UNIFORM MIXING OF QUANTUM WALKS AND ASSOCIATION SCHEMES

by

Natalie E. Mullin

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2013

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In recent years quantum algorithms have become a popular area of mathematical research. Farhi and Gutmann introduced the concept of a quantum walk in 1998. In this thesis we investigate mixing properties of continuous-time quantum walks from a mathematical perspective. We focus on the connections between mixing properties and association schemes.

There are three main goals of this thesis. Our primary goal is to develop the algebraic groundwork necessary to systematically study mixing properties of continuous-time quantum walks on regular graphs. Using these tools we achieve two additional goals: we construct new families of graphs that admit uniform mixing, and we prove that other families of graphs never admit uniform mixing.

We begin by introducing association schemes and continuous-time quantum walks. Within this framework we develop specific algebraic machinery to tackle the uniform mixing problem. Our main algebraic result shows that if a graph has an irrational eigenvalue, then its transition matrix has at least one transcendental coordinate at all nonzero times.

Next we study algebraic varieties related to uniform mixing to determine information about the coordinates of the corresponding transition matrices. Combining this with our main algebraic result we prove that uniform mixing does not occur on even cycles or prime cycles. However, we show that the probability distribution of a quantum walk on a prime cycle gets arbitrarily close to uniform.

Finally we consider uniform mixing on Cayley graphs of elementary abelian groups. We utilize graph quotients to connect the mixing properties of these graphs to Hamming graphs. This enables us to find new results about uniform mixing on Cayley graphs of $\mathbb{Z}_3^d$ and $\mathbb{Z}_4^d$.

Acknowledgements

First and foremost, I am grateful for the guidance of my supervisor, Chris Godsil. Throughout my graduate career, his direction and knowledge has positively shaped my research. I would like to thank him for his generosity of ideas.

Next I offer thanks to my committee members: Eric Moorhouse, David Wagner, Andrew Childs, and Jason Bell. Their thoughtful comments have greatly improved this thesis. I appreciate the time and effort they contributed.

Finally, I would like to thank Brent for his endless optimism. His encouragement was invaluable during the writing process.

Table of Contents

1 Introduction **1**

1.1 Main Results 2
1.2 Graph Theory Tools 4

2 Association Schemes **7**

2.1 Introduction 7
2.2 Cayley Graphs 8
2.3 Strongly Regular Graphs 9
2.4 Association Schemes 12
2.5 Bose-Mesner Algebra 13
2.6 Krein Parameters 15
2.7 Hamming Schemes 17
2.8 Cyclic Schemes 19
2.9 Cyclic Duality 22

3 Quantum Walks **27**

3.1 Introduction 27
3.2 Transition Matrices 28
3.3 Mixing Properties 31
3.4 Mixing on Complete Graphs 33
3.5 Graph Complements 35
3.6 Mixing in Association Schemes 37

4 Algebraic Connections **39**

4.1 Introduction 39
4.2 Algebraic vs. Transcendental Numbers 40
4.3 Cyclotomic Number Theory 42
4.4 Kronecker's Theorem 44
4.5 Type-II Matrices 47
4.6 Systems of Polynomial Equations 48

4.7 Cyclic n-roots 50

5 Bipartite Graphs and Cycles **53**
5.1 Introduction 53
5.2 Bipartite Graphs 54
5.3 Even Cycles 56
5.4 Prime Cycles 57
5.5 ϵ-Uniform Mixing on Prime Cycles 58

6 Strongly Regular Graphs **63**
6.1 Introduction 63
6.2 Type-II Matrices and SRGs 63
6.3 Uniform Mixing on SRGs 66
6.4 Construction from Hadamard Matrices 68
6.5 Conference Graphs, Revisited 72

7 Products and Quotients **79**
7.1 Motivation and Tools 79
7.2 Graph Products 80
7.3 Graph Quotients 84
7.4 Quotients of Hamming Graphs 87
7.5 Linear Graphs 90

8 Quotients of Hamming Graphs **95**
8.1 Introduction 95
8.2 Linear Codes 96
8.3 Cubelike Graphs 98
8.4 Quotients of $H(d,3)$ 104
8.5 Quotients of $H(d,4)$ 108
8.6 General Quotients 112

9 Future Research **115**
9.1 Open Problems 115

References **119**

Index **125**

Chapter 1

Introduction

In recent years quantum algorithms have become a popular area of mathematical research. The continuous-time quantum walk was introduced in 1998 by Farhi and Gutmann [25]. Subsequently this model has been harnessed for a variety of applications within the realm of quantum computing. For example, quantum walks have been used in a black box graph transversal algorithm [21] and as a universal quantum computation model [20]. In this thesis we investigate continuous-time quantum walks from a mathematical perspective. We focus on the connections between the mixing properties of continuous-time quantum walks and association schemes. We are particularly interested in walks that reach uniform probability densities at a particular times. If a continuous-time quantum walk on a graph has this property, then we say that the graph admits *uniform mixing*.

There are three main goals of this thesis. Our primary goal is to develop the algebraic groundwork necessary to systematically study mixing properties of continuous-time quantum walks on regular graphs. Using our algebraic tools we achieve two additional goals: we construct new families of graphs that admit uniform mixing, and we prove that other families of graphs never admit uniform mixing.

Our methods heavily rely on the framework of association schemes. There are several reasons why this is a suitable approach. First, all of the graphs that are currently known to admit uniform mixing are intrinsically related to association schemes. Towards our goal of finding additional graphs that admit uniform mixing, it makes sense to begin our search with graphs within this realm. Moreover, association schemes are endowed with algebraic properties that directly relate to the mixing properties of continuous-time quantum walks. Using these properties, we derive necessary algebraic properties of graphs that admit uniform mixing. In turn, this enables us to show that certain infinite families of graphs do not admit uniform mixing.

Finally, and perhaps most importantly, association schemes are a natural framework because they provide a unifying language for the wide assortment of mathematical tools that we use. These tools include classical results in transcendental number theory, properties of algebraic varieties, and duality theory in coding theory. Thus, in a purely abstract light, this thesis can be viewed as a case study of the usefulness of association schemes.

1.1 Main Results

We summarize the main new results in this thesis, and we attempt to give a perspective on their significance. For an undirected graph X with adjacency matrix A, we let

$$U(t) = \exp(itA)$$

denote the transition matrix corresponding the the continuous-time quantum walk. The mixing matrix of a graph is an $n \times n$ matrix whose (j,k)-entry is given by

$$M(t)_{j,k} = |U(t)_{j,k}|^2.$$

The probability densities of the walk are given by the columns of the mixing matrix $M(t)$. One of our main goals in this thesis is to develop general machinery for detecting whether or not there exists some t such that the columns of $M(t)$ correspond to the uniform distribution. If such a time exists, we say that the graph X admits uniform mixing.

The following result is one of the most important results in this thesis. It is due to the author, and its proof relies heavily on the Gelfond-Schneider theorem of transcendental number theory.

Theorem 4.2.4. *Let X denote a graph. If the entries of the transition matrix $U(t)$ are all algebraic for some nonzero time t, then the ratio of any two eigenvalues of X must be rational.* □

This result does not require the graph to be in an association scheme. However, when the graph is in an association scheme, it is often possible to use the additional structure to show that $U(t)$ must have all algebraic entries at time t if uniform mixing occurs. This contradicts Theorem 4.2.4 and proves that the corresponding graph does not admit uniform mixing.

Prior to the work presented in this thesis, it was known that the cycles of length three and four admit uniform mixing, while the cycle of length five does not admit uniform mixing [16]. Also, Adamczak et al. [1] showed that C_n does not admit uniform mixing if $n = 2^u$ for $u \geq 3$, or if $n = 2^u m$ where m is not the sum of two integer squares and $u \geq 1$. It was conjectured by Ahmadi, Belk, Tamon, and Wendler in [3] that uniform mixing does not occur on the cycle of length n if $n \geq 5$. Using Theorem 4.2.4 we make significant progress towards proving this conjecture. First we show that uniform mixing does not occur on cycles of even length greater than four. This theorem is a joint result of the author and Godsil.

Theorem 5.3.1. *The cycle of length four is the unique even cycle that admits uniform mixing.* □

Next we show that uniform mixing cannot occur on cycles of prime length greater than three. This result is due to the author.

Theorem 5.4.1. *The cycle of length three is the unique cycle of odd prime order that admits uniform mixing.* □

We also consider cycles that come very close to admitting uniform mixing. Graphs with this property are said to admit ϵ-uniform mixing. The precise definition is given in Section 3.3. The following result is due to the author. Its proof relies heavily on Kronecker's Theorem.

Theorem 5.5.2. *Let p denote an odd prime. The cycle of length p admits ϵ-uniform mixing.* □

Another goal of this thesis is to describe new families of graphs that admit uniform mixing. The *Hamming graph* $H(d, n)$ is the graph whose vertex set is the set of all elements of $\mathbb{Z}_n^d$. Two vertices in $H(d, n)$ are adjacent if and only if they differ in exactly one coordinate. If $n = 2$, then we say the graph is a binary Hamming graph. The first family of graphs discovered to admit uniform mixing were the binary Hamming graphs [40]. Subsequent work considers variations of binary Hamming graphs ([7], [24], [18]). In this thesis we focus on quotients of Hamming graphs. The following new result is due to the author, and it is an extension of the work of [7].

Theorem 8.3.7. *Let Γ denote a subgroup of $\mathbb{Z}_2^d$ such that every pair of elements in Γ differs in at least three coordinates. Further suppose that $|\Gamma| = 4$. The graph $H(d, 2)/\Gamma$ admits uniform mixing at time $t = \pi/4$ if and only if $\Gamma = \langle v_1, v_2 \rangle$ for some v_1, v_2 in $\mathbb{Z}_2^d$ such that one of the following holds:*

(i) $wt(v_1) \equiv wt(v_2) \pmod 4$ *and* $wt(v_1 + v_2) \equiv 2 \pmod 4$

(ii) $wt(v_1) \equiv wt(v_2) + 2 \pmod 4$ *and* $wt(v_1 + v_2) \equiv 0 \pmod 4$. □

We also consider Hamming graphs $H(d, n)$ for $n \geq 3$. Aside from the Hamming graphs themselves, the mixing properties of these graphs have not been studied before. We completely characterize quotients of $H(d, 3)$ and $H(d, 4)$ that admit uniform mixing at times $t = 2\pi/9$ and $t = \pi/4$, respectively. As a consequence, we obtain infinite families of graphs that admit uniform mixing. Two particular families are given in the pair of following results. Both of these results are new and due to the author.

Theorem 8.4.4. *Let $d \geq 3$. The folded Hamming graph over $H(d, 3)/\langle \mathbf{1} \rangle$ admits uniform mixing at $t = 2\pi/9$ if and only if $d \equiv 1, 2 \pmod 3$.* □

Theorem 8.5.5. *Let $d \geq 3$. The folded Hamming graph $H(d, 4)/\langle \mathbf{1} \rangle$ admits uniform mixing at $t = \pi/4$ if and only if d is odd.* □

1.2 Graph Theory Tools

There are standard graph theory tools that we utilize throughout this thesis. In this section, we briefly recall some of the background results that we assume in our work. If we do not explicitly mention otherwise, the graphs we are considering in this thesis are simple and undirected. A *multigraph* is a graph that possibly has multiple edges between certain pairs of vertices and loops. Let $X = (V, E)$ denote a graph on n vertices. If each vertex of X has k neighbours, then we say that X is *k-regular* or that X has valency k. We let K_n denote the *complete graph* on n vertices. This is a graph on n vertices such that every pair of vertices is adjacent. The *adjacency matrix* A of X is an $n \times n$ matrix indexed by elements of V such that

$$A_{u,v} = \begin{cases} 1 & \text{if } u \text{ is adjacent to } v \\ 0 & \text{otherwise} \end{cases}$$

for each pair of u and v in V. Since X is undirected, we see that A is symmetric.

Theorem 1.2.1. *Every real symmetric matrix is diagonalizable.* □

This result implies that the adjacency matrix of X has n eigenvalues. We often refer to the eigenvalues of the adjacency matrix simply as the eigenvalues of the graph.

Corollary 1.2.2. *The sum of the eigenvalues of a graph, with multiplicity, is* 0. □

In addition to these basic linear algebra tools, we also utilize group theory tools. For two graphs $X = (V_1, E_1)$ and $Y = (V_2, E_2)$, we say that X is *isomorphic* to Y if there exists a bijection from V_1 to V_2 such that

$$\{u, v\} \in E_1 \iff \{\phi(u), \phi(v)\} \in E_2,$$

for all vertices u and v in V_1. An isomorphism from X to itself is called an *automorphism*, and the set of all isomorphisms forms a group, which we denote by $\mathrm{Aut}(X)$. If the automorphism group of a graph acts transitively on its vertices, then we say the graph is *vertex transitive*. If the automorphism group of a graph acts transitively on the arcs of the graphs, then we say the graph is *arc transitive*. And finally, if a graph is isomorphic to its complement, then we say the graph is *self-complementary*.

Chapter 2

Association Schemes

2.1 Introduction

Association schemes provide a framework to study a wide range of combinatorial problems, including graph theory and coding theory. For practical purposes, association schemes provide a convenient unifying language for the different tools used in this thesis. In a deeper sense, the underlying structure of the association schemes enables us to use such a diverse range of tools.

Association schemes were first studied by Bose and others in the realm of design theory. In 1973 Delsarte recognized that association schemes were a unifying object underlying coding theory and design theory. Delsarte's PhD thesis [23] led to association schemes being regarded as one of the foundations of combinatorics.

This chapter provides useful background material concerning the structure of association schemes. We begin by introducing Cayley graphs, which serve as useful building blocks of association schemes. Then we investigate the association schemes with two classes. The non-trivial examples of such schemes are called strongly regular graphs. Next we formally introduce general association schemes. Finally, we investigate several important examples — namely Hamming schemes and cyclic schemes. We pay particular attention to the inherent duality of cyclic association schemes.

The results in this chapter are not new, but they are essential to establishing our algebraic viewpoint. The association scheme notation introduced in this chapter will be used throughout the rest of the thesis, and the examples we see will be essential to our subsequent work.

2.2 Cayley Graphs

We start by introducing Cayley graphs. For our purposes, Cayley graphs are a tool for using the structure of a finite group to construct a graph. We use them as the building blocks of certain association schemes. We follow the treatment given in Godsil and Royle [31].

Definition 2.2.1. *Let G denote a group, and let C denote an inverse-closed subset of G. The $X(G, C)$ is a graph whose vertex set is identified with the elements of G. Two vertices u and v in G are adjacent if and only if*

$$vu^{-1} \in C.$$

From the definition, we see that every Cayley graph must be regular. In fact, every Cayley graph has a transitive group of automorphisms. We call such graphs *vertex-transitive*.

Lemma 2.2.2. *Cayley graphs are vertex transitive.*

Proof. Let X denote the Cayley graph $X(G, C)$. The group G acts regularly on the vertices of X as

$$\theta_g : x \to xg.$$

It is straightforward to verify that G is a subgroup of the automorphism group of X. Therefore X is vertex transitive. □

Conversely, a result due to Sabidussi implies that every graph with a regular automorphism group acting on it is a Cayley graph for that group [44]. Next we focus on some examples of Cayley graphs. First we see that cycles are Cayley graphs.

(2.2.3) *Let C_n denote a cycle of length n, and let $\mathbb{Z}_n$ denote the integers modulo a positive n. The cycle C_n is a Cayley graph over $\mathbb{Z}_n$, and in particular*

$$C_n \cong X(\mathbb{Z}_n, \{-1, 1\}).$$

Now we consider a slightly more complicated family of Cayley graphs: the Paley graphs. Let q denote a prime power, and let $\mathbb{F}_q$ denote the finite field of order q. Further let ω denote a multiplicative generator of $\mathbb{F}_q^*$. Recall that $\mathbb{F}_q^*$ is a cyclic group for all q. The set of nonzero squares of $\mathbb{F}_q$ is the multiplicative subgroup generated by ω^2. In terms of ω we note that

$$-1 = \omega^{(q-1)/2}.$$

This implies that -1 is a square if and only if $q \equiv 1 \pmod 4$, and equivalently S is closed under multiplication by -1 if and only if $q \equiv 1 \pmod 4$. This leads to the following definition. Suppose that q is a prime power such that $q \equiv 1 \pmod 4$, the *Paley graph* of order q is the Cayley graph $X(\mathbb{F}_q^+, S)$, where S denotes the set of nonzero squares. We let P_q denote the Paley graph of order q. As an explicit example, we consider the Paley graph of order five. The nonzero squares of $\mathbb{F}_5$ are $\{-1, 1\}$, and so we have

$$P_5 \cong C_5.$$

Since the Paley graphs are Cayley graphs, by Lemma 2.2.2 we know that Paley graphs are vertex transitive. In fact, the Paley graphs possess additional symmetry properties: the Paley graphs are arc-transitive and self-complementary.

Suppose X is an arc-transitive graph. All pairs of adjacent vertices in X must have a constant number of common neighbours. Likewise all pairs of adjacent vertices must have a constant number of common non-neighbours. Since Paley graphs are self-complementary, the automorphism group of P_q acts transitively on the ordered pairs of vertices that are not adjacent to each other. Therefore all pairs of non-adjacent vertices must have a constant number of common neighbours and common non-neighbours. Graphs with these extra regularity conditions are called strongly regular. We investigate these graphs in more detail in the next section.

2.3 Strongly Regular Graphs

Strongly regular graphs are an important family of graphs. Aside from the Paley graphs, other famous strongly regular graphs include the Petersen graph and line graphs of $K_{n,n}$. In this section, we formally introduce strongly regular graphs and determine their spectrum. We emphasize the connection between the algebraic properties of the adjacency matrix and the combinatorial properties of the graph. These properties are shared with the more general family of association schemes. Strongly regular graphs are a well-studied class of graphs and there is a wealth of knowledge about them that extends far beyond what is included in this thesis. See Cameron's survey [14] or Brouwer and Haemer's book [11], for example.

Definition 2.3.1. *A graph X of order n is strongly regular if it is not complete or edgeless and there exist constants k, a and c such that:*

(i) X is k-regular;

(ii) Every pair of adjacent vertices has a common neighbours;

(iii) Every pair of nonadjacent vertices has c common neighbours.

We express the parameters of a strongly regular graph with the array (n, k, a, c). For example, the cycle of length five has parameter set $(5, 2, 0, 1)$, and the Petersen graph has parameter set $(10, 3, 0, 1)$.

Suppose that X is a strongly regular graph with parameters (n, k, a, c) and adjacency matrix A. Further let $\overline{X}$ denote the complement of X, and let $\bar{A}$ denote the adjacency matrix of $\overline{X}$. Counting the common non-neighbours of pairs of vertices shows that $\overline{X}$ is also strongly regular with parameters

$$(n, n-k-1, n-2k+c-2, n-2k+a).$$

In terms of A, we can express $\bar{A}$ as

$$\bar{A} = J - I - A, \tag{2.1}$$

where I is the identity matrix, and J is the all-ones matrix.

Recall that the (u, w)-entry of A^2 is equal to the number of walks of length two from vertex u to vertex w in X. Combining this observation with Equation 2.1 enables us to express A^2 as

$$\begin{aligned} A^2 &= aA + c\bar{A} + kI \\ &= aA + c(J - A - I) + kI \\ &= (a-c)A + (k-c)I + cJ. \end{aligned}$$

Any strongly regular graph with parameters (n, k, a, c) satisfies the equation above. The converse also holds, as we see in the next well-known result. A proof of this result appears in [31], for example.

Lemma 2.3.2. *A graph X is strongly regular with parameters (n, k, a, c) if and only if its adjacency matrix A satisfies*

$$A^2 - (a-c)A - (k-c)I = cJ. \qquad \square$$

Note that Lemma 2.3.2 can be taken as an algebraic definition of strongly regular graphs. It is also useful to note that we compute the following matrix products:

$$\begin{aligned} A^2 &= kI + aA + c\bar{A} \\ \bar{A}^2 &= (n-k-1)I + (n-2k+c-2)A + (n-2k+a)\bar{A} \end{aligned}$$

$$\bar{A}A = (J - A - I)A = (k - a - 1)A + (k - c)\bar{A} = A\bar{A}.$$

Now we shift our focus to the spectral properties of strongly regular graphs. If X is a regular and connected graph, then the all-ones vector is a simple eigenvector of X with eigenvalue k. Building from this, we completely determine the spectrum of X in terms of its parameters. The following result is well-known. A proof is given in Godsil and Royle [31]. For completeness, we include a proof here.

Lemma 2.3.3. *Let X denote a connected strongly regular graph with parameters (n, k, a, c). The nontrivial eigenvalues of X are given by*

$$\theta, \tau = \frac{1}{2}\left(a - c \pm \sqrt{(a-c)^2 + 4(k-c)}\right).$$

For notational convenience, we assume $\theta > \tau$. The multiplicities of these eigenvalues are

$$m_\theta = \frac{1}{2}\left(n - 1 - \frac{(n-1)(a-c) + 2k}{\sqrt{(a-c)^2 + 4(k-c)}}\right)$$
$$m_\tau = \frac{1}{2}\left(n - 1 + \frac{(n-1)(a-c) + 2k}{\sqrt{(a-c)^2 + 4(k-c)}}\right).$$

Proof. Suppose that v is an eigenvector of A corresponding to a nontrivial eigenvalue θ. Then $\mathbf{1}^T v = 0$, and so

$$\left(A^2 - (a-c)A - (k-c)I\right) v = \left(\theta^2 - (a-c)\theta - (k-c)\right) v = 0.$$

This implies that θ is a root of

$$x^2 - (a-c)x - (k-c) = 0.$$

We solve this equation using the quadratic formula, and we assume that θ and τ are the two roots with $\theta \geq \tau$. Let m_θ and m_τ denote the multiplicities of θ and τ, respectively. Since the trace of A is zero, we know that the sum of the eigenvalues with multiplicity is equal to zero. Therefore the multiplicities satisfy

$$1 + m_\theta + m_\tau = n$$
$$k + m_\theta \theta + m_\tau \tau = 0.$$

We solve this system directly to determine m_θ and m_τ in terms of θ and τ, and then we substitute our expression of θ and τ in terms of the strongly regular graph parameters to obtain our desired result. □

Of course, the multiplicities of the eigenvalues of a graph must be positive integers, and so our expression for m_τ and m_θ in Lemma 2.3.3 implies that either $(a-c)^2+4(k-c)$ is a square or $(n-1)(a-c)=-2k$. These two cases imply that either θ and τ are integers or $m_\tau = m_\theta$. (We note that both cases could occur simultaneously.) A strongly regular graph with $m_\tau = m_\theta$ is called a *conference graph*.

Let X denote a strongly regular graph. Now that we know the spectrum of X, we determine the spectrum of its complement $\overline{X}$. Suppose that $\overline{X}$ is also connected. Then the all-ones vector is an eigenvector of $\overline{X}$ with simple eigenvalue $n-k-1$, which is the valency of $\overline{X}$. The other eigenvalues can be deduced from Equation 2.1. If v is an eigenvector of X with the nontrivial eigenvalue θ, then $\mathbf{1}^T v = 0$ and

$$\bar{A}v = (J - A - I)\,v = -Av - v = (-\theta - 1)v.$$

This implies that $-1-\theta$ is an eigenvalue with multiplicity m_θ of $\overline{X}$. Similarly, we see that $-1-\tau$ is an eigenvalue with multiplicity m_τ of $\overline{X}$. We highlight the fact that X and $\overline{X}$ share the same eigenspaces. This is the key property of association schemes, which we will see in the next section.

2.4 Association Schemes

Recall that a strongly regular graph X on n vertices and its complement partition the edges of K_n in such a way that they share the same eigenspaces. We wish to generalize this desirable algebraic property. Suppose that we have an edge decomposition of K_n into d graphs $\{X_1, \ldots, X_d\}$. Let A_r denote the adjacency matrix of X_r for $1 \le r \le d$, and let $A_0 = I$, the $n \times n$ identity matrix. Further let $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$. Since the graphs partition the edges set of the complete graph, we note that

$$\sum_{r=0}^{d} A_r = J,$$

where J is the $n \times n$ all-ones matrix.

Definition 2.4.1. *The matrices in $\mathcal{A}$ form a symmetric d-class* association scheme *if and only if there exist constants $p_{j,k}(r)$ for $0 \le j,k,r \le d$ such that*

$$A_j A_k = \sum_r p_{j,k}(r) A_r.$$

The constants $p_{j,k}(r)$ are called *intersection parameters*. Combinatorially, the intersection parameters $p_{j,k}(r)$ exist if and only if for every edge $\{x, y\}$ in X_r there are a constant number of vertices z such that $\{x, z\}$ is an edge of X_j and $\{z, y\}$ is an edge of X_k. In particular, their existence implies every graph X_j in the scheme is regular with valency $p_{j,j}(0)$. For convenience, we let n_j denote the valency $p_{j,j}(0)$.

As a point of notation, we refer to the graphs $\{X_1, \ldots, X_d\}$ as an association scheme if their adjacency matrices, together with the identity matrix, form an association scheme as defined above.

From the definition of a strongly regular graph, we see that if A is the adjacency matrix of a strongly regular graph, then $\mathcal{A} = \{I, A, \bar{A}\}$ is an association scheme.

We offer another important family of association schemes. Suppose that $X = (V, E)$ is a connected graph. For any two vertices u and v in V, let $\operatorname{dist}(u, v)$ denote the length of the shortest path in X between u and v. A *distance-regular graph* is a regular graph such that the number of common neighbours of u and v is determined by the distance $\operatorname{dist}(u, v)$ between u and v. For example, every strongly regular graph is a distance-regular graph with diameter two. The cycle graphs are also distance-regular graphs. Refer to [10] for more information about distance-regular graphs.

Let X denote a distance-regular graph with diameter d, and let $A_0, \ldots, A_d$ denote the $(0, 1)$-matrices indexed by vertices of X such that

$$(A_j)_{u,v} = \begin{cases} 1 & \text{if } \operatorname{dist}(u, v) = j \\ 0 & \text{otherwise.} \end{cases}$$

It is useful to note that the matrices $\{A_0, A_1, \ldots, A_d\}$ form an association scheme.

2.5 Bose-Mesner Algebra

Let $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$ denote an association scheme. From an algebraic viewpoint, the existence of the intersection parameters guarantees that the real vector space spanned by $\{A_0, \ldots, A_d\}$ is closed under multiplication and multiplication among elements in the vector space is commutative. Hence $\mathbb{C}[\mathcal{A}]$ is a commutative algebra of dimension $d + 1$. We refer to $\mathbb{C}[\mathcal{A}]$ as the *Bose-Mesner algebra* of the scheme. Bose and Mesner [9] introduced what is now called the Bose-Mesner algebra of an association scheme.

Suppose that A and B are two $m \times n$ matrices. The *Schur product* $A \circ B$ is the $m \times n$ matrix given by

$$(A \circ B)_{j,k} = A_{j,k} B_{j,k}.$$

Since the matrices in $\mathcal{A}$ are adjacency matrices of edge-disjoint graphs, we see that

$$A_j \circ A_k = \delta_{j,k} A_j,$$

where $\delta_{j,k}$ is the Kronecker delta. Let $\mathcal{A}$ denote a d-class association scheme. The matrices in $\mathcal{A}$ are idempotents under Schur multiplication. Since $\mathbb{C}[\mathcal{A}]$ is spanned by $\mathcal{A}$, we see that the entire Bose-Mesner algebra is closed under Shur multiplication. Furthermore, each matrix in $\mathcal{A}$ is a real symmetric matrix, and so the spectral decomposition theorem of linear algebra ensures that each matrix A_i is individually diagonalizable. The additional properties of an association scheme guarantees that the matrices in $\mathcal{A}$ are simultaneously diagonalizable. Therefore it is possible to decompose $\mathbb{R}^n$ into $d+1$ pairwise orthogonal common eigenspaces. Refer to Godsil [28] for further details on these observations.

For a d-class association scheme, we let $\{E_0, E_1, \ldots, E_d\}$ denote the projections onto the common eigenspaces of $\mathbb{R}^n$. We refer to these matrices as the *spectral idempotents* of the scheme. For notational convenience, we always assume that $E_0 = \frac{1}{n}J$ is the projection onto $\mathbb{R}\mathbf{1}$. We define the eigenvalues of the scheme to be the constants $p_j(k)$ for $0 \leq j, k \leq d$ such that

$$A_j E_k = p_j(k) E_k.$$

The $d+1$ spectral idempotents form a basis of $\mathbb{C}[\mathcal{A}]$. See Chapter 12 of [28] for the proof of this observation. For this reason, we often refer to the spectral idempotents as the *dual basis* of the scheme. Since the Bose-Mesner algebra is closed under Schur multiplication, there exists coordinates $q_j(k)$ in $\mathbb{R}$ for $0 \leq j, k \leq d$ such that

$$A_j \circ E_j = \frac{1}{n} q_j(k) A_k.$$

These coordinates $q_j(k)$ are called the *dual eigenvalues* of the association scheme. Let P and Q denote $(d+1) \times (d+1)$ matrices such that

$$P_{j,k} = p_k(j) \quad \text{and} \quad Q_{j,k} = q_k(j).$$

Note that P is the change of basis matrix from $\mathcal{A}$ to the dual basis, and $\frac{1}{n}Q$ is the inverse of P. 9 There are a couple useful tricks for relating Shur multiplication and regular multiplication in the Bose-Mesner algebra. For a matrix M, let $\mathrm{sum}(M)$ denote the sum of each entry of M. First note that for two square matrices A and B, we have

$$\mathrm{sum}(A \circ B) = \mathrm{tr}(AB^T).$$

For notational convenience, we let m_j denote the multiplicity of the eigenvalue corresponding to E_j. Since the trace of a matrix is invariant under conjugation, we have that $m_j = \mathrm{tr}(E_j)$. Using these two observations, we directly relate the eigenvalues and dual eigenvalues of the scheme.

Lemma 2.5.1. *The eigenvalues and dual eigenvalues of the scheme satisfy*

$$q_k(j) = \frac{m_k}{n_j} p_j(k).$$

Proof. From the definition of the eigenvalues of the scheme, we have

$$A_j E_k = p_j(k) E_k. \tag{2.2}$$

Taking the trace of both sides of this equality we obtain

$$\mathrm{tr}(A_j E_k) = p_j(k)\mathrm{tr}(E_k) = p_j(k) m_k.$$

Alternatively, we derive the following expression for $\mathrm{tr}(A_j E_k)$ in terms of the dual eigenvalues:

$$\begin{aligned} \mathrm{tr}(A_j E_k) &= \mathrm{sum}(A_j \circ E_k) \\ &= \frac{q_k(j)}{n} \mathrm{sum}\left(A_j\right) \\ &= q_k(j) n_j. \end{aligned}$$

Substituting this back into Equation 2.2 gives us our desired expression. □

2.6 Krein Parameters

In this section we introduce additional association scheme parameters. Once again we rely on the fact that the spectral idempotents $\{E_0, E_1, \ldots, E_d\}$ form a basis of the Bose-Mesner algebra $\mathbb{C}[\mathcal{A}]$. Since $\mathbb{C}[\mathcal{A}]$ is closed under Schur multiplication, there exist coordinates $q_{i,j}(k)$ for $0 \leq j, k, r \leq d$ such that

$$E_j \circ E_k = \frac{1}{n} \sum_{r=0}^{d} q_{j,k}(r) E_r.$$

The coordinates $q_{j,k}(r)$ are called the *Krein parameters* of the scheme. They are dual to the intersection parameters. Certain trivial Krein parameters are easy to compute. The following is well-known. A proof is given in [28], for example.

