph is not connected, the characterization of the connected components of the graph is desirable. For Cayley graphs, the connected component of the identity is the subgroup $\langle S\rangle$, and each of the cosets of $\langle S\rangle$ in G are the connected components of the graph. This does not extend directly to group-subgroup pair graphs, since the connected component of the identity may include vertices from $G-H$. In particular, the subgroup $\langle S_H \cup \widetilde{S_O}\rangle$ of H is the subgroup of elements of H that lie on the identity component. The cosets of this subgroup are the intersection of H with certain connected components of the graph.

Proposition 2.2.5. *Let $U = \langle S_H \cup \tilde{S_O}\rangle$. Then the identity component Γ_e of the pair-graph $\mathcal{G}(G,H,S)$ is $U \cup US_O$. The remaining connected components of the pair-graph $\mathcal{G}(G,H,S)$ are either of the type $\Gamma_h = h\Gamma_e$ for $h \in H$ or the type $\{x\}$ for $x \in G-H$.*

Proof. The first statement follows from the preceding discussion and the definition of the pair-graph $\mathcal{G}(G,H,S)$. Any path $(e, g_1, g_2, \dots, g_n)$ from the identity e to g_n corresponds uniquely to a path $(h, hg_1, \dots, hg_n)$ from h to hg_n so the connected component of $h \in H$ is $\Gamma_h = h\Gamma_e$. Take $x \in G-H$, if x is an isolated vertex its connected component is $\{x\}$, otherwise it is connected to an $h \in H$ and its connected component is of the type Γ_h. □

A consequence of the above proposition is that an arbitrary connected component Γ of $\mathcal{G}(G,H,S)$ has cardinality equal to $|\Gamma_e|$ or 1. Moreover, for first case, we also have $|\Gamma \cap H| = |\Gamma_e \cap H|$ and $|\Gamma - H| = |\Gamma_e - H|$.

For Cayley graphs, the number of connected components of the graph is the index $[G : \langle S\rangle]$. The existence of isolated vertices even for nontrivial pair-graphs makes the formulation slightly more complicated.

Theorem 2.2.6. *The number of connected components of $\mathcal{G}(G,H,S)$ is*

$$[H : \langle S_H \cup \widetilde{S_O}\rangle] + |G-H| - |HS_O|. \tag{2.2}$$

Proof. By Proposition 2.2.5, the first term in the formula is the number of connected components Γ_h that occur on H, the second and third terms count the number of isolated points in $G-H$, by Proposition 2.1.5. Since there are not edges between elements of $G-H$, this is the number of connected components of the graph. □

Proposition 2.2.5 and Theorem 2.2.6 completely characterize the connected components for the pair-graphs $\mathcal{G}(G,H,S)$ for given group G, subgroup H and valid subset $S \subset G$.

Example 2.2.7. For the pair-graph of Example 2.1.2 we have $S = \{\bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$. Since $h = \bar{3} = 8-5 \in S-S$ is a generator of H, the first term in formula (2.2) is 1, the second term is 8 and all the cosets are represented so the last term is 8, resulting in 1 connected component. As for the pair-graphs generated by S and S' of Example 2.2.4, in both cases the first term is 2, the second term is 8, and the final term is 4 for the graph generated by S and 8 for the graph generated by S', therefore $\mathcal{G}(G,H,S)$ has 6 connected components and $\mathcal{G}(G,H,S')$ has two connected components as it is confirmed visually in the diagrams.

2.3 Further properties of group-subgroup pair graphs

Vertex transitivity and group actions

A graph is *vertex transitive* when for any pair of different vertices x and y there is graph automorphism φ such that $\varphi(x) = y$. Cayley graphs are naturally vertex transitive by means of left translations L_g with $g \in G$. Any vertex transitive graph must be regular, therefore by Proposition 2.1.7, we have the following result.

Proposition 2.3.1. *Nontrivial pair-graphs $\mathcal{G}(G,H,S)$ are not vertex transitive when $[G:H] \geqslant 3$ or when $[G:H] = 2$ and S_H is not empty.*

The left translation L_h by $h \in H$ on $\mathcal{G}(G,H,S)$ is a graph isomorphism. Clearly, for any pair of elements x, y of a coset Hx there is an $h \in H$ such that $L_h(x) = y$. However, the left action by an arbitrary $g \in G$ is not necessarily a graph automorphism. For instance, in Example 2.1.2 the action of $g = 1$ is not a graph automorphism, as the image of 0 is 1, and degree$(\bar{0}) = 5$, but degree$(\bar{1}) = 2$.

Let $\mathcal{L}(G)$ be the set of complex valued functions defined on the group G, and consider $\lambda_H : H \to \mathrm{GL}(\mathcal{L}(G))$ the left permutation representation of H given by the action $\lambda_H(h)f(x) = f(h^{-1}x)$ for $h \in H$ and $x \in G$.

Proposition 2.3.2. *Let A be the adjacency operator for a group-subgroup pair graph $\mathcal{G}(G,H,S)$, then for any $h \in H$*

$$\lambda_H(h)A = A\lambda_H(h).$$

Proof. Note that for the pair-graph $\mathcal{G}(G,H,S)$ and $f \in \mathcal{L}(G)$, the adjacency operator is given by

$$Af(y) = \begin{cases} \sum_{s\in S} f(ys) & \text{if } y \in H \\ \sum_{s \in S\cap Hy} f(ys^{-1}) & \text{if } y \in G - H \end{cases}$$

The result then follows from direct calculation using the fact that for any $x \in G$ and $h \in H$, x and $h^{-1}x$ belong to the same coset. □

For $h \in H$, $\lambda_H(h)$ is a permutation matrix for the elements of G corresponding to the left multiplication by h. By Theorem 15.2 of [1], a bijection φ of the vertices of a graph is a graph automorphism if $M_\varphi A = AM_\varphi$, where M_φ is the permutation matrix associated with φ. Moreover, Proposition 2.3.2 shows that eigenspaces V_μ of the adjacency operator are H-invariant under the permutation representation. Therefore, one can use the degree of the irreducible representations of the subgroup H to obtain lower bounds for multiplicity of the eigenvalues of the pair-graph $\mathcal{G}(G,H,S)$.

Proposition 2.3.3. *Let S be a subset G with S_H symmetric and ψ be a H-invariant automorphism of G. Then the pair-graphs $\mathcal{G}(G,H,S)$ and $\mathcal{G}(G,H,\psi(S))$ are isomorphic.*

Proof. For any $h \in H, x \in G - H, s \in S$, we have

$$\begin{aligned}(h,hs) &\longmapsto (\psi(h),\psi(h)\psi(s))\\(x,xs^{-1}) &\longmapsto (\psi(x),\psi(x)\psi(s)^{-1}).\end{aligned}$$

Since ψ is H-invariant, it is a graph isomorphism with inverse ψ^{-1}. □

Examples of such automorphisms are the inner automorphisms $\psi_h(g) = h^{-1}gh$ with $h \in H$.

Proposition 2.3.4. *Let S be a subset of G with S_H symmetric and $R_{h'}$ the right translation by $h' \in H$. Then the pair-graphs $\mathcal{G}(G,H,S)$ and $\mathcal{G}(G,H,S_H \cup R_{h'}(S_O))$ are isomorphic.*

Proof. The map $\varphi_{h'} : G \to G$ given by $\varphi_{h'}(x) = xh'$ for $x \in G-H$ and $\varphi_{h'}(h) = h$ for $h \in H$ is clearly bijective. For $h \in H$ and $s \in S_H$, the edge (h,hs) is fixed by $\varphi_{h'}$. As for $h \in H, s \in S_O$, we have

$$\begin{aligned}(h,hs) &\longmapsto (h,hsh') = (h,hs'),\\(x,xs^{-1}) &\longmapsto (xh',xs^{-1}) = (xh',xh's'^{-1}),\end{aligned}$$

with $s' = sh' \in R_{h'}(S_O)$. Therefore the map $\varphi_{h'}$ is an graph isomorphism with inverse $\varphi_{h'^{-1}}$. □

Bipartite group-subgroup pair graphs

For a group G and symmetric subset S, if there is an homomorphism $\chi : G \to \{-1,1\}$, such that $\chi(S) = \{-1\}$ then the Cayley graph $\mathcal{G}(G,S)$ is bipartite, this condition is also necessary when the graph is connected, for a proof see chapter 4 of [4]. It is clear that the existence of such homomorphism also implies that the pair-graph $\mathcal{G}(G,H,S)$ is bipartite, since it is a subgraph of the Cayley graph $\mathcal{G}(G,S \cup S^{-1})$. In general, the bipartiteness of the pair-graph $\mathcal{G}(G,H,S)$ is not enough to construct a homomorphism from G to $\{-1,1\}$.

