Uniform Mixing on Cayley Graphs over $\mathbb{Z}_3^d$

by

Hanmeng Zhan

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2014

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

This thesis investigates uniform mixing on Cayley graphs over $\mathbb{Z}_3^d$. We apply Mullin's results on Hamming quotients, and characterize the $2(d+2)$-regular connected Cayley graphs over $\mathbb{Z}_3^d$ that admit uniform mixing at time $2\pi/9$. We generalize Chan's construction on the Hamming scheme $\mathcal{H}(d,2)$ to the scheme $\mathcal{H}(d,3)$, and find some distance graphs of the Hamming graph $H(d,3)$ that admit uniform mixing at time $2\pi/3^k$ for any $k \geq 2$. To restrict the mixing time, we derive a sufficient and necessary condition for uniform mixing to occur on a Cayley graph over $\mathbb{Z}_3^d$ at a given time. Using this, we obtain three results. First, we give a lower bound of the valency of a Cayley graph over $\mathbb{Z}_3^d$ that could admit uniform mixing at some time. Next, we prove that no Hamming quotient $H(d,3)/\langle \mathbf{1} \rangle$ admits uniform mixing at time earlier than $2\pi/9$. Finally, we explore the connected Cayley graphs over $\mathbb{Z}_3^3$ with connected complements, and show that five complementary graphs admit uniform mixing with earliest mixing time $2\pi/9$.

Acknowledgements

I owe my deepest gratitude to my supervisor, Chris Godsil, for his guidance, motivation and caring throughout my master studies. Chris Godsil is not only a knowledgeable yet modest professor, but also an observant and considerate mentor. His generosity, perceptible or not, has positively affected both my research and my life.

Next, I would like to thank my thesis readers, Eric Katz and Kevin Purbhoo, for their detailed and constructive feedback. Those comments have greatly improved the presentation of this thesis.

Special thanks to Ada Chan and Natalie Mullin, two of my seniors in quantum uniform mixing. This thesis benefited a lot from their work.

Lastly, my heartfelt appreciation goes to my parents and Wei, for their endless spiritual support during my life.

Contents

Chapter 1

Introduction

The first quantum walk model was introduced by Farhi and Gutmann [13] in 1997. Later in the field of quantum information processing, Christandl et al [11] proposed a class of qubit networks where perfect state transfer occurs on every two-dimensional quantum state within a fixed period. Compared to the classical random walks, quantum walks provide a speedup in the algorithms for many theoretical and practical problems [9, 10]. In this thesis, we study the model of the continuous-time quantum walks, which is defined using the Schrödinger equation and an evolution operator of the system [23]. In particular, we are interested in the quantum walks that are uniform mixing at certain times, that is, the quantum walks that represent uniform probability distributions at these times.

This thesis follows the mathematical formulation of quantum walks on undirected graphs due to Godsil [17]. Let X be a graph with adjacency matrix A. The transition matrix

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

determines the quantum walk on X. When all the entries in $U(t)$ have the same absolute value, we say that X admits uniform mixing at time t.

Uniform mixing on graphs is rare. The known examples are the complete graphs on two, three or four vertices given by Ahmadi et al [2], some Cayley graphs over abelian groups given by Chan [6, 7] and Mullin [22], and the Cartesian products of existing graphs with uniform mixing. On the other hand, some graphs are proved to be resistant to uniform mixing [18]. As an extension of the work by Mullin [22] and Chan [7], we find all $2(d+2)$-regular connected Cayley graphs over $\mathbb{Z}_3^d$ that admit uniform mixing at time $2\pi/9$, some distance graphs of $H(d,3)$ that admit uniform mixing at $2\pi/3^k$, and some distance graphs of $H(d,4)$ that admit uniform mixing at $\pi/2^k$. We also show that the quotient $H(d,3)/\langle \mathbf{1} \rangle$ never admits uniform mixing earlier than the known time $2\pi/9$.

In [22], Mullin showed that every connected linear Cayley graph over $GF(q)^r$ is a quotient of the Hamming graph $H(d,q)$ for some q. Using a weight distribution condition, Mullin found some quotient graphs $H(d,q)/\langle \mathbf{1} \rangle$ that admit uniform mixing at time $\pi/4$ for $q = 2, 4$, and at time $2\pi/9$ for $q = 3$. She also characterized the quotient graphs $H(d+2,2)/\Gamma$ with $|\Gamma| = 4$ that admit uniform mixing at time $\pi/4$. In addition to the known examples, we characterize the quotient graphs $H(d+2,3)/\Gamma$ with $|\Gamma| = 9$ that admit uniform mixing at time $2\pi/9$.

1.0.1 Theorem. *Let $\Gamma = \langle a, b \rangle$ be a subgroup of $\mathbb{Z}_3^{d+2}$ such that the code generated by a and b has minimum distance at least three. The quotient graph $H(d+2,3)/\Gamma$ admits uniform mixing at time $2\pi/9$ if and only if one of the following holds:*

(i)
- $a^T b \equiv 0 \pmod 3$, *and*
- $\mathrm{wt}(a) \not\equiv 0 \pmod 3$, $\mathrm{wt}(b) \not\equiv 0 \pmod 3$.

(ii)
- $a^T b \not\equiv 0 \pmod 3$, *and*
- $\mathrm{wt}(a) \not\equiv \mathrm{wt}(b) \pmod 3$ *or* $\mathrm{wt}(a) \equiv \mathrm{wt}(b) \equiv 0 \pmod 3$. □

When exploring Cayley graphs over $\mathbb{Z}_3^d$, we also seek for other potential times of uniform mixing. We notice that the spectral decompositions of these graphs can be derived from the characters ψ_a of the underlying group $\mathbb{Z}_3^d$. More specifically, if X is a Cayley graph over $\mathbb{Z}_3^d$ with connection set $\mathcal{C}$, then $\psi_a(\mathcal{C})$ is an eigenvalue with eigenvector ψ_a, for every $a \in \mathbb{Z}_3$. Based on the spectrum, we define a rational function in x over the integers by

$$f_g(x) := \left(\sum_{(a-b)^T g = 0} x^{m_{ab}} \right) - 3^d$$

where m_{ab} is determined by the difference of $\psi_a(\mathcal{C})$ and $\psi_b(\mathcal{C})$. We give a condition for uniform mixing to occur on the Cayley graphs over $\mathbb{Z}_3^d$ in terms of these f_g's.

1.0.2 Theorem. *$X(\mathbb{Z}_3^d, \mathcal{C})$ admits uniform mixing at time t if and only if e^{3it} is a zero of*

$$\gcd\{f_g : g \in \mathbb{Z}_3^d\}. \qquad \square$$

One consequence of Theorem 1.0.2 is a basic lower bound for the size of the connection set $\mathcal{C}$ such that $X(\mathbb{Z}_3^d, \mathcal{C})$ admits uniform mixing at a particular time.

1.0.3 Corollary. *Let $\phi(n)$ be the Euler's totient function. If*

$$|\mathcal{C}| < \phi(n) + 2$$

then uniform mixing does not occur on $X(\mathbb{Z}_3^d, \mathcal{C})$ at time $2\pi/3n$. $\square$

The other application of Theorem 1.0.2 is that we can restrict the mixing times of a graph to some choices. For instance, by checking the factors of $f_{\mathbf{1}}$, we show that $2\pi/9$ is the earliest possible time when the quotient $H(d,3)/\langle \mathbf{1} \rangle$ admits uniform mixing.

1.0.4 Theorem. *For $d > 1$, if uniform mixing occurs on $H(d,3)/\langle \mathbf{1} \rangle$ at time t, then $t = 2k\pi/9$ for some integer k coprime to 3.* $\square$

The same idea can be applied to the cubelike graphs to obtain the following result.

1.0.5 Theorem. *If uniform mixing occurs on the folded cubes $H(d+1,2)/\langle \mathbf{1} \rangle$ at time t, then $t = k\pi/4$ for some odd integer k.* $\square$

We also compute $\gcd(f_0, f_{e_1})$ for all the 20 connected Cayley graphs over $\mathbb{Z}_3^3$, and find 10 graphs that admit uniform mixing at $2\pi/9$, which is again the earliest time that mixing occurs. This moves our search to Cayley graphs over $\mathbb{Z}_3^4$ and larger groups. Recent work by Chan [7] shows that there exist distance graphs of the d-cube that admit uniform mixing at time $\pi/2^k$ for $k \geq 2$, which suggests a direction in finding Cayley graphs with earlier unifom mixing. The proof of Chan's result heavily exploits the algebraic properties of association schemes. We study the properties of the eigenvalues of a Hamming scheme, and show that Chan's construction is generalizable to the schemes $\mathcal{H}(d,3)$ and $\mathcal{H}(d,4)$. The following are our examples of graphs with uniform mixing earlier than the Hamming graphs.

1.0.6 Theorem. *For $k \geq 2$ and $r \in \{3^k - 1, 3^k - 4, 3^k - 7\}$, the r-distance graphs X_r of the Hamming graph $H(2 \cdot 3^k - 9, 3)$ admit uniform mixing at time $2\pi/3^k$.* □

1.0.7 Theorem. *For $k \geq 2$, the distance graph $X_{2^{k-2}}$ of the Hamming graph $H(2^{k-1} - 1, 4)$ and the distance graphs $X_{2^{k-1}-1}$, $X_{2^{k-1}}$ of the Hamming graph $H(2^k - 2, 4)$ admit uniform mixing at time $\pi/2^k$,* □

We briefly describe the content of the thesis. In the first two chapters, we present background material on continuous quantum walks and on Cayley graphs. Chapter 4 provides a complete survey of prior knowledge about uniform mixing. In Chapter 5 and 6, we develop the main results, as summarized above. The final chapter will be a discussion about the open problems.

Chapter 2

Quantum Walks

We start with the background on continuous-time quantum walks. In [13], Farhi and Gutmann introduced the concept of continuous-time quantum walks on decision trees as an extension of classical random walks. Later in the field of quantum information processing, Christandl et al [11] proposed a class of qubit networks where perfect state transfer occurs on every two-dimensional quantum state within a fixed period. Abundant research on quantum computation has shown the computational superiority of quantum algorithms over their classical counterparts in many cases [9, 10].

One interesting phenomenon in quantum walks is uniform mixing. It provides purely random probability distributions, which are desirable inputs in some algorithms. In this chapter, we follow the mathematical description of quantum walks given by Godsil [17], and introduce some standard techniques for testing uniform mixing on undirected graphs. Following this, we summarize some known types of graphs that admit uniform mixing.

A *quantum system* is a d-dimensional inner product space over $\mathbb{C}$ with all one-dimensional subspaces as its states. The evolution of the system is determined by a unitary operator U, and the measurement is represented by a Hermitian matrix H. Each eigenspace of H is a possible outcome of this measurement. In quantum computing, it is conventional to assume that the eigenspaces of H are spanned by the standard basis vectors $e_1, e_2, \dots, e_d$. If at some time t, the system were in the state represented by a unit vector z, then the outcome of a measurement with H is e_r with probability

$$|\langle e_r, z\rangle|^2$$

that is, the r-th entry of the Schur product $z \circ \bar{z}$.

2.1 Transition Matrices

For a Hermitian matrix A, we define the *transition operator* $U(t)$ by

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

We see that $U(t)$ is unitary since

$$U(t)^* = \exp(-itA) = U(-t)$$

and so it determines the evolution of a quantum system. If the initial state of this system is e_u, then at time t, the probability that this system is in the state e_v is given by

$$e_v^T \left(U(t)e_u \circ \overline{U(t)e_u} \right) = e_v^T \left(U(t) \circ U(-t) \right) e_u.$$

Hence, the outcome of a measurement with respect to the standard basis is completely determined by

$$M(t) := U(t) \circ U(-t)$$

which we will call the *mixing matrix*.

One candidate for the Hermitian matrix A is the adjacency matrix of an undirected graph X. In this case, A is real symmetric, and so both $U_X(t)$ and $M_X(t)$ are symmetric. For example, the transition matrix of K_2 is

$$\begin{aligned} U_{K_2}(t) &= \sum_{k\geq 0} \frac{(it)^k}{k!} A^k \\ &= \sum_{k\geq 0} \frac{(it)^{2k}}{(2k)!} I + \sum_{k\geq 0} \frac{(it)^{2k+1}}{(2k+1)!} A \\ &= \cos(t) I + i\sin(t) A \\ &= \begin{pmatrix} \cos(t) & i\sin(t) \\ i\sin(t) & \cos(t) \end{pmatrix}. \end{aligned}$$

Not all graphs have transition matrices in such neat form. However, as we will see in Section 2.3, there is a decomposition of the transition matrix based on the spectrum of the graph.

2.2 Perfect State Transfer and Uniform Mixing

Since $U(t)$ is unitary, each column of the mixing matrix M represents a probability distribution. We are interested in two types of distributions. When $M(t)_{uv} = 1$, namely, when there is a complex scalar γ such that

$$U(t)e_u = \gamma e_v$$

we say that X admits *perfect state transfer* from the vertex u to the vertex v at time t. When we have uniform distribution in each column, or equivalently, when

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

for all vertices u and v, we say that X admits *uniform mixing* at time t.

The latter case can be described using type-II matrices. If H is a matrix with non-zero entries, we define the *Schur inverse* of H to be the matrix whose entries are the inverses of the entries in H:

$$H^{(-)}_{jk} := \frac{1}{H_{jk}}$$

A complex $n \times n$ matrix H is *type-II* if

$$HH^{(-)} = nI$$

When all entries of H have the same absolute value, H is called a *flat matrix*. Thus $U(t)$ is flat if uniform mixing occurs at time t. We have the following characterization due to Godsil [18].

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

Proof. $U(t)$ is flat if and only if all entries in $\sqrt{n}U(t)$ have absolute value one, if and only if

$$(\sqrt{n}U(t))^{(-)} = \overline{\sqrt{n}U(t)} = \sqrt{n}U(-t)$$

if and only if

$$\sqrt{n}U(t)(\sqrt{n}U(t))^{(-)} = nI.$$

□

A flat type-II matrix is called a *complex Hadamard matrix*. Hence the above lemma is equivalent to the following.