Lemma 2.6.1. *The Krein parameters of any association scheme satisfy the following:*

(i) $q_{j,k}(r) = q_{k,j}(r)$*;*

(ii) $q_{j,0}(r) = \delta_{j,r}$*;*

(iii) $q_{j,k}(0) = \delta_{j,k} m_j$*.*

Proof. Shur multiplication is commutative, which implies (i). Since $E_0 = \frac{1}{n}J$, we see that

$$E_j \circ E_0 = \frac{1}{n}E_j.$$

This proves (ii). Next observe that since the columns and rows of $E_1, \dots, E_d$ are orthogonal to $\mathbf{1}$, we have

$$q_{j,k}(0) = \mathbf{1}^T \left(E_j \circ E_k\right) \mathbf{1}.$$

But we also have

$$\mathbf{1}^T \left(E_j \circ E_k\right) \mathbf{1} = \operatorname{sum}(E_j \circ E_k) = \operatorname{tr}(E_j E_k) = \delta_{i,j} m_j,$$

which proves (iii). □

General Krein parameters are more complicated to compute. However, if the eigenvalues of the scheme are known, then we can use the following result to determine the Krein parameters. This result is well-known.

Lemma 2.6.2. *Let $\mathcal{A}$ denote a d-class association scheme with eigenvalues $p_j(r)$ for $0 \leq j, r \leq d$. The Krein parameters of a d-class association scheme are given by*

$$q_{j,k}(r) = \frac{m_j m_k}{n} \sum_{s=0}^{d} \frac{p_s(j) p_s(k) p_s(r)}{n_s^2}.$$

Proof. We begin by noting that

$$\frac{1}{n} q_{j,k}(r) E_r = E_r \left(E_j \circ E_k\right).$$

Taking the trace of both sides of this equation yields

$$\begin{aligned}\frac{1}{n}q_{j,k}(r)m_r &= \text{sum}\,(E_r \circ E_j \circ E_k)\\ &= \frac{1}{n^3}\sum_{l=0}^{d} q_r(l)q_j(l)q_k(l)\text{sum}\,(A_l)\\ &= \frac{1}{n^2}\sum_{l=0}^{d} q_r(l)q_j(l)q_k(l)n_l.\end{aligned}$$

This implies that the Krein parameters can be written in terms of the dual eigenvalues as

$$q_{j,k}(r) = \frac{1}{nm_r}\sum_{l=0}^{d} q_r(l)q_j(l)q_k(l)n_l.$$

Now recalling Lemma 2.5.1, we can rewrite this expression for $q_{j,k}(r)$ in terms of the eigenvalues of the scheme as

$$q_{j,k}(r) = \frac{m_j m_k}{n}\sum_{l=0}^{d}\frac{p_l(r)p_l(j)p_l(k)}{n_l^2}. \qquad \square$$

The Krein parameters can be shown to be the eigenvalues of a positive semi-definite matrix, and therefore they are nonnegative. This provides a feasibility test for potential parameters of an association scheme. It is also useful to note that in special cases, the Krein parameters coincide with the intersection parameters. An association scheme is *formally self-dual* if

$$p_j(k) = q_j(k)$$

for $1 \leq j, k \leq d$ for some ordering of the basis matrices $\mathcal{A}$ and the spectral idempotents. In the following sections, we introduce the Hamming schemes and cyclic schemes, both of which have this property.

2.7 Hamming Schemes

In this section we investigate the Hamming schemes. They provide an in-depth illustration of an association scheme, and they are also important in our later work. For more information about Hamming schemes, see [15] and [28].

We begin by introducing some coding theory terminology. Let Q be an alphabet with n symbols, and let u and v be two words of length d. The

Hamming distance $\text{dist}(u, v)$ between two words u and v is the number of coordinates in which they differ. For example, if $Q = \{0, 1\}$, then

$$\text{dist}(0001, 1011) = 2.$$

Suppose that S is a subset of all possible words of length d. We say that S has *minimum Hamming distance* t, if the distance between any two words in S is at least t.

The *Hamming graph* $H(d, n)$ is the graph whose vertex set is the set of all words of length d. Two words in $H(d, n)$ are adjacent if and only if they differ in exactly one coordinate. If $n = 2$, then we say the graph is a *d-cube*. The family of d-cubes are also referred to as *hypercubes* or *binary Hamming graphs*. For example, $H(2, 2)$ is isomorphic to C_4, and $H(3, 2)$ is isomorphic to the classic cube on eight vertices. More generally, $H(2, n)$ is isomorphic to the line graph $L(K_{n,n})$.

In practice, it is convenient to assume that $Q = \mathbb{Z}_n$. This endows our set of words with natural addition and subtraction operations. The Hamming graph $H(d, n)$ is a Cayley graph over $\mathbb{Z}_n^d$ with scalar multiples of the standard basis vectors $e_1, \dots, e_d$ as its connection set. We define the *Hamming weight* $\text{wt}(v)$ of an element in $\mathbb{Z}_n^d$ to be the number of nonzero coordinates of v. The Hamming distance can be rephrased in terms of the Hamming weight as

$$\text{dist}(u, v) = \text{wt}(u - v).$$

Often it is useful to keep track of the indices of the nonzero coordinates of an element of $\mathbb{Z}_n^d$. For a vector u in $\mathbb{Z}_n^d$, we let $\text{supp}(u)$ denote the set of indices of nonzero coordinates of u. For example,

$$\text{supp}((1, 2, 2, 0, 0)) = \{1, 2, 3\}.$$

With all of this notation under our belt, we are ready to define the *Hamming scheme* $\mathcal{H}(d, n)$. The vertices of $\mathcal{H}(d, n)$ are the elements of $\mathbb{Z}_n^d$. The matrices of our scheme are the $d + 1$ matrices $\{A_0, A_1, \dots, A_d\}$ whose rows and columns are each indexed by $\mathbb{Z}_n^d$ such that

$$(A_j)_{u,v} = \begin{cases} 1 & \text{if } \text{dist}(u, v) = j \\ 0 & \text{otherwise} \end{cases}.$$

Note that $A_0 = I$. If we restrict our consideration to the case when $n = 2$, then A_1 is the adjacency matrix of the d-cube. The eigenvalues of A_1 are the integers

$$d - 2i, \quad i = 0, ..., d$$

with respective multiplicities given by $\binom{d}{i}$.

There are two other important association schemes that can be derived from binary Hamming graphs. First we consider the graph X_2 whose adjacency matrix is A_2 in the Hamming scheme $\mathcal{H}(d, 2)$. Note that two vertices in A_2 are adjacent if and only if the corresponding elements of $\mathbb{Z}_2^d$ are at Hamming distance two from each other. Since the Hamming graph $H(d, 2)$ is bipartite, we see that X_2 has two connected components. The *halved d-cube* is the subgraph of X_2 induced by the elements of $\mathbb{Z}_2^d$ with even Hamming weight. This graph is distance-regular, and therefore the distance matrices of the graph form an association scheme.

Our second association scheme is derived from the so-called *folded d-cube*. The folded d-cube is the graph obtained from $H(d, 2)$ by adding edges between vertices at distance d. The folded d-cube is also a distance-regular graph. Thus the distance matrices of the folded d-cube form an association scheme.

2.8 Cyclic Schemes

In this section we consider the cyclic association schemes. These schemes arise naturally from the distance partition of the cycle graphs. We begin by introducing the cyclic schemes and their parameters. One of our key observations is that every matrix in the Bose-Mesner algebra of the association scheme can be expressed as a complex polynomial in C, where C is the adjacency matrix of a directed cycle of order n. The results in this section are not new. However, the setup and viewpoint we develop in this section is critical to our subsequent original results about continuous-time quantum walks on cycles.

We fix an arbitrary positive integer n such that $n \geq 3$. Recall that the cycle of length n, denoted C_n, is a Cayley graph over $\mathbb{Z}_n$ with connection set $\{1, n-1\}$. Let $d = \lfloor \frac{n}{2} \rfloor$. For $0 \leq r \leq d$ we define the following adjacency matrices.

$$[A_r]_{j,k} = \begin{cases} 1 & \text{if } \ j-k \in \{r, -r\} \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

Note that A_0 is the $n \times n$ identity matrix, and A_1 is the adjacency matrix of the cycle C_n. Let $\mathcal{A} = \{A_0, \ldots, A_d\}$. The set of matrices $\mathcal{A} = \{A_0, \ldots, A_d\}$ form the *cyclic association scheme* of order n.

First we show that $\mathcal{A}$ is an association scheme. To do this, it is best to consider a particular underlying permutation matrix C that is the adjacency matrix of a directed cycle. We index the rows and columns of C with elements of $\mathbb{Z}_n$ such that

$$C_{j,k} = \begin{cases} 1 & \text{if } j - k = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Let $e_1, \dots, e_n$ denote the standard basis of $\mathbb{C}^n$ such that each subscript is identified with an element of $\mathbb{Z}_n$. Then we have

$$Ce_j = e_{j+1},$$

where the indices are computed in $\mathbb{Z}_n$. This implies that every cyclic matrix of order n can be expressed as a polynomial in C. In particular, we see that $C^n = I$ and each matrix in $\mathcal{A}$ can be expressed as polynomial in C as

$$A_j = \begin{cases} C^j + C^{-j} & \text{if } j \notin \{0, n/2\} \\ \frac{1}{2}(C^j + C^{-j}) & \text{if } j \in \{0, n/2\}. \end{cases}$$

With this in mind, we verify that $\mathcal{A}$ satisfies the definition of an association scheme. Our definition of the matrices in $\mathcal{A}$ implies that

$$\sum_{r=0}^{d} A_r = J,$$

where J is the $n \times n$ all-ones matrix. Consider two matrices A_j and A_k in $\mathcal{A}$ such that $j, k \notin \{0, n/2\}$. We note that

$$\begin{aligned} A_j A_k &= \left(C^j + C^{-j}\right)\left(C^k + C^{-k}\right) &(2.3)\\ &= C^{j+k} + C^{-j+k} + C^{j-k} + C^{-j-k} &(2.4)\\ &= A_{j+k} + A_{j-k}, &(2.5) \end{aligned}$$

where the indices are computed in $\mathbb{Z}_n$ and A_r is identified with A_{n-r} for all $1 \leq r \leq n-1$. Also note that if $j \in \{0, n/2\}$, then $A_j A_k = A_{j+k}$ for $1 \leq k \leq d$. This confirms that $\mathcal{A}$ is an association scheme.

Our work above sheds light on a couple of important properties of the cyclic association scheme $\mathcal{A}$. First, we explicitly see that the intersection numbers of the scheme are given by

$$p_{j,k}(r) = \begin{cases} 1 & \text{if } j - k = \pm r \text{ or } j + k = \pm r \\ 0 & \text{otherwise.} \end{cases}$$

Second, we see that each matrix in the Bose-Mesner algebra $\mathbb{C}[\mathcal{A}]$ can be expressed as a complex polynomial in C.

Lemma 2.8.1. *For every matrix M in $\mathbb{C}[\mathcal{A}]$, there exists a unique polynomial $p(x)$ in $\mathbb{C}[x]$ with degree at most $n-1$ such that*

$$M = p(C). \qquad \square$$

Now we consider the eigenvalues of the cyclic scheme $\mathcal{A}$. Let ω denote the primitive n-th root of unity given by

$$\omega = e^{2\pi i/n}.$$

For $1 \leq r < \lfloor n/2 \rfloor$, let E_r denote the matrix given by

$$E_r = \sum_{j=0}^{n-1} \left(\omega^{jr} + \omega^{-jr}\right) C^j. \tag{2.6}$$

Otherwise, if $r = 0$ or $r = n/2$, then we let E_r denote the matrix given by

$$E_r = \frac{1}{n} \sum_{j=0}^{n-1} \omega^{jr} C^j. \tag{2.7}$$

For the matrices in our association scheme $\mathcal{A}$, we see that

$$\begin{aligned} A_j E_r &= \left(C^j + C^{-j}\right) E_r \\ &= \left(\omega^{jr} + \omega^{(-jr}\right) E_r \\ &= \left(\omega^{jr} + \omega^{-jr}\right) E_r. \end{aligned}$$

Therefore we see that the columns of E_r are eigenvectors of $\mathcal{A}$ with the same eigenvalues. For a matrix M, let M^* denote the conjugate transpose of M. With this notation we have that

$$E_r^* E_r = \begin{cases} I & \text{if } \ j = k \\ 0 & \text{otherwise.} \end{cases}$$

As desired, we note that $E_0 = \frac{1}{n} J$. Using the properties of these eigenvectors, we further note that

$$E_r^2 = E_r \quad \text{and} \quad A_j E_r = \left(\omega^{jr} + \omega^{-jr}\right) E_r.$$

Therefore each E_r is a projection onto an eigenspace of $\mathcal{A}$. In particular, the explicit eigenvalues of the cyclic scheme are

$$p_j(r) = \omega^{jr} + \omega^{-jr}.$$

If n is odd, then each of the nontrivial eigenvalues has multiplicity 2. However, if n is even, then both E_0 and E_d are projections onto one-dimensional eigenspaces.

As an aside, we note that each additive character on $\mathbb{Z}_n$ gives rise to an orthogonal idempotent. In general, it is well-known that for a Cayley graph over a finite abelian group G, the additive characters will give rise to $|G|$ pairwise orthogonal eigenvectors.

Cyclic schemes are distance-regular. Moreover, a cyclic scheme of odd order has the interesting property that each of its nontrivial eigenspaces has the same dimension. Association schemes with this property are called *pseudocyclic schemes*. The cyclic schemes of odd order are the only schemes that are both distance-regular and pseudocyclic [51]. In the next section we shift our focus to duality properties of cyclic schemes.

2.9 Cyclic Duality

In this section, we consider the discrete Fourier transform on the Bose-Mesner algebra of the cyclic association scheme. This duality map will be crucial to our later work with continuous-time quantum walks on cycles. The work in this section is not original. We closely follow the approach used in Godsil's unpublished notes.

Throughout this section, let $\mathcal{A}$ denote the cyclic association scheme on n vertices, and let $d = \lfloor n/2 \rfloor$. Recall that the Bose-Mesner algebra $\mathbb{C}[\mathcal{A}]$ is the set of all complex symmetric circulant matrices of order n. As we saw in the previous section, each matrix in $\mathbb{C}[\mathcal{A}]$ can be expressed as complex polynomial of the form $p(C)$, where C is the adjacency matrix of a directed cycle of order n. Let ω denote a primitive n-th root of unity. For simplicity, we assume that

$$\omega = e^{2\pi i/n}.$$

This assumption is for computational convenience. In practice, any primitive n-th root of unity will work. Now we consider an arbitrary matrix M in $\mathbb{C}[\mathcal{A}]$. From our reasoning in the previous section, we know that there exists a unique polynomial $p(x)$ of degree at most $n-1$ in $\mathbb{C}[x]$ such that $M = p(C)$. The *discrete Fourier transform* Θ is defined such that

$$\Theta(M) = \sum_{j=0}^{n-1} p(\omega^j) C^j.$$

In particular, we see that map Θ is a linear operator of $\mathbb{C}[\mathcal{A}]$. We now investigate some more useful properties of our duality map Θ.

Lemma 2.9.1. *If M is in $\mathbb{C}[\mathcal{A}]$, then $\Theta^2(M) = nM$.*

Proof. Recall that there exists $p(x)$ in $\mathbb{C}[x]$ such that $p(C) = M$. We proceed by showing that

$$\Theta^2(C^k) = n\left(C^k\right)^T = nC^{-k}$$

for all $0 \le k \le d$. Since Θ is a linear map, this proves that $\Theta^2(M) = nM^T$, which implies our desired result when we restrict to the symmetric matrices in the Bose-Mesner algebra $\mathbb{C}[\mathcal{A}]$. To begin, we consider an arbitrary matrix of the form C^k. We compute the image of C^k under θ^2 to be

$$\begin{aligned}\Theta^2(C^k) &= \Theta\left(\sum_{j=0}^{n-1}\omega^{jk}C^j\right)\\ &= \sum_{j=0}^{n-1}\omega^{jk}\Theta\left(C^j\right)\\ &= \sum_{s=0}^{n-1}\left(\sum_{j=0}^{n-1}\omega^{j(k+s)}\right)C^s.\end{aligned}$$

Since ω is an n-th root of unity, we know that

$$\sum_{j=0}^{n-1}\omega^{j(k+s)} = \begin{cases} n & \text{if } k+s \equiv 0 \pmod{n} \\ 0 & \text{otherwise.}\end{cases}$$

Therefore we have $\Theta^2(C^k) = nC^{-k} = n\left(C^k\right)^T$. □

Next we consider the image of the spectral idempotents and Schur idempotents of the $\mathbb{C}[\mathcal{A}]$.

Lemma 2.9.2. *For each spectral idempotent $\{E_0, \ldots, E_d\}$ and Schur idempotent $\{A_0, \ldots, A_d\}$ of $\mathbb{C}[\mathcal{A}]$ we have*

$$\Theta(E_r) = A_r \quad \textit{and} \quad \Theta(A_r) = nE_r.$$

Proof. Suppose that $r \neq 0$. Using the expression for the spectral idempotents given in Equation 2.6, we compute that

$$\Theta(E_r) = \frac{1}{n}\sum_{k=0}^{n-1}\left(\sum_{j=0}^{n-1}\omega^{j(k+r)} + \omega^{j(k-r)}\right)C^k$$

$$= C^r + C^{-r} = A_r.$$

If $r = 0$, then similar reasoning gives us

$$\begin{aligned}\Theta(E_0) &= \frac{1}{n}\sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\omega^{jk}C^k \\ &= C^0 = A_0.\end{aligned}$$

Thus if $0 \leq r \leq d$ we have $\Theta(E_r) = A_r$. By Lemma 2.9.1, we know that $\Theta^2(E_r) = nE_r$, and so therefore $\Theta(A_r) = nE_r$. □

Finally, we see the connection between the duality map and Schur multiplication.

Lemma 2.9.3. *If M and N are two matrices in $\mathbb{C}[\mathcal{A}]$, then*

$$\Theta(MN) = \Theta(M) \circ \Theta(N) \quad \textit{and} \quad \Theta(M \circ N) = \frac{1}{n}\Theta(M)\Theta(N).$$

Proof. Let $f(x)$ and $g(x)$ denote polynomials in $\mathbb{C}[x]$ such that $M = f(C)$ and $N = g(C)$. First we compute the image of MN under the duality map to be

$$\begin{aligned}\Theta(MN) &= \sum_{j=0}^{n-1} f(\omega^j)g(\omega^j)C^j \\ &= \left(\sum_{j=0}^{n-1} f(\omega^j)C^j\right) \circ \left(\sum_{j=0}^{n-1} g(\omega^j)C^j\right) \\ &= \Theta(M) \circ \Theta(N).\end{aligned}$$

This proves the first claim. Now we consider the first equality applied to the matrices $\Theta(M)$ and $\Theta(N)$. Simplifying with Lemma 2.9.1 implies that

$$\begin{aligned}\Theta\left(\Theta(M)\Theta(N)\right) &= \Theta(\Theta(M)) \circ \Theta(\Theta(N)) \\ &= nM \circ nN = n^2(M \circ N).\end{aligned}$$

Next we take the image under Θ of both sides of the last equality. Another application of Lemma 2.9.1 gives us

$$n\Theta(M)\Theta(N) = n^2\Theta(M \circ N),$$

which is equivalent to the second claim. □

The following corollary will be useful in our later work. If we consider the special case when the Schur product of two matrices is a scalar multiple of the all-ones matrix.

Corollary 2.9.4. *If M and N are matrices in $\mathbb{C}[\mathcal{A}]$, then*

$$\Theta(M)\Theta(N) = nI \quad \textit{if and only if} \quad M \circ N = \frac{1}{n}J$$

where I and J are the $n \times n$ identity matrix and all-ones matrix, respectively.

Proof. By the second claim of that Lemma 2.9.3, we know that

$$\frac{1}{n}\Theta(M)\Theta(N) = \Theta(M \circ N). \tag{2.8}$$

Therefore $\Theta(M)\Theta(N) = nI$ if and only if

$$\Theta(M \circ N) = I. \tag{2.9}$$

Taking the image under Θ of both sides of Equation 2.9 and simplifying using Lemma 2.9.1 and Lemma 2.9.2 results in

$$M \circ N = \frac{1}{n}\Theta(I) = \frac{1}{n}J. \tag{2.10}$$

Conversely, assume that Equation 2.10 holds. If we take the image under Θ of both sides, then we see that Equation 2.9 must hold as well. □

We note that the results in this section generalize to all formally self-dual association schemes. For example, the Hamming schemes are also formally self-dual, and we can define a duality map with similar properties.

Chapter 3

Continuous-time Quantum Walks

3.1 Introduction

In recent years, quantum algorithms have become a popular area of mathematical research. Fahri and Gutmann [25] introduced the concept of a quantum walk in 1998. Following this, Childs et al. found a graph in which the continuous-time quantum walk spreads exponentially faster than any classical algorithm for a certain black-box problem [21]. Subsequently continuous-time quantum walks have been used in quantum search algorithms for other applications [43]. Recent work of Childs shows that the continuous-time quantum walk model is a universal computational model [20].

In this chapter, we introduce continuous-time quantum walks using algebraic language. We begin by defining the transition and mixing matrices associated with a continuous-time quantum walk. Next we explore various metrics associated with quantum walks. We pay close attention to the uniform mixing property. Following this, we investigate continuous-time quantum walks on complete graphs, and we see that the behaviour of a quantum walk contrasts starkly with the behaviour of a classical random walk. To conclude this chapter, in Section 3.6 we establish specific necessary and sufficient conditions for uniform mixing of a continuous-time quantum walk to occur on a graph in an association scheme.

Most of the results were previously known. The two exceptions are Theorem 3.5.3 and Theorem 3.6.1. Both of these results are due to the author. Much of our understanding of quantum walks comes from the surveys of Kempe [36] and Ambainis [4]. We follow the mathematical notation given in [29].

3.2 Transition Matrices

In this section, we introduce continuous-time quantum walks on graphs, and we explore some of the basic properties of the corresponding transition matrices. First we consider classical continuous random walks on graphs. Suppose that X is an undirected graph, and let A denote its adjacency matrix. A continuous random walk on X is determined by a family of matrices of the form $M(t)$, indexed by the vertices of X and parameterized by a real positive time t. In particular, the probability of starting at vertex u and reaching vertex v at time t is given by

$$M(t)_{u,v}.$$

Let Δ denote the diagonal matrix indexed by the vertices of X such that $\Delta_{u,u}$ denotes the degree of vertex u. We define a continuous random walk on X by setting

$$M(t) = \exp(t(A - \Delta)).$$

Each column of $M(t)$ corresponds to a probability density of a walk whose initial state is the vertex indexing that column. In particular, the entries of a column of $M(t)$ are nonnegative numbers that sum to one. Note that $\{M(t) : t \in \mathbb{R}\}$ is a multiplicative group isomorphic to $\mathbb{R}$.

Within the realm of quantum computing, Fahri and Gutmann [25] proposed an analogous *continuous quantum walk*. For a real symmetric matrix A, we define the transition operator of the walk to be

$$U(t) = \exp(itA).$$

For practical purposes, it is desirable that A is sparse. The entries of $U(t)$ will not necessarily be real. In this model, the probability densities of the walk are given by the columns of $U(t) \circ U(t)^*$. As we will see later, these are probability densities since each $U(t)$ is unitary. In this thesis, we consider the case when A is the adjacency matrix of a graph X. If X is regular, then this walk is equivalent, up to a phase factor, to a walk defined using the Laplacian of the same graph. For more information about continuous-time quantum walks, see [36] and [4].

For a graph X with adjacency matrix A, we say that $U(t) = \exp(itA)$ is the *transition matrix* of X. If the graph in question is unclear, we may use the notation $U_X(t)$ to denote the transition matrix of the graph X. For the rest of this section, we focus on the transition matrix of a continuous-time quantum walk. First we recall a well-known result about exponential functions. We provide a proof for completeness.

Lemma 3.2.1. *If M and N are a pair of commuting matrices, then*

$$\exp(M+N) = \exp(M)\exp(N).$$

Proof. Using the definition of the exponential function, we see that

$$\exp(M+N) = \sum_{k\geq 0} \frac{1}{k!}(M+N)^k.$$

Since M and N commute we can further simplify this expression to

$$\begin{aligned}\exp(M+N) &= \sum_{k\geq 0} \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} M^j N^{k-j} \\ &= \sum_{k\geq 0} \sum_{j=0}^{k} \left(\frac{1}{j!}M^j\right)\left(\frac{1}{(k-j)!}N^{k-j}\right) \\ &= \left(\sum_{k\geq 0} \frac{1}{k!}M^k\right)\left(\sum_{k\geq 0} \frac{1}{k!}N^k\right).\end{aligned}$$

This yields our desired expression. □

This immediately implies the following result.

Corollary 3.2.2.

$$U(t_1+t_2) = U(t_1)U(t_2).$$ □

For a square complex matrix M, we let M^* denote the conjugate transpose of M. As usual, I denotes the identity matrix of the same order as M. We say that a complex matrix M is *unitary* if

$$MM^* = I.$$

Corollary 3.2.3. *Let X denote an undirected graph. The corresponding transition matrix $U(t)$ is a symmetric unitary matrix.*

Proof. Let A denote the adjacency matrix of X. Since X is undirected, it follows that A and $U(t)$ are both symmetric. Furthermore, since A satisfies $A = A^*$, we see that $U(t)^* = U(-t)$. Using Lemma 3.2.1, we deduce that

$$\begin{aligned} I &= \exp(itA - itA) \\ &= \exp(itA)\exp(-itA) \\ &= U(t)U(-t) \\ &= U(t)U(t)^*. \end{aligned}$$

Thus $U(t)$ is unitary. □

Now we use the spectral decomposition of A to determine a useful re-formulation of the transition matrix $U(t)$. This highlights the connection between the continuous-time quantum walk and the spectrum of the graph.

Lemma 3.2.4. *Let X denote a graph with adjacency matrix A. If the spectral decomposition of A is*

$$A = \theta_0 E_0 + \cdots + \theta_d E_d,$$

then the spectral decomposition of $U(t)$ is

$$U(t) = \sum_{r=0}^{d} e^{\theta_r it} E_r. \tag{3.1}$$

Proof. Suppose that A has the spectral decomposition given above. Recall that each E_r satisfies

$$E_r^2 = E_r.$$

Therefore we have that

$$\begin{aligned} U(t) &= \exp(itA) \\ &= \sum_{k\geq 0} \frac{1}{k!}(itA)^k \\ &= \sum_{k\geq 0} \frac{1}{k!} \sum_{r=0}^{d} (\theta_r it)^k E_r \\ &= \sum_{r=0}^{d} \left(\sum_{k\geq 0} \frac{1}{k!} (\theta_r it)^k \right) E_r \\ &= \sum_{r=0}^{d} e^{\theta_r it} E_r. \end{aligned}$$

This yields our desired expression for $U(t)$. □

Now we consider what information we can deduce about the transition matrix from the automorphism group of the graph. Intuitively, it makes sense that there is a natural correspondence between the probability distributions of two vertices in the same orbit under the automorphism group of X. We formalize this intuition in the following lemma.

Lemma 3.2.5. *Let X denote a graph, and suppose there exists an automorphism of X that sends the ordered pair of vertices (j,k) to (v,w). Then*

$$U(t)_{j,k} = U(t)_{v,w}.$$

Proof. If there exists an automorphism of X that sends (j,k) to (v,w), then there exists a corresponding permutation matrix P such that

$$Pe_j = e_v \quad \text{and} \quad Pe_v = e_w.$$

Let A denote the adjacency matrix of X. Since P corresponds to an automorphism of X, we see that P satisfies

$$P^T P = I \quad \text{and} \quad P^T AP = A.$$

From this we deduce that $P^T A^k P = A^k$ for all positive integers k. Applying this to the transition matrix, we see that

$$\begin{aligned} P^T U(t) P &= P^T \left(\sum_{k \geq 0} \frac{(it)^k}{k!} A^k \right) P \\ &= \sum_{k \geq 0} \frac{(it)^k}{k!} (P^T AP)^k \\ &= U(t). \end{aligned}$$

This implies that

$$e_j^T P^T APe_k = e_v^T Ae_w,$$

and so our result follows. □

If we are working with vertex transitive graphs, then the above lemma tells us that it is sufficient to compute the first row of the transition matrix.

3.3 Mixing Properties

In this section, we explore the mixing properties of continuous-time quantum walks. As opposed to classical random walks on graphs, the probability distribution of a continuous-time quantum walk does not converge to a stationary distribution. Aharonov, Ambainis, Kempe, and Vazirani first introduced the *average mixing* property of a quantum walk, which is the limit of the average of the probability distributions over time [2]. This is referred to as *average mixing*. The work of Aharonov et al. was focused on a discrete quantum walk. Many of the earlier papers that studied quantum walks were concerned with average uniform mixing. See [21] and[37], for example.

Moore and Russell [40] were the first to introduce and study the uniform mixing property of continuous-time quantum walks. In their work and some subsequent publications, it is referred to as *instantaneous uniform mixing* to differentiate it from average uniform mixing. We say that a complex matrix A is a *flat matrix* if each of its entries has the same modulus. A graph X admits *uniform mixing* at time t if $U(t)$ is flat. Equivalently, since $U(t)$ is unitary, we see that a graph X admits uniform mixing if and only if

$$|U(t)_{u,v}|^2 = \frac{1}{|X|},$$

for each pair of vertices u and v in X. We define the mixing matrix $M(t) = U(t) \circ U(t)^*$. In terms of the mixing matrix, uniform mixing occurs if and only if

$$M(t) = \frac{1}{n} J.$$

This confirms that the probability distribution of the walk is uniform at time t if the transition matrix is flat at time t. In their introductory work, Moore and Russell show that the binary Hamming graphs admit uniform mixing [40]. They claim that the uniform mixing time is more relevant for hypercubes than the average mixing time, since the hypercubes does not admit average uniform mixing. Subsequent works considered uniform mixing on various graphs. For example, cycles were studied in [3], [1], and [16]. Also, variants of the Hamming graphs were studied in [24], [18], and [7], and Cayley graphs of the symmetric group were studied in [27]. In this thesis, we extend the known results of uniform mixing on cycles and quotients of Hamming graphs.

