Discrete Mathematics Letters
www.dmlett.com

Discrete Math. Lett. **7** (2021) 58–65
DOI: 10.47443/dml.2021.0057

Research Article

On the non-existence of Abelian Moore Cayley graphs with excess one

Wei He*

College of Liberal Arts and Sciences, National University of Defense Technology, 410073 Changsha, China

(Received: 31 May 2021. Received in revised form: 11 July 2021. Accepted: 12 July 2021. Published online: 15 July 2021.)

Abstract

The order of an Abelian Cayley graph of degree $2n$ and diameter 2 cannot exceed $2n^2+2n+1$, which is the famous Abelian Cayley-Moore bound. Leung and Zhou [*J. Combin. Theory Ser. A* **171** (2020) Art# 105157] recently shown that such a graph attaining the aforementioned bound exists if and only if $n=1,2$. This note is concerned with the Abelian Cayley graphs of degree $2n$ and diameter 3, whose order is $2n^2+2n+2$, one larger than the Abelian Cayley-Moore bound of degree $2n$ and diameter 2. Their generating set denoted by S satisfies $|\tilde{S}^2|=2n^2+2n+1$ where $\tilde{S}=S\cup\{e\}$, e being the identity element of the underlying group. For $n=1,2$, it is easy to find examples. For $n>2$, several non-existence results for infinitely many values of n are provided by using two methods, which are related to symmetric polynomials theories and algebraic number theory.

Keywords: Abelian Cayley graph; degree-diameter problem; Moore bound; symmetric functions; group ring.

2020 Mathematics Subject Classification: 05C25, 05C35, 05E05.

1. Introduction

For positive integers d and k, denote by $n_{d,k}$ the largest order of a graph of maximum degree d and diameter k. The well-known and widely studied *degree-diameter problem* is to determine the largest number $n_{d,k}$. The famous upper bound on the number $n_{d,k}$ is the *Moore bound*, which gives $n_{d,k}\leq 1+d+d(d-1)+\cdots+d(d-1)^{k-1}$ for every $d,k\geq 1$. Except for $k=1$ or $d\leq 2$, graphs achieving the Moore bound exist only for $k=2$ and $d=3,7$, and possibly 57; see [1,6,8]. Until now, it is not known yet whether a Moore graph of degree $d=57$ and diameter $k=2$ on 3250 vertices exists. For a summary on the history and development on this topic, we refer the reader to the survey paper of Miller and Širáň [14].

Let G be a finite group with identity element e and let $S\subset G$ be a unit-free, inverse-closed generating set for G (i.e. $e\notin S$, $S=S^{-1}$). The *Cayley graph* $\Gamma(G,S)$ for the underlying group G and the generating set S is a graph with vertex set $V(\Gamma)=G$ and edge set $E(\Gamma)=\{\{g,h\}|g,h\in G, g^{-1}h\in S\}$. As the generating set S is closed, $g^{-1}h\in S$ implies that $h^{-1}g\in S$ and therefore our Cayley graphs are undirected. In particular, when G is Abelian, we call $\Gamma(G,S)$ an *Abelian Cayley graph*. For a Cayley graph $\Gamma(G,S)$, denoting $S\cup\{e\}$ by $\tilde{S}$, it is easy to show that its diameter is k if and only if k is the smallest integer such that all elements of G appear in $\tilde{S}^k$ $\left(\tilde{S}^k=\left\{\prod_{i=1}^k s_i : s_i\in\tilde{S} \text{ for } i=1,2,...,k\right\}\right)$ and its degree is $|S|$.

For an Abelian Cayley graph with $|S|=2n$ and diameter k, denote by $A_C(2n,k)$ its largest order. The upper bound on $A_C(2n,k)$ is given by

$$A_C(2n,k)\leq \sum_{i=0}^{\min\{k,n\}} 2^i\binom{k}{i}\binom{n}{i}. \tag{1}$$

The right-hand-side of the above inequality is also called the *Abelian Cayley-Moore bound*, obtained first by Dougherty and Faber in [7], and we denote its value by $M_C(2n,k)$. Obviously, $M_C(2n,2)=2n^2+2n+1$. An Abelian Cayley graph whose order meets $M_C(2n,k)$ is called an *Abelian Cayley-Moore graph*.

