Some results on uniform mixing on abelian Cayley graphs

Xiwang Cao
Department of Math,
Nanjing University of Aeronautics and Astronautics
email: xwcao@nua.edu.cn

Joint work with Jinlong Wan and Keqing Feng

Open Problems in Algebraic Combinatorics Workshop
May 3-7, 2021

This talk is based on the following paper:
Xiwang Cao, Jinlong Wan, Keqin Feng, Some results on uniform mixing on abelian Cayley graphs, arXiv:1911.07495

Background and Introduction

Quantum algorithms stand in the central stage of quantum information processing and computation and are the research field of both mathematicians and engineers around a few decades.

- In 1998, Fahri and Gutmann [1] first introduced the concept of quantum walk,
- Childs *et al.* [2] found a graph in which the continuous-time quantum walk spreads exponentially faster than any classical algorithm for a certain black-box problem.
- Childs also showed that the continuous-time quantum walk model is a universal computational model. [3]

---

[1] E. Farhi and S. Gutmann, Quantum computation and decision trees. Phys. Rev. A (3), 58(2)(1998) 915-928.

[2] A. Childs, R. Cleve, E. Deotto, E. Farhi, S.Gutmann, D. Spielman, Exponential algorithmic speedup by a quantum walk, in: Proc. 35th ACM Symp. Theory of Computing, 2003, pp. 59-68.

[3] A. M. Childs. Universal computation by quantum walk. Phys. Rev. Lett., 102(18)(2009) 180501.

Let $\Gamma = (V, E)$ be an undirected simple graph where V is the vertex set and E is the edge set. Let A be the adjacency matrix of Γ, i.e.,

$$A = (a_{uv})_{u,v \in V}, \text{ where } a_{uv} = \begin{cases} 1, & \text{if } (u, v) \in E, \\ 0, & \text{otherwise.} \end{cases}$$

A continuous random walk on Γ is determined by a family of matrices of the form $M(t)$, indexed by the vertices of Γ and parameterized by a real positive time t. The (u, v)-entry of $M(t)$ represents the probability of starting at vertex u and reaching vertex v at time t. Define a continuous random walk on Γ by setting

$$M(t) = \exp(t(A - D)),$$

where D is a diagonal matrix. Then each column of $M(t)$ corresponds to a probability density of a walk whose initial state is the vertex indexing the column.

For a connected simple graph Γ with adjacency matrix A, the *transfer matrix* of Γ is defined as the following $n \times n$ matrix:

$$H(t) = H_\Gamma(t) = \exp(\imath t A) = \sum_{s=0}^{+\infty} \frac{(\imath t A)^s}{s!} = (H_{g,h}(t))_{g,h \in V}, \quad t \in \mathbb{R},$$

where $\imath = \sqrt{-1}$ and $n = |V(\Gamma)|$ is the number of vertices in Γ.

Definition 2.1

A graph Γ admits uniform mixing if

$$|H(t)_{uv}| = \frac{1}{\sqrt{n}}$$

for each pair of vertices u and v in Γ, where n is the size of the points set V.

An example

Let $\Gamma = K_2$,

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

Then

$$H(t) = e^{itA} = I_2 + \sum_{j=1}^{+\infty} \frac{(itA)^j}{j!} = \sum_{j=0}^{+\infty} \frac{(-1)^j t^{2j}}{(2j)!} I_2 + \sum_{j=0}^{+\infty} \frac{(-1)^j i t^{2j+1}}{(2j+1)!} A.$$

Thus we get

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

Let $t = \pi/4$. Then $|H(t)_{u,v}| = 1/\sqrt{2}$.

Up to date, the known graphs having uniform mixing are rare, we list some of them as follows:

- the star $K_{1,3}$, [4];
- complete graphs K_2, K_3, K_4, [5];
- Hamming graphs $H(d,2)$, $H(d,3)$ and $H(d,4)$, (Ref. 4);
- the Paley graph of order nine, [6];
- some strongly regular graphs from regular symmetric Hadamard matrices, (Ref. 4);
- some linear Cayley graphs over $\mathbb{Z}_2^d$, $\mathbb{Z}_3^d$ and $\mathbb{Z}_4^d$, (Ref. 4);
- the Cartesian product of graphs which admit uniform mixing at the same time, (Ref. 4);

---

[4] C. Godsil, H. Zhan, Uniform mixing on Cayley graphs, Electronic J. Combin., 24(3)(2017)♯P3.20.