Theorem 2.3.5. *If there is a group homomorphism $\chi : H \to \{-1,1\}$, such that $\chi(S_H) = \{-1\}$ and $\chi(\widetilde{S_O}) = \{1\}$, then the pair-graph $\mathcal{G}(G,H,S)$ is bipartite. The converse holds when the pair-graph is connected.*

Proof. Suppose the homomorphism χ exists, then we will prove that there are no cycles of odd length in the pair-graph. Since any cycle of nonzero length starting on $x \in G-H$ contains at least one element of $h \in H$ we restrict to cycle starting on $h \in H$. Suppose there is one such path of odd length l, and as in the proof of Lemma 2.2.1 we see that this path consists of elements of S_H and $\widetilde{S_O}$, namely

$$h = hs'_1 s'_2 \dots s'_{n+k}, \tag{2.3}$$

where $s'_i \in S_H \cup \widetilde{S_O}$, k is the number of elements of S_H and n is the number of elements of $\widetilde{S_O}$. In particular, we have

$$l = 2n + k,$$

so that k is odd. We apply the homomorphism to (2.3) to get

$$\chi(h) = (-1)^k (1)^n \chi(h) = -\chi(h),$$

and the result follows from this contradiction. On the other hand suppose that the pair-graph is bipartite and connected and let V_+ and V_- be the bipartition of the graph, with $e \in V_+$. For $hinH$, set

$$\chi(h) = \begin{cases} 1 & \text{if } h \in V_+ \\ -1 & \text{if } h \in V_- \end{cases},$$

from this and the bipartiteness of the graph it follows that $\chi(S_H) = \{-1\}$ and $\chi(\widetilde{S_O}) = \{1\}$. Note that since the graph is bipartite and connected, we can write

$$\chi(h) = (-1)^{l(e,h)},$$

where $l(e,h)$ is the length of a path from e to h in $\mathcal{G}(G,H,S)$, in other words, the word length of h with the generators S_H and $\widetilde{S_O}$. It is clear that with this definition the map χ is a homomorphism that satisfies the required conditions.

□

Example 2.3.6. Let $G = A_4$, the alternating group of 4 letters, H, the Klein four-group embedded as a subgroup of G, and $S = \{(1,2)(3,4),\ (1,4)(2,3),\ (1,2,3),\ (1,4,3),\ (2,3,4),\ (2,4,3)\}$, using cycle notation. Observe that $(1,3,2)$, the inverse of $(1,2,3)$, is not contained in S. The pair-graph $\mathcal{G}(G,H,S)$ is a bipartite graph. The graph is presented in Figure 2.6, with the vertices of the bipartition shown in different shapes.

The homomorphism $\chi : H \to \{-1,1\}$ is given by

$$\chi(e) = 1, \qquad \chi((1,3)(2,4)) = 1,$$
$$\chi((1,2)(3,4)) = -1, \qquad \chi((1,4)(2,3)) = -1,$$

it is easy to verify that it has the required properties. On the other hand, any homomorphism $\rho : G \to \{-1,1\}$ with $\rho(S) = \{-1\}$, would have $\rho(S^{-1}) = \{-1\}$, but in this case $(1,3,2) = (1,2)(3,4) \cdot (1,4,3)$, therefore there are no homomorphisms that satisfy the condition $\rho(S) = \{-1\}$.

Note that in the case $S_H = \varnothing$, the sets H and $G - H$ form a bipartition of $\mathcal{G}(G,H,S)$, therefore the pair-graph $\mathcal{G}(G,H,S)$ is bipartite. In this case, the corresponding homomorphism $\chi : H \to \{-1,1\}$ is the trivial one: $\chi(h) = 1$, for all $h \in H$.

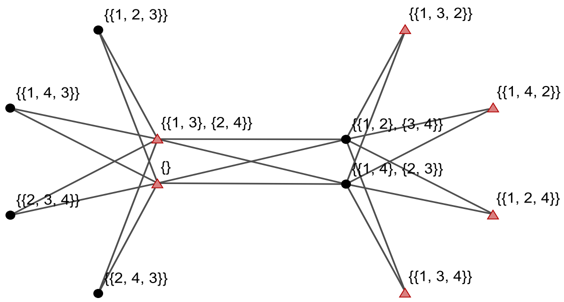

Figure 2.6: The bipartite pair-graph $\mathcal{G}(G, H, S)$.

Some remarks on infinite pair-graphs

In this section we consider the case G is an infinite group, H a given subgroup of G and S a subset of G such that S_H is symmetric. The definition for group-subgroup pair graph $\mathcal{G}(G, H, S)$ remains the same as in Definition 2.1.1.

The results on degree structure of Section 2.1 hold without any changes when the generating set S and the index $[G : H]$ are finite. For instance, if $G = \mathbb{Z}$, $H = 3\mathbb{Z}$ and $S = \{-6, 1, 4, 5, 6, 11\}$, then the vertices of H in the resulting pair-graph $\mathcal{G}(G, H, S)$ have degree 6 and the vertices of the cosets $3\mathbb{Z} + 1$ and $3\mathbb{Z}+2$ have degree 2. Note that when the generating set S and the index $[G : H]$ are not finite, the inequality of Corollary 2.1.8 cannot be used, otherwise the results on that section apply without changes.

The results of connectedness, and in particular Theorem 2.2.3 and Proposition 2.2.5 hold without modification. It is important to note that when the index $[G : H]$ is not finite a corresponding *connected* group-subgroup pair graph has vertices with infinite degree, in other words, the resulting graph is not *locally finite*.

When the pair-graph contains no isolated vertices, then the number of connected components is given by

$$[H : \langle S_H \cup \widetilde{S_O} \rangle]$$

as in Theorem 2.2.6. The results of Sections 2.3 on group actions and 2.3 on bipartite pair-graphs hold without changes.

2.4 Structure theorems for connected pair-graphs

For this section fix a finite group G and subgroup H. We consider three cases, depending on the choice of subset S. The first case is when S_H is empty, and the corresponding graph $\mathcal{G}(G, H, S)$ contains no degree one vertices, in other words, $|Hg \cap S| > 1$ for $g \in G - H$.

For each i we define a corresponding symmetric multiset:

$$\hat{S}_i = \{s_i s_j^{-1} | s_i, s_j \in S_i, j \neq i\},$$

and the union

$$\hat{S} = \bigcup_{i=1}^{k} \hat{S}_i.$$

Note that each set $\hat{S}_i$ has cardinality $|S_i|(|S_i|-1)$. We will consider the Cayley (multi-)graph $\mathcal{G}(H,\hat{S})$ and its barycentric division $\mathcal{G}^{(2)}(H,\hat{S})$, namely, we construct a strong graph morphism from $\mathcal{G}^{(2)}(H,\hat{S})$ to the pair-graph $\mathcal{G}(G,H,S)$. Let $\phi : \mathcal{G}^{(2)}(H,\hat{S}) \to \mathcal{G}(G,H,S)$ be defined on the vertices by

$$\phi(h) = h,$$
$$\phi((h, hs_is_j^{-1})) = hs_i,$$

where $h \in H$ and $s_is_j^{-1} \in \hat{S}$. Since the pair-graph is connected and by the definition of $\hat{S}$, it follows that this is a surjective map. Now, the induced map on the edges satisfies

$$\phi((h,(h,hs_is_j^{-1}))) = (\phi(h), \phi((h,hs_is_j^{-1}))) = (h, hs_i),$$

and the right hand side is a vertex of the pair-graph $\mathcal{G}(G,H,S)$, therefore ϕ is a graph homomorphism. Conversely, let (h,hs_i) be an edge of $\mathcal{G}(G,H,S)$ with $s_i \in S_l$. Since by assumption there are no vertices of degree one, there is a $s_j \in S_l$ such that $s_is_j^{-1} \in \hat{S}$. Now, since $(h, s_is_j^{-1})$ is an edge of $\mathcal{G}(H,\hat{S})$ and

$$\phi((h,(h,hs_is_j^{-1}))) = (h,hs_i),$$

therefore the map ϕ is a surjective *strong graph morphism*. By the homomorphism theorem for graphs, we have

$$\mathcal{G}(G,H,S) \simeq \mathcal{G}^{(2)}(H,\hat{S})/\sim_\phi,$$

where $\sim_\phi$ is the congruence induced by ϕ. Since all the congruences that we consider are of this type, we write $\sim$ for the congruence $\sim_\phi$.

