Uniform Mixing on Cayley Graphs

Chris Godsil   Hanmeng Zhan

Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, Canada

{cgodsil,h3zhan}@uwaterloo.ca

Submitted: Feb 24, 2017; Accepted: Jul 18, 2017; Published: Jul 28, 2017
Mathematics Subject Classifications: 05C50, 05E30, 81P45

Abstract

We provide new examples of Cayley graphs on which the quantum walks reach uniform mixing. Our first result is a complete characterization of all $2(d+2)$-regular Cayley graphs over $\mathbb{Z}_3^d$ that admit uniform mixing at time $2\pi/9$. Our second result shows that for every integer $k \geqslant 3$, we can construct Cayley graphs over $\mathbb{Z}_q^d$ that admit uniform mixing at time $2\pi/q^k$, where $q = 3, 4$.

We also find the first family of irregular graphs, the Cartesian powers of the star $K_{1,3}$, that admit uniform mixing.

Keywords: quantum walk; uniform mixing; Cayley graph

1 Introduction

A continuous-time quantum walk on a graph X is defined by the transition matrix

$$U(t) := \exp(itA) = \sum_{k\geqslant 0} \frac{(itA)^k}{k!},$$

where A is the adjacency matrix of X. The probability that at time t, the quantum walk with initial state represented by u is in the state represented by v is

$$\left|U(t)_{uv}\right|^2.$$

We say X admits *uniform mixing* at time t if the above probability is the same for all vertices u and v. A weaker version of uniform mixing, called *local uniform* mixing, occurs if the probability distribution given by a column of $U(t)$ is uniform.

Uniform mixing on graphs is rare, and almost all the known examples are Cayley graphs. The current list of Cayley graphs contains the complete graphs K_2, K_3 and K_4

[1], the Hamming graphs $H(d,2)$, $H(d,3)$ and $H(d,4)$ [2, 8], the Paley graph of order nine [6], some strongly regular graphs from regular symmetric Hadamard matrices [6], some linear Cayley graphs over $\mathbb{Z}_2^d$, $\mathbb{Z}_3^d$ and $\mathbb{Z}_4^d$ [3, 9], and the Cartesian product of graphs which admit uniform mixing at the same time. These graphs share the following features.

(a) They are Cayley graphs over abelian groups;

(b) They have integer eigenvalues;

(c) Their mixing times are rational multiples of π.

That being said, a graph that admits uniform mixing is not necessarily vertex-transitive or even regular. As we will see in Section 11, the star $K_{1,3}$ admits uniform mixing at time $2\pi/\sqrt{27}$. The Cartesian powers of $K_{1,3}$ are so far the only family of irregular graphs found to admit uniform mixing, and the only family to which none of the above features applies.

Although characterizing uniform mixing in general seems daunting, the problem can be reduced if we require some regularity on the graphs. The vertex transitive graphs, which provide most of the known examples, satisfy the property that for any two vertices u and v, there is a graph automorphism that maps u to v. The transition matrix of a vertex-transitive graph is entirely determined by one of its rows. Therefore for all Cayley graphs, uniform mixing is equivalent to local uniform mixing.

In this paper, we provide new examples of Cayley graphs over $\mathbb{Z}_q^d$ that admit uniform mixing. Our examples contain both an infinite family of Cayley graphs on which mixing occurs at time $2\pi/9$, and infinite families of Cayley graphs on which mixing occurs arbitrarily faster. Theorem 10 provides a complete characterization of $2(d+2)$-regular Cayley graphs over $\mathbb{Z}_3^d$ that admit uniform mixing at time $2\pi/9$. Theorem 20, Theorem 21 and Theorem 22 show that, for an arbitrarily large integer k, we can construct families of Cayley graphs over $\mathbb{Z}_q^d$ that admit uniform mixing at time $2\pi/q^k$, where $q=3,4$. These examples extend the results of Mullin [9] and Chan [3].

2 Quotients of Hamming Graphs

A *Cayley graph* over the additive group $\mathbb{Z}_q^d$ is a graph with vertex set $\mathbb{Z}_q^d$ and edge set

$$\{(g,h) : h-g \in C\}$$

for some subset C of $\mathbb{Z}_q^d$. We will follow Godsil and Royle [7] and denote this graph by $X(\mathbb{Z}_q^d, C)$, and call C the *connection set*. Further, we assume C is inverse-closed and does not contain the identity element, so that $X(\mathbb{Z}_q^d, C)$ is a simple graph. Note here q is not necessarily a prime power – we will think of the vertex set $\mathbb{Z}_q^d$ as a module in this paper.

While no extra algebraic structure of $\mathbb{Z}_q^d$ is needed to define a Cayley graph, it is often convenient to view the underlying group $\mathbb{Z}_q^d$ as a $\mathbb{Z}_q$-module. Two easy observations follow. First, if ϕ is a module automorphism of $\mathbb{Z}_q^d$, then the two Cayley graphs $X(\mathbb{Z}_q^d, C)$ and $X(\mathbb{Z}_q^d, \phi(C))$ are isomorphic. Second, $X(\mathbb{Z}_q^d, C)$ is connected if and only if its connection set contains a basis of $\mathbb{Z}_q^d$. An example of connected Cayley graphs over $\mathbb{Z}_q^d$ is the *Hamming graph* $H(d,q)$, whose connection set consists of non-zero multiples of the standard basis $\{e_1, e_2, \ldots, e_d\}$ of $\mathbb{Z}_q^d$.

We will pay special attention to the quotient graphs of Hamming graphs, as they form an important family of Cayley graphs over $\mathbb{Z}_q^d$. The *Hamming distance* of two elements in $\mathbb{Z}_q^d$ is the number of coordinates in which they differ. Consider a submodule Γ of $\mathbb{Z}_q^d$ with Hamming distance at least three. The partition of $\mathbb{Z}_q^d$ by the cosets of Γ satisfies three properties:

(i) every coset is a coclique;

(ii) every vertex is adjacent to at most one vertex in a coset;

(iii) if some vertex in the coset $g + \Gamma$ is adjacent to a vertex in another coset $h + \Gamma$, then there is a matching between $g + \Gamma$ and $h + \Gamma$.

The *quotient graph* of $H(d,q)$ induced by Γ, denoted $H(d,q)/\Gamma$, is a graph with a vertex for each coset of Γ, such that two vertices are adjacent if there is a matching between the two associated cosets. We note that every quotient graph of $H(d,q)$ is a Cayley graph for a quotient module of $\mathbb{Z}_q^d$.

