2006

Integral circulant graphs with the spectral Ádám property

Christopher F. Cusanza
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

Recommended Citation

Cusanza, Christopher F., "Integral circulant graphs with the spectral Ádám property" (2006). *Master's Theses*. 2875.

DOI: <https://doi.org/10.31979/etd.drak-xmy4>

https://scholarworks.sjsu.edu/etd_theses/2875

This Thesis is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Theses by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

INTEGRAL CIRCULANT GRAPHS WITH
THE SPECTRAL ÁDÁM PROPERTY

A Thesis

Presented to

The Faculty of the Department of Mathematics
San José State University

In Partial Fulfillment

of the Requirements for the Degree
Master of Science

by

Christopher F. Cusanza

May 2006

UMI Number: 1436901

INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleed-through, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

UMI Microform 1436901

Copyright 2006 by ProQuest Information and Learning Company.

All rights reserved. This microform edition is protected against unauthorized copying under Title 17, United States Code.

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

© 2006

Christopher F. Cusanza

ALL RIGHTS RESERVED

APPROVED FOR THE DEPARTMENT OF MATHEMATICS

Dr. Wasin So

Dr. Bradley W. Jackson

Dr. Edward F. Schmeichel

APPROVED FOR THE UNIVERSITY

ABSTRACT

INTEGRAL CIRCULANT GRAPHS WITH THE SPECTRAL ÁDÁM PROPERTY

by Christopher F. Cusanza

A graph is an integral circulant if it has a circulant adjacency matrix and all its eigenvalues are integers. The spectral Ádám property is a condition on the uniqueness of the adjacency spectrum of a circulant graph. We show that for p and q prime, certain integral circulant graphs of order pq^k have the spectral Ádám property. In preparation we present the basic properties of circulant graphs and derive an expression for their eigenvalues. We also derive a necessary and sufficient condition for a circulant graph to have integer eigenvalues. The sufficient condition is proved using elementary number theory. Necessity is proved using basic results from the theory of field extensions. The graph isomorphism problem is related to the question of unique spectra in that two graphs with different spectra can't be isomorphic.

CONTENTS

CHAPTER

1	INTRODUCTION	1
1.1	Circulant Graphs and the Spectral Ádám Property	1
1.2	Spectral Properties of Regular Graphs	6
1.3	Circulant Graphs as Cayley graphs	7
2	EIGENVALUES OF CIRCULANT MATRICES	11
2.1	Concepts from Matrix Theory	11
2.2	Eigenvalues of a Circulant Matrix	12
3	INTEGRAL CIRCULANT MATRICES	17
3.1	Preliminaries	17
3.1.1	Number Theory	17
3.1.2	Greatest Common Divisor Partitions	18
3.1.3	Ramanujan Sums	21
3.1.4	Cyclotomic Polynomials and Field Extensions	24
3.2	The Space of Integral Circulant Matrices	25
4	INTEGRAL CIRCULANT GRAPHS	29
4.1	Eigenvalues of a Circulant Graph	29

4.2	Integral Circulant Graphs	30
4.3	Prime Power Order	34
5	INTEGRAL CIRCULANTS WITH THE SPECTRAL ÁDÁM PROPERTY	37
5.1	Order pq^k , where $p < q$ and $k > 0$	37
5.2	Order qp^2 , where $p < q$	41
5.3	Order qp^k , where $p < q$ and $k > 2$	46
	BIBLIOGRAPHY	48

TABLES

Table

5.1	Eigenvalues of integral circulants of order 12. Each graph is identified by the gcd classes in its symbol.	42
5.2	Eigenvalues of integral circulants of order $q2^2$ where $q > 2$. Each graph is identified by the gcd classes in its symbol. The column labeled m_0 contains the multiplicity of the largest eigenvalue.	44
5.3	Integral circulants of order qp^2 where $p > 2$. Each graph is identified by the gcd classes in its symbol.	47

FIGURES

Figure

1.1	Isospectral graphs of order 5.	3
4.1	Integral circulants of order 8.	32
4.2	Non-integral circulants of order 8 and their symbols.	32

CHAPTER 1

INTRODUCTION

1.1 Circulant Graphs and the Spectral Ádám Property

In this thesis all graphs are simple, that is, finite graphs without directed edges, without loops, and having at most one edge between each pair of vertices. A *graph* Γ is a pair of sets (V, E) where each element of E is an unordered pair of distinct elements of V . The elements of V and E are the *vertices* and *edges*, respectively, of Γ . The *complement* of Γ , denoted $\bar{\Gamma}$, is the graph with vertex set V and edge set $\{\{x, y\} : \{x, y\} \notin E\}$. The number of elements in V is called the *order* of Γ . If Γ has order n , then a bijection $f : V \rightarrow \{0, \dots, n-1\}$ is called a *labeling* of Γ . Given a labeling f of Γ , the *adjacency matrix* of Γ is the 0, 1-matrix $A = [a_{ij}]$ where $a_{ij} = 1$ if and only if $\{f^{-1}(i), f^{-1}(j)\}$ is in E . Note that the indices i and j of the entries of A range from 0 to $n-1$, not 1 to n . This is the convention for matrix and vector indices throughout this thesis. If $\Gamma = (V, E)$ and $\Gamma' = (V', E')$ are graphs of the same order, then an *isomorphism* from graph Γ to Γ' is a bijection $g : V \rightarrow V'$ such that $\{x, y\} \in E$ if and only if $\{g(x), g(y)\} \in E'$.

An *eigenvalue* of a matrix A is a number λ for which there is a nonzero vector v such that $Av = \lambda v$. If A is an adjacency matrix of graph Γ then the *eigenvalues* of Γ are the eigenvalues of A . A graph is *integral* if all its eigenvalues are integers. Eigenvalues can also be defined as the roots of the characteristic polynomial $\chi(A; x) =$

$\det(xI - A)$ of A . The *multiplicity* of an eigenvalue λ is the degree of the factor $x - \lambda$ in $\chi(A; x)$. The *spectrum* of A is the multiset of eigenvalues, or the collection of eigenvalues counting multiplicity. It is denoted

$$\text{spec}(A) = \begin{pmatrix} \lambda_0 & \dots & \lambda_k \\ m_0 & \dots & m_k \end{pmatrix},$$

where $k < n$, and the λ_j are distinct. If A is an adjacency matrix of graph Γ we also say that this multiset is the *spectrum* of Γ . Two graphs with the same spectrum are called *isospectral*. Since a graph of order n has n eigenvalues, isospectral graphs must be of the same order. Since the adjacency matrices of isomorphic graphs differ only by a permutation similarity, isomorphic graphs are isospectral. Isospectral graphs are not necessarily isomorphic.

Example 1.1.1. Let $V = \{0, 1, 2, 3, 4\}$, $E = \{\{4, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}\}$, and $E' = \{\{0, 1\}, \{0, 2\}, \{0, 3\}, \{0, 4\}\}$. The adjacency matrix for graph $\Gamma = (V, E)$ is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

The adjacency matrix for graph $\Gamma' = (V, E')$ is

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Γ and Γ' have the same characteristic polynomial $x^3(x+2)(x-2)$, and thus the same spectrum:

$$\text{spec}(\Gamma) = \text{spec}(\Gamma') = \begin{pmatrix} -2 & 0 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

They are not isomorphic since Γ has an isolated vertex, but Γ' doesn't (see Figure 1.1).

Figure 1.1: Isospectral graphs of order 5.

Definition 1.1.2. A *circulant matrix* is a matrix $C = [c_{ij}]$ such that $c_{ij} = c_{0,j-i}$ for all $i, j = 0, \dots, n-1$, where the subscripts are taken modulo n . In other words, C is a matrix in which each row is equal to the previous row shifted to the right by one position. If u is a $1 \times n$ vector, $\text{circ}(u)$ denotes the $n \times n$ circulant matrix that has u as its first row.

Definition 1.1.3. A graph Γ is a *circulant graph* or *circulant* if there is a labeling of its vertices such that the adjacency matrix of Γ is a circulant matrix.

Definition 1.1.4. Let $u = [u_0, \dots, u_{n-1}]$ be a 0, 1-vector and $S = \{j \in \{1, \dots, n-1\} : u_j = 1\}$. The circulant graph with adjacency matrix $\text{circ}(u)$ is denoted $\Gamma_n(S)$ and S is called a *symbol* of $\Gamma_n(S)$.

It is possible that for $S \neq T$, $\Gamma_n(S)$ is isomorphic to $\Gamma_n(T)$. A simple example is $S = \{1, 4\}$ and $T = \{2, 3\}$. Both of these sets are symbols for the cycle of order

5. In fact for any $S \subset \{1, \dots, n-1\}$ the circulant graph with symbol $lS = \{ls \pmod n : s \in S\}$, where $\gcd(l, n) = 1$, is always isomorphic to $\Gamma_n(S)$. The question of whether this is a necessary condition on the symbol for isomorphism was raised by Ádám [Ád67].

Definition 1.1.5. Let S, T be subsets of $\{1, \dots, n-1\}$ and x an integer. Define xS to be $\{xs \pmod n : s \in S\}$. If $T = lS$ for some l such that $\gcd(l, n) = 1$, then we say S is *proportional* to T and write $S \sim T$.

A circulant that is isomorphic only to circulants with proportional symbols is said to have the *Ádám property*. Elspas and Turner [ET70] gave an order 16 example of a circulant graph that does not have the Ádám property, showing Ádám's conjecture to be false. It was later shown [Muz95] that any circulant of an order that is the product of distinct primes has the Ádám property.

The spectral Ádám property is a generalization of the Ádám property that relates the symbol of a circulant to its spectrum.

Definition 1.1.6. Let S and T be subsets of $\{1, \dots, n-1\}$. The graph $\Gamma_n(S)$ satisfies the *spectral Ádám property* (abbreviated SAP) if for any subset T of $\{1, \dots, n-1\}$, $\Gamma_n(T)$ has the same spectrum as $\Gamma_n(S)$ if and only if $T \sim S$.

If a graph satisfies the spectral Ádám property, then it must satisfy the Ádám property. The contrapositive is easily proved. Suppose $\Gamma_n(S)$ does not have the Ádám property. Then there is a graph $\Gamma_n(T)$ isomorphic to $\Gamma_n(S)$, but $T \not\sim S$. Since $\Gamma_n(T)$ is isomorphic to $\Gamma_n(S)$, their adjacency matrices differ only by a permutation similarity and they must have the same spectrum. Thus $\Gamma_n(S)$ does not satisfy SAP.

Mans, Pappalardi and Shparlinsky [MPS02] proved that certain circulants with symbols of the form $\{a, b, n-a, n-b\}$ for $0 < a < b < n/2$ satisfy SAP.

We attempt to show that integral circulant graphs of order pq^k satisfy SAP. We will see (Theorem 4.2.8) that if S and T are the symbols of integral circulant graphs and $S \sim T$, then $S = T$. Thus an integral circulant graph $\Gamma_n(S)$ has the spectral Ádám property if and only if $\text{spec}(\Gamma_n(S)) \neq \text{spec}(\Gamma_n(T))$ for all $T \neq S$.

In the remainder of this chapter we study circulant graphs as regular graphs and as Cayley graphs. The regularity of circulants provides information about largest eigenvalues and relates the eigenvalues of a circulant graph to the eigenvalues of its complement. In the section on Cayley graphs we see that the components of a circulant graph are also circulant graphs and relate the symbol of a circulant to the number of components it has.

Chapter 2 is a derivation of an expression for the eigenvalues of circulant matrices.