Proposition 2.4.1. *Let G be a finite group, H a subgroup and S a subset of G such that S_H is empty and the corresponding pair-graph $\mathcal{G}(G,H,S)$ is connected and has no degree one vertices. Then, with the foregoing notation,*

$$\mathcal{G}(G,H,S) \simeq \mathcal{G}^{(2)}(H,\hat{S})/\sim.$$

The second case is when the pair-graph has not degree one vertices. In this case, using the proposition above we immediately get:

Proposition 2.4.2. *Let G be a finite group, H a subgroup and S a subset of G such that the corresponding pair-graph $\mathcal{G}(G,H,S)$ is connected and has no degree one vertices. Then, with the foregoing notation,*

$$\mathcal{G}(G,H,S) \simeq \mathcal{G}(H,S_H) \oplus \mathcal{G}^{(2)}(H,\hat{S_O})/\sim.$$

The operation $\oplus$ in the proposition above is the *generalized edge sum*. The vertices (resp. edges) of the resulting graph is the union of the vertices (resp. edges) of the summands.

Now, define the subset of S_O

$$\bar{S} = \bigcup_{|S_i|=1} S_i,$$

and set $\mathcal{G}_1 = \mathcal{G}(G, H, \bar{S})$. This graph contains all the degree one vertices of the pair-graph $\mathcal{G}(G, H, S)$.

Theorem 2.4.3. *Let G be a finite group, H a subgroup and S a subset of G such that the corresponding pair-graph (G, H, S) is connected. Then, with the foregoing notation,*

$$\mathcal{G}(G, H, S) \simeq \mathcal{G}(H, S_H) \oplus \mathcal{G}^{(2)}(H, \hat{S_O})/\sim \oplus\ \mathcal{G}_1.$$

2.5 Spectra of group-subgroup pair graphs

A set of apparent eigenvalues of a group-subgroup pair graph

The trivial eigenvalue of a k-regular graph is $\mu = k$ and it corresponds to any constant eigenfunction f on the vertices of the graph. By extension, the trivial eigenvalue of a Cayley graph $\mathcal{G}(G, S)$ is $\mu = |S|$. In this section we extend this notion to the group-subgroup pair graphs.

Theorem 2.5.1. *Let G be a group, H a subgroup of G of index $[G : H] = k + 1 \geq 2$, S a subset of G such that S_H is symmetric and $|S_O| \neq 0$. Then*

$$\mu^{\pm} = \frac{|S_H| \pm \sqrt{|S_H|^2 + 4\left(\sum_1^k |S_i|^2\right)}}{2} \tag{2.4}$$

are eigenvalues of the graph $\mathcal{G}(G, H, S)$. The corresponding eigenfunctions are defined by

$$f^{\pm}(y) = \begin{cases} \mu^{\pm}, & \text{if } y \in H \\ |S_i| & \text{if } y \in Hx_i, \quad i \in [k]. \end{cases}$$

Proof. From (2.4), the numbers $\mu^{\pm}$ satisfy

$$(\mu^{\pm})^2 - |S_H|\mu^{\pm} - \sum_{i=1}^{k} |S_i|^2 = 0.$$

Then, for $h \in H$, we have

$$\begin{aligned} Af^{\pm}(h) &= \sum_{s \in S} f^{\pm}(hs) \\ &= \sum_{s \in S_H} f^{\pm}(hs) + \sum_{i=1}^{k} \sum_{s \in S_i} f^{\pm}(hs) \\ &= |S_H| \mu^{\pm} + \sum_{i=1}^{k} |S_i|^2 = (\mu^{\pm})^2 \\ &= \mu^{\pm} f(h). \end{aligned}$$

Similarly, for $x \in Hx_i$, $i = 1, \dots, k$,

$$\begin{aligned} Af^{\pm}(x) &= \sum_{s \in S_i} f(xs^{-1}) \\ &= \mu^{\pm} |S_i| \\ &= \mu^{\pm} f^{\pm}(x). \end{aligned}$$

□

Note that for the case $|S_O| = 0$, μ^+ is an eigenvalue with corresponding eigenvector f^+ as defined in the above Theorem, but $f^- \equiv 0$ so it is not an eigenfunction.

Proposition 2.5.2. *The eigenvalue μ^+ is the largest eigenvalue of the graph $\mathcal{G}(G, H, S)$ with multiplicity $[H, \langle S_H \cup \widetilde{S_O} \rangle]$.*

Proof. First, consider the case of a connected pair-graph $\mathcal{G}(G, H, S)$, in particular $|S_i| \neq 0$ for all $0 \neq i \in [k]$ and the eigenfunction f^+ takes only positive values. By Theorem 8.1.4 and Corollary 8.1.5 of [9], any eigenfunction that only takes nonzero values of the same sign corresponds to the largest eigenvalue, which has multiplicity 1. The eigenfunction f^+ satisfies this condition, therefore corresponds to the largest eigenvalue and it is an eigenvalue of multiplicity one, so the statement of the proposition follows.

For the remaining case, let $h \in H$ and consider the connected component Γ_h as a subgraph of $\mathcal{G}(G, H, S)$ and note that $f^+|_{\Gamma_h}$ is an eigenfunction of Γ_h with eigenvalue μ^+. Then by the argument above, μ^+ is the largest eigenvalue of Γ_h with multiplicity 1. Now, it is well known that the characteristic polynomial $p_{\mathcal{G}}(x)$ of the graph $\mathcal{G} = \mathcal{G}(G, H, S)$ is the product of the characteristic polynomials of its connected components,

$$p_{\mathcal{G}}(x) = p_{\Gamma_{h_1}}(x) p_{\Gamma_{h_2}}(x) \dots p_{\Gamma_{h_r}}(x) x^l,$$

where r is the number of connected components of $\mathcal{G}(G, H, S)$ containing elements of H and l the number of isolated vertices. Moreover, since μ^+ is the largest root of $p_{\Gamma_{h_i}}(x)$ for each $h_i \in H$, then is the largest root of $p_{\mathcal{G}}(x)$ and therefore the largest eigenvalue of $\mathcal{G}(G, H, S)$. Furthermore, since μ^+ is a simple eigenvalue for each of the subgraphs Γ_{h_i}, then by Theorem 2.2.6 μ^+ is an eigenvalue of $\mathcal{G}(G, H, S)$ with multiplicity equal to $r = [H, \langle S_H \cup \widetilde{S_O} \rangle]$. □

Example 2.5.3. Let $G = \mathbb{Z}/12\mathbb{Z}$, $H \simeq \mathbb{Z}/4\mathbb{Z}$ as a subgroup of G and $S = \{\bar{1}, \bar{3}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}$. The pair-graph $\mathcal{G}(G, H, S)$ (shown in Figure 2.7) has the eigenvalue $\mu^+ = 4$ with multiplicity 1 and $\mu^- = -2$ with multiplicity 4, the remaining eigenvalues are $\mu = 2$ with multiplicity 2 and $\mu_0 = 0$ with multiplicity 5.

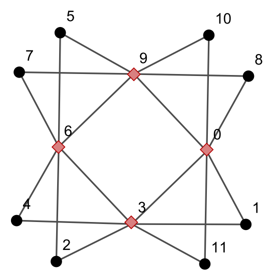

Figure 2.7: The pair-graph $\mathcal{G}(G, H, S)$ of Example 2.5.3

By Proposition 2.5.2, when S_H is empty the eigenvalue μ^- is the most negative eigenvalue of the group-subgroup pair graph. In the general case, the above example shows the eigenvalue μ^- may have higher multiplicity even when μ^+ has multiplicity 1.

From the decomposition of the characteristic polynomial of the adjacency matrix, we can obtain a lower bound for the multiplicity of the eigenvalue $\mu_0 = 0$.

Proposition 2.5.4. *Let G be a group and H a subgroup of G of index $[G : H] \geq 2$. The multiplicity of the eigenvalue $\mu_0 = 0$ of a nontrivial pair-graph $\mathcal{G}(G, H, S)$ is at least*

$$|G| - |H| - \min(|HS_O|, |H|) = \begin{cases} |G| - |H| & \text{if } S_O = \varnothing. \\ |G| - 2|H| & \text{if } S_O \neq \varnothing. \end{cases}$$

In particular, if $[G : H] > 2$, μ_0 is an eigenvalue of the pair-graph $\mathcal{G}(G, H, S)$.

Proof. First, suppose that the pair-graph $\mathcal{G}(G, H, S)$ contains isolated vertices, then from the factorization of the characteristic polynomial of the adjacency matrix we have that $\mu_0 = 0$ is an eigenvalue with multiplicity at least the number of isolated components, by Theorem 2.2.6 this number is $|G| - |H| - |HS_O|$. For a general pair-graph $\mathcal{G}(G, H, S)$, consider an eigenfunction f associated with the eigenvalue $\mu_0 = 0$ with $f(h) = 0$ for $h \in H$, then f must satisfy the $|H|$ linear equations

$$\sum_{s \in S_O} f(hs) = 0.$$

The matrix B corresponding to this system is a $|H| \times |G - H|$ matrix, then from elementary linear algebra it holds that $|H|$ is an upper bound for the rank of B.