Lemma 1. *Let C be the connection set of the Hamming graph $H(d,q)$. For a submodule Γ of $\mathbb{Z}_q^d$ with Hamming distance at least three, let*

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

Then

$$H(d,q)/\Gamma \cong X(\mathbb{Z}_q^d/\Gamma, C/\Gamma).$$

Proof. Let $g + \Gamma$ and $h + \Gamma$ be two vertices of $X(\mathbb{Z}_q^d, C)/\Gamma$. They are adjacent if and only if there exist $x, y \in \Gamma$ and $c \in C$ such that $(g + x) - (h + y) = c$, or equivalently,

$$(g + \Gamma) - (h + \Gamma) = c + \Gamma \in C + \Gamma. \qquad \square$$

3 Linear Cayley Graphs

A Hamming graph $H(d,q)$ is known to admit uniform mixing if and only if $q \in \{2, 3, 4\}$. As uniform mixing on $H(d,q)$ implies uniform mixing on some of its quotient graphs, for our interest it is important to understand which Cayley graphs are quotients of $H(d,q)$. In this section, we show that quotient graphs of $H(d,q)$ are exactly the *linear* Cayley graphs over $\mathbb{Z}_q^d$, that is, graphs $X(\mathbb{Z}_q^d, C)$ for which $C \cup \{\mathbf{0}\}$ is closed under multiplication by $\mathbb{Z}_q$.

Since $\mathbb{Z}_2$ has only one non-zero element, the connection set of every Cayley graph over $\mathbb{Z}_2^d$ is trivially closed under multiplication of the non-zero elements of $\mathbb{Z}_2$. Similarly, for

Cayley graphs over $\mathbb{Z}_3^d$, since we assume the connection set is inverse-closed, it is closed under multiplication of the only two non-zero elements of $\mathbb{Z}_3$. Thus, all Cayley graphs over $\mathbb{Z}_2^d$ or $\mathbb{Z}_3^d$ are linear, and we can characterize uniform mixing on them in terms of the submodules that induce the quotients.

Theorem 2. *Let $X(\mathbb{Z}_q^r, C)$ be a connected linear Cayley graph with valency $d(q-1)$. Then $X(\mathbb{Z}_q^r, C)$ is isomorphic to a quotient graph $H(d,q)/\Gamma$ for some submodule Γ of $\mathbb{Z}_q^d$, where $|\Gamma| = q^{d-r}$ and Γ has Hamming distance at least three.*

Proof. Let C be the connection set of X. We can partition 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 multiples of each other, and the first r cells contains a basis of $\mathbb{Z}_q^d$. Since C_j is a cyclic group, we may assume $C_j = \langle v_j \rangle$. Define a module homomorphism from C to $\mathbb{Z}_q^r \times \mathbb{Z}_q^{d-r}$ by

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

where $\{e_1, e_2, \ldots, e_d\}$ is the standard basis of $\mathbb{Z}_q^d$. Let

$$C' = \{f(v) : v \in C\}.$$

Then C' consists of all non-zero multiples of a basis of $\mathbb{Z}_q^r \times \mathbb{Z}_q^{d-r}$. Thus, $X(\mathbb{Z}_q^d, C')$ is isomorphic to the Hamming graph $H(d,q)$. Let ϕ be a module automorphism of $\mathbb{Z}_q^d$ that maps a basis in C' to the standard basis. Let Γ' be the submodule of $\mathbb{Z}_q^d$ generated by $\{e_{r+1}, e_{r+2}, \ldots, e_d\}$, and Γ the image of Γ' under ϕ. Clearly $|\Gamma| = q^{d-r}$. By Lemma 1,

$$H(d,q)/\Gamma \cong X(\mathbb{Z}_q^d, C')/\Gamma' \cong X(\mathbb{Z}_q^r, C).$$

Since we started with a simple Cayley graph, Γ must have Hamming distance at least three. □

Conversely, for any quotient graph $H(d,q)/\Gamma$, where Γ has minimum distance at least three, we can find a connection set of the linear Cayley graph isomorphic to $H(d,q)/\Gamma$.

Theorem 3. *Let Γ be a submodule of $\mathbb{Z}_q^d$ with size q^{d-r} and Hamming distance at least three. Let Q be a parity check matrix of Γ, and C the set of non-zero multiples of the columns of Q. Then $H(d,q)/\Gamma$ is isomorphic to the $d(q-1)$-regular graph $X(\mathbb{Z}_q^r, C)$.*

Proof. Without loss of generality, we may assume Γ is generated by the columns of the following block matrix

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

where S is square and invertible over $\mathbb{Z}_q$. Let

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

We have

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

that is, P defines a module automorphism ϕ of $\mathbb{Z}_q^d$ that maps Γ to the submodule generated by $\{e_{r+1}, e_{r+2}, \dots, e_d\}$. Note that the partitioned matrix

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

is a parity check matrix of Γ. If D is the connection set of $H(d,q)$ and C the multiples of columns of Q, then by Lemma 1,

$$\begin{aligned} H(d,q)/\Gamma &\cong X(\mathbb{Z}_q^d/\Gamma, D/\Gamma) \\ &\cong X(\mathbb{Z}_q^d/\phi(\Gamma), \phi(D)/\phi(\Gamma)) \\ &\cong X(\mathbb{Z}_q^d, C). \end{aligned}$$

Finally, since the minimum distance of Γ is the minimum number of linearly dependent columns of its parity check matrix Q, no two columns of Q are multiples of each other. It follows that $X(\mathbb{Z}_q^r, C)$ has valency $d(q-1)$. □

The quotient approach provides a convenient way to characterize uniform mixing on linear Cayley graphs. If $X = H(d,q)/\Gamma$, the vertices of X are cosets $\Gamma + v$ of the subgroup, and each entry of $U_X(t)$ is a block sum of the entries of $U_{H(d,q)}(t)$. More specifically, the $(0,v)$-entry of $U_X(t)$ can be expressed as follows. For more details, see Mullin's thesis [9, Ch 8].

Theorem 4 (Mullin)**.** *Let $X = H(d,q)/\Gamma$. We have*

$$U(t)_{0,v} = \left(\frac{e^{-it}}{q}\right)^d \sum_{a \in \Gamma + v} (e^{qit} + q - 1)^{d - \mathrm{wt}(a)} (e^{qit} - 1)^{\mathrm{wt}(a)}.$$

For each coset $\Gamma + v$, let $W_v(x,y)$ denote its homogeneous weight enumerator. Note that the right hand side of the above equation is

$$W_v(e^{qit} + q - 1, e^{qit} - 1).$$

For the $(0,0)$-entry, MacWilliams' identity simplifies the expression to

$$U(t)_{0,0} = \left(\frac{e^{-it}}{q}\right)^d |\Gamma| W_{\Gamma^\perp}(e^{qit}, 1).$$

Thus we have a necessary condition for uniform mixing.

