Spectra of Semidirect Products of Cyclic Groups

Nathan Fox[1]
University of Minnesota-Twin Cities

Abstract

The spectrum of a graph is the set of eigenvalues of its adjacency matrix. A group, together with a multiset of elements of the group, gives a Cayley graph, and a semidirect product provides a method of producing new groups. This paper compares the spectra of cyclic groups to those of their semidirect products, when the products exist. It was found that many of the interesting identities that result can be described through number theory, field theory, and representation theory. The main result of this paper gives a formula that can be used to find the spectrum of semidirect products of cyclic groups.

1 Introduction

Given a graph, its spectrum is defined as the set of eigenvalues of its adjacency matrix. The adjacency matrix encodes all of the information about a graph in a compact form. A group, together with a multiset of elements, gives a Cayley graph. Semidirect products are an interesting way of producing small, non-abelian groups. The semidirect products that we will consider are built from cyclic groups. We will examine the spectra of cyclic groups as well as those of their semidirect products, when the products exist. Our main technical result (Theorem 4.1) is a general formula which factors the characteristic polynomial of the adjacency matrix of the Cayley graph of a semidirect product of cyclic groups as a product of characteristic polynomials of some simple matrices, as follows:

$$\chi\left(A\left(C\left(\mathbb{Z}/n \rtimes_k \mathbb{Z}/m, S\right)\right)\right) = \prod_{i=0}^{n-1} \chi\left(\sum_{x^a y^b \in S} \Omega_{ia}\left(C_m\right)^b\right).$$

[1]This reasearch was carried out at Canisius College with funding from the National Science Foundation. The author would like to thank Dr. Terrence Bisson for his assistance.

Here S is an arbitrary set of elements in the group; the notation will be explained in Section 3.1. Several applications of this result are given; in particular, Theorem 4.4 seems to be new.

Section 2 will provide some background information on spectra of graphs, on Cayley graphs, and on semidirect products. Section 3 will discuss how the adjacency matrices for Cayley graphs relate to representation theory. In particular we interpret the regular representation of a finite group in terms of Cayley graphs (the *adjacency representation*). In the remainder of the section we describe an isomorphic representation (the *natural representation*) for semidirect products of cyclic groups. Section 4 begins with a proof of the main theorem, and then it presents a number of applications of this theorem. Finally, Section 5 illustrates an elegant result related to representations and Cayley graphs, while mentioning potential future extensions of this research.

2 Background

In this paper we work with directed graphs.

Definition 2.1. *The adjacency matrix of a directed graph X with n vertices is an $n \times n$ matrix in which the ij^{th} entry is the number of directed edges from vertex i to vertex j in X, where the vertices in X are numbered from 1 to n.*

A major component of algebraic graph theory is the study of the eigenvalues of a graph. The eigenvalues of a graph are simply the eigenvalues of the adjacency matrix of the graph, that is, the roots of the characteristic polynomial of the adjacency matrix. For more information on algebraic graph theory, see [3], for instance.

An immediate thought is whether the order of the numbering affects the characteristic polynomial. The answer is that it does not: isomorphic graphs are isospectral. The converse is not true, however. There are graphs whose characteristic polynomials are the same, yet they are not isomorphic.

For a graph X, let $A(X)$ denote the adjacency matrix of the graph, and for a square matrix M, let $\chi(M)$ denote the characteristic polynomial of M.

The spectrum of a graph reflects certain properties of the graph. For example, multiplicities of eigenvalues make implications about symmetries of the graph. Additionally, the eigenvalues encode information about long paths. Therefore, it is important to discover methods of computing these eigenvalues, or characteristic polynomials, more quickly than building a large adjacency matrix and taking a determinant. Specifically, we will look at a type of directed graph that is derived from a group: a *Cayley graph*.

Definition 2.2. *Given a group G and a multiset S such that $s \in S$ for all $s \in S$, the* ***Cayley graph with generators*** *S is a directed graph with one vertex corresponding to each group element, and for each pair of elements $g_1, g_2 \in G$ there is an edge from g_1 to g_2 for each element $s \in S$ such that $g_1 s = g_2$. Denote this graph as $C(G, S)$.*

Note that S generates the graph, but not necessarily the group. The Cayley graph will be connected if and only if S generates the group. It is more useful, though, to consider arbitrary multisets of elements of the group.

More specifically, we shall examine Cayley graphs of specific groups that can be built from less complicated pieces: semidirect products of cyclic groups.

2.1 Semidirect Products of Groups

In general, spectra of Cayley graphs can be quite complicated. The spectra of finite abelian groups are known, but comparatively little is known about the spectra of even the smallest non-abelian groups. The least complicated non-abelian groups can be built from cyclic groups using a *semidirect product*.

Definition 2.3. *Given two groups G and H and a group homomorphism $\varphi : H \longrightarrow \mathrm{Aut}(G)$, the* **Semidirect Product** *of G and H with respect to φ, denoted $G \rtimes_\varphi H$ (or, simply, $G \rtimes H$) is a new group with set $G \times H$ and multiplication operation $(g_1, h_1)(g_2, h_2) = (g_1 \varphi(h_1) g_2, h_1 h_2)$.*

In practice, Definition 2.3 can be complicated to use. Luckily, when G and H are both cyclic, there is a nice presentation. For this paper, we will use multiplicative notation for cyclic groups, where $\mathbb{Z}/n$ is generated by an element x such that $x^n = e$.

