Circulant Graphs and Their Spectra

A Thesis
Presented to
The Division of Mathematics and Natural Sciences
Reed College

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Arts

Julia F. Lazenby

May 2008

Approved for the Division
(Mathematics)

_____

David Perkinson

Acknowledgements

The research for this thesis began under the clever guidance of Terry Bisson at Canisius College, and continued under the patient encouragement of Daniel Bump and Dave Perkinson. Writing this thesis was one of the most exciting and rewarding experiences I have had as a student, and I know that I have these three professors to thank for that. I also know that my four years at Reed would not have been the same without the encouragement, support, and welcome distractions from my parents, grandparents, knitting-night friends, and Steve. Thank you. Research for this study was supported by a Reed College Undergraduate Research Initiative Grant.

Table of Contents

Abstract

This thesis examines the eigenvalues of the adjacency matrix of Cayley graphs of cyclic groups and their relationship to graph isomorphisms. In the first chapter, I will give new criteria for which Cayley graphs of cyclic groups of any order can be completely determined–up to isomorphism–by the eigenvalues of their adjacency matrices. In the second chapter, I will present a new construction for nonisomorphic Cayley graphs of cyclic groups of order $2^r p$ for some integer $r \geq 2$ and an odd prime p that have the same list of eigenvalues.

Introduction

When I tell people that my thesis is on graph theory they usually smile knowingly and say, "Oh. Okay." I have seen this look often and have learned to assume that their minds are drifting back to their first algebra class when they were presented with $y = 2x + 3$ and asked to draw it on a piece of graph paper. While my thesis has nothing to do with slopes, midpoints, or y-intercepts, anybody who has asked about my thesis should not be scared away. If we think back to our first exposure to graphs we can remember putting a dot at $(0, 3)$ and then at (2,7) and (-1,1), and once we had enough dots, we would draw lines between them. Therein lies the connection between the graphs of this thesis and the graphs of seventh grade: dots and lines.

0.1 Graphs and Types of Graphs

In the graphs of this thesis it does not matter where you draw the dots. All that really matters is how many dots you draw and which dots you choose to connect. Perhaps some more formal definitions will be helpful at this point.

Definition 0.1.1. A *graph* X is a nonempty set of vertices, $V(X)$, and a set of edges, $E(X)$, which consist of pairs of elements of $V(X)$. If $\{v_1, v_2\} \in E(X)$, then v_1 is said to be *adjacent* to v_2. The graph X is said to be a *directed graph* (*digraph*) if elements of $E(X)$ are ordered pairs, and *undirected* if they are not.

Note that if X is undirected and $\{v_1, v_2\} \in E(X)$, then v_2 is also adjacent to v_1. However, if X is directed, then v_2 need not be adjacent to v_1. This thesis focuses on directed graphs. So, whenever the word "graph" is used it will be referring to a directed graph unless otherwise stated. Fortunately, no statements made in this thesis will exclude the possibility of an undirected graph since undirected graphs can be seen as a special type of directed graph where $\{v_1, v_2\}$ is an element of the edge set iff $\{v_2, v_1\}$ is an element of the edge set.

The graphs defined above are often referred to as *simple graphs*. There are other graphs known as multigraphs and pseudographs. The definition of these graphs varies quite a bit in the literature (especially for the multigraph). For this paper I will use the definitions I find to be the most common.

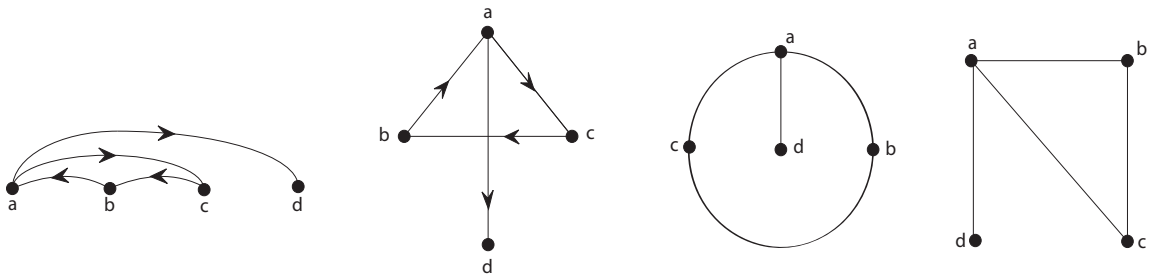
Definition 0.1.2. A *multigraph* is a graph that allows for the edge set to be a multiset. A *pseudograph* is a graph that allows for the edge set to be a multiset and for elements of the vertex set to be adjacent to themselves. Thus, $\{v, v\}$ could be an element of the edge multiset of a pseudograph. Such edges are called *loops*.

It is often helpful to visualize a graph as a diagram. To draw a graph, simply draw a dot (or any shape you see fit) for each vertex and then draw a line connecting each adjacent pair of vertices. Draw arrows for edges in directed graphs to signify order.

Example 0.1.1. Let X be a graph where

$$\begin{aligned} V(X) &= \{a, b, c, d\} \\ \text{and} \quad E(X) &= \{\{a, c\}, \{c, b\}, \{b, a\}, \{a, d\}\}. \end{aligned}$$

Here are four different ways to draw X. (The first two are directed graphs, and the second two are undirected graphs.)



Seeing as how there are so many different ways to represent the same graph, it is important to have a concept of which graphs really are the same.

Definition 0.1.3. Two graphs X and Y are said to be *isomorphic* if there exists a bijection φ from $V(X)$ to $V(Y)$ such that $\{x_1, x_2\} \in E(X)$ iff $\{\varphi(x_1), \varphi(x_2)\} \in E(Y)$.

Graph isomorphisms will be a very important theme throughout this thesis. It is a good idea to convince yourself that the two graphs in Figure 0.1 really are isomorphic.

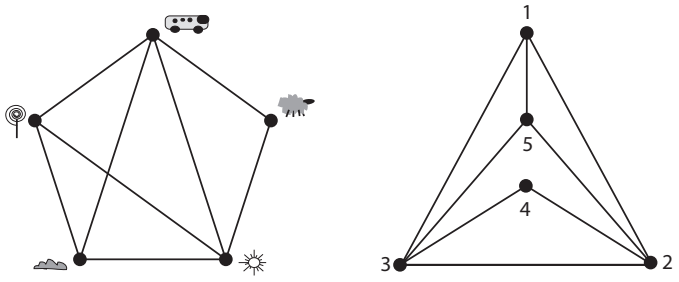


Figure 1: Two isomorphic graphs

Besides the fact that graphs are fun to draw and fun to think about, they are also very useful. Sociologists use graphs to represent social structures. Chemists use graphs to represent molecules. The people at Google have made quite a bit of money by working with graphs of internet sites. Every time you open up an in-flight

magazine and see a map covered in arched lines showing where the airline has flights, that is a graph. Graphs can be found everywhere and are used by everybody in some way or another. It is no surprise then, that mathematicians want to know as much as we can about graphs.

0.2 The Spectrum of a Graph

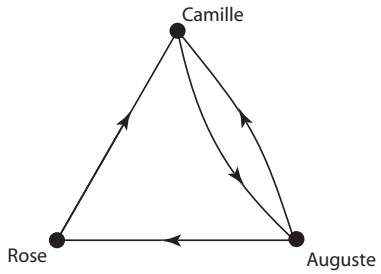
Graphs don't just represent structures, they can also answer questions about structures. If a plague hits one city, what cities will it spread to and how long will it take? If Chicago is snowed in, how should airline passengers who were expecting to fly through Chicago be redirected? When asking questions like this about graphs, we can run tests on all n vertices and all of the edges. (There can be up to $n(n-1)$ edges on a graph. There is no limit to the number of edges that can be on a pseudograph.) Running these tests is often a very slow process for even the fastest of computers. This is why mathematicians look for faster ways to store information about graphs. One of the most popular ways to gather a lot of information about graphs in very little time is by studying the spectrum of the adjacency matrix of a graph.

Definition 0.2.1. The *adjacency matrix* of a graph X is the matrix $A(X)$ with rows and columns indexed by vertices of X. Each entry A_{ij} is equal to the number of times the edge $\{i, j\}$ appears in $E(X)$.

The adjacency matrix is not the only matrix used to represent graphs. (Two other popular options are the incidence matrix and the Laplacian.) Therefore, in general, when talking about the spectrum of a graph it is good to mention which matrix you are referring to. However, I will only be considering the adjacency matrix, and so, the definition of spectrum for this thesis will always read as follows:

Definition 0.2.2. The *spectrum* of a graph X, denoted $Spec(X)$, is the spectrum (list of eigenvalues) of the adjacency matrix of X. We say that two graphs are *isospectral* (or *cospectral*) if they have the same spectrum.

Example 0.2.1. Calculating the spectrum of a graph Y:
Let Y be a love triangle:



The adjacency matrix of Y is

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

and thus the spectrum of the love triangle is the roots of polynomial $1 + x + x^3$.

Although there are many different ways to make the adjacency matrix of a single graph, the spectrum will always be the same.

Remark 0.2.1. If two graphs are isomorphic, then they must also be isospectral.

It is easy to see that this remark is true since two graphs are isomorphic if and only if their adjacency matrices are similar by a permutation matrix. Similarly, all possible adjacency matrices for a graph will be similar by a permutation matrix.

When mathematicians first started studying the spectrum of a graph, they hoped that Remark 0.2.1 went both ways. That is to say, they hoped that the spectrum could tell us everything about a graph up to isomorphism. If this were the case, then we would only have to keep track of the eigenvalues of the graph rather than all of the vertices and edges. However, this is an unrealistic hope. Despite intense effort, it is not known if there is polynomial-time algorithm for determining whether two graphs are isomorphic. Discovering that the eigenvalues of a graph tell us everything about a graph up to isomorphism would produce such an algorithm. While this is possible, it is unlikely. Even without understanding the concepts behind algorithm runtimes, some simple examples demonstrate that isopectrality need not imply an isomorphism. Figure 2 is one such example. While the spectrum cannot tell us everything about

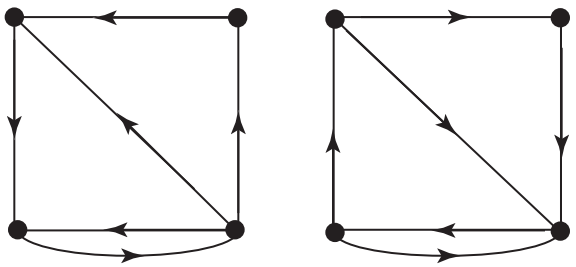


Figure 2: Two isospectral but nonisomorphic graphs

every graph, it has proved to be an invaluable tool. The spectrum of a graph can tell us how many vertices and edges a graph has as well as how many paths there are of a certain length from any given vertex to another. (See (GR01), (CRS97) for more information.) Spectral graph theory has proved useful outside the world of mathematics as well. Physicists, mechanical engineers, geographers, and programers of search engines all use results developed by spectral graph theory. (DGT81) gives an interesting example of how "isospectral" molecules are used in chemistry.

0.3 Cayley Graphs and Circulant Graphs

The adjacency matrix has already demonstrated how a graph can be represented as an algebraic structure. Now, we will examine how to represent an algebraic structure with a graph.

Definition 0.3.1. Let G be a group and S be a subset of $G\backslash\{id\}$. We say that a graph X is a *Cayley graph* of G with *connection set* S, written $X = \mathrm{Cay}(G, S)$, if

(i) $V(X) = G$

(ii) $E(X) = \{\{g, sg\} \mid g \in G, s \in S\}$

If we allow for S to be a multiset of elements of G, then X is a Cayley pseudograph.

This thesis will be focusing on a special type of Cayley graph defined as follows:

Definition 0.3.2. Let $\mathbb{Z}_n$ denote the additive group of integers modulo n, and let $S \subseteq \mathbb{Z}_n\backslash\{0\}$. If $X = \mathrm{Cay}(\mathbb{Z}_n, S)$, then we say X is a *circulant graph* of *order* n.

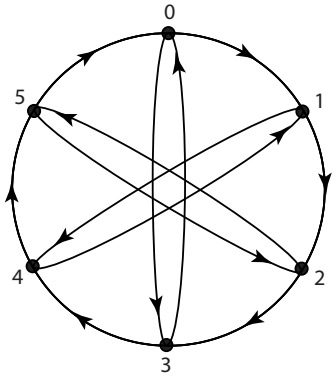


Figure 3: The graph $\mathrm{Cay}(\mathbb{Z}_6, \{1, 3\})$.

Another definition for a circulant graph is any graph with a circulant adjacency matrix (an $n \times n$ matrix of natural numbers whose rows are a cyclically shifted list of length n). It is easy to see that these two definitions are the same. Since the adjacency matrices of these graphs are circulant, it is no surprise that there is a simple and elegant formula for the spectra of circulant graphs.