Therefore the kernel of B has dimension at least $|G|-2|H|$, so the multiplicity of the eigenvalue $\mu_0 = 0$ is at least $|G| - 2|H|$. The result follows from considering the two cases at the same time. □

From the above discussion, for a given pair-graph $\mathcal{G}(G, H, S)$ with $[G : H] \geq 2$ there is a set $\{\mu^+, \mu^-, \mu_0\}$ of eigenvalues that are apparent from the properties of the group, subgroup and generating set.

Definition 2.5.5. *The* trivial eigenvalues *of the group-subgroup pair graph* $\mathcal{G}(G, H, S)$ *is the set given by*

- $\{|S|\}$ *when* $[G : H] = 1$, *or* $\{|S|, -|S|\}$ *if the graph is bipartite.*
- $\{\mu^+, \mu^-\}$ *when* $[G : H] = 2$.
- $\{\mu^+, \mu^-, \mu_0\}$ *when* $[G : H] > 2$.

Example 2.5.6. The pair-graph in Example 2.1.3 has $|S_O| = |S| = 16$, with four cosets of degree 2 and two cosets of degree 4, therefore the trivial eigenvalues are $\mu^{\pm} = \pm 4\sqrt{3}$, and $\mu_0 = 0$ with multiplicity bounded below by 35. The pair-graph in Example 2.3.6 has $|S_H| = 2$ and $|S_1| = |S_2| = 2$, so its trivial eigenvalues are $\mu^+ = 4$, $\mu^- = -2$ and $\mu_0 = 0$ with multiplicity at least 4.

Eigenfunctions for nontrivial eigenvalues

When the pair-graph $\mathcal{G}(G, H, S)$ is connected, the eigenfunction corresponding to the trivial eigenvalue μ^+ is constant on the cosets. The situation for the remaining eigenvalues is given in the following result.

Proposition 2.5.7. *Retain the notation of Theorem 2.5.1 and let f be an eigenvalue of the pair-graph $\mathcal{G}(G, H, S)$ associated with a nontrivial eigenvalue μ. Then, for any coset Hx_i*

$$\sum_{x \in Hx_i} f(x) = 0. \tag{2.5}$$

Moreover, if g is an eigenfunction associated with the eigenvalue $\mu_0 = 0$, then

$$\sum_{h \in H} g(h) = \sum_{i=1}^{k} |S_i| \sum_{x \in Hx_i} g(x) = 0. \tag{2.6}$$

Proof. For a fixed $s \in S_i$, we have

$$\sum_{h \in H} f(hs) = \sum_{x \in Hx_i} f(x).$$

Then, summing over all $s \in S_i$,

$$\sum_{s \in S_i} \sum_{h \in H} f(hs) = |S_i| \sum_{x \in Hx_i} f(x) \tag{2.7}$$

Note that this includes the case $Hx_0 = H$. Similarly, we see that

$$\begin{aligned} |S_i| \sum_{h \in H} f(h) &= \sum_{x \in Hx_i} \sum_{s \in S_i} f(xs^{-1}) \\ &= \mu \sum_{x \in Hx_i} f(x) \end{aligned} \tag{2.8}$$

Therefore, summing (2.7) over all S_i and S_H,

$$\mu \sum_{h \in H} f(h) = |S_H| \sum_{h \in H} f(h) + \sum_{i=1}^{k} |S_i| \sum_{x \in Hx_i} f(x) \tag{2.9}$$

Now, multiplying (2.9) by μ and using (2.8) on the right-hand side gives

$$\mu^2 \sum_{h \in H} f(h) = |S_H| \mu \sum_{h \in H} f(h) + \sum_{i=1}^{k} |S_i|^2 \sum_{h \in H} f(h).$$

If $\mu \neq 0$ and $\sum_{h \in H} f(h) \neq 0$ it follows that $\mu = \mu^{\pm}$, contradicting the hypothesis. Therefore, (2.5) follows for $\mu \neq 0$. The result (2.6) for $\mu = 0$ follows from (2.8) and (2.9). □

Proposition 2.5.8. *Let f be an eigenfunction of the pair-graph $\mathcal{G}(G, H, S)$ associated with the eigenvalue μ. If $f|_H \not\equiv 0$ and f is constant on the cosets of H then μ is a trivial eigenvalue.*

Proof. For $h \in H$, we have

$$\mu f(h) = |S_H| f(h) + \sum_{i=1}^{k} |S_i| f(x_i), \tag{2.10}$$

and

$$\mu f(x_i) = |S_i| f(h). \tag{2.11}$$

If $\mu = 0$ then $f|_H \equiv 0$, contradicting the hypothesis. Then, substituting (2.11) into (2.10) we obtain

$$f(h)(\mu^2 - \mu |S_H| - \sum_{i=1}^{k} |S_i|^2) = 0.$$

Since $f(h) \neq 0$, μ is one of the trivial eigenvalues. □

Returning to the ideas following Proposition 2.3.2, let V be the subspace of $\mathcal{L}(G)$ consisting of functions constant on the cosets of H. This is a H-invariant subspace under the permutation representation λ_H, and the restriction to this subspace corresponds to the trivial representation of H in $\mathcal{L}(G)$. Then Proposition 2.5.8 shows that any eigenspace $V_\mu \subset V$ corresponds to either one of the trivial eigenvalues $\mu^{\pm}$ or the zero eigenvalue (when $f|_H \equiv 0$).

As an application, we relate the nontrivial eigenvalues of two pair-graphs with complementary generating set.

Corollary 2.5.9. *Let S be a subset of G with $S_H = \varnothing$, and set $S' = (G-H)-S$. If f is an eigenfunction of $\mathcal{G}(G,H,S)$ associated with a nonzero eigenvalue $\mu \neq \mu^{\pm}$, then f is an eigenfunction of $\mathcal{G}(G,H,S')$ corresponding to the eigenvalue $-\mu$.*

Proof. Denote the adjacency operator of the graphs $\mathcal{G}(G,H,S)$, $\mathcal{G}(G,H,S')$ and $\mathcal{G}(G,H,G-H)$ by A, B and C respectively, so that $C = A + B$. We have

$$Bf(x) = (C - A)f(x) = Cf(x) - \mu f(x),$$

therefore it is enough to prove $Cf(x) = 0$. In other words, that

$$\sum_{h\in H} f(h) = 0,$$

$$\sum_{x\in G-H} f(x) = 0,$$

this is true by Proposition 2.5.7. □

Example 2.5.10. For $G = \mathbb{Z}/20\mathbb{Z}$, $H = \mathbb{Z}/10\mathbb{Z}$, and $S = \{\bar{3}, \bar{5}, \bar{7}\}$, $S' = \{\bar{1}, \bar{3}, \bar{5}, \bar{13}, \bar{15}, \bar{17}, \bar{19}\}$ we have $\mathcal{G}(G,H,S)$ and $\mathcal{G}(G,H,S')$ pair-graphs shown in Figure 2.8.

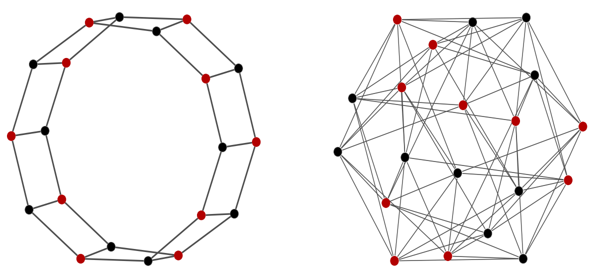

Figure 2.8: The pair-graphs with the same nontrivial eigenvalues, shown in Table 2.1.

λ_i	μ_i
3	7
$\frac{1}{2}(3+\sqrt{5})$	$\frac{1}{2}(3+\sqrt{5})$
$\frac{1}{2}(3+\sqrt{5})$	$\frac{1}{2}(3+\sqrt{5})$
$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
1	1
$\frac{1}{2}(-1+\sqrt{5})$	$\frac{1}{2}(-1+\sqrt{5})$
$\frac{1}{2}(-1+\sqrt{5})$	$\frac{1}{2}(-1+\sqrt{5})$
$\frac{1}{2}(3-\sqrt{5})$	$\frac{1}{2}(3-\sqrt{5})$
$\frac{1}{2}(3-\sqrt{5})$	$\frac{1}{2}(3-\sqrt{5})$

Table 2.1: Table of nontrivial eigenvalues for the pair-graphs of Figure 2.8.