We are also interested in when the mixing matrix is close to uniform. We will see example of graphs that do not admit uniform mixing, although their mixing matrix gets arbitrarily close to the uniform distribution. We formalize this notion with the following definition. Let $||\cdot||$ denote the

Frobenius norm. More explicitly, for two $n \times n$ matrices A and B we have

$$||A - B|| = \sqrt{\sum_{j=1}^{n} \sum_{j=1}^{n} |A_{j,k} - B_{j,k}|^2}.$$

We say that a graph X admits ϵ-uniform mixing if and only if for every $\epsilon > 0$, there exists some time t such that the corresponding mixing matrix $U(t)$ satisfies

$$||U(t) \circ U(t)^* - \frac{1}{n} J|| < \epsilon.$$

In the subsequent chapters of this thesis, we focus on detecting whether or not particular families of graphs admit uniform mixing or ϵ-uniform mixing. If we make certain assumptions about the underlying structure of the graph, then it is feasible to confirm whether or not uniform mixing occurs. However, our understanding of uniform mixing on general graphs is still incomplete. For example, it is not known whether or not a graph has to be regular to admit uniform mixing. For small graphs, we know that a graph on four or less vertices must be regular in order to admit uniform mixing. We conjecture that no graphs on five vertices admit uniform mixing, although we only have empirical evidence to support this claim.

3.4 Mixing on Complete Graphs

In this section we first consider continuous-time quantum walks on complete graphs. This is a reformulation of the work done by Ahmadi, Belk, and Tamon [3]. The details are useful for considering uniform mixing on graph complements and the Hamming graphs. Our approach in this section is straightforward: first, we derive an expression for the transition matrix of a continuous-time quantum walk on a complete graph. Next, we compute the the modulus of its entries and determine necessary and sufficient conditions for uniform mixing to occur.

For notational convenience, let $E_0 = \frac{1}{n} J$. To begin, recall that the spectral decomposition of K_n is

$$A(K_n) = (n-1)E_0 - (I - E_0),$$

where J and I are the all-ones and identity matrix of order $n \times n$, respectively. Thus transition matrix is given by

$$U_{K_n}(t) = e^{(n-1)it} E_0 + e^{-it} (I - E_0)$$

$$= \frac{1}{n}\left(e^{(n-1)it} + (n-1)e^{-it}\right) I + \frac{1}{n}\left(e^{(n-1)it} - e^{-it}\right)(J - I).$$

Using this expression, we determine the times at which the transition matrix of K_n is flat. This reproduces a result due to Ahmadi, Belk, Tamon, and Wendler [3].

Theorem 3.4.1. *The complete graph K_n admits uniform mixing if and only if $n \in \{2, 3, 4\}$.*

Proof. The transition matrix is flat if and only if the diagonal and off diagonal terms have the same modulus. From our work above, we see that $U_{K_n}(t)$ is flat at time t if and only if

$$\left|\frac{1}{n}\left(e^{(n-1)it} - e^{-it}\right)\right| = \left|\frac{1}{n}\left(e^{(n-1)it} + (n-1)e^{-it}\right)\right|.$$

This holds if and only if

$$2 - \left(e^{nit} + e^{-nit}\right) = 1 + (n-1)^2 + (n-1)\left(e^{nit} + e^{-nit}\right),$$

which is equivalent to

$$\begin{aligned} e^{nit} + e^{-nit} &= \frac{1 - (n-1)^2}{n} \\ &= -n + 2. \end{aligned}$$

Since $|e^{nit} + e^{-nit}| \leq 2$, this equation has a solution if and only if

$$|-n + 2| \leq 2.$$

We conclude that K_n admits uniform mixing if and only if $n \in \{2, 3, 4\}$. More specifically, K_2 and K_4 admit uniform mixing at $t = \pi/4$, and K_3 admits uniform mixing at $t = \pi/9$. □

Note that the modulus of the diagonal entries of the transition matrix of K_n is larger than the off-diagonal terms *at all times* t if $n > 4$. Therefore if we consider a quantum walk on K_n with $n > 4$, the probability of remaining in the initial state is much higher than the probability of moving to a different state.

3.5 Graph Complements

In this section we prove two general results that relate uniform mixing on a regular graph to uniform mixing on its complement. One of these results is given in [30], and the other result is due to the author. We start by deriving a convenient expression for the transition matrix of the complement of a regular graph.

Lemma 3.5.1. *Suppose X is a k-regular graph on n vertices. Let $U_X(t)$ denote the transition matrix of X, and let $U_{\overline{X}}(t)$ denote the transition matrix of the complement of X. These two transition matrices are related by the following equation*

$$U_{\overline{X}}(t) = e^{-it}\overline{U_X(t)} + (e^{i(n-k-1)t} - e^{(-k-1)it})\frac{1}{n}J.$$

Proof. Let A denote the adjacency matrix of k-regular graph X, and let $\bar{A}$ denote the adjacency matrix of its complement $\bar{X}$. Let $E_0 = \frac{1}{n}J$. Since X is regular, we have

$$U_X(t)E_0 = e^{kit}E_0.$$

Using this we obtain the following expression for the transition matrix of $\overline{X}$

$$\begin{aligned} \exp(\bar{A}it) &= \exp((J-I-A)it) = \exp((J-I)it)\exp(-itA) \\ &= \left(e^{i(n-1)t}E_0 + e^{-it}\left(I - E_0\right)\right)U_X(-t) \\ &= \left(e^{-it}I + (e^{i(n-1)t} - e^{-it})E_0\right)U_X(-t) \\ &= e^{-it}U_X(-t) + (e^{i(n-k-1)t} - e^{(-k-1)it})E_0. \end{aligned}$$

Finally we recall that $U_X(-t) = \overline{U_X(t)}$. □

When t is an integer multiple of $2\pi/n$, the above expression for $U_{\overline{X}}(t)$ can be expressed in a simplified form. This leads to the following result, which appears in [30].

Theorem 3.5.2. *Let X denote a regular graph on n vertices, and let t denote an integer multiple of $2\pi/n$. At time t, uniform mixing occurs on X if and only if it occurs on the complement $\overline{X}$.*

Proof. When t is an integer multiple of $2\pi/n$, we have that $e^{tin} = 1$ and so

$$e^{i(n-k-1)t} - e^{(-k-1)it} = 0.$$

In this case, Lemma 3.5.1 implies that

$$U_{\overline{X}}(t) = e^{-it}\overline{U(t)}.$$

Therefore $U_{\overline{X}}(t)$ is flat if and only if $U_X(t)$ is flat. □

At other times t, we still obtain useful information about the transition matrix of $\overline{X}$ from the transition matrix of X. The following result is due to the author.

Theorem 3.5.3. *If X is regular graph with at least five vertices and X admits uniform mixing, then X and $\overline{X}$ must both be connected.*

Proof. Let A denote the adjacency matrix of X, and suppose that X is not connected. Let u and v denote two vertices that lie in different components of X. Recall that the (j,k)-entry of the r-th power of A is the number of walks of length r between u and v in A. Since u and v are disconnected, we deduce that the (u,v)-entry of $\exp(itA)$ is 0. Therefore uniform mixing cannot occur on X.

Of course, it also immediately follows that the (u,v)-entry of $\overline{U_X(t)}$ is 0. Recall from Lemma 3.5.1 that

$$U_{\overline{X}}(t) = e^{-it}\overline{U_X(t)} + (e^{i(n-k-1)t} - e^{(-k-1)it})\frac{1}{n}J.$$

This implies that the (u,v)-entry of $U_{\overline{X}}(t)$ is $(e^{i(n-k-1)t} - e^{(-k-1)it})/n$. Note that

$$\left|(e^{i(n-k-1)t} - e^{(-k-1)it})/n\right|^2 = (2 - 2\cos nt)/n^2.$$

If $n > 4$, then $(2 - 2\cos nt)/n^2 < 1/n$. Thus if $n > 4$, then for all times t the modulus squared of the (u,v)-entry of $U_{\overline{X}}$ is strictly less that $1/n$. This implies that uniform mixing does not occur on $\overline{X}$ either. □

As we saw earlier, both C_4 and K_4 admit uniform mixing, and so the vertex bound in the above result is tight. Also, the above result provides an alternative proof of the following, which is originally due to Ahmadi *et al.* [3].

Corollary 3.5.4. *Any complete multipartite graph with more than four vertices does not admit uniform mixing.*

Proof. If X is a complete multipartite graph, then its complement $\overline{X}$ is disconnected. By Theorem 3.5.3, we conclude that X does not admit uniform mixing. □

With the notable exception of K_2, K_3, K_4, and C_4, we don't have an example of a graph that admits uniform mixing whose complements doesn't also admit uniform mixing. This suggests that a stronger result than Theorem 3.5.2 might be true.

3.6 Mixing in Association Schemes

Now we focus on uniform mixing in association schemes. In this section we see that uniform mixing occurs if and only if there is a unimodular solution to a system of equations in terms of the Krein parameters of the association scheme.

Let $\mathcal{A} = \{A_0, \ldots, A_d\}$ denote a d-class association scheme of order n with dual basis $\{E_0, \ldots, E_d\}$. We consider a graph X denote the graph with adjacency matrix A in $\mathbb{C}[\mathcal{A}]$ and eigenvalues $\theta_0, \ldots, \theta_d$ such that

$$A = \theta_0 A_0 + \cdots + \theta_d A_d.$$

We consider the transition matrix of a continuous-time quantum walk on X, which is given by

$$U(t) = \exp(itA).$$

Recall that uniform mixing occurs on X at time t if and only if

$$U(t) \circ U(-t) = \frac{1}{n} J = E_0.$$

As we saw earlier, the matrices in the Bose-Mesner algebra $\mathbb{C}[\mathcal{A}]$ are simultaneously diagonalizable. In terms of the dual basis we have

$$U(t) \circ U(-t) = \sum_{i=0}^{d} \sum_{j=0}^{d} e^{(\theta_i - \theta_j)it} E_i \circ E_j.$$

Using the Krein parameters from Section 2.5 this matrix can be expressed as a linear combination of $\{E_1, \ldots, E_d\}$ as follows:

$$U(t) \circ U(-t) = \frac{1}{n} \sum_{k=0}^{d} \left(\sum_{i=0}^{d} \sum_{j=0}^{d} q_{i,j}(k) e^{(\theta_i - \theta_j)it} \right) E_k. \tag{3.2}$$

Using Lemma 2.6.1, we compute the coordinate of E_0 in the expression for $U(t) \circ U(-t)$ in (3.2) and we obtain

$$\sum_{i=0}^{d} \sum_{j=0}^{d} q_{i,j}(0) e^{(\theta_i - \theta_j)it} = \sum_{j} m_j = n.$$

With this we further simplify (3.2) to

$$U(t) \circ U(-t) = E_0 + \frac{1}{n} \sum_{k=1}^{d} \left(\sum_{i=0}^{d} \sum_{j=0}^{d} q_{i,j}(k) e^{(\theta_i - \theta_j)it} \right) E_k. \tag{3.3}$$

We formalize these observations into the following theorem.

Theorem 3.6.1. *Let $\mathcal{A}$ denote a d-class association scheme. Suppose X is a graph whose adjacency matrix A is contained in $\mathbb{C}[\mathcal{A}]$ with eigenvalues $\theta_0, \dots, \theta_d$. Uniform mixing occurs on X at time t if and only if*

$$\sum_{i=0}^{d} \sum_{j=0}^{d} q_{i,j}(k) e^{(\theta_i - \theta_j)it} = 0 \tag{3.4}$$

for all $1 \leq k \leq d$. □

We note that the system of equations given in the theorem above only depends on the parameters of the scheme. That is to say, given an association scheme and its parameter set, we can give necessary and sufficient conditions for uniform mixing to occur in terms of the parameters of the scheme. However, as we see in later sections, it is not always straightforward to determine whether or not a solution to the corresponding system of equations exists.

Chapter 4

Algebraic Connections

4.1 Introduction

In this chapter we introduce a set of algebraic tools for determining whether or not uniform mixing occurs on graphs in an association scheme. To understand the importance of these tools, we rephrase our main problem. Recall that when uniform mixing occurs on a graph X at the time t, the corresponding transition matrix $U(t)$ is flat. Thus detecting uniform mixing in an association scheme is equivalent to finding flat unitary matrices in the Bose-Mesner algebra that are in exponential form.

If we drop the requirement of exponential form, it is still difficult to determine whether the Bose-Mesner algebra of a scheme contains a flat unitary. Flat unitary matrices are a subset of a broader class of matrices called *type-II matrices*. With this in mind, we ask the following relaxation of our original question: are there type-II matrices in the Bose-Mesner algebra? If the answer to this question is no, then we immediately rule out the possibility of uniform mixing occurring on the graphs in the scheme. If the answer is yes, then we try to determine whether or not any of the type-II matrices are scalar multiples of flat unitaries in exponential form.

There are two distinct advantages to working with type-II matrices. First, the coordinates of a type-II matrix in an association scheme correspond to solutions in an algebraic variety. This enables an algebraic formulation of our relaxed problem. In certain cases we cannot explicitly describe all of the type-II matrices related to a given scheme, but we can still tease out useful information about their coordinates. Second, there is a substantial body of literature about type-II matrices, and it is possible to build upon known results. In particular, our later work with cyclic schemes relies heavily upon the classification of cyclic type-II matrices given by Haagerup [33]. Likewise, the study of uniform mixing on strongly regular graphs relies heavily upon the classification of type-II matrices given by Chan and Godsil [19] and Chan [17].

As we proceed through this chapter, our algebraic approach will become more concrete. We begin this chapter by reviewing the necessary algebraic and transcendental number theory. Using these observations, we prove Theorem 4.2.4, which is an essential result for much of our later work. Next we give an overview of type-II matrices and demonstrate the connection between type-II matrices and uniform mixing. In particular, we highlight their connection to uniform mixing.

The main result in this chapter is Theorem 4.2.4. It is due to the author. At the present time, it is the most useful method known to show that uniform mixing does not occur on a graph.

4.2 Algebraic vs. Transcendental Numbers

We begin by reviewing some algebraic and transcendental number theory. In this section, we prove that if the entries of the transition matrix are all algebraic, then there are significant restrictions on the eigenvalues of the underlying graph. In later sections, we will see that if uniform mixing occurs on certain graphs, then the entries of the corresponding transition matrix must be algebraic.

First recall that an *algebraic number* is the root of a polynomial in $\mathbb{Q}[x]$. Trivially, all rational numbers are algebraic. Irrational numbers such as $\sqrt{2}$ are also algebraic. The set of algebraic numbers forms a ring under addition and multiplication. And, perhaps more usefully, the root of a polynomial whose coefficients are algebraic numbers is also an algebraic number. The next two lemmas are well-known. For example, proofs can be found in [45].

Lemma 4.2.1. *Let M denote an $n \times n$ matrix with algebraic entries. The eigenvalues of M are algebraic numbers.*

Proof. The eigenvalues of M are roots of the characteristic equation given by

$$\det(M - xI) = 0.$$

The entries of M are algebraic, and so $\det(M - xI)$ is a polynomial with algebraic coefficients. It follows that the eigenvalues of M are algebraic numbers. □

In particular, if we apply the above lemma to the adjacency matrix of a graph, we see that the eigenvalues of the graph are roots of a polynomial in $\mathbb{Z}[x]$. Roots of such polynomials are called *algebraic integers*. Thus all of the eigenvalues of an adjacency matrix must be algebraic integers. The only rational numbers that are algebraic integers are the integers themselves. From these observations, we immediately deduce the following well-known result.

Lemma 4.2.2. *Let X denote a graph with adjacency matrix A. Each eigenvalue of A is either irrational or an integer.* □

A *transcendental number* is a number in $\mathbb{C}$ that is not algebraic. For example, π and e are well-known transcendental numbers. In general it is difficult to prove that a number is transcendental. One of the most useful tools for detecting transcendental numbers is the famous Gelfond-Schneider Theorem. The following formulation of this theorem is due to Michel Waldschmidt [13].

Theorem 4.2.3 (Gelfond-Schneider)**.** *If x and y are two nonzero complex numbers with x irrational, then at least one of the numbers x, e^y, or e^{xy} is transcendental.* □

Now apply the Gelfond-Schneider theorem to the entries of a transition matrix. This result is due to the author, and it appears in [30].

Theorem 4.2.4. *Let X denote a graph. If all of the entries of the transition matrix $U(t)$ are algebraic for a particular nonzero time t, then the ratio of any two eigenvalues of X must be rational.*

Proof. Let A denote the adjacency matrix of X, and let $\{\theta_0, \dots, \theta_d\}$ denote the eigenvalues of A. Recall that each eigenvalue of A is an algebraic number. Also recall from Lemma 3.2.4 that we can express the transition matrix as

$$U(t) = \sum_{k=0}^{d} e^{it\theta_k} E_k. \tag{4.1}$$

From this we see that the eigenvalues of $U(t)$ are $\{e^{it\theta_0}, \dots, e^{it\theta_d}\}$. If all entries of $U(t)$ are algebraic, then the eigenvalues of $U(t)$ must be algebraic. Consider two distinct eigenvalues θ_r and θ_s. If we suppose that θ_r/θ_s is irrational, then Theorem 4.2.3 implies that one of

$$\{\theta_r/\theta_s, e^{it\theta_s}, e^{it\theta_s(\theta_r/\theta_s)}\}$$

must be transcendental, which is a contradiction. Therefore θ_r/θ_s must be rational for every pair of eigenvalues θ_r and θ_s of X. □

If we restrict our consideration to regular graphs, then Theorem 4.2.4 can be reformulated as follows.

Theorem 4.2.5. *Suppose that X is a regular graph with transition matrix $U(t)$. If H is a matrix with all algebraic entries and there exists a nonzero time t such that*

$$U(t) = \gamma H,$$

for some γ in $\mathbb{C}$, then X must have integral eigenvalues.

Proof. By a well-known result from linear algebra, we know that for the complex matrix itA we have

$$\det(U(t)) = \det(\exp(itA)) = e^{\mathrm{tr}(itA)} = 1.$$

Under our assumption that $U(t) = \gamma H$, this result implies that

$$\gamma^n \det(H) = 1.$$

Since H has all algebraic entries, it follows that $\det(H)$ is an algebraic number. This implies that γ is algebraic, and hence all of the entries of $U(t)$ must be algebraic. Theorem 4.2.4 shows that the ratio of any two eigenvalues must be rational. Since X is regular, the largest eigenvalue is an integer, and so the rest of the eigenvalues of X must be rational. By Lemma 4.2.2, we conclude that all of the eigenvalues of X must be integers. □

4.3 Cyclotomic Number Theory

In this section we recall some essential background information about the number theory related to the eigenvalues of cycles. In turn, this will be useful for determining information about the eigenvalues of the transition matrices of cycles. The eigenvalues of a cycle lie in a cyclotomic number field. For more information about cyclotomic fields see [50], for example. Recall from Section 2.8 that the eigenvalues of the cycle C_n have the form

$$\theta_r = \omega^r + \omega^{-r} = 2\cos(2\pi r/n),$$

where $\omega = e^{2\pi i/n}$. If n is even, then $\theta_0 = 2$ and $\theta_{n/2} = -2$ are eigenvalues with multiplicity one. All of the other eigenvalues have multiplicity two and modulus strictly less that two. If n is odd, then θ_0 is the only eigenvalue with multiplicity one, and every nontrivial eigenvalue has multiplicity two. The results in this section are not new. In fact, our first result has been known for quite some time. A proof is given in Olmsted's 1945 paper [41].

Theorem 4.3.1. *If α is in $\mathbb{Q}$, then $\cos(\alpha\pi)$ is in $\mathbb{Q}$ if and only if*

$$\cos(\alpha\pi) \in \{0, \pm 1/2, \pm 1\}. \qquad \square$$

In particular, if we assume that $\alpha = 2\pi/n$ for some positive integer n, then this result restricts the possible values for n such that $\cos(2\pi/n)$ is rational. We note the following correspondences.

$$\begin{aligned} \cos(2\pi/n) &= 1/2 \implies n = 6 & \cos(2\pi/n) &= -1/2 \implies n = 3 \\ \cos(2\pi/n) &= 1 \implies n = 1 & \cos(2\pi/n) &= -1 \implies n = 2 \\ \cos(2\pi/n) &= 0 \implies n = 4. \end{aligned}$$

Therefore $\cos(2\pi/n)$ is rational if and only if $n \in \{1, 2, 3, 4, 6\}$. As an immediate consequence of this observation, we deduce that the cycle C_n has an irrational eigenvalue for all but five values of n.

Lemma 4.3.2. *If $n = 5$ or $n \geq 7$, then C_n has an irrational eigenvalue.*

Proof. Using the notation above, we note that $\theta_1 = 2\cos(2\pi/n)$ is an eigenvalue of C_n. If we assume $n = 5$ or $n \geq 7$, then Theorem 4.3.1 implies that θ_1 is irrational. $\square$

Now we narrow our focus to cycles of prime length. Suppose that p is an odd prime. Let $d = (p-1)/2$, and let $\theta_1, \ldots, \theta_d$ denote the nontrivial eigenvalues of C_p. Also let ϕ denote the Euler phi function. As before, ω is the primitive p-root of unity given by

$$\omega = e^{2\pi i/p}.$$

Using this notation, we investigate number fields related to the cyclic schemes. The following results are well-known. See [45], for example.

Lemma 4.3.3. *Each of the eigenvalues $\theta_0, \ldots, \theta_d$ can be expressed as a polynomial in θ_1 with integral coefficients.*

Proof. First recall that $\theta_0 = 2$ is trivially a polynomial in θ_1. Next note that

$$(\omega + \omega^{-1})^2 = \omega^2 + \omega^{-2} + 2.$$

Rearranging this equation yields $\theta_2 = \theta_1^2 - 2$. More generally, for $2 \leq k \leq d$, we see that $(\omega + \omega^{-1})^k$ can be expressed as an integral linear combination of $1, \theta_1, \ldots, \theta_{k-1}$. By induction we conclude that each eigenvalue $\theta_0, \ldots, \theta_d$ can be expressed as a polynomial in θ_1 with integral coefficients. $\square$

Using this lemma, we obtain useful information about the smallest number field containing all of the eigenvalues of the cycle.

Lemma 4.3.4. *The extension field* $\mathbb{Q}(\theta_1, \dots, \theta_d)$ *is isomorphic to* $\mathbb{Q}(\theta_1)$*, and*

$$[\mathbb{Q}(\theta_1) : \mathbb{Q}] = (p-1)/2.$$

Proof. By Lemma 4.3.3, we immediately see that $\mathbb{Q}(\theta_1, \dots, \theta_d)$ is isomorphic to $\mathbb{Q}(\theta_1)$. Recall that the cyclotomic field $\mathbb{Q}(\omega)$ is an algebraic extension of $\mathbb{Q}$, and

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(p) = p - 1,$$

where ϕ denotes the Euler phi function. Since ω is the root of a quadratic polynomial over $\mathbb{Q}(\theta_1)$ and θ_1 is real, we see that $[\mathbb{Q}(\theta_1) : \mathbb{Q}] = (p-1)/2$. □

Finally, we obtain a very useful theorem about the linear independence of a subset of the eigenvalues of the cycle.

Theorem 4.3.5. *The set* $\{1, \theta_1, \theta_2, \dots, \theta_{(p-3)/2}\}$ *is linearly independent over* $\mathbb{Q}$*.*

Proof. Suppose, for a contradiction, that there exists some rational coefficients α_k for $0 \leq k \leq (p-3)/2$ such that

$$\alpha_0 + \alpha_1\theta_1 + \alpha_2\theta_2 + \cdots + \alpha_{(p-3)/2}\theta_{(p-3)/2} = 0,$$

with at least one α_k nonzero. Since we have $\theta_k = \omega^k + \omega^{-k}$, we see can re-express this equation in terms of ω as

$$\alpha_0 + \alpha_1(\omega + \omega^{-1}) + \alpha_2(\omega^2 + \omega^{-2}) + \cdots + \alpha_{(p-3)/2}(\omega^{(p-3)/2} + \omega^{-(p-3)/2}) = 0.$$

Multiplying both sides by $\omega^{(p-3)/2}$ yields a polynomial equation in terms of ω with rational coefficients and degree at most $p-3$. This contradicts the fact that $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$. □

These results about cyclotomic number theory will be crucial in our later work with cycles.

4.4 Kronecker's Theorem

In this section, we consider an important result due to Kronecker. We follow the treatment given in [12]. In addition to this result, we state two lemmas related to the Frobenius norm. We apply all of these results to prime cycles in Section 5.5.

Our work in this section centres around the eigenvalues of the transition matrix. Let X denote a graph with adjacency matrix A, and suppose that the spectral decomposition of A is

$$A = \theta_0 E_0 + \cdots + \theta_d E_d.$$

Recall that the transition matrix of X can be expressed as

$$U(t) = e^{it\theta_k} E_0 + e^{it\theta_1} E_1 + \cdots + e^{it\theta_d} E_d.$$

For a real number x, we note that

$$e^{\theta_j it} = e^{ix} \quad \text{if and only if} \quad 2\pi \text{ divides } \theta_j t - x.$$

Rephrased, we note that

$$e^{\theta_j it} = e^{ix} \quad \text{if and only if} \quad \frac{\theta_j t}{2\pi} - \frac{x}{2\pi} \in \mathbb{Z}.$$

For this reason, we wish to consider the scaled exponents of the eigenvalues of $U(t)$ as elements of the additive group $\mathbb{R}/\mathbb{Z}$. Recall that the direct product of d copies of $\mathbb{R}/\mathbb{Z}$ is a *compact torus*. Suppose that t is an element of a compact torus T. We say that t is a *generator* if the smallest closed subgroup of T containing t is T itself.

Theorem 4.4.1 (Kronecker)**.** *Let $(t_1, \ldots, t_r)$ denote an element of $\mathbb{R}^r$, and let t be the image of this point in $T = (\mathbb{R}/\mathbb{Z})^r$. Then t is a generator of T if and only if $\{1, t_1, \ldots, t_r\}$ are linearly independent over $\mathbb{Q}$.* □

In Section 5.5 we use Kronecker's Theorem to show that certain flat unitary matrices are contained in the closure of the subgroup of unitary matrices given by

$$\{U(t) : t \in \mathbb{R}\}.$$

Now we give two basic lemmas that make our application of Kronecker's Theorem more straightforward. Our goal is to relate the matrix norms corresponding to $U(t)$ and $U(t) \circ U(-t)$.

Intuitively, it makes sense that if the coordinates of $U(t)$ are close to the coordinates of a flat matrix, then the probability distribution of $U(t) \circ U(-t)$ is close to uniform. To show this, we need the following inequality for complex numbers.

Lemma 4.4.2. *If α and β are two complex numbers such that $|\alpha|, |\beta| \leq 1$, then*

$$\left||\alpha|^2 - |\beta|^2\right|^2 \leq 4|\alpha - \beta|^2.$$

Proof. Since $|\alpha| \leq 1$ and $|\beta| \leq 1$, it follows that $|\alpha| + |\beta| \leq 2$. The Triangle Difference Inequality implies that

$$||\alpha| - |\beta|| \leq |\alpha - \beta|.$$

Combining these two observations gives us

$$\left||\alpha|^2 - |\beta|^2\right| = ||\alpha| - |\beta|| \, ||\alpha| + |\beta|| \leq 2 \, ||\alpha| - |\beta|| \leq 2|\alpha - \beta|.$$

Squaring both side yields our desired inequality. □

Using this lemma, we formalize our intuition that if $U(t)$ is close to flat at some time t, then $U(t) \circ U(-t)$ will be close to uniform. This straightforward result is due to the author.

Lemma 4.4.3. *Suppose that A and B are symmetric $n \times n$ complex matrices, such that*

$$||A - B|| \leq \epsilon,$$

for some positive real number ϵ. Then

$$||A \circ A^* - B \circ B^*|| \leq 2\epsilon.$$

Proof. From the definition of $|| \cdot ||$ and our assumptions on A and B, we have that

$$||A - B||^2 = \sum_{j=1}^{n} \sum_{j=1}^{n} |A_{j,k} - B_{j,k}|^2 \leq \epsilon^2.$$

Applying Lemma 4.4.2, we see that

$$\begin{aligned} ||A \circ A^* - B \circ B^*||^2 &= \sum_{j=1}^{n} \sum_{k=1}^{n} \left||A_{j,k}|^2 - |B_{j,k}|^2\right|^2 \\ &\leq \sum_{j=1}^{n} \sum_{j=1}^{n} 4 \left|A_{j,k} - B_{j,k}\right|^2 \\ &\leq 4\epsilon^2. \end{aligned}$$

This proves our desired inequality. □

4.5 Type-II Matrices

In this section we introduce type-II matrices. These matrices were first defined in the study of spin models [34]. We draw attention to a special subclass of type-II matrices: the complex Hadamard matrices. We see that uniform mixing occurs on a graph at time t if and only if the transition matrix at time t is a complex Hadamard matrix. For practical purposes, though, much of our work is within the more general framework of type-II matrices.

For an $m \times n$ matrix A with all nonzero entries, the *Schur inverse* $A^{(-)}$ is given by

$$A^{(-)}_{i,j} = \frac{1}{A_{i,j}}.$$

As desired, it follows that

$$A \circ A^{(-)} = J.$$

We are now equipped to define the family of matrices we are interested in.

Definition 4.5.1. *A complex $n \times n$ matrix A is a type-II matrix if*

$$AA^{(-)T} = nI. \tag{4.2}$$

Using the language of type-II matrices, we reformulate the definition of uniform mixing.

Lemma 4.5.2. *The graph X admits uniform mixing at time t if and only if $\sqrt{n}U(t)$ is a type-II matrix.*

Proof. We note that a complex number x satisfies $|x| = 1$ if and only if $\bar{x} = x^{-1}$. Therefore the transition matrix satisfies

$$U(t) \circ U(t)^* = \frac{1}{n}J \quad \text{if and only if} \quad \sqrt{n}U(t)^* = \frac{1}{\sqrt{n}}U(t)^{(-)T}.$$

Since $U(t)$ is a symmetric unitary matrix, it follows that $U(t)^{(-)T} = U(t)^{-1}$. We conclude that $U(t)$ is flat if and only if $\sqrt{n}U(t)$ is type-II. □

Now we highlight a special subclass of type-II matrices. If M is a type-II matrix and each entry of M satisfies $|M_{j,k}| = 1$, then the matrix M is called a *complex Hadamard* matrix. This is a natural generalization of the famous real Hadamard matrices whose entries are all in $\{1, -1\}$. We give a standard definition below.

Definition 4.5.3. *A complex $n \times n$ matrix M is a complex Hadamard matrix if and only if*

(i) $MM^* = nI$.

(ii) $M \circ \overline{M} = J$.