2.2.2 Corollary. *The graph X admits uniform mixing at time t if and only if $\sqrt{n}U(t)$ is a complex Hadamard matrix.* □

Take K_2 as an example. Its transition matrix evaluated at time $\pi/2$ and $\pi/4$ are

$$U_{K_2}\left(\frac{\pi}{2}\right) = i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$U_{K_2}\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

Therefore, K_2 admits perfect state transfer from vertex 1 to vertex 2 at time $\pi/2$, and admits uniform mixing at time $\pi/4$.

2.3 Spectral Decomposition

The adjacency matrix A of an undirected graph is diagonalizable. For each eigenvalue θ_r of A, let E_r be the orthogonal projection onto the eigenspace belonging to θ_r. Then the E_r's are pairwise orthogonal real idempotents which sum to I. The spectral decomposition of A expresses A in a linear combination of these idempotents:

$$A = \sum_r \theta_r E_r.$$

By the spectral properties, a function in A may also be written as a linear combination of the E_r's.

2.3.1 Lemma. *Let A be a real symmetric matrix with spectral decomposition*

$$A = \sum_r \theta_r E_r.$$

If f is an analytic function defined on the spectrum of A, then

$$f(A) = \sum_r f(\theta_r) E_r.$$ □

Applying the above lemma to each term in $U(t)$, we obtain the spectral decomposition of the transition matrix.

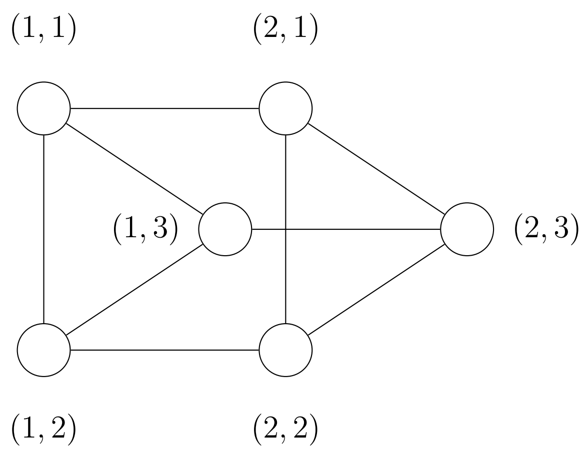

Figure 2.1: $K_2 \square K_3$

2.3.2 Theorem. *If the spectral decomposition of A is*

$$A = \sum_i \theta_r E_r$$

then

$$U(t) = \sum_r e^{i\theta_r t} E_r. \qquad \square$$

2.4 Cartesian Product of Graphs

In this section, we introduce an operation on graphs that produces new examples of graphs with perfect state transfer (uniform mixing) from the existing ones. Given two graphs X and Y, the Cartesian product $X \square Y$ is the graph with vertex set $V(X) \times V(Y)$ where (x_1, y_1) is adjacent to (x_2, y_2) if one of the following holds:

- $x_1 = x_2$, and y_1 is adjacent to y_2 in Y.
- $y_1 = y_2$, and x_1 is adjacent to x_2 in X.

Figure 2.1 gives the Cartesian product of the complete graphs K_2 and K_3.

If A and B are the corresponding adjacency matrices of X and Y, then the adjacency matrix of $X \mathbin{\square} Y$ is $A \otimes I + I \otimes B$. It turns out that we can obtain the transition matrix of $X \mathbin{\square} Y$ directly from those of X and Y.

2.4.1 Theorem. *Let X and Y be two graphs. Then*

$$U_{X \square Y} = U_X \otimes U_Y.$$

Proof. Notice that $A \otimes I$ and $I \otimes B$ commute:

$$(A \otimes I)(I \otimes B) = A \otimes B = (I \otimes B)(A \otimes I)$$

so the transition matrix of $X \square Y$ is

$$\begin{aligned} U_{X \square Y} &= \exp\left(it\left(A \otimes I + I \otimes B\right)\right) \\ &= \exp((itA \otimes I) + (I \otimes itB)) \\ &= (\exp(itA) \otimes I)(I \otimes \exp(itB)) \\ &= \exp(itA) \otimes \exp(itB) \\ &= U_X \otimes U_Y. \end{aligned}$$

□

Since the entries of $U_{X \square Y}(t)$ are products of the entries of $U_X(t)$ and $U_Y(t)$, we see that the set of graphs with uniform mixing is closed under Cartesian products. In fact, we have the following observation due to Best et al [3].

2.4.2 Lemma. *$X \mathbin{\square} Y$ admits uniform mixing at time t if and only if both X and Y admit uniform mixing at time t.* □

This gives a way to construct new graphs with perfect state transfer (uniform mixing) from the known ones. For instance, an d-cube Q_d is the d-th Cartesian power of K_2. Its transition matrix is

$$U_{Q_d}(t) = U_{K_2}(t)^n = \begin{pmatrix} \cos(t) & i\sin(t) \\ i\sin(t) & \cos(t) \end{pmatrix}^{\otimes d}.$$

The quantum walk on K_2 tells us that the d-cube admits perfect state transfer between any pair of antipodal vertices at time $\pi/2$, and admits uniform mixing at time $\pi/4$, for any positive integer d.

2.5 Uniform Mixing on Complete Graphs

Uniform mixing on graphs is rare. The known graphs that admit uniform mixing are the complete graphs on two, three or four vertices, the Cartesian products of existing graphs with uniform mixing and some linear Cayley graphs [7, 22].

We will use the spectral decomposition to study uniform mixing in complete graphs. For K_q, the eigenvalues are $\theta_0 = q-1$ and $\theta_1 = -1$, and the corresponding idempotents are $E_0 = \frac{1}{q}J$ and $E_1 = I - \frac{1}{q}J$. Hence,

$$\begin{aligned} U_{k_q}(t) &= e^{i(q-1)t}\frac{1}{q}J + e^{-it}\left(I - \frac{1}{q}J\right) \\ &= \frac{1}{q}\left(e^{i(q-1)t} + (q-1)e^{-it}\right) I + \frac{1}{q}\left(e^{i(q-1)t} - e^{-it}\right)(J-I). \end{aligned} \tag{2.5.1}$$

We see that $U_{K_q}(t)$ is flat if and only if

$$\left|e^{i(q-1)t} + (q-1)e^{-it}\right| = \left|e^{i(q-1)t} - e^{-it}\right|$$

which restricts q to $\{2, 3, 4\}$. Further calculations show that uniform mixing occurs at time $\pi/4$ on K_2 and K_4, and occurs at time $2\pi/9$ on K_3.

Chapter 3

Cayley Graphs and Association Schemes

All the known graphs with uniform mixing are Cayley graphs constructed from finite abelian groups. As the quantum walk of a graph lies in its adjacency algebra, some of the mixing conditions on Cayley graphs can be nicely described using the language of association schemes, which provides a unified approach to many combinatorial topics including coding theory, design theory and graph theory. For details on association schemes, see Chapter 2 in [4]. In this chapter, we introduce the basic properties of Cayley graphs and association schemes. With these tools, we can build the isomorphism between linear Cayley graphs and the quotient Hamming graphs in Chapter 5, and investigate the relation between distance graphs of Hamming graphs and the Hamming scheme in Chapter 6.

3.1 Cayley Graphs

Let G be a group and $\mathcal{C}$ be a subset of G. The Cayley graph $X(G, \mathcal{C})$ is a graph with vertex set G and edge set

$$E = \{(g, h) : hg^{-1} \in \mathcal{C}\}.$$

We call $\mathcal{C}$ the connection set. Usually it is assumed that $\mathcal{C}$ does not contain the identity of the group G, in which case the graph is loopless. When $\mathcal{C}$ is closed under inverses, $X(G, \mathcal{C})$ is an undirected graph. In the rest of this thesis, all the Cayley graphs will be loopless and undirected.

For an element $x \in G$, the map $g \mapsto gx$ determines an automorphism of $X(G, \mathcal{C})$, which implies that $X(G, \mathcal{C})$ is vertex transitive. We are interested in the Cayley graphs whose vertices are the elements of a module.

3.1.1 Lemma. *Let G be the additive group of a module. For any automorphism L of the module, we have*

$$X(G, L(\mathcal{C})) \cong X(G, \mathcal{C})$$

where $L(\mathcal{C}) = \{L(c) : c \in \mathcal{C}\}$.

As an example, the Hamming graph $H(d, q)$ is a graph whose vertex set consists of all d-tuples from an alphabet of q symbols, and two vertices are adjacent if they differ in exactly one coordinate. For practical purposes, we can take $\mathbb{Z}_q^d$ as the alphabet. Then two vertices in $H(d, q)$ are adjacent if their difference is a non-zero multiple of a standard basis vector. By Lemma 3.1.1, the Hamming graph $H(d, q)$ is the Cayley graph $X(\mathbb{Z}_q^d, \mathcal{C})$ where $\mathcal{C}$ is the set of non-zero multiples of any basis of $\mathbb{Z}_q^d$.

When G is the additive group of a vector space, the Cayley graph $X(G, \mathcal{C})$ is called a *linear graph* if $\mathcal{C}$ is closed under multiplication by nonzero scalars in the underlying field. This applies to the Hamming graphs $H(d, q)$ where q is a prime power. In this case, instead of $\mathbb{Z}_q^d$, we construct our Hamming graph over a vector space $GF(q)^d$. By definition, $H(d, q)$ is a linear graph.

3.2 Association Schemes

In this section, we introduce asssociation schemes using the notions in Godsil's unpublished notes [15]. An association scheme with d classes is a set $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$ of 01-matrices that satisfies the following conditions:

- $A_0 = I$.
- $\sum_{j=0}^{d} A_j = J$.
- $A_j^T \in \mathcal{A}$ for $j = 0, 1, \cdots, n$.
- $A_j A_k = A_k A_j \in \operatorname{span}(\mathcal{A})$.

By the last condition, the association scheme $\mathcal{A}$ generates an algebra over $\mathbb{C}$, which we call the Bose-Mesner algebra $\mathbb{C}[\mathcal{A}]$ of $\mathcal{A}$. The second condition implies that $A_0, A_1, \ldots, A_d$ are linearly independent, so $\mathbb{C}[\mathcal{A}]$ has dimension $d+1$. Since each element in $\mathbb{C}[\mathcal{A}]$ is a 01-matrix, $\mathbb{C}[\mathcal{A}]$ is closed under Schur multiplication as well as complex conjugation and matrix transposition.

An association scheme is symmetric if $A_0, A_1, \ldots, A_d$ are symmetric. A natural way to obtain symmetric association schemes is setting A_i's to be the adjacency matrices of some carefully chosen undirected graphs on the same vertex set. One such class of schemes arises from distance regular graphs, which are regular graphs such that for any two vertices u and v, the number of vertices at distance i from u and at distance j from v only depends on the distance between u and v.

Let X be a distance regular graph of diameter d. Let X_r be the graph with the same vertex set where two vertices are adjacent if they are at distance r in X. Let $A_r = A(X_r)$. Then $\mathcal{A} = \{I, A_1, A_2, \ldots, A_d\}$ satisfies the four conditions above and is a symmetric association scheme. Consider a simple example where $X = K_q$. Since K_q is distance regular of diameter one, the scheme has one class, namely, $\mathcal{A} = \{I_q, J_q - I_q\}$. This is the simplest association scheme.

A *Hamming scheme* $\mathcal{H}(d,q)$ is an association scheme constructed from the Hamming graph $H(d,q)$, which is distance regular of diameter n. Note that $\mathcal{H}(1,q) = \{I_q, J_q - I_q\}$. In fact, $\mathcal{H}(d,q)$ is the generalized Hamming scheme $\mathcal{H}(n, \mathcal{H}(1,q))$. Refer to [16] by Godsil for further information on generalized Hamming schemes. We will discuss some results on uniform mixing in $\mathcal{H}(d,2)$ by Chan [7] in Chapter 4, and move to $\mathcal{H}(d,3)$ in Chapter 6.

3.3 Parameters of Association Schemes

Recall that the spectral decomposition of a diagonalizable matrix A is

$$A = \sum_r \theta_r E_r$$

where E_r's are pairwise orthogonal idempotents that sum to I. If A is the adjacency matrix of a distance regular graph X, then these E_r's are also the idempotents in the spectral decomposition of $A_i = A(X_i)$. We state without proof a general theorem that applies in all association schemes. Detailed derivation can be found in the work on generalized Hamming schemes due to Godsil [16].

3.3.1 Theorem. *The Bose-Mesner algebra of an association scheme $\mathcal{A}$ has a basis of idempotents $E_0, E_1, \ldots, E_d$ such that*

- $E_j E_k = \delta_{j,k} E_j$.
- $\sum_{j=0}^{d} E_j = I$. □

The above theorem implies that there are scalars $p_r(s)$, which are called the *eigenvalues of an association scheme $\mathcal{A}$*, such that

$$A_r = \sum_{s=0}^{n} p_r(s) E_s$$

for $r = 0, 1, \cdots, n$. For example, the idempotents in the Bose-Mesner algebra of $\{I_q, J_q - I_q\}$ are

$$E_0 = \frac{1}{q} J_q, E_1 = I_q - \frac{1}{q} J_q$$

and the eigenvalues are

$$p_0(0) = 1, p_0(1) = 1, p_1(0) = q - 1, p_1(1) = -1.$$

Now we introduce one more parameter of $\mathcal{A}$, which plays a role in characterizing uniform mixing in association schemes. Suppose the matrices in $\mathcal{A}$ are of size $n \times n$. Since the Bose-Mesner algebra $\mathbb{C}[\mathcal{A}]$ is closed under Schur multiplication, there exist scalars $q_{r,s}(k)$ such that

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

These scalars $q_{r,s}(k)$ are called the *Krein parameters* of $\mathcal{A}$. The following is a mixing condition in association schemes due to Mullin [22].

3.3.2 Theorem. *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 $\theta_0, \theta_1, \ldots, \theta_d$. Uniform mixing occurs on time t if and only if*

$$\sum_{r=0}^{d} \sum_{s=0}^{d} q_{r,s}(k) e^{(\theta_r - \theta_s)it} = 0$$

for all $1 \leq k \leq d$. □

Hence, if we know the Krein parameters of a scheme, we can determine whether uniform mixing occurs in its Bose-Mesner algebra.