Proposition 2.1. *Given cyclic groups $\mathbb{Z}/n$ and $\mathbb{Z}/m$, a semidirect product $\mathbb{Z}/n \rtimes \mathbb{Z}/m$ between them corresponds to a choice of integer k such that $k^m \equiv 1 \pmod{n}$. The semidirect product group is given by $\mathbb{Z}/n \rtimes \mathbb{Z}/m = \langle x, y \mid x^n = e, y^m = e, yxy^{-1} = x^k \rangle$, and will be denoted $\mathbb{Z}/n \rtimes_k \mathbb{Z}/m$.*

A proof of this proposition can be found in [2]. The idea is that k gives a group homomorphism from $\mathbb{Z}/m$ to $\mathrm{Aut}\left(\mathbb{Z}/n\right)$.

When constructing an adjacency matrix for a Cayley graph of a semidirect product of cyclic groups, we will always assume that the vertices are ordered such that the first row and column of the matrix correspond to the identity, the next $n-1$ rows and columns correspond to powers of x in increasing order, and then each block of n rows and columns corresponds to the powers of y in ascending order (and within each block, the powers of x take the same order).

3 Cayley Graphs and Representations

Representation theory is the study of embedding groups as subgroups of $GL_N\left(\mathbb{F}\right)$ for some integer N and some field $\mathbb{F}$. The embedding map is a homomorphism $\psi : G \longrightarrow GL_N\left(\mathbb{F}\right)$, and we say that the representation is *faithful* if ψ is injective. In this paper, we are mainly concerned with representations of groups of order n embedded in $GL_n\left(\mathbb{C}\right)$, or, more specifically, $GL_n\left(\mathbb{Q}\left[\omega\right]\right)$ for some root of unity ω. Note that all of the fields that we are concerned with have characteristic zero.

Given a group G and an element $g \in G$, let $A_g = A\left(C\left(G, \{g\}\right)\right)$, the adjacency matrix of the Cayley graph with one generator. Additionally, given a group G and a multiset S of elements of G, let $A_S = A\left(C\left(G, S\right)\right)$.

Theorem 3.1. *Given a group G and an element $g \in G$, consider the set $\Gamma = \{A_g \mid g \in G\}$ and the map $\psi : G \longrightarrow \Gamma$ given by $\psi\left(g\right) = A_g$. Then, ψ gives a faithful representation for G in $GL_{|G|}\left(\mathbb{Q}\right)$.*

Proof. Consider $X = C\left(G, G\right)$ Each matrix in Γ determines a subgraph of X. Consider two matrices $A_{g_1}, A_{g_2} \in \Gamma$. The matrix A_{g_1} gives the number of paths in X of length one from a group element h_1 to a group element h_2 following only paths corresponding to multiplication by g_1. Similarly, A_{g_1} gives the number of paths in X of length one from a group element h_1 to a group element h_2 following only paths corresponding to multiplication by g_2. Thus, $A_{g_1}A_{g_2}$ gives the number of paths in X of length two from a group element h_1 to a group element h_2 following only paths corresponding to a multiplication by g_1 followed by a multiplication by g_2. This is equivalent to following only paths of length one corresponding to multiplication by g_1g_2.

Thus, $A_{g_1}A_{g_2} = A_{g_1g_2}$. Therefore, it is clear that Γ is a faithful representation for G with injection ψ. □

Based on this theorem, we can define a group representation based on the adjacency matrices of Cayley graphs.

Definition 3.1. *The* ***adjacency representation*** *of a group G is the representation given by ψ.*

This is called the regular representation in the literature [5]. The next theorem will allow for simple computation of adjacency matrices when multiple generators are used.

Theorem 3.2. *Given a group G and a multiset S of elements of G,*

$$A_S = \sum_{s \in S} A_s.$$

Proof. The proof is by induction on $|S|$.

For the base case, $|S| = 1$. This means that $S = \{s\}$ for some $s \in G$. It is obviously true that

$$A_S = A_s = \sum_{r \in \{s\}} A_r.$$

Now, as an inductive hypothesis, assume that if $|S| < h$, then

$$A_S = \sum_{s \in S} A_s.$$

Let $|S| = h$. $S = T \uplus \{s\}$ for some $s \in G$ and some multiset T. Clearly, every edge in $C(G, T)$ is present in $C(G, S)$ because $T \subset S$. All of the additional edges come from $C(G, \{s\})$. Thus, $A_S = A_T + A_s$. By the inductive hypothesis,

$$A_S = A_s + \sum_{t \in T} A_t = \sum_{s \in S} A_s$$

as required. □

3.1 Preliminary Notation and Results

The following definitions and propositions will be extremely important for the remainder of the paper. They will be used, beginning in the next section, to describe representations of semidirect products.