The problem whether Abelian Cayley-Moore graphs exist or not has been studied extensively. Leung and Zhou [10] proved that Abelian Cayley-Moore graphs of diameter 2 exist if and only if $n=1,2$. As the Abelian Cayley-Moore bound is sometimes hard to be met, several researchers working in this field try to find a larger lower bound of $A_C(2n,k)$; see [4,7,11–13,17,18].

For a Cayley graph $\Gamma(G,S)$ of degree $2n$ and diameter $k+1$, suppose that G has size $M_C(2n,k)+\lambda$, where λ is a small positive integer. If $\tilde{S}$ satisfies $|\tilde{S}^k|=M_C(2n,k)$, borrowing the terminology of Bannai and Ito [2], we call the parameter λ the *excess*. We give two Abelian Cayley graphs of diameter 3 and excess 1 as follows, which are also the examples of the graphs we research for $n=1,2$.

*E-mail address: he.wei.hc@outlook.com

Example 1.1. *Let C_m denote the cyclic group of order m generated by g.*

- *For $n = 1$, let $G = C_6$ and $S = \{g^{\pm 1}\}$. The graph $\Gamma(G, S)$ is the 6-cycle.*
- *For $n = 2$, let $G = C_{14}$. Define $S = \{g^{\pm 1}, g^{\pm 4}\}$. The graph $\Gamma(G, S)$ is depicted in Figure 1. The corresponding packing of $\mathbb{Z}^2$ by Lee spheres of radius 2 is given in Figure 2.*

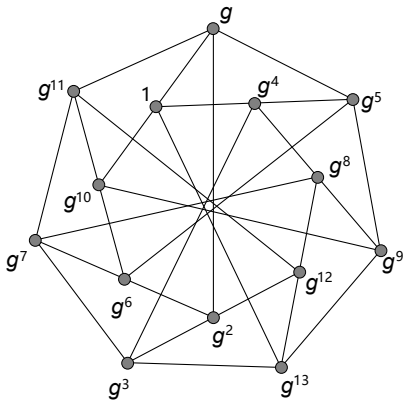

Figure 1: The Cayley graph in C_{14} generated by $\{g^{\pm 1}, g^{\pm 4}\}$.

7	8	9	10	11	12	13	0	1	2	3	4	5
3	4	5	6	7	8	9	10	11	12	13	0	1
13	0	1	2	3	4	5	6	7	8	9	10	11
9	10	11	12	13	0	1	2	3	4	5	6	7
5	6	7	8	9	10	11	12	13	0	1	2	3
1	2	3	4	5	6	7	8	9	10	11	12	13
11	12	13	0	1	2	3	4	5	6	7	8	9
7	8	9	10	11	12	13	0	1	2	3	4	5
3	4	5	6	7	8	9	10	11	12	13	0	1
13	0	1	2	3	4	5	6	7	8	9	10	11

Figure 2: The almost lattice packing of $\mathbb{Z}^2$ by Lee spheres of radius 2 associated with S.

In this paper, we consider the Abelian Cayley graphs $\Gamma(G, S)$ of degree $2n$, diameter 3 and excess 1 (i.e. $|G| = M_C(2n, 2) + 1 = 2n^2 + 2n + 2$). Such Abelian Cayley graphs also provide almost lattice packings of $\mathbb{Z}^2$ by Lee spheres of radius 2 with a small amount of blank.

The rest of this paper is organized as follows. In Section 2, we review some basic notations on group ring to obtain the necessary and sufficient condition on this problem and translate the problem into several group ring equations. In Section 3, we provide some results about the non-existence of Abelian Cayley graphs for infinitely many values of n by utilizing two approaches. The first approach involves the symmetric polynomials which is similar to the one used in [9] by Kim. The second one is close to the one used in [20] which requires that $|G|$ must have small prime divisors.