Corollary 5. *If $H(d,q)/\Gamma$ admits uniform mixing at time t, then*

$$|W_{\Gamma^\perp}(e^{qit}, 1)|^2 = |\Gamma^\perp|.$$

We already know that uniform mixing occurs on $H(d,2), H(d,3)$ and $H(d,4)$ at time $\pi/4, 2\pi/9$ and $\pi/4$, respectively. It is natural to see if their quotients also admit uniform mixing at these special times.

Corollary 6. *(a) $H(d,2)/\Gamma$ admits uniform mixing at time $\pi/4$ if and only if for each coset $\Gamma+v$,*

$$|W_v(i,1)|^2 = |\Gamma|;$$

(b) $H(d,3)/\Gamma$ admits uniform mixing at time $2\pi/9$ if and only if for each coset $\Gamma+v$,

$$|W_v(e^{2\pi i/3},1)|^2 = |\Gamma|;$$

(c) $H(d,4)/\Gamma$ admits uniform mixing at time $\pi/4$ if and only if for each coset $\Gamma+v$,

$$|W_v(-1,1)|^2 = |\Gamma|.$$

Consider the binary $[17,9,5]$-quadratic code. A numerical check on the weight distributions of its cosets shows that it admits uniform mixing at time $\pi/4$.

4 Quotient Graphs with One Generator

For a quotient graph $H(d,q)/\Gamma$, the entries of its transition matrix are block sums of the transition matrix of $H(d,q)$. As functions of the time t, these block sums can be greatly simplified if we plug in the time τ_q when $H(d,q)$ admits uniform mixing. Thus, at the specific time τ_q, whether uniform mixing occurs on $H(d,q)/\Gamma$ is fully determined by the weight distributions of the cosets of Γ. For details see Mullin's Ph.D. thesis [9, Ch 8].

The *Hamming weight* $\mathrm{wt}(a)$ of an element a in $\mathbb{Z}_q^d$ is the number of non-zero entries of a. In this section, we characterize quotients $H(d,q)/\langle a\rangle$ that admit uniform mixing at time τ_q, where the submodule is generated by one element a with Hamming weight $\mathrm{wt}(a)$ at least three. As a special case, the "folded" Hamming graphs $H(d,q)/\langle \mathbf{1}\rangle$ have been studied in [9]. In general, Theorem 3 gives the matrix Q representing the connection set of $H(d,q)/\langle a\rangle$. By row reduction, column permutation, and column scaling of Q, it is not hard to see that $H(d,q)/\langle a\rangle$ is a Cartesian product of a Hamming graph and a folded Hamming graph. Combining this observation and the results on the folded Hamming graphs, we give the following characterization.

Theorem 7. *Let a be a vector in $\mathbb{Z}_q^d$ with $\mathrm{wt}(a) \geqslant 3$, where $q=2,3,4$. Then*

(a) Uniform mixing occurs on $H(d,2)/\langle a\rangle$ at time $\tau_2=\pi/4$ if and only if $\mathrm{wt}(a)$ is odd;

(b) Uniform mixing occurs on $H(d,3)/\langle a\rangle$ at time $\tau_3=2\pi/9$ if and only if $\mathrm{wt}(a)$ is not divisible by three;

(c) Uniform mixing occurs on $H(d,4)/\langle a\rangle$ at time $\tau_4=\pi/4$ if and only if $\mathrm{wt}(a)$ is odd.

This theorem takes care of all the connected $(d+1)(q-1)$-regular Cayley graphs over $\mathbb{Z}_q^d$, which admit uniform mixing at τ_q, for $q\in\{2,3,4\}$.

5 Quotient Graphs with Two Generators

We move on to the quotients of Hamming graphs where the submodules are generated by two elements. Our goal is to characterize the $2(d+2)$-regular Cayley graphs over $\mathbb{Z}_3^d$ that admit uniform mixing at time $2\pi/9$, as given in Theorem 10. The tool we use is the *weight distribution* of a code, that is, the sequence

$$(\alpha_0, \alpha_1, \alpha_2, \cdots)$$

where α_j is the number of of codewords with Hamming weight j. To begin, we need the following conditions on the cosets of Γ from [9, Ch 8].

Theorem 8 (Mullin). *Let Γ be a submodule of $\mathbb{Z}_3^d$ with Hamming distance at least three such that $|\Gamma| = 3^s$. For any coset of Γ, let n_j be the number of elements in it with weight j modulo three. Uniform mixing occurs on $H(d,q)/\Gamma$ at time $2\pi/9$ if and only if the weight distribution of every coset of Γ satisfies*

$$n_0n_1 + n_0n_2 + n_1n_2 = 3^{2s-1} - 3^{s-1}.$$

Since we have to examine the weight distribution of every coset of Γ, it helps to understand the relation between the weights of Γ and the weights of $\Gamma + c$ for each vector c. Suppose Γ is generated by s elements, and let M be the matrix with the generators of Γ as its columns. Then each element in Γ can be written as My for some vector $y \in \mathbb{Z}_3^s$, and is uniquely associated to an element $My + c$ in the coset $\Gamma + c$. We will refer to

$$\operatorname{wt}(My + c) - \operatorname{wt}(My)$$

as the *weight change* of the element My with respect to c. The following gives the necessary condition on the weight changes for both Γ and $\Gamma + c$ to satisfy the weight distribution condition in Theorem 8.