Theorem 0.3.1. *If $X = Cay(\mathbb{Z}_n, S)$, then $Spec(X) = \{\lambda_x \mid x \in \mathbb{Z}_n\}$ where*

$$\lambda_x = \sum_{s \in S} \exp(\frac{2\pi i x s}{n}).$$

Example 0.3.1. Let $X = \mathrm{Cay}(\mathbb{Z}_6, \{1, 3\})$ (as in Figure 0.3), and $\omega = \exp(\frac{\pi i}{3})$.

$$\begin{aligned} Spec(X) &= \{\omega^1 + \omega^3,\ \omega^2 + \omega^0,\ \omega^3 + \omega^3,\ \omega^4 + \omega^0,\ \omega^5 + \omega^3,\ \omega^0 + \omega^0\} \\ &= \{\omega^1 - 1,\ \omega^2 + 1,\ -2,\ \omega^4 + 1,\ \omega^5 - 1,\ 2\}. \end{aligned}$$

Proof. Let T be a linear operator corresponding to the adjacency matrix of a circulant graph $X = \mathrm{Cay}(\mathbb{Z}_n, \{a_1, a_2, \cdots, a_m\})$. If f is any real function on the vertices of X we have

$$T(f)(x) = f(x + a_1) + f(x + a_2) + \cdots + f(x + a_m).$$

Let ω be a primitive n^{th} root of unity and let $g(x) = \omega^{i\,x}$ for some $i \in \mathbb{Z}_n$. Then,

$$\begin{aligned} T(g)(x) &= \omega^{ix+ia_1} + \omega^{ix+ia_2} + \cdots + \omega ix + ia_m \\ &= \omega^{ix}\left(\omega^{ia_1} + \omega^{ia_2} + \cdots + \omega^{ia_m}\right). \end{aligned}$$

Thus, g is an eigenfunction and $\omega^{ia_1} + \omega^{ia_2} + \cdots + \omega^{ia_m}$ is an eigenvalue. □

When I first began to work with this formula I had a strong feeling that the spectra of circulant graphs tells us even more about the graphs than we already thought, and in fact, it does. It was previously known that when circulant graphs are of prime order, their spectra determines them completely up to isomorphism. There were also several examples proving that this cannot be the case for all circulant graphs. However, that was all that was known. In Chapter 1, I will prove that there are graphs on any number of vertices (not just prime) that are completely determined up to isomorphism by their spectra.

In Chapter 2, I will present a new method for constructing circulant graphs that are isospectral and nonisomorphic. Many such constructions exist for graphs that are not Cayley graphs. However, only two such constructions exist for Cayley graphs (one discovered by Babai in 1979 (Bab79) and another discovered by Lubotsky et al. in 2005 (LSV06)), and none have been presented for circulant graphs.

The final chapter of this thesis presents a few further thoughts and open questions.

Chapter 1

A New Spectral Characterization

We say that a family of graphs can be characterized by its spectra if the only isospectral graphs in that family are also isomorphic. (CRS97) gives a list of a dozen different types of graphs that can be characterized by their spectra. There has also been a lot of recent interest in the isomorphism problem for circulant graphs. (See (Muz04), (MKP01), (Li99), (Pál87).) Determining when circulant graphs can be characterized by their spectra fits into both of these fields. All that was previously known was that circulant graphs of prime order are characterized by their spectra. There were also several examples proving that not all circulant graphs can be characterized by their spectra (see (ET70) and (GHM77) for a few), but that is all that has been said about the spectral characterization of circulant graphs. The following theorem gives some different criteria for when circulant graphs can be characterized by their spectra.

Theorem 1.0.2. *Let X be a circulant graph (or pseudograph) of order $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ where $p_1 < p_2 < \cdots < p_s$ are primes. Let the size of the connections set (or multiset) of X be m. If $p_1 \geq m$ and either $s = 1$ or $p_2 > p_1(m-1)$, then any circulant graph isospectral to X must be isomorphic to X.*

In order to prove this theorem we will be working quite a bit with group rings rather than the roots of unity themselves.

1.1 Terms and Results for a Related Group Ring

Let $G = \langle z \mid z^n = 1 \rangle$, and let ω be a (fixed) primitive n^{th} root of unity. Let $\varphi : \mathbb{Z}G \to \mathbb{Z}[\omega]$, be defined by the equation $\varphi(z) = \omega$. An element of $\mathbb{Z}G$ can be uniquely written as $\alpha = \sum_{i=0}^{n-1} C_i z^i$. I will call this representation "normal form." I will refer to coefficients C_j for values of j that may be greater than n. In these cases, I am referring to C_i where $i \equiv j \mod n$. Let $\varepsilon(\alpha) = \sum_{i=0}^{n-1} C_i$. The number of nonzero coefficients is denoted by $\varepsilon_0(\alpha)$. Let $\mathcal{S}(\alpha)$ denote the multi-set of elements of G where the multiplicity of $z^i \in \mathcal{S}(\alpha)$ is C_i.

For any finite subset $H \subseteq G$, let $\sigma(H) = \sum_{h \in H} h$. Two basic properties of $\sigma(H)$ are that $\varepsilon(\sigma(H)) = \varepsilon_0(\sigma(H)) = |H|$ (the cardinality of H), and that, if H is a subgroup, $\sigma(H)h = \sigma(H)$ for any $h \in H$. If H is not the trivial group and h is not an

identity element, this property still holds. So, we must have $\sigma(H) \in \ker(\varphi)$, since $\varphi(h) \neq 1$ and $\mathbb{Z}[\omega]$ is an integral domain.

Lemma 1.1.1. *If H is a subgroup of G, then the ideal $\mathbb{Z}G\sigma(H)$ consists of all $\sum c_g g$ such that c_g is constant on the cosets of H.*

Proof. Let $\alpha = \sum_{g\in G} b_g g$, and $\alpha\sigma(H) = \sum_{g\in G} c_g\, g$. Then, for each $x \in G$ we have

$$c_x = \sum_{g\in G, h\in H, gh=x} b_g = \sum_{h\in H} b_{xh^{-1}}.$$

Letting $\pi \in H$,

$$\begin{aligned} c_{x\pi} &= \sum_{h\in H} b_{x(\pi h^{-1})} \\ &= \sum_{h\in H} b_{xh} \quad . \end{aligned}$$

So, c_g is constant over the cosets. □

Let $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ where $p_1 < p_2 < \cdots < p_s$ are primes. Let P_i be the unique subgroup of G with order p_i. Theorem 3.3 of Lam and Leung's paper, (LL00), reads as follows:

> *(1) If $s = 1$, $\mathbb{N}G \cap \ker(\varphi) = \mathbb{N}\sigma(P_1)$. (2) If $s = 2$, $\mathbb{N}G \cap \ker(\varphi) = \mathbb{N}P_1\sigma(P_2) + \mathbb{N}P_2\,\sigma(P_1)$.*

However, the following example proves this theorem wrong.

Example 1.1.1. Let $n = 12$ and ω be a primitive 12^{th} root of unity. Thus, $P_1 = \{1, z^6\}$ and $P_2 = \{1, z^4, z^8\}$. The sum $z^2 + z^6 + z^{10}$ is not an element of $\mathbb{N}P_1\sigma(P_2) + \mathbb{N}P_2\,\sigma(P_1)$, but it is an element of $\mathbb{N}G \cap \ker(\varphi)$ since $\omega^2(1 + \omega^4 + \omega^8) = 0$.

Although this example proves the theorem wrong, I believe the mistake is only in a typo because I have rewritten the theorem below in such a way that the proof supplied by Lam and Leung for Theorem 3.3 of (LL00) holds true.

Lemma 1.1.2. *(1) If $s = 1$, $\mathbb{N}G \cap \ker(\varphi) = \mathbb{N}G\sigma(P_1)$. (2) If $s = 2$, $\mathbb{N}G \cap \ker(\varphi) = \mathbb{N}G\sigma(P_2) + \mathbb{N}G\,\sigma(P_1)$.*

Thus, we can see that if $s < 3$, $\mathbb{N}G \cap \ker(\varphi) = \sum_i \mathbb{N}G\sigma(P_i)$. Corollary 4.9 of the same paper, (LL00), gives information for when $s \geq 3$. Corollary 4.9 reads as follows:

> *Any element $u \in \mathbb{N}G \cap \ker(\varphi)$ with $\varepsilon_0(u) < p_1(p_2 - 1) + p_3 - p_2$ lies in $\sum_i \mathbb{N}G\sigma(P_i)$.*

This corollary will have an important role in proving the following lemma.

Lemma 1.1.3. *Let α and β be elements of $\mathbb{N}G$ such that $\varepsilon(\alpha) = \varepsilon(\beta) = m$ and $\mathcal{S}(\alpha) \cap \mathcal{S}(\beta) = \emptyset$. If $m \leq p_1$ and either $s = 1$ or $p_2 > p_1(m-1)$, then*

$$\varphi(\alpha) = \varphi(\beta) \Rightarrow \alpha = g_\alpha \sigma(P_1) \text{ and } \beta = g_\beta \, \sigma(P_1)$$

for any $g_\alpha \in \mathcal{S}(\alpha)$ and $g_\beta \in \mathcal{S}(\beta)$.

Proof. Let $\alpha = z^{a_1} + z^{a_2} + \cdots + z^{a_m}$ and $\beta = z^{b_1} + z^{b_2} + \cdots + z^{b_m}$. Since $\mathcal{S}(\alpha) \cap \mathcal{S}(\beta) = \emptyset$, it must be the case that $z^{a_i} \neq z^{b_j}$ for any i, j pair. Therefore, for $\varphi(\alpha) = \varphi(\beta)$, m must be greater than one. Using the fact that $z^{a_i}\sigma(P_1) \in \ker(\varphi) \cap \mathbb{N}G$ for all i, we can deduce the following:

$$\begin{aligned} 0 &= \varphi(\alpha \, \sigma(P_1)) \\ &= \varphi(\alpha) + \varphi\left(\alpha \, \sigma(P_1 \backslash \{1\})\right) \\ &= \varphi(\beta) + \varphi\left(\alpha \, \sigma(P_1 \backslash \{1\})\right) \\ &= \varphi\left(\beta + \alpha \, \sigma(P_1 \backslash \{1\})\right). \end{aligned}$$

Let $\gamma = \beta + \alpha \, \sigma(P_1 \backslash \{1\})$. I have just shown that $\gamma \in \ker(\varphi) \cap \mathbb{N}G$. Now, I wish to show that $\gamma \in \sum_i \mathbb{N}G \, \sigma(P_i)$. Recall that if p_3 does not exist, $\gamma \in \sum_i \mathbb{N}G \, \sigma(P_i)$. Assuming that p_3 does exist, we have

$$\begin{aligned} \varepsilon_0(\gamma) &\leq \varepsilon(\gamma) \\ &= \varepsilon(\beta) + \varepsilon\left(\alpha \, \sigma(P_1 \backslash \{1\})\right) \\ &= m + m(p_1 - 1) \\ &= p_1 m \\ &\leq (p_1)^2 \\ &\leq (p_1)^2 (m-1) \\ &< (p_1)^2 (m-1) + 2 \\ &= p_1(p_1(m-1)) + (p_2 + 2) - p_2 \\ &\leq p_1(p_2 - 1) + p_3 - p_2. \end{aligned}$$

By Corollary 4.9 of Lam and Leung's paper, $\gamma \in \sum_i \mathbb{N}G \, \sigma(P_i)$. Thus, in either case $\gamma \in \sum_i \mathbb{N}G \, \sigma(P_i)$, and we can write $\gamma = \sum_{i=1}^{s} \sum_{g \in G} x_{i,g} \, g \, \sigma(P_i)$. Supposing $x_{2,h} \geq 1$ for some $h \in G$, we can express $\varepsilon(\gamma)$ in two different ways:

$$x_{2,h} p_2 + n_1 p_1 + n_2 p_2 + \cdots + n_s p_s = \varepsilon(\gamma) = m p_1$$

for some $n_i \in \mathbb{N}$. Using the hypotheses that $p_1 \geq m$ and $p_2 > p_1(m-1)$ we can deduce:

$$\begin{aligned} n_1 p_1 + n_2 p_2 + \cdots + n_s p_s &= m p_1 - x_{2,h} p_2 \\ &\leq m p_1 - p_2 \\ &< p_1. \end{aligned}$$

Since p_1 is the smallest of the primes that divide n, $n_i = 0$ for all $1 \leq i \leq s$. This tells us that $mp_1 = x_{2,h}\, p_2$. This would imply that p_2 divides m, but this is a contradiction because p_2 is greater than m. Therefore, we can conclude that $x_{2,g} = 0$ for all $g \in G$. Similarly, we can conclude that $x_{i,g} = 0$ for all $i \geq 2$, and thus, $\gamma \in \mathbb{N}G\,\sigma(P_1)$.

For the remainder of this proof, let $\gamma = \sum_{i=0}^{p_1-1} x_i z^i$ be the unique representation of γ. And let $\mathfrak{S}(i)$ represent the following four statements:

$$\begin{array}{rll} & 1) & x_{a_1} \geq i \\ & 2) & i < m \\ & 3) & z^{a_{1+i}} = z^{a_1 + \frac{l_i n}{p_1}} \quad \text{(for some } 1 \leq \ell_i < p_1\text{)} \\ \text{and} & 4) & a_1 \neq a_{1+i}. \end{array}$$

After arbitrarily choosing a_1, I will show by induction that we can recursively order the a_i so that $\mathfrak{S}(i)$ is true for all $i \leq p_1 - 1$.

Statement (2) of $\mathfrak{S}(1)$ must be true because $m > 1$. Since $z^{a_1}\sigma(P_1\backslash\{1\}) = z^{a_1+\frac{n}{p_1}} + z^{a_1+\frac{2n}{p_1}} + \cdots + z^{a_1+\frac{(p_1-1)n}{p_1}}$, we can see that $x_{a_1+\frac{n}{p_1}} \geq 1$. We can then use Lemma 1.1.1 to conclude that $x_{a_1} \geq 1$. Therefore, statement (1) of $\mathfrak{S}(1)$ is true, and $z^{a_1} \in \mathcal{S}(\gamma)$. Since $\mathcal{S}(\alpha) \cap \mathcal{S}(\beta) = \emptyset$, we can conclude that $z^{a_1} \notin \mathcal{S}(\beta)$, and thus we know that $z^{a_1} \in \alpha\,\sigma(P_1\backslash\{1\})$ since $\gamma = \beta + \alpha\,\sigma(P_1\backslash\{1\})$. For this to be true, it must be the case that $z^{a_1} \in z^{a_i}(P_1\backslash\{1\})$ for some i. We know that $i \neq 1$ because z^{a_1} cannot be an element of $z^{a_1}(P_1\backslash\{1\})$. Without loss of generality, we can say $z^{a_1} \in z^{a_2}(P_1\backslash\{1\})$. Notice that this causes statement (4) of $\mathfrak{S}(1)$ to be satisfied. We can also conclude that $z^{a_1} = z^{a_2+\ell n/p_1}$ for some $\ell \neq 0$. This then allows us to rewrite z^{a_2} as $z^{a_2} = z^{a_1+(p_1-\ell)n/p_1}$. Letting $\ell_1 = (p_1 - \ell)$, we can see that statement (3) of $\mathfrak{S}(1)$ is also true. Hence, $\mathfrak{S}(1)$ is true.