2. A necessary and sufficient condition

For convenience, we assume that G is a multiplicative group with identity element e. The group ring $\mathbb{Z}[G]$ denotes a set of formal sums $\sum_{g\in G} a_g g$ where $a_g \in \mathbb{Z}$. For any set A whose elements belong to G (A may be a multiset), we identify A with the group ring element $\sum_{g\in G} a_g g$, where a_g is the multiplicity of g appearing in A. The addition of elements in $\mathbb{Z}[G]$ is defined as follows:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g.$$

The multiplication is defined by

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) := \sum_{g\in G} \left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g.$$

Moreover,

$$\lambda \cdot \left(\sum_{g \in G} a_g g \right) := \sum_{g \in G} (\lambda a_g)\, g.$$

where $\lambda \in \mathbb{Z}$. For $A = \sum_{g \in G} a_g g$ and $t \in \mathbb{Z}$, we define

$$A^{(t)} := \sum_{g \in G} a_g g^t.$$

For any $A = \sum_{g \in G} a_g g$ and $\chi \in \widehat{G}$ where $\widehat{G}$ is the character group of G, we define $\chi(A) = \sum_{g \in G} a_g \chi(g)$. The following *inversion formula* gives us a strategy to calculate a_h for all $h \in G$ and shows that A is completely determined by its character value $\chi(A)$, where χ ranges over $\widehat{G}$.

Lemma 2.1. *Let G be an Abelian group. If $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$, then*

$$a_h := \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A)\chi(h^{-1}), \tag{2}$$

for all $h \in G$.

Group rings and the associated characters are of great significance to research the difference sets and related topics. See [3, 16] and the references within. In the rest of this paper, by abuse of notation, we will use the same symbol to denote a subset in G and the associated element in $\mathbb{Z}[G]$. Moreover, we use $|A|$ to denote the number of distinct elements in A, rather than the counting of elements with multiplicity unless stating it specially.

For the Abelian Cayley graph $\Gamma(G, S)$ which we research, we can prove that there is only one element of order 2 in G.

Lemma 2.2. *Assume that $\Gamma(G, S)$ is an Abelian Cayley graph of $|S| = 2n$, diameter 3 and excess 1. G is a multiplicative group with identity element e. Then there is only one element f of order 2 in G and $f \notin \tilde{S}^2$.*

Proof. Since $2 \mid |G|$ and $4 \nmid |G|$, there is only one element f of order 2 in G. By the order of S and S is inverse-closed, we see that $f \notin S$. Moreover, if $f \in \tilde{S}^2$, then there exist $a, b \in S$ such that $f = ab = a^{-1}b^{-1}$, which means $|\tilde{S}^2| < 2n^2 + 2n + 1$. However, by the assumption that $\Gamma(G, S)$ is of diameter 3 and excess 1, $|\tilde{S}^2| = 2n^2+2n+1$ which is a contradiction. Therefore, $f \notin \tilde{S}^2$. □

In the rest part of this section, we present a necessary and sufficient condition for the existence of an Abelian Cayley graph $\Gamma(G, S)$ which we research in the language of group ring equations.

Theorem 2.1. *Let G be an Abelian multiplicative group of order $2n^2+2n+2$ with identity element e, and S an inverse-closed subset of size $2n$ in G. $\Gamma(G, S)$ is of excess 1 if and only if $T = S \cup \{e\}$ (For convenience, we use T rather than $\tilde{S}$ to denote $S \cup \{e\}$) viewed as an element in $\mathbb{Z}[G]$ satisfying*

(a) $e \in T$,

(b) $T = T^{(-1)}$,

(c) $T^2 = 2G - T^{(2)} + 2ne - 2f$.

Proof. Suppose that $S = \{a_1, \cdots, a_n\} \bigcup \{a_1^{-1}, \cdots, a_n^{-1}\}$. By definition, $T = e + \sum_{i=1}^{n} (a_i + a_i^{-1})$. Hence, (a) and (b) are obviously satisfied.

In the language of group ring, we have

$$e + f + \sum_{i=1}^{n} (a_i + a_i^{-1} + a_i^2 + a_i^{-2}) + \sum_{1 \leqslant i < j \leqslant n} (a_i + a_i^{-1})(a_j + a_j^{-1}) = G.$$

By computation, we have

$$\begin{aligned} T^2 &= \left(e + \sum_{i=1}^{n} (a_i + a_i^{-1}) \right)^2 \\ &= e + 2\sum_{i=1}^{n} (a_i + a_i^{-1}) + \left(\sum_{i=1}^{n} (a_i + a_i^{-1}) \right)^2 \end{aligned}$$

$$
\begin{aligned}
&=e+2\sum_{i=1}^{n}(a_i+a_i^{-1})+\sum_{i=1}^{n}(a_i^2+a_i^{-2})+2\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1})+2ne\\
&=2e+2\sum_{i=1}^{n}(a_i+a_i^{-1})+2\sum_{i=1}^{n}(a_i^2+a_i^{-2})+2\sum_{1\leqslant i<j\leqslant n}(a_i+a_i^{-1})(a_j+a_j^{-1})\\
&\quad+(2n-1)e-\sum_{i=1}^{n}(a_i^2+a_i^{-2})\\
&=2(G-f)+2ne-T^{(2)}\\
&=2G-T^{(2)}+2ne-2f.
\end{aligned}
$$

Therefore, (c) holds.