Lemma 9. *Let Γ be a submodule of $\mathbb{Z}_3^d$ with size 3^s and minimum distance three, and let $\Gamma + c$ be a coset of Γ. For $j = 0, 1, 2$, let Γ_j denote the set of elements in Γ with weight congruent to j modulo three. Let m_j be the number of elements in Γ_j whose weight change with respect to c is one modulo three. If both Γ and $\Gamma + c$ satisfy the weight distribution condition in Theorem 8, then either $m_j = 0$ for all j, or m_j satisfies the following:*

$$\begin{gathered} m_0 + m_1 + m_2 = 3^{s-1} \\ (m_0n_0 + m_1n_1 + m_2n_2) + 3(m_0m_1 + m_1m_2 + m_0m_2) = 3^{2s-1} - 3^{2s-2}. \end{gathered}$$

Proof. We will calculate the weights over $\mathbb{Z}_3$. Let My be an element in Γ. Notice that

$$\operatorname{wt}(My + c) = (My + c)^T(My + c) = \operatorname{wt}(My) + \operatorname{wt}(c) + 2c^T My.$$

Since $\mathrm{wt}(c)$ depends only on c, and the condition in Theorem 8 is symmetric on n_0, n_1, n_2, we may assume without loss of generality that $\mathrm{wt}(c) = 0$. If $c^T M = 0$, then the weight change of each element in Γ is zero. Otherwise, there are exactly 3^{s-1} vectors y such that

$$2c^T My = 1.$$

Therefore

$$m_0 + m_1 + m_2 = 3^{s-1}.$$

Notice that for each solution y to $2c^T My = 1$, the vector $2y$ is a solution to $2c^T My = 2$. Thus there are equal number of elements in Γ_j with weight change one and weight change two. It follows that in the coset $\Gamma + c$, the number of elements with weight j is

$$n'_j = n_j - 2m_j + m_{j-1} + m_{j+1},$$

where the subcripts are calculated modulo three. Since $\Gamma + c$ satisfies the weight distribution conditon in Theorem 8,

$$n'_0 n'_1 + n'_0 n'_2 + n'_1 n'_2 = 3^{2s-1} - 3^{s-1}.$$

This together with the fact that

$$n_0 n_1 + n_0 n_2 + n_1 n_2 = 3^{2s-1} - 3^{s-1}$$

yields

$$(m_0 n_0 + m_1 n_1 + m_2 n_2) + 3(m_0 m_1 + m_1 m_2 + m_0 m_2) = 3^{2s-1} - 3^{2s-2}. \qquad \square$$

With the above observation, we characterize the quotient graphs $H(d, q)/\langle a, b\rangle$ that admit uniform mixing at time $2\pi/9$ in terms of the generators a and b.

Theorem 10. *Uniform mixing occurs on $H(d, 3)/\langle a, b\rangle$ at time $2\pi/9$ if and only if one of the following holds:*

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

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

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

$$n_0 n_1 + n_0 n_2 + n_1 n_2 = 24$$
$$n_0 + n_1 + n_2 = 9$$

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

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

be a matrix and let

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

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

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

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 the four elements $\{w_1, w_2, w_3, w_4\}$ 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 $c \in \mathbb{Z}_3^d$. By Lemma 9, the weight changes m_0, m_1, m_2 are either zero, or satisfy

$$\begin{aligned} m_0 + m_1 + m_2 &= 3, \\ (m_0n_0 + m_1n_1 + m_2n_2) + 3(m_0m_1 + m_0m_2 + m_0m)_3 &= 18. \end{aligned} \tag{1}$$

In the latter case, the weight changes are either

$$m_0 = m_1 = m_2 = 1$$

or

$$\{m_0, m_1, m_2\} = \{0, 1, 2\}.$$

It is easy to see that if $m_0 = m_1 = m_2 = 1$, then $W(\Gamma + c) = W(\Gamma)$. Suppose

$$\{m_0, m_1, m_2\} = \{0, 1, 2\}.$$

Then by Equation (1), when $W(\Gamma) = (1, 4, 4)$, we have

$$\begin{aligned} n_0 = 1, &\quad n_1 = n_2 = 4 \\ m_0 = 0, &\quad \{m_1, m_2\} = \{1, 2\} \end{aligned}$$

and when $W(\Gamma) = (2, 2, 5)$, we have

$$\begin{aligned} n_0 = 5, &\quad n_1 = n_2 = 2 \\ m_0 = 2, &\quad \{m_1, m_2\} = \{0, 1\}. \end{aligned}$$

Since the weight distribution of $\Gamma + c$ is

$$n'_j = n_j - 2m_j + m_{j-1} + m_{j+1}$$

again we have $W(\Gamma + c) = W(\Gamma)$. □

It is perhaps surprising that in all the characterizations discussed so far, the condition for a quotient graph $H(d, q)/\Gamma$ to admit uniform mixing only relies on the group generators, although Theorem 8 suggests checking the weight distribution of every coset of this group. It would reduce the problem of checking uniform mixing on $H(d, q)/\Gamma$ at time τ_q considerably if this was true in general.

6 Hamming Schemes

In this section, we construct Cayley graphs over $\mathbb{Z}_q^d$ that admit uniform mixing earlier than the complete graph K_q. The construction is based on the association scheme which spans the adjacency algebra of a Hamming graph, called the Hamming scheme. We introduce the basic concepts of association schemes and some useful results on the eigenvalues of Hamming schemes.

An *association scheme* with d classes is a set $\mathcal{A} = \{A_0, A_1, \dots, A_d\}$ of 01-matrices that satisfies the following conditions:

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

The association scheme $\mathcal{A}$ generates an algebra over $\mathbb{C}$, which is referred to as the *Bose-Mesner algebra* of $\mathcal{A}$. This algebra has an orthogonal basis of idempotents $E_0, E_1, \dots, E_d$. Thus for each matrix A_r in the scheme, there are scalars $p_r^{(d)}(s)$ such that

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

These scalars are called the eigenvalues of the scheme $\mathcal{A}$. When d is clear from the context, we drop the superscript and write $p_r(s)$. The following theorem due to Chan [3] shows that whether a graph admits uniform mixing depends only on its spectrum and the eigenvalues of the Bose-Mesner algebra containing its adjacency matrix.

Theorem 11 (Chan). *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_q if and only if there exist scalars $t_0, t_1, \dots, t_d$ such that

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

A *Hamming scheme* $\mathcal{H}(d, q)$ is an association scheme constructed from the Hamming graph $H(d, q)$. The matrix A_j is the adjacency matrix of the r-th distance graph of

$H(d,q)$, which has the same vertex set as $H(d,q)$ such that two vertices are adjacent if they are at distance r in $H(d,q)$. The eigenvalues of the scheme $\mathcal{H}(d,q)$ satisfy

$$p_r^{(d)}(s) = [x^r](1+(q-1)x)^{d-s}(1-x)^s, \tag{2}$$

for $s = 0, 1, \cdots, d$. These are called the *Krawtchouk polynomials.* They satisfy the following properties.