Now I assume that $\mathfrak{S}(i)$ is true for all $i \leq j$ for some $j < p_1 - 1$ in order to show that $\mathfrak{S}(j+1)$ is also true. In order to see that statement (1) of $\mathfrak{S}(j+1)$ is true, I will rewrite γ. For the following equations, assume that a sum from a to b is zero if $b < a$.

$$\begin{aligned} \gamma &= \beta + \alpha\,\sigma(P_1\backslash\{1\}) \\ &= \beta + \sum_{i=0}^{j} z^{a_{1+i}}\sigma(P_1\backslash\{1\}) + \sum_{i=j+2}^{m} z^{a_i}\sigma(P_1\backslash\{1\}) \quad \text{(by stmt. (2) of } \mathfrak{S}(j)\text{)} \\ &= \beta + \sum_{i=0}^{j} z^{a_1+\frac{\ell_i n}{p_1}}\sigma(P_1\backslash\{1\}) + \sum_{i=j+2}^{m} z^{a_i}\sigma(P_1\backslash\{1\}) \text{ (by (3) of } \mathfrak{S}(i)\text{, letting } \ell_0 = 0) \\ &= \beta + \sum_{i=0}^{j} \left(z^{a_1}\,\sigma(P_1) - z^{a_1+\frac{\ell_i n}{p_1}} \right) + \sum_{i=j+2}^{m} z^{a_i}\sigma(P_1\backslash\{1\}) \\ &= \beta + (j+1)z^{a_1}\sigma(P_1) - \sum_{i=0}^{j} z^{a_1+\frac{\ell_i n}{p_1}} + \sum_{i=j+2}^{m} z^{a_i}\sigma(P_1\backslash\{1\}) \\ &= \beta + (j+1)\sum_{\ell=0}^{p_1-1} z^{a_i+\frac{\ell n}{p_1}} - \sum_{i=0}^{j} z^{a_1+\frac{\ell_i n}{p_1}} + \sum_{i=j+2}^{m} z^{a_i}\sigma(P_1\backslash\{1\}) \end{aligned}$$

This makes it easier to see that for every $0 \leq \ell < p_1 - 1$:

$$x_{a_1+\frac{\ell n}{p_1}} \geq \begin{cases} j & \text{if } \ell = \ell_i \text{ for some } 0 \leq i \leq j \\ j+1 & \text{otherwise.} \end{cases}$$

Since $j < p_1 - 1$, there must be some ℓ such that $x_{a_1+\frac{\ell n}{p_1}} \geq j+1$. Due to Lemma 1.1.1, we can see that $x_{a_1} \geq j+1$ as well. Hence, statement (1) of $\mathfrak{S}(j+1)$ is true.

Due to statement (3) and (4) of $\mathfrak{S}(i)$, we know that the multiplicity of z^{a_1} in $\mathcal{S}(\sum_{i=0}^{j} z^{a_1}\,\sigma(P_1) - z^{a_1+\ell_i n/p_1})$ is exactly j. Thus, for $x_{a_1} \geq j+1$, it must be the case that $z^{a_1} \in \mathcal{S}(\beta)$ or $z^{a_1} \in \mathcal{S}(\sum_{i=j+2}^{m} z^{a_i}\sigma(P_1\backslash\{1\}))$. Since $\mathcal{S}(\alpha) \cap \mathcal{S}(\beta) = \emptyset$, z^{a_1} must be an element of the latter support. This implies that the sum must not be zero. Thus, $m \geq j+2$ which causes statement (2) of $\mathfrak{S}(j+1)$ to be satisfied. Without loss of generality, we can say $z^{a_1} \in z^{a_{j+2}}(P_1\backslash\{1\})$. We can then conclude that statements (3) and (4) for $\mathfrak{S}(j+1)$ are true, and therefore $\mathfrak{S}(i)$ is true for all $i < p_1$. We can use statement (3) and the hypothesis that $m \leq p_1$ to conclude that $m = p_1$.

A similar process can be used to prove any of the four statements for any a_j, not just for a_1. It is most important to note that statement (4) is true for all pairs of elements in the support of α. With this in mind, we can conclude the following:

$$i \neq j \Rightarrow a_{1+i} \neq a_{1+j} \Rightarrow a_1 + \frac{\ell_i n}{p_1} \neq a_1 + \frac{\ell_j n}{p_1} \Rightarrow \ell_i \neq \ell_j.$$

Now we can rewrite α in terms of z^{a_1}

$$\begin{aligned} \alpha &= z^{a_1} + z^{a_2} + \cdots + z^{a_m} \\ &= z^{a_1} + z^{a_1+\frac{l_1 n}{p_1}} + \cdots + z^{a_1+\frac{l_{m-1} n}{p_1}} \\ &= z^{a_1}\sigma(P_1) \quad \text{(because all } \ell_i \text{ are unique and } m = p_1.) \end{aligned}$$

Since a_1 was chosen arbitrarily and there is no way to distinguish between α and β, we can say $\alpha = z^{a_i}\,\sigma(P_1)$ and $\beta = z^{b_i}\,\sigma(P_1)$ for any $1 \leq i \leq m$. □

Corollary 1.1.4. *Let $G = \langle z \mid z^n = 1\rangle$ where $n = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$ and $p_1 < p_2 < \cdots < p_s$ are primes. Let α and β be elements of $\mathbb{N}G$ such that $\varepsilon(\alpha) = \varepsilon(\beta) = m$. Suppose*

$$\begin{aligned} & (i) \quad p_1 \geq m; \\ & (ii) \quad \text{either } s = 1 \text{ or } p_2 > p_1(m-1) \\ \text{and} \quad & (iii) \quad \varphi(\alpha) = \varphi(\beta). \end{aligned}$$

Then, we either have [1] $\alpha = \beta$ or [2] $m = p_1$, $\alpha = g_\alpha\sigma(P_1)$ for any $g_\alpha \in \mathcal{S}(\alpha)$, and $\beta = g_\beta\sigma(P_1)$ for any $g_\beta \in \mathcal{S}(\beta)$.

Proof. In $\mathbb{N}G$, let $\alpha = \tilde{\alpha}+\alpha'$ and $\beta = \tilde{\beta}+\beta'$ such that $\alpha' = \beta'$ and $\mathcal{S}(\tilde{\alpha})\cap\mathcal{S}(\tilde{\beta}) = \emptyset$. If $\tilde{\alpha} = \tilde{\beta} = 0$, then $\alpha = \alpha' = \beta' = \beta$ and the proof is finished. For the rest of this proof, assume that $\tilde{\alpha} \neq 0$. Since $\varphi(\alpha) = \varphi(\beta)$ and $\varphi(\alpha') = \varphi(\beta')$, we have $\varphi(\tilde{\alpha}) = \varphi(\tilde{\beta})$. We

can then use Lemma 1.1.3 to conclude that $\tilde{\alpha} = g_\alpha\,\sigma(P_1)$ and $\tilde{\beta} = g_\beta\,\sigma(P_1)$ for some $g_\alpha \in \mathcal{S}(\alpha), g_\beta \in \mathcal{S}(\beta)$. Since $\tilde{\alpha} \neq 0$ we know that $\varepsilon(\tilde{\alpha}) \neq 0$. Thus, we have

$$\begin{aligned} m = \varepsilon(\alpha) &= \varepsilon(\tilde{\alpha}) + \varepsilon(\alpha') \\ &= \varepsilon(z^{a_i}\sigma(P_1)) + \varepsilon(\alpha') \\ &= p_1 + \varepsilon(\alpha'). \end{aligned}$$

Since $m \leq p_1$, we conclude $\varepsilon(\alpha') = 0$, and hence $\alpha' = 0$. Similarly, $\beta' = 0$. Therefore $\alpha = \tilde{\alpha} = g_\alpha\,\sigma(P_1)$ and $\beta = \tilde{\beta} = g_\beta\,\sigma(P_1)$. □

With these results, we now have the tools to prove Theorem 1.0.2.

1.2 Proof of Theorem 1.0.2

Proof. Suppose Y is a circulant graph (or multigraph) which is isospectral to X. The graph Y must be of order n as well. From Theorem 0.3.1, we can see that the largest eigenvalue of X is m. Thus, the largest eigenvalue of Y must be m as well. This implies that Y must have a connection set (or multiset) of size m. We can write $X = \mathrm{Cay}(\mathbb{Z}_n, A)$ and $Y = \mathrm{Cay}(\mathbb{Z}_n, B)$ where $A = \{a_1, a_2, \cdots, a_m\}$ and $B = \{b_1, b_2, \cdots, b_m\}$.

Let ω be a primitive n^{th} root of unity. For the proof of this theorem, I will order the eigenvalues in the spectra of X and Y such that λ_i, the i^{th} value in the spectrum of X, is $\lambda_i = \omega^{i\,a_1} + \omega^{i\,a_2} + \cdots + \omega^{i\,a_m}$, and μ_i, the i^{th} eigenvalue in the spectrum of Y, is $\mu_i = \omega^{i\,b_1} + \omega^{i\,b_2} + \cdots + \omega^{i\,b_m}$.

Since X and Y are isospectral, there is a $0 \leq j < n$ such that $\lambda_1 = \mu_j$. That is to say, $\omega^{a_1} + \omega^{a_2} + \cdots + \omega^{a_m} = \omega^{jb_1} + \omega^{jb_2} + \cdots + \omega^{jb_m}$. Letting φ be the usual mapping from $\mathbb{Z}\langle z : z^n = 1\rangle$ to $\mathbb{Z}[\omega]$ and $\sigma(P_1) = \sum_{i=0}^{p_1-1} z^{i\frac{n}{p_1}}$, we can use Corollary 1.1.4 to conclude that either [1] $z^{a_1} + z^{a_2} + \cdots + z^{a_m} = z^{jb_1} + z^{jb_2} + \cdots + z^{jb_m}$ or [2] $z^{a_1} + z^{a_2} + \cdots + z^{a_m} = z^{a_i}\,\sigma(P_1)$ for any $a_i \in A$. I wish to show that in either case, there is exists some $t \in \mathbb{Z}_n$ and an ordering of B such that $\omega^{a_i} = \omega^{t\,b_i}$ for all $1 \leq i \leq m$.

Case 1. $z^{a_1} + z^{a_2} + \cdots + z^{a_m} = z^{jb_1} + z^{jb_2} + \cdots + z^{jb_m}$. This implies that $A = \{jb_1, jb_2, \cdots, jb_m\}$. Thus, letting $t = j$, there is an ordering of B such that $a_i = tb_i$ for all $1 \leq i \leq m$.

Case 2. $z^{a_1} + z^{a_2} + \cdots + z^{a_m} = z^{a_i}\,\sigma(P_1)$ for any $a_i \in A$. This implies that $\lambda_1 = \omega^{a_i} + \omega^{a_i + \frac{n}{p_1}} + \cdots + \omega^{a_i + (p_1-1)\frac{n}{p_1}} = 0$, and $A = \{a_i, a_i + \frac{n}{p_1}, \cdots, a_i + (p-1)\frac{n}{p_1}\}$. Therefore,

$$\lambda_x = \omega^{xa_i} + \omega^{xa_i + x\frac{n}{p_1}} + \cdots + \omega^{xa_i + x(p_1-1)\frac{n}{p_1}} = \begin{cases} 0 & \text{if } p_1 \nmid x \\ m\omega^{xa_i} & \text{if } p_1 \mid x \end{cases}$$

for any $a_i \in A$. Since X and Y are isospectral, $\mu_1 = 0$ or $\mu_1 = m\omega^{a_1 x}$ for some $x \in \mathbb{Z}_n$. If $\mu_1 = m\omega^{xa_1}$, then $B = \{xa_1, xa_1, \cdots, xa_1\}$ and μ_y will not equal zero for any $y \in \mathbb{Z}_n$. This cannot be the case since $\mu_j = \lambda_1 = 0$. Therefore, $\mu_1 = 0$. By

Corollary 1.1.4, we can conclude that $\mu_1 = \varphi(z^{b_i}\sigma(P_1))$ and

$$\mu_y = \begin{cases} 0 & \text{if } p_1 \nmid y \\ m\omega^{yb_i} & \text{if } p_1 \mid y \end{cases} \tag{1.1}$$

for any $b_i \in B$.

We know that there must be some y such that $\mu_y = \lambda_{p_1} = m\omega^{p_1 a_i}$. By equation (1.1) we know that $p_1 \mid y$. Letting $tp_1 = y$ we have:

$$\begin{aligned} \lambda_{p_1} &= \mu_{tp_1} \Rightarrow \\ m\omega^{p_1 a_i} &= m\omega^{p_1 t b_i} \Rightarrow \\ (\omega^{p_1 a_i})^{1/p_1} &= (\omega^{p_1 t b_i})^{1/p_1} \\ \omega^{a_i} &= \omega^{tb_i}\zeta \qquad (\text{where } \zeta \text{ is a } p_i^{th} \text{ root of unity}) \Rightarrow \\ &= \omega^{tb_i + h\frac{n}{p_1}} \quad (\text{for some } 0 \le h < p_1) \\ &= \omega^{tb_k} \end{aligned}$$

for any $a_i \in A$ and some $b_k \in B$. We can reorder B such that $\omega^{a_i} = \omega^{tb_i}$.