For the other direction of the proof, we only need to define $S=T\setminus\{e\}$ and the verification is straightforward. □

3. Main results

In this section, we intend to apply two approaches to prove non-existence results of T satisfying (a), (b) and (c) in Theorem 2.1. The first one is an imitation of the method provided by Kim in [9]. The second one based on the necessary and sufficient condition mentioned in Section 2 is close to the one used in [20] by Zhang and Zhou which requires $|G|$ having small prime divisors.

3.1. A symmetric polynomial approach

First we apply the Kim's approach to this problem. Compared with the original one in [9], we do not need the assumption that $|G|$ is a prime, but n^2+n+1 is a prime.

Theorem 3.1. *Assume that G is an Abelian additive group of order $2(n^2+n+1)$ for $n>1$ where $p=n^2+n+1$ is a prime. Let a be the smallest positive integer for which $p\mid 4^a+4n+2$ and b be the smallest positive integer for which $p\mid 4^b-1$. (Let $a=\infty$ if there is no a with $p\mid 4^a+4n+2$.) If the equation $a(x+1)+by=n$ has no nonnegative integer solutions, then S which is an inverse-closed and unitfree subset of size $2n$ in G and satisfies $|T^2|=2n^2+2n+1$ ($T=S\cup\{e\}$) does not exist.*

Proof. Assume that there exists such S. Separate S into $R=\{r_i : i=1,...,n\}$ and $R^{(-1)}=\{r_i^{-1} : r_i\in R\}$. Since $|T^2|=2n^2+2n+1$, then by Lemma 2.2,

$$\{0\},\{\pm r_i : i=1,...,n\},\{\pm 2r_i : i=1,...,n\},\{\pm r_i\pm r_j : 1\leq i<j\leq n\}$$

form a partition of $G\setminus\{f\}$ where f is the unique element of order 2.

Assume H is a subgroup of G of index n^2+n+1. Let $\rho: G\to G/H$ be the canonical homomorphism and $x_i=\rho(r_i)$. Then the multisets

$$\{0\},\{*\ \pm r_i : i=1,...,n\ *\},\{*\ \pm 2r_i : i=1,...,n\ *\},\{*\ \pm r_i\pm r_j : 1\leq i<j\leq n\ *\}$$

form a partition of $2G/H\setminus\{0\}$. For an integer k, by calculation,

$$
\begin{aligned}
&\sum_{i=1}^{n}(x_i^{2k}+(-x_i)^{2k}+(2x_i)^{2k}+(-2x_i)^{2k})\\
&+\sum_{1\leq i<j\leq n}((x_i+x_j)^{2k}+(x_i-x_j)^{2k}+(-x_i+x_j)^{2k}+(-x_i-x_j)^{2k})\\
=&(4^k+4n+2)S_{2k}+2\sum_{t=1}^{k-1}\binom{2k}{2t}S_{2t}S_{2(k-t)},
\end{aligned}
$$

where $S_t:=\sum_{i=1}^{n}x_i^t$. Since this is also the sum of the $2k$-th powers of every element in $2G/H\setminus\{0\}$,

$$(4^k+4n+2)S_{2k}+2\sum_{t=1}^{k-1}\binom{2k}{2t}S_{2t}S_{2(k-t)}=\begin{cases}0, & p-1\nmid 2k;\\ -2, & p-1\mid 2k.\end{cases}\tag{3}$$

Let a and b be the least positive integers satisfying $p\mid 4^a+4n+2$ and $p\mid 4^b-1$. Define

$$X=\{ax+by : x\geq 1, y\geq 0\}.$$

We prove the following two claims by induction on k.