Lemma 12. *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 (2),

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

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

We will use property (iii) frequently, so we rephrase it in the matrix form. Let $P^{(d)}$ be the eigenvalue matrix for the scheme $\mathcal{H}(d,q)$. Let

$$C_d = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

be an $d \times d$ circulant matrix. Then Property (iii) is equivalent to

$$\begin{pmatrix} I_{d-1} & 0 \\ 0 & 0 \end{pmatrix}(I_d - C)P^{(d)}\begin{pmatrix} I_{d-1} & 0 \\ 0 & 0 \end{pmatrix} = qP^{(d-1)} \tag{3}$$

7 Sufficient Conditions for Uniform Mixing in Hamming Schemes

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. For notational convenience, let $\mathcal{B}(q)$ denote the Bose-Mesner algebra of the Hamming scheme $\mathcal{H}(d,q)$. For $q \in \{2,3,4\}$, we can construct complex Hadamard matrices in $\mathcal{B}(q)$ from a primitive q-th roots of unity.

Lemma 13. *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 $\mathcal{B}(q)$.

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 $U_{K_q}(\tau_q)$ for some mixing time τ_q 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 thus a complex Hadamard matrix of order q^2. Lastly, a unimodular scalar multiple of a complex Hadamard matrix is again a complex Hadamard matrix. □

The following generalizes Lemma 3.2 in [3].

Lemma 14. *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 $k \geqslant 2$.*

(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

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

Suppose $A \in \mathcal{B}(q)$ has spectral decomposition

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

By Equation (4.2) in [5, Sec 4],

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

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

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

for $s = 0, 1, \cdots, d$. It follows that

$$\sqrt{q^d} e^{i\theta_0 t} = e^{i\beta}(1 + (q-1)\zeta_{6-q})^d \tag{4}$$

and

$$e^{i(\theta_s - \theta_0)t} = \left(\frac{1 - \zeta_{6-q}}{1 + (q-1)\zeta_{6-q}}\right)^s, \tag{5}$$

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

(i) For $q = 2$, Equation (5) 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 (5) 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 (5) 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 exist $t, \beta \in \mathbb{R}$ that satisfy Equation 4 and 5. That is, X admits uniform mixing at time t. □

Equation 3 tells us that we can check the above conditions by looking at the eigenvalues of $\mathcal{B}(q-1)$.

Corollary 15. *Let X be a graph in $\mathcal{B}(q)$ with adjacency matrix*

$$a_0 + a_1A_1 + \cdots + a_dA_d.$$

If $q = 2$ and there is $\epsilon \in \{1, -1\}$ such that

$$P^{(d-1)} \begin{pmatrix} a_1 \\ \cdots \\ a_d \end{pmatrix} \equiv \epsilon 2^{k-2}\mathbf{1} \pmod{2^k},$$

then X admits uniform mixing at time $\pi/2^k$. If $q = 3$ or $q = 4$, and there is $\epsilon \in \{1, -1\}$ such that

$$P^{(d-1)} \begin{pmatrix} a_1 \\ \cdots \\ a_d \end{pmatrix} \equiv \epsilon q^{k-2}\mathbf{1} \pmod{q^{k-1}},$$

then X admits uniform mixing at time $2\pi/q^k$.

8 Faster Uniform Mixing on Distance Graphs

We apply the sufficient conditions developed in the last section to the distance graphs of Hamming graphs, as their eigenvalues are known. In Lemma 3.3 of [3], Chan derived a more accessible condition for uniform mixing in $\mathcal{H}(d, 2)$ using Property (iv) in Lemma 12. However, this property holds only for $q = 2$. To extend her result, we need more general properties for $q \in \{2, 3, 4\}$. The first one is a corollary to Lemma 14.

Corollary 16. *Suppose $d \geqslant 1$, $r \geqslant 1$ and $k \geqslant 2$. 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 12, 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 14, X_r admits uniform mixing at time $\pi/2^k$. □

With the help from the smaller scheme $\mathcal{H}(d-1,q)$, we are able to construct examples in $\mathcal{H}(d,q)$ that admit faster uniform mixing. It turns out that the conditions on the eigenvalues can be further simplified using Lemma 12. From now on, we focus on the Hamming schemes $\mathcal{H}(d,3)$ and $\mathcal{H}(d,4)$, as the examples in $\mathcal{H}(d,2)$ are given in [3].

Lemma 17. *For $d \geqslant 1$, $r \geqslant 1$ and $k \geqslant 2$, 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 12, we have

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

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 $s \geqslant 1$,

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

It follows from Corollary 16 that X_r 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 on 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 $h = 1, 2, \cdots, k-2$. It follows 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 $h = 1, 2, \cdots, k-2$. Continuing this procedure, 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. □

With a similar argument, we can reduce the conditions for faster uniform mixing in $\mathcal{H}(d,4)$ to the following.

Lemma 18. *For $d \geqslant 1$, $r \geqslant 1$ and $k \geqslant 2$, 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 prime. To find the pairs (d,r) that satisfy the divisibility conditions, we need the following number theory result due to Kummer [4, Ch 9].

Theorem 19 (Kummer)**.** *Let p be a prime number. 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.*

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

Theorem 20. *For $k \geqslant 2$ 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 17, X_{3^k-1} and X_{3^k-7} in $\mathcal{H}(2 \cdot 3^k - 9, 3)$ admit uniform mixing at time $2\pi/3^k$. Similar argument applies to X_{3^k-4}. □

Some new examples in $\mathcal{H}(d, 4)$ can be obtained in a similar way.

Theorem 21. *For $k \geqslant 2$, 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 $\pi/2^k$.*

9 Faster Mixing in Schemes

In this section, we give another family of graphs in $\mathcal{H}(d, q)$ that have faster uniform mixing. These are unions of some distance graphs of the Hamming graph $H(d, q)$. Compared to the examples obtained in the last section, these graphs have smaller sizes.

Theorem 22. *In the Hamming scheme $\mathcal{H}(2k + 1, 3)$, the graph with adjacency matrix*

$$\sum_{\ell} A_{3\ell+i}$$

has uniform mixing at time $2\pi/3^k$.