In either case, we can order B such that $\omega^{a_i} = \omega^{tb_i}$ for all $1 \le i \le m$. Similarly, there is a reordering of B (which may be different than the ordering just mentioned) such that for some $k \in \mathbb{Z}_n$, $\omega^{k\,a_i} = \omega^{b_i}$ for all i. For the remainder of this proof, we will assume that B is ordered in such a way that $\omega^{a_i} = \omega^{tb_i}$ and $\omega^{k\,a_i} = \omega^{b_{\pi(i)}}$ where π is a permutation of $\mathbb{Z}_n$. For each $1 \le i \le m$ there must be some $\ell \le m$ such that $\pi^\ell(i) = i$. Thus, we have

$$\omega^{a_i k^\ell t^{\ell-1}} = \omega^{b_{\pi(i)} k^{\ell-1} t^{\ell-1}} = \omega^{a_{\pi(i)} k^{\ell-1} t^{\ell-2}} = \omega^{a_{\pi^{\ell-1}(i)} k} = \omega^{b_{\pi^\ell(i)}} = \omega^{b_i}.$$

Since it is also true that $\omega^{a_i} = \omega^{t\,b_i}$, it must be the case that $(a_i, n) = (b_i, n)$ for all $1 \le i \le m$.

Let $g_i = (a_i, n) = (b_i, n)$, $g = (g_1, g_2, \cdots, g_m)$, and $d = (t, g)$. Since $\omega^{a_i} = \omega^{t\,b_i}$, we can conclude that $(b_i, n) = (a_i, n) = (tb_i, n)$ for all i. Thus, $(t, n/g_i) = 1$ for all i. This implies that $(t, n/g) = 1$, and finally, that $(t, n/d) = 1$.

Let $\tau = t + \frac{n}{d}$. Then,

$$\begin{aligned} \tau b_i &= (t + \frac{n}{d})b_i \\ &\equiv t\,b_i \mod n \\ &\equiv a_i \mod n \end{aligned} \tag{1.2}$$

for all $1 \le i \le m$. Since $(t, n/d) = 1$, we can conclude that $(\tau, n) = 1$. Therefore, we can define a graph isomorphism, ψ, by $\psi(v) = \tau v$ where v is a vertex of a Cayley graph of $\mathbb{Z}_n$. Using this isomorphism, we have

$$\begin{aligned} Y &\cong \psi(Y) \\ &= \mathrm{Cay}(\mathbb{Z}_n, \{\tau b_1, \tau b_2, \cdots, \tau b_m\}) \\ &= \mathrm{Cay}(\mathbb{Z}_n, \{a_1, a_2, \cdots, a_m\}) \\ &= X. \end{aligned}$$

□

Now that we have proved the theorem, we can conclude the following corollary:

Corollary 1.2.1. *Circulant graphs (pseudographs) with connection sets (multisets) containing only one or two elements are characterized by their spectra.*

Cvetković proved a similar theorem in his doctoral thesis. He proved that any 2-regular undirected graph is characterized by its spectrum (Cve71). (The term *k-regular* means a graph for which every vertex is adjacent to exactly k other vertices.) However, the theorem does not explicitly deal with undirected graphs.

Chapter 2

A New Construction

As seen in the previous chapter, it is hard to find families of graphs that are characterized by their spectra. However, it is equally hard (if not harder) to find examples of graphs that not characterized by their spectra, especially when dealing with Cayley graphs. There are several methods for constructing isospectral, nonisomorphic graphs. (See (GM82) for a good overview.) However, these methods do not apply to Cayley graphs. Before 2005, the only known construction for isospectral, nonisomorphic Cayley graphs was due to Babai who gave examples for the dihedral group of order $2p$ (where p is a prime) (Bab79). In 2005, Lubotzky et al. published a construction for isospectral, nonisomorphic Cayley graphs of the group $\mathrm{PSL}_d(\mathbb{F}_q)$ for every $d \geq 5$ ($d \neq 6$) and prime power $q > 2$ (LSV06). In this chapter, I will present a construction for isospectral, nonisomorphic circulant graphs.

2.1 Defining the Graphs

Theorem 2.1.1. *Let $n = 2^r p$, where p is an odd prime and $2 \leq r$. Let $X = Cay(\mathbb{Z}_n, A)$ and $Y = Cay(\mathbb{Z}_n, B)$ where A and B depend on r and p as follows:*

$$\begin{aligned} A &= \{1 + i2^r \mid 0 \leq i \leq \frac{p-1}{2}\} \cup \{1 + j2^r + \frac{n}{2} \mid 1 \leq j \leq \frac{p-1}{2}\} \\ B &= \{1 - i2^r \mid 0 \leq i \leq \frac{p-1}{2}\} \cup \{1 - j2^r + \frac{n}{2} \mid 1 \leq j \leq \frac{p-1}{2}\}. \end{aligned}$$

The graphs X and Y are isospectral, nonisomorphic graphs.

Sections 2.2 through 2.4 are dedicated to proving this theorem. Whenever I refer to X and Y in this chapter, it should be assumed that I am referring to the graphs X and Y defined above.

Example 2.1.1. Let $n = 2^2 \cdot 3 = 12$. Then we have, $A = \{1, 5\} \cup \{11\} = \{1, 5, 11\}$ and $B = \{1, 9\} \cup \{3\} = \{1, 3, 9\}$. Thus, $X = \mathrm{Cay}(\mathbb{Z}_{12}, A)$ and $Y = \mathrm{Cay}(\mathbb{Z}_{12}, B)$. These two graphs are shown in Figure 2.1.1. We can verify that these graphs are

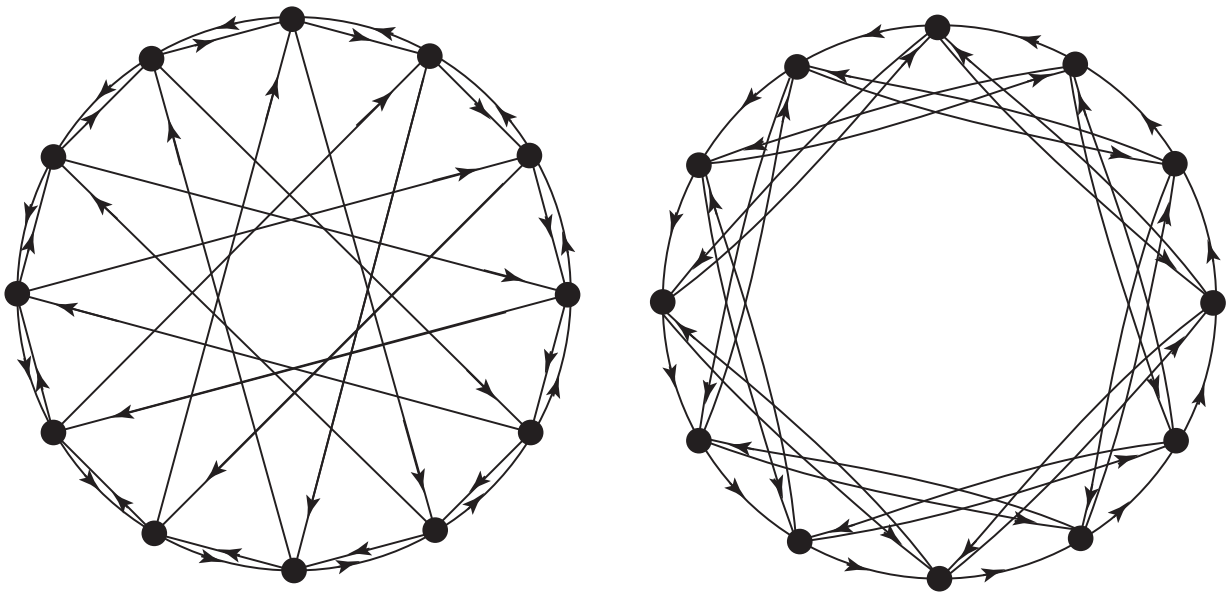


Figure 2.1: The graphs when $n = 12$.

isospectral. Let ω be a primitive 12^{th} root of unity.

The spectrum of X	The spectrum of Y
$\omega^1 + \omega^5 + \omega^{11}$	$\omega^1 + \omega^3 + \omega^9 = \omega^1 + \omega^5 + \omega^{11}$
$\omega^2 + \omega^{10} + \omega^{10}$	$\omega^2 + \omega^6 + \omega^6 = \omega^8 + \omega^4 + \omega^4$
$\omega^3 + \omega^3 + \omega^9$	$\omega^3 + \omega^9 + \omega^3$
$\omega^4 + \omega^8 + \omega^8$	$\omega^4 + \omega^0 + \omega^0 = \omega^{10} + \omega^2 + \omega^2$
$\omega^5 + \omega^1 + \omega^7$	$\omega^5 + \omega^3 + \omega^9 = \omega^5 + \omega^1 + \omega^7$
$\omega^6 + \omega^6 + \omega^6$	$\omega^6 + \omega^6 + \omega^6$
$\omega^7 + \omega^{11} + \omega^5$	$\omega^7 + \omega^9 + \omega^3 = \omega^7 + \omega^{11} + \omega^5$
$\omega^8 + \omega^4 + \omega^4$	$\omega^8 + \omega^0 + \omega^0 = \omega^2 + \omega^{10} + \omega^{10}$
$\omega^9 + \omega^9 + \omega^3$	$\omega^9 + \omega^3 + \omega^9$
$\omega^{10} + \omega^2 + \omega^2$	$\omega^{10} + \omega^6 + \omega^6 = \omega^4 + \omega^8 + \omega^8$
$\omega^{11} + \omega^7 + \omega^1$	$\omega^{11} + \omega^9 + \omega^3 = \omega^{11} + \omega^7 + \omega^1$
$\omega^0 + \omega^0 + \omega^0$	$\omega^0 + \omega^0 + \omega^0$

I have ordered the spectra of these graphs in order to help motivate the upcoming Lemma 2.2.2.

2.2 Isospectrality

I will show that X and Y are always isospectral, but before I do that, I need to introduce a short lemma.

Lemma 2.2.1. *Let ω be a primitive n^{th} root of unity. For any integer, $k \geq 0$,*

$$\sum_{i=0}^{(p-1)/2} \omega^{i\,2^{r+k}} = \sum_{i=0}^{(p-1)/2} \omega^{i\,2^r}$$

Proof. For any $s > r$ we have

$$\begin{aligned}
\sum_{i=0}^{p-1} \omega^{i\,2^s} &= \sum_{i=0}^{(p-1)/2} \omega^{i\,2^s} + \sum_{i=(p+1)/2}^{p-1} \omega^{i\,2^s} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{i\,2^s} + \sum_{i=0}^{(p-3)/2} \omega^{(i+\frac{p+1}{2})2^s} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{i\,2^s} + \sum_{i=0}^{(p-3)/2} \omega^{i\,2^s + n2^{s-r-1} + 2^{s-1}} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{(2i)2^{s-1}} + \sum_{i=0}^{(p-3)/2} \omega^{(2i+1)2^{s-1}} \\
&= \sum_{i=0}^{p-1} \omega^{i\,2^{s-1}}
\end{aligned}$$

By induction on the difference of s and r, we can conclude that Lemma 2.2.1 is true. □

From now on, I will order the spectra of X and Y such that λ_x and μ_x, the x^{th} eigenvalues in the spectrum of X and Y respectively, are

$$\begin{aligned}
\lambda_x &= \sum_{i=0}^{(p-1)/2} \omega^{x(1+i2^r)} + \sum_{j=1}^{(p-1)/2} \omega^{x(1+j2^r+\frac{n}{2})} \\
\mu_x &= \sum_{i=0}^{(p-1)/2} \omega^{x(1-i2^r)} + \sum_{j=1}^{(p-1)/2} \omega^{x(1-j2^r+\frac{n}{2})}
\end{aligned}$$

(Notice that the spectra in Example 2.1.1 are ordered this way.) In order to make calculations a bit clearer, I will also break down the eigenvalues of X and Y into two parts. Let

$$\lambda_{x,\alpha} = \sum_{i=0}^{(p-1)/2} \omega^{x(1+i2^r)}, \qquad \lambda_{x,\beta} = \sum_{j=1}^{(p-1)/2} \omega^{x(1+j2^r+\frac{n}{2})},$$

$$\mu_{x,\alpha} = \sum_{i=0}^{(p-1)/2} \omega^{x(1-i2^r)}, \text{ and } \quad \mu_{x,\beta} = \sum_{j=1}^{(p-1)/2} \omega^{x(1-j2^r+\frac{n}{2})}.$$

We can see that $\lambda_{x,\alpha} + \lambda_{x,\beta} = \lambda_x$ and $\mu_{x_\alpha} + \mu_{x,\beta} = \mu_x$.

At this point we have all of the tools and terminology to be able to prove the following lemma and thus conclude that the spectra of X and Y are the same.

Lemma 2.2.2. *Letting μ_x and λ_x be as defined above, we have:*

$$\lambda_x = \begin{cases} \mu_{x+n/2} & \text{if } (x,n) = 2^m \text{ for some } m > 0 \\ \mu_x & \text{otherwise} \end{cases}.$$

Proof. I will break the proof down into three cases based on whether or not p or 2 divide x.

Case 1. $(x,n) = 1$. In this case we have

$$\begin{aligned}
\lambda_{x,\alpha} - \mu_{x,\beta} &= \sum_{i=0}^{(p-1)/2} \omega^{x(1+i2^r)} - \sum_{j=1}^{(p-1)/2} \omega^{x(1-j2^r+\frac{n}{2})} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{x(1+i2^r)} + \omega^{\frac{n}{2}} \sum_{j=1}^{(p-1)/2} \omega^{x(1-j2^r+\frac{n}{2})} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{x+xi2^r} + \sum_{j=1}^{(p-1)/2} \omega^{x-xj2^r+n(\frac{x+1}{2})} \\
&= \omega^x \left(\sum_{i=0}^{(p-1)/2} \omega^{(x\,i)2^r} + \sum_{j=1}^{(p-1)/2} \omega^{(-x\,j)2^r} \right) \\
&= \omega^x \left(\sum_{i=0}^{p-1} \omega^{(x\,i)2^r} \right) \\
&= \omega^x \left(\sum_{j=0}^{p-1} \omega^{j2^r} \right) \qquad \text{where } j = x\,i \\
&= \omega^x(0) \\
&= 0.
\end{aligned}$$

Thus, we have $\lambda_{x,\alpha} = \mu_{x,\beta}$. Similarly,

$$\begin{aligned}
\mu_{x,\alpha} - \lambda_{x,\beta} &= \sum_{i=0}^{(p-1)/2} \omega^{x(1-i2^r)} - \sum_{j=1}^{(p-1)/2} \omega^{x(1+j2^r+\frac{n}{2})} \\
&= \omega^x \left(\sum_{i=0}^{(p-1)/2} \omega^{(-x\,i)2^r} + \sum_{j=1}^{(p-1)/2} \omega^{(x\,j)2^r} \right) \\
&= \omega^x \sum_{j=0}^{p-1} \omega^{j2^r} \\
&= 0.
\end{aligned}$$

Therefore, $\mu_{x,\alpha} = \lambda_{x,\beta}$ and $\lambda_x = \mu_x$.