Chapter 4

Earlier Work

In this chapter, we summarize the earlier work about uniform mixing on several families of regular graphs including complete graphs, cycles, bipartite graphs, strongly regular graphs, conference graphs, and Cayley graphs. These results can be found in [1, 2, 5, 6, 7, 18, 22].

4.1 Circulant Graphs

A matrix is circulant if each row is a right shift of the row above it. A graph with circulant adjacency matrix is called a circulant graph. Two examples of circulant graphs are the complete graphs K_n and the cycles C_n. In [2], Ahmadi et al noted that every $n \times n$ circulant matrix is unitarily diagonalizable by the Fourier matrix

$$F = \frac{1}{\sqrt{n}} V(\omega)$$

where w is the n-th root of unity, and $V(w)$ is the Vandermonde matrix whose ij-entry is w^{ij}, for $i, j = 0, 1, \cdots, n-1$. Based on the spectral properties of circulant graphs, Ahmadi et al had the following result on complete graphs.

4.1.1 Theorem. *Except for K_2, K_3, K_4, no complete graph admits uniform mixing.* □

For the cycles, they remarked that the eigenvalues of C_n are

$$\cos\left(\frac{2\pi j}{n}\right), \quad j = 0, 1, \cdots, n-1$$

Following this, Carlson et al [5] proved that no uniform mixing occurs on C_5. Soon after that, Adamczak et al [1] showed the non-uniform mixing property on cycles with the following lengths.

4.1.2 Theorem. *If n satisfies one of the following:*

- $n = 2^u$, *where* $u \geq 3$.
- $n = 2^u m$, *where* $u \geq 1$ *and* m *is not the sum of two integer squares.*

then no uniform mixing occurs on the cycle C_n. □

These supports the following conjecture due to Ahmadi et al [2].

4.1.1 Conjecture. *Except for* C_3, C_4, *no cycle admits uniform mixing.*

Further study on cycles by Godsil, Mullin and Roy [18] employed an algebraic number theoretic approach. Recall that the eigenvalues of a graph are the zeros of its characteristic polynomial and hence algebraic integers. The following two observations made by Mullin [18, pp. 6-7] link the algebraic property of the entries of a transition matrix with that of the eigenvalues.

4.1.3 Theorem. *Let X denote a graph. If at some non-zero time t all entries of the transition matrix $U(t)$ are algebraic numbers, then the ratio of any two non-zero eigenvalues of X must be rational.* □

4.1.4 Corollary. *Suppose that X is a regular graph with transition matrix $U(t)$. Further suppose that H is a matrix with all algebraic entries such that*

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

for some non-zero time t and some γ in $\mathbb{C}$. Then X must have all integral eigenvalues. □

The even cycles belong to the family of bipartite graphs. By a result due to Godsil on bipartite graphs, which we will mention in the next section, if uniform mixing occurs on an even cycle, its transition matrix must have algebraic entries. Noticing that $\cos(2\pi j/n)$ is irrational when $n = 5$ or $n \geq 7$, Mullin derived the following result.

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

This partly answered Conjecture 4.1.1. The general case for odd cycles is trickier, but the prime ones were solved by Mullin in [18, 22] using cyclic p-roots. A cyclic n-root is the solution of the form $z = (z_0, z_1, \ldots, z_{n-1})$ to the following system:

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

Mullin showed that a solution to this system is equivalent to a circulant type-II matrix with ones down the diagonal.

4.1.6 Lemma. *The matrix $\sum_{j=0}^{n-1} x_j C_j$ is a type-II matrix with ones down the diagonal if and only if $(x_1 x_0^{-1}, x_2 x_1^{-1}, \cdots, x_0 x_{n-1}^{-1})$ is a cyclic n-root.* □

Due to Haagerup [20], there are only finitely many cyclic p-roots when p is prime. Using this, Godsil, Mullin and Roy [18] proved that all the cyclic p-roots have algebraic coordinates, and thus $U(t)$ is a scalar multiple of a matrix with algebraic entries. By Corollary 4.1.4, C_p must have rational eigenvalues to admit uniform mixing, which restricts p to 3.

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

4.2 Bipartite Graphs

We move to the results on bipartite graphs, which were given by Godsil, Mullin and Roy in [18]. It was shown that the transition matrix $U(t)$ of a bipartite graph can be partitioned into four blocks, where the diagonal ones are real, and the off-diagonal ones are purely imaginary. Godsil characterized the entries of $U(t)$ for bipartite graphs when t is a mixing time.

4.2.1 Theorem. *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.* □

Following this, the scaled transition matrix $\sqrt{n}U(t)$ of a bipartite graph is a real Hadamard matrix [18], whose order is either two or a multiple of four.

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

Finally, Godsil, Mullin and Roy extended Theorem 4.1.2 to all regular bipartite graphs.

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

4.3 Complete Multipartite Graphs

A *complete multipartie graph* is a graph where two vertices are adjacenct if and only if they are in different partite sets of the vertex set. If all partite sets have the same size, it is called a *balanced complete multipartite graph*. It was originally proved by Ahmadi et al in [2] that $K_{2,2}$ is the only balanced complete multipartite graph that admit uniform mixing. In [22], Mullin reproduced this result using the following fact she discovered on graph complements.

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

Since the complement of a complete multipartite graph is disconnected, the above result implies the following.

4.3.2 Theorem. *No complete multipartite graph with more than four vertices admits uniform mixing.* □

4.4 Strongly Regular Graphs

We start this section by introducing strongly regular graphs using the definition given by Godsil and Royle in [19]. A graph X is called (n, k, a, c)*-strongly regular* if it is k-regular on n vertices, each pair of adjacenct vertices has a

common neighbors, and each pair of non-adjacent vertices has c common neighbors. It has exactly three eigenvalues k, θ, τ, and the spectral decomposition of its transition matrix is

$$U(t) = e^{ikt} E_k + e^{i\theta t} E_\theta + e^{i\tau t} E_\tau$$

A strongly regular graph X is *primitive* if both X and $\overline{X}$ are connected. Otherwise, it is called *imprimitive*. The only imprimitive strongly regular graphs are the disjoint unions of complete graphs of the same size. Chan [6] defined the following matrix

$$W := I + xA + y\overline{A}$$

where $A = A(X), \overline{A} = A(\overline{X})$, and discovered a necessary condition on the parameters for W being a complex Hadamard matrix.

4.4.1 Theorem. *X be a primitive strongly regular graph with eigenvalues k, θ, τ. If W is a complex Hadamard matrix, then X or $\overline{X}$ has one of the following parameter sets (n, k, a, c):*

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

Applying the above theorem, Godsil, Mullin and Roy [18] classfied the primitive strongly regular graphs that admit uniform mixing.

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

- *$J - 2A$ is a regular symmetric Hadamard matrix of order $4\theta^2$ with constant diagonal and positive row sum and θ is even.*
- *$J - 2A - 2I$ is a regular symmetric Hadamard matrix of order $4\theta^2$ with constant diagonal and positive row sum and θ is odd.*
- *The Paley graph of order 9, which has parameters* $(9, 4, 1, 2)$. □

4.5 Cayley graphs

In this section, we discuss some results about uniform mixing on Cayley graphs of symmetric groups and some abelian groups.

The transposition Cayley graph is a Cayley graph $X(S_n, T_n)$ over the symmetric group S_n with the set T_n of all transpositions as its connection set. Ahmadi et al conjectured in [2] that no Cayley graph $X(S_n, T_n)$ admits uniform mixing unless $n \neq 2$. This was soon proved by Gerhardt and Watrous in [14]. They looked at the Cayley graphs $X(S_n, C_\lambda)$ where C_λ is the conjugacy class of S_n that consists of all permutations having cycle structure described by the partition λ of n, and the following was implied by their results.

4.5.1 Theorem. *Uniform mixing does not occur on the transposition Cayley graph $X(S_n, T_n)$ for $n > 2$.* $\square$

We now move to the Cayley graphs over $\mathbb{Z}_q^d$ for $q \in \{2, 3, 4\}$. The first known Cayley graphs over $\mathbb{Z}_q^d$ that admit uniform mixing are the Hamming graphs $H(d, q)$ with $q \in \{2, 3, 4\}$. Followig this, Best et al [3] studied the folded d-cubes $H(d, 2)/\langle \mathbf{1} \rangle$ and characterized the ones that admit uniform mixing. It is worth noting that every Cayley graph over $\mathbb{Z}_2^d$ or $\mathbb{Z}_3^d$ is a *linear graph*, meaning that its connection set is closed under non-zero scalar multiplication. In [22], Mullin showed that the connected linear Cayley graphs over $GF(q)^r$ are quotients of the Hamming graphs $H(d, q)$ for some d (we treat this in detail in the next chapter). Hence every connected Cayley graph over $\mathbb{Z}_2^r$ is a quotient of $H(d, 2)$ for some d, and every connected Cayley graph over $\mathbb{Z}_3^r$ is a quotient of $H(d, 3)$ for some d. By the properties of equitable partitions and graph quotients, Mullin determined the transition matrix of a Hamming quotient.

4.5.2 Lemma. *Let Γ be a subgroup of $\mathbb{Z}_q^d$ with Hamming distance at least three. The transition matrix of the quotient graph $H(d, 3)/\Gamma$ satisfies*

$$U(t)_{0,v+\Gamma} = \frac{1}{n^d} \sum_{u \in v+\Gamma} (e^{(q-1)it} + (q-1)e^{-it})^{d-\mathrm{wt}(u)} (e^{(q-1)it} - e^{-it})^{\mathrm{wt}(u)}. \quad \square$$

Recall that uniform mixing occurs on K_2 and K_4 at time $\pi/4$ and occurs on K_3 at time $2\pi/9$. Using weight distributions of linear codes, Mullin established the following condition for the Cayley graphs over $\mathbb{Z}_2^d$, $\mathbb{Z}_3^d$ and the linear Cayley graphs over $\mathbb{Z}_4^d$ to admit uniform mixing at these times, respectively.

4.5.3 Theorem. *Let Γ be a subgroup of $\mathbb{Z}_2^d$ with minimum distance at least three. For each coset $v+\Gamma$, define n_j to be the number of elements a in $v+\Gamma$ such that $\mathrm{wt}(a) \equiv j \pmod 4$. 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*

$$(n_0 - n_2)^2 + (n_1 - n_3)^2 = |\Gamma|. \qquad \square$$

4.5.4 Theorem. *Let Γ be a subgroup of $\mathbb{Z}_3^d$ with minimum distance at least three such that $|\Gamma| = 3^s$, and let n_j be the number of elements a in the coset $v+\Gamma$ such that $\mathrm{wt}(a) \equiv j \pmod 3$. 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*

$$n_0 n_1 + n_0 n_2 + n_1 n_2 = 3^{2s-1} - 3^{s-1}. \qquad \square$$

4.5.5 Theorem. *Let Γ be a subgroup of $\mathbb{Z}_4^d$ with minimum distance at least three, and let n_j be the number of elements a in the coset $v+\Gamma$ such that $\mathrm{wt}(a) \equiv j \pmod 2$. 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*

$$(n_0 - n_1)^2 = |\Gamma|. \qquad \square$$

With this quotient approach, Mullin reproduced a result on the quotients $H(d,2)/\langle \mathbf{1} \rangle$ by Fan and Luo [13], and proved analogous results on the quotients $H(d,3)/\langle \mathbf{1} \rangle$ and $H(d,4)/\langle \mathbf{1} \rangle$.

4.5.6 Theorem. *If $d \geq 3$, then the quotient graph $H(d,2)/\langle \mathbf{1} \rangle$ admits uniform mixing at time $\pi/4$ if and only if d is odd.* $\square$

4.5.7 Theorem. *The quotient graph $H(d,3)/\langle \mathbf{1} \rangle$ admits uniform mixing at time $2\pi/9$ if and only if $d \equiv 1, 2 \pmod 3$.* $\square$

4.5.8 Theorem. *The quotient graph $H(d,4)/\langle \mathbf{1} \rangle$ admits uniform mixing at time $\pi/4$ if and only if d is odd.* $\square$

In addition, Mullin characterized the quotients $H(d,2)/\Gamma$ with $|\Gamma| = 4$ that admit uniform mixing at time $\pi/4$.

4.5.9 Theorem. *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 $\pi/4$ 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) $\mathrm{wt}(v_1) \equiv \mathrm{wt}(v_2) \pmod 4$ *and* $\mathrm{wt}(v_1+v_2) \equiv 2 \pmod 4$.

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

One example of the Cayley graphs over $\mathbb{Z}_2^d$, as we have seen in Chapter 2, is the d-cube, which admits uniform mixing at time $\pi/4$. Apart from this, Chan [7] has discovered some distance graphs of the d-cube that admit uniform mixing at earlier times. These Cayley graphs lie in the Hamming scheme $\mathcal{H}(d,q)$ with $q = 2$, whose eigenvalues $p_r(s)$ are the Krawtchouk polynomials [8],

$$p_r(s) = [x^r](1+(q-1)x)^{n-s}(1-x)^s.$$

Chan constructed a complex Hadamard matrix in the Bose-Mesner algebra of $\mathcal{H}(d,2)$:

$$H = (I_2 + \epsilon(J_2 - I_2))^{\otimes n}$$

where $\epsilon \in \{-1,1\}$. If the transition matrix of a graph X is equal to a unimodular scalar of H at time t, then X admits uniform mixing at t. More specifically, we have the following mixing conditions on the eigenvalues due to Chan [7].

4.5.10 Lemma. *Let X be a graph with adjacency matrix A belonging to the Bose-Mesner algebra of $\mathcal{H}(d,2)$. Suppose $AE_s = \theta_s E_s$, for $s = 0,1,\cdots,d$, where E_s' are the idempotents of the scheme. If there exists $\epsilon \in \{-1,1\}$ such that*

$$\theta_s - \theta_0 \equiv \epsilon s 2^{k-1} \pmod{2^{k+1}}$$

for $s = 0,1,\cdots,d$, then there exists $\beta \in \mathbb{R}$ such that

$$\sqrt{2^n} e^{-\pi i/2^k} A = e^{i\beta} H.$$

That is, X admits instantaneous uniform mixing at time $\pi/2^k$. □

Using two number theory results due to Lucas and Kummer [12] on base p representation for prime p, Chan proved the existence of graphs with earlier mixing time by exhibiting the following families of examples.