Claim 1: If $1 \leq k < \frac{p-1}{2}$ is not in X, then $S_{2k} = 0$.
By induction on k, suppose that $S_{2k} = 0$ for each $k \leq k_0 - 1$ that is not in X. Assume that $k_0 \notin X$. As X is closed under addition, for each t, either t or $k_0 - t$ is not in X.

Since any integer k for which $p \mid 4^k + 4n + 2$ must be of the form $a + by$ whence $k \in X$. This implies $p \nmid 4^{k_0} + 4n + 2$. By (3) and the induction hypothesis,

$$0 = (4^{k_0} + 4n + 2)S_{2k_0} + 2\sum_{t=1}^{k_0-1} \binom{2k_0}{2t} S_{2t}S_{2(k_0-t)} = (4^{k_0} + 4n + 2)S_{2k_0}.$$

Hence, $S_{2k_0} = 0$.

Let e_k be the elementary symmetric polynomials with respect to $x_1^2, x_2^2, ..., x_n^2$.

Claim 2: If $1 \leq k \leq n < \frac{p-1}{2}$ is not in X, then $e_k = 0$.
We again prove by induction on k, suppose that $e_k = 0$ for all $k \leq k_0 - 1$ not in X and $k_0 \notin X$. Since X is closed under addition, for each $0 < t < k_0$, at least one of t and $k_0 - t$ is not in X. By Claim 1 and the inductive hypothesis, $e_t = 0$ or $S_{2(k_0-t)} = 0$. Together with Newton identities on $x_1^2, x_2^2, ..., x_n^2$, we have

$$k_0 e_{k_0} = e_{k_0-1}S_2 - e_{k_0-2}S_4 + \cdots + (-1)^{k_0-1}S_{2k_0} = (-1)^{k_0-1}S_{2k_0} = 0.$$

then $e_{k_0} = 0$.

Note that $e_n = x_1^2 \cdots x_n^2$, it is clear that none of $x_1, ..., x_n$ is 0. Then $e_n \neq 0$. By Claim 2, $n \in X$. This finishes the proof. □

By MAGMA [5] program, in $1 < n \leq 10^5$, n has 10750 choices to make $n^2 + n + 1$ be a prime. However, only $n = 2$ and $n = 3$ are not excluded by Theorem 3.1 in these values. The detailed result is showed in Table 1. Actually, Zhang and Zhou [20, Subsection 3.1] provide a generalization of Kim's approach which requires that $2n^2 + 2n + 1$ has a prime divisor larger that $2n + 1$.

In [20, Subsection 3.2], the approach to deal with $|G|$ with a small prime divisor was put forward. Next, we use this approach to deal with $|G| = 2n^2 + 2n + 2$ with a small prime divisor.

3.2. The method of Zhang and Zhou

By Lemma 2.2, we know that G has a unique element of order 2 denoted by f. Therefore, for any subgroup H of G, if $|H|$ is even, then H must contain f. Let $\overline{(\cdot)} : G \to G/H$ be the canonical homomorphism. Then $\bar{f}$ is the identity element in G/H. For $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, we define $\overline{A} = \sum_{g\in G} a_g \bar{g}$. Assume a subgroup $H \leq G$ of even order m, the following two equations must hold for T satisfying Conditions (b) and (c).

(b') $\overline{T} = \overline{T}^{(-1)}$,

(c') $\overline{T}^2 = 2mG/H - \overline{T}^{(2)} + 2n - 2$.

Here, for the convenience of description, we use 1 to denote the identity element $\bar{e}$ in G/H. Hence $(2n-2)\bar{e}$ is simply written as $(2n - 2)$.

First, we consider a very special case for which Conditions (b') and (c') hold.

Lemma 3.1. *Let K be an Abelian group of order v with identity element e_K and $S = a \cdot e_K + bK \in \mathbb{Z}[K]$. If v and m are positive integers such that $a + vb = 2n + 1$ and $mv = 2n^2 + 2n + 2$, and S satisfies*

$$S^2 = 2mK - S + (2n - 2)e_K, \tag{4}$$

then $8n - 7$ is a square in $\mathbb{Z}$.