Definition 3.2. *Let C_h be the $h \times h$ matrix with entries*

$$c_{ij} = \begin{cases} 1, \text{ when } j - i \equiv 1 \pmod{h} \\ 0, \text{otherwise} \end{cases}.$$

This matrix is denoted C_h because it is a circulant matrix [?davis]. C could also denote "cyclic", as C_h is the adjacency matrix for the Cayley graph of $\mathbb{Z}/h$ with $S = \{x\}$ (where $x^h = e$).

Proposition 3.1. *The matrix $(C_h)^d$ is given by*

$$c_{ij} = \begin{cases} 1, \text{ when } j - i \equiv d \pmod{h} \\ 0, \text{otherwise} \end{cases}.$$

Proof. The first part of the proof is by induction on d.

For the base case, let $d = 1$. The definition of C_h completes the proof of this case, as $(C_h)^1 = C_h$.

Now, let $b > 1$. Assume that $(C_h)^{b-1}$ is given by the specified formula. $(C_h)^b = (C_h)^{b-1} C_h$, and entries that are one in this matrix are those where the i^{th} row of $(C_h)^{b-1}$ has a one in the k^{th} column and the k^{th} row of C_h has a one in the j^{th} column. All other entries are zero. This occurs when

$$\begin{cases} k - i \equiv b - 1 \pmod{h} \\ j - k \equiv 1 \pmod{h} \end{cases}.$$

Solving the first equation for k yields $k \equiv b - 1 + i \pmod{h}$. Substituting this into the other equation gives $j - b + 1 - i \equiv 1 \pmod{h}$, or $j - i \equiv b \pmod{h}$, as required.

Now, let $d < 1$. Note that, by the previous steps, $(C_h)^h = I$. Thus, $(C_h)^d = \left((C_h)^h\right)^m \cdot (C_h)^d = (C_h)^{mh+d}$. Since $h > 0$, there must exist an integer m such that the quantity $mh + d > 0$, and this quantity will be congruent to d modulo h. Thus, the proposition holds for all integers d. $\square$

Definition 3.3. *Suppose that m, n, and k satisfy $m^k \equiv 1 \pmod{n}$. For given h, let let Ω_h be the $m \times m$ matrix with entries*

$$\Omega_{ij} = \begin{cases} \omega^{hk^{i-1}}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}$$

where $\omega = e^{\frac{2\pi i}{n}}$ is a primitive n^{th} root of unity.

(In general, the primitive h^{th} root of unity $e^{\frac{2\pi i}{h}}$ will be denoted ω_h, but sometimes the subscript will be omitted if the meaning seems clear.)

This matrix is denoted Ω_h because it contains roots of unity, which are denoted by ω.

Proposition 3.2. *Powers of the matrix Ω_h are given by $(\Omega_h)^a = \Omega_{ha}$*

Proof. $(\Omega_h)^a$ is an $m \times m$ matrix with entries

$$\Omega_{ij} = \begin{cases} \omega^{hak^{i-1}}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}.$$

This is clearly equal to Ω_{ha}. □

3.2 Representations of Semidirect Products of Cyclic Groups

When it is known that G is a semidirect product of cyclic groups, another representation in $GL_{|G|}(\mathbb{C})$ can be found. This new representation will have a form such that computation of characteristic polynomials, and hence, eigenvalues, is easier than in the adjacency representation. First, however, it is useful to examine exactly what form the matrices in the adjacency representation take. For the following theorem, recall that A_g is the adjacency matrix of a Cayley graph with one generator.

Let x be a generator for $\mathbb{Z}/n$ and y a generator for $\mathbb{Z}/m$.

Theorem 3.3. *For a semidirect product $\mathbb{Z}/n \rtimes_k \mathbb{Z}/m$, A_x is an $m \times m$ block matrix with $n \times n$ matrix entries given by*

$$x_{ij} = \begin{cases} (C_n)^{k^{i-1}}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}$$

and A_y is an $m \times m$ block matrix with $n \times n$ matrix entries given by

$$y_{ij} = \begin{cases} I, \text{ when } j - i \equiv 1 \pmod{n} \\ 0, \text{otherwise} \end{cases}.$$

Proof. Consider the group element $g = x^a y^b$. $gx = x^a y^b x = x^{a+k^b} y^b$, so A_x is in the required form. $gy = x^a y^{b+1}$, so A_y is in the required form. □

Now, we can find a representation such that computation is easier.

Theorem 3.4. *Let X be an $n \times n$ block matrix with $m \times m$ matrix entries given by*

$$x_{ij} = \begin{cases} \Omega_i, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}$$

and let Y be an $n \times n$ block matrix with $m \times m$ matrix entries given by

$$y_{ij} = \begin{cases} C_m, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}.$$

The matrices X and Y generate a faithful representation of $\mathbb{Z}/n \rtimes_k \mathbb{Z}/m$ with injection φ such that $\varphi\left(x^a y^b\right) = X^a Y^b$.

Proof. We will show that $X^n = I$, $Y^m = I$, and $YXY^{-1} = X^k$, thereby precisely showing that φ produces a representation. Showing that no smaller power of X or Y is trivial will show that φ is injective.