Chapter 3 contains a characterization of circulant matrices that have integer entries and integer eigenvalues. This characterization describes the first row of a circulant matrix in terms of number theoretic functions. The notion of Ramanujan sums is used to give a sufficient condition for the eigenvalues of a circulant to be integers. Cyclotomic polynomials are introduced to show that this condition is also necessary.

Chapter 4 uses the results of chapter 3 to characterize integral circulant graphs in terms of their symbols. Some properties of integral circulants are explored. The chapter ends with a proof that all integral circulants of prime power order satisfy SAP.

In Chapter 5, certain graphs of order pq^k are shown to satisfy SAP.

1.2 Spectral Properties of Regular Graphs

A graph is *regular* if all of its vertices have the same degree. A graph is called *k-regular* if all of its vertices have degree k . Circulant graphs are regular since each row of a circulant adjacency matrix contains the same number of 1s. The following are standard spectral results concerning regular graphs.

Theorem 1.2.1 ([Big93, p. 14]). *If Γ is a k -regular graph, then*

- (a) k is an eigenvalue of Γ ,
- (b) if Γ is connected, the multiplicity of k is 1, and
- (c) $k \geq |\lambda|$ for any eigenvalue λ of Γ .

Proof. (a) Let A be an adjacency matrix for Γ , and e a column vector of all ones. Since Γ is k -regular, we have $Ae = ke$ and thus k is an eigenvalue of Γ .

(b) and (c) See, e.g., [Big93, p. 14] or [Wes01, p. 460] □

Theorem 1.2.2. *The multiplicity of the largest eigenvalue of regular graph Γ is equal to the number of components of Γ .*

Proof. Let Γ be a k -regular graph. Then each component of Γ is a k -regular graph. By the previous theorem, k is the largest eigenvalue of Γ and each component of Γ has k as an eigenvalue with multiplicity 1. □

Theorem 1.2.3. *Let Γ be a regular graph of order n with eigenvalues $k \geq \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_{n-1}$. The eigenvalues of $\bar{\Gamma}$ are $n - k - 1, -1 - \lambda_1, -1 - \lambda_2, \dots, -1 - \lambda_{n-1}$.*

Proof. See, e.g., [Wes01, p. 461]. □

Theorem 1.2.3 implies that if Γ is regular with integer eigenvalues, then $\bar{\Gamma}$ is regular with integer eigenvalues.

Theorem 1.2.4. *Regular graphs Γ and Δ have the same spectrum if and only if $\bar{\Gamma}$ and $\bar{\Delta}$ have the same spectrum.*

Proof. The result follows from Theorem 1.2.3. □

1.3 Circulant Graphs as Cayley graphs

Definition 1.3.1. A *Cayley graph* $\text{Cay}(G, S)$ is a graph defined on a group G and a subset S of the elements of G that is closed under inversion and doesn't contain the identity element. The vertices of $\text{Cay}(G, S)$ are the elements of G . The edges of $\text{Cay}(G, S)$ describe the result of the group operation between elements of G and S , i.e., the edge set is $\{\{x, xy\} : x \in G \text{ and } y \in S\}$.

Definition 1.3.2. The *cyclic group* $\mathbb{Z}_n$ is the group with elements $\{0, 1, \dots, n-1\}$ and the operation of addition modulo n .

Theorem 1.3.3. *The Cayley graph $\text{Cay}(\mathbb{Z}_n, S)$ is isomorphic to $\Gamma_n(S)$.*

Proof. Let A be the circulant adjacency matrix of $\Gamma_n(S)$ for the symbol S . We can take the vertices of $\Gamma_n(S)$ to be the elements of $\mathbb{Z}_n$ so that row i of A corresponds to vertex i . Now, let $\{x, x+y\}$ be an edge of $\text{Cay}(\mathbb{Z}_n, S)$, where $y \in S$. By the definition of symbol, $\{0, y\}$ is an edge of $\Gamma_n(S)$ if and only if $y \in S$. From the definition of circulant matrix, $\{x, x+y\}$ is an edge of $\Gamma_n(S)$ if and only if $\{0, y\}$ is an edge of $\Gamma_n(S)$. Thus, the identity function on $\mathbb{Z}_n$ is an isomorphism from $\text{Cay}(\mathbb{Z}_n, S)$ to $\Gamma_n(S)$. □

Definition 1.3.4. A graph is *vertex transitive* if for any two vertices x and y , there is an automorphism that takes x to y . This implies that all the vertices of a vertex transitive graph have the same degree and thus all vertex transitive graphs are regular.

Theorem 1.3.5. *All Cayley graphs are vertex transitive.*

Proof. See [Big93, p. 123]. □

In the case of the circulant $\text{Cay}(\mathbb{Z}_n, S)$, the function $f(j) = j + y - x \pmod{n}$ is an automorphism that takes vertex x to vertex y .

Theorem 1.3.6. *The Cayley graph $\text{Cay}(G, S)$ is connected if and only if S generates G .*

Proof. Assume $\text{Cay}(G, S)$ is connected. Let s be an element of S and x an element of G . Since $\text{Cay}(G, S)$ is connected, it contains an xs -path $s, v_1, v_2, \dots, v_k, x$. From the definition of $\text{Cay}(G, S)$, there exist $s_0, \dots, s_k$ in S such that $v_1 = ss_0$, $v_2 = v_1s_1$, $\dots$, $v_k = v_{k-1}s_{k-1}$, and $x = v_k s_k$. Thus $x = ss_0s_1 \dots s_k$ is in $\langle S \rangle$.

Now assume S generates G . Let x and y be in G . Since $G = \langle S \rangle$, there exist $s_0, \dots, s_k$ such that $x^{-1}y = s_0s_1 \dots s_k$. Thus $y = xs_0s_1 \dots s_k$. Using the definition of a Cayley graph, this implies there is an xy -walk $x, xs_0, xs_0s_1, \dots, y$ in $\text{Cay}(G, S)$. □

Theorem 1.3.7. *The components of $\text{Cay}(G, S)$ are isomorphic copies of $\text{Cay}(\langle S \rangle, S)$, where $\langle S \rangle$ is the group generated by the elements in S .*

Proof. From the definition of a Cayley graph, $\text{Cay}(\langle S \rangle, S)$ is a subgraph of $\text{Cay}(G, S)$. The last theorem implies that $\text{Cay}(\langle S \rangle, S)$ is a component of $\text{Cay}(G, S)$. All of the components of $\text{Cay}(G, S)$ are isomorphic since $\text{Cay}(G, S)$ is vertex transitive. □

The next lemma is a basic result from number theory.

Lemma 1.3.8. *Let $S = \{s_1, \dots, s_r\}$ be a set of integers and d their greatest common divisor. Then the set $\{a_1s_1 + \dots + a_rs_r : a_1, \dots, a_r \in \mathbb{Z}\}$ is equal to $\{ad : a \in \mathbb{Z}\}$.*

Proof. See, e.g., [IR90, p. 4]. □

Lemma 1.3.9. *Let S be a subset of $\mathbb{Z}_n$ and d the greatest common divisor of the elements of $S \cup \{n\}$. Then $\langle S \rangle = \langle d \rangle$ and $|\langle S \rangle| = \frac{n}{d}$.*

Proof. A number x is in $\langle S \rangle$ if and only if $x = a_1 s_1 + \cdots + a_r s_r \pmod{n}$ for some $s_1, \dots, s_r \in S$ and integers $a_1, \dots, a_r$. By the previous lemma, $a_1 s_1 + \cdots + a_r s_r = ad$ for some integer a . Then we have $x = ad \pmod{n} \in \langle d \rangle$. Since d divides n , the elements of $\langle d \rangle$ are $0, d, 2d, \dots, (\frac{n}{d} - 1)d$ and thus $|\langle S \rangle| = |\langle d \rangle| = \frac{n}{d}$. $\square$

Theorem 1.3.10. *Let S be a subset of $\mathbb{Z}_n$ and d the greatest common divisor of the elements of $S \cup \{n\}$. Then the number of components of $\Gamma_n(S)$ is d , and each component is isomorphic to $\Gamma_{\frac{n}{d}}(\frac{1}{d}S)$.*

Proof. By Theorem 1.3.3, $\Gamma_n(S) = \text{Cay}(\mathbb{Z}_n, S)$. Each component of $\text{Cay}(\mathbb{Z}_n, S)$ is a copy of $\text{Cay}(\langle S \rangle, S)$ (Theorem 1.3.7), and $\langle S \rangle = \langle d \rangle$ (Lemma 1.3.9). Thus there are $\frac{n}{|\langle d \rangle|} = d$ components.

It suffices to show that $\Gamma_{\frac{n}{d}}(\frac{1}{d}S)$ is isomorphic to the component of $\Gamma_n(S)$ which contains vertex 0. Let g be the bijection from S to $\frac{1}{d}S$ given by $g(x) = \frac{x}{d}$. Now, $\{0, a\}$ is an edge of $\Gamma_n(S)$ if and only if $a \in S$, if and only if $g(a) \in \frac{1}{d}S$, if and only if $\{0, g(a)\}$ is an edge of $\Gamma_{\frac{n}{d}}(\frac{1}{d}S)$. Then since Cayley graphs are vertex transitive, g is an isomorphism. $\square$

Corollary 1.3.11. *The multiplicity of the largest eigenvalue of $\Gamma_n(S)$ is d .*

Proof. From Theorem 1.2.2, the multiplicity of the largest eigenvalue of $\Gamma_n(S)$ is equal to the number of components of $\Gamma_n(S)$. $\square$

Theorem 1.3.12. *Every component of a circulant graph is a circulant graph.*

Proof. It is a theorem of abstract algebra that every subgroup of a cyclic group is cyclic. $\square$

Theorem 1.3.13. *Let n be a positive integer. If all connected integral circulants of every order that divides n satisfy SAP, then all integral circulants of order n satisfy SAP.*

Proof. Let $\Gamma_n(S)$ be an integral circulant graph with $j > 1$ components. We need to show that for any $T \approx S$, $\Gamma_n(S)$ is not isospectral to $\Gamma_n(T)$. Suppose $\Gamma_n(T)$ is isospectral to $\Gamma_n(S)$. By Theorem 1.2.2, $\Gamma_n(S)$ and $\Gamma_n(T)$ both have j components. From Theorems 1.3.10 and 1.3.12, $\Gamma_n(S)$ and $\Gamma_n(T)$ consist of j copies of connected integral circulants $\Gamma_{\frac{n}{j}}(\frac{1}{j}S)$ and $\Gamma_{\frac{n}{j}}(\frac{1}{j}T)$, respectively. By hypothesis, $\Gamma_{\frac{n}{j}}(\frac{1}{j}S)$ and $\Gamma_{\frac{n}{j}}(\frac{1}{j}T)$ satisfy SAP. This is a contradiction since the spectrum of a graph is the union of the spectra of its components. $\square$

CHAPTER 2

EIGENVALUES OF CIRCULANT MATRICES

The main goal of this chapter is to derive an expression for the eigenvalues of a circulant matrix. We begin with a review of some definitions and theorems from matrix theory.

2.1 Concepts from Matrix Theory

The material in this section can be found in [HJ85].

Definition 2.1.1. The *transpose* of a matrix $A = [a_{ij}]$, denoted A^T , is the matrix with entries a_{ji} . In other words, the rows of A^T are the columns of A and vice versa. The *conjugate* of A , denoted $\overline{A}$, is the matrix with entries that are the complex conjugates of the corresponding entries of A . The *Hermitian adjoint* of A is the matrix $A^* = \overline{A}^T$.