4.5.11 Theorem. *For $k \geq 2$ and $r \in \{2^{k+1}-7, 2^{k+1}-5, 2^{k+1}-3, 2^{k+1}-1\}$, the r-distance graphs of the Hamming graph $H(2^{k+2}-8, 2)$ admit uniform mixing at time $\pi/2^k$.* □

4.6 Summary

The only complete graphs that admit uniform mixing are K_2, K_3 and K_4, and the corresponding mixing times are $\pi/4$, $2\pi/9$ and $\pi/4$. No even cycle or prime cycle on more than three vertices admit uniform mixing. The number of vertices in a bipartite graph with uniform mixing is either two or divisible by four; if the graph is also regular, the number of vertices must be a sum of two integer squares. No balanced multipartite graph on more than four vertices admits uniform mixing. The only primitive strongly regular graphs with uniform mixing either come from regular symmetric Hadamard matrices, or is the Paley graph of order nine. For $q = 2, 3, 4$, a linear Cayley graph over $\mathbb{Z}_q^r$ is a quotient of $H(d, q)$ for some d, and whether it admits uniform mixing at the same time as $H(d, q)$ is determined by the weight distributions of the cosets of the corresponding subgroup. For earlier uniform mixing, there exist distance graphs over the d-cube that admit uniform mixing at $\pi/2^k$.

In the next two chapters, we will explore uniform mixing on the linear Cayley graphs over $\mathbb{Z}_3^d$ and $\mathbb{Z}_4^d$.

Chapter 5

Cayley Graphs over $\mathbb{Z}_3^d$

The last chapter has presented several results on uniform mixing on the Cayley graphs over $\mathbb{Z}_2^d$, $\mathbb{Z}_3^d$ and the linear Cayley graphs over $\mathbb{Z}_4^d$. In this chapter, we take a closer look at the Cayley graphs over $\mathbb{Z}_3^d$ with two different treatments. First, we apply Mullin's approach to uniform mixing on the quotients of $H(d,3)$ at time $2\pi/9$. Using weight distributions on the cosets of a subgroup, we describe the Hamming quotients $H(d+2,3)/\Gamma$ with valency $2(d+2)$that admit uniform mixing at $2\pi/9$. Next, we turn our interest to possible mixing time earlier than $2\pi/9$, and consider the spectral decompositions of the Cayley graphs over $\mathbb{Z}_3^d$, which are determined by the characters of the underlying groups. We provide another condition for uniform mixing at time t on these Cayley graphs, and use it to restrict the mixing time of $H(d,3)/\langle \mathbf{1} \rangle$ to $2\pi/9$.

5.1 Graph Quotients

A quotient of a graph X arises from an equitable partition of the vertices in X. Let $\pi = (C_1, C_2, \ldots, C_r)$ be a partition of $V(X)$. We say π is equitable if every vertex in C_j has the same number γ_{jk} of neighbors in C_k. Figure 5.1 is an example given by Brendan McKay [21] with equitable partition

$$\pi = \{\{1,2,4,5,7,8\},\{3,6\}\}.$$

Let G be an automorphism group of a graph X. Consider two orbits x^G and y^G. Since x is adjacent to y^g if and only if x^h is adjacent to y^{gh}, each

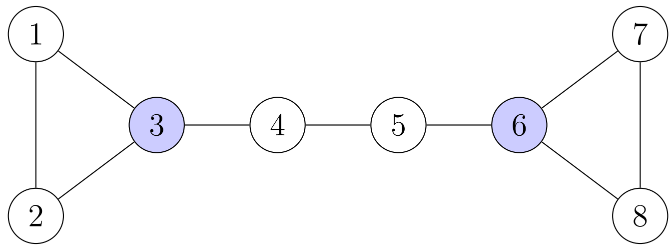

Figure 5.1: McKay's Example

element in x^G has the same number of neighbors in y^G. Hence, the orbits of G form an equitable partition of $V(X)$.

The *quotient graph* of X induced by an equitable partition

$$\pi = \{C_1, C_2, \ldots, C_r\}$$

is a directed graph with vertex set π and γ_{jk} arcs from C_j to C_k. We show that any quotient of a Cayley graph over an abelian group is also a Cayley graph.

5.1.1 Lemma. *Let $(G, +)$ be an abelian group. If Γ is a subgroup of G, then*

$$X(G, \mathcal{C})/\Gamma \cong X(G/\Gamma, \mathcal{C}/\Gamma)$$

where $\mathcal{C}/\Gamma = \{c + \Gamma : c \in \mathcal{C}\}$.

Proof. Since G is abelian, Γ is a normal subgroup, and so

$$G/\Gamma = \{g + \Gamma : g \in G\}$$

is a group with addition

$$(g + \Gamma) + (h + \Gamma) = (g + h) + \Gamma.$$

Let $g + \Gamma$ and $h + \Gamma$ be two vertices of $X(G, \mathcal{C})/\Gamma$. They are adjacent if and only if there exist $x, y \in \Gamma$ and $c \in \mathcal{C}$ such that $(g + x) - (h + y) = c$, if and only if

$$(g + \Gamma) - (h + \Gamma) = c + \Gamma \in \mathcal{C} + \Gamma.$$ □

If a graph is connected, so is its quotient. We have seen that when q is a prime power, $H(n, q)$ is a linear graph over a vector space. In fact, there are strong relations between the quotients of Hamming graphs and connected linear graphs for a vector space. The following theorem is an unpublished result due to Godsil, for a proof see Mullin [22, Ch.7] .

5.1.2 Theorem. *Every connected linear graph over $GF(q)^r$ with valency $(q-1)d$ is isomorphic to a quotient graph $H(d,q)/\Gamma$ for some d and some subgroup Γ of $GF(q)^d$, where $|\Gamma| = q^{d-r}$ and Γ has Hamming distance at least three.*

Proof. Let $\mathbb{F} = GF(q)$ and suppose $\mathcal{C}$ is the connection set of X. Notice that X is connected if and only if $\mathcal{C}$ contains a basis of V. We can partition $\mathcal{C}$ into cells $C_1, C_2, \ldots, C_d$ such that two elements lie in the same cell if and only if they are scalar multiples of each other, and the first r cells contains a basis of V. Then C_j is a cyclic group, and we may assume $C_j = \langle v_j \rangle$. Define a linear map from $\mathcal{C}$ to $\mathbb{F}^r \times \mathbb{F}^{d-r}$ by

$$\phi(v_j) = \begin{cases} (v_j, 0), & \text{if } v \in C_j \text{ for } j \in \{1, 2, \cdots, r\}, \\ (v_j, e_j), & \text{if } v_j \in C_j \text{ for } j \in \{r+1, r+2, \cdots, d\}. \end{cases}$$

Let

$$\mathcal{C}' = \{\phi(v) : v \in \mathcal{C}\}$$

Then $\mathcal{C}'$ consists of non-zero multiples of a basis of $\mathbb{F}^r \times \mathbb{F}^{d-r}$. Let Γ be the additive group of the vector space $\mathbb{F}^{d-r}$. We have

$$H(d,q)/\Gamma \cong X(\mathbb{F}^d, \mathcal{C}')/\Gamma \cong X(\mathbb{F}^r, \mathcal{C}). \qquad \square$$

The above proof constructed a map from linear Cayley graphs to Hamming quotients. Conversely, given a quotient graph $H(d,q)/\Gamma$ where Γ has Hamming distance at least three, we can find a connection set $\mathcal{C}$ of the Cayley graph that is isomorphic to $H(d,q)/\Gamma$. By Lemma 3.1.1, the connection set of a Cayley graph is not unique, but the following result gives a canonical form in terms of a matrix.

5.1.3 Theorem. *Let $GF(q)^d$ be a vector space. Let Γ be a subspace of $GF(q)^d$ with size q^{d-r} and Hamming distance at least three. If Γ is the column space of a matrix*

$$\begin{pmatrix} R \\ S \end{pmatrix}$$

where S is square and invertible, then $H(d,q)/\Gamma$ is a Cayley graph for $GF(q)^r$ with non-zero multiples of the columns of the matrix

$$\begin{pmatrix} I & -RS^{-1} \end{pmatrix}$$

as its connection set.

Proof. Suppose S is square and invertible. Let

$$P = \begin{pmatrix} I & RS^{-1} \\ 0 & S^{-1} \end{pmatrix}, \quad Q = \begin{pmatrix} I & RS^{-1} \end{pmatrix}$$

and let C, D be the sets of non-zero multiples of P, Q respectively. We have

$$P \begin{pmatrix} R \\ S \end{pmatrix} = \begin{pmatrix} 0 \\ I \end{pmatrix}.$$

Let Γ' be the column space of

$$\begin{pmatrix} 0 \\ I \end{pmatrix}.$$

If G and H are the additive groups of $GF(q)^n$ and $GF(q)^r$, then

$$H(n,q)/\Gamma \cong X(G/\Gamma', C/\Gamma') \cong X(H, D). \qquad \square$$

5.2 Quotients of $H(d, 3)$

We now focus on connected Cayley graphs over $\mathbb{Z}_3^n$. Since $H(d,3) = K_3^{\square d}$ admits uniform mixing at time $2\pi/9$, the first question is whether uniform mixing occurs on its quotients at the same time. We start with the following result on graph complements due to Godsil, Mullin and Roy [18].

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

This observation cuts our work in half on finding the Cayley graphs over $\mathbb{Z}_3^d$ with uniform mixing at time $2\pi/3^k$, where $k \geq d$. For example, by exploring the Cayley graphs over $\mathbb{Z}_3^3$ with valency at most 12, we find five graphs that admit uniform mixing at time $2\pi/9$, and so do their complements.

Using the weight distribution of Γ, Mullin [22] provided a characterization of the quotients $H(d,3)/\Gamma$ that admits uniform mixing at time $2\pi/9$. For a coset of Γ, we let n_j denote the number of elements in it with weight j modulo three.

5.2.2 Theorem. *Let Γ be 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 $2\pi/9$ if and only if the weight distribution of every coset of Γ satisfies*

$$n_0 n_1 + n_0 n_2 + n_1 n_2 = 3^{2s-1} - 3^{s-1}. \qquad \square$$

5.3 Groups with One Generator

We summarize the mixing property at $2\pi/9$ on $H(d+1,3)/\Gamma$ where Γ is generated by one element. We will show that these are either isomorphic to the quotient $H(d+1,3)/\langle \mathbf{1}\rangle$, or isomorphic to a Cartesian product of $H(s,3)/\langle \mathbf{1}\rangle$ with a Hamming graph, for some $s < d+1$. Uniform mixing at $2\pi/9$ in the former case was studied by Mullin in [22], and is characterized by the following.

5.3.1 Theorem. *The quotient graph $H(d+1,3)/\langle \mathbf{1}\rangle$ admits uniform mixing at time $2\pi/9$ if and only if $d \equiv 0, 1 \pmod 3$.* □

Let $\mathrm{wt}(a)$ denote the weight of the element a and let $\Gamma = \langle a\rangle$. By Theorem 5.1.3, the quotient $H(d+1,3)/\langle a\rangle$ is a Cayley graph over $\mathbb{Z}_3^d$ with the column space of some matrix Q whose first d columns are the standard basis as its connection set. By row reduction, column permutation, and column scaling of Q, we see that Q is equivalent to a block diagonal matrix

$$\begin{pmatrix} I_{d-\mathrm{wt}(a)} & 0 & 0 \\ 0 & I_{\mathrm{wt}(a)} & e_{d-\mathrm{wt}(a)+1} + e_{d-\mathrm{wt}(a)+2} + \cdots + e_d \end{pmatrix}.$$

This implies

$$H(d+1,3)/\langle a\rangle \cong H(d-\mathrm{wt}(a),3) \,\Box\, H(\mathrm{wt}(a),3)/\langle \mathbf{1}\rangle.$$

Recall that two graphs admit uniform mixing at time t if and only if their Cartesian product does. Since the Hamming graph $H(d-\mathrm{wt}(a),3)$ admits uniform mixing at $2\pi/9$, the left hand side admits uniform mixing at the same time if and only if the quotient $H(\mathrm{wt}(a),3)/\langle \mathbf{1}\rangle$ does. This leads to the following result.

5.3.2 Theorem. *Uniform mixing occurs on $H(d+1,3)/\langle a\rangle$ at time $2\pi/9$ if and only if $\mathrm{wt}(a)$ is congruent to one or two modulo three.* □

This theorem characterizes uniform mixing at time $2\pi/9$ on the connected Cayley graphs over $\mathbb{Z}_3^d$ with valency $2(d+1)$.

5.4 Groups with Two Generators

In this section, we apply Theorem 5.2.2 to the quotient graph $H(d+2,3)/\Gamma$ where Γ is generated by two elements. We give a sufficient and necessary condition on the group generators such that $H(d+2,3)/\Gamma$ admits uniform mixing at time $2\pi/9$.

5.4.1 Theorem. *Let Γ be a subgroup of $\mathbb{Z}_3^{d+2}$ with nine elements and minimum distance at least three. The quotient graph $H(d+2,3)/\Gamma$ admits uniform mixing at time $2\pi/9$ if and only if $\Gamma = \langle a, b\rangle$ for some $a, b \in \mathbb{Z}_3^{d+2}$ such that one of the following holds:*

(i)
- $a^T b \equiv 0 \pmod 3$, *and*
- $\operatorname{wt}(a) \not\equiv 0 \pmod 3$, $\operatorname{wt}(b) \not\equiv 0 \pmod 3$.

(ii)
- $a^T b \not\equiv 0 \pmod 3$, *and*
- $\operatorname{wt}(a) \not\equiv \operatorname{wt}(b) \pmod 3$ *or* $\operatorname{wt}(a) \equiv \operatorname{wt}(b) \equiv 0 \pmod 3$.

Proof. For notational convenience, we define the "weight structure" of the coset $\Gamma+c$ to be the tuple with coordinates n_0, n_1, n_2 in non-descending order, denoted by $W(\Gamma+c)$.