The table 2.1 contains the positive eigenvalues for both of the graphs. Since both graphs are bipartite the remaining eigenvalues correspond to the negatives of the ones shown. Note that $S \cup S' \neq G - H = \{\bar{1}, \bar{3}, \bar{5}, \ldots, \bar{19}\}$, but $S'' = R_4(S) = \{\bar{7}, \bar{9}, \bar{11}\}$ is such that $\mathcal{G}(G, H, S) \cong \mathcal{G}(G, H, S'')$ by Proposition 2.3.4, and $S'' \cup S' = G - H$.

When the subgroup is of index 2, the sum over the elements of any coset is zero for an eigenfunction of the corresponding pair-graph, including those associated with the zero eigenvalue. Therefore, the result of Corollary 2.5.9 holds for any nontrivial eigenvalue for the index 2 case. This is further explored in section 3.1.

Chapter 3

Applications

3.1 Spectra of regular pair-graphs and Ramanujan graphs

Nontrivial regular pair-graphs $\mathcal{G}(G,H,S)$ are bipartite when $[G:H]=2$. The spectra of these graphs is symmetric about 0 and the largest eigenvalue is the trivial eigenvalue $\mu^+=|S|$.

Let G be a finite group of order $2n$ and H the subgroup of index 2. Then, for any subset $S\subset G-H$ with $|S|=k$, let $S'=(G-H)-S$. We have $|S'|=n-k$ and any constant function f is an eigenfunction of both of the pair-graphs $\mathcal{G}(G,H,S)$ and $\mathcal{G}(G,H,S')$ corresponding to $\mu_1=k$ and $\lambda_1=n-k$, respectively. Similarly, for $c\in\mathbb{C}^\times$, the function $f=c(\delta_H-\delta_{G-H})$ is an eigenfunction of $\mathcal{G}(G,H,S)$ and $\mathcal{G}(G,H,S')$ corresponding to $\mu_{2n}=-k$ and $\lambda_{2n}=k-n$.

Lemma 3.1.1. *Let G be a group, H a subgroup of index 2 and S a subset of $G-H$ with $|S|=k$. Set $S'=(G-H)-S$. If the pair-graph $\mathcal{G}(G,H,S)$ is not connected, then there are independent eigenfunctions f and g of $\mathcal{G}(G,H,S)$ associated to $\mu=\pm k$ such that $f-g$ is an eigenfunction of $\mathcal{G}(G,H,S')$ corresponding to the eigenvalue $-\mu$.*

Proof. With the same notation as in the proof of Corollary 2.5.9, for a connected component Γ of $\mathcal{G}(G,H,S)$, consider the function $f=\delta_\Gamma$ or $f=\delta_{\Gamma\cap H}-\delta_{\Gamma-H}$, which can be verified to be eigenfunctions corresponding to $\mu=k$ and $\mu=-k$, respectively. We can similarly define g with respect to a different connected component Ω of $\mathcal{G}(G,H,S)$, then clearly f and g are linearly independent. Note that there are no isolated vertices on the graph, therefore by Proposition 2.2.5, all the connected components have the same cardinality, in particular $|\Gamma\cap H|=|\Omega\cap H|$ and $|\Gamma-H|=|\Omega-H|$. Then, we have

$$Cf(h)=\sum_{x\in G-H}f(x)=\sum_{x\in\Gamma-H}f(x)\qquad\text{for } h\in H,$$
$$Cf(x)=\sum_{h\in H}f(h)=\sum_{h\in\Gamma\cap H}f(h)\qquad\text{for } x\in G-H.$$

It follows that $Cf=\delta_H|\Gamma-H|+\delta_{G-H}|\Gamma\cap H|$ or $Cf=-\delta_H|\Gamma-H|+\delta_{G-H}|\Gamma\cap H|$ depending on the whether $\mu=k$ or $\mu=-k$. Then it is clear that $C(f-g)=0$ and

$$B(f-g)=(C-A)(f-g)=C(f-g)-A(f-g)=-\mu(f-g).$$

□

By Theorem 2.5.1, when $\mathcal{G}(G,H,S)$ is not connected the eigenvalue $\mu = k$ has multiplicity equal to the number c of connected components of $\mathcal{G}(G,H,S)$, then by Lemma 3.1.1 the graph $\mathcal{G}(G,H,S')$ also has the eigenvalue $\mu = k$ with multiplicity $c-1$. For regular pair-graphs we can reformulate the results of Corollary 2.5.9 and Lemma 3.1.1 as follows

Theorem 3.1.2. *Let G be a group of order $2n$, H a subgroup of index 2 and S a subset of $G-H$ with $|S| = k$. Suppose that $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_{2n}$ is the spectrum of the pair-graph $\mathcal{G}(G,H,S)$. Then there is a $(n-k)$-regular pair-graph $\mathcal{G}(G,H,S')$ with spectrum $\mu_1 \geqslant \mu_2 \geqslant \ldots \geqslant \mu_{2n}$ such that*

$$\lambda_i = \mu_i$$

for $i \neq 1, 2n$.

Remark 3.1.3. Theorem 3.1.2 defines a relation between the nontrivial spectra of graphs for complementary choices of S. Moreover, Example 2.5.10 shows that for a k-regular graph $\mathcal{G}(G,H,S)$, there can be more than one $(n-k)$-regular $\mathcal{G}(G,H,S')$ graph with the same nontrivial spectrum. In fact, if we find one, by using Proposition 2.3.4 with right actions of H we can obtain families of graphs with the same nontrivial spectrum.

Recall that a Ramanujan graph is a connected k-regular graph with the property

$$|\mu| \leqslant 2\sqrt{k-1},$$

for any eigenvalue μ different from $\pm k$.

Corollary 3.1.4. *Suppose that $[G:H] = 2$. Then a nontrivial regular connected pair-graph $\mathcal{G}(G,H,S)$ is a Ramanujan graph when*

$$|S| \geqslant n + 2 - 2\sqrt{n},$$

Proof. By Theorem 3.1.2, any k-regular pair-graph $\mathcal{G}(G,H,S)$ has nontrivial eigenvalues μ satisfying $|\mu| \leqslant \min\{k, n-k\}$. Also, the pair-graph $\mathcal{G}(G,H,S)$ is a Ramanujan graph when said trivial eigenvalues satisfy $|\mu| \leqslant 2\sqrt{k-1}$. Considering the two inequalities, it follows that all k-regular pair-graphs $\mathcal{G}(G,H,S)$ with $k \leqslant 2$ or $k \geqslant n + 2 - 2\sqrt{n}$ are Ramanujan graphs. □

Example 3.1.5. Let $G = \mathfrak{S}_4$, $H = A_4$. The set $S = \{(1,2), (1,3), (2,4), (3,4), (1,2,3,4), (1,3,2,4), (1,4,2,3), (1,4,3,2)\}$ is such that $|S| = 8$ satisfy the bound of the corollary, so the corresponding $\mathcal{G}(G,H,S)$ graph is Ramanujan. Its spectrum consist of ± 8 with multiplicity 1, ± 4 with multiplicity 2 and 0 with multiplicity 18. Note that it contains the eigenvalues ± 4 and as expected by Theorem 3.1.2, the corresponding complementary 4-regular graph, generated by $S' = \{(1,2), (3,4), (1,3,2,4), (1,4,2,3)\}$ has 3 connected components. Both of the pair-graphs are shown in Figure 3.1.

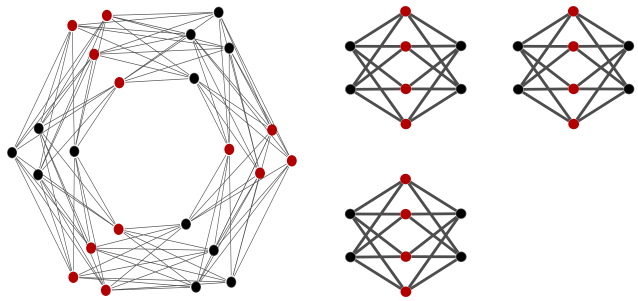

Figure 3.1: The Ramanujan pair-graph $\mathcal{G}(\mathfrak{S}_4, A_4, S)$ and its complementary pair-graph $\mathcal{G}(\mathfrak{S}_4, A_4, (\mathfrak{S}_4 - A_4) - S)$

Example 3.1.6. Let $G = \mathrm{GL}_2(\mathbb{F}_3)$ and $H = \mathrm{SL}_2(\mathbb{F}_3)$. Then $|G| = 48$ and $|H| = 24$, in this case by Corollary 3.1.4, for any subset S with $|S| \geqslant 17$, the resulting pair-graph $\mathcal{G}(G, H, S)$ graph is Ramanujan. For a particular choice of S we obtain the 17-regular Ramanujan pair graph $\mathcal{G}(G, H, S)$ shown in Figure 3.2. The corresponding pair-graph $\mathcal{G}(G, H, (G-H)-S)$, also shown on the same figure, generated by the complement of S in $G - H$, is a 7-regular Ramanujan graph. This shows that the result of Corollary 3.1.4 is not a necessary condition.