Definition 2.1.2. The matrix A is *symmetric* if $A = A^T$. If A is square and $A^*A = I$, then we say A is *unitary*.

Definition 2.1.3. A square matrix $A = [a_{ij}]$ is *diagonal* if $i \neq j$ implies $a_{ij} = 0$. The $n \times n$ diagonal matrix with diagonal entries $u_0, \dots, u_{n-1}$ is denoted $\text{Diag}(u_0, \dots, u_{n-1})$.

Definition 2.1.4. A matrix A is *unitarily diagonalizable* if there is a unitary matrix U and a diagonal matrix D such that $A = UDU^*$.

Theorem 2.1.5. *Let $A = UDU^*$, where U is unitary and $D = \text{Diag}(\lambda_0, \dots, \lambda_{n-1})$. Then the eigenvalues of A are $\lambda_0, \dots, \lambda_{n-1}$ and column j of U is an eigenvector of A corresponding to eigenvalue λ_j .*

Proof. See, e.g., [HJ85, pp. 46, 101]. □

2.2 Eigenvalues of a Circulant Matrix

The following derivation parallels that of [Dav94, pp. 31-33, 66-68, 72-73]. The approach is to show that any circulant matrix is diagonalized by a certain unitary matrix called the Fourier transform matrix. The entries of the Fourier transform matrix are roots of unity and the eigenvalues of a circulant matrix are shown to be a sum of roots of unity.

Definition 2.2.1. An n -th root of unity is a solution of the equation $x^n = 1$ in the complex numbers. If we let $\omega = e^{\frac{2\pi i}{n}}$, then the n -th roots of unity are the n complex numbers $\omega^0, \omega^1, \dots, \omega^{n-1}$.

Theorem 2.2.2. *If j is a positive integer and n an integer greater than 1, then $1 + \omega^j + (\omega^j)^2 + \dots + (\omega^j)^{n-1} = 0$.*

Proof. Simple calculations show that $x^n - 1 = (x - 1)(1 + x + x^2 + \dots + x^{n-1})$. The number ω^j is a root of $x^n - 1$, since $(\omega^j)^n = 1$ implies $(\omega^j)^n - 1 = 0$. Since $j > 0$, we have $\omega^j \neq 1$. Thus ω^j must be a root of $1 + x + x^2 + \dots + x^{n-1}$. □

Definition 2.2.3. A *primitive n -th root of unity* is an n -th root of unity ω^j such that $\gcd(j, n) = 1$.

Definition 2.2.4. The Fourier Transform Matrix F_n is the $n \times n$ matrix with entries $f_{st} = \frac{1}{\sqrt{n}} \omega^{st}$ for $0 \leq s, t \leq n - 1$.

Example 2.2.5.

$$F_6 = \frac{1}{\sqrt{6}} \begin{pmatrix} \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 \\ \omega^0 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} \\ \omega^0 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} \\ \omega^0 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} \\ \omega^0 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} \end{pmatrix} = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & 1 & \omega^3 & 1 & \omega^3 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

It is immediate from the definition of F_n that it is symmetric. Therefore, $F_n^* = \overline{F_n}^T = \overline{F_n}$.

Theorem 2.2.6. F_n is unitary.

Proof. $F_n F_n^* = [\frac{1}{n} \sum_{r=1}^n f_{sr} \overline{f_{rt}}] = [\frac{1}{n} \sum_{r=0}^{n-1} \omega^{sr} \omega^{-rt}] = [\frac{1}{n} \sum_{r=0}^{n-1} \omega^{r(s-t)}] = I$. The last equality is due to Theorem 2.2.2. $\square$

Definition 2.2.7. The *basic permutation circulant* W_n is the $n \times n$ circulant matrix with first row $[0, 1, 0, \dots, 0]$.

Multiplying a matrix A on the right by W_n has the effect of shifting all the columns of A to the right by one. Therefore W_n^2 is a circulant with first row $[0, 0, 1, 0, \dots, 0]$. This idea is generalized in the next theorem.

Theorem 2.2.8. Let x be the $1 \times n$ vector with a 1 in its $(j+1)$ -st column and zero everywhere else. Then $W_n^j = \text{circ}(x)$.

Theorem 2.2.9. Let $u = [u_0, \dots, u_{n-1}]$. Then $\text{circ}(u) = u_0 I + u_1 W_n + \dots + u_{n-1} W_n^{n-1}$.

Proof. This follows from the previous theorem and matrix arithmetic. $\square$

If we define for the vector u a polynomial $f_u(x) = \sum_{j=0}^{n-1} u_j x^j$ then the result of the last theorem is expressed compactly as $\text{circ}(u) = f_u(W_n)$.

Theorem 2.2.10. *Let $\Omega = \text{Diag}(1, \omega, \omega^2, \dots, \omega^{n-1})$. The product $F_n \Omega F_n^*$ is equal to the basic permutation circulant W_n .*

Proof. Since F_n is unitary, it is sufficient to show that $W_n F_n = F_n \Omega$. Multiplying by the permutation W_n on the left simply shifts the rows of F_n up by one, taking the first row to the last. Thus the s, t entry of $W_n F_n$ is

$$\frac{1}{\sqrt{n}} \omega^{(s+1)t}.$$

Multiplying F_n on the right by diagonal matrix Ω has the effect of multiplying each column t of F_n by ω^t , the t, t entry of Ω . Then the s, t entry of $F_n \Omega$ is

$$\frac{1}{\sqrt{n}} \omega^{st} \omega^t = \frac{1}{\sqrt{n}} \omega^{(s+1)t}.$$

□

Theorem 2.2.11. *Let $u = [u_0, \dots, u_{n-1}]$ and $\Lambda = \text{Diag}(f_u(1), f_u(\omega), \dots, f_u(\omega^{n-1}))$. Then $\text{circ}(u) = F_n \Lambda F_n^*$.*

Proof.

$$\begin{aligned} \text{circ}(u) &= f_u(W_n) \\ &= \sum_{j=0}^{n-1} u_j W_n^j \\ &= \sum_{j=0}^{n-1} u_j (F_n \Omega F_n^*)^j \\ &= F_n \left(\sum_{j=0}^{n-1} u_j \Omega^j \right) F_n^* \\ &= F_n \left(\sum_{j=0}^{n-1} u_j \text{Diag}(1^j, \omega^j, \dots, \omega^{(n-1)j}) \right) F_n^* \end{aligned}$$

$$\begin{aligned}
&= F_n \left(\text{Diag} \left(\sum_{j=0}^{n-1} u_j, \sum_{j=0}^{n-1} u_j \omega^j, \dots, \sum_{j=0}^{n-1} u_j \omega^{(n-1)j} \right) \right) F_n^* \\
&= F_n \Lambda F_n^*.
\end{aligned}$$

□

Thus the circulant matrix $\text{circ}(u)$ is diagonalized by the unitary matrix F_n . From Theorem 2.1.5, the columns of F_n are a set of eigenvectors with the diagonal entries of Λ as the corresponding eigenvalues.

Theorem 2.2.11 establishes an ordering of the eigenvalues of a circulant matrix and motivates the following definitions.

Definition 2.2.12. For $0 \leq t \leq n-1$, the t -th eigenvalue of a circulant matrix $\text{circ}(u)$ is the sum $\sum_{j=0}^{n-1} u_j \omega^{jt}$ and is denoted $\lambda_t(\text{circ}(u))$.

Definition 2.2.13. The spectral sequence of a circulant matrix $\text{circ}(u)$ is the vector $[\lambda_0(\text{circ}(u)), \lambda_1(\text{circ}(u)), \dots, \lambda_{n-1}(\text{circ}(u))]$.

Theorem 2.2.14. Let $u = [u_0, \dots, u_{n-1}]$. The spectral sequence of $\text{circ}(u)$ is equal to $\sqrt{n} F_n u^T$.

Proof.

$$\begin{aligned}
\sqrt{n} F_n u^T &= \sqrt{n} \left[\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} u_j \omega^0, \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} u_j \omega^j, \dots, \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} u_j \omega^{(n-1)j} \right]^T \\
&= [\lambda_0(\text{circ}(u)), \lambda_1(\text{circ}(u)), \dots, \lambda_{n-1}(\text{circ}(u))]^T.
\end{aligned}$$

□

It is important to note that two circulant matrices could potentially have the same spectrum, but different spectral sequences.

Example 2.2.15. Let $u = [0, 1, 0, 1, 0, 1, 0, 1]$. The spectral sequence of $\text{circ}(u)$ is

$$\sqrt{8}F_8u^T = [4, 0, 0, 0, -4, 0, 0, 0].$$

The spectral sequence of $\text{circ}(-u)$ is $\sqrt{8}F_8(-u)^T = -\sqrt{8}F_8u^T = [-4, 0, 0, 0, 4, 0, 0, 0]$.

Both $\text{circ}(u)$ and $\text{circ}(-u)$ have the spectrum

$$\begin{pmatrix} -4 & 0 & 4 \\ 1 & 6 & 1 \end{pmatrix}.$$

CHAPTER 3

INTEGRAL CIRCULANT MATRICES

In this chapter we develop a characterization, following [So06], of circulant matrices that have integer entries and integer eigenvalues. A similar characterization of symmetric circulant matrices with rational entries and rational eigenvalues is given in [BM79, pp. 145-147].

3.1 Preliminaries

3.1.1 Number Theory

If n is a positive integer, a *totative* of n is a positive integer j less than n such that $\gcd(j, n) = 1$. For example, the set of totatives of 12 is $\{1, 5, 7, 11\}$. The *totient function* $\phi(n)$, sometimes called the Euler totient function, is defined as the number of totatives of n . If $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ is the factorization of n into prime powers, then the totient function can be expressed as $\phi(n) = n \prod_{j=1}^r \left(1 - \frac{1}{p_j}\right)$. If p and q are primes, and k a positive integer, then $\phi(p) = p - 1$, $\phi(p^k) = (p - 1)p^{k-1}$, and $\phi(qp^k) = (q - 1)(p - 1)p^{k-1}$. The totient function is *multiplicative*, that is, if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. A multiplicative function is determined by its effect on powers of primes: if $f(x)$ is multiplicative, then $f(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}) = f(p_1^{a_1}) f(p_2^{a_2}) \dots f(p_k^{a_k})$.

The *Mobius function* is defined as

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square free} \\ 1 & \text{if } n = 1 \text{ or } n \text{ is a product of an even number of distinct primes} \\ -1 & \text{if } n \text{ is a product of an odd number of distinct primes.} \end{cases}$$

For example, $\mu(3) = -1$, $\mu(6) = 1$, and $\mu(12) = 0$. The number of positive divisors of n is denoted $\tau(n)$. The set of *proper divisors* of n is the subset of divisors of n which excludes n .

Theorem 3.1.1. *Let j , k , and d be positive integers. Then $\gcd(j, k) = 1$ if and only if $\gcd(jd, kd) = d$.*

Proof. Suppose $\gcd(j, k) = 1$. Let $e = \gcd(jd, kd)$. Since d divides jd and kd , by the definition of $\gcd$, d divides e . This allows us to write $e = e'd$ for some positive integer e' . $e = e'd$ implies that e' divides j and k . Thus $e' = 1$ and $e = d$. Conversely, assume $\gcd(jd, kd) = d$. Then $\gcd(j, k) = 1$, otherwise $\gcd(jd, kd) > d$. $\square$

3.1.2 Greatest Common Divisor Partitions

For any positive integer n there is a partition of the set $\{0, \dots, n-1\}$ such that each equivalence class corresponds to a divisor of n . We refer to the classes of this partition as *greatest common divisor classes* of n or the *gcd classes* of n .