[5] A. Ahmadi, R. Belk, C. Tamon, C. Wendler, On mixing in continuous-time quantum walks on some circulant graphs, Quantum Comput. Inf., 3 (2003) 611-618.

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

Motivation

Contribution

A characterization of abelian Cayley graphs having uniform mixing is presented. Some concrete constructions of such graphs are provided. Specifically, for cubelike graphs, it is shown that the Cayley graph $\mathrm{Cay}(\mathbb{F}_2^{2k}; S)$ has uniform mixing if the characteristic function of S is bent. Moreover, a difference-balanced property of the eigenvalues of an abelian Cayley graph having uniform mixing is established. Furthermore, it is proved that an integral abelian Cayley graph exhibits uniform mixing if and only if the underlying group is one of the groups: $\mathbb{Z}_2^d, \mathbb{Z}_3^d, \mathbb{Z}_4^d$ or $\mathbb{Z}_2^r \otimes \mathbb{Z}_4^d$ for some integers $r \geq 1, d \geq 1$. Thus the classification of integral abelian Cayley graphs having uniform mixing is completed.

Preliminaries

Let G be an abelian group with order n, the exponent of G (the maximal order of elements of G) be m. Denote

$$\mathbb{C}^G = \{f : f \text{ is a complex-valued function on } G\}.$$

For $f_1, f_2 \in \mathbb{C}^G$, define

$$\langle f_1, f_2 \rangle = \sum_{x \in G} f_1(x)\overline{f_2(x)},$$

where $\overline{f_2(x)}$ is the complex conjugation of $f_2(x)$. Then $\mathbb{C}^G$ is a Hilbert space with the above scalar product.

Let $\widehat{G}$ be the character group of G consisting of the homomorphisms

$$\chi : G \to T_m = \{z \in \mathbb{C} : z^m = 1\}.$$

Then the set $\{\frac{1}{\sqrt{n}}\chi_a : a \in G\}$ form an orthonormal basis of $\mathbb{C}^G$.

For any $f \in \mathbb{C}^G$, its Fourier transform is defined by

$$\widehat{f}(a) = \sum_{x \in G} f(x)\overline{\chi_a(x)} = \langle f, \chi_a \rangle.$$

The inverse transform is determined by

$$f(x) = \frac{1}{n} \sum_{a \in G} \widehat{f}(a)\chi_a(x) = \sum_{a \in G} \langle f, \frac{1}{\sqrt{n}}\chi_a \rangle \frac{1}{\sqrt{n}}\chi_a(x).$$

Bent functions over finite abelian groups

Definition 4.1

Let G be an abelian group of order n. A function $f \in \mathbb{C}^G$ is called bent on G if for every $a \in G$, we have

$$|\widehat{f}(a)| = \sqrt{n}.$$

Cayley graphs over abelian groups

Let G be a finite abelian group of order n. The operation of G is addition, the identity element of G is 0. Let S be a subset of G with $|S| = d \geq 1$. The Cayley graph $\Gamma = \mathrm{Cay}(G, S)$ is defined by

$$\begin{aligned} V(\Gamma) &= G, \text{ the set of vertices,} \\ E(\Gamma) &= \{(u, v) : u, v \in G, u - v \in S\}, \text{ the set of edges.} \end{aligned}$$

We assume that $0 \notin S$ and $S = -S := \{-s : s \in S\}$ (which means that Γ is a simple graph) and $G = \langle S \rangle$ (G is generated by S which means that Γ is connected).