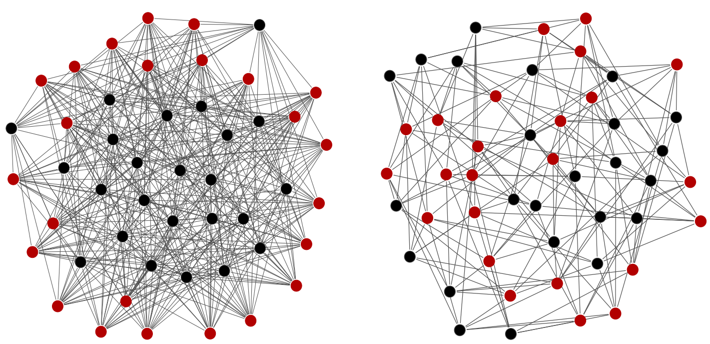

Figure 3.2: The Ramanujan pair-graphs $\mathcal{G}(G, H, S)$ and $\mathcal{G}(G, H, (G-H)-S)$.

Since for a group G with a subgroup H of index 2, the class of regular connected (bipartite) pair-graphs $\mathcal{G}(G, H, S)$ is an strict superset of that of bipartite connected Cayley graphs $\mathcal{G}(G, S)$, Corollary 3.1.4 results in Ramanujan graphs that are not Cayley graphs for the given group.

3.2 Linear error-correcting codes

One of the problems of information theory is that of transmission of information reliably over a noisy channel. We will consider only the binary symmetric channel, that is, the information is represented by elements of $\mathbb{F}_2^l$ for some positive integer l and each bit is flipped during transmission with a given probability p. In order to correct the error on the transmission the source message $m \in \mathbb{F}_2^k$ is encoded into a codeword $c \in \mathbb{F}_2^n$ with $n \geq k$ by adding redundancy, in other words,

$$c = Gm$$

for some transformation G. The redundancy added is used by the decoder to recover a decoded message $\hat{m} \in \mathbb{F}_2^k$ from the received message $r \in \mathbb{F}_2^n$. The transmission is successful if m and $\hat{m}$ are (approximately) equal. The ratio $\frac{k}{n}$ of the lengths of the source message and the codeword is called information rate of the code.

When the transformation G is linear, we say that the code is linear. In practice, a linear code $\mathcal{C}$ of type (n, k) is a k dimensional $\mathbb{F}_2$-vector subspace of $\mathbb{F}_2^n$. The code corresponds to the image of G in the foregoing discussion. The matrix representation $\mathbf{G} \in \mathrm{Mat}_{k,n}(\mathbb{F}_2)$ of G is called the generator matrix of the code, and any matrix $\mathbf{H} \in \mathrm{Mat}_{n-k,n}(\mathbb{F}_2)$ such that

$$\mathbf{H}^{\mathrm{t}}\mathbf{G} = 0$$

is called a parity-check matrix of the code. Therefore, the parity-check matrix can be interpreted as a set of linear conditions that an element $t \in \mathbb{F}_2^n$ must satisfy in order to be an element of $\mathcal{C}$. It is clear then that a linear code $\mathcal{C}$ is determined by its parity-check matrix.

The *Tanner graph* $\mathcal{T}$ of $\mathcal{C}$ is a graph that represents the parity-check matrix of a linear code $\mathcal{C}$. The vertices of $\mathcal{T}$ consist of two sets P and C. Each vertex p of P represents a parity-check condition of the code and each vertex c of C represents a bit of the codeword, in other words, they represent rows and columns of $\mathbf{H}$, respectively. The vertices p and c are adjacent if the corresponding entry of H is nonzero, it follows that the Tanner graph $\mathcal{T}$ is a bipartite graph. Conversely, from a bipartite graph $\mathcal{G}$ one may define a linear code $\mathcal{C}$ by taking as P and C the bipartition of the vertices. If the cardinalities of P and C are n and l, respectively, the associated code is a $(n-l, n)$-type code. For detailed information on linear codes and Tanner graphs, the reader is referred to [10] or [13].

For a group G, subgroup H of index $[G : H] > 2$ and generating set S with $S_H = \varnothing$, the corresponding pair-graph $\mathcal{G}(G, H, S)$ is bipartite. The code associated with the pair-graph $\mathcal{G}(G, H, S)$, denoted by $\mathcal{C}(G, H, S)$, is a $(|G| - 2|H|, |G - H|, 2)$-type code with information rate $r = \frac{[G:H]-2}{[G:H]-1}$. The parity-check matrix $\mathcal{H}$ of this code is the submatrix of the adjacency matrix of $\mathcal{C}(G, H, S)$ corresponding to the rows associated with elements H and the columns associated with elements $G - H$.

Example 3.2.1. Consider $G = \mathbb{Z}/20\mathbb{Z}$, $H \simeq \mathbb{Z}/5\mathbb{Z}$ the subgroup of index $[G : H] = 4$ and $S = \{\bar{1}, \bar{2}, \bar{3}, \bar{7}, \bar{9}\}$. In this case, the rate of the resulting code $\mathcal{C}(G, H, S)$ is $r = \frac{3}{4}$. The resulting pair-graph $\mathcal{G}(G, H, S)$ and the Tanner graph representation of the resulting code are shown in Figure 3.3.

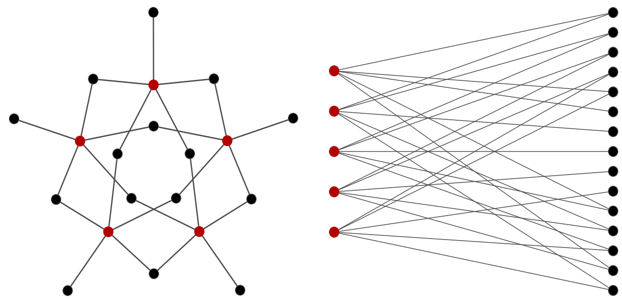

Figure 3.3: The Tanner graph representation of the code

The class of *low-density parity check (LDPC)* codes, or *Gallager codes*, consists of linear codes with sparse parity-check matrices, or equivalently, with sparse graph representation. Gallager codes are good codes in the sense of minimum distance between codewords. Gallager codes are divided into regular, where the vertices in each partition have the same degree, and irregular, with no restriction on the degree of the vertices. Irregular Gallager codes are known to perform better than regular ones at decoding [12]. From the results of Section 2.1 one can see that both regular and irregular Gallager codes may be modeled using group-subgroup pair graphs. Moreover, the sparsity of the code $\mathcal{C}(G,H,S)$ may be measured by $\frac{|S|}{|G-H|-|H|}$, the proportion of nonzero entries of the associated parity-check matrix.

Example 3.2.2. Set $G = \mathrm{GL}_2(\mathbb{F}_5)$, where $\mathbb{F}_5$ is the finite field of 5 elements and $H = \mathrm{SL}_2(\mathbb{F}_5)$, then for a particular subset S of 7 elements taken from the complement of H in G, we obtain the pair-graph $\mathcal{G}(G,H,S)$ shown in Figure 3.4. The resulting pair-graph is a connected graph consisting of 480 vertices of degrees $2,3$ and 7. This pair-graph is associated with a $(240,360)$-type code $\mathcal{C}(G,H,S)$ of rate $\frac{2}{3}$ and with a proportion on nonzero entries on the parity-check matrix of $\frac{7}{360} \approx 0.019$.

According to the general theory, Gallager codes associated with group-subgroup pair graphs are good in the sense of minimum distance, nevertheless it would be desirable to study the performance of encoding and decoding for particular choices of group G, subgroup H and generating set S.

3.3 Full spectrum of generalized cycle graph

In this section we consider the pair-graph $C_{2n,m} = \mathcal{G}(\mathbb{Z}/(n(m+1)\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, S)$, where S is a subset with $S_H = \varnothing$ and $|S_i| = 2$. We call $C_{n,m}$ the *generalized cycle* of length $2n$ and degree m. The degree of the vertices of H is $2m$ and of $G-H$ is 2, therefore the number of edges of the graph is $2nm$. When $m=1$ we have the usual cycle graph C_{2n}. Note that a cycle with no repeated vertices in

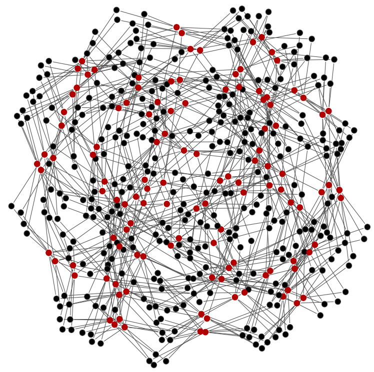

Figure 3.4: The pair-graph $\mathcal{G}(\mathrm{GL}_2(\mathbb{F}_5), \mathrm{SL}_2(\mathbb{F}_5), S)$.