Definition 3.1.2. For positive integers n and d , define the set $G_n(d)$ by

$$G_n(d) = \{j : 0 \leq j < n, \gcd(n, j) = d\}.$$

The set $G_n(1)$ is just the set of totatives of n , so $|G_n(1)| = |\phi(n)|$. If d isn't a divisor of n , then $G_n(d) = \emptyset$. Since any nonnegative integer less than n has exactly one greatest common divisor with n , the set $\{G_n(d) : d \mid n\}$ is a partition of $\{0, \dots, n-1\}$.

Example 3.1.3. The divisors of 12 are 1, 2, 3, 4, 6, and 12.

$$G_{12}(1) = \{1, 5, 7, 11\}$$

$$G_{12}(2) = \{2, 10\}$$

$$G_{12}(3) = \{3, 9\}$$

$$G_{12}(4) = \{4, 8\}$$

$$G_{12}(6) = \{6\}$$

$$G_{12}(12) = \{0\}$$

Notice that $G_{12}(2) = 2\{1, 5\} = 2G_6(1)$, $G_{12}(3) = 3\{1, 3\} = 3G_4(1)$, etc.

Theorem 3.1.4. *If n , d , and d' are positive integers such that $n = dd'$ then $G_n(d) = dG_{d'}(1)$.*

Proof. The result follows from Theorem 3.1.1. □

From Theorem 3.1.4 we see that $|G_n(d)| = |G_{\frac{n}{d}}(1)| = \phi(\frac{n}{d})$ for any divisor d of n .

Theorem 3.1.5. *Let m and n be positive integers and $T = \{jm + kn \pmod{mn} : j \in G_n(1) \text{ and } k \in G_m(1)\}$. If $\gcd(m, n) = 1$, then $G_{mn}(1) = T$.*

Proof. Let $x = jm + kn$ be an element of T where $j \in G_n(1)$ and $k \in G_m(1)$. Suppose $x \notin G_{mn}(1)$. Then $\gcd(x, mn) = d$ for some d greater than 1. Let p be a prime such that $p \mid d$. Since p divides mn , it must divide either m or n . Without loss of generality, say $p \mid m$. This allows us to write $m = pm'$ where m' is a positive integer. Also, since p divides x , there is a positive integer q such that $jpm' + kn = qp$. This implies that $p \mid k$ or $p \mid n$. But neither can be the case since $\gcd(k, m) = 1$ and $\gcd(m, n) = 1$. This shows that $T \subset G_{mn}(1)$. Now to finish the proof we only need

that T and $G_{mn}(1)$ have the same number of elements. This is done by showing that each combination of $j \in G_n(1)$ and $k \in G_m(1)$ produces a distinct number $jm + kn \pmod{mn}$. Suppose $jm + kn \equiv j'm + k'n \pmod{mn}$. Then there is an l such that $(j - j')m = (k - k')n + lmn$. Therefore $j - j' \equiv 0 \pmod{mn}$, and $j \equiv j' \pmod{mn}$. Since j and j' are elements of $G_n(1)$ they are positive and less than n , and consequently must be equal. Similarly, $k = k'$. Then $|T| = |G_n(1)||G_m(1)| = \phi(n)\phi(m) = \phi(mn)$, using that the function ϕ is multiplicative. $\square$

Theorem 3.1.6. *Let l be an integer such that $\gcd(n, l) = 1$. Then $lG_n(d) = G_n(d)$ for any divisor d of n .*

Proof. Assume $d = 1$. First we will show that $lG_n(1) \subset G_n(1)$ and then that $|lG_n(1)| = |G_n(1)|$. By definition, if $x \in lG_n(1)$ then $x \equiv lj \pmod{n}$ for some $0 < j < n$, with $\gcd(n, j) = 1$. Since $\gcd(n, j) = 1$ and $\gcd(n, l) = 1$ we have $\gcd(lj, n) = 1$. This implies $\gcd(lj \pmod{n}, n) = 1$, since $lj - kn \equiv lj \pmod{n}$ for any integer k . Thus x is in $G_n(d)$. To see $|lG_n(1)| = |G_n(1)|$, suppose $lj \equiv lj' \pmod{n}$ where $0 < j, j' < n$ and $\gcd(n, j) = \gcd(n, j') = 1$. This implies $lj = lj' + kn$ for some integer k . Subtracting lj' from both sides and factoring out l produces $l(j - j') = kn$. Since $\gcd(n, l) = 1$, it must be that l divides k . We can then write $l(j - j') = lk'n$. Canceling the l leaves $j - j' = k'n$. Since $|j - j'| < n$, it follows that $j - j' = 0$ and thus $j = j'$.

Now assume $d > 1$. By Theorem 3.1.4, $G_n(d) = dG_{\frac{n}{d}}(1)$. From first part of this proof and the fact that $\gcd(\frac{n}{d}, l) = 1$, we get $dG_{\frac{n}{d}}(1) = dlG_{\frac{n}{d}}(1) = ldG_{\frac{n}{d}}(1)$. Using $G_n(d) = dG_{\frac{n}{d}}(1)$ again produces the result. $\square$

3.1.3 Ramanujan Sums

Ramanujan sums are sums of roots of unity that resemble the formula given in the last chapter for the eigenvalues of a circulant matrix. Later we will express the eigenvalues of an integral circulant matrix in terms of Ramanujan sums.

Definition 3.1.7. A sum $c_t(n) = \sum_{j \in G_n(1)} \omega_n^{jt}$, where $\omega_n = e^{2\pi i/n}$ and t is an integer, is called a *Ramanujan sum* or a *Ramanujan trigonometric sum* ([Ram18]).

Lemma 3.1.8. If $d \mid n$, then $c_t\left(\frac{n}{d}\right) = \sum_{j \in G_n(d)} \omega_n^{jt}$

Proof.

$$\begin{aligned}
 c_t\left(\frac{n}{d}\right) &= \sum_{j \in G_{\frac{n}{d}}(1)} \omega_{\frac{n}{d}}^{jt} \\
 &= \sum_{j \in G_{\frac{n}{d}}(1)} \omega_n^{jtd} \\
 &= \sum_{j \in dG_{\frac{n}{d}}(1)} \omega_n^{jt} \\
 &= \sum_{j \in G_n(d)} \omega_n^{jt} \quad (\text{Theorem 3.1.4})
 \end{aligned}$$

□

Lemma 3.1.9. Let m and n be integers such that $\gcd(m, n) = 1$. Then $c_t(mn) = c_t(m)c_t(n)$.

Proof. Using Theorem 3.1.5,

$$\begin{aligned}
 c_t(mn) &= \sum_{j \in G_{mn}(1)} e^{2\pi i \frac{jt}{mn}} \\
 &= \sum_{j \in G_m(1)} \sum_{k \in G_n(1)} e^{2\pi i \frac{(nj+mk+lmn)t}{mn}}
 \end{aligned}$$

for some integer l . Manipulating this expression with complex arithmetic gives

$$\begin{aligned}
\sum_{j \in G_m(1)} \sum_{k \in G_n(1)} e^{2\pi i \frac{(nj+mk+lmn)t}{mn}} &= \sum_{j \in G_m(1)} \sum_{k \in G_n(1)} e^{2\pi i \frac{jt}{m}} e^{2\pi i \frac{kt}{n}} \\
&= \left(\sum_{j \in G_m(1)} e^{2\pi i \frac{jt}{m}} \right) \left(\sum_{k \in G_n(1)} e^{2\pi i \frac{kt}{n}} \right) \\
&= c_t(m) c_t(n)
\end{aligned}$$

□

Lemma 3.1.10. *For any integer t , $c_t(n) = \frac{\phi(n)}{\phi(\frac{n}{\gcd(n,t)})} \mu\left(\frac{n}{\gcd(n,t)}\right)$. Furthermore, $c_t(n)$ is an integer.*

Proof. From Lemma 3.1.9, $c_t(n)$ is multiplicative. The function $\frac{\phi(n)}{\phi(\frac{n}{\gcd(n,t)})} \mu\left(\frac{n}{\gcd(n,t)}\right)$ is multiplicative since it is the composition of multiplicative functions. Any multiplicative function is determined by its action on powers of primes, so we just need to show that $c_t(p^k) = \frac{\phi(p^k)}{\phi(\frac{p^k}{\gcd(p^k,t)})} \mu\left(\frac{p^k}{\gcd(p^k,t)}\right)$. To begin, notice that $\gcd(p^k, t) = p^r$ for some r in $\{0, \dots, k\}$. Then we have

$$\begin{aligned}
\frac{\phi(p^k)}{\phi(\frac{p^k}{\gcd(p^k,t)})} \mu\left(\frac{p^k}{\gcd(p^k,t)}\right) &= \frac{\phi(p^k)}{\phi(\frac{p^k}{p^r})} \mu\left(\frac{p^k}{p^r}\right) \\
&= \frac{\phi(p^k)}{\phi(p^{k-r})} \mu(p^{k-r}) \\
&= \begin{cases} 0 & \text{if } r < k-1 \\ -p^k & \text{if } r = k-1 \\ (p-1)p^{k-1} & \text{if } r = k, \end{cases}
\end{aligned}$$

To show that $c_t(p^k)$ is equal to this last expression we use the fact that the set $G_{p^k}(1)$ is equal to the set difference $\{1, 2, \dots, p^k - 1\} - \{p, 2p, \dots, (p^{k-1} - 1)p\}$.

Case $r < k - 1$: Define t' by $t = t'p^r$. Since $\gcd(t, p^k) = p^r$, we have $\gcd(t', p^{k-r}) = 1$.

$$\begin{aligned}
c_t(p^k) &= \sum_{j \in G_{p^k}(1)} e^{2\pi i \frac{jt}{p^k}} \\
&= \sum_{j \in G_{p^k}(1)} e^{2\pi i \frac{jt'}{p^{k-r}}} \\
&= \sum_{j=1}^{p^k-1} e^{2\pi i \frac{jt'}{p^{k-r}}} - \sum_{j \in \{p, \dots, (p^{k-1}-1)p\}} e^{2\pi i \frac{jt'}{p^{k-r}}} \\
&= -1 - (-1)
\end{aligned}$$

Case $r = k - 1$: Define t' by $t = t'p^{k-1}$. Since $\gcd(t, p^k) = p^{k-1}$, we have $\gcd(t', p) = 1$.

$$\begin{aligned}
c_t(p^k) &= \sum_{j \in G_{p^k}(1)} e^{2\pi i \frac{jt}{p^k}} \\
&= \sum_{j \in G_{p^k}(1)} e^{2\pi i \frac{jt'}{p}} \\
&= \sum_{j=1}^{p^k-1} e^{2\pi i \frac{jt'}{p}} - \sum_{j \in \{p, \dots, (p^{k-1}-1)p\}} e^{2\pi i \frac{jt'}{p}} \\
&= -1 - (p^{k-1} - 1) \\
&= -p^{k-1}
\end{aligned}$$

Case $r = k$: Define t' by $t = t'p^k$.

$$\begin{aligned}
c_t(p^k) &= \sum_{j \in G_{p^k}(1)} e^{2\pi i \frac{jt}{p^k}} \\
&= \sum_{j \in G_{p^k}(1)} e^{2\pi i jt'} \\
&= \sum_{j \in G_{p^k}(1)} 1 \\
&= \phi(p^k) \\
&= (p-1)p^{k-1}
\end{aligned}$$

In each of the three cases, $c_t(p^k)$ is an integer. Therefore $c_t(n)$ is always an integer. $\square$

3.1.4 Cyclotomic Polynomials and Field Extensions

The following are standard definitions and results from the theory of field extensions. See, for example, [Gri99] or [Hun74].