By Theorem 5.2.2, the quotient graph $H(d+2,3)/\langle a, b\rangle$ admits uniform mixing at time $2\pi/9$ if and only if the weight distribution of every coset $\Gamma+c$ satisfies

$$n_0n_1 + n_0n_2 + n_1n_2 = 24$$
$$n_0 + n_1 + n_2 = 9$$

which holds if and only if for all c,

$$W(\Gamma + c) \in \{(1, 4, 4), (2, 2, 5)\}.$$

We first show that $W(\Gamma)$ lies in the above set if and only if one of the conditions (i) and (ii) holds. Let

$$M = \begin{pmatrix} a & b \end{pmatrix}$$

and let

$$y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

be a vector in $\mathbb{Z}_3^2$. The weight of My is

$$\mathrm{wt}(My) = y^T M^T M y = \mathrm{wt}(y_1)\,\mathrm{wt}(a) + \mathrm{wt}(y_2)\,\mathrm{wt}(b) + 2y_1y_2a^Tb.$$

Thus the weights of the elements in Γ are

label	weight	multiplicity
w_0	0	1
w_1	$\mathrm{wt}(a)$	2
w_2	$\mathrm{wt}(b)$	2
w_3	$\mathrm{wt}(a) + \mathrm{wt}(b) + a^Tb$	2
w_4	$\mathrm{wt}(a) + \mathrm{wt}(b) + 2a^Tb$	2

Since Γ is a group of order nine, n_0 is odd and n_1, n_2 are even. We consider two cases.

(a) Suppose

$$W(\Gamma) = (1, 4, 4).$$

Then half of $\{w_1, w_2, w_3, w_4\}$ are one, and the rest are two.

- $\mathrm{wt}(a) = \mathrm{wt}(b) \neq 0$. Then $w_3 = w_4 \notin \{0, w_1\}$ if and only if $a^Tb = 0$.
- $\mathrm{wt}(a) = 2\,\mathrm{wt}(b) \neq 0$. Then $w_3 = a^Tb = 2w_4$. It follows that two of $\{w_1, w_2, w_3, w_4\}$ are one and the others are two if and only if $a^Tb \neq 0$.

(b) Suppose

$$W(\Gamma) = (2, 2, 5).$$

Then half of $\{w_1, w_2, w_3, w_4\}$ are zero, and the rest are one and two respectively.

- $\mathrm{wt}(a) = \mathrm{wt}(b) = 0$. Then $w_3 = a^Tb = 2w_4$. Thus $\{w_3, w_4\} = \{1, 2\}$ if and only if $a^Tb \neq 0$.
- $\mathrm{wt}(a) = 2\,\mathrm{wt}(b) \neq 0$. Then $w_3 = a^Tb = 2w_4$. It follows that $w_3 = w_4 = 0$ if and only if $a^Tb = 0$.

Summarizing the above yields the conditions (i) and (ii).

Next we show that if

$$W(\Gamma) \in \{(1, 4, 4), (2, 2, 5)\}$$

then
$$W(\Gamma + c) = W(\Gamma)$$
for all $c \in \mathbb{Z}_3^d$. First, the weight of the element $My + c$ in $\Gamma + c$ is
$$\mathrm{wt}(My + c) = (My + c)^T (My + c) = \mathrm{wt}(My) + 2(y_1 a^T c + y_2 a^T b) + \mathrm{wt}(c).$$
Since adding $\mathrm{wt}(c)$ to each weight does not change the weight structure, we may assume without loss of generality that $\mathrm{wt}(c) = 0$. Let
$$s_1 = a^T c,\ s_2 = b^T c,\ s_3 = a^T c + 2b^T c,\ s_4 = a^T c + b^T c.$$
Then the weights of $\Gamma + c$ are
$$\{0\} \cup \{w_j + \alpha s_j : \alpha = 1, 2,\ j = 1, 2, 3, 4\}.$$
Note that if we fix any two of $\{s_1, s_2, s_3, s_4\}$, then the others are linear combinations of these two elements. Thus if any two of $\{s_1, s_2, s_3, s_4\}$ are zero, then all of them are zero, in which case
$$W(\Gamma + c) = W(\Gamma).$$
Now if neither of $\{s_1, s_2, s_3, s_4\}$ is zero, then $s_1 = s_2$ or $s_1 = 2s_2$, which implies that one of s_3 and s_4 is zero, a contradiction. Hence it suffices to consider the case where exactly one of $\{s_1, s_2, s_3, s_4\}$ is zero.

(a) Suppose
$$W(\Gamma) = (1, 4, 4).$$
Then $n_0 = 1$ and $n_1 = n_2 = 4$. There are two cases of the weight changes, one of which is shown below.

$\mathrm{wt}(My)$	0	1	1	1	1	2	2	2	2
$\mathrm{wt}(My + c)$	0	1	1	0	2	0	1	0	1

(b) Suppose
$$W(\Gamma) = (2, 2, 5).$$
Then $n_0 = 5$ and $n_1 = n_2 = 2$. There are two cases of the weight changes, one of which is shown below.

$\mathrm{wt}(My)$	0	0	0	0	0	1	1	2	2
$\mathrm{wt}(My + c)$	0	1	2	1	2	1	1	0	1

In all cases, we have
$$W(\Gamma + c) = W(\Gamma). \qquad \square$$

This theorem characterizes uniform mixing at time $2\pi/9$ on the connected Cayley graphs over $\mathbb{Z}_3^d$ with valency $2(d + 2)$.

5.5 A Spectral Approach

We have seen several examples of Cayley graphs $X(\mathbb{Z}_3^d, \mathcal{C})$ that admit uniform mixing at time $2\pi/9$. In this section, we examine the quantum walk of $X(\mathbb{Z}_3^d, \mathcal{C})$ at other times, and give a mixing condition based on its spectral decomposition. It turns out that the eigenvalues and eigenvectors of a Cayley graph over an abelian group are determined by the characters of its underlying group. This is discussed in Chapter 6 of Godsil's unpublished notes [15]. Here we state the result for the Cayley graphs over $\mathbb{Z}_3^d$.

5.5.1 Lemma. *Let X be a Cayley graph over $\mathbb{Z}_3^d$ with connection set $\mathcal{C}$. For an element a of the vector space $\mathbb{Z}_3^d$, let $\psi_a : \mathbb{Z}_3^d \to \mathbb{C}$ be the map given by*

$$\psi_a(x) = e^{2\pi i a^T x/3}.$$

Then ψ_a is an eigenvector for $A(X)$ with eigenvalue $\psi_a(\mathcal{C})$, and

$$\psi_a(\mathcal{C}) = \frac{1}{2}(3|\mathcal{C} \cap a^{\perp}| - |\mathcal{C}|).$$

Moreover, the eigenvectors defined above are pairwise orthogonal, and they form a group isomorphic to the additive group of $\mathbb{Z}_3^d$. □

The transition matrix of a Cayley graph is determined by its first row, and we can obtain these entries using spectral decomposition.

5.5.2 Lemma. *The $0g$-entry of the transition matrix of $X(\mathbb{Z}_3^d, \mathcal{C})$ is*

$$U_X(t)_{0,g} = \frac{1}{3^d} \sum_{a \in \mathbb{Z}_3^d} e^{i\psi_a(\mathcal{C})t} \psi_a(g).$$

Proof. By Lemma 5.5.1,

$$V_\theta = \left\{ \frac{1}{\sqrt{3^d}} \psi_a : \psi_a(\mathcal{C}) = \theta \right\}$$

is an orthonormal basis of the eigenspace of θ. Hence the idempotents representing the projection onto the eigenspace of θ is

$$E_\theta = \frac{1}{3^d} \sum_{a:\psi_a(\mathcal{C})=\theta} \psi_a \psi_a^*.$$

By the spectral decomposition of $U_X(t)$, we have

$$U_X(t) = \frac{1}{3^d} \sum_{a \in \mathbb{Z}_3^d} e^{i\psi_a(\mathcal{C})t} \psi_a \psi_a^*.$$

Lastly note that

$$\psi_a(0)\overline{\psi}_a(g) = \overline{\psi}_a(g) = \psi_{-a}(g).$$ □

In the rest of this chapter, we will denote the eigenvalues of $X(\mathbb{Z}_3^d, \mathcal{C})$ by

$$\theta_a := \psi_a(\mathcal{C}).$$

Uniform mixing occurs on $X(\mathbb{Z}_3^d, \mathcal{C})$ when the first row of $U(t)$ is flat. More specifially, we have the following obeservation.

5.5.3 Lemma. *Let X be a Cayley graph over $\mathbb{Z}_3^d$ with connection set $\mathcal{C}$. Uniform mixing occurs on X at time t if and only if for all $g \in \mathbb{Z}_3^d$,*

$$\sum_{a,b\colon (a-b)^T g = 0} e^{i(\theta_a - \theta_b)t} = 3^d.$$

Proof. The condition

$$|U_X(t)_{0,g}|^2 = \frac{1}{3^d}$$

is equivalent to

$$\begin{aligned}
3^d &= \left| \sum_{a \in \mathbb{Z}_3^d} e^{i\theta_a t} e^{i\frac{2\pi}{3} a^T g} \right| \\
&= \sum_{a,b \in \mathbb{Z}_3^d} e^{i(\theta_a - \theta_b)t} e^{i\frac{2\pi}{3}(a-b)^T g} \\
&= \sum_{(a-b)^T g = 0} e^{i(\theta_a - \theta_b)t} + \sum_{(a-b)^T g = 1} e^{i(\theta_a - \theta_b)t} \left(e^{i\frac{2\pi}{3}} + e^{-i\frac{2\pi}{3}} \right) \\
&= \sum_{(a-b)^T g = 0} e^{i(\theta_a - \theta_b)t} - \sum_{(a-b)^T g = 1} e^{i(\theta_a - \theta_b)t}. && (5.5.1)
\end{aligned}$$

Applying 5.5.1 to the 00-entry of the transition matrix, we have

$$3^d = \sum_{a,b} e^{i(\theta_a - \theta_b)t} = \sum_{(a-b)^T g = 0} e^{i(\theta_a - \theta_b)t} + 2 \sum_{(a-b)^T g = 1} e^{i(\theta_a - \theta_b)t}. \qquad (5.5.2)$$

Combining 5.5.1 and 5.5.2 yields the desired condition. □

By Lemma 5.5.1, the difference between two eigenvalues of $X(\mathbb{Z}_3^d, \mathcal{C})$ is

$$\theta_a - \theta_b = \frac{3}{2}\left(|\mathcal{C} \cap a^\perp| - |\mathcal{C} \cap b^\perp|\right)$$

which is divisible by 3. Let

$$m_{ab} := \frac{\theta_a - \theta_b}{3}.$$

We define a rational function in x over the integers by

$$f_g(x) := \left(\sum_{a,b\colon (a-b)^T g = 0} x^{m_{ab}}\right) - 3^d. \tag{5.5.3}$$

Note that by symmetry in a and b, this is a palindromic polynomial divided by some power of x. The time t satisfies

$$\sum_{a,b\colon (a-b)^T g=0} e^{i(\theta_a - \theta_b)t} = 3^d$$

if and only if e^{3it} is a zero of f_g. Thus, we obtain a characterizaion for uniform mixing on Cayley graphs over $\mathbb{Z}_3$ in terms of these f_g's.

5.5.4 Theorem. *$X(\mathbb{Z}_3^d, \mathcal{C})$ admits uniform mixing at time t if and only if e^{3it} is a zero of*

$$\gcd\{f_g : g \in \mathbb{Z}_3^d\}. \qquad \square$$

For example, we compute $\gcd(f_{\mathbf{0}}, f_{\mathbf{1}})$ for the quotients

$$H(d+1, 3)/\left\langle \mathbf{1} \right\rangle$$

with $d = 2, 3, 4$. The calculation of $f_{\mathbf{1}}$ is done in Corollary 5.6.4, and $f_{\mathbf{0}}$ is computed similarly.

d	$\gcd(f_{\mathbf{0}}, f_{\mathbf{1}})$
3	$\Phi_3(x)^2$
4	$\Phi_3(x)$
5	1

It follows that uniform mixing cannot occur at time earlier than $2\pi/9$ in these graphs. We will prove this result for all positive integers d over $\mathbb{Z}_3^d$ in the next section. Now we use the above theorem to give a lower bound on the valency of Cayley graphs over $\mathbb{Z}_3^d$ with uniform mixing at time $2\pi/3n$.

5.5.5 Corollary. *Let $\phi(n)$ be the Euler's totient function. If uniform mixing occurs on $X(\mathbb{Z}_3^d, \mathcal{C})$ at time $2\pi/3n$, then*

$$|\mathcal{C}| \geq \phi(n) + 2$$

Proof. Let $g \in \mathcal{C}$. For $a, b \in \mathbb{Z}_3^d$ such that $(a-b)^T g = 0$,

$$|\mathcal{C} \cap a^\perp| - |\mathcal{C} \cap b^\perp| \leq |\mathcal{C}| - 2.$$

Hence

$$\deg(f_g) \leq |\mathcal{C}| - 2.$$

If $X(\mathbb{Z}_3^d, \mathcal{C})$ admits uniform mixing at $2\pi/3n$, then f_g is divisible by the n-th cyclotomic polynomial $\Phi_n(n)$ with degree $\phi(n)$. Thus

$$\phi(n) \leq |\mathcal{C}| - 2. \qquad \square$$

5.6 The Quotient $H(d+1,3)/\langle \mathbf{1} \rangle$

In this section, we prove that $2\pi/9$ is the earliest mixing time for the quotient $H(d+1,3)/\langle \mathbf{1} \rangle$. We start with its eigenvalues using the formula from the last section.

5.6.1 Lemma. *The eigenvalues for $H(d+1,3)/\langle \mathbf{1} \rangle$ are*

$$\theta_a = \begin{cases} 2d - 1 - 3\,\mathrm{wt}(a) + 3, & a^T \mathbf{1} = 0, \\ 2d - 1 - 3\,\mathrm{wt}(a), & a^T \mathbf{1} \neq 0. \end{cases}$$

Proof.