X^a is an $n \times n$ block matrix with $m \times m$ matrix entries given by

$$x_{ij} = \begin{cases} (\Omega_i)^a = \Omega_{ia}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}.$$

Since $(\Omega_h)^n = I$ for all h by Proposition 3.2, $X^n = I$. Also, note that Ω_1 is a diagonal matrix containing a primitive n^{th} root of unity in the upper left corner. Thus, no smaller power of this matrix, and, hence, no smaller power of X, can be the identity.

Y^b is an $n \times n$ block matrix with $m \times m$ matrix entries given by

$$y_{ij} = \begin{cases} (C_m)^b, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}.$$

Based on Proposition 3.1, $Y^m = I$, and no smaller power of Y is trivial (as no smaller power of C_m is trivial).

Y^{-1} is an $n \times n$ block matrix with $m \times m$ matrix entries given by

$$y_{ij} = \begin{cases} (C_m)^{-1}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}.$$

Thus, YXY^{-1} is an $n \times n$ block matrix with $m \times m$ matrix entries given by

$$a_{ij} = \begin{cases} C_m \Omega_i (C_m)^{-1}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}.$$

To show that this equals X^k it suffices to show that $C_m \Omega_h (C_m)^{-1} = \Omega_{hk}$. $C_m \Omega_h$ is an $m \times m$ matrix with entries

$$a_{ij} = \begin{cases} \omega^{hk^{j-1}}, \text{ when } j - i \equiv 1 \,(\text{mod}\, m) \\ 0, \text{otherwise} \end{cases}.$$

Multiplying this by $(C_m)^{-1}$ (as given by Proposition 3.1) yields

$$a_{ij} = \begin{cases} \omega^{hk^j}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}.$$

This precisely equals Ω_{hk}, thereby completing the proof. □

Definition 3.4. *The* ***natural representation*** *of* $\mathbb{Z}/n \rtimes_k \mathbb{Z}/m$ *is the representation given by* φ*.*

We say that two representations M and N of a group G are *isomorphic* if the matrices M_g and N_g corresponding to a group element g are similar (that is, one can be obtained from the other via a change of basis) and for all group elements, that change of basis is the same. This allows the isomorphism to be applied to linear combinations of representation matrices as well:

Let P be the change of basis matrix to move from one representation to an isomorphic one, let A and B be matrices in the first representation, and let A' and B' be their corresponding matrices in the second representation (so $A' = PAP^{-1}$ and $B' = PBP^{-1}$). Then, for scalars a and b, $P(aA + bB)P^{-1} = PaAP^{-1} + PbBP^{-1} = aPAP^{-1} + bPBP^{-1} = aA' + bB'$, which corresponds to $aA + bB$ by the same isomorphism.

Theorem 3.5. *The adjacency representation and the natural representation of* $\mathbb{Z}/n \rtimes_k \mathbb{Z}/m$ *are isomorphic group representations.*

Proof. It is well-known that two representations over a field of characteristic zero are isomorphic if the traces of corresponding matrices are the same [5]. I will show that $\operatorname{tr}\left(A_{x^a y^b}\right) = \operatorname{tr}\left(X^a Y^b\right)$ in all cases. Note that $x^a y^b = e$ if and only if $X^a Y^b = I$. Clearly $\operatorname{tr}(A_e) = \operatorname{tr}(I) = mn$. This proves the identity case.

Now, consider representations of the element $x^a y^b$, where $x^a y^b \neq e$. The adjacency representation of this element is $A_{x^a y^b}$. $C\left(\mathbb{Z}/n \rtimes_k \mathbb{Z}/m, \left\{x^a y^b\right\}\right)$ has no self-loops, so all of the diagonal entries of $A_{x^a y^b}$ are zero. Thus, $\operatorname{tr}\left(A_{x^a y^b}\right) = 0$. The natural representation of this element is $X^a Y^b$. Clearly, X^a has matrix entries given by

$$x_{ij} = \begin{cases} (\Omega_i)^a = \Omega_{ia}, \text{ when } i = j \\ 0, \text{otherwise} \end{cases}$$

and Y^b has matrix entries given by

$$y_{ij} = \begin{cases} (C_m)^b, \text{ when } i = j \\ 0, \text{otherwise} \end{cases} .$$

Thus, $X^a Y^b$ has matrix entries given by

$$xy_{ij} = \begin{cases} (\Omega_i)^a (C_m)^b = \Omega_{ia} (C_m)^b, \text{ when } i = j \\ 0, \text{otherwise} \end{cases} .$$

Clearly, if $b \not\equiv 0 \pmod{m}$, this matrix has zeroes down the diagonal, and, therefore, has trace 0.

Consider the case where $b = 0$. I will show that $\operatorname{tr}(X^a) = 0$ (if $a \not\equiv 0 \pmod{n}$).

$$\operatorname{tr}(X^a) = \sum_{i=0}^{n-1} \operatorname{tr}(\Omega_{ia}) = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \omega^{iak^j}.$$

Now, assume that $iak^j = r$ for some value of r. Clearly, $r = sa$ for some s. Thus, we have $ik^j = s$, or $i = k^{-j}s$. Thus, for each value of s, there will be m terms in the double sum that equal sa. This means that the double sum equals

$$m \sum_{i=0}^{n-1} \omega^i = m \left(\frac{\omega^n - 1}{\omega - 1} \right) = 0$$

as required. Therefore, these two group representations are isomorphic. □

Now that we know that these representations are isomorphic, we can convert between the two representations at will. Any group-theoretic statement that is true with the adjacency representation is also true with the natural representation. In particular, corresponding matrices will have the same characteristic polynomial. This fact will be quite important in the proof of the main theorem, in the next section.