Definition 3.1.11. The field of polynomials in variable x with rational coefficients is denoted $\mathbb{Q}[x]$. Elements of $\mathbb{Q}[x]$ are called *rational polynomials*.

Definition 3.1.12. A rational polynomial is *monic* if the coefficient of its highest order term is 1.

Definition 3.1.13. A rational polynomial $p(x)$ of degree n is *irreducible over $\mathbb{Q}$* if for any rational polynomials $q(x)$ and $r(x)$ such that $p(x) = q(x)r(x)$, the degree of $q(x)$ and $r(x)$ are 1 and n , or vice versa.

Definition 3.1.14. The polynomial $\Phi_n(x) = \prod_{j \in G_n(1)} (x - \omega^j)$ is called the n -th cyclotomic polynomial.

It is evident from Definition 3.1.14 that the roots of $\Phi_n(x)$ are the primitive n -th roots of unity.

Theorem 3.1.15. $\Phi_n(x)$ is monic, irreducible and has rational coefficients.

Proof. See, e.g., [Gri99, pp. 240-241]. □

Definition 3.1.16. A field E is an *extension* of field F if F is a subfield of E .

Definition 3.1.17. Let E be an extension of $\mathbb{Q}$ and c an element of E such that c is the root of a nonzero polynomial in $\mathbb{Q}[x]$. Let J_c denote the set of all $a(x)$ in $\mathbb{Q}[x]$ such that $a(c) = 0$. The *minimum polynomial* of c over $\mathbb{Q}$ is the unique monic polynomial that divides every element of J_c .

Theorem 3.1.18. If ρ is a primitive n -th root of unity, then the minimum polynomial of ρ over $\mathbb{Q}$ is $\Phi_n(x)$.

Proof. Let $e(x)$ be the minimum polynomial of J_ρ . Since $\Phi_n(\rho) = 0$, we have $\Phi_n(x) \in J_\rho$ and $e(x)$ divides $\Phi_n(x)$. Then since $\Phi_n(x)$ is irreducible and monic, $e(x) = \Phi_n(x)$. □

Example 3.1.19. The field of complex numbers $\mathbb{C}$ is an extension of $\mathbb{Q}$. The complex numbers i and $-i$ are the primitive fourth roots of unity. The minimum polynomial of i over $\mathbb{Q}$ is $\Phi_4(x) = (x+i)(x-i) = x^2+1$. Let $p(x) = x^4-1$ and $q(x) = x^3+2x^2+x+2$ be polynomials in $\mathbb{Q}[x]$. i is a root of $p(x)$ and $q(x)$ since $p(i) = 1 - 1 = 0$ and $q(i) = -i + 2(-1) + i + 2 = 0$. The polynomials $p(x)$ and $q(x)$ can be factored in $\mathbb{Q}[x]$ as $\Phi_4(x)(x+1)(x-1)$ and $\Phi_4(x)(x+2)$ respectively.

3.2 The Space of Integral Circulant Matrices

Definition 3.2.1. The *indicator vector* of a set $S \subset \{1, \dots, n-1\}$ is the $1 \times n$ vector $ind(S)$, where $ind(S)_j = 1$ if $j \in S$ and $ind(S)_j = 0$ otherwise.

Definition 3.2.2. The set of circulant matrices with a first row that is an integer combination of the indicator vectors of gcd classes is

$$\mathcal{A}_n = \{ \text{circ}(u) : u = \sum_{d|n} a_d \text{ind}(G_n(d)) \text{ for some } a_d \in \mathbb{Z} \}.$$

Example 3.2.3.

$$\text{ind}(G_8(1)) = \text{ind}(\{1, 3, 5, 7\}) = [0, 1, 0, 1, 0, 1, 0, 1],$$

$$\text{ind}(G_8(2)) = \text{ind}(\{2, 6\}) = [0, 0, 1, 0, 0, 0, 1, 0],$$

$$\text{ind}(G_8(4)) = \text{ind}(\{4\}) = [0, 0, 0, 0, 1, 0, 0, 0], \text{ and}$$

$$\text{ind}(G_8(8)) = \text{ind}(\{0\}) = [1, 0, 0, 0, 0, 0, 0, 0].$$

The circulant matrices

$$\text{circ}(\text{ind}(G_8(1))), \text{circ}(\text{ind}(G_8(2))), \text{circ}(\text{ind}(G_8(4))), \text{ and } \text{circ}(\text{ind}(G_8(8)))$$

are in $\mathcal{A}_8$. The first row of any element of $\mathcal{A}_8$ has the form

$$[a_8, a_1, a_2, a_4, a_1, a_2, a_1],$$

where a_1, a_2, a_4 , and a_8 are integers.

Lemma 3.2.4. *Let $u = [u_0, \dots, u_{n-1}]$ be an integer vector. Then $\text{circ}(u) \in \mathcal{A}_n$ if and only if $s, t \in G_n(j)$ implies $u_s = u_t$ for any proper divisor j of n .*

Proof. Follows from the definition of $\mathcal{A}_n$. □

Lemma 3.2.5. *If $\text{circ}(u) \in \mathcal{A}_n$, then $\text{circ}(u)$ has integer eigenvalues.*

Proof. From Definition 2.2.12, $\lambda_t(\text{circ}(u)) = \sum_{j=0}^{n-1} u_j \omega^{tj}$. Since $\text{circ}(u) \in \mathcal{A}_n$, and using the definition of gcd classes,

$$\begin{aligned}
\lambda_t(\text{circ}(u)) &= \sum_{j=0}^{n-1} u_j \omega^{tj} \\
&= \sum_{d|n} \sum_{j \in G_n(d)} u_j \omega^{tj} \\
&= \sum_{d|n} u_d \sum_{j \in G_n(d)} \omega^{tj} \\
&= \sum_{d|n} u_d c_t \left(\frac{n}{d} \right).
\end{aligned}$$

The final sum is an integer since Ramanujan sums are integers (Lemma 3.1.10). $\square$

Lemma 3.2.6. *Let $u = [u_0, \dots, u_{n-1}]$ be an integer vector such that $\text{circ}(u)$ has the integral spectral sequence $v = [v_0, \dots, v_{n-1}]$. Then $\text{circ}(v) \in \mathcal{A}_n$.*

Proof. By Lemma 3.2.4 it is sufficient to show that if d is a proper divisor of n and $s, t \in G_n(d)$ then $v_s = v_t$. Let d, s , and t be as described, and $s' = \frac{s}{d}$, and $t' = \frac{t}{d}$. Both s' and t' are integers since $s, t \in G_n(d)$. Let $f(x) = \sum_{j=0}^{n-1} u_j x^{dj}$ and $p(x) = f(x) - \lambda_s(\text{circ}(u))$. Since u has integer entries, $p(x)$ has integer and a priori rational coefficients. Evaluating $p(x)$ at $\omega^{s'}$ gives $p(\omega^{s'}) = f(\omega^{s'}) - \lambda_s(\text{circ}(u)) = \lambda_s(\text{circ}(u)) - \lambda_s(\text{circ}(u)) = 0$. That is, $\omega^{s'}$ is a root of $p(x)$. If $\omega^{t'}$ is a root of $p(x)$, then $0 = p(\omega^{t'}) = f(\omega^{t'}) - \lambda_s(\text{circ}(u))$, which implies $\lambda_s(\text{circ}(u)) = f(\omega^{t'}) = \lambda_t(\text{circ}(u))$. So we just need to show that $\omega^{t'}$ is a root of $p(x)$. Observe that $\gcd(s', \frac{n}{d}) = \gcd(t', \frac{n}{d}) = 1$. Therefore $\omega^{s'}$ and $\omega^{t'}$ are roots of $\Phi_{\frac{n}{d}}(x)$. By Theorem 3.1.18, $\Phi_{\frac{n}{d}}(x)$ is the minimum polynomial of $\omega^{s'}$ over $\mathbb{Q}$. By definition of the minimum polynomial, $\Phi_{\frac{n}{d}}(x)$ divides $p(x)$. Then since $\omega^{t'}$ is a root of $\Phi_{\frac{n}{d}}(x)$, it is a root of $p(x)$. $\square$

Theorem 3.2.7. *Let u be an integer vector. Then $\text{circ}(u)$ has integer eigenvalues if and only if $\text{circ}(u) \in \mathcal{A}_n$.*

Proof. Assume $\text{circ}(u)$ has integer eigenvalues. Let v be the spectral sequence of $\text{circ}(u)$. By Theorem 2.2.14, $\sqrt{n}F_n u^T = v^T$. Multiplying on the left by $\sqrt{n}F_n^*$ yields $\sqrt{n}F^* \sqrt{n}F_n u^T = \sqrt{n}F_n^* v^T$. Since F_n is unitary, we have $nu^T = \sqrt{n}F_n^* v^T$. Using that $F^* = \overline{F_n}$, and that u and v are integer vectors, $nu^T = \sqrt{n}F^* v^T = \sqrt{n}\overline{F} v^T = \overline{\sqrt{n}F_n v^T} = \sqrt{n}F_n v^T$. By applying Theorem 2.2.14 again, $nu^T = \sqrt{n}F_n v^T$ implies that nu is the spectral sequence for $\text{circ}(v)$. By Lemma 3.2.6, $\text{circ}(nu)$ is in $\mathcal{A}_n$. From the definition of $\mathcal{A}_n$, $\text{circ}(u)$ is also in $\mathcal{A}_n$.

Conversely, assume that $\text{circ}(u) \in \mathcal{A}_n$. From Lemma 3.2.5, $\text{circ}(u)$ has integer eigenvalues. □

CHAPTER 4

INTEGRAL CIRCULANT GRAPHS

4.1 Eigenvalues of a Circulant Graph

Theorem 4.1.1. *The eigenvalues of $\Gamma_n(S)$ are $\lambda_t(\Gamma_n(S)) = \sum_{j \in S} \omega^{jt}$, $0 \leq t \leq n-1$. Furthermore, $\lambda_t(\Gamma_n(S))$ is real for all $0 \leq t \leq n-1$.*

Proof. $\lambda_t(\Gamma_n(S)) = \lambda_t(\text{circ}(\text{ind}(S))) = \sum_{j=0}^{n-1} \text{ind}(S)_j \omega^{jt} = \sum_{j \in S} \omega^{jt}$. Adjacency matrices are real and symmetric, and therefore Hermitian. Hermitian matrices have real eigenvalues (see [HJ85, p. 104]). $\square$

Theorem 4.1.2. *Let $\Gamma_n(S)$ be an integral circulant and t a positive integer less than n . Then $\lambda_t(\Gamma_n(S)) = \lambda_{n-t}(\Gamma_n(S))$.*

Proof. By the last theorem, $\lambda_t(\Gamma_n(S)) = \sum_{j \in S} \omega^{jt} = \overline{\sum_{j \in S} \omega^{jt}} = \sum_{j \in S} \omega^{-jt}$. Since $\omega^{jn} = 1$, we have $\sum_{j \in S} \omega^{-jt} = \sum_{j \in S} \omega^{jn} \omega^{-jt} = \sum_{j \in S} \omega^{j(n-t)} = \lambda_{n-t}(\Gamma_n(S))$. $\square$

Theorem 4.1.3. *Let $\Gamma_n(S)$ be a circulant graph and λ any one of its eigenvalues. Then $\lambda_0(\Gamma_n(S)) \geq \lambda$.*