The folded Hamming graph $H(d+1,3)/\langle \mathbf{1} \rangle$ is a Cayley graph over $\mathbb{Z}_3^d$ with connection set

$$\mathcal{C} = \{\pm e_1, \pm e_2, \cdots, \pm e_d, \pm \mathbf{1}\}$$

Note that $e_j \in a^\perp$ if and only if the j-th entry of a is zero. Thus

$$|\mathcal{C} \cap a^\perp| = \begin{cases} 2(d - \mathrm{wt}(a) + 1), & a^T\mathbf{1} = 0 \\ 2(d - \mathrm{wt}(a)), & a^T\mathbf{1} \neq 0 \end{cases}$$

Then the result follows from Lemma 5.5.1. □

With this in mind, we calculate the weight distribution of the underlying group $\mathbb{Z}_3^d$, and give an explicit expression of $f_\mathbf{1}$.

5.6.2 Lemma. *Let n_j denote the number of elements in $\langle\mathbf{1}\rangle^\perp$ with weight j. Then*

$$n_j = \frac{1}{3}\binom{d}{j}(2^j + 2(-1)^j).$$

Proof. The homogeneous weight enumerator of a linear code C is given by

$$W_C(x,y) = \sum_{j=0}^{d} n_j x^{d-j} y^j.$$

We apply this to the code generated by $\mathbf{1}$,

$$W_{\langle\mathbf{1}\rangle}(x,y) = x^d + 2y^d.$$

By MacWilliams' Theorem,

$$\begin{aligned} W_{\langle\mathbf{1}\rangle^\perp}(x,y) &= \frac{1}{3} W_{\langle\mathbf{1}\rangle}(x+2y, x-y) \\ &= \frac{1}{3}\sum_{j=0}^{d}\binom{d}{j}(2^j + 2(-1)^j)x^{d-j}y^j. \end{aligned}$$

□

5.6.3 Lemma. *Let ℓ_j denote the number of elements in*

$$\{a \in \mathbb{Z}_3^d : a^T\mathbf{1} = 1\}$$

with weight j. Then

$$\ell_j = \frac{1}{3}\binom{d}{j}(2^j - (-1)^j).$$

Proof. The total number of elements in $\mathbb{Z}_3^d$ with weight j is $\binom{d}{j}2^j$. Since $a \mapsto 2a$ gives a bijection between

$$\{a : w(a) = w,\, a^T g = 1\}$$

and

$$\{a : w(a) = w,\, a^T g = 2\}$$

we have

$$2\ell_j = \binom{d}{j}2^j - n_j$$

which determines ℓ_j. □

5.6.4 Corollary. *For the Hamming quotient $H(d+1,3)/\langle \mathbf{1}\rangle$,*

$$f_{\mathbf{1}}(x) = \frac{1}{3x^d}(2x^2+5x+2)^d + \frac{2}{3x^d}(-1)^d(x^2-2x+1)^d - 3^d. \tag{5.6.1}$$

Proof. By the above two lemmas,

$$\begin{aligned} f_{\mathbf{1}}(x) &= \sum_{(a-b)^T\mathbf{1}=0} x^{m_{ab}} - 3^d \\ &= \sum_{a^T\mathbf{1}=b^T\mathbf{1}=0} x^{\mathrm{wt}(a)-\mathrm{wt}(b)} + 2\sum_{a^T\mathbf{1}=b^T\mathbf{1}=1} x^{\mathrm{wt}(a)-\mathrm{wt}(b)} - 3^d \\ &= \sum_{j=0}^{d}\sum_{k=0}^{d}(n_jn_k + 2\ell_j\ell_k)x^{j-k} - 3^d \\ &= \frac{1}{3}\sum_{j=0}^{d}\sum_{k=0}^{d}\binom{d}{j}\binom{d}{k}\left(2^{j+k} + 2(-1)^{j+k}\right)x^{j-k} - 3^d. \end{aligned}$$

We calculate the double sum on the right hand side. First,

$$\begin{aligned} \sum_{j=0}^{d}\sum_{k=0}^{d}\binom{d}{j}\binom{d}{k}2^{j+k}x^{j-k} &= \sum_{k=0}^{d}\binom{d}{k}\left(\frac{2}{x}\right)^k\sum_{j=0}^{d}\binom{d}{j}(2x)^j \\ &= \left(\frac{2}{x}+1\right)^d(2x+1)^d \end{aligned}$$

by binomial expansion. Likewise,

$$\begin{aligned}\sum_{j=0}^{d}\sum_{k=0}^{d}\binom{d}{j}\binom{d}{k}2(-1)^{j+k}x^{j-k} &= 2\sum_{k=0}^{d}\binom{d}{k}\left(-\frac{1}{x}\right)^{k}\sum_{j=0}^{d}\binom{d}{j}(-x)^{j}\\ &= 2\left(1-\frac{1}{x}\right)^{d}(1-x)^{d}.\end{aligned}$$

Rearranging this in $f_{\mathbf{1}}$ yields the desired expression. □

It is clear that $f_{\mathbf{1}}$ is palindromic. Moreover, Equation 5.6.1 makes it easy to substitute $x+1/x$ by another variable z. If x is on the unit circle of the complex plane, then $1/x=\bar{x}$ and so z is real. Using this fact, we prove that $H(d+1,3)/\langle \mathbf{1}\rangle$ never admits uniform mixing except at time $2k\pi/9$ for some k coprime to 3.

5.6.5 Theorem. *If uniform mixing occurs on $H(d+1,3)/\langle \mathbf{1}\rangle$ at time t, then $t=2k\pi/9$ for some integer k coprime to 3.*

Proof. Let

$$z = x+\frac{1}{x}$$

and substitute this into equation 5.6.1,

$$h_{\mathbf{1}}(z)=\frac{1}{3}(2z+5)^{d}+\frac{2}{3}(-1)^{d}(z-2)^{d}-3^{d}.$$

We remark that any zero of $f_{\mathbf{1}}$ on the unit circle corresponds uniquely to a zero of $h_{\mathbf{1}}$ in the real interval $[-2,2]$. Note that

$$h_{\mathbf{1}}(-1)=0$$

which implies that $e^{2i\pi/3}$ is a zero of $f_{\mathbf{1}}$. Further, when $d>1$,

$$h_{\mathbf{1}}(2)\neq 0$$

so it suffices to consider the interval $[-2,2)$. The derivative of $h_{\mathbf{1}}$ is

$$h_{\mathbf{1}}'(z)=\frac{2d}{3}(2z+5)^{d-1}-\frac{2d}{3}(2-z)^{d-1}$$

Since

$$\frac{2z+5}{2-z}=-2-\frac{9}{z-2}$$

which is greater than or equal to 1 when $z\in[-1,2)$, and is less than 1 and greater than 0 when $z\in[-2,-1)$, $z=-1$ is the stationary point and the only zero of $h_{\mathbf{1}}$ in the interval $[-2,2)$. Hence, $H(d+1,3)/\langle \mathbf{1}\rangle$ does not admit uniform mixing at time other than $2k\pi/9$ for some k coprime to 3. □

The method we used in this section restricts the mixing times to certain choices. However, it is not an easy way to prove uniform mixing actually occurs at some time, unless the connection set is symmetric enough, in which case we have fewer constraints. We note that the r-distance graph of $H(d,3)$ is a Cayley graph over $\mathbb{Z}_3^d$ whose connection set consists of all the elements in $\mathbb{Z}_3^d$ with weight r, which is symmetric about all coordinates. Thus, these graphs are likely to admit uniform mixing. In fact, as we will see in the next chapter, there are families of graphs in the Hamming scheme $\mathcal{H}(d,3)$ that admit uniform mixing at time $2\pi/3^k$.

5.7 Cayley Graphs over $\mathbb{Z}_3^3$

The Cayley graphs over $\mathbb{Z}_3^3$ have 27 vertices. By Theorem 4.3.2, only the connected ones with connected complements could admit uniform mixing. We calculate $\gcd(f_0, f_{e_1})$ for these graphs which are not Cartesian products, and list the results in the following chart. Here $\mathcal{C}'$ is the subset of $\mathcal{C}$ where the first non-zero entry is one for each element.

$\mathcal{C}'\backslash\{e_1, e_2, \ldots, e_d\}$	$\gcd(f_0, f_{e_1})$	earliest mixing time
$\emptyset$	$\Phi_3(x)$	$2\pi/9$
$\{(1,1,1)\}$	$\Phi_3(x)^2$	$2\pi/9$
$\{(1,1,1),(1,1,2)\}$	1	∞
$\{(1,1,0),(1,0,1)\}$	$\Phi_3(x)$	$2\pi/9$
$\{(1,1,0),(1,0,1),(1,2,1)\}$	$\Phi_3(x)$	$2\pi/9$
$\{(1,1,0),(1,0,1),(1,1,1)\}$	$\Phi_3(x)$	$2\pi/9$
$\{(0, 1, 1), (1, 2, 2), (1, 2, 0), (1, 0, 1)\}$	$\Phi_3(x)$	$2\pi/9$
$\{(1, 0, 1), (1, 0, 2), (1, 2, 0), (0, 1, 1)\}$	$\Phi_3(x)$	$2\pi/9$
$\{(1, 0, 1), (1, 2, 1), (1, 2, 2), (1, 1, 0), (0, 1, 1)\}$	1	∞
$\{(1, 1, 1), (1, 0, 1), (1, 0, 2), (1, 2, 0), (0, 1, 1)\}$	$\Phi_3(x)$	$2\pi/9$
$\{(0, 1, 2), (1, 2, 1), (1, 1, 2), (1, 0, 2), (1, 0, 1)\}$	1	∞

$\{(1, 2, 2), (1, 1, 2), (1, 1, 0), (1, 0, 1), (0, 1, 1), (1, 2, 1)\}$	1	∞
$\{(1, 2, 0), (0, 1, 1), (1, 0, 1), (1, 0, 2), (1, 1, 0), (1, 2, 2)\}$	1	∞
$(0, 1, 2), (1, 2, 1), (1, 1, 2), (1, 0, 2), (0, 1, 1), (1, 0, 1)$	$\Phi_3(x)$	$2\pi/9$
$\{(1, 1, 0), (1, 2, 2), (1, 2, 0), (1, 1, 1), (0, 1, 1), (1, 0, 1), (1, 0, 2)\}$	1	∞
$\{(0, 1, 2), (1, 2, 2), (1, 2, 1), (1, 1, 2), (1, 0, 2), (0, 1, 1), (1, 0, 1)\}$	$\Phi_3(x)$	$2\pi/9$
$\{(1, 1, 2),(1, 2, 2),(1, 0, 1), (0, 1, 1),(1, 1, 1),(1, 2, 1), (1, 0, 2),(0, 1, 2)\}$	1	∞
$\{(1, 1, 0),(1, 2, 2),(1, 0, 1), (0, 1, 1),(1, 1, 1),(1, 2, 1), (1, 0, 2),(0, 1, 2),(1, 1, 2)\}$	1	∞

Using either the quotient approach or the spectral approach, we found five complementary pairs of connected Cayley graphs over $\mathbb{Z}_3^3$ that admit uniform mixing at time $2\pi/9$.

5.8 Analogy with Cubelike Graphs

In the end of this chapter, we apply the idea in Section 5.5 to the cubelike graphs, and state the corresponding results without proof.

5.8.1 Lemma. *Let X be a Cayley graph over $\mathbb{Z}_2^d$ with connection set $\mathcal{C}$. For an element a of the vector space $\mathbb{Z}_2^d$, let $\psi_a : \mathbb{Z}_2^d \to \mathbb{C}$ be the map given by*

$$\psi_a(x) = (-1)^{a^T x}.$$

Then ψ_a is an eigenvector for $A(X)$ with eigenvalue $\psi_a(\mathcal{C})$, and

$$\psi_a(\mathcal{C}) = 2|\mathcal{C} \cap a^{\perp}| - |\mathcal{C}|.$$

Moreover, the eigenvectors defined above are pairwise orthogonal, and they form a group isomorphic to the additive group of $\mathbb{Z}_2^d$. □

We denote the eigenvalues of $X(\mathbb{Z}_2^d, \mathcal{C})$ by

$$\theta_a := \psi_a(\mathcal{C})$$

and let

$$m_{ab} := \frac{\theta_a - \theta_b}{3}.$$

5.8.2 Theorem. *Let*

$$f_g(x) := \left(\sum_{a,b:\,(a-b)^T g=0} x^{m_{ab}} \right) - 2^d.$$

$X(\mathbb{Z}_3^d, \mathcal{C})$ admits uniform mixing at time t if and only if e^{2it} is a zero of

$$\gcd\{f_g : g \in \mathbb{Z}_2^d\}.$$ □

5.8.3 Corollary. *Let $\phi(n)$ be the Euler's totient function. If*

$$|\mathcal{C}| < \phi(n) - 1$$

then uniform mixing does not occur on $X(\mathbb{Z}_2^d, \mathcal{C})$ at time π/n. □

5.8.4 Theorem. *If uniform mixing occurs on the folded cubes $H(d+1, 2)/\langle \mathbf{1} \rangle$ at time t, then $t = k\pi/4$ for some odd integer k.* □

Chapter 6

Mixing in Hamming Distance Graphs

So far, our examples of Cayley graphs over $\mathbb{Z}_3^d$ admit uniform mixing at time no earlier than $2\pi/9$. However, this is not true in general. In this chapter, we investigate the graphs whose adjacency matrices are in the adjacecy algebra of $H(d,3)$. We introduce the concepts of an association scheme and its Bose-Mesner algebra. The condition for uniform mixing to occur in a Bose-Mesner algebra is equivalent to the algebra containing a complex Hadamard matrix. We review the characterization of uniform mixing in the Bose-Mesner algebra of $\mathcal{H}(d,2)$ given by Chan [7], and extend her work to $\mathcal{H}(d,3)$ and $\mathcal{H}(d,4)$. Finally, we give a family of graphs in $\mathcal{H}(d,3)$ that admit uniform mixing at time $2\pi/3^k$, and a family of graphs in $\mathcal{H}(d,4)$ that admit uniform mixing at time $\pi/2^k$. By Lemma 5.2.1, their complements admit uniform mixing at the corresponding times as well.

6.1 Eigenvalues of the Hamming Schemes

In [7], Chan showed that whether a graph X admits uniform mixing depends only on its spectrum and the eigenvalues of the Bose-Mesner algebra containing its adjacency matrix.