Translated into the language of complex Hadamard matrices, Lemma 4.5.2 is equivalent to the following.

Corollary 4.5.4. *Uniform mixing occurs on X at time t if and only if $\sqrt{n}U(t)$ is a complex Hadamard matrix.* □

For all known examples of graphs that admit uniform mixing, the corresponding entries of $\sqrt{n}U(t)$ are roots of unity. Such matrices are called *Butson-type* complex Hadamard matrices. For a survey of known results about complex Hadamard matrices see [47] and [46]. As we observe in the next section, the advantage of working with type-II matrices is that Definition 4.5.1 translates into an equivalent system of polynomial equations. Generally, if we consider a complex number x, there is no way to express its conjugate $\bar{x}$ as a polynomial in x. Thus it is not easy to use an algebraic approach directly with complex Hadamard matrices.

4.6 Systems of Polynomial Equations

Next we define a system of multivariate polynomials whose common solutions correspond to the coordinates of type-II matrices. We show that a matrix is type-II if and only if its matrix coordinates are the coordinates of a point in an algebraic variety. This translation from matrices to algebraic varieties is crucial for our further characterization of the type-II matrices in exponential form.

To begin, recall that an $n \times n$ complex matrix M is a type-II matrix if and only if it satisfies $MM^{(-)} = nI$. First we introduce a variable $x_{j,k}$ for each entry of M. In terms of these variables, the (u, v)-entry of $MM^{(-)}$ is

$$\left(MM^{(-)}\right)_{u,v} = \sum_j x_{u,j} x_{j,v}^{-1}. \tag{4.3}$$

We wish to express these equations as a system of polynomial equations, and so we introduce another n^2 variables indexed as $y_{j,k}$ for $1 \le j, k \le n$ such that

$$x_{j,k} y_{j,k} = 1.$$

Putting this together, we see that M is a type-II matrix if and only if the coordinates $x_{j,k}$ of M correspond to a complex solution to the following system of polynomial equations:

$$\begin{aligned} \textstyle\sum_j x_{u,j}y_{j,u} &= n \quad \text{for } 1 \leq u \leq n \\ \textstyle\sum_j x_{u,j}y_{j,v} &= 0 \quad \text{for } 1 \leq u, v \leq n \text{ and } u \neq v \\ x_{u,v}y_{u,v} &= 1 \quad \text{for } 1 \leq u, v \leq n. \end{aligned} \tag{4.4}$$

This is a system of polynomial equations with $2n^2$ variables and $2n^2$ equations. However, if M is a type-II matrix, then any scalar multiple αM with $\alpha \in \mathbb{C}$ is also a type-II matrix. Thus we can assume that the diagonal terms satisfy $x_{j,j} = 1$ for $1 \leq j \leq n$. If we assume M is in the Bose-Mesner algebra of an association scheme, then we can further reduce the complexity of the corresponding system.

The solutions to (4.4) form an algebraic variety. The rest of this section deals with algebraic varieties. The results and notation we use are given in Cox, Little, and O'Shea [22].

Let $\mathbb{F}$ denote a field, and let $f_1, \ldots, f_s$ denote polynomials in $\mathbb{F}[x_1, \ldots, x_r]$. Further let $V(f_1, f_2, \ldots, f_s)$ denote the following set:

$$\{(a_1, a_2, \ldots, a_r) \in \mathbb{F}^r : f_j(a_1, a_2, \ldots, a_r) = 0 \text{ for all } 1 \leq j \leq s\}.$$

We say that $V(f_1, f_2, \ldots, f_s)$ is the *affine variety* defined by $f_1, f_2, \ldots, f_s$. If we consider strongly regular graphs, for example, it is possible to determine all of the type-II matrices in the Bose-Mesner algebra by finding all of the solutions in the corresponding affine variety. In other cases, such as the cycles of prime order, it is difficult to explicitly determine all solutions, but it is known that there are a finite number of solutions in the corresponding affine variety. With this in mind, we are interested in the following well-known result.

Theorem 4.6.1. *Let $f_1, \ldots, f_r$ denote a set of r polynomials in $\mathbb{Q}[x_1, \ldots, x_r]$. If the affine variety $V(f_1, f_2, \ldots, f_r)$ over $\mathbb{C}$ has finite number of points, then the coordinates of each point are algebraic.*

Proof. Let $I = \langle f_1, f_2, \ldots, f_r \rangle$. First we compute a Groebner basis for I using lexicographic ordering. Since $V(I)$ is a finite set, Theorem 6 on page 243 of [22] states that for each j in $1 \leq j \leq n$ there is some $m_j \geq 0$ such that $x_j^{m_j}$ is the leading term of an element in the Groebner basis [22]. This implies that if $(a_1, a_2, \ldots, a_r)$ is a solution in $V(I)$, then a_r is the root of univariate polynomial with coefficients in $\mathbb{Q}$. In other words, a_r is an algebraic number. Inductively we see that each a_j is an algebraic number for $1 \leq j \leq r$. □

In the next section, we compute the system of polynomial equations corresponding to circulant type-II matrices of prime order. We see that there are a finite number of solutions to this system, which enables us to apply Theorem 4.6.1.

4.7 Cyclic n-roots

In this section, we consider circulant type-II matrices. These are commonly known as *cyclic n-roots*, and they were introduced by Björck as a method for studying biunimodular sequences [8]. In terms of matrices, biunimodular sequences are equivalent to complex Hadamard matrices. To begin, we give Björck's original definition of a cyclic n-root and show that it is equivalent to a circulant type-II matrix with ones down the diagonal. Next we summarize a key result due to Haagerup that proves there are a finite number of cyclic p-roots when p is an odd prime. This result is crucial to our work with uniform mixing on prime cycles given in Section 5.4. We end this section by briefly discussing what is known about cyclic n-roots for general n. The results in this section are all due to either Börck or Haagerup or both.

In [8] Björck introduced cyclic n-roots for every n in $\mathbb{Z}$ such that $n \geq 2$ as the solutions of the form $z = (z_0, \ldots, z_{n-1})$ to the following system of $n+1$ polynomial equations:

$$\begin{aligned} z_0 + z_1 + \cdots + z_{n-1} &= 0 \\ z_0 z_1 + z_1 z_2 + \cdots + z_{n-1} z_0 &= 0 \\ &\vdots \\ z_0 z_1 \cdots z_{n-2} + z_1 z_2 \cdots z_{n-1} + \cdots + z_{n-1} z_0 \cdots z_{n-3} &= 0 \\ z_0 z_1 \cdots z_{n-1} &= 1. \end{aligned} \tag{4.5}$$

First we show that a solution to this system is equivalent to a circulant type-II matrix. Let M denote a circulant matrix of order n with all entries nonzero. We index the rows and columns of M by elements of $\mathbb{Z}_n$. Using the notation introduced in Section 2.8, we let C denote the cyclic permutation matrix given by

$$C_{j,k} = \begin{cases} 1 & \text{if } \ j-k=1 \\ 0 & \text{otherwise.} \end{cases}$$

Recall that $C^n = I$ and every circulant matrix of order n can be expressed as a polynomial in C. Let $x = (x_0, x_1, \ldots, x_{n-1})$ denote a vector in $\mathbb{C}^n$ such that $x_j = M_{1,j+1}$. We express M in terms of C as

$$M = \sum_{j=0}^{n-1} x_j C^j \quad \text{and} \quad M^{(-)T} = \sum_{j=0}^{n-1} x_j^{-1} C^{-j}. \tag{4.6}$$

Recall that M is a type-II matrix if and only if $MM^{(-)T} = nI$. Using the expression for M and $M^{(-)T}$ given above, we compute the following system in which all of the indices are computed in $\mathbb{Z}_n$:

$$\begin{aligned} MM^{(-)T} &= \left(\sum_{j=0}^{n-1} x_j C^j\right)\left(\sum_{j=0}^{n-1} x_j^{-1} C^{-j}\right) \\ &= \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} x_j x_k^{-1} C^{j-k} \\ &= \sum_{r=0}^{n-1}\left(\sum_{j=0}^{n-1} x_j x_{j-r}^{-1}\right) C^r. \end{aligned}$$

Since $\{I, C, \ldots, C^{n-1}\}$ is a linearly independent set of matrices, we see that the right hand side of the equation above is equal to nI if and only if the coordinates with respect to C^{-r} are 0 for all $1 \le r \le n-1$. This implies that M is type-II if and only if

$$\sum_{j=0}^{n-1} x_j x_{j-r}^{-1} = 0 \quad \text{for all } \ 1 \le r \le n-1. \tag{4.7}$$

Now we define a corresponding $z = (z_0, z_1, \ldots, z_{n-1})$ in $\mathbb{C}^n$ such that

$$z_j = x_{j+1} x_j^{-1},$$

where the indices of x are computed in $\mathbb{Z}_n$. The next result shows the one-to-one correspondence between cyclic n-roots and cyclic type-II matrices with constant diagonal one. This is equivalent to a result given by Björck [8].

Lemma 4.7.1. *The matrix $\sum_{j=0}^{n-1} x_j C^j$ is a type-II matrix with diagonal one if and only if $(x_1 x_0^{-1}, x_2 x_1^{-1}, \ldots, x_0 x_{n-1}^{-1})$ is a cyclic n-root.*

Proof. For all j and r such that $0 \le j, r \le n-1$, the coordinates of x and z satisfy

$$\prod_{k=j-r}^{j-1} z_k = x_{j-r}^{-1}\left(x_{j-r+1} x_{j-r+1}^{-1}\right) \cdots \left(x_{j-1}^{-1} x_{j-1}\right) x_j = x_j x_{j-r}^{-1},$$

where again the indices of x and z are computed in $\mathbb{Z}_n$. Substituting this into (4.7) gives us the first $n-1$ equations of (4.5). Further note that our choice of z necessarily satisfies

$$\prod_{j=0}^{n-1} z_j = 1.$$

Therefore if x satisfies (4.7), then z is a cyclic n-root. Conversely, suppose that z is a cyclic n-root and define $x_0 = 1$ and

$$x_j = \prod_{r=0}^{j-1} z_r$$

for $1 \leq j \leq n-1$. Since z satisfies (4.5), our reasoning above implies that x satisfies (4.7). Thus $M = \sum_{j=0}^{n-1} x_j C^j$ is a type-II matrix with constant diagonal one. □

The most important result of this section is due to Haagerup [33].

Theorem 4.7.2. *If p is an odd prime, there are only a finite number of cyclic p-roots.* □

In light of Lemma 4.7.1, Haagerup's result tells us that there are only a finite number of cyclic type-II matrices of order $p \times p$ with constant diagonal one. In the language of association schemes, this result implies the following.

Corollary 4.7.3. *Let p denote an odd prime, and let $\mathcal{A}$ denote the cyclic association scheme of order p. There are a finite number of type-II matrices in $\mathbb{C}[\mathcal{A}]$ with constant diagonal one.* □

Unfortunately this result does not hold for cyclic n-roots when n is not a prime. It was shown by Backelin that if n is a multiple of a square integer, then there are infinitely many cyclic n-roots [5].

Chapter 5

Bipartite Graphs and Cycles

5.1 Introduction

Following Moore and Russell's work with uniform mixing on binary Hamming schemes, several researchers considered the uniform mixing properties of cycles. Ahmadi et al. show that the cycles C_3 and C_4 admit uniform mixing [3]. This is as a consequence of their work with complete graphs and complete multipartite graphs. They also make following conjecture.

Conjecture 5.1.1 (Ahmadi, Belk, Tamon, Wendler 2003)**.** *Other than C_3 and C_4, no cycle C_n admits uniform mixing.*

Following this conjecture, in 2007, Adamczak et al. [1] showed that C_n does not admit uniform mixing if $n = 2^u$ for $u \geq 3$, or if $n = 2^u m$ where $m \equiv 3 \pmod 4$ and $u \geq 1$. In the same year, Carlson et al. show that uniform mixing does not occur on C_5 [16]. Prior to the work presented in this chapter, this was the current state of Conjecture 5.1.1. One of our main results in this chapter shows that uniform mixing does not occur on cycles of even length or odd prime length.

We begin this chapter by summarizing Godsil's work with uniform mixing on bipartite graphs. We use these results in conjunction with Theorem 4.2.5 to show that uniform mixing cannot occur on a cycle of even length other than C_4. This is a joint result of Godsil and the author, and it settles Conjecture 5.1.1 for the even case. Next we consider uniform mixing on cycles of prime length. Using our algebraic tools from Chapter 4, we show that uniform mixing does not occur on a cycle of prime length. This result is due to the author.

Finally, we show that ϵ-uniform mixing occurs on prime cycles. This implies that the corresponding probability distribution gets arbitrarily close to the uniform distribution. This result is due to the author.

5.2 Bipartite Graphs

In this section we consider uniform mixing on bipartite graphs. We are primarily concerned with even cycles. However, the results in this section apply to all bipartite graphs. All of this work in this section appears in [30].

To begin, suppose that X is a bipartite graph on n vertices with adjacency matrix A. We assume the rows and columns of A are ordered such that

$$A = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix}.$$

Since A is a block matrix, we easily compute the even and odd powers of A.

$$\begin{aligned} A^{2k} &= \begin{pmatrix} (BB^T)^k & 0 \\ 0 & (B^TB)^k \end{pmatrix} \\ A^{2k+1} &= \begin{pmatrix} 0 & (BB^T)^kB \\ (B^TB)^kB^T & 0 \end{pmatrix}. \end{aligned}$$

Now we derive an expression for the transition matrix of X in terms of these blocks.

$$\begin{aligned} U(t) = e^{itA} &= \sum_{k\geq 0} \frac{1}{k!}(itA)^k \\ &= \sum_{k\geq 0} \frac{(-1)^k t^{2k}}{(2k)!} \begin{pmatrix} (BB^T)^k & 0 \\ 0 & (B^TB)^k \end{pmatrix} \\ &+ i\sum_{k\geq 0} \frac{(-1)^k t^{2k+1}}{(2k+1)!} \begin{pmatrix} 0 & (BB^T)^kB \\ (B^TB)^kB^T & 0 \end{pmatrix} \end{aligned}$$

To simplify notation we write $U(t)$ in block form as

$$U(t) = \begin{pmatrix} F_1(t) & iK(t) \\ iK^T(t) & F_2(t) \end{pmatrix}.$$

We pay particular attention to the fact that $F_1(t)$, $F_2(t)$, and $K(t)$ are all real matrices for all times t. This observation leads to the following result, which appears in [30].

Lemma 5.2.1. *Suppose X is a bipartite graph on $n > 2$ vertices with transition matrix $U(t)$. If X admits uniform mixing at time t, then each entry of $\sqrt{n}U(t)$ is a fourth root of unity.*

Proof. If X admits uniform mixing at time t, then

$$|U(t)_{j,k}| = \frac{1}{\sqrt{n}}$$

for all $1 \leq j, k \leq n$. In terms of the blocks that comprise $U(t)$, this means that all of the entries of the real matrices $F_1(t)$, $F_2(t)$ and $K(t)$ are equal to $\pm 1/\sqrt{n}$. Hence all entries of $\sqrt{n}U(t)$ are fourth roots of unity. □

This observation can be used to rederive Kay's result [35] concerning the phase factors for perfect state transfer in bipartite graphs. This proof appears in [30].

Theorem 5.2.2. *If X is a bipartite graph on $n > 2$ vertices that admits uniform mixing, then n is divisible by four.*

Proof. Let $U(t)$ denote the transition matrix of X, and suppose that X admits uniform mixing at time t. By Lemma 5.2.1, we know that each entry of $U(t)$ must be a fourth root of unity.

Let Γ_1 and Γ_2 denote the two colours classes on X. For convenience, we assume that the vertices in Γ_1 correspond to the first $|\Gamma_1|$ rows of $U(t)$. Let D denote the diagonal matrix of order $n \times n$ such that

$$D_{u,u} = \begin{cases} 1 & \text{if } u \in \Gamma_1 \\ i & \text{if } u \in \Gamma_2. \end{cases}$$

Let H denote the matrix given by

$$H = \sqrt{n}DU(t)D.$$

In terms of the blocks of $U(t)$, we see that

$$H = \sqrt{n} \begin{pmatrix} F_1 & -K \\ -K^T & -C_2 \end{pmatrix}.$$

This implies that H is a real matrix with entries equal to 1 or -1. A straightforward computation also reveals that

$$HH^* = nDU(t)DD^*U(t)^*D^* = nI.$$

Therefore H is a real Hadamard matrix. It is well known that if H is a real Hadamard matrix of order n such that $n > 2$, then n is divisible by four. A proof of this fact is given in Chapter 18 of Van Lint and Wilson [49], for example. □

Adamczak et al. [1] show that if uniform mixing occurs on C_{2m}, then m must be a sum of two squares. Here we show that this is true for all regular bipartite graphs.

Theorem 5.2.3. *If X is a regular, bipartite graph with n vertices that admits uniform mixing, then n is the sum of two integer squares.*

Proof. Suppose X is a regular bipartite graph with transition matrix $U(t)$. Further suppose that X admits uniform mixing at time t. By Lemma 5.2.1, each of the entries of $\sqrt{n}U(t)$ is a fourth root of unity. In particular, this implies that

$$\sqrt{n}U(t)\mathbf{1} = (a + ib)\mathbf{1} \quad \text{and} \quad \sqrt{n}U(t)^*\mathbf{1} = (a - ib)\mathbf{1}$$

for some integers a and b where $\mathbf{1}$ is the all-ones vector. Taking the product of both of these expressions yields

$$nU(t)U(t)^*\mathbf{1} = (a - ib)(a + ib)\mathbf{1} = (a^2 + b^2)\mathbf{1}.$$

Since $U(t)$ is unitary, we know that $U(t)U(t)^* = I$. We conclude that $n = a^2 + b^2$. □

5.3 Even Cycles

In this section we narrow our focus to cycles of even length, which are precisely the bipartite cycles. Relying on our work from previous sections, we show that uniform mixing cannot occur on any even cycle other than C_4. This result appears in [30]. This is an extension of the work of Adamczak et al. [1], which shows that if uniform mixing occurs on C_{2m}, then m must be a sum of two squares.

Theorem 5.3.1. *The cycle C_4 is the unique even cycle that admits uniform mixing.*

Proof. First recall that C_4 admits uniform mixing at time $t = \pi/4$. Now we consider C_{2m} for $m \geq 3$ with transition matrix $U(t)$. Suppose for a contradiction that C_{2m} admits uniform mixing. From Theorem 5.2.2, it follows that m must be even, and so we must have $m \geq 4$. Furthermore, by Lemma 5.2.1, we see that each entry of $U(t)$ is algebraic. Theorem 4.2.5 implies that all of the eigenvalues of C_{2m} must be integers. This is a contradiction to Lemma 4.3.2, which shows that C_{2m} has an irrational eigenvalue if $m \geq 4$. □

We pause for a moment to appreciate the simplicity of the proof given above. This is our first illustration of the power of our main result from Chapter 4. We give another application of Theorem 4.2.5 in the next section, as we attack the more difficult case of cycles of odd prime order.

5.4 Prime Cycles

Dealing with odd cycles in general is a tricky matter. In this section we restrict our attention to cycles of odd prime order. There are two previously known results about the mixing properties of odd cycles. First, Ahmadi, Belk, Tamon, and Wendler show that C_3 admits uniform mixing [3]. This is a consequence of their work on complete graphs. Second, with considerably more effort, Carlson et al. show that uniform mixing does not occur on C_5 [16].

In this section we extend these two results to show that C_p does not admit uniform mixing for any prime p such that $p \geq 5$. This result is due to the author and appears in [30]. We rely on the framework of cyclic p-roots introduced in Section 4.7, along with our staple result: Theorem 4.2.5.

Theorem 5.4.1. *The cycle C_3 is the unique cycle of odd prime order that admits uniform mixing.*

Proof. Let p denote an odd prime such that $p \geq 5$, and let $U(t)$ denote the transition matrix of C_p. Suppose that C_p admits uniform mixing at time t. This implies that $\sqrt{n}U(t)$ is a type-II matrix that is a scalar multiple of a cyclic p-root. Haagerup's work, stated in this thesis as Theorem 4.7.2, shows that there are a finite such number of cyclic p-roots. Applying Theorem 4.6.1, we know that all of these cyclic p-roots must have algebraic coordinates. Therefore $U(t)$ must be a scalar multiple of a matrix with all algebraic entries. In turn, Theorem 4.2.5 implies that C_p must have all integral eigenvalues. This contradicts the fact that C_p has an irrational eigenvalue, which we proved in Lemma 4.3.2. □

One crucial fact that separates the prime cycle case from general cycles is Haagerup's result concerning the finiteness of cyclic p-roots. If we could show for some $n \geq 5$ that there are finite number of cyclic n-roots, then the machinery used above would be sufficient to show that uniform mixing does not occur on C_n. Unfortunately this does not seem to be the case if n is not a prime. For example, there are an infinite number of cyclic 9-roots [47].

An alternative approach to dealing with uniform mixing on general cycles might be to relate the transition matrix of C_n to the transition matrix C_p for some prime factor p such that p divides n. It might be possible to do this using graph quotients. We investigate graph quotients in Chapter 7.

5.5 ϵ-Uniform Mixing on Prime Cycles

In the last section we saw that uniform mixing does not occur on C_p when p is an odd prime greater than three. However, our proof does not give us any insight about whether or not the probability distribution of the quantum walk gets close to uniform. In this section, we show the probability distribution of a continuous-time quantum walk on C_p gets close to uniform at certain times. Graphs with this property are said to admit ϵ-uniform mixing. The work in this section is due to the author.

The fact that C_p admits ϵ-uniform mixing is interesting because it gives us more information about the nature of a continuous-time quantum walk on a cycle. Also, it confirms that we cannot bound the modulus of any entry of $U(t)$ away from $1/\sqrt{n}$. In a broad sense, it justifies the necessity of the more sophisticated approach that we took to deal with uniform mixing on C_p.

Throughout this section we rely on the notation and concepts introduced in Section 2.8. In particular, we let $\mathcal{A} = \{A_0, \ldots, A_d\}$ denote the cyclic association scheme on p vertices. Since p is an odd prime, we see that $\mathcal{A}$ has $d = (p-1)/2$ classes. We further let $\{E_0, \ldots, E_d\}$ denote the spectral idempotents of $\mathcal{A}$, and let Θ denote the discrete Fourier transform described in Section 2.9. Recall that the image of each spectral idempotent under the duality map is

$$\Theta(E_r) = A_r.$$

To begin our new work, we define

$$F = \sum_{r=0}^{d} \omega^{r^2} E_r, \tag{5.1}$$

where $\omega = e^{i2\pi/p}$.

Lemma 5.5.1. *The matrix F is a flat unitary matrix.*

Proof. First we verify that F is unitary. We do this by a direct computation. It is convenient to recall that

$$E_r^2 = E_r \quad \text{and} \quad E_r E_j = 0 \text{ if } r \neq j.$$

Using these observations we see that

$$FF^* = \left(\sum_{r=0}^{d} \omega^{r^2} E_r\right)\left(\sum_{r=0}^{d} \omega^{-r^2} E_r\right) = \sum_{r=0}^{d} E_r = I.$$

Next we use the duality map Θ to show that F is flat. Since Θ is linear, we have

$$\begin{aligned}
\Theta(F)\Theta(F^*) &= \left(\sum_{r=0}^{d} \omega^{r^2} \Theta(E_r)\right)\left(\sum_{r=0}^{d} \omega^{-r^2} \Theta(E_r)\right) \\
&= \left(\sum_{r=0}^{d} \omega^{r^2} A_r\right)\left(\sum_{r=0}^{d} \omega^{-r^2} A_r\right) \\
&= \left(\sum_{j=0}^{p-1} \omega^{j^2} C^j\right)\left(\sum_{j=0}^{p-1} \omega^{-j^2} C^j\right) \\
&= \sum_{k=0}^{p-1} \left(\sum_{j=0}^{p-1} w^{j^2-(k-j)^2}\right) C^k \\
&= \sum_{k=0}^{p-1} \omega^{-k^2} \left(\sum_{j=0}^{p-1} w^{jk}\right) C^k \\
&= pC^0 = pI.
\end{aligned}$$

By Corollary 2.9.4, we know that $\Theta(F)\Theta(F^*) = pI$ implies that

$$F \circ F^* = \frac{1}{p} J.$$

Therefore F is flat. □

Our goal is to show that $U(t)$ gets arbitrarily close to a complex scalar multiple of F as t ranges over all real numbers. Since F is a flat matrix, achieving this goal implies that C_p admits ϵ-uniform mixing. This result is due to the author and appears in [30]. The proof of this result relies heavily on Kronecker's Theorem and the ideas developed in Section 4.4.

Theorem 5.5.2. *The odd prime cycle C_p admits ϵ-uniform mixing.*

Proof. Let $U'(t)$ denote the scaled transition matrix given by

$$U'(t) = e^{-2it}U(t) = E_0 + e^{(\theta_1 - 2)it}E_1 + \cdots + e^{(\theta_d - 2)it}E_d. \tag{5.2}$$

Note that $U'(t)$ is a unitary matrix, and $U'(t)$ is flat if and only if $U(t)$ is flat. Let ϵ denote a positive real number. We proceed by showing that there exists some time t such that

$$||U'(t) - F|| < \frac{\epsilon}{2}.$$

We consider $U'(t)$ at times that are an integer multiple of $2\pi/p$. For any s in $\mathbb{Z}$, we see that Equation 5.2 becomes

$$U'(2s\pi/p) = \sum_{r=0}^{d} e^{2s(\theta_r - 2)\pi i/p}E_r.$$

In terms of e, we express Equation 5.1 as

$$F = \sum_{r=0}^{d} e^{2r^2\pi i/p}E_r.$$

Our goal is to find a time t such that the coordinates of F and $U'(t)$ are close to the same value. In terms of the exponents of these coefficients, this is equivalent to finding some integer s such that $\frac{1}{p}r^2 \approx \frac{1}{p}(\theta_r - 2)s$ in $(\mathbb{R}/\mathbb{Z})$ for $0 \le r \le d$. For two elements x and y in $\mathbb{R}/\mathbb{Z}$, we define the distance $|x - y|_{\mathbb{R}/\mathbb{Z}}$ to be

$$|x - y|_{\mathbb{R}/\mathbb{Z}} = \inf_{k \in \mathbb{Z}} |x - y - k|,$$

where the norm on the right hand side of the definition is the absolute value of $x - y - k$ considered as a real number.

From Theorem 4.3.5, we know that $1, \theta_1, \ldots, \theta_{d-1}$ are linearly independent over $\mathbb{Q}$, and consequently $\left\{1, \frac{1}{p}(\theta_1 - 2), \ldots, \frac{1}{p}(\theta_{d-1} - 2)\right\}$ is linearly independent over the rationals.

By Kronecker's Theorem (Theorem 4.4.1), we see that

$$D = \left\{ \left(\frac{1}{p}(\theta_1 - 2)s, \ldots, \frac{1}{p}(\theta_{d-1} - 2)s \right) : s \in \mathbb{Z} \right\}$$

is dense in $(\mathbb{R}/\mathbb{Z})^{d-1}$.

Therefore for any $\delta > 0$, we can find some s in $\mathbb{Z}$ such that

$$\left| \frac{1}{p}(\theta_r - 2)s - \frac{r^2}{p} \right|_{\mathbb{R}/\mathbb{Z}} < \delta \tag{5.3}$$

in $(\mathbb{R}/\mathbb{Z})$ for all $1 \le r \le d-1$. It remains to consider the coordinates of $U'(t)$ and F with respect to E_d. Recall that for a cyclic association scheme we have

$$\theta_d = -1 - \theta_1 - \theta_2 \cdots - \theta_{d-1}.$$

We can use this to derive an expression for the d-th coordinate of $U'(t)$ in terms of the first $d-1$ coordinates.

$$\begin{aligned}
\frac{1}{p}(\theta_d - 2)s &= \frac{1}{p}\left(-3 - \sum_{r=1}^{d-1} \theta_r\right) s \\
&= -\frac{1}{p}(2(d-1)+3)s - \sum_{r=1}^{d-1} \frac{1}{p}(\theta_r - 2)s \\
&= -s - \sum_{r=1}^{d-1} \frac{1}{p}(\theta_r - 2)s.
\end{aligned}$$

Now working in $\mathbb{R}/\mathbb{Z}$, we see that the exponent of the d-th coordinate of $U'(t) - F$ is

$$\begin{aligned}
\frac{1}{p}(\theta_d - 2)s - \frac{1}{p}d^2 &= -s - \sum_{r=1}^{d-1} \frac{1}{p}(\theta_r - 2)s - \frac{1}{p}d^2 &\quad (5.4)\\
&= \sum_{r=1}^{d-1} \left(\frac{1}{p}(\theta_r - 2)s - \frac{1}{p}r^2\right) + \frac{1}{p}\sum_{r=0}^{d} r^2. &\quad (5.5)
\end{aligned}$$

Note that

$$\frac{1}{p}\sum_{r=1}^{d} r^2 = \frac{d(d+1)(2d+1)}{6p} = \frac{(p-1)(p+1)}{24}$$

Since p is an odd prime, we know that both $p-1$ and $p+1$ are even, and exactly one of those values is divisible by 4. Therefore $(p-1)(p+1)$ is divisible by 8. Since we are assuming that $p \neq 3$, we also know that $p-1$ or $p+1$ is divisible by 3. It follows that

$$\frac{(p-1)(p+1)}{24} \in \mathbb{Z}.$$

must be an integer. We simplify Equation 5.4 in $\mathbb{R}/\mathbb{Z}$ to

$$\frac{1}{p}(\theta_d - 2)s - \frac{1}{p}d^2 = \sum_{r=1}^{d-1} \left(\frac{1}{p}(\theta_r - 2)s - \frac{1}{p}r^2 \right)$$

Now we use this expression and Inequality 5.3 to bound the coefficient d-th coordinate of $U'(t) - F$ in terms of δ as follows:

$$\left| \frac{1}{p}(\theta_d - 2)s - \frac{1}{p}d^2 \right|_{\mathbb{R}/\mathbb{Z}} \leq \sum_{r=1}^{d-1} \left| \frac{1}{p}(\theta_r - 2)s - \frac{1}{p}r^2 \right|_{\mathbb{R}/\mathbb{Z}} < (d-1)\delta.$$

This implies that for any $\epsilon > 0$, we can find a sufficiently small δ such that

$$||U'(2s\pi/p) - F|| < \frac{\epsilon}{2}.$$

By Lemma 4.4.3, it follows that

$$||U'(2s\pi/p) \circ U'(2s\pi/p)^* - \frac{1}{n}J|| < \epsilon.$$

Finally, we note that $U'(2s\pi/p) \circ U'(2s\pi/p)^* = U(2s\pi/p) \circ U(2s\pi/p)^*$, which proves that ϵ-uniform mixing occurs on C_p. □

We take note of several aspects of this proof. First, the matrix F is the dual of a Fourier-type matrix that is well-known to be flat and unitary. It is very possible that the same approach could be used with a different choice of a flat unitary matrix. Second, we see from Kronecker's Theorem that the first d eigenvalues of the transition matrix are essentially independent from each other. This tells us that the continuous-time quantum walk on C_p hits a wide range of probability distributions. One obvious drawback of this proof is that we do not have any insight into the time at which the probability distribution will be within ϵ of the uniform distribution.