4 Characteristic Polynomials of Semidirect Products of Cyclic Groups

The following is our main result about characteristic polynomials of semidirect products of cyclic groups. It can be applied in numerous specific cases to yield information about the spectra of Cayley graphs of semidirect products of cyclic groups. Sometimes, it can even lead to explicit formulas for the eigenvalues.

Theorem 4.1. *The characteristic polynomial of the semidirect product of two cyclic groups is given by the following:*

$$\chi\left(A\left(C\left(\mathbb{Z}/n \rtimes_k \mathbb{Z}/m, S\right)\right)\right) = \prod_{i=0}^{n-1} \chi\left(\sum_{x^a y^b \in S} \Omega_{ia}\left(C_m\right)^b\right)$$

Proof. Let $G = \mathbb{Z}/n \rtimes_k \mathbb{Z}/m$. By Theorem 3.2,

$$\chi\left(A\left(C\left(G, S\right)\right)\right) = \chi\left(\sum_{s\in S} A\left(C\left(G, \{s\}\right)\right)\right) = \chi\left(\sum_{s\in S} A_s\right).$$

Since $s \in G$, it can be written uniquely as $x^a y^b$ for some $0 \le a < n$ and some $0 \le b < m$. Thus, the formula becomes

$$\chi\left(\sum_{x^a y^b \in S} A_{x^a y^b}\right) = \chi\left(\sum_{x^a y^b \in S} X^a Y^b\right),$$

by Theorem 3.5. Then, by Definition 3.4 (and Theorem 3.5), it becomes

$$\prod_{i=0}^{n-1} \chi\left(\sum_{x^a y^b \in S} \left(\Omega_i\right)^a \left(C_m\right)^b\right) = \prod_{i=0}^{n-1} \chi\left(\sum_{x^a y^b \in S} \Omega_{ia}\left(C_m\right)^b\right)$$

by Proposition 3.2, as required. □

The rest of this section and all of the next section will show a variety of ways in which this formula can be applied. The easiest examples allow for direct computation of eigenvalues, whereas other applications only allow for computation of a characteristic polynomial.

4.1 Spectra of Finite Abelian Groups

An immediate application of Theorem 4.1 is to the calculation of spectra of Cayley graphs of finite abelian groups. For example, the following theorem about the spectra of cyclic groups was proved at the 2006 REU project at Canisius [4].

Proposition 4.1. *The eigenvalues of $C(\mathbb{Z}/n, S)$ are given by*

$$\left\{\lambda \mid \lambda = \sum_{s\in S} \omega^{xs}, x \in \mathbb{Z}, 1 \le x \le n\right\}.$$

Proof. Clearly, $\mathbb{Z}/n \cong \mathbb{Z}/n \times \mathbb{Z}/1 \cong \mathbb{Z}/n \rtimes_1 \mathbb{Z}/1$. That means that $\Omega_h = I_1 \omega^h$. Thus, by Theorem 4.1,

$$\begin{aligned}\chi\left(A\left(C\left(\mathbb{Z}/n, S\right)\right)\right) &= \prod_{i=0}^{n-1} \chi\left(\sum_{x^a\in S} \Omega_{ia}\right) &&= \prod_{i=0}^{n-1} \chi\left(\sum_{x^a\in S} I_1\omega^{ia}\right)\\ &= \prod_{i=0}^{n-1} \chi\left(I_1 \sum_{x^a\in S} \omega^{ia}\right) &&= \prod_{i=0}^{n-1} \left(\lambda - \sum_{x^a\in S} \omega^{ia}\right)\end{aligned}$$

which is clearly the required formula. □

A much more general result can also be proved regarding spectra of finite abelian groups.

Theorem 4.2. *Let $x_1, \ldots, x_h$ be generators for cyclic groups $\mathbb{Z}/n_1, \ldots, \mathbb{Z}/n_h$. The eigenvalues of the Cayley graph of this product group with generators S has eigenvalues*

$$\left\{\lambda \mid \lambda = \sum_{s\in S} \prod_{i=1}^{h} \omega_{n_i}^{j_i a_i}, 0 \le j_b < n_b\right\},$$

where each s in the sum is written as

$$s = \prod_{b=1}^{h} x_i^{a_i}$$

for some sequence of values a_i.