6.1.1 Theorem. *Let X be a graph on v vertices whose adjacency matrix belongs to the Bose-Mesner algebra of $\mathcal{A}$. Let $p_j(s)$ be the eigenvalues of $\mathcal{A}$.*

Suppose the spectral decomposition of $A(X)$ is

$$A(X) = \sum_{s=0}^{d} \theta_s E_s$$

The continuous quantum walk of X is uniform mixing at time τ if and only if there exist scalars $t_0, t_1, \ldots, t_d$ such that

- $|t_0| = |t_1| = \cdots = |t_d| = 1$
- $\sqrt{v}e^{i\tau\theta_s} = \sum_{j=0}^{d} p_j(s)t_j$ *for* $s = 0, 1, \cdots, d$. □

In this section, we look at the eigenvalues of the Hamming schemes derived by Chan, and discuss some properties of these eigenvalues, which will be instrumental in finding graphs with uniform mixing in the Bose-Mesner algebra of a Hamming scheme.

The Hamming scheme $\mathcal{H}(d, q)$ consists of the adjacency matrices of the distance graphs of the Hamming graph $H(d, q)$. It is noted by Godsil in [16] that $\mathcal{H}(d, q)$ is a generalized Hamming scheme of $\mathcal{H}(1, q)$. The following construction of a generalized Hamming scheme comes from [16].

Suppose $\mathcal{A}$ is a d-class association scheme with vertex set V. For two elements $v, w \in V^n$, let $h(v, w)$ be the vector of length $d+1$ with r-th entry equal to the number of coordinates j such that v_j and w_j are r-related in $\mathcal{A}$. For any integer vector x of length $d+1$ whose entries sum to n, we define A_x to be the 01-matrix with rows and columns indexed by V^n, and with $A_{v,w}$ equal to one if and only if $h(v, w) = x$. These matrices form a generalied Hamming scheme, denoted $\mathcal{H}(n, \mathcal{A})$.

If the base scheme $\mathcal{A}$ is the Hamming scheme $\mathcal{H}(1, q)$, then x is a vector of length two, and two n-tuples from V^n are adjacent in a graph with adjacency matrix A_x if there are x_0 coordinates that are equal, that is, 0-related. The following result due to Godsil describes the relation between the idempotents of the association schemes $\mathcal{H}(n, \mathcal{A})$ and $\mathcal{A}$.

6.1.2 Theorem. *Let $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$ be an association scheme with d classes. Let α be a vector of length $d+1$ with non-negative integer entries summing to n. The adjacency matrices in $\mathcal{H}(n, \mathcal{A})$ are*

$$A_\alpha = \sum A_{j_1} \otimes A_{j_2} \otimes \cdots \otimes A_{j_r}$$

where A_r occurs exactly α_r times, for $r = 0, 1, \cdots, d$, and the principal idempotents of $\mathcal{H}(n, \mathcal{A})$ are

$$E_\alpha = \sum E_{j_1} \otimes E_{j_2} \otimes \cdots \otimes E_{j_r}$$

where E_r occurs exactly α_r times, for $r = 0, 1, \cdots, d$. □

Using this relation, Chan [7] showed that the eigenvalues of $\mathcal{H}(d, q)$ satisfy

$$p_r^{(d)}(s) = [x^r](1 + (q-1)x)^{d-s}(1-x)^s \tag{6.1.1}$$

for $s = 0, 1, \cdots, d$. These coincide with the Krawtchouk polynomials $k_r(s, q, d)$ [8]. When d is clear in the context, we write $p_r(s)$ for short. We have the following properties.

6.1.3 Lemma. *Let $p_r(s)$ be the eigenvalues of the Hamming scheme $\mathcal{H}(d, q)$. Then*

(i) $p_r(s) = \sum_h (-q)^h (q-1)^{r-h} \binom{d-h}{r-h} \binom{s}{h}$.

(ii) $p_r(s) - p_r(s-1) + (q-1)p_{r-1}(s) + p_{r-1}(s-1) = 0$.

(iii) $p_r^{(d+1)}(s) - p_r^{(d+1)}(s+1) = q p_{r-1}^{(d)}(s)$.

(iv) If $q = 2$, then

$$p_{r-1}(s) - p_{r-1}(s+2) = 4 \sum_h (-2)^h \binom{d-2-h}{r-2-h} \binom{s}{h}.$$

Proof. By Equation (6.1.1),

$$\begin{aligned}
p_r(s) &= [x^r](1 + (q-1)x)^{d-s}(1 + (q-1)x - qx)^s \\
&= [x^r] \sum_h \binom{s}{h} (1 + (q-1)x)^{d-h} (-qx)^h \\
&= \sum_h \left([x^h] \binom{s}{h} (-qx)^h \right) \left([x^{r-h}](1 + (q-1)x)^{d-h} \right) \\
&= \sum_h (-q)^h (q-1)^{r-h} \binom{d-h}{r-h} \binom{s}{h}.
\end{aligned}$$

Properties (ii) and (iii) follow from Equation (6.1.1), and Property (iv) follows from the above three properties for $q = 2$. □

6.2 Uniform Mixing in Hamming Schemes

Recall that a graph on n vertices admits uniform mixing at time t if and only if $\sqrt{n}U(t)$ is equal to a complex Hadamard matrix. Let $\mathcal{B}(q)$ denote the Bose-Mesner algebra of the Hamming scheme $\mathcal{H}(d,q)$. Using Theorem 6.1.1, Chan showed that $\mathcal{B}(q)$ contains a complex Hadamard matrix if and only if $q \in \{2,3,4\}$ [7]. In the case $q=2$, Chan constructed a complex Hadamard matrices in $\mathcal{B}(2)$,

$$e^{i\beta}(I_2 + \epsilon(J_2 - I_2))^{\otimes d}$$

where $\beta \in \mathbb{R}$ and $\epsilon \in \{1,-1\}$, equated it with the scaled transition matrix $\sqrt{2^d}U(t)$ of a graph with adjacency matrix in $\mathcal{B}(2)$, and derived a sufficient condition for the quantum walk being uniform mixing at time $\pi/2^k$. These examples suggest a direction in finding graphs with uniform mixing at earlier times. We extend her construction to $\mathcal{B}(q)$ with $q \in \{2,3,4\}$.

6.2.1 Lemma. *Let ζ_q be a primitive q-th root of unity. For $q \in \{2,3,4\}$, the matrix*

$$e^{i\beta}(I_q + \zeta_{6-q}(J_q - I_q))^{\otimes d}$$

is a complex Hadamard matrix in the Bose-Mesner algebra of $\mathcal{H}(d,q)$. □

Proof. First note that $I_q + \zeta_{6-q}(J_q - I_q)$ is a complex Hadamard matrix of order q for $q \in \{2,3,4\}$. In fact, it is a scalar multiple of $U_{K_q}(\tau)$ where τ is a mixing time of K_q. Now if H_1 and H_2 are both complex Hadamard matrices of order q, then $H_1 \otimes H_2$ is flat and

$$(H_1 \otimes H_2)(H_1 \otimes H_2)^{(-)} = (H_1 H_1^{(-)}) \otimes (H_2 H_2^{(-)}) = q^2 I_{q^2}.$$

Therefore $H_1 H_2$ is a complex Hadamard matrix of order q^2. Lastly, a unimodular scalar of a complex Hadamard matrix is again a complex Hadamard matrix. □

The following is an analog to Lemma 3.2 in Chan's work [7].

6.2.2 Lemma. *Let X be a graph in $\mathcal{B}(q)$ with eigenvalues $\theta_0, \theta_1, \ldots, \theta_d$, and let $\epsilon \in \{1,-1\}$. Suppose $k \geq 2$.*

(i) If $q=2$, and

$$\theta_s - \theta_0 \equiv \epsilon 2^{k-1} s \pmod{2^{k+1}}$$

for $s = 0,1,\cdots,d$, then X admits uniform mixing at time $\pi/2^k$.

(ii) If $q=3$, and

$$\theta_s - \theta_0 \equiv \epsilon 3^{k-1} s \pmod{3^k}$$

for $s=0,1,\cdots,d$, then X admits uniform mixing at time $2\pi/3^k$.

(iii) If $q=4$, and

$$\theta_s - \theta_0 \equiv 2^k s \pmod{2^{k+1}}$$

for $s=0,1,\cdots,d$, then X admits uniform mixing at time $\pi/2^k$.

Proof. Suppose $q \in \{2,3,4\}$. Let

$$\begin{aligned} H_q &= e^{i\beta}(I_q + \zeta_{6-q}(J_q - I_q))^{\otimes d} \\ &= e^{i\beta}\left((1+(q-1)\zeta_{6-q})\left(\frac{1}{q}J_q\right) + (1-\zeta_{6-q})\left(I_q - \frac{1}{q}J_q\right)\right)^{\otimes d} \end{aligned}$$

and let $A \in \mathcal{B}(q)$ with spectral decomposition

$$A = \sum_{r=0}^{d} \theta_r E_r.$$

By Theorem 6.1.2,

$$H_q = e^{i\beta}\sum_{r=0}^{d}(\zeta_{6-q})^r A_r$$

where A_r is the adjacency matrix of the r-distance graph of $H(d,q)$. Hence the condition

$$\sqrt{q^d}e^{itA} = H_q$$

is equivalent to

$$\sqrt{q^d}e^{it\theta_s} = e^{i\beta}\left(1+(q-1)\zeta_{6-q}\right)^{d-s}\left(1-\zeta_{6-q}\right)^s$$

for $s=0,1,\cdots,d$, which gives

$$\sqrt{q^d}e^{i\theta_0 t} = e^{i\beta}(1+(q-1)\zeta_{6-q})^d \tag{6.2.1}$$

and

$$e^{i(\theta_s-\theta_0)t} = \left(\frac{1-\zeta_{6-q}}{1+(q-1)\zeta_{6-q}}\right)^s \tag{6.2.2}$$

For $s=0,1,\cdots,d$.

(i) For $q = 2$, Equation (6.2.2) reduces to

$$\frac{2^k}{\pi}(\theta_s - \theta_0)t \equiv \epsilon 2^{k-1}s \pmod{2^{k+1}}.$$

(ii) For $q = 3$, Equation (6.2.2) reduces to

$$\frac{3^k}{2\pi}(\theta_s - \theta_0)t \equiv \epsilon 3^{k-1}s \pmod{3^k}.$$

(iii) For $q = 4$, Equation (6.2.2) reduces to

$$\frac{2^k}{\pi}(\theta_s - \theta_0)t \equiv 2^k s \pmod{2^{k+1}}.$$

Thus, for $q \in \{2, 3, 4\}$, if $\theta_s - \theta_0$ satisfies the corresponding condition in the lemma, then there exists $t, \beta \in \mathbb{R}$ that satisfy Equation 6.2.1 and 6.2.2. That is, X admits uniform mixing at time t. □

Chan derived a more accessible condition in Lemma 3.3 of [7] for uniform mixing in $\mathcal{H}(d, 2)$ using Property (iv) in Lemma 6.1.3. However, this property holds only for $q = 2$. To generalize Chan's result, we use another method that works for $q \in \{2, 3, 4\}$, and obtain new distance graphs that admit uniform mixing earlier than the Hamming graphs. First, we have the following corollary to Lemma 6.2.2.

6.2.3 Corollary. *Suppose $d \geq 1$, $r \geq 1$ and $k \geq 2$. Let X_r be the r-distance graph of the Hamming graph $H(d, q)$, and let $\epsilon \in \{1, -1\}$.*

(i) If $q = 2$, and

$$p_{r-1}^{(d-1)}(s) \equiv \epsilon 2^{k-2} \pmod{2^k}$$

for $s = 0, 1, \cdots, d-1$, then X_r admits uniform mixing at time $\pi/2^k$.

(ii) If $q = 3$, and

$$p_{r-1}^{(d-1)}(s) \equiv \epsilon 3^{k-2} \pmod{3^{k-1}}$$

for $s = 0, 1, \cdots, d-1$, then X_r admits uniform mixing at time $2\pi/3^k$.

(iii) If $q = 4$, and

$$p_{r-1}^{(d-1)}(s) \equiv 2^{k-2} \pmod{2^{k-1}}$$

for $s = 0, 1, \cdots, d-1$, then X_r admits uniform mixing at time $\pi/2^k$.

Proof. We prove this for $q = 2$; the other two cases are similar.

Suppose
$$p_{r-1}^{(d-1)}(s) \equiv \epsilon 2^{k-2} \pmod{2^k}$$
for $s = 0, 1, \cdots, d-1$. By Property (iii) in Lemma 6.1.3, this implies
$$p_r(s+1) - p_r(s) \equiv -\epsilon 2^{k-1} \pmod{2^{k+1}}.$$
It follows that
$$\begin{aligned} p_r(s) - p_r(0) &= p_r(s) - p_r(s-1) + \cdots + p_r(1) - p_r(0) \\ &= -\epsilon s 2^{k-1} \pmod{2^{k+1}} \end{aligned}$$
By Lemma 6.2.2, X_r admits uniform mixing at time $\pi/2^k$. □

We now focus on the Hamming schemes $\mathcal{H}(d, 3)$ and $\mathcal{H}(d, 4)$. By further exploiting Lemma 6.1.3, we obtain the following two results.

6.2.4 Lemma. *For $d \geq 1$, $r \geq 1$ and $k \geq 2$, if there exists $\epsilon \in \{-1, 1\}$ such that the following holds*

(i) $2^{r-1}\binom{d-1}{r-1} \equiv \epsilon 3^{k-2} \pmod{3^{k-1}}$,

(ii) 3^{k-h-1} *divides* $\binom{d-h-1}{r-h-1}$ *for* $h = 1, 2, \cdots, k-2$,

then the distance graphs X_r and X_{d-r+1} in the Hamming scheme $\mathcal{H}(d, 3)$ admit uniform mixing at time $2\pi/3^k$.