Case 2. $p|x$. Letting $x = py$, we have

$$\begin{aligned}
\lambda_x &= \sum_{i=0}^{(p-1)/2} \omega^{py(1+i2^r)} + \sum_{j=1}^{(p-1)/2} \omega^{py(1+j2^r+\frac{n}{2})} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{py+(iy)n} + \sum_{j=1}^{(p-1)/2} \omega^{py+(jy)n+py\frac{n}{2}} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{py-(iy)n} + \sum_{j=1}^{(p-1)/2} \omega^{py-(jy)n+py\frac{n}{2}} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{py(1-i2^r)} + \sum_{j=1}^{(p-1)/2} \omega^{py(1-j2^r+\frac{n}{2})} \\
&= \mu_x.
\end{aligned}$$

Case 3. $(x, n) = 2^m$ for some $m > 0$. Letting $x = y2^m$, where $(y, n) = 1$, we have

$$\begin{aligned}
\lambda_{x,\alpha} - \mu_{x+\frac{n}{2},\beta} &= \sum_{i=0}^{(p-1)/2} \omega^{y2^m(1+i2^r)} - \sum_{j=1}^{(p-1)/2} \omega^{(y2^m+\frac{n}{2})(1-j2^r+\frac{n}{2})} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{y2^m+i\,y2^{r+m}} + \sum_{j=1}^{(p-1)/2} \omega^{\frac{n}{2}+y2^m-j\,y2^{r+m}+\frac{n}{2}} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{y2^m+i\,y2^{r+m}} + \sum_{j=0}^{(p-3)/2} \omega^{y2^m-(\frac{p-1}{2}-j)y2^{r+m}} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{y2^m+i\,y2^{r+m}} + \sum_{j=0}^{(p-3)/2} \omega^{y2^m-ny2^{m-1}+y2^{r+m-1}+jy2^{r+m}} \\
&= \omega^{y2^m} \left(\sum_{i=0}^{(p-1)/2} \omega^{(2i)\,y2^{r+m-1}} + \sum_{j=0}^{(p-3)/2} \omega^{(2j+1)y2^{r+m-1}} \right) \\
&= \omega^{y2^m} \sum_{i=0}^{p-1} \omega^{i\,y2^{r+m-1}} \\
&= \omega^{y2^m} \sum_{j=0}^{p-1} \omega^{j2^{r+m-1}} \\
&= \omega^{y2^m} \sum_{j=0}^{p-1} \omega^{j2^r} \qquad \text{(by Lemma 2.2.1)} \\
&= 0.
\end{aligned}$$

Therefore, $\lambda_{x,\alpha} = \mu_{x+\frac{n}{2},\beta}$. We can also see that

$$\begin{aligned}
\mu_{x+\frac{n}{2},\alpha} - \lambda_{x,\beta} &= \sum_{i=0}^{(p-1)/2} \omega^{(y2^m+\frac{n}{2})(1-i2^r)} - \sum_{j=1}^{(p-1)/2} \omega^{y2^m(1+j2^r+\frac{n}{2})} \\
&= \sum_{i=0}^{(p-1)/2} \omega^{y2^m+\frac{n}{2}-iy2^{r+m}} + \omega^{\frac{n}{2}} \sum_{j=1}^{(p-1)/2} \omega^{y2^m+jy2^{r+m}} \\
&= \omega^{y2^m+\frac{n}{2}} \left(\sum_{i=0}^{(p-1)/2} \omega^{-(\frac{p-1}{2}-i)y2^{r+m}} + \sum_{j=1}^{(p-1)/2} \omega^{jy2^{r+m}} \right) \\
&= \omega^{y2^m+\frac{n}{2}} \left(\sum_{i=0}^{(p-1)/2} \omega^{(2i+1)y2^{r+m-1}} + \sum_{j=1}^{(p-1)/2} \omega^{(2j)y2^{r+m-1}} \right) \\
&= \omega^{y2^m+\frac{n}{2}} \sum_{i=0}^{p-1} \omega^{iy2^{r+m-1}} \\
&= \omega^{y2^m+\frac{n}{2}} \sum_{j=0}^{p-1} \omega^{j2^{r+m-1}} \\
&= \omega^{y2^m+\frac{n}{2}} \sum_{j=0}^{p-1} \omega^{j2^r} \quad \text{by Lemma 2.2.1} \\
&= 0.
\end{aligned}$$

Hence, $\mu_{x+\frac{n}{2},\alpha} = \lambda_{x,\beta}$, and $\lambda_x = \mu_{x+\frac{n}{2}}$. □

2.3 No Repeated Eigenvalues

Trying to prove that these graphs are not isomorphic turned out to be a difficult expedition. However, I eventually realized that it may be easier to prove that the graphs have no repeated eigenvalues in their spectra and then go from there. (The next section will explain how this implies that the graphs are not isomorphic.) In order to prove that the graphs have no repeated eigenvalues I will be using the same group ring and homomorphism, φ, from Chapter 1.

Since we have proved in the previous section that the graphs have the same spectrum, we only need to prove that one of the graphs has no repeated eigenvalues.

Theorem 2.3.1. *Let $n = 2^r p$ where r is an integer such that $r \geq 2$ and p is any odd prime, and let*

$$A = \{1 + i2^r \mid 0 \leq i \leq (p-1)/2\} \cup \{1 + j2^r + p2^{r-1} \mid 1 \leq j \leq (p-1)/2\}.$$

If $X = Cay(\mathbb{Z}_n, A)$, then X has no repeated eigenvalues.

Proof. I will order the eigenvalues of X so that the x^{th} eigenvalue of the spectrum of X is

$$\lambda_x = \sum_{i=0}^{(p-1)/2} \omega^{x(1+i2^r)} + \sum_{j=1}^{(p-1)/2} \omega^{x(1+j2^r+n/2)} \tag{2.1}$$

.

Suppose that there is some y such that $\lambda_x = \lambda_y$ (in order to show that $x \equiv y \mod n$). Therefore, $\lambda_x - \lambda_y = 0 = \lambda_x + \omega^{n/2}\lambda_y = 0$. Let $\alpha \in \mathbb{N}G$ be defined by

$$\alpha = \sum_{i=0}^{(p-1)/2} z^{x(1+i2^r)} + z^{y(1+i2^r)+n/2} + \sum_{j=1}^{(p-1)/2} z^{x(1+j2^r+n/2)} + z^{y(1+j2^r+n/2)+n/2}. \tag{2.2}$$

For the rest of this proof, let $\alpha = \sum_{k=0}^{n-1} C_k z^k$ be the normal form of α.

Since $\varphi(\alpha) = \lambda_x + \omega^{n/2}\lambda_y = 0$, we know that $\alpha \in \mathbb{N}G \cap \ker(\varphi)$. By Lemma 1.1.2, α must also be an element of $\mathbb{N}G\,\sigma(H_2) + \mathbb{N}G\,\sigma(H_p)$ where H_2 and H_p are the unique subgroups of G of size 2 and p, respectively. Thus, we can write

$$\alpha = \sum_{g\in G} a_g\, g\, \sigma(H_2) + \sum_{g\in G} b_g\, g\, \sigma(H_p), \tag{2.3}$$

where a_g, $b_g \in \mathbb{N}$. Therefore,

$$\begin{aligned} \varepsilon(\alpha) &= \varepsilon\left(\sum_{g\in G} a_g\, g\, \sigma(H_2) + \sum_{g\in G} b_g\, g\, \sigma(H_p)\right) \\ &= \sum_{g\in G}(2a_g + pb_g). \end{aligned}$$

However, we defined α by an explicit formula (see equation 2.2) and can calculate the exact value of $\varepsilon(\alpha)$. Namely $\varepsilon(\alpha) = \frac{p+1}{2}\cdot 2 + \frac{p-1}{2}\cdot 2 = 2p$. Therefore, we know that

$$\sum_{g\in G}(2a_g + pb_g) = 2p. \tag{2.4}$$

So, either $a_g = 0$ for all $g \in G$ or $b_g = 0$ for all $g \in G$. This implies that either $\alpha \in \mathbb{N}G\,\sigma(H_2)$ or $\alpha \in \mathbb{N}G\,\sigma(H_p)$.

At this point I will break the proof up into cases based on whether p and 2 divide x. In each case I will show that α must be an element of $\mathbb{N}G\,\sigma(H_2)$ and then that $x \equiv y \mod n$.

Case 1. x is odd. In this case, $z^{x(1+i2^r)+n/2} = z^{x(1+i2^r+n/2)}$ for all i. Therefore,

$$\sum_{i=1}^{(p-1)/2} z^{x(1+i2^r)} + z^{x(1+i2^r+n/2)} = \sum_{i=1}^{(p-1)/2} z^{x(1+i2^r)}\sigma(H_2)$$

Using the notation of Equation 2.3, we can see that $a_{z^{x(1+i2^r)}}$ is at least one. Thus, b_g must be zero for all g and we can conclude that $\alpha \in \mathbb{N}G\,\sigma(H_2)$. Let β be defined by

$$\begin{aligned}\beta &= \alpha - \sum_{i=1}^{(p-1)/2} z^{x(1+i2^r)} + z^{x(1+i2^r+n/2)} \\ &= z^x + \sum_{i=0}^{(p-1)/2} z^{y(1+i2^r)+n/2} + \sum_{j=1}^{(p-1)/2} z^{y(1+j2^r+n/2)+n/2}. \end{aligned} \tag{2.5}$$

Since β is the difference of two elements of $\mathbb{N}G\,\sigma(H_2)$, we know that β must also be an element of $\mathbb{N}G\,\sigma(H_2)$. Let $\beta = \sum_{k=0}^{n-1} B_k z^k$ be the normal form of β. We can see that $B_x \geq 1$. By Lemma 1.1.1, we know that $B_{x+n/2} \geq 1$ as well. Therefore, $z^{x+n/2} = z^{y(1+i2^r)+n/2}$ for some $0 \leq i \leq (p-1)/2$ or $z^{x+n/2} = z^{y(1+j2^r+n/2)+n/2}$ for some $1 \leq j \leq (p-1)/2$. Which is to say,

$$x \equiv y(1+i2^r) \text{ or } y(1+j2^r+n/2) \mod n.$$

Therefore, y must be odd as well, and we can conclude that $z^{y(1+i2^r)} = z^{y(1+i2^r+n/2)+n/2}$ for all i. Then,

$$\sum_{i=1}^{(p-1)/2} z^{y(1+i2^r+n/2)+n/2} + z^{y(1+i2^r)+n/2} = \sum_{i=1}^{(p-1)/2} z^{y(1+i2^r)}\sigma(H_2) \in \mathbb{N}G\,\sigma(H_2).$$

Thus,

$$\beta - \sum_{i=1}^{(p-1)/2} z^{y(1+i2^r+n/2)+n/2} + z^{y(1+i2^r)+n/2} = z^x + z^{y+n/2} \in \mathbb{N}G\,\sigma(H_2).$$

By Lemma 1.1.1, we can conclude that $z^{x+n/2} = z^{y+n/2}$, and therefore, $x \equiv y \mod n$.

Case 2. $2|x$ *and* $p|x$. In this case we have

$$\begin{aligned}\alpha &= \sum_{i=0}^{(p-1)/2} z^{x(1+i2^r)} + z^{y(1+i2^r)+n/2} + \sum_{j=1}^{(p-1)/2} z^{x(1+j2^r+n/2)} + z^{y(1+j2^r+n/2)+n/2} \\ &= \sum_{i=0}^{(p-1)/2} z^x + z^{y(1+i2^r)+n/2} + \sum_{j=1}^{(p-1)/2} z^x + z^{y(1+j2^r+n/2)+n/2} \\ &= p\,z^x + \sum_{i=0}^{(p-1)/2} z^{y(1+i2^r)+n/2} + \sum_{j=1}^{(p-1)/2} z^{y(1+j2^r+n/2)+n/2}. \end{aligned} \tag{2.6}$$

This implies that $C_x \geq p$. Since $i \not\equiv j \mod p$ implies that $x + i2^r \not\equiv x + j2^r \mod n$, we know that for all $0 \leq i < p$, C_{x+i2^r} are referring to distinct coefficients. Therefore, we can conclude that

$$\varepsilon(\alpha) \geq \sum_{i=0}^{p-1} C_{x+i2r}.$$

If $\alpha \in \mathbb{N}G\,\sigma(H_p)$, then we could conclude that

$$\begin{aligned}\varepsilon(\alpha) &\geq \sum_{i=0}^{p-1} C_{x+i2r} \\ &= \sum_{i=0}^{p-1} C_x \quad \text{(by Lemma 1.1.1)} \\ &\geq \sum_{i=0}^{p-1} p \\ &= p^2 \\ &> 2p.\end{aligned}$$

This is a contradiction because we already know that $\varepsilon(\alpha) = 2p$. Therefore, $\alpha \notin \mathbb{N}G\,\sigma(H_p)$, and we can assume that $\alpha \in \mathbb{N}G\,\sigma(H_2)$.