Proof. By calculation, we obtain

$$\begin{aligned} S^2 &= (ae_K + bK)^2 \\ &= a^2 e_K + 2abK + b^2 vK \\ &= a^2 e_K + (ab + b(2n + 1))K. \end{aligned}$$

By checking the coefficient of e_K in (4), we get

$$a^2 + a - 2n + 2 = 0,$$

which shows that $8n - 7$ must be a square in $\mathbb{Z}$. □

As 3 is the smallest prime dividing $|G|$, let us look at the existence of $\overline{T}$ in G/H which is isomorphic to the cyclic group C_3 of order 3.

Proposition 3.1. *Suppose that $G/H \cong C_3$, $8n-7$ is a non-square. Then there is no $\overline{T} \in \mathbb{Z}[C_3]$ of size $2n+1$ satisfying Conditions (b') and (c').*

Proof. We proceed by way of contradiction, assume that there exists $\overline{T} \in \mathbb{Z}[C_3]$ satisfying Conditions (b') and (c'). Note that $\overline{T}^{(2)} = \overline{T}^{(-1)} = \overline{T}$. Thus $\overline{T} = a + bG/H$ for some $a, b \in \mathbb{Z}_{\geq 0}$, and by Condition (c') we have

$$\overline{T}^2 = 2mG/H - \overline{T} + 2n - 2.$$

By Lemma 3.1, it contradicts our assumption that $8n-7$ is a non-square. Hence, there is no $\overline{T} \in \mathbb{Z}[C_3]$ satisfying Conditions (b') and (c'). □

To get stronger non-existence results, we need to apply some konwledge on the algebraic number theory.

Lemma 3.2 ([19], page 263)**.** *If m is a square-free integer, with prime factorization*

$$m = 2^t \prod_j p_j,$$

where the p_j are the distinct odd primes appearing in m, $t = 0$ or 1. Let $m' = \prod_j p_j$. Then the smallest cyclotomic field containing $\mathbb{Q}(\sqrt{m})$ is

$$\begin{aligned} &\mathbb{Q}(\zeta_{m'}) \quad if \quad m \equiv 1 \pmod 4; \\ &\mathbb{Q}(\zeta_{4m'}) \quad if \quad m \equiv -1 \pmod 4; \\ &\mathbb{Q}(\zeta_{8m'}) \quad if \quad m \equiv 2 \pmod 4. \end{aligned}$$

Next, we look at $v = 7$, which is the second smallest possible odd prime dividing $|G|$. In order to deal with this case, we need to exploit the theory about the decomposition of a prime p into prime ideals in $\mathbb{Z}[\zeta_\omega]$, which can be found in [15].

Lemma 3.3. *Let p be a prime and let ζ_ω be a primitive ω-th root of unity in $\mathbb{C}$. If $\omega = p^r\omega'$ with $\gcd(\omega', p) = 1$, then the prime ideal decomposition of (p) in $\mathbb{Z}[\zeta_\omega]$ is*

$$(p) = (P_1P_2...P_d)^e,$$

where P_i's are distinct prime ideals, $e = \varphi(p^r)$, $d = \varphi(\omega')/f$ and f is the order of p modulo ω'. If t is an integer not divisible by p and $t \equiv p^s \pmod{\omega'}$ for a suitable integer s, then the field automorphism $\sigma_t : \zeta_{\omega'} \mapsto \zeta_{\omega'}^t$ fixes the ideals P_i.

Theorem 3.2. *Suppose that $G/H \cong C_7$, $8n-7$ is a non-square. Then there is no subset $\overline{T} \in \mathbb{Z}[C_7]$ of size $2n+1$ satisfying Conditions (b') and (c').*

Proof. By way of contradiction, assume that there exists a subset $\overline{T} \in \mathbb{Z}[C_7]$ satisfying Conditions (b') and (c'), then

$$f_i = \overline{T}^{(2^i)}\overline{T}^{(2^i)} + \overline{T}^{(2^{i+1})} - 2n + 2 \equiv 0 \pmod{G/H}, \tag{5}$$

for $i = 0, 1, 2$. Thinking of them as polynomials with variables $\overline{T}^{(2^i)}$, we calculate the resultants of f_0, f_1 and f_2 to obtain a polynomial h having only one variable $\overline{T}$. All above can be done by MAGMA [5]. Furthermore, we factorize $h \pmod{G/H}$ into 2 irreducible factors

$$h \equiv (\overline{T}^2 + \overline{T} - 2n + 2)l \pmod{G/H},$$

where

$$l = \overline{T}^6 - \overline{T}^5 - (6n-7)\overline{T}^4 + (4n-5)\overline{T}^3 + (12n^2 - 30n + 19)\overline{T}^2 - (4n^2 - 12n + 9)\overline{T} - 8n^3 + 32n^2 - 42n + 19.$$