$C_{2n,m}$ is of length 4 or $2n$. Figure 3.5 shows the generalized cycle $C_{8,2}$, note that it has 12 vertices and 16 edges.

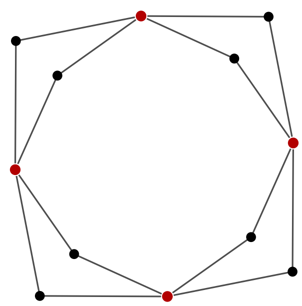

Figure 3.5: The generalized cycle $C_{8,2} = \mathcal{G}(\mathbb{Z}/(12\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, S)$.

In this section we use the structure theorem of section 2.4 to compute the spectrum of $C_{2n,m}$.

Theorem 3.3.1. *The spectrum of $C_{2n,m}$ is given by*

$$\pm\sqrt{2m(1+\cos(\frac{2\pi x}{n}))},$$

for $x = 0, 1, 2, \ldots, n-1$ and the eigenvalue 0 *with multiplicity $n(m-1)$.*

Proof. We note that the pair-graph $\mathcal{G}(G, H, S)$, with $G = \mathbb{Z}/(n(m+1)\mathbb{Z}$ and $H = \mathbb{Z}/n\mathbb{Z}$, is isomorphic to $\mathcal{G}^{(2)}(H, \hat{S})$ by Proposition 2.4.1. We claim that actually the pair-graph is isomorphic to $\mathcal{G}^{(2)}(H, \tilde{S})$. Since the map ϕ is surjective, it is enough to check that the vertex and edge sets have the same cardinality. By the remark after the definition of $\hat{S}_i$, we have that $|\hat{S}| = 2m$. Then the Cayley graph $\mathcal{G}(H,\hat{S})$ has nm edges, therefore the barycentric division $\mathcal{G}^{(2)}(H,\hat{S})$ has $n(m+1)$ vertices and $2nm$ edges, which proves the claim.

Now, the eigenvalues of $\mathcal{G}(H,\hat{S})$ are given by

$$\lambda_i = \sum_{s\in\hat{S}} \chi_i(s),$$

where χ_i is an irreducible character of H. Now, we note that $\mathcal{G}(H,\hat{S})$ is isomorphic to the Cayley graph $\mathcal{G}(H,R)$ where the multiset R contains the elements $\{-1,1\}$ with multiplicity m. Using this and the explicit form of the irreducible characters of H, we have

$$\lambda_i = 2m\cos(\frac{2\pi x}{n}),$$

with $x = 0,1,2,\ldots,n-1$. Finally, using a theorem of Hashimoto ([7], page 231 Cor. 3.18), the eigenvalues of $\mathcal{G}^{(2)}(H,\hat{S})$ are given by

$$\pm\sqrt{\lambda_i + 2m} = \pm\sqrt{2m(1+\cos(\frac{2\pi x}{n}))},$$

for $x = 0,1,2,\ldots,n-1$ and 0 with multiplicity $n(m-1)$. □

Note that is key to the result above the fact that the pair-graph $C_{n,m}$ is isomorphic to $\mathcal{G}^{(2)}(H,\hat{S})$, in other words, the the fiber of $x \in G-H$ of the canonical inclusion

$$\eta : \mathcal{G}^{(2)}(H,\hat{S}) \to \mathcal{G}(G,H,S) = C_{n,m}$$

consists of only one element.

Future works

In this work we introduced the group-subgroup pair-graph as an extension of Cayley graphs. From this point of view we proved the basic properties of the pair-graphs by analogy of those of Cayley graphs, and naturally this approach also suggests some further topics of study of pair-graphs.

Harmonic analysis on pair-graphs

As mentioned in the Introduction, a regular graph $\mathcal{G}$ is vertex-transitive, therefore we can regard it as a homogeneous space $\mathcal{G} = G/H$, where G is a group of automorphisms of the graph and H is the stabilizer of a vertex. Then one can use the representation theory of homogeneous spaces to obtain a decomposition of the adjacency operator A of the graph $\mathcal{G}$ in terms of irreducible components of G. In the case of Cayley graphs, the identification as a homogeneous space is trivial and the relation between the eigenvalues of the adjacency operator and the irreducible representations of G is well known. For more information of this approach, the reader is referred to [5].

In principle, this approach cannot be used for pair-graphs as they are non-regular in general, and therefore not vertex-transitive. Yet, as shown in section 2.5, there is a relation between the eigenvalues of the adjacency operator and the representation of the subgroup H. In particular, the trivial eigenvalues were related to the trivial representation of H. Moreover, in Section 2.4 we showed how the structure of the pair-graph is related to certain Cayley graphs on H, and in Section 3.3 we used a particular case of this relation to compute the eigenvalues of the generalized cycle graph in terms of irreducible characters of H. It would interesting to see if these kind of results can be extended to more general choices of group, subgroup and generating set. This kind of results would be important for several problems, including random walks on pair-graphs.

Explicit construction of expanders and Ramanujan graphs

In Section 3.1, we presented a way of constructing bipartite Ramanujan pair-graphs $\mathcal{G}(G, H, S)$ that do not arise as Cayley graphs $\mathcal{G}(G, S)$. Moreover, the bipartite $X^{p,q}$ graphs of Lubotzky, Phillips and Sarnak can be considered as group-subgoup pair-graphs. Therefore, there maybe a way to construct new families of Ramanujan graphs (or expander graphs) using group-subgroup pair-graphs. We would, however, need to have more detailed information on the relation between the representations of the group and subgroup and the eigenvalues of the graph, as described above.

On the other hand, the concept of expander and Ramanujan graphs can be expanded to nonregular graphs (see for example, [7]), so it would be interesting to consider the construction of families of nonregular expanders and Ramanujan graphs using pair-graphs in the way that Cayley graphs were used to construct Ramanujan graphs.

Concrete construction of pair-graph based codes

In Section 3.2 we briefly described how pair-graphs may be used to model error-correcting codes and give some formulas of the basic parameters of the resulting codes, in particular to show that we can obtain Low density parity check codes using this method. However, in order for a code to be useful in practice we would need to have some estimates of the performance of decoding under the known algorithms, for example the algorithm of belief propagation. This requires understanding of the geometry of the resulting Tanner graph, in particular the length of circuits and the girth of the graph. This suggests the study of girth and diameter, among other graph properties, of pair-graphs in terms of the group, subgroup and generating set.

Appendix A

Relation with group-subgroup matrices

The motivation for the group-subgroup pair graph comes from the extension of the group determinant for group-subgroup pairs, called *wreath determinant for group-subgroup pairs*. In this appendix we show how one can relate the adjacency matrix of a Cayley graph with the group matrix of the corresponding group; then, by extending the idea for the matrix used for the wreath determinant for group-subgroup pairs we obtain the rows corresponding to the subgroup on the adjacency matrix of a certain group-subgroup pair graph, which is enough to determine the complete adjacency graph.

For a group $G = \{g_1, \ldots, g_n\}$, consider a polynomial ring R containing the indeterminates x_{g_i}, for $g_i \in G$, then the *group matrix* is a matrix $\mathcal{M}(G,\phi)$ in $\mathrm{Mat}_{n,n}(R)$ defined by

$$\mathcal{M}(G,\phi)_{i,j} = x_{g_i^{-1}g_j}$$

for $i,j \in [n]$ and where $\phi : G \to [n]$ is an enumeration function for G, used implicitly. The determinant $\Theta(G)$ of the group matrix is called *group determinant* of G and does not depend on the chosen enumeration of the elements of G. For i,j we have $(g_i^{-1}g_j)^{-1} = g_j^{-1}g_i$, therefore for any element x_g, the corresponding transpose element is $x_{g^{-1}}$.

Similarly, for a group G of order kn, and subgroup H of order n we define the matrix $\mathcal{M}(G,H,\phi,\tau) \in \mathrm{Mat}_{n,kn}(R)$ by

$$\mathcal{M}(G,H,\phi,\tau)_{i,j} = x_{h_i^{-1}g_j},$$

for $h_i \in H$, $g_j \in G$, $i \in [n], j \in [nk]$ and where $\phi : G \to [nk]$ and $\tau : H \to [n]$ are enumerations functions for G and H. Note that by considering only the columns corresponding to elements of H of the matrix $\mathcal{M}(G,H,\phi,\tau)$ one obtains the group matrix of H with respect to the orderings τ and $\phi|_H$.