Since $C_x \geq p$, Lemma 1.1.1 tells us that $C_{x+n/2} \geq p$. From Equation 2.6, we can see that for this to be true, $z^{x+n/2} = z^{y(1+i2^r)+n/2}$ for all $0 \leq i \leq (p-1)/2$ and $z^{x+n/2} = z^{y(1+j2^r+n/2)+n/2}$ for all $1 \leq j \leq (p-1)/2$. That is to say

$$x + n/2 \equiv y(1 + j2^r + n/2) + n/2 \equiv y(1 + i2^r) + n/2 \mod n$$

for all $0 \leq i \leq (p-1)/2$ and $1 \leq j \leq (p-1)/2$. Since $y(1 + j2^r + n/2) + n/2 \equiv y(1 + i2^r) + n/2 \mod n$, we can conclude that $yp2^{r-1} \equiv y2^r(i-j) \mod n$ and therefore, that p and 2 must divide y. We can then rewrite α as

$$\begin{aligned}\alpha &= p\,z^x + \sum_{i=0}^{(p-1)/2} z^{y(1+i2^r)+n/2} + \sum_{j=1}^{(p-1)/2} + z^{y(1+j2^r+n/2)+n/2} \\ &= p(z^x + z^{y+n/2}).\end{aligned}$$

Since $\alpha \in \mathbb{N}G\,\sigma(H_2)$, $z^{x+n/2} = z^{y+n/2}$. Hence, $x \equiv y \mod n$.

Case 3. $2|x$ *and* $p \nmid x$. Since x and y are interchangeable, we may use *Case 1* to conclude that y must be even as well. In *Case 2*, we saw that if x is even and p divides x, then p must also divide y. Again, since x and y were chosen arbitrarily, we can assume that p does not divide y in this case. Therefore, we have

$$\begin{aligned}\alpha &= \sum_{i=0}^{(p-1)/2} z^{x(1+i2^r)} + z^{y(1+i2^r)+n/2} + \sum_{j=1}^{(p-1)/2} z^{x(1+j2^r+n/2)} + z^{y(1+j2^r+n/2)+n/2} \\ &= z^x + z^{y+n/2} + \sum_{i=1}^{(p-1)/2} 2z^{x(1+i2^r)} + 2z^{y(1+i2^r)+n/2}. \qquad (2.7)\end{aligned}$$

Suppose that $\alpha \in \mathbb{N}G\,\sigma(H_p)$ (in order to arrive at a contradiction). Since $C_{x(1+2^r)} \geq 2$, Lemma 1.1.1 tells us that $C_{x(1+2^r)+i2^r} \geq 2$ for all $i \in \mathbb{Z}_p$. Since $(x, p) = 1$ we know

that for all $0 \leq j < p$ there exists $0 \leq i < p$ such that $j \equiv x(i-1) \mod p$, and thus, $x(1+2^r) + j2^r \equiv x(1+i2^r) \mod n$. Therefore, we can say that $C_{x(1+i2^r)} \geq 2$ for all $0 \leq i < p$. If

$$x(1+i2^r) \equiv x(1+j2^r) \mod n$$

for $i \neq j \mod p$, then

$$\text{then } 0 \equiv x2^r(j-i) \mod n.$$

This is a contradiction because p does not divide x. Therefore, the coefficients $C_{x(1+i2^r)}$ are referring to unique terms for each $0 \leq i < p$. Then, we know

$$\begin{aligned} \varepsilon(\alpha) &\geq \sum_{i=0}^{p-1} C_{x(1+i2^r)} \\ &= \sum_{i=0}^{p-1} C_x \quad \text{(by Lemma 1.1.1)} \\ &\geq \sum_{i=0}^{p-1} 2 \\ &= 2p. \end{aligned}$$

Since we know that $\varepsilon(\alpha) = 2p$, we know that all inequalities must be equalities. This implies that

$$\begin{aligned} \sum_{i=0}^{p-1} C_{x(1+i2^r)} &= \varepsilon(\alpha) \\ &= \varepsilon\left(\sum_{i=0}^{p-1} 2z^{x(1+i2^r)}\right) + \varepsilon\left(\alpha - \sum_{i=0}^{p-1} 2z^{x(1+i2^r)}\right) \\ &= \sum_{i=0}^{p-1} C_{x(1+i2^r)} + \varepsilon\left(\alpha - \sum_{i=0}^{p-1} 2z^{x(1+i2^r)}\right) \end{aligned}$$

Therefore, $\varepsilon\left(\alpha - \sum_{i=0}^{p-1} 2z^{x(1+i2^r)}\right) = 0$ and

$$\alpha = \sum_{i=0}^{p-1} 2z^{x(1+i2^r)}. \tag{2.8}$$

Since $(p, 2^r) = 1$ there exist k and ℓ such that $kp = 1 + \ell 2^r$. We will choose k and ℓ such that $0 < \ell < p$. I will now break this case up into two sub-cases based on the size of ℓ.

Sub-case 3.1. $\ell \leq (p-1)/2$. By Equation 2.7, we know that $C_{y(1+\ell 2^r)+n/2} \geq 2$. So, by Equation 2.8, we know that $z^{y(1+\ell 2^r)+n/2} = z^{x(1+i2^r)}$ for some $0 \leq i < p$. If $z^{y(1+\ell 2^r)+n/2} = z^{x(1+\ell 2^r)}$, then $C_{x(1+\ell 2^r)} \geq 3$. This is a contradiction to Equation 2.8

since we have already established that $x(1+i2r) \not\equiv x(1+j2^r) \mod n$ whenever $i \not\equiv j \mod p$. Therefore $z^{y(1+\ell 2^r)+n/2} = z^{x(1+i2^r)}$ for some $i \neq \ell \mod p$. This is to say that

$$y(1+\ell 2^r) + n/2 \equiv p(yk + 2^{r-1}) \equiv x(1+i2^r) \mod n.$$

We know that p cannot divide x, and if p divides $1 + i2^r$, then i must be congruent to ℓ. Therefore, we have arrived a contradiction and we can conclude that when $0 < \ell \leq (p-1)/2$, $\alpha \notin \mathbb{N}G\,\sigma(H_p)$.

Sub-case 3.2. $(p-1)/2 < \ell < p$. By Equation 2.8, we know that $C_{x(1+\ell 2^r)} = 2$. Therefore, by Equation 2.7, we know that $z^{x(1+\ell 2^r)}$ is equal to $z^{x(1+i2^r)}$ or $z^{y(1+i2^r)+n/2}$ for some $0 \leq i \leq (p-1)/2$. In either case, this would imply that p divides $(1+i2^r)$. This a contradiction since i cannot be congruent to $\ell \mod p$. Therefore, in both sub-cases, $\alpha \notin \mathbb{N}G\,\sigma(H_p)$.

We can now assume that $\alpha \in \mathbb{N}G\,\sigma(H_2)$. Since $x(1+i2^r) + a\frac{n}{2} \not\equiv x(1+j2^r) + b\frac{n}{2} \mod n$ whenever $i \not\equiv j \mod p$ for any $a, b \in \{0,1\}$ we can assume that the coefficients $C_{x(1+i2^r)}$ and $C_{x(1+i2^r)+n/2}$ are referring to unique terms for all $0 \leq i \leq (p-1)/2$. Thus, for some $\beta \in \mathbb{N}G\,\sigma(H_2)$, we can write

$$\begin{aligned} \alpha &= \sum_{i=0}^{(p-1)/2} \left(C_{x(1+i2^r)} z^{x(1+i2^r)} + C_{x(1+i2^r)+n/2} z^{x(1+i2^r)+n/2}\right) + \beta \qquad (2.9) \\ &= \sum_{i=0}^{(p-1)/2} C_{x(1+i2^r)} \left(z^{x(1+i2^r)} + z^{x(1+i2^r)+n/2}\right) + \beta \quad \text{(by Lemma 1.1.1).} \end{aligned}$$

Therefore,

$$\begin{aligned} 2p = \varepsilon(\alpha) &= \sum_{i=0}^{(p-1)/2} \left(2\,C_{x(1+i2^r)}\right) + \varepsilon(\beta) \\ &\geq 2 + 2 \cdot 2\frac{(p-1)}{2} + \varepsilon(\beta) \quad \text{(from Equation 2.7)} \\ &= 2p + \varepsilon(\beta). \end{aligned}$$

Which implies that $\varepsilon(\beta) = 0$ and all inequalities must be equalities. We can conclude that

$$\alpha = \sum_{i=0}^{(p-1)/2} C_{x(1+i2^r)} \left(z^{x(1+i2^r)} + z^{x(1+i2^r)+n/2}\right)$$

and

$$\sum_{i=0}^{(p-1)/2} C_{x(1+i2^r)} = 1 + 2\frac{(p-1)}{2}.$$

Looking again at Equation 2.7, we can conclude that for these equalities to be true, $C_x = 1$ and $C_{x(1+i2^r)} = 2$ for all $1 \leq i \leq (p-1)/2$. Thus, $C_k = 1$ iff $z^k = z^x$ or $z^k = z^{x+n/2}$.

We can now repeat the same process focusing on the y-terms instead of the x-terms. Since $C_{y(1+i2^r)}$ and $C_{y(1+i2^r)+n/2}$ are referring to distinct terms for all $0 \leq i \leq (p-1)/2$, we can write

$$\begin{aligned}\alpha &= \sum_{i=0}^{(p-1)/2} \left(C_{y(1+i2^r)} z^{y(1+i2^r)} + C_{y(1+i2^r)+n/2} z^{y(1+i2^r)+n/2}\right) + \gamma \\ &= \sum_{i=0}^{(p-1)/2} C_{y(1+i2^r)+n/2} \left(z^{y(1+i2^r)} + z^{y(1+i2^r)+n/2}\right) + \gamma\end{aligned}$$

for some γ. Using the same logic from Equation 2.9 onward, we will conclude that $C_k = 1$ iff $z^k = z^{y+n/2}$ or $z^k = z^y$. Therefore, z^x is equal to z^y or $z^{y+n/2}$. If $z^x = z^{y+n/2}$, then $C_x \geq 2$. This is a contradiction. It must be the case that, $z^x = z^y$. Therefore, $x \equiv y \mod n$ in all three cases. □

2.4 Non-Isomorphic

In 1967, Ádám made the conjecture that $\text{Cay}(\mathbb{Z}_n, S_1)$ and $\text{Cay}(\mathbb{Z}_n, S_2)$ are isomorphic iff $S_1 = qS_2$ where $(q, n) = 1$ and $qS_2 = \{qs \mid s \in S_2\}$ (Ádá67). In 1969, Elspas and Turner showed that Ádám's conjecture was true if $\text{Cay}(\mathbb{Z}_n, S_1)$ and $\text{Cay}(\mathbb{Z}_n, S_2)$ have no repeated eigenvalues (ET70). Since we have just seen that the graphs defined in this chapter have no repeated eigenvalues, Ádám's conjecture holds. Thus, all we need to show is that our graphs' connection sets are not equivalent by multiplication by a number relatively prime to n.

Lemma 2.4.1. *Let $n = 2^r p$, where p is an odd prime and $2 \leq r$. Let A and B be sets that depend on r and p as follows:*

$$\begin{aligned}A &= \{1 + i2^r \mid 0 \leq i \leq \frac{p-1}{2}\} \cup \{1 + j2^r + \frac{n}{2} \mid 1 \leq j \leq \frac{p-1}{2}\} \\ B &= \{1 - i2^r \mid 0 \leq i \leq \frac{p-1}{2}\} \cup \{1 - j2^r + \frac{n}{2} \mid 1 \leq j \leq \frac{p-1}{2}\}\end{aligned}$$

One of these sets will be comprised of numbers that are all relatively prime to n and the other set will contain exactly two values that are divisible by p.

Proof. For this proof, it is helpful to rewrite B as the equivalent set mod n:

$$B = \{1 + i2^r \mid \frac{p+1}{2} \leq i \leq p\} \cup \{1 + j2^r + \frac{n}{2} \mid \frac{p+1}{2} \leq j \leq p-1\}.$$

Since $(p, 2^r) = 1$ there exist k and ℓ such that $kp = 1 + \ell 2^r$. We will choose k and ℓ such that $0 < \ell < p$. The number $1 + \ell 2^r$ will be an element of either A or B depending on whether or not ℓ is greater than $(p-1)/2$. We can also conclude that $1 + \ell 2^r + n/2$, which will be in the same set as $1 + \ell 2^r$, is also divisible by p. Thus, we can see that one of the sets will have at least two elements that are divisible by p. Furthermore,

$$1 + i2^r \equiv 1 + i2^r + \frac{n}{2} \not\equiv 0 \mod p$$

whenever $i \not\equiv \ell \mod p$. Therefore, there can be no other elements of either set that are divisible by p. Since all of the elements in both A and B are odd, we can conclude that all of the elements in both A and B besides $1+\ell 2^r$ and $1+\ell 2^r+n/2$ are relatively prime to n. □

By this lemma, we can see that A and B cannot be equivalent via multiplication by a number relatively prime to n, and therefore, the results of Elspas and Turner mentioned above tell us that the circulant graphs of order n with connection sets A and B must not be isomorphic.

2.5 Extending the Construction

We can use the same connection sets to create even more circulant graphs of order n where $n = 2^r p$ for some prime p. Letting A and B be as define in Section 2.1, we can create the new connection sets as follows:

$$\begin{aligned} \tilde{A} &= A \cup qA \\ \tilde{B} &= B \cup qB \end{aligned}$$

where q is relatively prime to n and $qA = \{q\,a \mid a \in A\}$. Now, we can use these connection sets to create two new graphs (or pseudographs), $\tilde{X} = \mathrm{Cay}(\mathbb{Z}_n, \tilde{A})$ and $\tilde{Y} = \mathrm{Cay}(\mathbb{Z}_n, \tilde{B})$.

Lemma 2.5.1. *The graphs described above,*

$$\begin{aligned} \tilde{X} &= Cay(\mathbb{Z}_n, A \cup qA) \\ \tilde{Y} &= Cay(\mathbb{Z}_n, B \cup qB), \end{aligned}$$

have the same spectrum.