Proof. According to [5], a representation with matrices of dimension

$$\prod_{i=1}^{h} n_h \times \prod_{i=1}^{h} n_h$$

can be built as a tensor product from the natural representations of the cyclic groups, and it will clearly be isomorphic to the analog built as a tensor product of the adjacency representations. All of the matrices in this representation will be diagonal, so the eigenvalues of their linear combinations will be the linear combinations of their entries. These are precisely the eigenvalues specified by the formula. □

Corollary 4.1. *Let x be a generator for $\mathbb{Z}/n$, and let y be a generator for $\mathbb{Z}/m$. The eigenvalues of $C\left(\mathbb{Z}/n \times \mathbb{Z}/m, \{x, y\}\right)$ are*

$$\left\{\lambda \mid \lambda = \omega_n^i + \omega_m^j, 0 \leq i < n, 0 \leq j < m\right\}.$$

Proof. Apply Theorem 4.2 with $h = 2$, $n_1 = n$, $n_2 = m$, and $S = \{x, y\}$. □

4.2 Examples of Spectra of Semidirect Products of Cyclic Groups

In addition to confirming known results about abelian groups, Theorem 4.1 can also be used to investigate spectra of non-abelian semidirect products. The least complicated such groups are *dihedral groups.*

Definition 4.1. *The* ***dihedral group of order*** *$2n$, denoted D_{2n}, is $\mathbb{Z}/n \rtimes_{-1} \mathbb{Z}/2$.*

Theorem 4.1 leads to a general form for the characteristic polynomials of Cayley graphs of dihedral groups with arbitrary generators.

Theorem 4.3.

$$\chi\left(A\left(C\left(D_{2n}, S\right)\right)\right) =$$
$$\prod_{i=0}^{n-1}\left(\lambda^2 - \lambda\sum_{x^a\in S}\left(\omega^{ia}+\omega^{-ia}\right) + \left(\sum_{x^a\in S}\sum_{x^b\in S}\omega^{ia}\omega^{-ib} - \sum_{x^a y\in S}\sum_{x^b y\in S}\omega^{ia}\omega^{-ib}\right)\right)$$

Proof. Applying Theorem 4.1 yields

$$\chi\left(A\left(C\left(D_{2n}, S\right)\right)\right) = \prod_{i=0}^{n-1}\chi\left(\sum_{x^a\in S}\Omega_i + \sum_{x^a y\in S} C_2\right).$$

$$\sum_{x^a\in S}\Omega_i + \sum_{x^a y\in S} C_2 = \begin{bmatrix} \sum_{x^a\in S}\omega^{ia} & \sum_{x^a y\in S}\omega^{ia} \\ \sum_{x^a y\in S}\omega^{-ia} & \sum_{x^a\in S}\omega^{-ia} \end{bmatrix}.$$

This is a 2×2 matrix with complex entries. It has characteristic polynomial

$$\left(\lambda - \sum_{x^a\in S}\omega^{ia}\right)\left(\lambda - \sum_{x^a\in S}\omega^{-ia}\right) - \left(\sum_{x^a y\in S}\omega^{ia}\right)\left(\sum_{x^a y\in S}\omega^{-ia}\right)$$

$$= \lambda^2 - \lambda\sum_{x^a\in S}\left(\omega^{ia}+\omega^{-ia}\right) + \left(\sum_{x^a\in S}\sum_{x^b\in S}\omega^{ia}\omega^{-ib} - \sum_{x^a y\in S}\sum_{x^b y\in S}\omega^{ia}\omega^{-ib}\right).$$

Substituting this into the original formula yields

$$\prod_{i=0}^{n-1}\left(\lambda^2 - \lambda\sum_{x^a\in S}\left(\omega^{ia}+\omega^{-ia}\right) + \left(\sum_{x^a\in S}\sum_{x^b\in S}\omega^{ia}\omega^{-ib} - \sum_{x^a y\in S}\sum_{x^b y\in S}\omega^{ia}\omega^{-ib}\right)\right)$$

as required. □

An application of Theorem 4.3 leads to the following theorem, which was shown at the 2006 REU at Canisius [1].

Corollary 4.2. $\chi\left(A\left(C\left(D_{2n}, \{x, y\}\right)\right)\right) = \lambda^n \cdot \chi\left(A\left(C\left(\mathbb{Z}/n, \{\pm 1\}\right)\right)\right)$

Proof. Applying Theorem 4.3 yields

$$\begin{aligned}\chi\left(A\left(C\left(D_{2n},\{x,y\}\right)\right)\right) &= \prod_{i=0}^{n-1}\left(\lambda^2-\lambda\left(\omega^i+\omega^{-i}\right)+\left(\omega^i\omega^{-i}-\omega^i\omega^{-i}\right)\right)\\ &= \prod_{i=0}^{n-1}\lambda\left(\lambda-\left(\omega^i+\omega^{-i}\right)\right)\\ &= \lambda^n\prod_{i=0}^{n-1}\left(\lambda-\left(\omega^i+\omega^{-i}\right)\right)\\ &= \lambda^n\chi\left(A\left(C\left(\mathbb{Z}/n,\{\pm 1\}\right)\right)\right)\end{aligned}$$

by Proposition 4.1, as required. □

Another relatively well-behaved type of semidirect product is that formed between two cyclic groups of odd prime order. Theorem 4.4 is another application of Theorem 4.1.