Also, it is very possible that this proof could be generalized to show that ϵ-uniform mixing occurs on cycles of length p^2 for an odd prime p. However, more care is needed to choose a suitable flat unitary to approximate.

Finally, we note that Theorem 5.5.2 implies that the Cartesian product of cycles of prime length admit ϵ-uniform mixing. This yields an infinite family of non-cycles that admit ϵ-uniform mixing but do not admit uniform mixing.

Chapter 6

Strongly Regular Graphs

6.1 Introduction

In this chapter we consider uniform mixing on strongly regular graphs. We approach this problem via type-II matrices. We start by formulating a system of equations whose solutions correspond to type-II matrices in the Bose-Mesner algebra of a strongly regular graph. Then we summarize Godsil and Chan's classification of type-II matrices in Bose-Mesner algebras of strongly regular graphs [19]. Next we present Chan's further classification of flat type-II matrices, which are also known as scaled complex Hadamard matrices [17]. This leads to the characterization of strongly regular graphs that admit uniform mixing given in [30].

To provide a more in-depth understanding, we offer an alternative construction of the strongly regular graphs that admit uniform mixing. This construction is an unpublished result due to Godsil. We also a offer a new, direct proof that the Paley graph of order nine is the unique conference graph that admits uniform mixing.

6.2 Type-II Matrices and SRGs

Throughout this section we focus on the following question: given a particular strongly regular graph, is there a type-II matrix in its Bose-Mesner algebra? In 1970, Goethals and Seidel answered this question for flat type-II matrices with real entries [32]. These matrices are more commonly known as real Hadamard matrices, or simply Hadamard matrices. We phrase their result in the language of type-II matrices.

Theorem 6.2.1. *If X is a strongly regular graph with adjacency matrix A, then $\mathbb{R}[\mathcal{A}]$ contains a flat type-II matrix if and only if X is a Latin square-type or negative Latin square-type graph.* □

We begin our work on the general case by describing the affine varieties corresponding to type-II matrices in the Bose-Mesner algebra of a strongly regular graph. Suppose that X is a strongly regular graph with parameters (n, k, a, c). Let A and $\bar{A}$ denote the adjacency matrices of X and its complement, respectively. Recall that $\bar{A} = J - A - I$. Also recall from Section 2.3 that

$$\begin{aligned} A^2 &= kI + aA + c\bar{A} \\ \bar{A}^2 &= (n-k-1)I + (n-2k+c-2)A + (n-2k+a)\bar{A} \\ \bar{A}A &= (J-A-I)A = (k-a-1)A + (k-c)\bar{A} = A\bar{A}. \end{aligned}$$

Now further suppose that W is a matrix such that

$$W = I + xA + y\bar{A},$$

for some $x, y \neq 0$ in $\mathbb{C}$. In terms of these coefficients, we have

$$\begin{aligned} WW^{(-)T} &= \left(I + xA + y\bar{A}\right)\left(I + x^{-1}A + y^{-1}\bar{A}\right) \\ &= I + A^2 + \bar{A}^2 + (x + x^{-1})A + (y + y^{-1})\bar{A} + (xy^{-1} + x^{-1}y)\bar{A}A. \end{aligned}$$

Substituting in our expressions for A^2, $\bar{A}^2$ and $A\bar{A}$ above yields

$$WW^{(-)T} = nI + w_1 A + w_2 \bar{A}, \tag{6.1}$$

where we have

$$\begin{aligned} w_1 &= n - 2k + 2a + (k-a-1)(xy^{-1} + x^{-1}y) + x + x^{-1} \\ w_2 &= n - 2k + 2c - 2 + (k-c)(xy^{-1} + x^{-1}y) + y + y^{-1}. \end{aligned}$$

Note that $WW^{(-)T} = nI$ if and only if $w_1 = w_2 = 0$. We summarize this observation in the following result. This result appears in [19].

Lemma 6.2.2. *Let X denote a strongly regular graph with parameters (n, k, a, c). Let A and $\bar{A}$ denote the adjacency matrices of X and its complement, respectively. The matrix W given by*

$$W = I + xA + y\bar{A},$$

is a type-II matrix if and only if x and y satisfy the following system of polynomials.

$$n - 2k + 2a + (k-a-1)(xy^{-1} + x^{-1}y) + x + x^{-1} = 0 \tag{6.2}$$

$$n - 2k + 2c - 2 + (k-c)(xy^{-1} + x^{-1}y) + y + y^{-1} = 0. \tag{6.3}$$

These polynomial equations define a variety in $\mathbb{C}^2$. □

There is a significant amount of nontrivial work necessary to determine all of the solutions of the affine variety given in Lemma 6.2.2. This was accomplished by Godsil and Chan in [19].

Theorem 6.2.3. *Let X be a primitive strongly regular graph with parameters (n, k, a, c) and eigenvalues θ and τ such that $\theta > \tau$. Let A denote the adjacency matrix of X and $\bar{A}$ denote the adjacency matrix of its complement. Suppose*

$$W = I + xA + y\bar{A}.$$

Then W is a type-II matrix if and only if one of the following holds, where x and y are interchangeable:

(a) $y = x = \frac{1}{2}(2 - n \pm \sqrt{n^2 - 4n})$;

(b) $x = 1$ *and* $y = 1 + \frac{1}{2(k-\lambda)}\left(-n \pm \sqrt{n^2 - 4(k-\lambda)n}\right)$ *and $\bar{A}$ is the matrix of a symmetric $(n, \overline{k}, \lambda)$-design where $\overline{k} = n - k - 1$;*

(c) $x = -1$ *and* $y = \frac{1}{2}(\lambda \pm \sqrt{\lambda^2 - 4})$ *where* $\lambda = (1 + \theta\tau)^{-1}(2 - 2\theta\tau - n))$ *and A is the incidence matrix of a symmetric design;*

(d) $x + x^{-1}$ *is a zero of the quadratic* $z^2 - \alpha z + \beta - 2$ *with*

$$\alpha = \frac{1}{\theta\tau}[n(\theta + \tau + 1) + (\theta + \tau)^2],$$
$$\beta = \frac{1}{\theta\tau}[-n - n(1 + \theta + \tau)^2 + 2\theta^2 + 2\theta\tau + 2\tau^2]$$

and

$$y = \frac{1}{(x + x^{-1})}\left(\frac{\theta\tau x - 1}{(\theta + 1)(\tau + 1)}(x + x^{-1} - 2 + n) - (n - 2)x - 2\right);.$$

□

Note that some of the type-II matrices given in this theorem are not flat. For example, the coordinates given in Theorem 6.2.3 (a) satisfy

$$\left|\frac{1}{2}(2 - n + \sqrt{n^2 - 4n})\right| < 1 \quad \text{and} \quad \left|\frac{1}{2}(2 - n - \sqrt{n^2 - 4n})\right| > 1,$$

for $n > 4$. The type-II matrix with these coordinates is called the Potts model. In a subsequent paper, Chan determines all of the strongly regular graphs from Theorem 6.2.3 that contain flat type-II matrices in their Bose-Mesner algebra [17].

Theorem 6.2.4. *Let X denote a strongly regular graph with parameters (n, k, a, c) and eigenvalues θ and τ such that $\theta > \tau$. Let A and $\bar{A}$ denote the adjacency matrices of X and its complement, respectively, and suppose that W is a matrix such that*

$$W = 1 + xA + y\bar{A}$$

for some x, y in $\mathbb{C}$ with $|x| = |y| = 1$. The matrix W is a type-II matrix if and only if X has one of the following parameter sets (n, k, a, c):

(i) $(4\theta^2, 2\theta^2 - \theta, \theta^2 - \theta, \theta^2 - \theta)$

(ii) $(4\theta^2, 2\theta^2 + \theta, \theta^2 + \theta, \theta^2 + \theta)$

(iii) $(4\theta^2 - 1, 2\theta^2, \theta^2, \theta^2)$

(iv) $(4\theta^2 + 4\theta + 1, 2\theta^2 + 2\theta, \theta^2 + \theta - 1, \theta^2 + \theta)$

(v) $(4\theta^2 + 4\theta + 2, 2\theta^2 + \theta, \theta^2 - 1, \theta^2)$. □

The corresponding coordinates of the flat type-II matrices in the theorem above are the (x, y) solutions given in Theorem 6.2.3. In the next section, we will further distill these flat type-II matrices and determine which of them correspond to transition matrices of the corresponding graph.

6.3 Uniform Mixing on SRGs

In this section, we present a classification of strongly regular graphs that admit uniform mixing. This result is a continuation of Chan's work from the previous section, and it appears in [30]. In particular, this result determines which of the matrices listed in Theorem 6.2.4 are scalar multiples of the corresponding transition matrix.

Let X denote a strongly regular graph with parameters (n, k, a, c) and nontrivial eigenvalues θ and τ. Further let E_θ and E_τ denote the spectral idempotents corresponding to θ and τ, respectively. As usual, we have $E_0 = \frac{1}{n}J$. Recall that the transition matrix of X can be expressed as

$$U(t) = e^{kit}E_0 + e^{\theta it}E_\theta + e^{\tau it}E_\tau. \tag{6.4}$$

If X admits uniform mixing at time t, then $U(t)$ is a flat unitary. This implies that

$$U(t) = \frac{\gamma}{\sqrt{n}}H, \tag{6.5}$$

for some flat type-II matrix H and some γ in $\mathbb{C}$ such that $|\gamma| = 1$. The matrix H must be in the Bose Mesner algebra of X. Thus, if we suppose that uniform mixing occurs on X, then the transition matrix must satisfy

$$\begin{aligned} U(t) &= \tfrac{\gamma}{\sqrt{n}} \quad \left(I + xA + y\bar{A}\right) \\ &= \tfrac{\gamma}{\sqrt{n}} \quad ((1 + kx + (n-k-1)y)E_0 + (1 + \theta x + (-1-\theta)y)E_\theta \\ &\qquad +(1 + \tau x + (-1-\tau)y))E_\tau). \end{aligned} \tag{6.6}$$

By comparing Equation 6.6 and Equation 6.4, we obtain the following *characterizing equations*:

$$e^{kit} = \frac{\gamma}{\sqrt{n}}(1 + kx + (n-k-1)y) \tag{6.7}$$

$$e^{\theta it} = \frac{\gamma}{\sqrt{n}}(1 + \theta x + (-1-\theta)y) \tag{6.8}$$

$$e^{\tau it} = \frac{\gamma}{\sqrt{n}}(1 + \tau x + (-1-\tau)y). \tag{6.9}$$

For each of the possible parameter sets given in Theorem 6.2.4, the corresponding type-II matrices are in exponential form if and only if the characterizing equations above are satisfied. The following result determines which of the flat type-II matrices determined by Theorem 6.2.4 arise as a transition matrix of the underlying strongly regular graph. This result appears in [30]. The proof requires technical case-by-case analysis.

Theorem 6.3.1. *A primitive strongly regular graph X with adjacency matrix A has uniform mixing if and only if one of the following holds.*

(a) $J - 2A$ is a regular symmetric Hadamard matrix of order $4\theta^2$ with constant diagonal and positive row sum and θ is even.

(b) $J - 2A - 2I$ is a regular symmetric Hadamard matrix of order $4\theta^2$ with constant diagonal and positive row sum and θ is odd.

(c) The Paley graph of order nine, which has parameters $(9, 4, 1, 2)$. □

The proof of this result requires several technical details. One drawback of the proof is that it fails to shed much light on other mixing properties of the strongly regular graphs. Essentially the proof is a result about a very specific family of flat type-II matrices, rather than about the transition matrices themselves. It would be interesting to prove that uniform mixing cannot occur without resorting to the technical classification of type-II matrices given in Theorem 6.2.3. We partially accomplish this in Section 6.5 by giving a new, direct proof that the Paley graph of order nine is the unique conference graph that admits uniform mixing.

In the following section, we explicitly construct the graphs described in Theorem 6.3.1 (a) and (b) that admit uniform mixing. From this construction we directly verify that these graphs admit uniform mixing.

6.4 Construction from Hadamard Matrices

In this section we further explore the exceptional strongly regular graphs that admit uniform mixing. We give a construction of these graphs which makes their mixing properties more apparent. These constructions and observations are due to Godsil.

Let H denote an $n \times n$ symmetric real Hadamard matrix with constant diagonal and constant row sum. For any pair of distinct rows of H, the number of entries that are equal must be the same as the number of entries that are not equal. As a consequence, the order n must be even. The symmetry of H implies that

$$HH^T = H^2 = nI.$$

Therefore the eigenvalues of H are $\pm\sqrt{n}$. Let m_1 and m_2 denote the multiplicities of $\sqrt{n}$ and $-\sqrt{n}$, respectively, as eigenvalues of H. Since H is a real symmetric matrix, it is diagonalizable, and therefore the spectrum has order n.

For the moment, we assume that H has constant diagonal 1. This implies that $\operatorname{tr}(H) = n$, and so the sum of the eigenvalues with multiplicity is equal to n. Using this information we determine m_1 and m_2 in terms of n by solving the following system.

$$m_1 + m_2 = n \tag{6.10}$$

$$\sqrt{n}m_1 - \sqrt{n}m_2 = n. \tag{6.11}$$

This yields

$$m_1 = \frac{1}{2}\left(n + \sqrt{n}\right) \quad \text{and} \quad m_2 = \frac{1}{2}\left(n - \sqrt{n}\right).$$

On the other hand, if H has constant diagonal -1, then $\sqrt{n}$ is an eigenvalue with multiplicity m_2 and $-\sqrt{n}$ is an eigenvalue with multiplicity m_1. In either case, the multiplicities of H must be positive integers, and so we immediately deduce that n must be a perfect square.

Recall our assumption that H has constant row sum. This implies that the all-ones vector $\mathbf{1}$ is an eigenvector of H. Therefore we have either

$$H\mathbf{1} = \sqrt{n}\mathbf{1} \quad \text{or} \quad H\mathbf{1} = -\sqrt{n}\mathbf{1}.$$

Let ρ denote the eigenvalue of H corresponding to $\mathbf{1}$, and let A be the $\{-1, 0, 1\}$-matrix such that

$$A = \frac{1}{2}(J - H).$$

Note that if H has constant diagonal 1, then A is a symmetric $\{0, 1\}$-matrix. On the other hand, if H has constant diagonal -1, then $A - I$ is a symmetric $\{0, 1\}$-matrix. Our aim is to define a strongly regular graph with adjacency matrix A or $A - I$ depending on the sign of the diagonal of H. Thus we wish to determine the spectral decomposition of A. Since H has constant row sum, we immediately deduce that

$$A\mathbf{1} = \frac{1}{2}(n - \rho)\mathbf{1}.$$

As usual, we set $E_0 = \frac{1}{2}J$. Next we observe that

$$(\rho I - H)^2 = nI - 2\rho H + nI = 2\rho(\rho I - H)$$

and thus we have an idempotent

$$E_1 = \frac{1}{2\rho}(\rho I - H).$$

Next we compute the eigenvalue of A associated to E_1. Multiplying A by the all-ones vector yields

$$\frac{1}{2}(J - H)E_1 = \frac{1}{4\rho}\left(\rho J - \rho H - \rho J + nI\right) = \frac{1}{4}(\rho I - H) = \frac{\rho}{2}E_1.$$

This implies that the columns of E_1 are eigenvectors of A with eigenvalue $\rho/2$. Next we see that

$$\begin{aligned}(J - H)(I - E_0 - E_1) &= J - H - (n - \rho)E_0 - \rho E_1 \\ &= \rho E_0 - \frac{1}{2}(\rho I - H) - H \\ &= \rho E_0 - \frac{1}{2}H - \frac{\rho}{2}I\end{aligned}$$

$$= -\rho\left(I - E_0 - E_1\right).$$

Therefore the columns of $I - E_0 - E_1$ are eigenvectors for A with eigenvalue $-\rho/2$. Hence if we define E_2 to be

$$E_2 = I - E_0 - E_1,$$

then E_0, E_1, E_2 are the idempotents in the spectral decomposition of A. Now we suppose that H has constant diagonal one. As we saw earlier, A is a symmetric $\{0,1\}$-matrix with zeros down the diagonal. Hence A is the adjacency matrix of a graph X. Based on this spectral decomposition of A, we see that X has exactly two nontrivial eigenvalues, which implies that X is strongly regular. However, we do not actually need to use this property of X to see that uniform mixing occurs. Instead we deduce that uniform mixing occurs directly from the spectral decomposition.

Lemma 6.4.1. *Let H denote a symmetric real Hadamard matrix with constant diagonal 1 and constant row sum ρ. Let X denote the graph with adjacency matrix $\frac{1}{2}(J-H)$. Uniform mixing occurs on X at time $t = \frac{\pi}{\rho}$ if ρ is divisible by four.*

Proof. Let E_0, E_1 and E_2 denote the idempotents given above. Our earlier work shows that the spectral decomposition of A is

$$A = \frac{1}{2}(n-\rho)E_0 + \frac{1}{2}\rho E_1 - \frac{1}{2}\rho E_2.$$

Utilizing this spectral decomposition, we see that the transition matrix of X is

$$U(t) = e^{(n-\rho)it/2}E_0 + e^{\rho/2it}E_1 + e^{-\rho/2it}E_2.$$

Conveniently we note that $\frac{1}{\rho}H$ is a flat unitary, and

$$E_0 - E_1 + E_2 = I - 2E_1 = \frac{1}{\rho}H.$$

If $U(t)$ is a scalar multiple of $\frac{1}{\rho}H$, then we know that uniform mixing occurs. In terms of the coordinates of the spectral idempotents, $U(t)$ is a scalar multiple of $\frac{1}{\rho}H$ if and only if

$$e^{(n-\rho)it/2} = \gamma, \quad e^{\rho it/2} = -\gamma, \quad \text{and} \quad e^{-\rho it/2} = \gamma,$$

for some complex number γ such that $|\gamma| = 1$. This system is satisfied if

$$t = \pm\frac{\pi}{2} \quad \text{and} \quad \rho \equiv 0 \pmod 4.$$

This yields our desired result. □

The theorem above deals with the case when H had constant diagonal 1. Next we consider the case when H has constant row sum and constant diagonal -1. In this case $A-I$ is a symmetric $\{0,1\}$-matrix with zeros down the diagonal. Since $A-I$ has two nontrivial eigenvalues, it is the adjacency matrix of a strongly regular graph.

Lemma 6.4.2. *Let H denote a symmetric real Hadamard matrix with constant diagonal -1 and constant row sum ρ. Let X denote the graph with adjacency matrix $\frac{1}{2}(J-H-2I)$. Uniform mixing occurs on X at time $t=\pi/\rho$ if $\rho \equiv 2 \pmod 4$.*

Proof. In terms of our earlier notation, the adjacency matrix of X is $A-I$. Let E_0, E_1 and E_2 denote the idempotents given above. Our earlier work shows that the spectral decomposition of $A-I$ is

$$A-I=\frac{1}{2}(n-\rho-2)E_0+\frac{1}{2}(\rho-2)E_1-\frac{1}{2}(\rho+2)E_2.$$

Utilizing this decomposition, we see that the transition matrix of X is

$$U(t)=e^{(n-\rho-2)it/2}E_0+e^{(\rho-2)/2it}E_1+e^{-(\rho+2)/2it}E_2.$$

Again we recall that $\frac{1}{\rho}H$ is a flat unitary, and

$$E_0-E_1+E_2=I-2E_1=\frac{1}{\rho}H.$$

If $U(t)$ is a scalar multiple of $\frac{1}{\rho}H$, then we know that uniform mixing occurs. In terms of the coordinates of the spectral idempotents, $U(t)$ is a scalar multiple of $\frac{1}{\rho}H$ if and only if

$$e^{(n-\rho-2)it/2}=\gamma,\quad e^{(\rho-2)it/2}=-\gamma,\quad \text{and}\quad e^{(-\rho-2)it/2}=\gamma,$$

for some complex number γ such that $|\gamma|=1$. This system is satisfied if

$$t=\pi/2 \quad \text{and} \quad \rho\equiv 2 \pmod 4.$$

This yields our desired result. □

6.5 Conference Graphs, Revisited

In this section, we offer a new, direct proof that the only conference graph that admits uniform mixing is the Paley graph of order nine. This result was originally proved in [30], as we saw in the previous section. However, the proof relies on the classification of flat type-II matrices given in [17], which in turn relies on the classification given in [19]. The alternative proof we offer in this section cuts out some of these middle steps. Restricting to conference graphs enables us to take a few shortcuts.

We begin by recalling some useful facts about conference graphs. Recall that a strongly regular graph X with nontrivial eigenvalues θ and τ is a conference graph if $m_\theta = m_\tau$. Conference graphs correspond to the similarly named conference matrices, which were first studied by Belevitch [6]. The canonical examples of a conference graph are the Paley graphs.

Suppose that X is a conference graph of order n. Using the condition that $m_\theta = m_\tau$, we can compute the eigenvalues themselves. They are

$$\theta, \tau = \frac{-1 \pm \sqrt{n}}{2}, \tag{6.12}$$

with $\theta > \tau$, as usual. From this we see that any conference graph of order n must have the parameter set

$$(n, (n-1)/2, (n-5)/4, (n-1)/4).$$

From this we see that a strongly regular graph X is a conference graph if and only if X and $\overline{X}$ have the same parameters.

Next we mention two interesting results concerning the order of a conference graph. The first is a classical result due to Belevitch [6]. A simpler proof is given by Seidel and van Lint [48].

Lemma 6.5.1. *If X is a conference graph of order n, then $n \equiv 1 \pmod 4$ and n must be the sum of two squares.* □

The next result has an elementary proof, which is given in Godsil and Royle [31].

Lemma 6.5.2. *If X is a strongly regular graph on a prime number of vertices, then X is a conference graph.* □

The Paley graphs are examples of conference graphs on a prime power number of vertices, but it is more difficult to construct conference graphs for other orders. Mathon discovered a general construction for conference graphs of order pq^2 where p is the order of a conference graph and $q = p - 2$ is a prime power [39]. This construction yields 64 conference graphs on 45 vertices. These are the smallest known conference graphs on a non prime power number of vertices.

Now we turn our attention to flat type-II matrices in the Bose-Mesner algebras of conference graphs. The following lemma gives a direct proof of a result that could be inferred from the work in [19] and [17].

Theorem 6.5.3. *Let X denote a conference graph of order n, and let $\mathcal{A} = \{I, A, \bar{A}\}$ denote the corresponding association scheme. If W is a flat type-II matrix in $\mathbb{C}[\mathcal{A}]$ such that*

$$W = I + xA + y\bar{A},$$

for some complex numbers x and y with $|x| = |y| = 1$, then $x = y^{-1}$ and

$$x + x^{-1} = \frac{-2 \pm 2\sqrt{n}}{n-1}.$$

Proof. Let $c = (n-1)/4$. Substituting the parameters of a conference graph into Equation 6.1 gives us

$$WW^{(-)T} = nI + w_1 A + w_2 \bar{A},$$

with

$$\begin{aligned} w_1 &= 2c - 1 + c(xy^{-1} + x^{-1}y) + x + x^{-1} \\ w_2 &= 2c - 1 + c(xy^{-1} + x^{-1}y) + y + y^{-1}. \end{aligned} \tag{6.13}$$

Since W is type-II, we must have $w_1 = w_2 = 0$. Subtracting w_2 from w_1 yields

$$w_1 - w_2 = x + x^{-1} - y - y^{-1} = 0.$$

Since $|x| = |y| = 1$, this implies that either $x = y$ or $x = y^{-1}$. If $x = y$, then the first equation in (6.13) becomes

$$0 = 4c - 1 + x + x^{-1}.$$

However, $|x + x^{-1}| \leq 2$, and so if $n \geq 5$, then $c \geq 1$ and this equation has no solution. This implies that $x = y^{-1}$, and both equations in (6.13) become

$$0 = 2c - 1 + c(x^2 + x^{-2}) + x + x^{-1}.$$

Let $\rho = x + x^{-1}$. Since $|x| = 1$, we have $x^2 + x^{-2} = \rho^2 - 2$. Therefore, in terms of ρ, our equation above becomes

$$0 = c\rho^2 + \rho - 1.$$

This implies that

$$\rho = \frac{-1 \pm \sqrt{1+4c}}{2c} = \frac{-2 \pm 2\sqrt{n}}{n-1}. \qquad \square$$

This result tells us that a flat type-II matrix in the Bose-Mesner algebra of a conference graph must be a scalar multiple of a matrix with all algebraic entries. With this in mind, we show that uniform mixing does not occur on conference graphs with non-square number of vertices. This result is given in [30]. The self-contained proof below is due to the author.

Theorem 6.5.4. *If X is a conference graph on a non-square number of vertices, then X does not admit uniform mixing.*

Proof. Let X denote a conference graph on n vertices such that n is not a square. The nontrivial eigenvalues of X, which we computed in (6.12), are irrational. Suppose for a contradiction that uniform mixing occurs on X, or, equivalently, that there exists some time t such that $U(t)$ is a flat type-II matrix. Theorem 6.5.3 implies that any such flat type-II matrix must be a scalar multiple of a matrix with algebraic entries. Therefore Theorem 4.2.5 implies that uniform mixing cannot occur. $\square$

Now we consider conference graphs on a square number of vertices. These conference graphs have all integer eigenvalues. In order to show uniform mixing cannot occur on these graphs, we utilize the fact that the association schemes corresponding to conference graphs are formally self-dual. To be explicit about this duality, we define the following duality map. Let X denote a conference graph, and let $\mathcal{A} = \{I, A, \bar{A}\}$ denote the corresponding association scheme. Further let E_0, E_θ, and E_τ denote the spectral idempotents. For any matrix M in $\mathbb{C}[\mathcal{A}]$, we define a map Θ such that

$$\Theta(wE_0 + xE_\theta + yE_\tau) = wI + xA + y\bar{A}.$$

This is analogous to the duality map, namely the discrete Fourier transform, that we defined for cyclic association schemes. There are several interesting properties of this duality map, but we only focus on what we need for our purposes in this section. In particular, the following lemma is a very specific formulation of a more general result about the duality map.

Lemma 6.5.5. *Let X denote a conference graph on n vertices, and let A and $\bar{A}$ denote the adjacency matrices of X and its complement, respectively. Let M denote the matrix given by*

$$M = E_0 + xE_\theta + yE_\tau.$$

The matrix M is a flat unitary matrix if and only if its dual $\Theta(M)$ is a flat type-II matrix.

Proof. It is convenient to re-index the eigenvalues and idempotents of the scheme, because we have been using slightly different indexing for the special case of strongly regular graphs. Let $A_0 = I$, $A_1 = A$, and let $A_2 = \bar{A}$. Likewise, let $E_0 = \frac{1}{n}J$, $E_1 = E_\theta$, and let $E_2 = E_\tau$. Let $k = (n-1)/2$ denote the valency of X. In terms of these indices, the eigenvalues of the scheme are given by

$$P = \begin{pmatrix} 1 & k & k \\ 1 & \theta & \tau \\ 1 & \tau & \theta \end{pmatrix},$$

where $p_j(k) = P_{k,j}$ for $0 \leq k \leq 2$. Note that P is the change of basis matrix of $\mathbb{C}[\mathcal{A}]$ that sends A_j to E_j for $0 \leq j \leq 2$. It is straightforward to compute that the inverse of P is given by

$$P^{-1} = \frac{1}{n}\begin{pmatrix} 1 & k & k \\ 1 & \theta & \tau \\ 1 & \tau & \theta \end{pmatrix}.$$

Thus we have

$$P^2 = nI.$$

Note that the entries of P^{-1} are the dual eigenvalues of the scheme. Let $\mathbf{x} = (1, x, y)$ denote the coordinates of M with respect to $\{E_0, E_1, E_2\}$, and let $\mathbf{z} = (\alpha, \beta, \gamma)$ denote the coordinates of M with respect to $\{A_0, A_1, A_2\}$. In terms of P, we have

$$P\mathbf{z} = \mathbf{x}.$$

Our critical observation is that M is a flat unitary matrix if and only if

$$|x| = |y| = 1 \quad \text{and} \quad |\alpha| = |\beta| = |\gamma| = 1/\sqrt{n}. \tag{6.14}$$

However, the coordinates of $\Theta(M)$ with respect to $\{A_0, A_1, A_2\}$ are given by $\mathbf{x}$. This implies that the coordinates of $\Theta(M)$ with respect to $\{E_0, E_1, E_2\}$ are given by

$$P\mathbf{x} = P^2\mathbf{z} = n\mathbf{z}.$$

From this we deduce that $\Theta(M)$ is a flat type-II matrix if and only if the equations in (6.14) hold. □

Armed with this understanding of the duality of conference graphs, we show that conference graphs on a square number of vertices do not admit uniform mixing. Again, this result is given in [30]. The self-contained proof below is due to the author.

Theorem 6.5.6. *Suppose that X is a conference graph on $n = m^2$ vertices for some integer m. If X admits uniform mixing, then $n = 9$.*

Proof. Let X denote a conference graph on n vertices such that $n = m^2$ for some integer m. From Lemma 6.5.1, we know that $m \geq 3$. Let θ and τ denote the nontrivial eigenvalues of X with $\theta > \tau$. Recall from (6.12) that θ and τ are integers when n is square. Let $\mathcal{A} = \{I, A, \bar{A}\}$ denote the corresponding association scheme.

The transition matrix of X is given by

$$U(t) = e^{kit}E_0 + e^{\theta it}E_\theta + e^{\tau it}E_\tau,$$

where $k = (n-1)/2$ is the valency of X. Using Lemma 6.5.5, we see that $U(t)$ is a flat matrix if and only if

$$H = I + e^{(\theta-k)it}A + e^{(\tau-k)it}\bar{A}$$

is a flat type-II matrix. By Theorem 6.5.3, this restricts the possible values of the coordinates of H. In particular, the two nontrivial coordinates must be inverses of each other, which implies that

$$e^{(\theta-k)it}e^{(\tau-k)it} = e^{(-2k-1)it} = e^{-nit} = 1.$$

Therefore t must be an integer multiple of $2\pi/n$. Furthermore, Theorem 6.5.3 tells us that

$$e^{(\theta-k)it} + e^{(-\theta+k)it} = 2\cos(2(\theta-k)\alpha\pi/n) = \frac{-2 \pm 2\sqrt{n}}{n-1}$$

for some α in $\mathbb{Z}$. As a consequence, we see that $\cos(2(\theta-k)\alpha\pi/n)$ is a rational number. From the classical trigonometric result given in Theorem 4.3.1, we must have

$$\left(\frac{-1 \pm \sqrt{n}}{n-1}\right) \in \left\{0, \pm\frac{1}{2}, \pm 1\right\}.$$

However, using the fact that $n = m^2$, we see that we must have

$$\frac{-1+\sqrt{n}}{n-1} = \frac{1}{m+1} \quad \text{or} \quad \frac{-1-\sqrt{n}}{n-1} = \frac{-1}{m-1}.$$

We conclude that if $m > 3$, then H is not a flat type-II matrix. □

We note that the Paley graph of order nine is the unique conference graph of order nine. Therefore Theorem 6.5.6 implies that the Paley graph of order nine is the unique conference graph that admits uniform mixing.