Proof. Order the eigenvalues of $\tilde{X}$ as follows: let the x^{th} eigenvalue of $\tilde{X}$ be

$$\tilde{\lambda}_x = \sum_{\tilde{a} \in \tilde{A}} \omega^{x\,\tilde{a}}$$

where ω is a primitive n^{th} root of unity. Letting $X = \mathrm{Cay}(\mathbb{Z}_n, A)$, as described in Section 2.1, and letting λ_x be the x^{th} eigenvalue of X by the ordering described in Section 2.2, we can see that

$$\begin{aligned} \tilde{\lambda}_x &= \sum_{\tilde{a} \in \tilde{A}} \omega^{x\,\tilde{a}} \\ &= \sum_{a \in A} \omega^{x\,a} + \omega^{x\,qa} \\ &= \lambda_x + \lambda_{qx}. \end{aligned}$$

Similarly, we can order the spectrum of $\tilde{Y}$ such that the x^{th} eigenvalue is

$$\tilde{\mu}_x = \mu_x + \mu_{qx}$$

where μ_x is the x^{th} eigenvalue of the spectrum of Y under the ordering described in Section 2.2. Thus, we have written the eigenvalues of $\tilde{X}$ and $\tilde{Y}$ in terms of the eigenvalues mentioned in Lemma 2.2.2, and we can use the results of the lemma. In order to do that, I will break down the proof into two cases.

Case 1. $(x, n) = 2^m$ *for some* $m > 0$. This implies that $(qx, n) = 2^m$. By Lemma 2.2.2 we can conclude that $\lambda_x = \mu_{x+n/2}$ and $\lambda_{qx} = \mu_{qx+n/2}$. Therefore,

$$\begin{aligned}
\tilde{\lambda_x} &= \lambda_x + \lambda_{qx} \\
&= \mu_{x+n/2} + \mu_{qx+n/2} \\
&= \mu_{x+n/2} + \mu_{q(x+n/2)} \quad \text{(since } q \text{ must be odd)} \\
&= \tilde{\mu}_{x+n/2}
\end{aligned}$$

Case 2. $(x, n) \neq 2^m$ *for any* $m > 0$. In this case, (qx, n) also does not equal 2^m for any m. Thus, by Lemma 2.2.2, $\lambda_x = \mu_x$ and $\lambda_{qx} = \mu_{qx}$, and we can conclude that $\tilde{\lambda_x} = \tilde{\mu_x}$. □

If we let $q = -1$ then we have two undirected graphs. When $r > 2$, the undirected graphs do not have any double edges (they are not pseudographs). Thus, we can create a pair of undirected isospectral graphs. At this point, it would seem logical to follow the process we used to show that the previous graphs were not isomorphic to show that these graphs are not isomorphic. However, these graphs can have repeated eigenvalues, and therefore the same process will not apply.

Example 2.5.1. Let $n = 2^3 \cdot 3 = 24$. In this case, $\tilde{A} = \{1, 3, 9, 15, 21, 23\}$ and $\tilde{B} = \{1, 5, 7, 17, 19, 23\}$. Letting ω be a primitive 24^{th} root of unity and keeping the ordering of the eigenvalues from the previous proof, we have

$$\tilde{\lambda}_6 = \omega^6 + \omega^{18} + \omega^6 + \omega^{18} + \omega^{18} + \omega^6 = 0$$

and

$$\tilde{\lambda}_{18} = \omega^{18} + \omega^{18} + \omega^6 + \omega^{18} + \omega^6 + \omega^{18} = 0$$

Although our previous method for proving that graphs are not isomorphic does not apply to these graphs, we can prove that some of them are not isomorphic. Musychuk proved that Ádám's conjecture (as described in the previous section) holds for graphs on n vertices when either n, $n/2$ or $n/4$ is an odd, square-free number (Muz95), (Muz97). It will still be the case that one of the connections sets (either $\tilde{A}$ or $\tilde{B}$) will contain values divisible by p, and the other connection set will be comprised entirely of values that are relatively prime to n. Therefore, when $n = 2^2 p$ for any odd prime p, these graphs cannot be isomorphic. It should also be noted that whenever $n = 2^r p$, the undirected graphs defined in this section will be multigraphs. As far as the rest of the graphs are concerned (namely, when $n = 2^r p$ for $r > 2$), it would be just as interesting to prove that these graphs are isomorphic as it would be to prove that they are not. Thus, we are left with the following open problem:

Question 2.5.2. *Are the graphs* $\tilde{X}$ *and* $\tilde{Y}$ *described in this section isomorphic for any values of* r*?*

More open problems are presented in the next chapter.

Chapter 3

Questions ± Answers

While I was in the process of writing this thesis many questions about the new characterization and the new construction came to mind. I was able to answer a few of the questions, but many remain open. I have decided to present both the answered and the open questions for any reader who is interested.

3.1 Questions About the New Characterization

Question 3.1.1. *Can Theorem 1.0.2 be extended to all abelian groups?*

There is a broader version of Theorem 0.3.1 which tells us that the eigenvalues of the Cayley graphs of abelian groups will also be sums of roots of unity. The methods for proving Theorem 1.0.2 might be used to prove a similar theorem for these Cayley graphs.

Question 3.1.2. *Are the criteria given in Theorem 1.0.2 the best possible criteria? That is to say, given two natural numbers n and m, is it the case that one of the following must the true: (1) n is prime or n and m satisfy the hypotheses of Theorem 1.0.2 thus causing any circulant graph of order n with a connection set of size m to be classified by its spectrum, or (2) there exist two circulant graphs of order n with connection sets of size m that are isospectral and nonisomorphic?*

To answer "yes" to this question, we would likely have to create more constructions like the one in the previous chapter. However, I would not recommend trying since the following table answers the question for us. I have run a computer test on graphs with a small number of vertices searching for isospectral nonisomorphic circulant graphs. Pseudographs were not considered. The results are presented in Table 3.1. Let's consider the case $n = 6$ and $m = 5$. Since $2 < 5$ and $3 < 2(5 - 1)$, we can see that a graph on 6 vertices with 5 elements in its connection set will not fall under the criteria of Theorem 1.0.2. Since 6 is not prime and Table 3.1 shows us that there are no isospectral nonisomorphic graphs on 6 vertices, the answer to Question 3.1.2 must be "no." This leads us to another open question:

Question 3.1.3. *What are the criteria by which circulant graphs can be characterized by their spectra?*

Table 3.1: Circulant graphs of order n with connections sets of order m

n	Values of m for which isospectral nonisomorphic graphs exist
2	none
3	none
4	none
5	none
6	none
7	none
8	none
9	none
10	4,5
11	none
12	3,4,5,6,7,8,9
13	none
14	4,5,6,7,8,9
15	5,6,7,8,9
16	4,5,6,7,8,9,10,11,12
17	none
18	3,4,5,6,7,8,9,10,11,12,13,14,15

3.2 Questions About the New Construction

The following two questions can be answered by Table 3.1. However, I have decided to include them for the sake of completion.

Question 3.2.1. *Is* $X = Cay(\mathbb{Z}_{12}, \{1, 3, 9\})$ *and* $Y = Cay(\mathbb{Z}_{12}, \{1, 5, 11\})$ *the smallest pair of isospectral, nonisomorphic circulant graphs?*

By "smallest" I mean graphs on the smallest number of vertices. This question is motivated by the surge of research done in the 60's in which mathematicians searched for the smallest pair of isospectral nonisomorphic graphs in every family. In (GHM77), Godsil gives a list of smallest such pairs in several different families of graphs. In this list he states that the smallest pair of isospectral, nonisomorphic, undirected circulant graphs is on twenty vertices. This led me to wonder about the directed case. Table 3.1 tells us that the directed graphs on ten vertices are the smallest. I will define the actual graphs below.

Example 3.2.1. Let $X = \text{Cay}(\mathbb{Z}_{10}, \{1, 2, 3, 6\})$ and $Y = \text{Cay}(\mathbb{Z}_{10}, \{1, 3, 4, 8\})$. The connection sets are not equivalent by multiplication by a prime. Therefore, since 10 is square-free, these graphs cannot be isomorphic (by the result presented in (Muz95) mentioned at the end of Chapter 2). We can also verify that these graphs have the

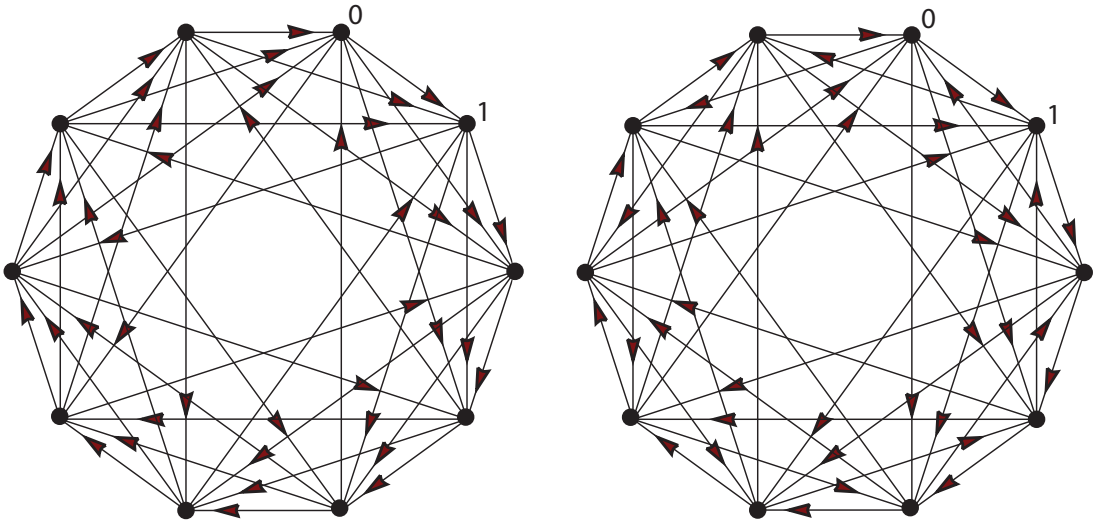


Figure 3.1: $\mathrm{Cay}(\mathbb{Z}_{10}, \{1,2,3,6\})$ and $\mathrm{Cay}(\mathbb{Z}_{10}, \{1,3,4,8\})$

same spectrum. Letting ω be a primitive tenth root of unity we have:

The spectrum of X	The spectrum of Y
$\omega^1 + \omega^2 + \omega^3 + \omega^6 = \omega^2 + \omega^3$	$\omega^1 + \omega^3 + \omega^4 + \omega^8 = \omega^1 + \omega^4$
$\omega^2 + \omega^4 + \omega^6 + \omega^2$	$\omega^2 + \omega^6 + \omega^8 + \omega^6$
$\omega^3 + \omega^6 + \omega^9 + \omega^8 = \omega^6 + \omega^9$	$\omega^3 + \omega^9 + \omega^2 + \omega^4 = \omega^3 + \omega^2$
$\omega^4 + \omega^8 + \omega^2 + \omega^4$	$\omega^4 + \omega^2 + \omega^6 + \omega^2$
$\omega^5 + \omega^0 + \omega^5 + \omega^0$	$\omega^5 + \omega^5 + \omega^0 + \omega^0$
$\omega^6 + \omega^2 + \omega^8 + \omega^6$	$\omega^6 + \omega^8 + \omega^4 + \omega^8$
$\omega^7 + \omega^4 + \omega^1 + \omega^2 = \omega^4 + \omega^1$	$\omega^7 + \omega^1 + \omega^8 + \omega^6 = \omega^7 + \omega^8$
$\omega^8 + \omega^6 + \omega^4 + \omega^8$	$\omega^8 + \omega^4 + \omega^2 + \omega^4$
$\omega^9 + \omega^8 + \omega^7 + \omega^4 = \omega^8 + \omega^7$	$\omega^9 + \omega^7 + \omega^6 + \omega^2 = \omega^9 + \omega^6$
$\omega^0 + \omega^0 + \omega^0 + \omega^0$	$\omega^0 + \omega^0 + \omega^0 + \omega^0$

Thus, this is the smallest pair of isospectral, nonisomorphic directed circulant graphs.