For any symmetric real matrix A of n by n, assume that its eigenvalues are $\lambda_i, 1 \leq i \leq n$, not necessarily distinct. We can form an orthogonal matrix $P = (p_1, \cdots, p_n)$, where p_i is an eigenvector of λ_i $(1 \leq i \leq n)$. So that we have the following spectral decomposition:

$$A = \lambda_1 E_1 + \cdots + \lambda_n E_n, \tag{4.1}$$

where $E_i = p_i p_i^* (1 \leq i \leq n)$ satisfy

$$E_i E_j = \begin{cases} E_i, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases} \tag{4.2}$$

Here we use the symbol superscript * to denote the conjugate transpose of a matrix. Therefore, we have the decomposition of the transfer matrix

$$H(t) = \exp(\imath \lambda_1 t) E_1 + \cdots + \exp(\imath \lambda_n t) E_n. \tag{4.3}$$

Particularly, when A is the adjacency matrix of an abelian Cayley graph $\Gamma = \mathrm{Cay}(G, S)$, take $P = \frac{1}{\sqrt{n}}(\chi_g(h))_{g,h\in G}$, where $n = |G|$ and $\chi_g \in \hat{G}$. Then P is a unitary matrix and

$$P^* A P = \mathrm{diag}(\lambda_g; g \in G),$$

where

$$\lambda_g = \sum_{s\in S} \chi_g(s), g \in G$$

are the eigenvalues of Γ.

Suppose that $\Gamma = \mathrm{Cay}(G, S)$ is a connected integral graph. Denote

$$
\begin{aligned}
M &= \gcd(d - \lambda_g : 0 \neq g \in G), d = |S|, && (4.4)\\
M_h &= \gcd(\lambda_{x+h} - \lambda_x : x \in G), 0 \neq h \in G, && (4.5)\\
D_G &= \gcd(M_h : 0 \neq h \in G). && (4.6)
\end{aligned}
$$

Lemma 4.2

Let notation be defined as above. Then we have
(1) $M||G|$;
(2) $M_h||G|(d-\lambda_h), d=|S|, 0\neq h\in G$.
(3) If G *is an abelian* p*-group, then both* D_G *and* M *are powers of* p.

A characterization of abelian Cayley graphs having uniform mixing

Theorem 5.1

Let Γ be a simple abelian Cayley graph. For each fixed real number t, define a complex-valued function on G by

$$G_t(g) = \exp(\imath \lambda_g t).$$

Then Γ has uniform mixing at time t if and only if G_t is a bent function on G.

Equivalently, we have

Corollary 5.2

Let notation be defined as above. Then Γ has uniform mixing at time t if and only if for every $h(\neq 0) \in G$, it holds that the correlation function

$$R_t(h) := \sum_{g \in G} \exp(\imath(\lambda_{g+h} - \lambda_g)t) = 0. \tag{5.1}$$

Corollary 5.3

Define an n by n matrix

$$W = (\exp(\imath \lambda_{x+y} t))_{x,y \in G}. \tag{5.2}$$

Then Γ has uniform mixing at time t if and only if W is a symmetric complex Hadamard matrix, namely, $W^T = W$ and $WW^* = nI_n$.

Corollary 5.2 and Corollary 5.3 are equivalent, we just give the proof of the second one.

Proof. Denote

$$z_g := \frac{1}{\sqrt{n}} \sum_{x \in G} \exp(\imath \lambda_x t) \chi_x(g), \forall g \in G. \tag{5.3}$$

Then Γ has uniform mixing at time t if and only if $|z_g| = 1$ for all $g \in G$. From (5.3), we get

$$\exp(\imath \lambda_x t) = \frac{1}{\sqrt{n}} \sum_{g \in G} z_g \overline{\chi_g(x)}, \forall x \in G. \tag{5.4}$$

Thus if $|z_g| = 1$ for all $g \in G$, then

$$\begin{aligned}
& \sum_{g\in G} \exp(\imath\lambda_{x+g}t)\overline{\exp(\imath\lambda_{y+g}t)} \\
= \quad & \frac{1}{n}\sum_{g\in G}\sum_{u\in G} z_u\overline{\chi_u(x+g)}\sum_{v\in G}\bar{z}_v\chi_v(y+g) \\
= \quad & \sum_{u\in G}|z_u|^2\chi_u(y-x) \\
= \quad & \sum_{u\in G}\chi_u(y-x) \\
= \quad & \begin{cases} 0, & \text{if } y \neq x, \\ n, & \text{if } y = x. \end{cases}
\end{aligned}$$

Thus W is a symmetric complex Hadamard matrix.
Conversely, if W is a complex Hadamard matrix, then by above computation, we have

$$\sum_{u \in G} |z_u|^2 \chi_u(a) = \begin{cases} 0, & \text{if } a \neq 0, \\ n, & \text{if } a = 0. \end{cases}$$

The desired result follows from the inverse Fourier transformation.
This completes the proof.