If we suppose that X is a conference graph on a square number of vertices, then $U(t)$ is a periodic function. Therefore if X does not admit uniform mixing, it does not admit ϵ-uniform mixing. However, if X is a conference graph on a non square number of vertices, then ϵ-uniform mixing is possible. In fact, our proof of Theorem 6.5.4 hints that ϵ-uniform mixing is possible on all conference graphs of non square order. An approach using Kronecker's Theorem, similar to our work in Section 5.5, might be sufficient to prove this result.

Chapter 7

Products and Quotients

7.1 Motivation and Tools

Graph products are a useful tool for building graphs from other graphs. For our purposes in this thesis, we are interested in relating the mixing properties of a quantum walk on a product graph and its factors. It is well-known that the Cartesian product of a finite number of graphs admits uniform mixing if and only if each of its factors admits uniform mixing [7]. Our eventual goal is to derive necessary and sufficient conditions for a quotient of a graph to admit uniform mixing.

This chapter provides the necessary background to work with graph products and quotients. Suppose that A is an $n \times m$ matrix and B is a $u \times v$ matrix. Recall that the *tensor product* $A \otimes B$ is the block matrix with $n \times m$ blocks of size $u \times v$. The (j, k)-block is given by

$$(A \otimes B)_{j,k} = A_{j,k}B.$$

As we will see, the adjacency matrix of a Cartesian product of graphs can be expressed using tensor products. The following observation is due to Godsil. It is useful when considering quantum walks on Cartesian products of graphs.

Lemma 7.1.1. *If E and M are a pair of matrices such that $E^2 = E$, then*

$$\exp(M \otimes E) = I \otimes (I - E) + \exp(M) \otimes E.$$

Proof. Again starting from the definition of the exponential function, we express $\exp(M \otimes E)$ as follows.

$$\exp(M \otimes E) = I \otimes I + \sum_{k \geq 1} \frac{1}{k!} M^k \otimes E$$

$$= I \otimes I - I \otimes E + \sum_{k \geq 0} \frac{1}{k!} M^k \otimes E$$
$$= I \otimes (I - E) + \exp(M) \otimes E.$$

This is our desired expression. □

As an immediate consequence, we have the following corollary.

Corollary 7.1.2. *If $A(X)$ is the adjacency matrix of a graph X, then*

$$\exp(A(X)it \otimes I) = U_X(t) \otimes I,$$

where $U_X(t)$ is the transition matrix of X. □

This expression will be especially useful when we consider quantum walks on Cartesian products of graphs in Section 7.2.

7.2 Graph Products

In this section, we consider the direct product and Cartesian product of graphs. We relate the transition matrix of a direct product to the transition matrix of its factors. Then we see that the Cartesian product is a useful tool for constructing large graphs that admit uniform mixing.

Recall that the *direct product* two graphs $X = (V_1, E_1)$ and $Y = (V_2, E_2)$, denoted $X \times Y$, is a graph on vertex set $V_1 \times V_2$. Two vertices (u_1, v_1) and (u_2, v_2) in $V_1 \times V_2$ are adjacent if and only if

$$\{u_1, u_2\} \in E_1 \text{ and} \{v_1, v_2\} \in E_2.$$

Let $A(X)$ and $A(Y)$ denote the adjacency matrices of X and Y, respectively. The adjacency matrix of $X \times Y$ is given by the following.

$$A(X \times Y) = A(X) \otimes A(Y).$$

We relate transition matrices of $X \times Y$ and its factors, X and Y, in the following result. This result appears in [29].

Lemma 7.2.1. *Let $A(X)$ and $A(Y)$ denote the adjacency matrices of graphs X and Y, respectively. If A has spectral decomposition*

$$A = \sum_r \theta_r E_r,$$

then

$$U_{X \times Y}(t) = \sum_r E_r \otimes U_Y(\theta_r t).$$

Proof. To simplify our notation, let $A = A(X)$ and $B = A(Y)$. First,

$$A \otimes B = \sum_r \theta_r E_r \otimes B.$$

Since the matrices $E_r \otimes B$ commute, by Lemma 3.2.1 we see

$$U_{X \times Y}(t) = \prod_r \exp\left(it\theta_r E_r \otimes B\right).$$

Using Lemma 7.1.1, we have

$$U_{X \times Y}(t) = \prod_r \left((I - E_r) \otimes I + E_r \otimes U_Y(\theta_r t)\right). \tag{7.1}$$

Note that $E_r E_s = 0$ if $r \neq s$ and $\sum_r E_r = I$. Therefore $\prod_r (I - E_r) = 0$. Since the cross-terms vanish in (7.1), we obtain our desired result. □

Now we turn our attention to continuous-time quantum walks on Cartesian products of graphs. We pay close attention to the connection between uniform mixing and the Cartesian product.

First recall that the *Cartesian product* of two graphs $X = (V_1, E_1)$ and $Y = (V_2, E_2)$, denoted $X \,\square\, Y$, is a graph on vertex set $V_1 \times V_2$. Two vertices (u_1, v_1) and (u_2, v_2) in $V_1 \times V_2$ are adjacent if and only if

$$\{u_1, u_2\} \in E_1 \text{ and } v_1 = v_2 \quad \text{OR} \quad u_1 = u_2 \text{ and } \{v_1, v_2\} \in E_2.$$

For example, the Cartesian product $K_n \,\square\, K_n$ is isomorphic to $L(K_{n,n})$. In the next section, we will see that the Hamming graph $H(d, n)$ is the Cartesian product of d copies of K_n. The Cartesian product is commutative and associative; for all graphs X, Y, and Z we have

$$X \,\square\, Y = Y \,\square\, X \quad \text{and} \quad X \,\square\, (Y \,\square\, Z) = (X \,\square\, Y) \,\square\, Z.$$

Let $A(X)$ and $A(Y)$ denote the adjacency matrices of X and Y, respectively. The adjacency matrix $A(X \,\square\, Y)$ of the Cartesian product of X and Y is given by the following:

$$A(X \,\square\, Y) = A(X) \otimes I + I \otimes A(Y). \tag{7.2}$$

With this in mind, we compute an expression for the transition matrix of $X \,\square\, Y$ in terms of the transition matrices of X and Y. The following result is well-known.

Lemma 7.2.2. *Let $U_X(t)$ and $U_Y(t)$ denote the transition matrices of X and Y, respectively. The transition matrix of $X \square Y$ is given by*

$$U_{X\square Y}(t) = U_X(t) \otimes U_Y(t).$$

Proof. Since $A(X) \otimes I$ and $I \otimes A(Y)$ commute, by Lemma 3.2.1 we have

$$\begin{aligned} U_{X\square Y}(t) &= \exp(A(X \square Y)it) \\ &= \exp(A(X)it \otimes I + I \otimes A(Y)it) \\ &= \exp(A(X)it \otimes I) \exp(I \otimes A(Y)it). \end{aligned}$$

Now using Lemma 7.1.1, we simplify this expression.

$$\begin{aligned} &= (U_X(t) \otimes I)\,(I \otimes U_Y(t)) \\ &= U_X(t) \otimes U_Y(t). \end{aligned}$$

This is our desired expression. □

Next we prove the following result concerning uniform mixing on the Cartesian products of graphs. This result is well-known. It shows that we can build graphs that admit uniform mixing from smaller graphs that admit uniform mixing.

Lemma 7.2.3. *The graph product $X \square Y$ admits uniform mixing at time t if and only if X and Y both admit uniform mixing at time t.*

Proof. Recall from Lemma 7.2.2 that

$$U_{X\square Y}(t) = U_X(t) \otimes U_Y(t).$$

If $U_X(t)$ and $U_Y(t)$ are flat, then so is $U_{X\square Y}(t)$. Suppose, without loss of generality, that $U_X(t)$ is not flat. There exists coordinates (u, v) and (w, z) such that

$$|U_X(t)_{u,v}| \neq |U_Y(t)_{w,z}|.$$

Let α denote an arbitrary entry of $U_Y(t)$. Note that $\alpha U_X(t)_{u,v}$ and $\alpha U_Y(t)_{w,z}$ are entries of $U_{X\square Y}(t)$ with different moduli. Thus $U_{X\square Y}(t)$ is not flat. □

This result can be applied to Hamming graphs. Recall from Section 2.7, that the Hamming graph $H(d, n)$ is a Cayley graph over $\mathbb{Z}_n^d$. Two d-tuples are adjacent if and only if they differ in exactly one coordinate. Using graph products, we express the Hamming graph $H(d, n)$ as the Cartesian product of d copies of the complete graph K_n.

$$H(d, n) := K_n^{\square d}.$$

Let $U(t)$ denote the transition matrix of $H(d,n)$. Then by Lemma 7.2.2 we have

$$U(t) = U_{K_n}(t)^{\otimes d}.$$

The following result is due to Best et al. [7]. We reproduce their proof using our prior observations.

Theorem 7.2.4. *Uniform mixing occurs on $H(d,n)$ if and only if*

$$n \in \{2,3,4\}.$$

Proof. Lemma 7.2.3 tells us that $H(d,n)$ admits uniform mixing if and only if K_n admits uniform mixing. By Theorem 3.4.1 we know that K_n admits uniform mixing if and only if $n \in \{2,3,4\}$. □

We make an important observation: the proof above does not require an explicit expression for the transition matrix of the Hamming graph $H(d,n)$. It only relies upon Theorem 3.4.1, which determines the complete graphs that admit uniform mixing. For completeness, and for future use, we derive an expression for the transition matrix now. First recall from Section 3.4 that the transition matrix of the complete graph K_n is

$$U_{K_n}(t) = \frac{1}{n}\left(e^{(n-1)it} + (n-1)e^{-it}\right) I_n + \frac{1}{n}\left(e^{(n-1)it} - e^{-it}\right)(J_n - I_n).$$

Applying Lemma 7.2.2, we see that the transition matrix of the Hamming graph is

$$\begin{aligned} U(t) &= U_{K_n}(t)^{\otimes d} \\ &= \left(\frac{1}{n}\left(e^{(n-1)it} + (n-1)e^{-it}\right) I_n + \frac{1}{n}\left(e^{(n-1)it} - e^{-it}\right)(J_n - I_n)\right)^{\otimes d}. \end{aligned}$$

We identify the vertices of $H(d,n)$ with elements of $\mathbb{Z}_n^d$. From this expression, we see that the $(0,u)$-entry of the transition matrix is

$$U(t)_{0,u} = \frac{1}{n^d}\left(e^{(n-1)it} - e^{-it}\right)^{\mathrm{wt}(a)}\left(e^{(n-1)it} + (n-1)e^{-it}\right)^{d-\mathrm{wt}(u)}. \tag{7.3}$$

These expressions are particularly useful when we consider quotients of Hamming graphs.

7.3 Graph Quotients

As we saw in Section 7.2, the Cartesian product is a tool for building graphs that admit uniform mixing using smaller graphs that admit uniform mixing as building blocks. In this section we consider the converse approach: we start with a large graph that admits uniform mixing and then construct a quotient graph that also admits uniform mixing. This turns out to be a fruitful way to approach uniform mixing on Cayley graphs over $\mathbb{Z}_2^d$ and $\mathbb{Z}_3^d$. We will see why in the following section. For now we focus on building the necessary general tools.

There are several related concepts of graph quotients in the literature. We follow the treatment of quotients and equitable partitions given in Godsil and Royle [31]. Let X denote a graph, and let $\mathcal{B}$ denote a partition of $V(X)$ into cells $\{B_1, B_2, \ldots, B_r\}$.

Definition 7.3.1. *A partition $\mathcal{B}$ is an equitable partition if for every vertex v in a cell B_j, the number of neighbours of v in B_k is a constant number $b_{j,k}$.*

Note that j and k are not necessarily distinct, and so every cell B_j must induce a regular subgraph. If j and k are distinct, then the set of edges with exactly one end in B_j and one end in B_k induce a semi-regular bipartite graph.

The *quotient graph* of X induced by $\mathcal{B}$ is the directed graph on the cells of $\mathcal{B}$ such that there are $b_{j,k}$ arcs between cells B_j and B_k. Let $A(X/\mathcal{B})$ denote the matrix whose (j,k)-entry is $b_{j,k}$. We refer to this matrix as the adjacency matrix of the quotient $X/\mathcal{B}$. In general it will not be a $(0,1)$-matrix or a symmetric matrix. The *characteristic matrix* P of an equitable partition $\mathcal{B}$ is a $|V(X)| \times r$ matrix with the characteristic vectors of the cells of $\mathcal{B}$ as columns. The matrix $P^T P$ is a diagonal matrix whose (j,j)-entry is equal to $|B_j|$. Thus $P^T P$ is invertible. The following ideas appear in Section 9.3 of Godsil and Royle [31].

Lemma 7.3.2. *Let $\mathcal{B}$ denote an equitable partition of the graph X with characteristic matrix P. Let A and $\widehat{A}$ denote the adjacency matrices of X and $X/\mathcal{B}$, respectively. These adjacency matrices satisfy*

$$AP = P\widehat{A}. \tag{7.4}$$

Proof. Let n denote the number of vertices in X, and let r denote the number of cell in $\mathcal{B}$. Note that AP and $P\widehat{A}$ are both integral matrices of order $n \times r$. The columns of P are indexed by cells of $\mathcal{B}$. Thus the (j,k)-th cell of AP denotes the number of vertices in X that are neighbours of the vertex j and also contained in the cell B_k. In terms of the parameters of the partition, this number is $b_{j,k}$. Similarly, the (j,k)-th cell of $P\widehat{A}$ is

$$\left(P\widehat{A}\right)_{j,k} = \widehat{A}_{c,k}$$

where B_c is the cell containing vertex j. Recall that $\widehat{A}_{c,k} = b_{j,k}$. Since the indices j and k were chosen arbitrarily, we conclude that Equation 7.4 holds for the adjacency matrices. □

In a sense, we can view Lemma 7.3.2 as an algebraic definition of an equitable partition. The reason we are interested in equitable partitions, as opposed to other possible partitions, is that we need the intertwining property described in Equation 7.3.2. The existence of the $b_{j,k}$ parameters of the partition is equivalent to Equation 7.3.2 holding. Lemma 7.3.2 also gives us a convenient formulation of the adjacency matrix of the quotient in terms of the adjacency matrix of the graph.

Corollary 7.3.3. *Let $\mathcal{B}$ denote an equitable partition of the graph X with characteristic matrix P. Let A and $\widehat{A}$ denote the adjacency matrices of X and $X/\mathcal{B}$, respectively. These adjacency matrices satisfy*

$$\widehat{A} = (P^T P)^{-1} P^T AP.$$

Proof. Recall that $P^T P$ is an invertible matrix. Multiplying both sides of Equation 7.4 by P^T on the left yields our desired result. □

Equitable partitions arise naturally from the automorphism group of a graph. If we consider any group H of automorphisms of a graph X, then the orbits form an equitable partition. To see this, we consider two orbits u^H and v^H. The action of H fixes these orbits set-wise. Thus we immediately see that if u is adjacent to β vertices in the v^H, then every vertex in u^H must be adjacent to β vertices in v^H. This implies $\mathcal{C}$ is an equitable partition.

These observations can be applied to quotients of Cayley graphs. In particular, the following result is well-known. See Theorem 3 in Praeger's paper [42], for example. Note that in order to match our assumed definition of a quotient graph, we temporarily relax our definition of a Cayley graph to include multigraphs. This is necessary since we are interested in Cayley graphs of the form $X(G/N, CN/N)$ where CN/N is possibly a multiset.

Theorem 7.3.4. *Let G be a finite group, and suppose that C is an inverse-closed subset of $G \setminus \{1\}$. If N is a normal subgroup of a group G, then*

$$X(G, C)/N \cong X(G/N, CN/N),$$

where CN/N is defined to be the multiset of cosets given by

$$\{cN : c \in C\}$$

Proof. Since N is a subgroup of G, we can identify right multiplication by elements of N with an automorphism group of $X(G, C)$. By our earlier observation, we see that the orbits of N form an equitable partition. This implies the quotient $X(G, C)/N$ is well-defined. The orbits of N can be identified with the left and right cosets of N in G, and since N is normal, this set of cosets form a group. Thus the vertices of $X(G, C)/N$ can naturally be identified with elements of the quotient group G/N. Given two cosets aN and bN, we see that the number of arcs from aN to bN is determined by the number of elements in the set

$$\left\{n \in N : bna^{-1} \in C\right\}.$$

However bna^{-1} is in C if and only if $bN(aN)^{-1}$ is in CN/N. □

Quotients of Cayley graphs over a normal subgroup are called *normal quotients*. In this thesis, we are interested in quotients of abelian Cayley graphs. Since every subgroup of an abelian group is normal, this result applies to all of the quotient cases that we deal with.

Of course, our primary focus is still the transition matrices of the graphs we are considering. In particular, we wish to relate the transition matrix of a graph to the transition matrix of its quotient. Using Lemma 7.3.2, we obtain the following result, due to Ge et al. [26]. This result applies generally to all quotient graphs.

Theorem 7.3.5. *Let $\mathcal{B}$ be an equitable partition of the graph X with characteristic matrix P. Let A denote the adjacency matrix of X, and let $\widehat{A}$ denote the adjacency matrix of $X/\mathcal{B}$. The matrices satisfy the following.*

$$\exp(\widehat{A}it) = \left(P^T P\right)^{-1} P^T \exp(itA)P.$$

Proof. Repeated application of Lemma 7.3.2 yields

$$P \exp(\widehat{A}it) = P\left(\sum_{k\geq 0} \frac{(it)^k}{k!} \widehat{A}^k\right)$$

$$= \left(\sum_{k \geq 0} \frac{(it)^k}{k!} A^k P \right)$$

$$= \left(\sum_{k \geq 0} \frac{(it)^k}{k!} A^k \right) P.$$

Therefore the exponential functions satisfy

$$P \exp(\widehat{A} it) = \exp(itA) P.$$

Multiplying both sides by P^T yields the desired result. □

In this next section, we consider quotients of Hamming graphs as an illustration of our quotient theory. It turns out that when we quotient a Cayley graph over a subgroup, the potentially pesky diagonal matrix $\left(P^T P\right)^{-1}$ reduces to a scalar multiple of the identity, which simplifies our computations.

7.4 Quotients of Hamming Graphs

Recall that one of the main goals of this thesis is to find new examples of graphs that admit uniform mixing. With this in mind, we pay particular attention to the Hamming graphs $H(d, n)$. As we saw earlier, these graphs are known to admit uniform mixing if $n \in \{2, 3, 4\}$ [40]. In this chapter, we develop tools for determining when quotients of Hamming graphs admit uniform mixing.

To begin, we consider some subgroup of Γ of $\mathbb{Z}_n^d$. Note that $\mathbb{Z}_n^d$ can be partitioned into $n^d/|\Gamma|$ cosets of Γ. Let $\mathcal{C}$ denote this partition into cosets. Note that $\mathcal{C}$ is an equitable partition by the comments given in Section 7.3. Let P denote the characteristic matrix of the partition. Since each coset of Γ has the same size, we see that

$$P^T P = |\Gamma| I,$$

where I denotes the $n^r \times n^r$ identity matrix. This is a nice simplification of our expressions relating the adjacency and transition matrices of the graph and its quotient. Furthermore, if we impose some mild restrictions on Γ, then the adjacency matrix of the quotient graph $H(d, n)/\Gamma$ is a symmetric $(0, 1)$-matrix with zeros down the diagonal. In this case, the quotient graph is a simple, undirected graph.

Lemma 7.4.1. *If Γ is a subgroup of $\mathbb{Z}_n^d$ with minimum Hamming distance at least three, then the adjacency matrix of the quotient $H(d,n)/\Gamma$ is a symmetric $(0,1)$-matrix with zeros down the diagonal.*

Proof. Let H denote the adjacency matrix of $H(d,n)$, and let A denote the adjacency matrix of $H(d,n)/\Gamma$. From Corollary 7.3.3 and our comments above, these adjacency matrices satisfy

$$A_{j,k} = \frac{1}{|\Gamma|} P_j^T H P_k,$$

where P_j and P_j denote characteristic vectors of the j-th and k-th cell, respectively. Since each coset of Γ has distance greater than three, no pair of vertices in the same coset have a common neighbour. Therefore HP_k is a $(0,1)$-vector. Suppose that u is a vertex in the jth coset and v is a vertex in the kth coset. Since the partition induced by cosets of Γ is equitable, we know that if one vertex in the j-th coset has a neighbour in the k-th cell, then all of the vertices on the j-th coset have a neighbour in the k-th coset. In terms of the adjacency matrix H, this implies that for all j and k we have

$$P_j^T H P_k = \begin{cases} |\Gamma| & \text{if } u \sim v \text{ in } H(d,n) \\ 0 & \text{otherwise.} \end{cases}$$

Thus A is a $(0,1)$-matrix. In particular, since each coset induces an independent set in $H(d,n)$, we see that for all j

$$P_j^T H P_j = 0,$$

which implies A has zeros down the diagonal. Furthermore, since H is a symmetric matrix, we see that $P_j^T H P_k = P_k^T H P_j$, and so A is symmetric. □

We note that the above observation is equivalent to noting that two distinct cosets in $H(d,n)$ are either disconnected or the edges between them induce a perfect matching.

We turn our attention to the transition matrices. We assume that Γ is a subgroup of $\mathbb{Z}_n^d$ with minimum Hamming distance at least three. Let $U_H(t)$ and $U(t)$ denote the transition matrix of the Hamming graph $H(d,n)$ and the quotient graph $H(d,n)/\Gamma$, respectively. By Theorem 7.3.5, we know that

$$U(t) = \left(P^T P\right)^{-1} P^T U_H(t) P = \frac{1}{|\Gamma|} P^T U_H(t) P. \tag{7.5}$$

Moreover, from Theorem 7.3.4, we know that the quotient graph $H(d,n)/\Gamma$ is a Cayley graph and hence is vertex-transitive. Recalling

Lemma 3.2.5, we see that in order to determine the specific entries of $U(t)$, it suffices to consider the first row of $U(t)$.

Lemma 7.4.2. *Let Γ denote a subgroup of $\mathbb{Z}_n^d$ with Hamming distance at least three. The transition matrix of the quotient satisfies*

$$U(t)_{0,v+\Gamma} = \frac{1}{n^d} \sum_{u \in v+\Gamma} \left(e^{(n-1)it} + (n-1)e^{-it}\right)^{d-wt(u)} \left(e^{(n-1)it} - e^{-it}\right)^{wt(u)}.$$

Proof. Let P_0 and $P_{v+\Gamma}$ denote the characteristic vectors of the cosets Γ and $v+\Gamma$. Let U_H denote the transition matrix of the Hamming graph $H(d,n)$ at time t. Starting with Equation 7.5 and simplifying, we have

$$\begin{aligned} U(t)_{0,v+\Gamma} &= \frac{1}{|\Gamma|} P_0^T U_H P_{v+\Gamma} \\ &= \frac{1}{|\Gamma|} \sum_{a \in \Gamma} \sum_{b \in v+\Gamma} (U_H)_{a,b}. \end{aligned}$$

Now we apply Lemma 3.2.5 to the term $(U_H)_{a,b}$ to obtain the following.

$$\begin{aligned} U(t)_{0,v+\Gamma} &= \frac{1}{|\Gamma|} \sum_{a \in \Gamma} \sum_{b \in v+\Gamma} (U_H)_{0,b-a} \\ &= \frac{1}{|\Gamma|} \sum_{c \in v+\Gamma} |\Gamma| (U_H)_{0,c} \\ &= \sum_{c \in v+\Gamma} (U_H)_{0,c}. \end{aligned}$$

By recalling the expression given for $(U_H)_{0,c}$ in Equation 7.3, we arrive at our desired result. □

Now that we have a concrete expression for the entries of the transition matrix, we have a starting point for analyzing the mixing properties of quotients of Hamming graphs. We will thoroughly investigate uniform mixing on quotients of Hamming graphs in Chapter 8. For the remainder of the current chapter, we highlight the connection between quotients of $H(d,2)$ and $H(d,3)$ and Cayley graphs over $\mathbb{Z}_2^r$ and $\mathbb{Z}_3^r$, respectively.

7.5 Linear Graphs

In this section, we consider Cayley graphs over the additive group of a vector space. We are particularly interested in the cases when the additive group is isomorphic to $\mathbb{Z}_2^r$ or $\mathbb{Z}_3^r$. Our main result of this section is the proof of an unpublished result due to Godsil which shows that every linear Cayley graph over the additive group of a field is isomorphic to the quotient of a Hamming graph. We use this result to tie together our work in Section 7.4 with the theory of continuous-time quantum walks on Cayley graphs over $\mathbb{Z}_2^r$ and $\mathbb{Z}_3^r$. We begin by introducing linear graphs, which are a particular family of Cayley graphs.

Definition 7.5.1. *Suppose that G is the additive group of a vector space over a finite field. The Cayley graph $X(G, C)$ is a linear graph if and only if the connection set C is closed under multiplication by nonzero elements of the underlying finite field.*

Let p denote a prime, and let $\mathbb{F}_p$ denote the finite field of order p. Note that the elementary abelian p-group $\mathbb{Z}_p^r$ is isomorphic to the additive group of an r-dimensional vector space over $\mathbb{F}_p$. As we see in the next lemma, all Cayley graphs over $\mathbb{Z}_2^r$ and $\mathbb{Z}_3^r$ are linear graphs. This provides two infinite families of linear graphs.

Lemma 7.5.2. *A Cayley graph over $\mathbb{Z}_2^r$ or $\mathbb{Z}_3^r$ is a linear graph.*

Proof. Note that $\mathbb{Z}_2^r$ is isomorphic to the additive group of $\mathbb{F}_2^r$. Since $\mathbb{F}_2$ only has one nonzero element, the connection set of every Cayley graph over the additive group of $\mathbb{F}_2^r$ is trivially closed under multiplication by nonzero elements of $\mathbb{F}_2$.

Likewise, $\mathbb{Z}_3^r$ is isomorphic to the additive group of $\mathbb{F}_3^r$. By our definition of a Cayley graph, we implicitly assume that a Cayley graph $X(\mathbb{Z}_3^r, C)$ is undirected and hence C is closed under multiplication by 1 and -1. Thus it is closed under multiplication by the only two nonzero elements of $\mathbb{F}_3$. □

Once we extend our consideration to Cayley graphs over $\mathbb{Z}_5^r$, for example, we see that non-linear graphs are possible.

As we saw earlier, the Cayley graph $X(G, C)$ is connected if and only if its connection set C generates the entire group G. This leads to a useful observation about linear graphs: if G is the additive group of an r-dimensional vector space V, then $X(G, C)$ is connected if and only if C contains a basis for V. This implies that the connection sets of connected linear graphs must contain a basis of the underlying vector space. Note that if $X(G, C)$ is a disconnected linear graph, then each of its connected components will be linear graphs. For this reason it is sufficient to consider connected Cayley graphs.

For an r-dimensional vector space V, the general linear group $GL(V)$ is the set of all $r \times r$ invertible matrices. The next result reveals that Cayley graphs over G are isomorphic if their connection sets are images of each other under multiplication by an element of $GL(V)$.

Lemma 7.5.3. *Let G denote the additive group of vector space V, and let $X(G, C)$ denote a Cayley graph over G. For any nonzero matrix M in $GL(V)$, we have*

$$X(G, C) \cong X(G, MC),$$

where $MC = \{Mv : v \in C\}$.

Proof. We proceed by showing that left multiplication by M is a graph isomorphism from $X(G, C)$ to $X(G, MC)$. Since G is the additive group of V and M is in $GL(V)$, it follows that left multiplication by M is a permutation of G. Now suppose that u and v are two elements of G. From the invertibility of M, we immediately see that

$$u - v \in C \quad \text{if and only if} \quad M(u - v) = Mu - Mv \in MC.$$

Therefore left multiplication by M is a graph isomorphism. □

This lemma implies that every connected linear graph is isomorphic to a linear graph whose connection set contains the standard basis. Recall that if n is a prime power, then the Hamming graph $H(d, n)$ is a linear Cayley graph with nonzero scalar multiples of the standard basis vectors as its connection set. The following corollary characterizes linear graphs that are Hamming graphs.

Corollary 7.5.4. *Let G denote the additive group of a vector space V over a finite field $\mathbb{F}$ of dimension n. A linear graph $X(G, C)$ is isomorphic to the Hamming graph $H(d, n)$ if and only if C is the set of all nonzero scalar multiples of a basis of V.*

Proof. From our definition of a Hamming graph, we see that the Hamming graph $H(d, n)$ is isomorphic to the linear graph $X(G, C)$. On the other hand, suppose $X(G, C)$ is linear graph and C is the set of all nonzero scalar multiples of a basis of V. By Lemma 7.5.3, all such linear graphs are isomorphic to $H(d, n)$. □

Using this connectedness property, we see that certain linear Cayley graphs are isomorphic to quotients of Hamming graphs. This is an unpublished result due to Godsil.

Theorem 7.5.5. *Let G denote the additive group of a vector space V of dimension r over a finite field $\mathbb{F}$ of order n. For every connected linear graph $X(G,C)$ with valency $(n-1)d$, there exists a subgroup Γ of $\mathbb{Z}_n^d$ such that*

$$X(G,C) \cong H(d,n)/\Gamma,$$

where $|\Gamma| = n^{d-r}$ and Γ has Hamming distance at least three.