For a matrix $A \in M_{n,kn}$, the wreath determinant of A is defined as

$$\mathrm{wrdet}_k(A) = \det{}^{-\frac{1}{k}}(A_{[k]}),$$

where $A_{[k]}$ is the row k-flexing of the matrix A and $\det^{\alpha}$ is the α-determinant. Note that wreath determinant is defined for rectangular matrices where the number of columns (resp. rows) is a multiple of the number of rows (resp.

columns). For an extensive exposition of the wreath determinant and its properties the reader is referred to [8]. In the paper [6], the authors define the wreath determinant for the pair G and H by

$$\Theta(G, H, \phi, \tau) = \mathrm{wrdet}_k(\mathcal{M}(G, H, \phi, \tau)).$$

In contrast with the ordinary group determinant, this wreath determinant for G and H depends on the enumeration functions ϕ and τ.

For a given group G and symmetric subset S, by evaluating the corresponding group matrix $\mathcal{M}(G, \phi)$ by the rule

$$\begin{cases} x_s = 1 & \text{if } s \in S \\ x_g = 0 & \text{if } g \notin S \end{cases}, \tag{A.1}$$

one obtains a symmetric matrix. Furthermore, since $g_i^{-1} g_j = s$ implies $g_i s = g_j$, the corresponding matrix is the adjacency matrix of the Cayley graph $\mathcal{G}(G, S)$.

Example A.0.2. Consider $\mathfrak{S}_3$, the symmetric group on three letters with the ordering ϕ given by $\mathfrak{S}_3 = \{e, (2,3), (1,2), (1,2,3), (1,3,2), (1,3)\}$, the group matrix is

$$\mathcal{M}(\mathfrak{S}_3, \phi) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_4 & x_3 & x_6 & x_5 \\ x_3 & x_5 & x_1 & x_6 & x_2 & x_4 \\ x_5 & x_3 & x_6 & x_1 & x_4 & x_2 \\ x_4 & x_6 & x_2 & x_5 & x_1 & x_3 \\ x_6 & x_4 & x_5 & x_2 & x_3 & x_1 \end{pmatrix},$$

where x_i stands for x_{g_i}. Set $S = \{(1,2), (1,2,3), (1,3,2)\}$, then evaluating by the rule (A.1) we get

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

which can be verified to be the adjacency matrix of the Cayley graph $\mathcal{G}(\mathfrak{S}_3, S)$.

Likewise, for group G, subgroup H and subset S as in definition 2.1.1, by evaluating the matrix $\mathcal{M}(G, H, \phi, \tau)$ using the rule (A.1) we obtain a matrix with nonzero entries (i, j) when $h_i^{-1} g_j = s \in S$. In other words, there are ones in the matrix exactly when $h_i s = g_j$, which is the relation for the edges of the group-subgroup pair graph $\mathcal{G}(G, H, S)$ in definition 2.1.1. The resulting matrix corresponds to the rows associated with the elements of H in the adjacency matrix of the pair-graph $\mathcal{G}(G, H, S)$ and can be completed by symmetry to obtain the complete adjacency matrix.

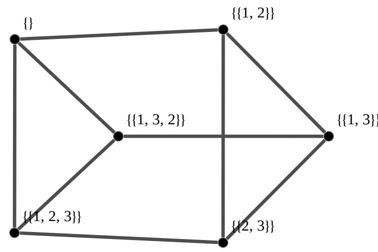

Figure A.1: The Cayley graph $\mathcal{G}(\mathfrak{S}_3, S)$.

Example A.0.3. Let $G = \mathbb{Z}/12\mathbb{Z}$, $H = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, and $S = \{\bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ as in Example 2.1.2, the corresponding matrix with respect to natural orderings ϕ and τ is

$$\mathcal{M}(\mathbb{Z}/12\mathbb{Z}, H, \phi, \tau) =$$
$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} \\ x_9 & x_{10} & x_{11} & x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} & x_0 & x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} & x_0 & x_1 & x_2 \end{pmatrix}.$$

Then, evaluating using (A.1), we get

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

which can be verified to correspond to the rows associated with elements of H in the adjacency matrix of the pair-graph $\mathcal{G}(\mathbb{Z}/12\mathbb{Z}, H, S)$ of Example 2.1.2.

Note that in order to be able to complete the matrix by symmetry it is necessary that $S_H = S \cap H$ is symmetric, otherwise the submatrix corresponding to elements of H is not symmetric. Also, when the group matrix is defined by $(x_{g_i g_j^{-1}})$ the resulting Cayley graph is defined by left multiplication, the same is true for the group-subgroup matrix for the wreath determinant and the group-subgroup pair graph.

Acknowledgements

This document would not have been possible without the support of several individuals and organizations. The following list is not complete and I would like to extend an apology to anyone who is omitted from it.

First, I would not have the opportunity to be writing this thesis without the financial support from the Japanese Government (MONBUKAGAKUSHO MEXT) scholarship.

My most sincere gratitude to Professor Masato Wakayama for his guidance as a supervisor, and for providing the motivation to this research and the invaluable discussions and support.

I have not enough words of gratitude to the members of the Wakayama seminar at Kyushu university, in particular to Hiroto Inoue, Genki Shibukawa and Kei Hamamoto, for their support as classmates, collaborators and more importantly, as friends.

I would also like to take this opportunity to thank the staff of the Graduate School of Mathematics Office and Integrated Sciences for Global Society Student Office for the support and seemingly undepletable patience at my requests.

Finally, it would be unforgivable not to mention the invaluable support I have received from my family. In particular, I dedicate this work to my mother and brother, from whom I received much encouragement, love and motivation. Muchas gracias por todo.

The computations and diagrams were elaborated using Mathematica 9.0 Student Edition. The source files for the diagrams can be downloaded from

http://www2.math.kyushu-u.ac.jp/˜ma213054/files/figures.nb.

Bibliography

[1] Norman Biggs, *Algebraic graph theory*, Cambridge Mathematical Library, 1996.

[2] Arthur Cayley, *Desiderata and suggestions: No. 2. the theory of groups: Graphical representations*, American Journal of Mathematics **1** (1878), no. 2, 174–176.

[3] H. S. M. Coxeter and W. O. J Moser, *Generators and relations for discrete groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 14, Springer Berlin Heidelberg, 1972.

[4] Guiliana Davidoff, Peter Sarnak, and Alain Valette, *Elementary number theory, group theory and Ramanujan graphs*, Cambridge University Press, London Mathematical Society student texts; 55, 2003.

[5] David Gurarie, *Symmetries and Laplacians. introduction to harmonic analysis, group representations and applications*, Dover Publications, 1992.

[6] Kei Hamamoto, Kazufumi Kimoto, Kazutoshi Tachibana, and Masato Wakayama, *Wreath determinants for group-subgroup pairs*, Journal of Combinatorial Theory, Series A **133** (2015), 76–96.

[7] Ki-ichiro Hashimoto, *Zeta functions of finite graphs and representations of p-adic groups*, Advanced Studies in Pure Mathemathics 15, Automorphic forms and geometry of arithmetics varieties **15** (1989), 211–280.

[8] Kazufumi Kimoto and Masato Wakayama, *Invariant theory for singular α-determinants*, Journal of Combinatorial Theory, Series A **115** (2008), 1 – 31.

[9] Ulrich Knauer, *Algebraic graph theory: morphisms, monoids, and matrices*, De Grutier studies in mathematics ; 41, 2011.

[10] Dave K. Kythe and Prem K. Kythe, *Algebraic and stochastic coding theory*, CRC Press, 2012.

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

[12] M. Luby, M. Mitzenmacher, D. Spielman M.A. Shokrollahi, and V. Stemann, *Practical loss-resilient codes*, Proceedings of the 29th annual ACM Symposium on Theory of Computing (1997), 150–159.

[13] David J.C. Mackay, *Information theory, inference, and learning algorithms*, Cambridge University Press, 2003.

[14] G. A. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their applications to the design of expanders and concentrator*, Journal Problems of Information Transmission **24,1** (1988), 51–60.

[15] Cid Reyes-Bustos, *Cayley-type graphs for group-subgroup pairs*, preprint (2015).

[16] Toshikazu Sunada, *Fundamental groups and Laplacians*, Proc. Taniguchi Symp. "Geometry and Analysis on Manifolds", Springer Lect. Notes in Math. **1339** (1987), 248–277.

[17] Audrey Terras, *Fourier analysis in finite groups and applications*, London Mathematical Society Sudent Texts, vol. 43, Cambridge Mathematical Library, 1999.