Proof. By Theorem 2.2.11, the $n \times 1$ vector e of 1s is an eigenvector corresponding to $\lambda_0(\Gamma_n(S))$. Since circulants are regular, $\text{circ}(\text{ind}(S))e = |S|e$. Thus $\lambda_0(\Gamma_n(S)) = |S|$, the degree of the vertices of $\Gamma_n(S)$. By Theorem 1.2.1, $|S|$ is greater than or equal to λ . $\square$

Theorem 4.1.4. *Let $S_1, \dots, S_m$ be pairwise disjoint subsets of $\{1, \dots, n-1\}$, and $S = \bigcup_{j=1}^m S_j$. The eigenvalues of $\Gamma_n(S)$ are $\lambda_t(\Gamma_n(S)) = \sum_{j=1}^m \lambda_t(\Gamma_n(S_j))$, $0 \leq t \leq n-1$.*

Proof. $\lambda_t(\Gamma_n(S)) = \sum_{j \in S} \omega^{jt} = \sum_{j=1}^m \sum_{l \in S_j} \omega^{lt} = \sum_{j=1}^m \lambda_t(\Gamma_n(S_j))$ $\square$

4.2 Integral Circulant Graphs

Theorem 4.2.1 ([So06]). *Let S be a subset of $\{1, \dots, n-1\}$. The circulant graph $\Gamma_n(S)$ is integral if and only if there is a subset D of the proper divisors of n such that $S = \bigcup_{d \in D} G_n(d)$.*

Proof. By the definition of a circulant graph, $\Gamma_n(S)$ is integral if and only if $\text{circ}(\text{ind}(S))$ is integral. From Theorem 3.2.7, $\text{circ}(\text{ind}(S))$ is integral if and only if it is in $\mathcal{A}_n$. This implies that $\text{ind}(S) = \sum_{d|n} a_d \text{ind}(G_n(d))$ for some $a_d \in \mathbb{Z}$. Since $\text{circ}(\text{ind}(S))$ is an adjacency matrix of a graph, $a_n = 0$ and the rest of the a_d are either 0 or 1. $\square$

Corollary 4.2.2 ([So06]). *There are at most $2^{\tau(n)-1}$ integral circulant graphs of order n .*

Proof. There are $\tau(n) - 1$ proper divisors of n and thus $2^{\tau(n)-1}$ subsets of the proper divisors of n . By Theorem 4.2.1 there is a subset of proper divisors of n corresponding to each integral circulant of order n . $\square$

There are not necessarily exactly $2^{\tau(n)-1}$ integral circulant graphs of order n since more than one symbol could correspond to the same graph.

Definition 4.2.3. Let S be a subset of $\{1, \dots, n-1\}$. If $S = \emptyset$ or $S = G_n(d)$ for some $d|n, d \neq n$, we say that integral circulant $\Gamma_n(S)$ is *elementary*. There are $\tau(n)$ elementary integral circulants of order n . An integral circulant is *compound* if it is not

elementary. If D is a subset of the proper divisors of n , denote the integral circulant $\Gamma_n(\bigcup_{d \in D} G_n(d))$ by $IC_n(D)$. For brevity, if d_1 and d_2 are proper divisors of n we write $IC_n(d_1, d_2)$ rather than $IC_n(\{d_1, d_2\})$.

Example 4.2.4 (Integral circulant graphs of order 8). The proper divisors of 8 are 1, 2 and 4. The elementary integral circulants of order 8 have symbols $\emptyset$, $G_8(1) = \{1, 3, 5, 7\}$, $G_8(2) = \{2, 6\}$, and $G_8(4) = \{4\}$ and are denoted $IC_8(\emptyset)$, $IC_8(1)$, $IC_8(2)$, $IC_8(4)$, respectively. There are four compound integral circulants of order 8: $IC_8(1, 2)$, $IC_8(1, 4)$, $IC_8(2, 4)$, $IC_8(1, 2, 4)$. They correspond to the different unions of two or more of the nonempty elementary symbols. All integral circulants of order 8 are shown in Figure 4.1.

Up to isomorphism there are four circulant graphs of order 8 that are not integral. They are $\Gamma_8(\{1, 7\})$, $\Gamma_8(\{1, 4, 7\})$, $\Gamma_8(\{1, 2, 6, 7\})$, and $\Gamma_8(\{1, 2, 4, 6, 7\})$ (see Figure 4.2).

In the proof of Lemma 3.2.5 we saw that the eigenvalues of an integral circulant matrix can be expressed in terms of Ramanujan sums. The next theorem makes explicit the relationship between the eigenvalues of an elementary integral circulant graph and the number theoretic formula for a Ramanujan sum given in Lemma 3.1.10.

Theorem 4.2.5. For $0 \leq t \leq n-1$, $\lambda_t(IC_n(d)) = \frac{\phi(\frac{n}{d})}{\phi(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, t)})} \mu\left(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, t)}\right)$

Proof. $\lambda_t(IC_n(d)) = \sum_{j \in G_n(d)} \omega^{jt} = c_t(\frac{n}{d}) = \frac{\phi(\frac{n}{d})}{\phi(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, t)})} \mu\left(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, t)}\right)$ □

Corollary 4.2.6. $\lambda_0(IC_n(d)) = \phi\left(\frac{n}{d}\right)$.

Figure 4.1: Integral circulants of order 8.

Figure 4.2: Non-integral circulants of order 8 and their symbols.

Proof.

$$\begin{aligned}
 \lambda_0(IC_n(d)) &= \frac{\phi\left(\frac{n}{d}\right)}{\phi\left(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, 0)}\right)} \mu\left(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, 0)}\right) \\
 &= \frac{\phi\left(\frac{n}{d}\right)}{\phi(1)} \mu(1) \\
 &= \phi\left(\frac{n}{d}\right)
 \end{aligned}$$

□

Corollary 4.2.7. $\lambda_1(IC_n(d)) = \mu\left(\frac{n}{d}\right)$.

Proof.

$$\begin{aligned}
 \lambda_1(IC_n(d)) &= \frac{\phi\left(\frac{n}{d}\right)}{\phi\left(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, 1)}\right)} \mu\left(\frac{\frac{n}{d}}{\gcd(\frac{n}{d}, 1)}\right) \\
 &= \frac{\phi\left(\frac{n}{d}\right)}{\phi\left(\frac{n}{d}\right)} \mu\left(\frac{n}{d}\right) \\
 &= \mu\left(\frac{n}{d}\right)
 \end{aligned}$$

□

Theorem 4.2.8. Let l and n be positive integers such that $\gcd(l, n) = 1$. If S is the symbol of an integral circulant, then $lS = S$, where $lS = \{ls \pmod{n} : s \in S\}$.

Proof. By Theorem 4.2.1, there is a subset D of the proper divisors of n such that $S = \bigcup_{d \in D} G_n(d)$. By Theorem 3.1.6 and the definition of gcd classes, $lS = \bigcup_{d \in D} lG_n(d) = \bigcup_{d \in D} G_n(d) = S$. □

Theorem 4.2.9. Let Γ be an integral circulant of order n and λ one of its eigenvalues. In addition, let D be a subset of the proper divisors of n such that for all $d \in D$, $\lambda_d(\Gamma) = \lambda$. Then the multiplicity of λ is at least $\sum_{d \in D} \phi\left(\frac{n}{d}\right)$.

Proof. Since Γ is an integral circulant, its adjacency matrix is in $\mathcal{A}_n$. Let v be the spectral sequence of Γ . By Lemma 3.2.6, $\text{circ}(v)$ is also in $\mathcal{A}_n$. If s is an element of D , then $s \in G_n(s)$. By Lemma 3.2.4, if $t \in G_n(s)$, then $\lambda_t(\Gamma) = \lambda_s(\Gamma)$. Thus the multiplicity of $\lambda_s(\Gamma) = \lambda$ is at least $|G_n(s)| = \phi(\frac{n}{s})$. Since gcd classes are disjoint, the multiplicity of λ is at least $\sum_{d \in D} \phi(\frac{n}{d})$. $\square$

Theorem 4.2.9 implies that the multiplicity of $\lambda_t(\Gamma)$ is at least $\phi(\frac{n}{\gcd(t,n)})$ for any $0 < t < n$.

4.3 Prime Power Order

This section contains a proof showing that integral circulant graphs of prime power order satisfy SAP. The approach is to show for any fixed order p^k , no two integral circulants have the same largest eigenvalue. We will represent largest eigenvalues as 0, 1-vectors. The next two lemmas will help show that no two such vectors are the same.

Lemma 4.3.1. *Let $a, b \in \{0, 1\}^n$, and x a $1 \times n$ vector with nonnegative integer entries. If $x_{k+1} > \sum_{j=1}^k x_j$ for all $1 \leq k \leq n-1$, and $ax^T = bx^T$ then $a = b$.*

Proof. Assume $a \neq b$. Let $R = \{j \in \mathbb{Z} : a_j \neq b_j\}$ and m the largest element of R . Suppose without loss of generality that $a_m = 1$ and $b_m = 0$. Then we have the contradiction:

$$\begin{aligned} ax^T &= \sum_{j=1}^n a_j x_j \\ &= \sum_{j=1}^m a_j x_j + \sum_{j=m+1}^n a_j x_j \end{aligned}$$

$$\begin{aligned}
&= \sum_{j=1}^m a_j x_j + \sum_{j=m+1}^n b_j x_j \text{ (since } m \text{ is the largest element of } R) \\
&\geq x_m + \sum_{j=m+1}^n b_j x_j \text{ (since } a_m = 1) \\
&> \sum_{j=1}^{m-1} x_j + \sum_{j=m+1}^n b_j x_j \\
&\geq \sum_{j=1}^m b_j x_j + \sum_{j=m+1}^n b_j x_j \text{ (since } b_m = 0) \\
&= \sum_{j=1}^n b_j x_j \\
&= bx^T
\end{aligned}$$

□

Lemma 4.3.2. *Let p be prime and k a positive integer. Then $p^k > \sum_{j=0}^{k-1} p^j$.*

Proof.

$$\begin{aligned}
p^k &> p^k - 1 \\
&= (p - 1) \sum_{j=0}^{k-1} p^j \\
&\geq \sum_{j=0}^{k-1} p^j
\end{aligned}$$

□

Theorem 4.3.3 ([So06]). *Let p be a prime number and k a positive integer. Every integral circulant order p^k satisfies SAP.*

Proof. Let Γ be the integral circulant with symbol $S = \bigcup_{d \in D} G_{p^k}(d)$, where D is a subset of the proper divisors of p^k . Theorem 4.1.3 tells us that $\lambda_0(\Gamma)$ is equal to the largest eigenvalue of Γ . By Corollary 4.2.6 and Theorem 4.1.4, $\lambda_0(\Gamma) = \sum_{d \in D} \phi(\frac{p^k}{d})$.