Suppose that $\Gamma = \mathrm{Cay}(G, S)$ is an integral abelian Cayley graph having uniform mixing at time t. Denote

$$A_h(X) := \sum_{g \in G} X^{\lambda_{g+h} - \lambda_g} \in \mathbb{Z}[X, X^{-1}], \forall h (\neq 0) \in G.$$

Let

$$d_h = \max\{\lambda_{g+h} - \lambda_g : g \in G\}, \text{ and } B_h(X) = X^{d_h} A_h(X).$$

Denote

$$a(X) := \gcd(B_h(X) : 0 \neq h \in G). \tag{6.1}$$

Theorem 6.1

Let notation be defined as above. Suppose that $\Gamma = \mathrm{Cay}(G, S)$ *is an integral abelian Cayley graph. Then the number of the time* t *in the interval* $(0, 2\pi)$ *such that* Γ *has uniform mixing at* t *is upper bounded by*

$$2 \max_{0 \neq h \in G} \{\lambda_{g+h} - \lambda_g : g \in G\}.$$

Moreover, assume that the $a(X)$ *in (6.1) has all its roots on the unit circle. If* $\Gamma = \mathrm{Cay}(G, S)$ *has uniform mixing at a time* t*, then* $\gamma = e^{\imath t}$ *is a root of unity.*

We recall some basic facts about cyclotomic fields. Let $\omega_n = \exp(\imath\frac{2\pi}{n})$ and $K = \mathbb{Q}(\omega_n)$ be the corresponding cyclotomic field. The Galois group of the extension $K/\mathbb{Q}$ is

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_\ell : \ell \in \mathbb{Z}^*\} \cong \mathbb{Z}_n^*,$$

where $\mathbb{Z}_n^* = \{\ell \in \mathbb{Z}_n : \gcd(\ell, n) = 1\}$ is the unit group of the ring $\mathbb{Z}_n = \mathbb{Z}/(n)$ and σ_ℓ is defined by $\sigma_\ell(\omega_n) = \omega_n^\ell$.

Lemma 6.2

Suppose that G is an abelian group of order n and $\Gamma = \mathrm{Cay}(G, S)$ is a Cayley graph. Then the following statements are equivalent:
(1) Γ is an integral graph;
(2) for every positive integer ℓ, $1 \leq \ell \leq n$, and $\gcd(\ell, n) = 1$, it holds that $\lambda_{\ell g} = \lambda_g$;
(3) for every positive integer ℓ with $\gcd(\ell, n) = 1$, it holds that $\ell S := \{\ell s : s \in S\} = S$.

Theorem 6.3

Let p, q be two different odd prime integers and G be the abelian group of order pq. If $\Gamma = \mathrm{Cay}(G, S)$ is an integral graph with connection set S, then Γ cannot admit uniform mixing at any time t.

Integral Cayley p-graphs

For any abelian group G and an abelian group H, a mapping f from G to H is called a *difference balanced function* if for every $a(\neq 0) \in G$ and every $b \in H$, the number of solutions to the following equation

$$f(x+a) - f(x) = b$$

is independent on the choice of a and b.

Theorem 6.4

Let G be an abelian group of an odd prime power order and $\Gamma = \mathrm{Cay}(G, S)$ be an integral Cayley p-graph. Let e' be a positive integer such that $p^{e'-1} | (\lambda_{g+h} - \lambda_g)$ for every $g, h \in G$. Let $H = p^{e'-1}\mathbb{Z}_p = \{p^{e'-1} j : j = 0, 1, \cdots, p-1\}$. Then Γ has uniform mixing at time $t = \frac{2\pi r}{p^{e'}}$ if and only if the mapping $\lambda : G \to H, g \mapsto p^{e'-1}(\lambda_g \pmod p)$ is a difference balanced function.