Proof. By Corollary 15, it suffices to show that for each $i = 0, 1, 2$ and the vector

$$a = \sum_{\ell} e_{3\ell+i},$$

there is $\epsilon \in \{1, -1\}$ such that

$$P^{(d-1)}a \equiv \epsilon 3^{k-1} \pmod{3^k}.$$

Also, Equation 2 indicates that the eigenvalues $p_r^{(2k)}(s)$ for $\mathcal{H}(2k,q)$ are the coefficients in

$$f_s(x) = (1+2x)^{2k-s}(1-x)^s.$$

Let $\zeta = e^{2\pi i/3}$. We have

$$f_s(1) = \begin{cases} 3^d, & s = 0 \\ 0, & s \neq 0 \end{cases}$$
$$f_s(\zeta) = -3^k\zeta^{-s}$$
$$f_s(\zeta^2) = -3^k\zeta^s.$$

Then

$$\begin{aligned}([x^0]+[x^3]+[x^6]+\cdots)f(x) &= \frac{1}{3}(f(1)+f(\zeta)+f(\zeta^2)) \\ &= \begin{cases} 3^{2k-1} - 2\cdot 3^{k-1}, & s = 0 \\ 3^{k-1} & s \neq 0 \end{cases} \\ &\equiv 3^{k-1}\mathbf{1} \pmod{3^k}.\end{aligned}$$

Similar computations can be carried out for

$$([x^1]+[x^4]+[x^7]+\cdots)f(x) = \frac{1}{3}(f(1)+\zeta^2 f(\zeta)+\zeta f(\zeta^2)),$$

and

$$([x^2]+[x^5]+[x^8]+\cdots)f(x) = \frac{1}{3}(f(1)+\zeta f(\zeta)+\zeta^2 f(\zeta^2)).$$ □

10 Mixing Times

The eigenvalues and eigenvectors of an abelian Cayley graph are determined by the group characters. For linear Cayley graphs over $\mathbb{Z}_q^d$, there is a simple expression of its eigenvalues in terms of the connection set C. With these observations, we derive a necessary and sufficient condition for uniform mixing to occur on linear Cayley graphs over $\mathbb{Z}_q^d$. This extends the result in [10, Ch 5] on the case where $q = 3$. Throughout this section, the inner product $\langle\cdot,\cdot\rangle$ is taken over $\mathbb{Z}_q$.

Lemma 23. *Let X be a Cayley graph over $\mathbb{Z}_q^d$ with connection set C. For an element $a \in \mathbb{Z}_q^d$, let $\psi_a : \mathbb{Z}_q^d \to \mathbb{C}$ be the map given by*

$$\psi_a(x) = e^{2\pi i\langle a,x\rangle/q}.$$

Then ψ_a is an eigenvector for $A(X)$ with eigenvalue $\psi_a(C)$. Moreover, the eigenvectors defined above are pairwise orthogonal, and they form a group isomorphic to the additive group $\mathbb{Z}_q^d$. Finally, if X is linear, the eigenvalues are integers and can be computed as follows

$$\psi_a(C) = \frac{1}{q-1}(q|C\cap a^\perp| - |C|). \tag{6}$$

We apply the spectral decomposition to Cayley graphs over $\mathbb{Z}_q^d$. Since Cayley graphs are vertex transitive, it suffices to look at the first row of the transition matrix.

Lemma 24. *Let $g \in \mathbb{Z}_q^d$. The $0g$-entry of the transition matrix of $X(\mathbb{Z}_q^d, C)$ is*

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

Proof. By Lemma 23,

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

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

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

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

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

Lastly note that

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

□

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

$$\theta_a := \psi_a(C).$$

For linear Cayley graphs, we can characterize uniform mixing as follows.

Lemma 25. *Let X be a linear Cayley graph over $\mathbb{Z}_q^d$ with connection set C. Uniform mixing occurs on X at time t if and only if for all $g \in \mathbb{Z}_q^d$,*

$$\sum_{a,b : \langle a-b, g \rangle = 0} e^{i(\theta_a - \theta_b)t} = q^d.$$

Proof. The condition

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

is equivalent to

$$\begin{aligned} q^d &= \left| \sum_{a \in \mathbb{Z}_q^d} e^{i\theta_a t} e^{i2\pi \langle a, g \rangle / q} \right|^2 \\ &= \sum_{a,b \in \mathbb{Z}_q^d} e^{i(\theta_a - \theta_b)t} e^{i2\pi \langle a-b, g \rangle / 9}. \end{aligned} \tag{7}$$

Now partition pairs (a, b) of group elements into q classes

$$K_\lambda = \{(a, b) : \langle a - b, g \rangle = \lambda\},$$

where $\lambda \in \mathbb{Z}_q$. Note that for any $\lambda \neq 0$, we have $(a, b) \in K_1$ if and only if $(\lambda a, \lambda b) \in K_\lambda$. Further, by the formula in Lemma 23,

$$\theta_a - \theta_b = \theta_{\lambda a} - \theta_{\lambda b}.$$

Therefore Equation 7 reduces to

$$\begin{aligned} q^d &= \sum_{(a,b)\in K_0} e^{i(\theta_a - \theta_b)t} + e^{i(\theta_a-\theta_b)t} \sum_{\lambda \neq 0} e^{i2\pi\lambda/q} \\ &= \sum_{(a,b)\in K_0} e^{i(\theta_a - \theta_b)t} - \sum_{(a,b)\in K_1} e^{i(\theta_a - \theta_b)t}. \end{aligned} \tag{8}$$

Applying 8 to the 00-entry of the transition matrix, we have

$$q^d = \sum_{a,b} e^{i(\theta_a-\theta_b)t} = \sum_{(a,b)\in K_0} e^{i(\theta_a-\theta_b)t} + (q-1) \sum_{(a,b)\in K_1} e^{i(\theta_a - \theta_b)t}. \tag{9}$$

Combining 8 and 9 yields the desired condition. □

By Lemma 23, the difference between two eigenvalues of $X(\mathbb{Z}_q^d, C)$ is

$$\theta_a - \theta_b = \frac{q}{q-1}\left(|C \cap a^\perp| - |C \cap b^\perp|\right)$$

which is divisible by q. Let

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

We define a rational function in x over the integers by

$$F_g(x) := \left(\sum_{a,b:\langle a-b,g\rangle} x^{m_{ab}} \right) - q^d. \tag{10}$$

Note that by symmetry in a and b, this is a palindromic polynomial divided by some power of x. The mixing times of $X(\mathbb{Z}_q^d, C)$ are determined by the roots of these rational functions.

Theorem 26. *$X(\mathbb{Z}_q^d, C)$ admits uniform mixing at time t if and only if e^{qit} is a zero of*

$$\gcd\{F_g : g \in \mathbb{Z}_q^d\}.$$

Proof. By Lemma 25, uniform mixing occurs at time t if and only if t satisfies

$$\sum_{a,b:\langle a-b,g\rangle=0} e^{i(\theta_a-\theta_b)t} = q^d$$

for all g, or equivalently, if and only if

$$\sum_{a,b:\langle a-b,g\rangle=0} (e^{qit})^{\frac{\theta_a-\theta_b}{q}} - q^d = 0,$$

which is exactly $F_g(e^{qit}) = 0$, for all g. □

For an application of the above result, consider the linear Cayley graph $X(\mathbb{Z}_q^d, C)$, where C consists of all non-zero multiples of $\{e_1, e_2, \dots, e_d, \mathbf{1}\}$. It is isomorphic to the quotient graph $H(d+1,q)/\langle\mathbf{1}\rangle$.