Since every $d \in D$ is of the form p^r for some $0 \leq r < k$, we can write $\lambda_0(\Gamma) = \sum_{j=0}^{k-1} a_j \phi(\frac{p^k}{p^j})$ where $a_j = 1$ if $p^j \in D$ and $a_j = 0$ otherwise. We have $\phi(\frac{p^k}{p^j}) = \phi(p^{k-j}) = (p-1)p^{k-j-1}$, so $\sum_{j=0}^{k-1} a_j \phi(\frac{p^k}{p^j}) = (p-1) \sum_{j=0}^{k-1} a_j p^{k-j-1}$. Let Δ be any integral circulant of order p^k such that $\lambda_0(\Delta) = \lambda_0(\Gamma)$. We can write $\lambda_0(\Delta) = (p-1) \sum_{j=0}^{k-1} b_j p^{k-j-1}$ for some b_j . By Lemmas 4.3.2 and 4.3.1, $a_j = b_j$ for all j . Therefore Γ and Δ have the same symbol. $\square$

CHAPTER 5

INTEGRAL CIRCULANTS WITH THE SPECTRAL ÁDÁM PROPERTY

In this chapter we attempt to show that for p and q prime, every integral circulant order pq^k satisfies SAP. We assume $p < q$ for the rest of the chapter and treat the two cases pq^k for $k > 0$ and qp^k for $k > 1$. Except when $p = 2$ the spectra of graphs of order pq^k can be distinguished by their largest eigenvalues. For the case qp^k , we prove that distinct spectra correspond to distinct symbols when $k = 2$, but for other values of k the question is still open.

5.1 Order pq^k , where $p < q$ and $k > 0$

The first theorem in this section covers the case of $p > 2$, and the second theorem $p = 2$. The general approach in both theorems is the same as in the case of prime power orders (Theorem 4.3.3).

Theorem 5.1.1. *Let $2 < p < q$. Every integral circulant of order pq^k satisfies SAP.*

Proof. Recall that an elementary integral circulant has symbol $G_n(d)$ for some proper divisor d of n (Definition 4.2.3). The $2k+1$ proper divisors of pq^k can be divided into three forms, pq^r with $k > r \geq 0$, q^r with $k > r \geq 0$, and q^k . Using Theorem 4.1.3 and Corollary 4.2.6, the largest eigenvalues of the elementary integral circulants of order

pq^k are

$$\begin{aligned}\lambda_0(IC_{pq^k}(q^k)) &= \phi(p) = p - 1 \\ \lambda_0(IC_{pq^k}(pq^r)) &= \phi(q^{k-r}) = (q - 1)q^{k-r-1} \\ \lambda_0(IC_{pq^k}(q^r)) &= \phi(pq^{k-r}) = (p - 1)(q - 1)q^{k-r-1},\end{aligned}$$

where $0 \leq r < k$. Let

$$a_m = \begin{cases} p - 1 & \text{if } m = 0 \\ (q - 1)q^{\frac{m+1}{2}-1} & \text{if } m \text{ is odd} \\ (p - 1)(q - 1)q^{\frac{m}{2}-1} & \text{otherwise} \end{cases}$$

for $0 \leq m \leq 2k$. That is, $\{a_m\}$ is just a finite sequence formed from these eigenvalues. Since $2 < p < q$, $\{a_m\}$ is strictly increasing. The largest eigenvalue of every integral circulant of order pq^k is a sum of one or more of terms of this sequence (this follows from Theorem 4.1.4). Therefore, by using Lemma 4.3.1 it is sufficient to show that $\sum_{j=0}^m a_j < a_{m+1}$ for $0 \leq m \leq 2k$. This is done by induction on m . The base case is simple: $a_0 = p - 1 < q - 1 = a_1$. Now assume $m > 0$. If m is even, then

$$\begin{aligned}\sum_{j=0}^m a_j &= a_m + a_{m-1} + \sum_{j=0}^{m-2} a_j \\ &< a_m + a_{m-1} + a_{m-1} \\ &= (p - 1)(q - 1)q^{\frac{m}{2}-1} + 2(q - 1)q^{\frac{m}{2}-1} \\ &= (p + 1)(q - 1)q^{\frac{m}{2}-1} \\ &< (q - 1)q^{\frac{m+2}{2}-1} \quad (\text{since } 2 < p < q) \\ &= a_{m+1}.\end{aligned}$$

Similarly, if m is odd, then

$$\begin{aligned}
\sum_{j=0}^m a_j &= a_m + \sum_{j=0}^{m-1} a_j \\
&< a_m + a_m \\
&= 2(q-1)q^{\frac{m+1}{2}-1} \\
&\leq (p-1)(q-1)q^{\frac{m+1}{2}-1} \\
&= a_{m+1}.
\end{aligned}$$

□

Next we consider circulants of order $2q^k$. It is not possible to distinguish the spectra of these graphs by using largest eigenvalues alone. Fortunately, we are able to use the eigenvalue λ_{q^k} by showing that its multiplicity is unique in connected graphs of this order.

Lemma 5.1.2. *For an integral circulant Γ of order $2m$, if $\lambda_0(\Gamma) = \lambda_m(\Gamma)$ then all the eigenvalues of Γ have even multiplicity. If $\lambda_0(\Gamma) \neq \lambda_m(\Gamma)$ then $\lambda_0(\Gamma)$ and $\lambda_m(\Gamma)$ are the only eigenvalues with odd multiplicity.*

Proof. According to Theorem 4.1.2 certain pairs of eigenvalues of a circulant graph are equal: $\lambda_1(\Gamma) = \lambda_{n-1}(\Gamma)$, $\lambda_2(\Gamma) = \lambda_{n-2}(\Gamma)$, etc. The eigenvalue $\lambda_0(\Gamma)$ is not included in these pairings, and since $n = 2m$ neither is $\lambda_m(\Gamma)$.

□

Theorem 5.1.3. *Let $2 < q$ and $k \geq 0$. Every integral circulant of order $2q^k$ satisfies SAP.*

Proof. By Theorem 1.3.13 we only need to consider connected graphs. These are the graphs whose largest eigenvalue has multiplicity 1. Let Γ be such a graph. By Lemma

5.1.2, $\lambda_0(\Gamma)$ and $\lambda_{q^k}(\Gamma)$ are the only eigenvalues of Γ that have odd multiplicities. Consequently, if another graph differs in these values, it can't be isospectral with Γ .

We now express the eigenvalues of Γ in terms of the eigenvalues of elementary integral circulants. Let d be a proper divisor of $2q^k$.

$$\lambda_0(IC_{2q^k}(d)) = \begin{cases} (q-1)q^{k-r-1} & \text{if } d = q^r, 0 \leq r < k \\ (q-1)q^{k-r-1} & \text{if } d = 2q^r, 0 \leq r < k \\ 1 & \text{if } d = q^k \end{cases}$$

$$\lambda_{q^k}(IC_{2q^k}(d)) = \begin{cases} (q-1)q^{k-r-1} & \text{if } d = q^r, 0 \leq r < k \\ -(q-1)q^{k-r-1} & \text{if } d = 2q^r, 0 \leq r < k \\ -1 & \text{if } d = q^k \end{cases}$$

Define $Q = [(q-1)q^{k-1}, (q-1)q^{k-2}, \dots, (q-1)q]$. The λ_0 eigenvalues of the elementary circulants of order $2q^k$ can be represented as the vector $\begin{bmatrix} Q & Q & 1 \end{bmatrix}$ and the λ_{q^k} eigenvalues as $\begin{bmatrix} -Q & Q & 1 \end{bmatrix}$. Thus, we have

$$\begin{bmatrix} Q & Q & 1 \\ -Q & Q & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \lambda_0(\Gamma) \\ \lambda_{q^k}(\Gamma) \end{bmatrix}$$

for some $x_1, x_2 \in \{0, 1\}^k$ and $x_3 \in \{0, 1\}$. If

$$\begin{bmatrix} Q & Q & 1 \\ -Q & Q & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} Q & Q & 1 \\ -Q & Q & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

for some $y_1, y_2 \in \{0, 1\}^k$ and $y_3 \in \{0, 1\}$, then

$$\begin{aligned} Qx_1 + Qx_2 + x_3 &= Qy_1 + Qy_2 + y_3 \\ -Qx_1 + Qx_2 - x_3 &= -Qy_1 + Qy_2 - y_3. \end{aligned}$$

Adding these equations gives $Qx_1 = Qy_1$. Using Lemma 4.3.1 and Lemma 4.3.2, this implies $x_1 = y_1$. Subtracting the equations gives $Qx_2 + x_3 = Qy_2 + y_3$. Using the lemmas as before, it follows that $x_2 = y_2$ and $x_3 = y_3$.

□

5.2 Order qp^2 , where $p < q$

We consider two subcases: $q2^2$ and qp^2 .

Integral circulants of order $q2^2$ may not have distinct largest eigenvalues. Table 5.1 shows the integral circulants of order twelve ($q = 3$). Notice that three of the elementary circulants have 2 as the largest eigenvalue. Many of the graphs have 3, 4, 5, 6, 7, 8 and 9 as the largest eigenvalue. However, it is easy to check with a computer program or even by inspection that all the integral circulants of order 12 have distinct spectra. Therefore, we focus on $q > 3$.

For a given q there are 32 integral circulants of order $q2^2$. Table 5.2 shows the largest eigenvalues and their multiplicities for these graphs. The multiplicities are calculated using Theorem 1.3.10. Using that $q > 3$ it can be shown that distinct expressions for λ_0 in the table correspond to distinct eigenvalues. That is, for any $q > 3$, we have $0 < 1 < 2 < 3 < q < q + 1 < q + 2 < 2q - 2$, etc. However, several of the graphs have the same expression for largest eigenvalue.

The left half of Table 5.2 contains the graphs whose symbols are the union of fewer than three gcd classes. The right half contains the graphs with symbols comprised of three or more gcd classes. Notice that each row in the table contains

a complementary pair of graphs. If two regular graphs have distinct spectra then their complements have distinct spectra (Theorem 1.2.3). This means it is sufficient to show that the graphs with symbols containing fewer than three gcd classes have spectra distinct from each other and from the graphs with symbols containing three or more gcd classes. Furthermore, by Theorem 1.3.13 it is only necessary to show that the connected graphs of order $q2^2$ satisfy SAP.

Theorem 5.2.1. *Let $q > 2$. Every integral circulant of order $q2^2$ satisfies SAP.*

Proof. The case of $q = 3$ can be verified by inspection. Assume $q > 3$. We show that the connected graphs with symbols that consist of fewer than three gcd classes have spectra distinct from each other and from the connected graphs with symbols consisting of three or more gcd classes. There are seven connected graphs of order $q2^2$ that have fewer than three gcd classes in their symbol.

Case 1, $IC_{q2^2}(1)$: This is the only connected graph with largest eigenvalue $2q-2$.

Case 2, $IC_{q2^2}(1, 2)$: This graph has the same largest eigenvalue as $IC_{q2^2}(1, 4)$. However, $IC_{q2^2}(1, 2)$ has 1 as an eigenvalue with multiplicity greater than $2q-2+q-1 = 3q-3$, whereas 1 is an eigenvalue of $IC_{q2^2}(1, 4)$ with multiplicity at most $q+3$. This follows from Theorem 4.2.9 and the fact that $\lambda_1(IC_{q2^2}(1, 2)) = \lambda_2(IC_{q2^2}(1, 2)) = 1$, but $\lambda_1(IC_{q2^2}(1, 4)) = -1$.

Case 3, $IC_{q2^2}(1, 4)$: Resolved by case 2.

Case 4, $IC_{q2^2}(1, 2q)$: This graph has the same largest eigenvalue as $IC_{q2^2}(1, q, 2q)$, but $IC_{q2^2}(1, q, 2q)$ is not connected.

Case 5, $IC_{q2^2}(1, q)$: This graph has the same largest eigenvalue as $IC_{q2^2}(2, 4, q)$, but these graphs can't be isospectral since Case 4 shows that their complements are not isospectral.