Theorem 6.5

Let p be an odd prime number and $G = \mathbb{Z}_p^r$ the elementary commutative p-group. If $\Gamma = \mathrm{Cay}(G, S)$ is an integral graph, then Γ has uniform mixing for some subset S if and only if $p = 3$.

When $p = 3, r = 2$, $S = \{(1, x) : x \in \mathbb{Z}_p\}$, then the eigenvalues of Γ are: $\lambda_{(00)} = 4$, $\lambda_{(01)} = \lambda_{(02)} = \lambda_{(11)} = \lambda_{(22)} = 1$, $\lambda_{(10)} = \lambda_{(20)} = \lambda_{(12)} = \lambda_{(21)} = -2$. The difference table of the eigenvalues is the following Table 1.

Table 1. $\lambda_{g+h} - \lambda_g$.

$h \backslash g$	00	10	20	01	11	21	02	12	22
01	-3	3	0	0	-3	3	3	0	-3
10	-6	0	6	0	-3	3	-3	3	0
11	-3	0	3	-3	0	3	-3	0	3
02	-3	0	3	3	-3	0	0	3	-3
12	-6	3	3	-3	-3	6	0	0	0
20	-6	6	0	-3	0	3	0	3	-3
21	-6	3	3	0	0	0	-3	6	-3
22	-3	3	0	-3	3	0	-3	3	0

It is a routine to check that each row is $\{0^{(3)}, 3^{(3)}, 6^{(3)}\} \pmod 9$. Thus $R_t(h) = 0$ for each $h \neq 0$ and then Γ has uniform mixing at time $t = \frac{2\pi}{9}$ by Corollary 5.2.

Theorem 6.6

Let p be a prime number and r be a positive integer. Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^r}, S)$ be an integral Cayley graph. Then Γ admits uniform mixing for some connection set S at some time t if and only if $p = 2, 3$ and $r = 1$, or $p = 2, 3$ and $r = 2$.

Theorem 6.7

Let G be an abelian group. Let $\Gamma = \mathrm{Cay}(G, S)$ be an integral Cayley graph. If Γ has uniform mixing at some time t, then G is an elementary p-group, where $p = 2$ or 3, or $G = \mathbb{Z}_4^d, \mathbb{Z}_2^r \otimes \mathbb{Z}_4^d$ for some integers $r \geq 1, d \geq 1$. Conversely, for such groups, there exist suitable connection set S such that the corresponding Cayley graphs admit uniform mixing.

cubelike graphs

Theorem 7.1

Let G be an abelian 2-group and $\Gamma = \mathrm{Cay}(G, S)$ be an integral simple Cayley graph. Let ν be defined by $D_G = \gcd(M_h : 0 \neq h \in G) = 2^\nu$. For every $0 \neq h \in G$, define the following sets:

$$\begin{aligned} N_2(h) &= \{g \in G : v_2(\lambda_{g+h} - \lambda_g) > \nu + 1\}, \\ N_1(h) &= \{g \in G : v_2(\lambda_{g+h} - \lambda_g) = \nu + 1\}, \\ N_0(h) &= \{g \in G : v_2(\lambda_{g+h} - \lambda_g) = \nu\}, \end{aligned}$$

and denote $n_i(h) = |N_i(h)|$, $i = 0, 1, 2$. Then Γ has uniform mixing at time $t = \frac{\pi}{2^{\nu+1}}$ if and only if for every $0 \neq h \in \mathbb{F}_{2^n}$, $n_2(h) = n_1(h)$.

Theorem 7.2

Let $G = (\mathbb{F}_2^{2k}, +)$ be an elementary 2-group and S be a subset of G. Let f be the characteristic function of S. Then $\Gamma = \mathrm{Cay}(G, S)$ has uniform mixing at time $t = \frac{\pi}{2^k}$ if f is a bent function on G.