Theorem 27. *If $H(d+1,q)/\langle\mathbf{1}\rangle$ admits uniform mixing at time t, then either*

(i) $q = 2, 4$ and $t = k\pi/4$ for some odd k, or

(ii) $q = 3$ and $t = 2k\pi/9$ for some k not divisible by 3.

Proof. We compute the function $F_{\mathbf{1}}(x)$. By Theorem 23, the eigenvalue θ_a is determined by $|C \cap a^\perp|$. Since the elements in C are non-zero multiples of $\{e_1, e_2, \dots, e_d, \mathbf{1}\}$, we have

$$\theta_a = \begin{cases} (q-1)d - q\,\mathrm{wt}(a) + (q-1), & \text{if } \langle a,\mathbf{1}\rangle = 0 \\ (q-1)d - q\,\mathrm{wt}(a) - 1, & \text{if } \langle a,\mathbf{1}\rangle \neq 0. \end{cases}$$

Now let α_j be the number of elements in $\langle\mathbf{1}\rangle^\perp$ with weight j. Since

$$W_{\mathbf{1}}(x,y) = x^d + (q-1)y^d$$

by MacWilliams' identity,

$$W_{\mathbf{1}^\perp} = \frac{1}{q}\left((x+(q-1)y)^d + (q-1)(x-y)^d\right).$$

Therefore

$$n_j = \frac{1}{q}\binom{d}{j}\left((q-1)^j + (-1)^j(q-1)\right).$$

To compute the weights of the other elements in $\mathbb{Z}_q^d$, note that for each $\lambda \neq 0$, there is a one-to-one correspondence between $\{g : \langle g,\mathbf{1}\rangle = \lambda\}$ and $\{g : \langle g,\mathbf{1}\rangle = 1\}$, so it suffices to compute the number of elements in

$$\{g : \langle g,\mathbf{1}\rangle = 1\}$$

with weight j, denoted β_j. Since the total number of elements in $\mathbb{Z}_q^d$ with weight j is

$$\binom{d}{j}(q-1)^j,$$

we have

$$(q-1)\beta_j = \binom{d}{j}(q-1)^j - \beta_j,$$

that is,

$$\beta_j = \frac{1}{q}\binom{d}{j}\left((q-1)^j - (-1)^j)\right).$$

Hence,

$$\begin{aligned}
F_{\mathbf{1}}(x) &= \sum_{a,b} x^{m_{ab}} - q^d \\
&= \sum_{a,b:\langle a,\mathbf{1}\rangle=\langle b,\mathbf{1}\rangle=1} x^{\mathrm{wt}(a)-\mathrm{wt}(b)} + (q-1)\sum_{a,b:\langle a,\mathbf{1}\rangle=\langle b,\mathbf{1}\rangle=1} x^{\mathrm{wt}(a)-\mathrm{wt}(b)} - q^d \\
&= \sum_j\sum_k (\alpha_j\alpha_k + (q-1)\beta_j\beta_k)x^{j-k} - q^d \\
&= \frac{1}{q}\sum_j\sum_k \binom{d}{j}\binom{d}{k}\left((q-1)^{j+k} + (-1)^{j+k}(q-1)\right)x^{j-k} - q^d \\
&= \frac{1}{q}\left((q-1)\left(x+\frac{1}{x}\right) + (q-1)^2 + 1\right) + \frac{q-1}{q}\left(2-\left(x+\frac{1}{x}\right)\right)^d - q^d.
\end{aligned}$$

Now let $z = x + 1/x$. Recall that $x = e^{iqt}$ for some t, so $-2 \leqslant z \leqslant 2$. Substitute z into $F_{\mathbf{1}}(x)$ and we have

$$F_{\mathbf{1}}(z) := \frac{1}{q}((q-1)z + (q-1)^2 + 1)^d + \frac{q-1}{q}(2-z)^d - q^d.$$

The derivative of $F_{\mathbf{1}}(z)$ is positive if and only if

$$((q-1)z + (q-1)^2 + 1)^{d-1} > (2-z)^{d-1}.$$

Notice that the expression in the brackets of the left hand side is at least

$$-2(q-1) + (q-1)^2 + 1 = (q-2)^2 \geqslant 0,$$

so $F'_{\mathbf{1}}(z) > 0$ if and only if

$$(q-1)z + (q-1)^2 + 1 > 2 - z,$$

that is, $z > 2 - q$. It follows that for $q > 4$,

$$F_{\mathbf{1}}(z) \leqslant F_{\mathbf{1}}(2) = q^{d-1} - q^d < 0.$$

Hence $H(d,q)/\langle\mathbf{1}\rangle$ does not admit uniform mixing when $q > 4$. For $q \in \{2,3,4\}$, we see that $z = 2 - q$ is the stationary point and the only zero in the interval $[-2,2]$. Therefore uniform mixing must occur at time t for which $2\cos(qit) = 2 - q$. □

For all the Cayley graphs over $\mathbb{Z}_q$ known to admit uniform mixing, the mixing time is of the form $2\pi/qn$ for some integer n. As a second consequence of Theorem 26, the degree of such a graph must be large enough for mixing to occur at time $2\pi/qn$.

Corollary 28. *Let $\phi(n)$ be the Euler's totient function. If uniform mixing occurs on $X(\mathbb{Z}_q^d, C)$ at time $2\pi/qn$, then*

$$|C| \geqslant \frac{q-1}{2}(\phi(n)+q-1).$$

Proof. Let $g \in C$. For $a, b \in \mathbb{Z}_q^d$ such that $\langle a-b, g\rangle = 0$,

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

Hence

$$\deg(f_g) \leqslant |C| - q + 1.$$

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

$$\phi(n) \leqslant \frac{2}{q-1}(|C| - q + 1). \qquad \square$$

11 Local and Global Uniform Mixing on Stars

For irregular graphs, local uniform mixing may be a better choice to start with. We follow Carlson et al [2] and show that the star $K_{1,n}$ admits local uniform mixing. In particular, uniform mixing in the global sense occurs on the claw $K_{1,3}$.