Proof. We assume that $X(G,C)$ is an arbitrary connected linear graph, and therefore C contains a basis of V. If C is precisely the set of all nonzero scalar multiples of a basis, then by Corollary 7.5.4 we know that $X(G,C)$ is isomorphic to $H(r,n)$. Thus we assume that $d > r$. Since X is linear we can partition C into equivalence classes $\{C_1, \dots, C_d\}$ such that

$$x, y \in C_j \quad \text{if and only if} \quad x = \alpha y \quad \text{for some } \alpha \in \mathbb{F}.$$

For notational convenience, we assume that the first r cells $C_1, \dots, C_r$ contain the nonzero scalar multiples of a basis of V. Let W denote a vector space of dimension $d-r$ over $\mathbb{F}$. We wish to lift the vectors in C to vectors in the direct product space $V \times W$, and so we consider the following injective map from C into $V \times W$.

$$\phi(v) = \begin{cases} (v,0) & \text{if } v \in C_j \text{ for } j \in \{1,\dots,r\} \\ (v,e_j) & \text{if } v \in C_{r+j} \text{ for } j \in \{r+1,\dots,d\}, \end{cases}$$

where $\{e_1, \dots, e_{d-r}\}$ is a basis of W. Now we define C_M to be the following set of $(p-1)d$ vectors in $V \times W$:

$$C_M = \{\phi(v) : v \in C\}.$$

By design, we see that C_M is the set of nonzero scalar multiples of a basis of $V \times W$. Let H denote the additive group of the vector space W. By Corollary 7.5.4 we know that the graph $X(G \times H, C_M)$ is a Hamming graph, or more precisely

$$X(G \times H, C_M) \cong H(d,n). \tag{7.6}$$

However, Theorem 7.3.4 implies that

$$X(G \times H, C_M)/H \cong X(G \times H/H, C_M H/H) \cong X(G,C).$$

Piecing together these observations, we conclude that

$$X(G, C) \cong H(d, n)/\Gamma.$$

We note that Γ is the image of H under the appropriate change of basis map, and so $|\Gamma| = n^{d-r}$. Moreover, since the adjacency matrix of $X(G, C)$ is a $(0, 1)$-adjacency matrix, we conclude that Γ must have Hamming distance at least three. □

This leads us directly to the following two corollaries.

Corollary 7.5.6. *Every connected, undirected Cayley graph over $\mathbb{Z}_2^r$ with valency d is a graph quotient $H(d, 2)/\Gamma$ for some subspace Γ such that $|\Gamma| = 2^{d-r}$ and Γ has minimum Hamming distance at least three.* □

Corollary 7.5.7. *Every connected, undirected Cayley graph over $\mathbb{Z}_3^r$ with valency $2s$ is a graph quotient $H(d, 3)/\Gamma$ for some subspace Γ such that $|\Gamma| = 3^{d-r}$ and Γ has minimum Hamming distance at least three.* □

We note that the proof of Theorem 7.5.5 that we give above is constructive. Not only does the proof show that linear graphs are quotients of Hamming graphs, but it gives us a recipe for constructing the corresponding quotient.

Chapter 8

Quotients of Hamming Graphs

8.1 Introduction

The binary Hamming graphs were the first graphs that were shown to admit uniform mixing [40]. This motivates us to consider uniform mixing on quotients of Hamming graphs. As an extra incentive, we keep in mind Corollaries 7.5.7 and 7.5.7, which state that a connected Cayley graph over $\mathbb{Z}_2^d$ and $\mathbb{Z}_3^d$ is a quotient graph of $H(d,2)$ or $H(d,3)$, respectively.

In this section we see that the quotient viewpoint is fruitful for finding new infinite families that admit uniform mixing. We begin by considering quotients over $H(d,2)$. These are the so-called cubelike graphs. Uniform mixing on these graphs has been well-studied. Using a quotient approach, we reproduce a result due to Fan and Luo [24] that characterizes the cubelike graphs that admit uniform mixing at time $t = \pi/4$. Applying this characterization it is possible to rediscover a result of Best et al. [7] that determines the folded d-cubes that admit uniform mixing at time $t = \pi/4$. Theorem 8.3.7 is an extension of these results about cubelike graphs. It is a new result due to the author.

We also investigate quotients of $H(d,n)$ for $n \geq 3$. This work is new. Most notably, we characterize quotients of $H(d,3)$ and $H(d,4)$ that admit uniform mixing at times $t = 2\pi/9$ and $t = \pi/4$, respectively. As a consequence of this characterization, we describe new infinite families of Cayley graphs over $\mathbb{Z}_3^d$ and $\mathbb{Z}_4^d$ that admit uniform mixing. Our approach is less fruitful when we consider quotients over $H(d,n)$ for $q \geq 5$. For these cases we give a convenient reformulation of the entries of the corresponding transition matrix, and we give some necessary conditions for uniform mixing to occur on quotients of $H(d,n)$ at time π/n.

Throughout this chapter, it is useful to bear in mind the following result due to Chan [18].

Theorem 8.1.1. *The Bose-Mesner algebra of the Hamming scheme $\mathcal{H}(d,n)$ contains a flat type-II matrix if and only if $n \in \{2,3,4\}$.* □

Consequently, any graph with an adjacency matrix in the Bose-Mesner algebra of $H(d,n)$ for $n \geq 5$, does not admit uniform mixing. However, graph quotients of $H(d,n)$ with n^s vertices will not necessarily have adjacency matrices in the Bose-Mesner algebra of $H(s,n)$.

8.2 Linear Codes

In this section we emphasize the connection between the entries of the transition matrix and the weight enumerator of the related linear code. We apply MacWilliams Theorem to obtain a useful reformulation of the entries of the transition matrix of the Hamming graph $H(d,n)$ when n is a prime.

Let $\mathbb{F}_n$ denote a finite field of order n. Recall that a *linear code* of length d is a linear subspace C of $\mathbb{F}_n^d$. Let $\langle \cdot, \cdot \rangle$ denote the non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$ from $\mathbb{F}_n^d \times \mathbb{F}_n^d \to \mathbb{F}_n$ defined by

$$\langle x, y \rangle = \sum_{j=1}^{d} x_j y_j,$$

for $x = (x_1, \dots, x_d)$ and $y = (y_1, \dots, y_d)$ in $\mathbb{F}_n^d$. The *dual code* $C^\perp$ is the subspace given by

$$C^\perp = \{y \in \mathbb{F}_n^d : \langle x, y \rangle = 0, \text{for all } x \in C\}.$$

Let C denote a $[d,r]$-linear code over $\mathbb{F}_n$, and let c_j denote the number of codewords in C with weight j. Recall that the *homogeneous weight enumerator* of C is given as

$$W_C(x,y) = \sum_{j=0}^{d} c_j x^{d-j} y^j.$$

We note that $W_C(x,y)$ is contained in $\mathbb{Z}[x,y]$. Next we let $c_j^\perp$ denote the number of codewords in the dual code $C^\perp$ with weight j. The homogenous weight enumerator of $C^\perp$ is

$$W_{C^\perp}(x,y) = \sum_{j=0}^{d} c_j^\perp x^{d-j} y^j.$$

Using this notation we state MacWilliams' Theorem for linear codes. See [38] for further information on MacWilliams' Theorem.

Theorem 8.2.1. *Let C be an $[d,r]$-linear code over $\mathbb{F}_n$. The weight enumerator of the dual code $C^\perp$ satisfies the following.*

$$W_{C^\perp}(x,y) = \frac{1}{n^r} W_C(x+(n-1)y, x-y). \qquad \square$$

If n is a prime, then $\mathbb{Z}_n$ is a finite field and Theorem 8.2.1 applies to the diagonal terms. This enables the following simplification of the diagonal terms in terms of $\Gamma^\perp$.

Lemma 8.2.2. *Let p denote a prime, and let Γ denote a subgroup of $\mathbb{Z}_p^d$ with minimum distance three such that $|\Gamma| = p^s$. The diagonal entries of the transition matrix of $H(d,p)/\Gamma$ are equal to*

$$\frac{e^{d(p-1)it}}{p^{d-s}} \sum_{a\in\Gamma^\perp} \left(e^{-pit}\right)^{wt(a)}.$$

Proof. Starting from Lemma 7.4.2 and applying Theorem 8.2.1 we obtain the following expression for $(0, 0+\Gamma)$-entry of the transition matrix of $H(d,p)/\Gamma$.

$$\begin{aligned}
U(t)_{0,0} &= \frac{1}{p^d} \sum_{a\in\Gamma} \left(e^{(p-1)it} + (p-1)e^{-it}\right)^{d-\mathrm{wt}(a)} \left(e^{(p-1)it} - e^{-it}\right)^{\mathrm{wt}(a)} \\
&= \frac{1}{p^d} W_\Gamma(e^{(p-1)it} + (p-1)e^{-it}, e^{(p-1)it} - e^{-it}) \\
&= \frac{1}{p^{d-s}} W_{\Gamma^\perp}(e^{(p-1)it}, e^{-it}) \\
&= \frac{1}{p^{d-s}} \sum_{a\in C^\perp} e^{(p-1)(d-\mathrm{wt}(a))it} e^{-\mathrm{wt}(a)it} \\
&= \frac{e^{d(p-1)it}}{p^{d-s}} \sum_{a\in C^\perp} \left(e^{-pit}\right)^{\mathrm{wt}(a)}.
\end{aligned}$$

Finally, recall that the diagonal of $U(t)$ is constant. $\square$

One shortcoming of this theorem is that it only applies to the diagonal terms of the transition matrix. However, recall that for the complete graphs K_n and Hamming graphs $H(d,n)$, it is sufficient to consider the diagonal term to show that uniform mixing does not occur if $n \geq 5$. Similarly, Lemma 8.2.2 is useful for showing that uniform mixing cannot occur on certain quotient graphs. We formalize the implicit necessary condition in the following corollary.

Corollary 8.2.3. *Let p denote a prime, and let Γ denote a subgroup of $\mathbb{Z}_p^d$ with minimum distance three such that $|\Gamma| = p^s$. If uniform mixing occurs on $H(d,p)/\Gamma$ at time t, then*

$$\left| \sum_{a \in \Gamma^\perp} \left(e^{-pit}\right)^{wt(a)} \right|^2 = p^{d-s}.$$

Proof. If uniform mixing occurs on $H(d,p)/\Gamma$, then $|U(t)_{0,0}|^2 = 1/p^{d-s}$. From Lemma 8.2.2, we see that

$$\begin{aligned} |U(t)_{0,0+\Gamma}|^2 &= \left| \frac{e^{d(p-1)it}}{p^{d-s}} \right|^2 \left| \sum_{a \in \Gamma^\perp} \left(e^{-pit}\right)^{\mathrm{wt}(a)} \right|^2 \\ &= \frac{1}{p^{2(d-s)}} \left| \sum_{a \in \Gamma^\perp} \left(e^{-pit}\right)^{\mathrm{wt}(a)} \right|^2 \end{aligned}$$

Therefore uniform mixing occurs if and only if the modulus squared on the right hand side is equal to p^{d-s}. □

The following sections deal with quotients of $H(d,n)$ separately based on the value of n. When n is a prime, this result can be applied to eliminate the possibility of uniform mixing at certain times.

8.3 Cubelike Graphs

Cayley graphs over $\mathbb{Z}_2^d$ are called *cubelike graphs*. By Theorem 7.5.6, we know that any Cayley graph over $\mathbb{Z}_2^d$ is isomorphic to a quotient graph $H(d,2)/\Gamma$ for an appropriate choice of Γ. In this section we investigate uniform mixing on cubelike graphs using a quotient perspective. From this perspective we give an alternative proof of Theorem 8.3.4, which is originally due to Fan and Luo [24]. As an application of this theorem, we can determine the folded d-cubes that admit uniform mixing at time $t = \pi/4$, which is the time at which the Hamming graph $H(d,2)$ admits uniform mixing. This result was originally proved by Best et al. for all times t [7]. We extend this result to quotients of the form $H(d,2)/\Gamma$ at time $t = \pi/4$ where $|\Gamma| = 4$. This result is due to the author. Finally, we briefly describe Chan's work in [18], which characterizes certain cubelike graphs whose adjacency matrix is in the Bose-Mesner algebra of the Hamming scheme $\mathcal{H}(d,2)$.

We begin by computing a convenient expression for the entries of the transition matrix of a quotient of a binary Hamming graph.

Lemma 8.3.1. *Let $H(d,2)$ denote the binary Hamming graph on $\mathbb{Z}_2^d$, and let Γ denote a subgroup of $\mathbb{Z}_2^d$ with minimum distance at least 3. If t is not equal to an odd multiple of $\pi/2$, then the $(0,v+\Gamma)$-entry of the transition matrix of $\mathbb{Z}_2^d/\Gamma$ is given by*

$$U(t)_{0,v+\Gamma} = \cos(t)^d \sum_{a\in v+\Gamma} (i\tan(t))^{wt(a)}.$$

Proof. Applying Lemma 7.4.2, we can express the $(0,v+\Gamma)$-entry of the transition matrix as

$$\begin{aligned} U(t)_{0,v+\Gamma} &= \frac{1}{2^d}\sum_{a\in v+\Gamma}\left(e^{it}-e^{-it}\right)^{\mathrm{wt}(a)}\left(e^{it}+e^{-it}\right)^{d-\mathrm{wt}(a)} \\ &= \cos(t)^d \sum_{a\in v+\Gamma}(i\sin(t))^{\mathrm{wt}(a)}\cos(t)^{-\mathrm{wt}(a)} \\ &= \cos(t)^d \sum_{a\in v+\Gamma}(i\tan(t))^{\mathrm{wt}(a)}. \end{aligned}$$

This yields our desired result. □

Recall that uniform mixing occurs on $H(d,2)$ at time $t=\pi/4$. We consider the distribution of the quotient at the same time. This will depend on the weights of elements in the cosets of Γ in $\mathbb{Z}_2^d$, and therefore we introduce some convenient notation to keep track of these weights.

Definition 8.3.2. *For a particular coset $v+\Gamma$ in $\mathbb{Z}_2^d$, let n_j denote the number of elements a in $v+\Gamma$ such that $wt(a)\equiv j \pmod 4$.*

It is also useful to recall that the parity of the weight of the sum of two vectors in $\mathbb{Z}_2^d$ can be determined from the parities of the summands. This elementary observation is given in the following lemma.

Lemma 8.3.3. *For any pair of vectors u,v in $\mathbb{Z}_2^d$, the following holds.*

$$wt(v+u) = wt(v) + wt(u) - 2|\operatorname{supp}(v)\cap\operatorname{supp}(u)|.$$ □

With this language we characterize quotients of $H(d,2)$ that admit uniform mixing at time $t = \pi/4$. This result was originally proved by Fan and Luo [24]. We offer a simpler proof using our quotient approach.

Theorem 8.3.4. *Let Γ denote a subgroup of $\mathbb{Z}_2^d$ with minimum distance at least three. Uniform mixing occurs on $H(d,2)/\Gamma$ at time $t = \pi/4$ if and only if the weight distribution of every coset of Γ satisfies*

$$(n_0 - n_2)^2 + (n_1 - n_3)^2 = |\Gamma|. \tag{8.1}$$

Proof. From Lemma 8.3.1 we see that

$$\begin{aligned} |U(\pi/4)_{0,v+\Gamma}|^2 &= \cos(\pi/4)^{2d} \left| \sum_{a \in v+\Gamma} (i \tan(\pi/4))^{\mathrm{wt}(a)} \right|^2 \\ &= \frac{1}{2^d} \left| \sum_{a \in v+\Gamma} i^{\mathrm{wt}(a)} \right|^2 \\ &= \frac{1}{2^d} \left| (n_0 - n_2) + i(n_1 - n_3) \right|^2 \\ &= \frac{1}{2^d} \left((n_0 - n_2)^2 + (n_1 - n_3)^2 \right). \end{aligned}$$

Since $H(d,2)/\Gamma$ is a graph on $2^d/|\Gamma|$ vertices, we know that uniform mixing occurs on $H(d,2)/\Gamma$ if and only if

$$|U(\pi/4)_{0,v+\Gamma}|^2 = \frac{|\Gamma|}{2^d}.$$

for every coset $v + \Gamma$. Therefore uniform mixing occurs if and only if Equation 8.1 holds for every coset. □

Utilizing some elementary number theory we deduce more information about the weight distribution of Γ for any quotient graph $H(d,2)$ that admits uniform mixing.

Corollary 8.3.5. *Suppose that Γ is a subgroup of $\mathbb{Z}_2^d$ of order 2^s with minimum distance at least three. Based on the parity of s, the following conditions determine whether or not $H(d,2)/\Gamma$ admits uniform mixing.*
If s is odd, the quotient graph $H(d,2)/\Gamma$ admits uniform mixing at time $t = \pi/4$ if and only if every coset satisfies

$$|n_0 - n_2| = |n_1 - n_3| = 2^{(s-1)/2}.$$

If s is even, $H(d,2)/\Gamma$ admits uniform mixing at time $t=\pi/4$ if and only if every coset satisfies

$$|n_0-n_2|=0, |n_1-n_3|=2^{s/2} \quad \text{or} \quad |n_0-n_2|=2^{s/2}, |n_1-n_3|=0.$$

Proof. If s is odd, then 2^s is not a square. In this case, 2^s is a sum of two squares if and only if each square is equal to 2^{s-1}. On the other hand, if s is even, then s^2 is a square. Thus one of the squares is equal to 2^s, and the other square is equal to 0. □

One major shortcoming to Theorem 8.3.4 is that in order to prove that uniform mixing occurs, the weight distribution of *every* coset of Γ needs to be computed.

As an immediate consequence of Theorem 8.3.4, we detect several obvious families of quotients that admit uniform mixing. The first family is the folded d-cubes, which are isomorphic to $H(d,2)/\langle \mathbf{1} \rangle$ for $d \geq 3$. These were shown to admit uniform mixing by Best, Kliegl, Mead-Gluchacki, and Tamon [7]. We note that the folded d-cube is isomorphic to the graph obtained from $H(d-1,2)$ by joining pairs of vertices at distance $d-1$. The Clebsch graph is an example of a folded 5-cube.

Theorem 8.3.6. *If $d \geq 3$, then the quotient graph $H(d,2)/\langle \mathbf{1} \rangle$ admits uniform mixing at time $t=\pi/4$ if and only if d is odd.*

Proof. Since $\Gamma = \langle \mathbf{1} \rangle$, we have $s=1$ in terms of our notation above. We consider each of the possible parities of d separately.
(a) $d \equiv 0 \pmod 2$

If d is also divisible by 4, then Γ satisfies

$$n_0=2, n_1=n_2=n_3=0,$$

and Equation 8.1 is not satisfied. If d is not divisible by 4, then Γ satisfies

$$n_0=n_2=1, n_1=n_3=0,$$

and again Equation 8.1 is not satisfied. Theorem 8.3.4 implies that uniform mixing does not occur if d is even.
(b) $d \equiv 1 \pmod 2$
The subgroup Γ contains one vector with weight zero and one vector of odd weight. In particular, Γ satisfies $n_0=1$, $n_2=0$, and $|n_1-n_3|=1$. Thus

$$(n_0-n_2)^2+(n_1-n_3)^2=2,$$

and so Equation 8.1 is satisfied. For any vector v in $\mathbb{Z}_2^d$, the coset of $v + \Gamma$ contains exactly one vector of even weight and one vector of odd weight. Thus regardless of the weight of v, we will have

$$|n_0 - n_2| = 1 \quad \text{and} \quad |n_1 - n_3| = 1,$$

and so Equation 8.1 is satisfied for every coset $v + \Gamma$. Using Theorem 8.3.4, we conclude that $H(d, 2)/\langle \mathbf{1} \rangle$ admits uniform mixing if and only if d is odd. □

Every $(d + 1)$-regular connected Cayley graph over $\mathbb{Z}_2^d$ can be expressed as a Cartesian product of a cube and a folded Hamming graph. In this light, Theorem 8.3.6 characterizes all of the $(d + 1)$-regular connected Cayley graphs over $\mathbb{Z}_2^d$ that admit uniform mixing at time $t = \pi/4$.

Next we apply Corollary 8.3.5 quotients of the form $H(d, 2)/\Gamma$ with $|\Gamma| = 4$. We characterize the $(d + 2)$-regular connected cubelike graphs that admit uniform mixing at time $t = \pi/4$. This result is due to the author, and it is an extension of the work of Best et al. [7].

Theorem 8.3.7. *Let Γ denote a subgroup of $\mathbb{Z}_2^d$ with four elements and minimum distance at least three. The graph $H(d, 2)/\Gamma$ admits uniform mixing at time $t = \pi/4$ if and only if $\Gamma = \langle v_1, v_2 \rangle$ for some v_1, v_2 in $\mathbb{Z}_2^d$ such that one of the following holds:*

(i) $wt(v_1) \equiv wt(v_2) \pmod 4$ *and* $wt(v_1 + v_2) \equiv 2 \pmod 4$

(ii) $wt(v_1) \equiv wt(v_2) + 2 \pmod 4$ *and* $wt(v_1 + v_2) \equiv 0 \pmod 4$.

Proof. By Corollary 8.3.5, we know that uniform mixing occurs at $t = \pi/4$ if and only if every coset Γ satisfies one of

$$|n_0 - n_2| = 0, |n_1 - n_3| = 2 \quad \text{or} \quad |n_0 - n_2| = 2, |n_1 - n_3| = 0.$$

For the identity coset, namely Γ itself, this conditions holds if and only if two nonzero vectors v_1 and v_2 in Γ satisfy (i) or (ii). It remains to show that every coset of Γ also has a suitable weight distribution modulo 4.

First suppose that v_1 and v_2 in Γ satisfy either (i) or (ii). We consider an arbitrary coset $u + \Gamma$ for some u in $\mathbb{Z}_2^d$. For notational convenience, let $v_3 = v_1 + v_2$ denote the third nonzero element of Γ. We note that $|\operatorname{supp}(u) \cap \operatorname{supp}(v_3)|$ can be expressed as:

$$|\operatorname{supp}(u) \cap \operatorname{supp}(v_1)| + |\operatorname{supp}(u) \cap \operatorname{supp}(v_2)| - 2|\operatorname{supp}(u) \cap \operatorname{supp}(v_1) \cap \operatorname{supp}(v_2)|.$$

Therefore either 0 or 2 of the following numbers are even:

$$\{|\operatorname{supp}(u)\cap\operatorname{supp}(v_1)|, |\operatorname{supp}(u)\cap\operatorname{supp}(v_2)|, |\operatorname{supp}(u)\cap\operatorname{supp}(v_3)|\}. \tag{8.2}$$

Using Lemma 8.3.3, we can relate the weights of Γ and $u+\Gamma$ as follows.

$$\begin{aligned} \operatorname{wt}(u) &= \operatorname{wt}(u) \\ \operatorname{wt}(u+v_1) &= \operatorname{wt}(u)+\operatorname{wt}(v_1)-2|\operatorname{supp}(u)\cap\operatorname{supp}(v_1)| \\ \operatorname{wt}(u+v_2) &= \operatorname{wt}(u)+\operatorname{wt}(v_2)-2|\operatorname{supp}(u)\cap\operatorname{supp}(v_2)| \\ \operatorname{wt}(u+v_3) &= \operatorname{wt}(u)+\operatorname{wt}(v_3)-2|\operatorname{supp}(u)\cap\operatorname{supp}(v_3)|. \end{aligned}$$

Since an even number of the support sizes in (8.2) are even and v_1 and v_2 satisfy (i) or (ii), we see that either

$$\begin{aligned} \operatorname{wt}(u) &\equiv \operatorname{wt}(u+v_3) \pmod 4 \\ \text{and}\ \operatorname{wt}(u+v_1) &\equiv \operatorname{wt}(u+v_2)+2 \pmod 4 \end{aligned}$$

or otherwise

$$\begin{aligned} \operatorname{wt}(u) &\equiv \operatorname{wt}(u+v_3)+2 \pmod 4 \\ \text{and}\ \operatorname{wt}(u+v_1) &\equiv \operatorname{wt}(u+v_2) \pmod 4. \end{aligned}$$

Thus the coset $u+\Gamma$ also satisfies one of

$$|n_0-n_2|=0, |n_1-n_3|=2 \quad \text{or} \quad |n_0-n_2|=2, |n_1-n_3|=0.$$

We conclude that uniform mixing occurs on $H(d,2)/\Gamma$ if and only if Γ contains two nonzero vectors v_1 and v_2 that satisfy (i) or (ii). □

We note that the proof above gives a necessary and sufficient condition for uniform mixing in terms of only Γ. For this special case, if the weight distribution of Γ satisfies Equation 8.1, then all of the cosets of Γ also satisfy Equation 8.1. It would be desirable to show that this is true in general.

Our methods above focus on uniform mixing on quotient graphs at time $t=\pi/4$. This is convenient because the underlying Hamming graphs admits uniform mixing at the same time. Of course, uniform mixing could occur at other times. Chan has found examples of graphs that admit uniform mixing at earlier times [18].

Theorem 8.3.8. *For $r \geq 2$, there exist graphs in the Bose-Mesner algebra of the Hamming graph $H(2^{k+2}-8,2)$ that admit uniform mixing at time $\pi/2^k$.* □

This result confirms that for any time $t > 0$ there exists a graph that admits uniform mixing at a time prior to t.

In the remainder of this section, we summarize other known families of cubelike graphs that admit uniform mixing. First we consider graphs whose adjacency matrix is contained in the Bose-Mesner algebra of a folded d-cube. This result is due to Chan [18] and generalizes the work in [7].

Theorem 8.3.9. *For $d \geq 3$, the Bose-Mesner algebra of the folded d-cube contains a flat type-II matrix if and only if d is odd.* □

Chan also investigates uniform mixing on graphs in the Bose-Mesner algebra of the association scheme of the halved d-cube. The following pair of results are due to Chan [18].

Theorem 8.3.10. *For $d \geq 3$, the Bose-Mesner algebra of the halved d-cube contains a flat type-II matrix if and only if d is odd.* □

Theorem 8.3.11. *For $d \geq 3$, the halved d-cube contains admits uniform mixing if and only if d is odd.* □

Finally, we note that Chan also classifies the so-called folded halved cubes with flat type-II matrices in their Bose-Mesner algebra [18]. Consequently, this work also determines which of the folded halved cubes admit uniform mixing. For more information about folded halved cubes, see page 141 of [10].

8.4 Quotients of $H(d, 3)$

In this section, we shift our focus to quotients of $H(d, 3)$. By Corollary 7.5.7, we know that any Cayley graph over $\mathbb{Z}_3^r$ is isomorphic to a quotient graph $H(d, 3)/\Gamma$ for an appropriate choice of Γ and d. Aside from the trivial cases of K_3 and $H(d, 3)$, uniform mixing on these quotients has not been studied before. Our results in this section are due to the author.

Our earlier work enables us to take care of the small cases with ease. As we saw in Theorem 3.4.1, the complete graph K_3 is the unique connected Cayley graph over $\mathbb{Z}_3$, and K_3 admits uniform mixing at time $t = 2\pi/9$. There are three connected Cayley graphs over $\mathbb{Z}_3^2$: K_9, $\overline{3 \times K_3}$, and $K_3 \square K_3$. We know that K_9 does not admit uniform mixing by Theorem 3.4.1. Furthermore, since $\overline{3 \times K_3}$ is the complement of a disconnected graph, Theorem 3.4.1 implies that uniform mixing does not occur. This leaves us $K_3 \square K_3$, which admits uniform mixing at $t = 2\pi/9$ by Theorem 3.4.1. Of course, we note that $K_3 \square K_3$ is isomorphic to the Paley graph P_9.

Using SAGE to explore the 20 connected Cayley graphs over $\mathbb{Z}_3^3$, we see that ten of these graphs admit uniform mixing at time $t = 2\pi/9$. These ten graphs are comprised of five complementary pairs of graphs. The other ten graphs do not admit uniform mixing at $t = 2\pi/9$ and do not appear to admit uniform mixing at any other time. The following work gives necessary and sufficient conditions on the weight distribution of Γ for uniform mixing to occur on $H(d,3)/\Gamma$ at time $t = 2\pi/9$.

We consider quotients of the form $H(d,3)/\Gamma$, where Γ is a subgroup of order 3^s in $\mathbb{Z}_3^d$ with distance at least three. We identify each vertex in the quotient graph with a coset of Γ in $\mathbb{Z}_3^d$. At time $t = 2\pi/9$ the entries of the transition matrix simplify to the following.

Lemma 8.4.1. *Let Γ denote a subgroup of $\mathbb{Z}_3^d$ with minimum distance at least three, and let $U(t)$ denote the transition matrix of $H(d,3)/\Gamma$. The $(0, v+\Gamma)$-entry of the transition matrix at time $t = 2\pi/9$ is given by*

$$U(2\pi/9)_{0,v+\Gamma} = \frac{1}{3^d}\left(e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right)^d \sum_{a \in v+\Gamma} \left(e^{\frac{2\pi i}{3}}\right)^{wt(a)}.$$

Proof. From Lemma 7.4.2, we know that

$$U(t)_{0,v+\Gamma} = \frac{1}{3^d} \sum_{a\in v+\Gamma} \left(e^{2it} - e^{-it}\right)^{\text{wt}(a)} \left(e^{2it} + 2e^{-it}\right)^{d-\text{wt}(a)}.$$

In particular, at time $t = 2\pi/9$, we obtain the following simplification.

$$\begin{aligned} U(2\pi/9)_{0,v+\Gamma} &= \frac{1}{3^d} \sum_{a\in v+\Gamma} \left(e^{\frac{4\pi i}{9}} - e^{\frac{-2\pi i}{9}}\right)^{\text{wt}(a)} \left(e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right)^{d-\text{wt}(a)} \\ &= \frac{1}{3^d}\left(e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right)^d \sum_{a\in v+\Gamma} \left(\frac{e^{\frac{4\pi i}{9}} - e^{\frac{-2\pi i}{9}}}{e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}}\right)^{\text{wt}(a)}. \end{aligned}$$

Using the fact that $e^{\frac{2\pi i}{3}} = -1/2 + i\sqrt{3}/2$, we deduce that

$$\begin{aligned} \left(e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right)^{-1} &= \left(5 + 2e^{\frac{2\pi i}{3}} + 2e^{\frac{-2\pi i}{3}}\right)^{-1} \left(e^{\frac{-4\pi i}{9}} + 2e^{\frac{2\pi i}{9}}\right) \\ &= \frac{1}{3}\left(e^{\frac{-4\pi i}{9}} + 2e^{\frac{2\pi i}{9}}\right). \end{aligned}$$

Combining this with our earlier expression for $U(2\pi/9)$ yields the following.

$$\begin{aligned} U(2\pi/9)_{0,v+\Gamma} &= \frac{1}{3^d}\left(e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right)^d \sum_{a\in v+\Gamma}\left(\frac{1}{3}\left(-1+2e^{\frac{2\pi i}{3}} - e^{\frac{-2\pi i}{3}}\right)\right)^{\mathrm{wt}(a)} \\ &= \frac{1}{3^d}\left(e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right)^d \sum_{a\in v+\Gamma}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)^{\mathrm{wt}(a)} \\ &= \frac{1}{3^d}\left(e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right)^d \sum_{a\in v+\Gamma}\left(e^{\frac{2\pi i}{3}}\right)^{\mathrm{wt}(a)}. \end{aligned}$$

This is our desired expression for $U(2\pi/9)_{0,v+\Gamma}$. □

As we see, the entries of $U(t)$ at time $t = 2\pi/9$ are determined by the weights modulo 3 of the cosets of Γ. Similar to the previous section, we introduce notation to keep track of the weight distribution of elements in the cosets of Γ.

Definition 8.4.2. *For a particular coset $v + \Gamma$, let n_j denote the number of elements a in $v + \Gamma$ such that $wt(a) \equiv j \pmod 3$.*

Using this language we can characterize the quotient $H(d, 3)/\Gamma$ that admit uniform mixing at time $t = 2\pi/9$.