Sketch of the proof: When f is bent, we can write

$$\widehat{F}(g) = 2^k(-1)^{\widetilde{f}(g)}.$$

The function $\widetilde{f}$ is called the dual of f. It is well-known that $\widetilde{f}$ is bent if and only if f is bent. Thus we have

$$\lambda_g = -2^{k-1}(-1)^{\widetilde{f}(g)}, g \neq 0. \tag{7.1}$$

Then

$$d - \lambda_g = d + 2^{k-1}(-1)^{\widetilde{f}(g)} = 2^{v_2(d)}\left[d' + 2^{k-v_2(d)-1}(-1)^{\widetilde{f}(g)}\right],$$

where $d = 2^{v_2(d)}d'$, d' is odd.

Without loss of generality, we assume that $d = 2^{n-1} - 2^{k-1}$, thus $v_2(d) = k - 1$ and $M = 2^k$, i.e., $\ell = k$. Taking $t = \frac{2\pi}{2M}$. Since

$$\widehat{F}(0) = \sum_{x \in G} (-1)^{f(x)} = 2^n - 2|S| = 2^k,$$

we know that $\widetilde{f}(0) = 0$. Noticing that $(-1)^f = 1 - 2f$ for any boolean function f, we get

$$R_t(h) = \sum_{g \in G} \exp(-\imath\pi(\widetilde{f}(g+h) - \widetilde{f}(g))) = \sum_{g \in G} (-1)^{\widetilde{f}(g+h) - \widetilde{f}(g)}. \tag{7.2}$$

Thus $R_t(h) = 0$ for all $h \neq 0$ if $\widetilde{f}$ is bent. It is known that $\widetilde{f}$ is bent if and only if f is bent. This completes the proof.

Conclusion Remarks

In this paper, we mainly present the following results:

1. A necessary and sufficient condition for an abelian Cayley graph having uniform mixing is provided (see Theorem 5.1, Corollary 5.2, Corollary 5.3).
2. For an integral abelian Cayley graph Γ having uniform mixing at time t, we show that $\exp(\imath t)$ is a root of unity under certain constrictions (see Theorem 6.1). We hope that some of the constrains can be removed.
3. For an abelian integral Cayley p-graph, we show that it has uniform mixing at a time of the form $2\pi r/p^{e'}$ if and only if its eigenvalues induces a certain difference-balanced mapping (see Theorem 6.4).

- For an abelian group G, we show that if $\mathrm{Cay}(G, S)$ is integral and has uniform mixing at some time t, then G is an elementary p-group, where $p = 2$ or 3, or $G = \mathbb{Z}_4^d, \mathbb{Z}_2^r \otimes \mathbb{Z}_4^d$ for some integers $r \geq 1, d \geq 1$. Conversely, if G is an elementary p-group, where $p = 2$ or 3, or if $G = \mathbb{Z}_4^d, \mathbb{Z}_2^r \otimes \mathbb{Z}_4^d$ for some integers $r \geq 1, d \geq 1$, then $\mathrm{Cay}(G, S)$ has uniform mixing at some time t for some connection set S. This gives a complete classification of integral abelian Cayley graphs having uniform mixing.
- For cubelike graphs, we show that $\Gamma = \mathrm{Cay}(\mathbb{F}_2^{2m}; S)$ has uniform mixing at time $t = \pi/2^m$ if f is a bent function, where f is the characteristic function of S (see Theorem 7.2).
- Some concrete constructions of graphs having uniform mixing are presented.

Open questions

For further research, we list the following open questions:
Open question 1: Find more properties of the characteristic function of S such that the Cayley graph $\mathrm{Cay}(\mathbb{Z}_3^n; S)$ (or $\mathrm{Cay}(\mathbb{Z}_4^n; S)$) has uniform mixing at some time t.
Open question 2: Find some lower bounds on the time t at which $\mathrm{Cay}(\mathbb{Z}_3^n; S)$ (or $\mathrm{Cay}(\mathbb{Z}_4^n; S)$) has uniform mixing.
Open question 3: If $\Gamma = \mathrm{Cay}(G, S)$ is an abelian Cayley graph having uniform mixing, prove or disprove that Γ is integral.
Open question 4: If $\Gamma = \mathrm{Cay}(G, S)$ is an abelian Cayley graph having uniform mixing at time t, prove or disprove that $\exp(\imath t)$ is a root of unity.

Thank you very much for your attention