We apply spectral decomposition to the adjacency matrix A of the star $K_{1,n}$. The eigenvalues of $K_{1,n}$ are $\theta_0 = 0$, $\theta_1 = \sqrt{n}$ and $\theta_2 = -\sqrt{n}$. Denote the projections onto these eigenspaces by E_0, E_1 and E_2. We have

$$\begin{aligned} E_0 &= \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & I - \frac{1}{n}J \end{pmatrix}, \\ E_1 &= \frac{1}{2n}\begin{pmatrix} n & \sqrt{n}\mathbf{1}^T \\ \sqrt{n}\mathbf{1} & J \end{pmatrix}, \\ E_2 &= \frac{1}{2n}\begin{pmatrix} n & -\sqrt{n}\mathbf{1}^T \\ -\sqrt{n}\mathbf{1} & J \end{pmatrix}, \end{aligned}$$

where J denotes the all-ones matrix. It follows that the transition matrix of $K_{1,n}$ is

$$\begin{aligned} U(t) &= e^{0\cdot it}E_0 + e^{\sqrt{n}it}E_1 + e^{-\sqrt{n}it}E_2 \\ &= \begin{pmatrix} \cos(\sqrt{n}t) & \frac{i}{\sqrt{n}}\sin(\sqrt{n}t)\,\mathbf{1} \\ \frac{i}{\sqrt{n}}\sin(\sqrt{n}t)\,\mathbf{1} & I + \frac{1}{n}(\cos(\sqrt{n}t) - 1)\,J \end{pmatrix}. \end{aligned}$$

The quantum walk starting with the central vertex is uniform mixing at time t if and only if

$$\left|\cos\left(\sqrt{n}t\right)\right| = \left|\frac{\sin\left(\sqrt{n}t\right)}{\sqrt{n}}\right|$$

or equivalently,

$$\tan\left(\sqrt{n}t\right) = \pm\sqrt{n}. \tag{11}$$

Thus, the star $K_{1,n}$ admits local uniform mixing at time

$$\pm\frac{\arctan\left(\sqrt{n}\right)}{\sqrt{n}} + k\pi$$

for all integers k.

For uniform mixing, one additional condition from the lower right block of $U(t)$ is

$$\left|1 + \frac{1}{n}\left(\cos\left(\sqrt{n}t\right) - 1\right)\right| = \left|\frac{1}{n}\left(\cos\left(\sqrt{n}t\right) - 1\right)\right|$$

or equivalently,

$$\cos\left(\sqrt{n}t\right) = 1 - \frac{n}{2}. \tag{12}$$

Combining Equation (11) and Equation (12), we see that the only solution is

$$n = 3, \quad t = \pm\frac{2\pi}{\sqrt{27}} + 2k\pi$$

for all integers k. Plugging this into $U(t)$ yields a flat matrix. We conclude that the only star that admits uniform mixing is the claw $K_{1,3}$, with earliest mixing time $2\pi/\sqrt{27}$. The Cartesian powers of $K_{1,3}$ then form an infinite family of irregular graphs that admit uniform mixing.

12 Open Problems

There are a number of open problems on unifom mixing, ranging across characterizing graphs that admit uniform mixing in some common family, determining the mixing times of a given graph, and constructing new examples. Following our notation in Section 4, we let τ_q denote the earliest time at which the complete graph K_q admits uniform mixing.

1. Question: To determine whether uniform mixing occurs on the quotient graph $H(d,q)/\Gamma$ at time τ_q, we have to check the weight distribution of every coset of Γ. Is it sufficient to just check the weight distribution of Γ?

   For groups with one or two generators, the weight distribution of any coset $\Gamma + c$ is merely a permutation of the weight distribution of Γ. For an example see Theorem 10. If this were true in general, it would be helpful in characterizing linear Cayley graphs with higher degrees.

2. Question: Is there a characterization of uniform mixing on non-linear Cayley graphs over $\mathbb{Z}_q^d$?

   This is one thing that the weight distribution condition does not tell. For $q \geqslant 4$, a Cayley graph over $\mathbb{Z}_q^d$ may not be linear, and thus may not be a quotient graph of $H(d,q)$. It is desirable to find another approach for these non-linear Cayley graphs.

3. Question: If a Cayley graph over $\mathbb{Z}_q^d$ admits uniform mixing, must its eigenvalues be integral?

   As we mentioned in Section 1, all the known Cayley graphs that admit uniform mixing have integer eigenvalues. It is unclear if this is a necessary condition. The first place to find a counterexample might be the Cayley graphs over $\mathbb{Z}_5^d$, as the eigenvalues are no longer guaranteed to be integral.

4. Question: If a Cayley graph over $\mathbb{Z}_q^d$ admits uniform mixing at time t, must t be a rational multiple of π?

   Again this is true for all the known examples. However, it may only apply to graphs with integer eigenvalues. Even for this smaller class of graphs, it would be interesting to confirm such an algebraic property of the mixing times.

5. Question: How fast can a Cayley graph over $\mathbb{Z}_q^d$ admit uniform mixing?

   So far, the best examples that admit uniform mixing earlier than τ_q are the distance graphs of $H(d,2)$ found in [3], and the distance graphs of $H(d,3)$ and $H(d,4)$ found in Section 8 of this paper. These families provide arbitrarily faster uniform mixing, although at the cost of larger vertex sets. In an effort to construct new examples with faster uniform mixing, a question arises as to whether there is a lower bound on the mixing time of a given graph.

6. Question: Are there more irregular graphs that admit uniform mixing?

   The star $K_{1,3}$ and its Cartesian powers suggest that there could be other irregular graphs that admit uniform mixing. As we did in Section 11, one may look at local uniform mixing on some common families of irregular graphs, and then impose more conditions for global uniform mixing.

References

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

[2] William Carlson, Allison Ford, Elizabeth Harris, Julian Rosen, Christino Tamon, and Kathleen Wrobel, *Universal mixing of quantum walk on graphs*, Quantum Information & Computation **7** (2007), 738–751.

[3] Ada Chan, *Complex Hadamard matrices, instantaneous uniform mixing and cubes*, arXiv:1305.5811 (2013).

[4] Leonard Eugene Dickson, *History of the Theory of Numbers. Vol. I: Divisibility and Primality*, Chelsea Publishing Co., New York, 1966.

[5] Chris Godsil, *Generalized Hamming schemes*, arXiv:1011.1044 (2010).

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

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

[8] Cristopher Moore and Alexander Russell, *Quantum walks on the hypercube*, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **2483** (2002), 164–178.

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

[10] Hanmeng Zhan, *Uniform Mixing on Cayley Graphs over Z_3^d*, Ph.D. thesis, University of Waterloo, 2014.