Theorem 4.4. *Let p_1 and p_2 be odd primes such that p_1 divides p_2-1. (It is well known that this condition is necessary and sufficient for a nontrivial semidirect product to exist* [2]*.) Let k give a nontrivial semidirect product. Then,*

$$\begin{aligned}\chi\left(A\left(C\left(\mathbb{Z}/p_2\rtimes_k\mathbb{Z}/p_1,\{x,y\}\right)\right)\right) &= \prod_{i=0}^{p_2-1}\left(\prod_{j=0}^{p_1-1}\left(\lambda-\omega^{ik^j}\right)-1\right)\\ &= \left((\lambda-1)^{p_1}+1\right)q\left(\lambda\right)^{p_1}\end{aligned}$$

for some polynomial $q(\lambda)$.

Theorem 4.4 will require two lemmas to be proven. The first lemma gives the beginnings of a form for the characteristic polynomials of these groups. This lemma will be presented in a more general form than required to prove the theorem, as it holds for any semidirect product $\mathbb{Z}/n\rtimes_k\mathbb{Z}/m$.

For the remainder of this paper, given m, n, and k satifying $m^k\equiv 1\ (\mathrm{mod}\ n)$, let $Z_i=\Omega_i+C_m$, where Ω_i and C_m are both $m\times m$.

Lemma 4.1. *For a semidirect product $\mathbb{Z}/n\rtimes_k\mathbb{Z}/m$, for every value of h,*

$$\chi\left(Z_h\right)=\prod_{j=0}^{m-1}\left(\lambda-\omega^{hk^j}\right)-1.$$

Proof. Of course $\chi(Z_h) = \det(\lambda I - Z_h)$. This matrix has binomials on the main diagonal, ones on the superdiagonal and in the lower left corner, and zeroes elsewhere. By Leibniz's formula,

$$\det A = \sum_{\sigma \in S_{mn}} \operatorname{sgn}(\sigma) \prod_{i=1}^{mn} a_{i,\sigma(i)}.$$

In $\lambda I - Z_h$, choosing a nonzero element in the first row amounts to choosing a nonzero element in either the last row (if the binomial on the main diagonal is chosen) or in the second row (if the -1 on the superdiagonal is chosen). It is clear that this process propagates so that the only permutations choosing only nonzero elements are the one that selects the diagonal entries (the identity permutation, which is even) and the one that selects the superdiagonal elements and the lower left element, which is a cycle of length m, and, hence, has sign $(-1)^{m+1}$. Since this term without the sign is the product of -1 m times, it is true that

$$\chi(Z_h) = \det(\lambda I - Z_h) = \prod_{j=0}^{m-1} \left(\lambda - \omega^{hk^j}\right) - 1$$

as required. □

Let p_2 be an odd prime. In order to state the next lemma, we need the following.

Definition 4.2. *Let $a, b \in \mathbb{Z}$. Let $\sim$ be the relation on $\mathbb{Z}/p_2^\times$ given by $a \sim b$ if $a = k^d b$ for some $d \in \mathbb{Z}$.*

Proposition 4.2. *$\sim$ is an equivalence relation.*

Proof. I will show that $\sim$ satisfies the axioms of an equivalence relation.
<u>Reflexivity:</u> $a = ak^0$, so $a \sim a$.
<u>Symmetry:</u> Let $a \sim b$. This means that there exists an integer d such that $ak^d = b$. Note that $bk^{-d} = a$, where k^{-d} is defined as the inverse of k modulo p_2 raised to the d power. This means that $b \sim a$.
<u>Transitivity:</u> Let $a \sim b$ and $b \sim c$. This means that there exist integers d_1 and d_2 such that $ak^{d_1} = b$ and $bk^{d_2} = c$. Note that $ak^{d_1}k^{d_2} = ak^{d_1+d_2} = c$. This means that $a \sim c$.
Therefore, $\sim$ is an equivalence relation. □

The second lemma establishes equality of characteristic polynomials of blocks within the partitions specified by Definition 4.2.

Lemma 4.2. *When working with a semidirect product of cyclic groups of odd prime order (so $n = p_2$ and $m = p_1$, if $a \sim b$, then $\chi(Z_a) = \chi(Z_b)$).*

Proof. First, I will show that all of the equivalence classes given by $\sim$ have the same size. Consider an arbitrary element $h \in \mathbb{Z}/p_2^{\times}$. The partition of $\mathbb{Z}/p_2^{\times}$ containing h is $\{m \mid m = hk^d \text{ for some } d\}$. Recall that $k^{p_1} \equiv 1 \pmod{p_2}$. Since p_1 is prime, no smaller power of k can be one. Thus, the size of the partition containing h must be p_1. Since h was arbitrary, all partitions must have size p_1 (and, hence, there are $\frac{p_2-1}{p_1}$ of them).

Each matrix Z contains p_1 roots of unity on the diagonal. The powers on $\omega_{p_2}^b$ are clearly one partition of $\mathbb{Z}/p_2^{\times}$. Thus, if $a \sim b$, the element in the upper left corner in Z_b will appear somewhere on the diagonal of Z_a. Since this element's exponent is in both partitions, they must be the same partition. Thus, the diagonal elements are the same; they are just in a different order. This results in the same characteristic polynomial, as polynomial multiplication over $\mathbb{Z}[\omega_{p_2}]$ is commutative. □

Now that all of the necessary machinery is in place, we can prove Theorem 4.4.