Case 6, $IC_{q2^2}(2, q)$: This is similar to case 2. $IC_{q2^2}(2, q)$ has the same largest

Table 5.2: Eigenvalues of integral circulants of order $q2^2$ where $q > 2$. Each graph is identified by the gcd classes in its symbol. The column labeled m_0 contains the multiplicity of the largest eigenvalue.

gcd classes	λ_0	m_0	λ_1	λ_2	λ_4	gcd classes	λ_0	m_0	λ_1	λ_2	λ_4
0	0	$4q$	0	0	0	$1, 2, 4, q, 2q$	$4q - 1$	1	-1	-1	-1
1	$2q - 2$	1	0	2	-2	$2, 4, q, 2q$	$2q + 1$	1	-1	-3	1
2	$q - 1$	2	1	-1	-1	$1, 4, q, 2q$	$3q$	1	-2	0	0
4	$q - 1$	4	-1	-1	-1	$1, 2, q, 2q$	$3q$	1	0	0	0
q	2	q	0	-2	2	$1, 2, 4, 2q$	$4q - 3$	1	-1	1	-3
$2q$	1	$2q$	-1	1	1	$1, 2, 4, q$	$4q - 2$	1	0	-2	-2
$1, 2$	$3q - 3$	1	1	1	-3	$4, q, 2q$	$q + 2$	1	-2	-2	2
$1, 4$	$3q - 3$	1	-1	1	-3	$2, q, 2q$	$q + 2$	1	0	-2	2
$1, q$	$2q$	1	0	0	0	$2, 4, 2q$	$2q - 1$	2	-1	-1	-1
$1, 2q$	$2q - 1$	1	-1	3	-1	$2, 4, q$	$2q$	1	0	-4	0
$2, 4$	$2q - 2$	2	0	-2	-2	$1, q, 2q$	$2q + 1$	1	-1	1	1
$2, q$	$q + 1$	1	1	-3	1	$1, 4, 2q$	$3q - 2$	1	-2	2	-2
$2, 2q$	q	2	0	0	0	$1, 4, q$	$3q - 1$	1	-1	-1	-1
$4, q$	$q + 1$	1	-1	-3	1	$1, 2, 2q$	$3q - 2$	1	0	2	-2
$4, 2q$	q	2	-2	0	0	$1, 2, q$	$3q - 1$	1	1	-1	-1
$q, 2q$	3	q	-1	-1	3	$1, 2, 4$	$4q - 4$	1	0	0	-4

eigenvalue as $IC_{q^2}(4, q)$. However, $IC_{q^2}(2, q)$ has 1 as an eigenvalue with multiplicity greater than $2q - 2 + q - 1 = 3q - 3$, whereas one is an eigenvalue of $IC_{q^2}(4, q)$ with multiplicity at most $q + 3$. This follows from the fact that $\lambda_1(IC_{q^2}(2, q)) = \lambda_4(IC_{q^2}(2, q)) = 1$, but $\lambda_1(IC_{q^2}(4, q)) = -1$.

Case 7, $IC_{q^2}(4, q)$: See Case 6. $\square$

The argument for integral circulants of order qp^2 where $2 < p < q$ requires the following fact about eigenvalue λ_1 .

Lemma 5.2.2. *If Γ is an integral circulant of order qp^2 , then $\lambda_1(\Gamma)$ is the eigenvalue of Γ with largest multiplicity.*

Proof. From Theorem 4.2.9 the multiplicity of $\lambda_1(\Gamma)$ is greater than or equal to $\phi(qp^2)$. Counting multiplicity, Γ has qp^2 eigenvalues, so the multiplicity of any eigenvalue other than $\lambda_1(\Gamma)$ is less than or equal to $qp^2 - \phi(qp^2)$. Then for $\lambda_1(\Gamma)$ to be the largest eigenvalue of Γ , we need $\phi(qp^2) > qp^2 - \phi(qp^2)$. Using that $\phi(qp^2) = (q-1)(p-1)p$ and solving for q , the required inequality becomes $q > \frac{2(p-1)}{p-2}$. The inequality holds since $q > 2$. $\square$

Lemma 5.2.3. $\phi(pq^2) > \phi(p) + \phi(q) + \phi(p^2) + \phi(pq)$.

Proof. Since the gcd classes of qp^2 form a partition of $\{0 \dots qp^2 - 1\}$, we have $qp^2 = \phi(1) + \phi(p) + \phi(q) + \phi(p^2) + \phi(pq) + \phi(qp^2)$. From the proof of the last theorem, $2\phi(qp^2) > qp^2$. $\square$

Theorem 5.2.4. *Let $2 < p < q$. Every integral circulant of order qp^2 satisfies SAP.*

Proof. For each choice of p and q there are 32 possible graphs in this class (table 5.3). Using the same reasoning about complements and connectivity as in the last theorem, we are left with seven connected graphs to consider. We show that the

spectra of these graphs are distinct from each other and from the connected graphs with symbols consisting of three or more gcd classes.

Case 1, $IC_{qp^2}(1)$: The largest eigenvalue of this graph $\phi(qp^2)$ is distinct. From Lemma 5.2.3, $\phi(qp^2)$ is larger than $\phi(p) + \phi(q) + \phi(p^2) + \phi(qp)$. And clearly $\phi(qp^2)$ plus any positive number is greater than $\phi(qp^2)$.

Case 2, $IC_{qp^2}(1, p)$: Since $\lambda_1(IC_{qp^2}(1, p)) = 1$ it is only necessary to consider graphs with $\lambda_1 = 1$. There are only two of these: $IC_{qp^2}(1, p, q)$ has a larger value for λ_0 and $IC_{qp^2}(p, q)$ has a smaller one.

Case 3, $IC_{qp^2}(1, p^2)$: $\lambda_0(IC_{qp^2}(1, p^2)) > \lambda_0(IC_{qp^2}(1, qp))$ since $\phi(q) > \phi(p)$. $\lambda_0(IC_{qp^2}(1, p^2)) \neq \lambda_0(IC_{qp^2}(1, q, qp))$ since $\phi(q) = q - 1 \neq p^2 - 1 = p(p - 1) + p - 1 = \phi(p^2) + \phi(p)$. The rest are easy to check.

Case 4, $IC_{qp^2}(1, q)$: $\lambda_0(IC_{qp^2}(1, q)) < \lambda_0(IC_{qp^2}(1, p, qp))$ since $\phi(p^2) = p(p - 1) < (p - 1)(q - 1) + p - 1 = \phi(qp) + \phi(p)$.

Case 5, $IC_{qp^2}(1, qp)$: Similar to case 1.

Case 6, $IC_{qp^2}(p, q)$: Easy to check since largest eigenvalue is less than $\phi(qp^2)$.

Case 7, $IC_{qp^2}(p^2, q)$: Easy to check since largest eigenvalue is less than $\phi(qp^2)$.

□

5.3 Order qp^k , where $p < q$ and $k > 2$

The largest eigenvalue λ_0 is not sufficient to distinguish these graphs. Furthermore, there is no obvious way to single out eigenvalues by multiplicity as we did with λ_1 in the last case. There are $2k + 1$ proper divisors of qp^k and thus 2^{2k+1} symbols to consider. Using the techniques presented in this thesis, it seems that an arbitrarily large number of special cases would need to be considered.

Table 5.3: Integral circulants of order qp^2 where $p > 2$. Each graph is identified by the gcd classes in its symbol.

gcd classes	λ_0	m_0	λ_1	gcd classes	λ_0	m_0	λ_1
1	$\phi(qp^2)$	1	0	p, p^2, q, qp	$\phi(qp) + \phi(q) + \phi(p^2) + \phi(p)$	1	-1
p	$\phi(qp)$	p	1	$1, p^2, q, qp$	$\phi(qp^2) + \phi(q) + \phi(p^2) + \phi(p)$	1	-2
p^2	$\phi(q)$	p^2	-1	$1, p, q, qp$	$\phi(qp^2) + \phi(qp) + \phi(p^2) + \phi(p)$	1	0
q	$\phi(p^2)$	q	0	$1, p, p^2, qp$	$\phi(qp^2) + \phi(qp) + \phi(q) + \phi(p)$	1	-1
qp	$\phi(p)$	qp	-1	$1, p, p^2, q$	$\phi(qp^2) + \phi(qp) + \phi(q) + \phi(p^2)$	1	0
$1, p$	$\phi(qp^2) + \phi(qp)$	1	1	p^2, q, qp	$\phi(q) + \phi(p^2) + \phi(p)$	1	-2
$1, p^2$	$\phi(qp^2) + \phi(q)$	1	-1	p, q, qp	$\phi(qp) + \phi(p^2) + \phi(p)$	1	0
$1, q$	$\phi(qp^2) + \phi(p^2)$	1	0	p, p^2, qp	$\phi(qp) + \phi(q) + \phi(p)$	p	-1
$1, qp$	$\phi(qp^2) + \phi(p)$	1	-1	p, p^2, q	$\phi(qp) + \phi(q) + \phi(p^2)$	1	0
p, p^2	$\phi(qp) + \phi(q)$	p	0	$1, q, qp$	$\phi(qp^2) + \phi(p^2) + \phi(p)$	1	-1
p, q	$\phi(qp) + \phi(p^2)$	1	1	$1, p^2, qp$	$\phi(qp^2) + \phi(q) + \phi(p)$	1	-2
p, qp	$\phi(qp) + \phi(p)$	p	0	$1, p^2, q$	$\phi(qp^2) + \phi(q) + \phi(p^2)$	1	-1
p^2, q	$\phi(q) + \phi(p^2)$	1	-1	$1, p, qp$	$\phi(qp^2) + \phi(qp) + \phi(p)$	1	0
p^2, qp	$\phi(q) + \phi(p)$	p	-2	$1, p, q$	$\phi(qp^2) + \phi(qp) + \phi(p^2)$	1	1
q, qp	$\phi(p^2) + \phi(p)$	q	-1	$1, p, p^2$	$\phi(qp^2) + \phi(qp) + \phi(q)$	1	0

BIBLIOGRAPHY

- [Ádá67] A. Ádám. Research problem 2-10. Journal of Combinatorial Theory, 2:393, 1967.
- [Big93] N.L. Biggs. Algebraic Graph Theory, Second Edition. Cambridge University Press, 1993.
- [BM79] W. G. Bridges and R. A. Mena. Rational circulants with rational spectra and cyclic strongly regular graphs. Ars. Combin., 8:143–161, 1979.
- [Dav94] Philip J. Davis. Circulant Matrices. Chelsea Publishing, 1994.
- [ET70] Bernard Elspas and James Turner. Graphs with circulant adjacency matrices. Journal of Combinatorial Theory, 9:297–307, 1970.
- [Gri99] P. Grillet. Algebra. Wiley Interscience Publication, 1999.
- [HJ85] Roger A. Horn and Charles R. Johnson. Matrix Analysis. Cambridge University Press, 1985.
- [Hun74] Thomas W. Hungerford. Algebra. Springer-Verlag, 1974.
- [IR90] Kenneth Ireland and Michael Rosen. A Classical Introduction to Modern Number Theory. Springer, 1990.
- [MPS02] Bernard Mans, Fancesco Pappalardi, and Igor Shparlinski. On the spectral adam property for circulant graphs. Discrete Mathematics, 254:309–329, 2002.
- [Muz95] Mikhail Muzychuk. Ádám’s conjecture is true in the square-free case. Journal of Combinatorial Theory, Series A 72:118–134, 1995.
- [Ram18] S. Ramanujan. On certain trigonometrical sums and their applications in the theory of numbers. Cambridge Phil. Trans., 22:259–276, 1918.
- [So06] Wasin So. Integral circulant graphs. Discrete Mathematics, 306:153–158, 2006.

- [Wes01] Douglas B. West. Introduction to Graph Theory. Prentice Hall, 2001.