Question 3.2.2. *Are all isospectral, nonisomorphic circulant graphs of even order?*

Before I collected the data to create Table 3.1, the only examples of isospectral, nonisomorphic, circulant graphs I had seen besides the ones constructed in Chapter 2 were of order 32, 16, and 20 (in (ET70) and (GHM77)). Thus, I wondered if all examples were even. However, there are several examples on 15 vertices. Here is one such pair:

Example 3.2.2. Let $X = \mathrm{Cay}(\mathbb{Z}_{15}, \{1,2,3,6\})$ and $Y = \mathrm{Cay}(\mathbb{Z}_{15}, \{1,3,4,8\})$. The number 15 is a square-free and odd number, and the connection sets are not equivalent via multiplication by some number relatively prime to 15. Therefore, we can conclude that the graphs are not isomorphic. Now, all that we must do is verify that they have

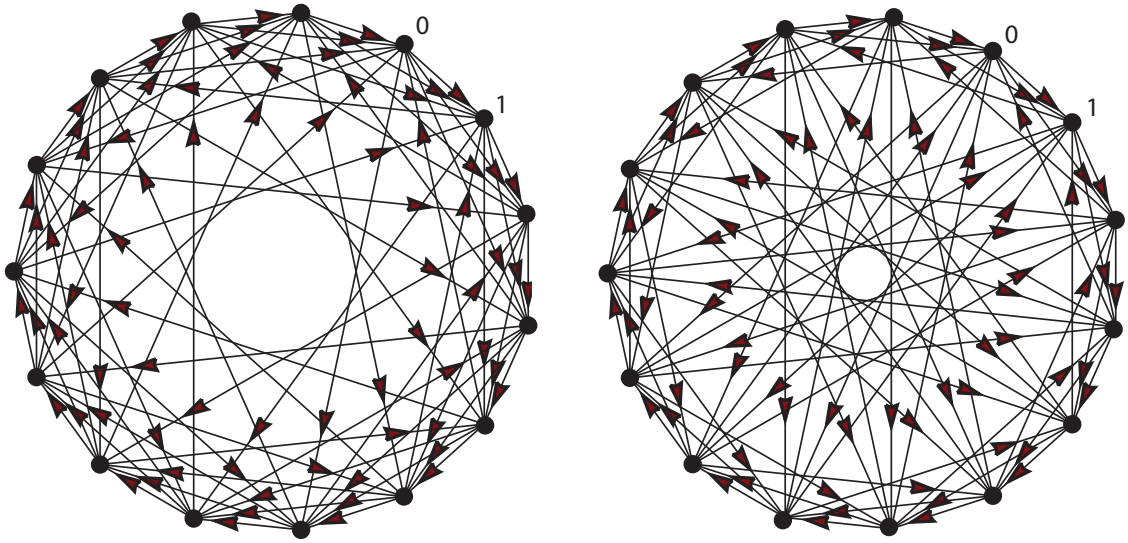


Figure 3.2: $\mathrm{Cay}(\mathbb{Z}_{15}, \{1, 2, 3, 11\})$ and $\mathrm{Cay}(\mathbb{Z}_{15}, \{1, 2, 7, 9, 12\})$

the same spectrum. In the following lists, I have put the sums that add to zero in parentheses. Letting ω be a primitive fifteenth root of unity, we have:

The spectrum of X	The spectrum of Y
$(\omega^1 + \omega^6 + \omega^{11}) + \omega^2 + \omega^3$	$(\omega^2 + \omega^7 + \omega^{12}) + \omega^1 + \omega^9$
$(\omega^2 + \omega^{12} + \omega^7) + \omega^4 + \omega^6$	$(\omega^4 + \omega^{14} + \omega^9) + \omega^2 + \omega^3$
$\omega^3 + \omega^3 + \omega^3 + \omega^6 + \omega^9$	$\omega^6 + \omega^6 + \omega^6 + \omega^3 + \omega^{12}$
$(\omega^4 + \omega^9 + \omega^{14}) + \omega^8 + \omega^{12}$	$(\omega^8 + \omega^{13} + \omega^3) + \omega^4 + \omega^6$
$(\omega^5 + \omega^0 + \omega^{10}) + \omega^{10} + \omega^0$	$(\omega^{10} + \omega^5 + \omega^0) + \omega^5 + \omega^0$
$\omega^6 + \omega^6 + \omega^6 + \omega^{12} + \omega^3$	$\omega^{12} + \omega^{12} + \omega^{12} + \omega^6 + \omega^9$
$(\omega^7 + \omega^{12} + \omega^2) + \omega^{14} + \omega^6$	$(\omega^{14} + \omega^4 + \omega^9) + \omega^7 + \omega^3$
$(\omega^8 + \omega^3 + \omega^{13}) + \omega^1 + \omega^9$	$(\omega^1 + \omega^{11} + \omega^6) + \omega^8 + \omega^{12}$
$\omega^9 + \omega^9 + \omega^9 + \omega^3 + \omega^{12}$	$\omega^3 + \omega^3 + \omega^3 + \omega^9 + \omega^6$
$(\omega^{10} + \omega^0 + \omega^5) + \omega^5 + \omega^0$	$(\omega^5 + \omega^{10} + \omega^0) + \omega^{10} + \omega^0$
$(\omega^{11} + \omega^6 + \omega^1) + \omega^7 + \omega^3$	$(\omega^7 + \omega^2 + \omega^{12}) + \omega^{11} + \omega^9$
$\omega^{12} + \omega^{12} + \omega^{12} + \omega^9 + \omega^6$	$\omega^9 + \omega^9 + \omega^9 + \omega^{12} + \omega^3$
$(\omega^{13} + \omega^3 + \omega^8) + \omega^{11} + \omega^9$	$(\omega^{11} + \omega^1 + \omega^6) + \omega^{13} + \omega^{12}$
$(\omega^{14} + \omega^9 + \omega^4) + \omega^{13} + \omega^{12}$	$(\omega^{13} + \omega^8 + \omega^3) + \omega^{14} + \omega^6$
$\omega^0 + \omega^0 + \omega^0 + \omega^0 + \omega^0$	$\omega^0 + \omega^0 + \omega^0 + \omega^0 + \omega^0$

Therefore, not all isospectral, nonisomorphic circulant graphs have an even number of vertices.

Question 3.2.3. *Let $X = Cay(\mathbb{Z}_n, A)$ and $Y = Cay(\mathbb{Z}_n, B)$ be isospectral. Must*

there exist some integer t and integer q relatively prime to n such that

$$A = \{ab + t \mid b \in B\}?$$

A quick computer test showed me that the answer to this question is "no." The graphs $\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 4, 5\})$ and $\mathrm{Cay}(\mathbb{Z}_8, \{1, 4, 5, 6\})$ have the same spectrum. However, there are no natural numbers q and t that satisfy the relation given above.

The next question deals with the undirected graphs discussed in Section 2.5.

Question 3.2.4. *What is the second largest eigenvalue of the undirected graphs defined in 2.5?*

A circulant, undirected graph with a connection set of order m is a *Ramanujan graph* if for all of the eigenvalues λ such that $|\lambda| \neq m$, we have $|\lambda| \leq 2\sqrt{m-1}$. Basically what this is saying is that Ramanujan graphs have the best possible spectral gap (or space between the largest and the second largest eigenvalues). The books (Ter99) and (DSV03) give a good introduction to spectral gaps and explain why we care so much about them.

Table 3.2: Undirected Graphs from Section 2.5 on $2^r p$ vertices

r	p	2^{nd} largest eigenvalue (approx. absolute value)	$2\sqrt{2p-1}$ (approx. value)	Ramanujan?
2	3	3.000	4.472	yes
2	5	5.854	6.000	yes
2	7	8.543	7.211	no
2	11	13.769	9.165	no
2	13	6.351	10.000	no
2	17	21.491	11.489	no
3	3	3.000	4.472	yes
3	5	4.980	6.000	yes
3	7	6.851	7.211	yes
3	11	10.513	9.165	no
3	13	12.329	9.165	no
4	3	4.243	4.472	yes
4	5	7.071	6.000	no
4	7	9.900	7.211	no
5	3	5.543	4.472	no

Although Table 3.2 shows that not all of the graphs defined in Section 2.5 can be Ramanujan, it is still of interest to know what the spectral gaps are. This remains as an open question.

Appendix A

Creating Table 3.1

To create Table 3.1, I used the following Mathematica program:

```
SetUp[num_] := Module[
   {nmin1},
   nmin1 = num - 1;
   w = Exp[2*Pi*I/num];
   primes =
    Complement[
     Table[If[GCD[t1, num] == 1, t1, null], {t1, 1, nmin1}], {null}];
   prLeng = Length[primes];
   pos = Table[t2, {t2, 1, nmin1}];
   cEigenvalues[n_, generators_] := Module[
     {eigen, teigen, g, j},
     eigen = Table[Sum[w^(g*j) , {g, generators}], {j, 0, n - 1}];
     teigen = Round[10000 N[eigen]];
     Return[teigen];
     ];
   RemoveIsos[gen_, list_] := Module[
     {table, newList},
     newList = list;
     Do[newList =
       Delete[newList,
        Position[newList, Sort[Mod[primes[[i]]*gen, num]], 1, 1]], {i,
        1, prLeng}];
     Return[newList];
     ];
   AddEigens[lis_] := Module[
     {eigs},
     eigs = cEigenvalues[num, lis];
     Return[{eigs, lis}];
     ];
```

```
   PrepList[m_] := Module[
     {gens, i, A},
     gens = Subsets[pos, {m}];
     i = 0; A = First[gens];
     While[Not[i == Length[gens]], i++; A = gens[[i]];
      gens[[i]] = AddEigens[A]; gens = RemoveIsos[A, gens]];
     Return[gens];
     ];
   ];

SearchQ[m_] := Module[
   {gens, i, j, l},
   gens = PrepList[m];
   l = Length[gens];
   Do[If[Complement[gens[[i, 1]], gens[[j, 1]]] == {},
     Print[{gens[[i, 2]], gens[[j, 2]]}], Null], {i, 1, l - 1}, {j,
     i + 1, l}];
   Return["finished searching"];
   ];

   TotalSearch[n_] := Module[
   {searchnums, nmin1},
   nmin1 = n - 1;
   SetUp[n];
   Table[Print["For m = " , s]; SearchQ[s], {s, 2, nmin1}];
   Return["That's All Folks!"];
   ];
```

Notice that this program rounds eigenvalues to the nearest $10,000^{th}$ decimal place. So, it would not be accurate enough for graphs with a large number of vertices. It is also quite inefficient, and I would not recommend using it for large graphs anyway. This is how you use the program to find isospectral, nonisomorphic graphs on n vertices:

1. Type "TotalSearch[n]"

2. The program will give you a list of pairs of connection sets that are not equivalent via multiplication by a number relatively prime to n. Each pair given produces a pair of isospectral circulant graphs. If n, $n/2$ or $n/4$ is a square-free, odd integer, then you can use the results of (Muz95) and (Muz97) to conclude that all of the pairs of graphs produced are not isomorphic. Therefore, you have a complete list (up to isomorphism) of connection sets that create isospectral, nonisomorphic graphs.

3. If neither n, $n/2$, nor $n/4$ is a square-free, odd integer, then some of the graphs created by the connection sets given may be isomorphic. You will have to use other means to check.

Here is an example of using the program to find all isospectral, nonisomorphic graphs on 8 vertices:

```
In[4]:= TotalSearch[8]

     For m = 2

     For m = 3
     {{1,2,5},{1,5,6}}

     For m = 4
     {{1,2,4,5},{1,4,5,6}}

     For m = 5

     For m = 6

     For m = 7

Out[4]= "That's All Folks!"
```

Since $\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$ is isomorphic to $\mathrm{Cay}(\mathbb{Z}_8, \{1, 5, 6\})$ and $\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 4, 5\})$ is isomorphic to $\mathrm{Cay}(\mathbb{Z}_8, \{1, 4, 5, 6\})$, we can conclude that there are no isospectral, nonisomorphic circulant graphs on 8 vertices.

References

[Ádá67] A. Ádám, *Research problem*, J. Combinatorial Theory **2** (1967), 229–230.

[Bab79] László Babai, *Spectra of Cayley graphs*, J. Combin. Theory Ser. B **27** (1979), no. 2, 180–189. MR MR546860 (81f:05090)

[CRS97] D. Cvetković, P. Rowlinson, and S. Simić, *Eigenspaces of graphs*, Encyclopedia of Mathematics and its Applications, vol. 66, Cambridge University Press, Cambridge, 1997. MR MR1440854 (98f:05111)

[Cve71] Dragoš M. Cvetković, *Graphs and their spectra*, Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz. (1971), no. 354–356, 1–50. MR MR0299508 (45 #8556)

[DGT81] S.S. D'Amato, B.M. Gimarc, and N. Trinajstić, *Isospectral and subspectral molecules*, Croat. Chem. Acta. **54** (1981), no. 1, 1–52.

[DSV03] Giuliana Davidoff, Peter Sarnak, and Alain Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London Mathematical Society Student Texts, vol. 55, Cambridge University Press, Cambridge, 2003. MR MR1989434 (2004f:11001)

[ET70] Bernard Elspas and James Turner, *Graphs with circulant adjacency matrices*, J. Combinatorial Theory **9** (1970), 297–307. MR MR0272659 (42 #7540)

[GHM77] C. Godsil, D. A. Holton, and B. McKay, *The spectrum of a graph*, Combinatorial mathematics, V (Proc. Fifth Austral. Conf., Roy. Melbourne Inst. Tech., Melbourne, 1976), Springer, Berlin, 1977, pp. 91–117. Lecture Notes in Math., Vol. 622. MR MR0544356 (58 #27642)

[GM82] C. D. Godsil and B. D. McKay, *Constructing cospectral graphs*, Aequationes Math. **25** (1982), no. 2-3, 257–268. MR MR730486 (85b:05124)

[GR01] Chris Godsil and Gordon Royle, *Algebraic graph theory*, Graduate Texts in Mathematics, vol. 207, Springer-Verlag, New York, 2001. MR MR1829620 (2002f:05002)

[Li99] Cai Heng Li, *Finite CI-groups are soluble*, Bull. London Math. Soc. **31** (1999), no. 4, 419–423. MR MR1687493 (2000d:05056)

[LL00] T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109. MR MR1736695 (2001f:11135)

[LSV06] Alexander Lubotzky, Beth Samuels, and Uzi Vishne, *Isospectral Cayley graphs of some finite simple groups*, Duke Math. J. **135** (2006), no. 2, 381–393. MR MR2267288 (2007j:05099)

[MKP01] Mikhail Muzychuk, Mikhail Klin, and Reinhard Pöschel, *The isomorphism problem for circulant graphs via Schur ring theory*, Codes and association schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001, pp. 241–264. MR MR1816402 (2002g:05128)

[Muz95] Mikhail Muzychuk, *Ádám's conjecture is true in the square-free case*, J. Combin. Theory Ser. A **72** (1995), no. 1, 118–134. MR MR1354970 (96m:05141)

[Muz97] ———, *On Ádám's conjecture for circulant graphs*, Discrete Math. **176** (1997), no. 1-3, 285–298. MR MR1477298 (98h:05141b)

[Muz04] ———, *A solution of the isomorphism problem for circulant graphs*, Proc. London Math. Soc. (3) **88** (2004), no. 1, 1–41. MR MR2018956 (2004h:05084)

[Pál87] P. P. Pálfy, *Isomorphism problem for relational structures with a cyclic automorphism*, European J. Combin. **8** (1987), no. 1, 35–43. MR MR884062 (88i:05097)

[Ter99] Audrey Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, vol. 43, Cambridge University Press, Cambridge, 1999. MR MR1695775 (2000d:11003)