Proof. In this proof, the Z matrices are determined as they were in Lemma 4.2. By Theorem 4.1,

$$\chi(A(C(\mathbb{Z}/p_2 \rtimes_k \mathbb{Z}/p_1, \{x, y\}))) = \prod_{i=0}^{n-1} \chi(Z_i) = \chi(Z_0) \prod_{i=1}^{n-1} \chi(Z_i).$$

By Lemma 4.1, $\chi(Z_0) = ((\lambda - 1)^{p_1} + 1)$, as needed. By Lemmas 4.2 and 4.2,

$$\prod_{i=1}^{n-1} \chi(Z_i)$$

is a perfect p_1^{th} power, as there are equivalences of characteristic polynomials over partitions of size p_1. This concludes the proof. □

Note that, in general, the entries in the matrices Z_n are complex numbers, and, hence, their characteristic polynomials have complex coefficients. Theorem 4.4 implies that the product of all of these characteristic polynomials is a polynomial with integer coefficients.

5 Additional Results

Many of the calculations in this paper work in a cyclotomic field extension of the rational numbers. When performing calculations in this field, an identity arises that provides a connection between various mathematical entities. This result provides a connection between roots of unity, matrices with integer coefficients, and determinants of block matrices. In general, finding the determinant of a block matrix is difficult, but in this specific case we get a simpler answer.

Let $M = A_x + A_y$, the $m \times m$ block matrices described in Theorem 3.3.

Theorem 5.1.

$$\chi(M) = \prod_{i=0}^{n-1} \left(\prod_{j=0}^{m-1} \left(\lambda - \omega^{ik^j} \right) - 1 \right) = \det \left(\prod_{j=0}^{m-1} \left(\lambda I - (C_n)^{k^j} \right) - I \right)$$

The proof of Theorem 5.1 will require the following lemma.

Lemma 5.1.

$$\chi(M) = \det \left(\prod_{j=0}^{m-1} \left(\lambda I - (C_n)^{k^j} \right) - I \right)$$

Proof. The formula $\chi(M) = \det(\lambda I - M)$ is derived by solving the equation $Mv = \lambda v$ so that the values of λ that are roots of the characteristic polynomial are the eigenvalues of M. Since M is a block matrix, I will solve for the eigenvalues in a different way.

Like before, start with $Mv = \lambda v$. Now, since M is an $m \times m$ block matrix, express v as an $m \times 1$ block matrix. Let the i^{th} block in v be denoted v_i. For example, if $m = 3$, then $v = \left[\begin{array}{c} v_1 \\ \hline v_2 \\ \hline v_3 \end{array} \right]$. This yields the following system of m equations:

$$\left\{ \; (C_n)^{k^j} v_j + v_{(j \bmod m)+1} = \lambda v_j \right.$$

for $j \in (\mathbb{Z}/(m+1) - \{0\})$. These equations can be rewritten into the form

$$\left\{ \; \left(\lambda I - (C_n)^{k^j} \right) v_j = v_{(j \bmod m)+1} \right.$$

for $j \in (\mathbb{Z}/(m+1) - \{0\})$. Starting from any one of these equations, substitutions can be done in a cyclic manner until the same vector appears on both sides of a single equation. Keeping in mind that all matrices of the form $\lambda I - (C_n)^{k^j}$ commute with each other, the following equation is the result of such a substitution into the last equation:

$$\left(\prod_{j=0}^{m-1}\left(\lambda I - (C_n)^{k^j}\right)\right) v_1 = v_1.$$

Rearranging yields

$$\left(\prod_{j=0}^{m-1}\left(\lambda I - (C_n)^{k^j}\right) - I\right) v_1 = 0.$$

This yields the desired result that the eigenvalues of M are given by the roots of

$$\det\left(\prod_{j=0}^{m-1}\left(\lambda I - (C_n)^{k^j}\right) - I\right)$$

so this must be an expression for $\chi(M)$. □

Now, Theorem 5.1 can be proved.

Proof. The left side, by Lemma 4.1, equals $\chi(M)$. The right side, by Lemma 5.1, equals $\chi(M)$. □

5.1 Future Directions

It would be useful to find a statement analogous to Theorem 4.1 for semidirect products of abelian groups in general, as opposed to only for semidirect products of cyclic groups. Such a tool could be used to analyze groups such as $A_4 = (\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/3$. Perhaps an even more general result could be found that would yield information about spectra for any semidirect product, or, more optimistically, for any finite group.

References

[1] T. Coon, *Combinatorics of the Figure Equation on Directed Graphs*, Rose-Hulman Institute of Technology: Undergraduate Math Journal **7** (2006).

[2] D. Dummit and R. Foote, *Abstract Algebra: Second Edition*, Prentice Hall, Upper Saddle River, NJ, 1999.

[3] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer, New York, 2001.

[4] J. Lazenby, *Circulant Graphs and Their Spectra*, Senior Thesis, Portland, OR, May 2008.

[5] J. Serre, *Linear Representations of Finite Groups*, Springer, New York, 1977.