Theorem 8.4.3. *Let Γ denote a subgroup of $\mathbb{Z}_3^d$ with minimum distance at least three such that $|\Gamma| = 3^s$. Uniform mixing occurs on $H(d, 3)/\Gamma$ at time $t = 2\pi/9$ if and only if the weight distribution of every coset of Γ satisfies*

$$n_0n_1 + n_0n_2 + n_1n_2 = 3^{2s-1} - 3^{s-1}. \tag{8.3}$$

Proof. We begin by recalling that

$$\left|e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right|^2 = 3^d.$$

Therefore from Lemma 8.4.1 we have

$$\begin{aligned} |U(t)_{0,v+\Gamma}|^2 &= \frac{1}{3^{2d}}\left|e^{\frac{4\pi i}{9}} + 2e^{\frac{-2\pi i}{9}}\right|^{2d}\left|\sum_{a\in v+\Gamma}\left(e^{\frac{2\pi i}{3}}\right)^{\mathrm{wt}(a)}\right|^2 \\ &= \frac{1}{3^d}\left|n_0 - \frac{1}{2}(n_1+n_2) + i\frac{\sqrt{3}}{2}(n_1-n_2)\right|^2. \end{aligned}$$

The modulus squared on the right hand side of the equation can be further simplified as follows.

$$\begin{aligned}\left|n_0 - \frac{1}{2}(n_1+n_2) + i\frac{\sqrt{3}}{2}(n_1-n_2)\right|^2 &= (n_0 - \frac{1}{2}(n_1+n_2))^2 + \frac{3}{4}(n_1-n_2)^2 \\ &= n_0^2+n_1^2+n_2^2 - n_1n_2 - n_0n_1 - n_0n_2 \\ &= (n_0+n_1+n_2)^2 - 3(n_0n_1+n_0n_2+n_1n_2) \\ &= 3^{2s} - 3(n_0n_1+n_0n_2+n_1n_2).\end{aligned}$$

From an earlier result, we know that uniform mixing occurs on $H(d,3)/\Gamma$ if and only if

$$|U(2\pi/9)_{0,v+\Gamma}|^2 = \frac{1}{3^{d-s}}$$

holds for every coset $v+\Gamma$. This implies that uniform mixing occurs if and only if

$$n_0n_1+n_0n_2+n_1n_2 = 3^{2s-1} - 3^{s-1}$$

holds for every coset $v+\Gamma$. □

Recall that the quotient graph $H(d,3)/\langle \mathbf{1}\rangle$ is the *folded Hamming graph* over $\mathbb{Z}_3^{d-1}$.

Theorem 8.4.4. *The folded Hamming graph over* $\mathbb{Z}_3^{d-1}$ *admits uniform mixing at* $t = 2\pi/9$ *if and only if* $d \equiv 1, 2 \pmod 3$.

Proof. Let $\Gamma = \langle \mathbf{1}\rangle$, which implies $s = 1$ in our above notation. Note that each coset of Γ has three elements, and so trivially we have

$$n_0+n_1+n_2 = 3$$

for every coset $v+\Gamma$. We consider the weight distribution of the cosets in two cases based on d modulo 3.

(a) $d \equiv 0 \pmod 3$
The weight distribution for Γ satisfies $n_0 = 3$ and $n_1 = n_2 = 0$, and so

$$n_0n_1+n_0n_2+n_1n_2 = 0.$$

Thus Γ does not satisfy (8.3) in this case.

(b) $d \equiv 1, 2 \pmod 3$
Without loss of generality, the weight distribution of Γ satisfies $n_0 = 1$, $n_1 = 2$, and $n_2 = 0$, and so

$$n_0n_1+n_0n_2+n_1n_2 = 2.$$

Thus Γ satisfies (8.3). Moreover, if we consider the coset $v+\Gamma$ such that $\mathrm{wt}(v) \equiv 1 \pmod 3$, then the weight distribution of $v+\Gamma$ satisfies $n_0 = 0$, $n_1 = 1$, and $n_2 = 2$. Thus the weight distribution for $v+\Gamma$ satisfies

$$n_0n_1 + n_0n_2 + n_1n_2 = 2.$$

Similarly, (8.3) holds for every coset of Γ.

By Theorem 8.4.3, we conclude that the folded Hamming graph admits uniform mixing at time $t = 2\pi/9$ if and only if $d \equiv 1, 2 \pmod 3$. □

Uniform mixing of quotients of $H(d,3)$ at times other than $2\pi/9$ is trickier, and we cannot say anything conclusively about general quotients of the form $H(d,3)$ at other times.

8.5 Quotients of $H(d,4)$

The Hamming graph $H(d,4)$ is the Cartesian product of d copies of K_4. In this section we consider the graph obtained by taking the quotient of $H(d,4)$ over some particular subgroup Γ of $\mathbb{Z}_4^d$. Our approach is similar to our work in the previous section. Using the weight distribution of the cosets of Γ, we determine which quotients of $H(d,4)$ admit uniform mixing at time $t = \pi/4$. This is a new result due to the author.

We begin by deriving an expression for the entries of the transition matrix at time $t = \pi/4$. Recall that uniform mixing occurs on the Hamming graph $H(d,4)$ at time $t = \pi/4$.

Lemma 8.5.1. *Let Γ denote a subgroup of $\mathbb{Z}_4^d$ with minimum distance at least three, and let $U(t)$ denote transition matrix of $H(d,4)/\Gamma$. The $(0, v+\Gamma)$-entry of $U(t)$ at time $t = \pi/4$ is given by*

$$U(\pi/4)_{0,v+\Gamma} = \left(\frac{e^{3i\pi/4}}{2}\right)^d \sum_{a \in v+\Gamma} (-1)^{wt(a)}.$$

Proof. Applying Lemma 7.4.2, we can express the $(0, v+\Gamma)$-entry of the transition matrix as

$$\begin{aligned} U(t)_{0,v+\Gamma} &= \frac{1}{4^d} \sum_{a \in v+\Gamma} \left(e^{3it} - e^{-it}\right)^{\mathrm{wt}(a)} \left(e^{3it} + 3e^{-it}\right)^{d-\mathrm{wt}(a)} \\ &= \left(\frac{e^{3it}}{4}\right)^d \sum_{a \in v+\Gamma} \left(1 - e^{-4it}\right)^{d-\mathrm{wt}(a)} \left(1 + 3e^{-4it}\right)^{\mathrm{wt}(a)}. \end{aligned}$$

Substituting in $t = \pi/4$ simplifies this expression to the following.

$$\begin{aligned} U(\pi/4)_{0,v+\Gamma} &= \left(\frac{e^{3i\pi/4}}{4}\right)^d \sum_{a\in v+\Gamma} 2^{d-\mathrm{wt}(a)} (-2)^{\mathrm{wt}(a)} \\ &= \left(\frac{e^{3i\pi/4}}{2}\right)^d \sum_{a\in v+\Gamma} (-1)^{\mathrm{wt}(a)}. \end{aligned}$$

This yields our desired result. □

Our expression for the transition matrix at time $t = \pi/4$ given above only depends on the parity of the weights of cosets of Γ. Again it is convenient to introduce notation to keep track of the number of elements of each parity.

Definition 8.5.2. *For a particular coset $v + \Gamma$, let n_j denote the number of elements a in $v + \Gamma$ such that $wt(a) \equiv j \pmod 2$.*

Using this notation, we characterize the quotient graphs of the form $H(d, 4)/\Gamma$ that admit uniform mixing at time $t = \pi/4$.

Theorem 8.5.3. *Let Γ denote a subgroup of $\mathbb{Z}_4^d$ with minimum Hamming distance at least three. Uniform mixing occurs on $H(d, 4)/\Gamma$ at time $t = \pi/4$ if and only if the weight distribution of every coset of Γ satisfies*

$$(n_0 - n_1)^2 = |\Gamma|. \tag{8.4}$$

Proof. Further simplification of Lemma 8.5.1 yields the following:

$$\begin{aligned} |U(\pi/4)_{0,v+\Gamma}|^2 &= \frac{1}{4^d} \left| \sum_{a\in v+\Gamma} (-1)^{\mathrm{wt}(a)} \right|^2 \\ &= \frac{1}{4^d} \left|n_0 - n_1\right|^2. \end{aligned}$$

Recall that uniform mixing occurs on $H(d, 4)/\Gamma$ if and only if

$$|U(t)_{0,v+\Gamma})|^2 = \frac{|\Gamma|}{4^d}$$

for every coset $v + \Gamma$. Therefore uniform mixing occurs at $t = \pi/4$ if and only if

$$(n_0 - n_1)^2 = |\Gamma|$$

for every coset $v + \Gamma$. □

As an immediate consequence of this theorem, we have the following necessary condition on the weight distribution of Γ for any quotient graph $H(d,4)$ that admits uniform mixing at time $t=\pi/4$.

Corollary 8.5.4. *Let Γ denote a subgroup of $\mathbb{Z}_4^d$ with minimum distance at least three. If the quotient graph $H(d,4)/\Gamma$ admits uniform mixing at time $t=\pi/4$, then $|\Gamma|=4^s$ for some positive integer s. Moreover, the weight distribution of Γ must be one of the following:*

(i) s is odd: $n_0 = 2^{2s-1}-2^{s-1}$, $n_1 = 2^{2s-1}+2^{s-1}$;

(ii) s is even: $n_0 = 2^{2s-1}+2^{s-1}$, $n_1 = 2^{2s-1}-2^{s-1}$.

Proof. Recall that n_0 and n_1 denote the number of elements in Γ with even and odd weight, respectively. If the quotient graph $H(d,4)/\Gamma$ admits uniform mixing at time $t=\pi/4$, then Theorem 8.5.3 implies that

$$|n_0 - n_1| = \sqrt{|\Gamma|}.$$

Since Γ is a subgroup of $\mathbb{Z}_4^d$ and n_0-n_1 is an integer, it must be the case that $|\Gamma|=4^s$ for some positive integer s. Therefore one of the following holds:

$$-n_0+n_1 = 2^s \quad \text{or} \quad n_0 - n_1 = 2^s.$$

Since $n_0+n_1=4^s$, this implies that either

$$n_1 = 2^{s-1}\left(2^s+1\right) \quad \text{or} \quad n_1 = 2^{s-1}\left(2^s-1\right).$$

For each element x in Γ such that $\mathrm{wt}(x)$ is odd, there is a subset of three scalar multiples $\{x,2x,3x\}$ such that

$$\mathrm{wt}(x)=\mathrm{wt}(2x)=\mathrm{wt}(3x).$$

Thus the elements in Γ with odd weight can be partitioned into sets of size three. It follows that n_1 is divisible by three. Note that

$$3|\left(2^s+1\right) \iff s \text{ is odd}.$$

We see n_1 is determined by the parity of s. The value of n_0 is immediately determined from n_1. □

Finally, we apply Theorem 8.5.3 to characterize the folded Hamming graphs over $\mathbb{Z}_4^d$ that admit uniform mixing.

Theorem 8.5.5. *The folded Hamming graph $H(d,4)/\langle \mathbf{1} \rangle$ admits uniform mixing at $t = \pi/4$ if and only if d is odd.*

Proof. Since $\Gamma = \langle \mathbf{1} \rangle$, we note that $s = 1$ in terms of our notation above. We consider two cases based on the parity of d.
(a) $d \equiv 0 \pmod 2$

In this case $\Gamma = \langle \mathbf{1} \rangle$ satisfies $n_0 = 4$. Therefore

$$n_0 \neq 2^{2s-1} - 2^{s-1} = 1.$$

By Corollary 8.5.4, we see that $H(d,4)/\langle \mathbf{1} \rangle$ does not admit uniform mixing.
(b) $d \equiv 1 \pmod 2$

Note that $\Gamma = \langle \mathbf{1} \rangle$ satisfies $n_0 = 1$ and $n_1 = 3$, and so

$$(n_0 - n_1)^2 = 4.$$

Therefore Γ satisfies (8.4). Next we consider a coset $v + \Gamma$. For j in $\mathbb{Z}_4$, let m_j denote the number of coordinates of v that are equal to j. The weights of the four elements of $v + \Gamma$ satisfy the following:

$$\begin{aligned} \mathrm{wt}(v) &\equiv m_1 + m_2 + m_3 \pmod 2; \\ \mathrm{wt}(v+1) &\equiv d - m_3 \pmod 2; \\ \mathrm{wt}(v+2) &\equiv d - m_2 \pmod 2; \\ \mathrm{wt}(v+3) &\equiv d - m_1 \pmod 2. \end{aligned}$$

By the Pigeonhole Principle, at least two of m_1, m_2, and m_3 must have the same parity. Without loss of generality, we assume $m_1 \equiv m_2 \pmod 2$. This implies that

$$m_1 + m_2 + m_3 \equiv m_3 \pmod 2.$$

And since d is odd, we see that

$$m_3 \not\equiv d - m_3 \pmod 2.$$

Thus we conclude that exactly three of the elements in the coset $v + \Gamma$ have the same weight modulo 2, and

$$(n_0 - n_1)^2 = 4.$$

Since $v + \Gamma$ was chosen arbitrarily, by Theorem 8.5.3 we conclude that $H(d,4)/\langle \mathbf{1} \rangle$ admits uniform mixing if and only if d is odd. $\square$

8.6 General Quotients

Now we wish to generalize our results from the previous sections to quotients of $H(d,n)$ for arbitrary n. We consider uniform mixing graph on quotients of $H(d,n)$ at time $t=\pi/n$. We focus on this time since the corresponding transition matrix entries are greatly simplified. At other times t we are unable to give any new results about uniform mixing. The following result is due to the author.

Theorem 8.6.1. *Let Γ denote a subgroup of $\mathbb{Z}_n^d$ with minimum Hamming distance at least three. If uniform mixing occurs on $H(d,n)/\Gamma$ at time $t=\pi/n$ then n must be even and $n^d/|\Gamma|$ must be a square.*

Proof. First we see that the $(0, v+\Gamma)$-entry of the transition matrix of $H(d,n)/\Gamma$ can be expressed as

$$\begin{aligned}
U(t)_{0,v+\Gamma} &= \left(\frac{e^{-it}}{n}\right)^d \sum_{a\in v+\Gamma} \left(e^{nit}-1\right)^{\mathrm{wt}(a)} \left(e^{nit}-1+n\right)^{d-\mathrm{wt}(a)} \\
&= \left(\frac{e^{-it}}{n}\right)^d \sum_{a\in v+\Gamma} \left(e^{nit}-1\right)^{\mathrm{wt}(a)} \sum_{j=0}^{d-\mathrm{wt}(a)} \binom{d-\mathrm{wt}(a)}{j} \left(e^{nit}-1\right)^{d-\mathrm{wt}(a)-j} n^j \\
&= \left(\frac{e^{-it}}{n}\right)^d \sum_{a\in v+\Gamma} \sum_{j=0}^{d-\mathrm{wt}(a)} \binom{d-\mathrm{wt}(a)}{j} \left(e^{nit}-1\right)^{d-j} n^j.
\end{aligned}$$

If we suppose that $t=\pi/n$, then this expression further reduces to the following.

$$U(\pi/n)_{0,v+\Gamma} = \left(\frac{e^{-i\pi/n}}{n}\right)^d \sum_{a\in v+\Gamma} \sum_{j=0}^{d-\mathrm{wt}(a)} \binom{d-\mathrm{wt}(a)}{j} (-2)^{d-j} n^j \tag{8.5}$$

Recall that uniform mixing occurs on $H(d,n)/\Gamma$ if and only if

$$|U_{0,v+\Gamma}(\pi/n)| = \frac{\sqrt{|\Gamma|}}{\sqrt{n^d}}.$$

From Equation 8.5, we see that

$$|U(\pi/n)_{0,v+\Gamma}| = \frac{1}{n^d}\left|\sum_{a\in v+\Gamma} \sum_{j=0}^{d-\mathrm{wt}(a)} \binom{d-\mathrm{wt}(a)}{j}(-2)^{d-j} n^j\right|.$$

Therefore if uniform mixing occurs, then for all cosets $v+\Gamma$ we must have

$$\sqrt{n^d|\Gamma|} = \left| \sum_{a\in v+\Gamma} \sum_{j=0}^{d-\mathrm{wt}(a)} \binom{d-\mathrm{wt}(a)}{j} (-2)^{d-j} n^j \right|.$$

By the integrality of the expression inside the absolute value sign, we see that this equality implies that $n^d|\Gamma|$ must be a square. Since $|\Gamma|$ divides n^d, this implies that $n^d/|\Gamma|$ is a square.

Now note that the identity coset $v+\Gamma$ is the unique coset containing the identity element. Therefore $n^d|\Gamma|$ must be divisible by 2. However, if $|\Gamma|$ is even, then n must also be even. □

It would be desirable to generalize this result to restrict the values of d and n such that $H(d,n)/\Gamma$ admits uniform mixing at any time t. However, it is unlikely this type of approach will be sufficient to show that uniform mixing never occurs on $H(d,n)/\Gamma$ for $n \geq 5$. We consider this problem and other open problems in Chapter 9.

Chapter 9

Future Research

We conclude this thesis by discussing five open research problems related to uniform mixing of continuous-time quantum walks. We pay close attention to problems that could be approached using the methods described in this thesis.

9.1 Open Problems

We begin with a fundamental open problem. In this thesis much of our work focused on uniform mixing on vertex transitive graphs. Intuitively, it would seem reasonable if uniform mixing only occurs on regular graphs, or possibly only on vertex transitive graphs. However, it seems to be difficult to prove this or find a counter example. Thus it would be significant to answer the following question: does a graph have to be regular in order for $\exp(itA)$ to be flat? A first step might be to give a lower bound on the size of a counterexample. It is straightforward to see that a graph of order four or less must be regular in order for $\exp(itA)$ to be flat. It would be reasonable to manually check all connected graphs of order five.

Our second open research problem is to show that uniform mixing does not occur on the cycle C_n for any $n \geq 5$. This conjecture is due to Ahmadi, Belk, Tamon, and Wendler in [3]. In this thesis, we extend the work in [16] and [1] and show that uniform mixing does not occur on C_n if n is even or prime. The smallest open case is C_9. One possible method to attack C_9 would be to show that there are a finite number of cyclic type-II matrices in exponential form. It is known that there are an infinite number of cyclic 9-roots [5], and so the assumption of exponential form would be crucial to this approach. More generally, it might be feasible to use a quotient approach to show that if uniform mixing does not occur on C_p and C_q, then it does not occur on C_{pq}.

The third open research problem is to consider the least possible time t for which a particular graph admits uniform mixing. This could be useful for practical algorithm design. Recall that if the Hamming graph $H(d, n)$ admits uniform mixing, then t is equal to the least possible mixing time of the complete graph K_n. However, Chan's work shows that faster mixing times are possible for quotients of binary Hamming graphs [18]. Recall from Theorem 8.4.4 that for certain values of d, the folded Hamming graph $H(d, 3)/\langle \mathbf{1} \rangle$ admits uniform mixing at time $t = 2\pi/9$. For example, it is unknown whether the folded Hamming graph admits uniform mixing before time $t = 2\pi/9$.

Next we shift our consideration to quotients of Hamming graphs. Currently we have no examples of quotients of $H(d, n)$ for $n \geq 5$ that admit uniform mixing. Chan's result in [18] proves that there are no flat type-II matrices in the Bose-Mesner algebra of the Hamming scheme $\mathcal{H}(d, n)$ for $n \geq 5$. This supports our following conjecture.

Conjecture 9.1.1. *A Cayley graph over $\mathbb{Z}_n^d$ does not admit uniform mixing for $n \geq 5$.*

Of course, Chan's result is far from sufficient to prove Conjecture 9.1.1. As we noted earlier, the adjacency matrix of a quotient of a Hamming graph does not need to be contained in the Bose-Mesner algebra of a Hamming scheme. Furthermore, Cayley graphs over $\mathbb{Z}_n^d$ for $n \geq 5$ are not necessarily quotients of Hamming graphs. By Theorem 5.5.2, we know that ϵ-uniform mixing occurs on certain Cayley graphs over $\mathbb{Z}_n^d$ if n is a prime. This confirms that it will be difficult to prove Conjecture 9.1.1 by bounding the modulus of the entries of the transition matrix. Instead, a more viable approach might be to take into account the algebraic properties of the entries of the transition matrix.

Our final open research problem is to further study the algebraic properties of the coefficients of the transition matrix. For all of our known examples of graphs that admit uniform mixing, we see that if uniform mixing occurs on the graph at time t, then e^{it} is a root of unity. This observation gives rise to the following conjecture.

Conjecture 9.1.2. *If a graph admits uniform mixing at time t, then e^{it} must be a root of unity.*

As a fair warning, this conjecture should be taken with a grain of salt. Our main reason for prudence is that we do not have a wide variety of examples of graphs that admit uniform mixing. All of the known examples are closely related to formally self-dual association schemes with integral eigenvalues, and consequently, uniform mixing occurs at time t on our known examples if and only if e^{it} is an algebraic integer. All complex roots of unity are algebraic integers of modulus one. However, the converse is not true [50]. Thus it would be interesting to prove this conjecture for a restricted subclass of graphs, such as all graphs with integral eigenvalues.

References

The numbers following each entry indicate the pages on which it is cited.

[1] William Adamczak, Kevin Andrew, Leon Bergen, Dillon Ethier, Peter Hernberg, Jennifer Lin, and Christino Tamon. Non-uniform mixing of quantum walk on cycles. *International Journal of Quantum Information*, 05(06):781–793, 2007. (3, 32, 53, 56, 115)

[2] Dorit Aharonov, Andris Ambainis, Julia Kempe, and Umesh Vazirani. Quantum walks on graphs. In *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, pages 50–59, New York, 2001. ACM. (32)

[3] Amir Ahmadi, Ryan Belk, Christino Tamon, and Carolyn Wendler. On mixing in continuous-time quantum walks on some circulant graphs. *Quantum Inf. Comput.*, 3(6):611–618, 2003. (3, 32, 33, 34, 36, 53, 57, 115)

[4] Andris Ambainis. Quantum walks and their algorithmic applications. *International Journal of Quantum Information*, 1(04):507–518, 2003. (28)

[5] Jörgen Backelin. Square multiples n give infinitely many cyclic n-roots. *Reports/Univ. of Stockholm*, 1989. (52, 115)

[6] V. Belevitch. Conference networks and Hadamard matrices. *Ann. Soc. Sci. Bruxelles Sér. I*, 82:13–32, 1968. (72)

[7] Ana Best, Markus Kliegl, Shawn Mead-Gluchacki, and Christino Tamon. Mixing of quantum walks on generalized hypercubes. *International Journal of Quantum Information*, 06(06):1135–1148, 2008. (3, 32, 79, 83, 95, 98, 101, 102, 104)

[8] Göran Björck. Functions of modulus 1 on Zn whose Fourier transforms have constant modulus, and cyclic n-roots. In *Recent Advances in Fourier Analysis and its Applications*, pages 131–140. Springer, 1990. (50, 51)

[9] R. C. Bose and Dale M. Mesner. On linear associative algebras corresponding to association schemes of partially balanced designs. *Ann. Math. Statist.*, 30:21–38, 1959. (13)

[10] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Springer-Verlag, Berlin, 1989. (13, 104)

[11] Andries E. Brouwer and Willem H. Haemers. Strongly regular graphs. In *Spectra of Graphs*, pages 115–149. Springer, 2012. (9)

[12] Daniel Bump. *Lie Groups*. Springer-Verlag, New York, 2004. (44)

[13] Edward B. Burger and Robert Tubbs. *Making Transcendence Transparent*. Springer-Verlag, New York, 2004. (41)

[14] Peter J Cameron. Strongly regular graphs. *Selected topics in graph theory*, 1:pp–337, 1978. (9)

[15] Peter J Cameron and JH van Lint. *Designs, graphs, codes, and their links*. Cambridge University Press, 1992. (17)

[16] William Carlson, Allison Ford, Elizabeth Harris, Julian Rosen, Christino Tamon, and Kathleen Wrobel. Universal mixing of quantum walk on graphs. *Quantum Inf. Comput.*, 7(8), 2007. (3, 32, 53, 57, 115)

[17] Ada Chan. Complex Hadamard matrices and strongly regular graphs. *arXiv:1102.5601 [math.CO]*, 2011. (40, 63, 65, 72, 73)

[18] Ada Chan. Complex Hadamard matrices, instantaneous uniform mixing and cubes. *arXiv preprint arXiv:1305.5811*, 2013. (3, 32, 96, 99, 103, 104, 116)

[19] Ada Chan and Chris Godsil. Type-II matrices and combinatorial structures. *Combinatorica*, 30(1):1–24, 2010. (40, 63, 64, 65, 72, 73)

[20] Andrew M Childs. Universal computation by quantum walk. *Physical review letters*, 102(18):180501, 2009. (1, 27)

[21] Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '03, pages 59–68, New York, NY, USA, 2003. ACM. (1, 27, 32)

[22] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1997. (49)

[23] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973. (7)

[24] Xiao-xia Fan and Yan-feng Luo. Mixing of continuous quantum walks on cubelike graphs. *Journal of Lanzhou University (Natural Science Edition)*, 49(1), 2013. (3, 32, 95, 98, 100)

[25] Edward Farhi and Sam Gutmann. Quantum computation and decision trees. *Phys. Rev. A (3)*, 58(2):915–928, 1998. (1, 27, 28)

[26] Yang Ge, Benjamin Greenberg, Oscar Perez, and Christino Tamon. Perfect state transfer, graph products and equitable partitions. *International Journal of Quantum Information*, 9(03):823–842, 2011. (86)

[27] Heath Gerhardt and John Watrous. Continuous-time quantum walks on the symmetric group. In *Approximation, Randomization, and Combinatorial Optimization*, volume 2764 of *Lecture Notes in Comput. Sci.*, pages 290–301. Springer, Berlin, 2003. (32)

[28] Chris Godsil. *Algebraic Combinatorics*. Chapman and Hall Mathematics Series. Chapman & Hall, New York, 1993. (14, 16, 17)

[29] Chris Godsil. State transfer on graphs. *Discrete Math.*, 312(1):129–147, 2012. (28, 80)

[30] Chris Godsil, Natalie Mullin, and Aidan Roy. Uniform mixing and association schemes. *arXiv preprint arXiv:1301.5889*, 2013. (35, 41, 54, 55, 56, 57, 59, 63, 66, 67, 72, 74, 76)

[31] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*. Springer-Verlag, New York, 2001. (8, 10, 11, 72, 84)

[32] J.-M. Goethals and J. J. Seidel. Strongly regular graphs derived from combinatorial designs. *Canad. J. Math.*, 22:597–614, 1970. (63)

[33] Uffe Haagerup. Cyclic p-roots of prime lengths p and related complex Hadamard matrices. *arXiv:0803.2629 [math.AC]*, pages 1–29, 2008. (40, 52)

[34] Vaughan Jones. On knot invariants related to some statistical mechanical models. *Pacific Journal of Mathematics*, 137(2):311–334, 1989. (47)

[35] Alastair Kay. Basics of perfect communication through quantum networks. *Phys. Rev. A*, 84:022337, Aug 2011. (55)

[36] Julia Kempe. Quantum random walks: an introductory overview. *Contemporary Physics*, 44(4):307–327, 2003. (28)

[37] Peter Lo, Siddharth Rajaram, Diana Schepens, Daniel Sullivan, Christino Tamon, and Jeffrey Ward. Mixing of quantum walk on circulant bunkbeds. *Quantum Information & Computation*, pages 370–381, 2006. (32)

[38] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Co., Amsterdam, 1977. (97)

[39] Rudolf Mathon. Symmetric conference matrices of order pq^2+1. *Canad. J. Math.*, 30(2):321–331, 1978. (73)

[40] Cristopher Moore and Alexander Russell. Quantum walks on the hypercube. In *Randomization and Approximation Techniques in Computer Science*, volume 2483 of *Lecture Notes in Comput. Sci.*, pages 164–178. Springer, Berlin, 2002. (3, 32, 87, 95)

[41] J. M. H. Olmsted. Discussions and notes: rational values of trigonometric functions. *Amer. Math. Monthly*, 52(9):507–508, 1945. (42)

[42] Cheryl E. Praeger. Finite normal edge-transitive Cayley graphs. *Bull. Austral. Math. Soc.*, 60(2):207–220, 1999. (85)

[43] Daniel Reitzner, Daniel Nagaj, and Vladimír Bužek. Quantum walks. *Acta Physica Slovaca. Reviews and Tutorials*, 61(6):603–725, 2011. (27)

[44] Gert Sabidussi. On a class of fixed-point-free graphs. *Proceedings of the American Mathematical Society*, 9(5):800–804, 1958. (8)

[45] Pierre Samuel. *Algebraic Theory of Numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970. (40, 43)

[46] F. Szöllősi. *Construction, classification and parametrization of complex Hadamard matrices*. PhD thesis, The University of Wisconsin - Madison, 2011. (48)

[47] Wojciech Tadej and Karol Życzkowski. A concise guide to complex Hadamard matrices. *Open Systems & Information Dynamics*, 13(02):133–177, 2006. (48, 57)

[48] J. H. van Lint and J. J. Seidel. Equilateral point sets in elliptic geometry. *Nederl. Akad. Wetensch. Proc. Ser. A*, 28:335–348, 1966. (72)

[49] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, Cambridge, 1992. (55)

[50] L.C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer-Verlag, 1997. (42, 117)

[51] Bangteng Xu and Harvey I. Blau. On pseudocyclic table algebras and applications to pseudocyclic association schemes. *Israel Journal of Mathematics*, 183(1):347–379, 2011. (22)

Index

d-cube, 18
k-regular, 4

adjacency matrix, 4
affine variety, 48
algebraic integer, 41
algebraic number, 40
arc transitive, 5
association scheme, 12
automorphism, 5
average mixing, 32

Bose-Mesner algebra, 13

Cartesian product, 81
Cayley graph, 8
compact torus, 44
conference graph, 12
continuous-time quantum walk, 28
cyclic association scheme, 19

direct product, 80
discrete Fourier transform, 22
distance-regular graph, 13
dual code, 94
dual eigenvalues, 14

equitable partition, 84

flat matrix, 32
folded d-cube, 19
formally self-dual, 17

graph, 5

halved d-cube, 19
Hamming distance, 18
Hamming graph, 18
Hamming scheme, 18
Hamming weight, 18
hypercubes, 18

intersection parameters, 13

Krein parameters, 16

linear code, 94
linear graph, 90

minimum Hamming distance, 18
mixing matrix, 28
multigraph, 4

normal quotients, 86

pseudocyclic schemes, 22

Schur product, 14
self-complementary graph, 5
strongly regular graph, 9

tensor product, 79
torus generator, 44
transcendental number, 41
transition matrix, 28

uniform mixing, 32
unitary, 29

vertex transitive, 5

weight enumerator, 94