Proof. From Lemma 6.1.3, we have
$$\begin{aligned} p_{r-1}^{(d-1)}(s) &= \sum_{h=0}^{d-1} (-3)^h 2^{r-h-1} \binom{d-h-1}{r-h-1} \binom{s}{h} \pmod{3^{k-1}} \\ &\equiv \sum_{h=0}^{k-2} (-3)^h 2^{r-h-1} \binom{d-h-1}{r-h-1} \binom{s}{h} \pmod{3^{k-1}}. \end{aligned}$$
By condition (i), when $s = 0$,
$$p_{r-1}^{(d-1)}(0) = 2^{r-1}\binom{d-1}{r-1} \equiv \epsilon 3^{k-2} \pmod{3^{k-1}}$$

and condition (ii), when $s \geq 1$,

$$\begin{aligned} p_{r-1}^{(d-1)}(s) &= p_{r-1}^{(d-1)}(0) + \sum_{h=1}^{k-2} (-3)^h 2^{r-h-1} \binom{d-h-1}{r-h-1} \binom{s}{h} \pmod{3^{k-1}} \\ &\equiv \epsilon 3^{k-2} \pmod{3^{k-1}}. \end{aligned}$$

It follows from Corollary 6.2.3 that X_{r+1} in $\mathcal{H}(d,3)$ admit uniform mixing at time $2\pi/3^k$. For X_{d-r+1}, first note that condition (i) is symmetric about r and $d-r+1$. By condition (ii), 3^{k-h-1} divides

$$\binom{d-h}{r-h} - \binom{d-h-1}{r-h-1} = \binom{d-h-1}{r-h}$$

for $h = 1, 2, \cdots, k-2$. This implies that 3^{k-h-2} divides

$$\binom{d-h-1}{r-h} - \binom{d-h-2}{r-h-1} = \binom{d-h-2}{r-h}$$

for $h = 1, 2, \cdots, k-2$. Continue in this fashion, we see that $3^{k-h-\ell}$ divides

$$\binom{d-h-\ell}{r-h}$$

for $h = 1, 2, \cdots, k-2$ and $\ell = 1, 2, \cdots, k-2$. Taking $h = 1$ for all ℓ shows that $3^{k-\ell-1}$ divides

$$\binom{d-\ell-1}{r-1} = \binom{d-\ell-1}{(d-r+1)-\ell-1}$$

for $\ell = 1, 2, \cdots, k-2$, which is exactly condition (ii) with r replaced by $d-r+1$. Hence, X_{d-r+1} admits uniform mixing at time $2\pi/3^k$ as well. □

6.2.5 Lemma. *For $d \geq 1$, $r \geq 1$ and $k \geq 2$, if the following two conditions hold*

(i) $3^{r-1}\binom{d-1}{r-1} \equiv 2^{k-2} \pmod{2^{k-1}}$,

(ii) 2^{k-2h-1} *divides* $\binom{d-h-1}{r-h-1}$ *for* $h = 1, 2, \cdots, \lfloor k/2 \rfloor - 1$,

then the distance graphs X_r and X_{d-r+1} in the Hamming scheme $\mathcal{H}(d,4)$ admit uniform mixing at time $\pi/2^k$. □

The above observations imply that our potential examples rely heavily on the divisibility of a binomial coefficient by some prime power. In fact, this is closely related to the base p representation of the binomial coefficients, where p is a prime. To find the pairs (d, r) that satisfy the divisibility conditions, we need the following number theory result due to Kummer in Chapter IX of [12].

6.2.6 Theorem. *Let p be a prime. The largest integer k such that p^k divides $\binom{N}{M}$ is the number of carries in the addition of $N - M$ and M in base p representation.* $\square$

To our interest, we look at the ternary representations of $d-r$ and $r-h-1$ in $\mathcal{H}(d, 3)$, and their binary representations in $\mathcal{H}(d, 4)$. The following are our examples of distance graphs that admit uniform mixing at times earlier than the Hamming graphs.

6.2.7 Theorem. *For $k \geq 2$ and $r \in \{3^k - 1, 3^k - 4, 3^k - 7\}$, the r-distance graphs X_r of the Hamming graph $H(2 \cdot 3^k - 9, 3)$ admit uniform mixing at time $2\pi/3^k$.*

Proof. Let $d = 2 \cdot 3^k - 9$ and $r = 3^k - 1$. Then

$$\begin{aligned} d - r &= 2 \cdot 3^{k-1} + 2 \cdot 3^{k-2} + \cdots + 2 \cdot 3^2 + 0 \cdot 3^1 + 1 \cdot 3^0 \\ r - 1 - h &= 2 \cdot 3^{k-1} + 2 \cdot 3^{k-2} + \cdots + 2 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0 - h. \end{aligned}$$

When $h = 0$, since $(d-r)+(r-1)$ has exactly $k-2$ carries, $\binom{d-1}{r-1}$ is divisible by 3^{k-2} but not divisible by 3^{k-1}. Then there exists $\epsilon \in \{-1, 1\}$ such that

$$2^{r-1}\binom{d-1}{r-1} \equiv \epsilon 3^{k-2} \pmod{3^{k-1}}.$$

For $h = 1$, the number of carries in $(d - r) + (r - 2)$ is still 2^{k-2}. When $h = 2, \cdots, k - 2$, the number of carries in $(d - r) + (r - h + 1)$ drops by at most one as h increases by one. Therefore $(d - r) + (r - h + 1)$ has at least $k - h - 1$ carries, and so 3^{k-h-1} divides $\binom{n-h}{r-h-1}$. By Theorem 6.2.4, X_{3^k-1} and X_{3^k-7} in $\mathcal{H}(2 \cdot 3^k - 7, 3)$ admit uniform mixing at time $2\pi/3^k$. Similar argument applies to X_{3^k-4}. $\square$

6.2.8 Theorem. *For $k \geq 2$, the distance graph $X_{2^{k-2}}$ of the Hamming graph $H(2^{k-1} - 1, 4)$ and the distance graphs $X_{2^{k-1}-1}$, $X_{2^{k-1}}$ of the Hamming graph $H(2^k - 2, 4)$ admit uniform mixing at time $\pi/2^k$,* $\square$

Chapter 7

Open Problems

We discuss some open problems in this chapter, which are centered around two basic questions we hope to answer:

1. What kind of graphs can admit uniform mixing?

2. If a graph admits uniform mixing, what are the possible mixing times?

7.1 Classifying the Graphs

All the known graphs with uniform mixing are regular. In particular, the graphs we dealt with in this thesis are vertex transitive. However, it is not known whether regularity is required for uniform mixing in general. On the other hand, if we relax our definition of uniform mixing and look at one single column of the transition matrix, there does exist irregular graphs such that $U(t)e_a$ is flat for some vertex a. For example, Carlson et al [5] showed that the quantum walk on the claw $K_{1,n}$ starting at the central vertex reaches uniform distribution at some time. Following this, Godsil proved that the cone of a regular graph with valency at most two admits uniform mixing from the central vertex in Chapter 16 of [17]. Therefore, we may want to look at the conditions on two vertices a and b for $U(t)e_a$ and $U(t)e_b$ to be flat simultaneously.

For the regular graphs that have been visited, there are still unsolved questions. For instance, the cycles C_n with $n > 5$ are conjectured to be resistant to uniform mixing by Ahmadi et al [2], but this is not proved for odd composite n. A second example is the Cayley graphs over $\mathbb{Z}_q^d$. We have seen several conditions for the linear ones with $q \in \{2, 3, 4\}$ to admit uniform mixing, but we know little about the others. In [22], Mullin conjectured that no Cayley graph over $\mathbb{Z}_q^d$ admits uniform mixing for $q \geq 5$, and suggested looking at the algebraic properties of the entries of the transition matrix. Meanwhile, except for a few examples, we do not have an efficient method to test whether uniform mixing can occur on a given Cayley graph. Thus, the next step may be to classify the Cayley graphs that do not admit uniform mixing at any time.

7.2 Mixing Times

We start this section with the furthest conclusion we can draw on the algebraic properties of the mixing times in our examples. As noted by Mullin [22], for each of the known examples with uniform mixing, the adjacency matrix is contained in a formally self-dual association scheme with integral eigenvalues, in which case the Krein parameters are rational. Therefore, by Theorem 3.3.2, if uniform mixing occurs at time t, then e^{it} is an algebraic number. However, the known mixing times t seem to satisfy a stronger condition: e^{it} is a root of unity. Moreover, if our graph has $n \geq 5$ vertices, then t is an integer multiple of $2\pi/n$. These lead to the following two conjectures, the first made by Mullin in [22].

7.2.1 Conjecture. *If a graph with integral eigenvalues admits uniform mixing at time t, then e^{it} must be a root of unity.*

7.2.2 Conjecture. *If a graph with integral eigenvalues on $n \geq 5$ vertices admits uniform mixing at time t, then t is an integer multiple of $2\pi/n$.*

By Lemma 5.2.1, one consequence of the last conjecture is that all graphs on at least five vertices with uniform mixing come in complementary pairs.

A second problem is the "uniqueness" of the mixing time in a time interval, for example, in $[0, 2\pi]$ for graphs with integral eigenvalues, whose transition matrices are periodic with period 2π. Of course, uniform mixing can occur at several times within this period. As we have seen in Chapter 2, the transition matrix of K_2 is

$$U(t) = \begin{pmatrix} \cos(t) & i\sin(t) \\ i\sin(t) & \cos(t) \end{pmatrix}.$$

Thus, $U(t)$ is flat at times $\pi/4$, $3\pi/4$, $5\pi/4$, and $7\pi/4$, which are mapped by e^{it} to the full set of the primitive fourth root of unity. By Theorem 3.3.2, if a graph with integral eigenvalues admits uniform mixing at time t, then all the algebraic conjugates of e^{it} with absolute value one give rise to new mixing times. What we are interested in but have not found is an example with uniform mixing at times t_1 and t_2, so that e^{it_1} and e^{it_2} are not algebraic conjugates of each other. We conjecture that these graph do not exist.

7.2.3 Conjecture. *Let X be a graph with integral eigenvalues that admits uniform mixing. There exists a monic irreducible polynomial f over the rationals such that X admits uniform mixing at t if and only if e^{it} is a zero of f.*

Another problem is to give a lower bound on the size of a graph or on the mixing time. In our examples from association schemes, earlier mixing occurs on graphs with more vertices and higher valencies. This gives rise to the following two quesions:

1. Given a time t, what is the smallest graph that may admit uniform mixing at t?

2. Given a graph, when is the earliest time at which it may admit uniform mixing?

By Corollary 5.5.5, we have a lower bound on the valency of a Cayley graph over $\mathbb{Z}_3^d$ that admits uniform mixing at time $t = 2\pi/3n$. However, this bound is not monotonic in n, and it does not work for the time t if e^{it} is not a root of unity. Hence more practical bounds are needed. A probabilistic approach may be the first step.

Bibliography

[1] William Adamczak, Kevin Andrew, Leon Bergen, Dillon Ethier, Peter Hernberg, Jennifer Lin, and Christino. Tamon, *Non-uniform mixing of quantum walk on cycles*, arXiv:0708.2096 (2007).

[2] Amir Ahmadi, Ryan Belk, Christino Tamon, and Carolyn Wendler, *On mixing in continuous-time quantum walks on some circulant graphs*, Quantum Info. Comput. **3** (2003), no. 6, 611–618.

[3] Ana Best, Markus Kliegl, Shawn Mead-Gluchacki, and Christino Tamon, *Mixing of quantum walks on generalized hypercubes*, arXiv:0808.2382 (2008).

[4] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier, *Distance-regular graphs*, Springer-Verlag, New York, 1989.

[5] William Carlson, Allison For, Elizabeth Harris, Julian Rosen, Christino Tamon, and Kathleen Wrobel, *Universal mixing of quantum walk on graphs*, Quantum Info. Comput. **7** (2007), no. 8, 738–751.

[6] Ada Chan, *Complex Hadamard matrices and strongly regular graphs*, arXiv:1102.5601 (2011).

[7] ———, *Complex Hadamard matrices, instantaneous uniform mixing and cubes*, arXiv:1305.5811 (2013).

[8] Laura Chihara and Dennis Stanton, *Zeros of generalized Krawtchouk polynomials*, Journal of Approximation Theory **60** (1990), no. 1, 43 – 57.

[9] Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman, *Exponential algorithmic speedup by a*

quantum walk, Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '03, ACM, 2003, pp. 59–68.

[10] Andrew M. Childs, Leonard J. Schulman, and Umesh V. Vazirani, *Quantum algorithms for hidden nonlinear structures*, Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (Washington, DC, USA), FOCS '07, IEEE Computer Society, 2007, pp. 395–404.

[11] Matthias Christandl, Nilanjana Datta, Tony C. Dorlas, Artur Ekert, Alastair Kay, and Andrew J. Landahl, *Perfect state transfer in quantum spin networks*, Physical Review Letters **92** (2004), no. 18, 187902.

[12] Leonard E. Dickson, *History of the Theory of Numbrs*, vol. I: Divisibility and primality, Chelsea Publishing Co., New York, 1966.

[13] Edward Farhi and Sam Gutmann, *Quantum computation and decision trees*, (1997).

[14] Heath Gerhardt and John Watrous, *Continuous-time quantum walks on the symmetric group*, Proc. RANDOM-APPROX (Sanjeev, SpringerVerlag, 2003, pp. 290–301.

[15] Chris Godsil, *Association Schemes*, 2010.

[16] ———, *Generalized Hamming Schemes*, arXiv:1011.1044 (2010).

[17] ———, *Graph Spectra and Quantum Walks*, 2012.

[18] Chris Godsil, Natalie Mullin, and Aidan Roy, *Uniform mixing and association schemes*, arXiv:1301.5889 (2013).

[19] Chris Godsil and Gordon Royle, *Algebraic Graph Theory*, Springer New York, 2001.

[20] Uffe Haagerup, *Cyclic p-roots of prime lengths p and related complex Hadamard matrices*, arXiv:0803.2629 (2008).

[21] Brendan D. McKay, *Topics in Computational Graph Theory*, Ph.D. thesis, University of Melbourne, 1980.

[22] Natalie Mullin, *Uniform Mixing of Quantum Walks and Association Schemes*, Ph.D. thesis, University of Waterloo, 2013.

[23] Salvador Elías Venegas-Andraca, *Quantum walks: A comprehensive review*, Quantum Information Processing **11** (2012), no. 5, 1015–1106.

Index