It is no doubt that h must be congruent to 0 modulo G/H. Because there is no zero divisors in the residue ring of $\mathbb{Z}[G/H]$ modulo (G/H) which is isomorphic to $\mathbb{Z}[X]/(\sum_{i=0}^{6} X^i)$, one of the two factors of h must be congruent to 0 modulo G/H.

Assume $\overline{T}^2 + \overline{T} - 2n + 2$ is congruent to 0 modulo G/H. Let $\chi \in \widehat{G/H}$ be a non-principal character. Then $\chi(\overline{T}) \in \mathbb{Z}[\zeta_7]$ is such that

$$\chi(\overline{T})^2 + \chi(\overline{T}) - 2n + 2 = 0, \tag{6}$$

which implies that $8n-7$ is a square in $\mathbb{Z}[\zeta_7]$. Because $8n-7$ is a non-square in $\mathbb{Z}$, we can assume $8n-7$ has a square divisor $8n-7 = tk^2$ where t is a square-free integer larger than 1 and $k \in \mathbb{Z}$. Then $t \equiv 1 \pmod 8$. Obviously $t > 7$. By

Lemma 3.2, the smallest cyclotomic field containing $\mathbb{Q}(\sqrt{8n-7})$ is $\mathbb{Q}(\zeta_t)$ rather than $Q(\zeta_7)$, so there is no $\chi(\overline{T})$ such that (6) holds. Hence, $\overline{T}^2+\overline{T}-2n+2$ cannot be congruent to 0 modulo G/H, then $l\equiv 0 \pmod{G/H}$.

Since l as a polynomial in $\overline{T}$ is of degree 6, we try to take a prime number p and consider the equation $\chi(l)=0$ modulo p. Let p be primitive modulo $v=7$, i.e. $p=3,5 \pmod v$. By Lemma 3.3, (p) is a prime ideal in $\mathbb{Z}[\zeta_v]$. Substitute X for $\chi(\overline{T}) \pmod p$ in $\chi(l)\equiv 0 \pmod p$ and let its coefficients be calculated modulo p. Then we obtain a polynomial $\bar{l}(X)$ in $\mathbb{F}_p[X]$.

Let τ_1 be a root of $\bar{l}(X)$. Suppose the degree of the minimal polynomial of τ_1 is s. Then the conjugates of τ_1 are $\tau_1^p,\tau_1^{p^2},\ldots,\tau_1^{p^{s-1}}$. As p is primitive modulo $v=7$, $p^{\frac{v-1}{2}}\equiv -1 \pmod v$. Since $\chi(\overline{T}^{(p)})\equiv\chi(\overline{T})^p \pmod p$ and $\overline{T}^{(-1)}=\overline{T}$,

$$\chi(\overline{T})=\chi(\overline{T}^{(-1)})=\chi\left(\overline{T}^{(p^{\frac{v-1}{2}})}\right)\equiv\chi(\overline{T})^{p^{\frac{v-1}{2}}} \pmod p.$$

Thus,

$$\tau_1^{p^3}=\tau_1^{p^{\frac{v-1}{2}}}=\tau_1$$

which means $s=1$ or $s=3$. Consequently all the roots $\tau_1,\tau_1^p,\ldots,\tau_1^{p^{s-1}}$ of $\bar{l}$ are in $\mathbb{F}_{p^3}$.

By $\chi(\overline{T}^{(p)})\equiv\chi(\overline{T})^p \pmod p$, we can calculate $\tau_i:=\chi(\overline{T}^{(2^i)})$ from τ_1 as follows:

$$\tau_i:\equiv\chi(\overline{T}^{(2^i)})\equiv\begin{cases}\tau_1^{p^{3-i}} \pmod p, & \text{if } p\equiv 3 \pmod 7;\\ \tau_1^{p^i} \pmod p, & \text{if } p\equiv 5 \pmod 7.\end{cases} \tag{7}$$

Consider the necessary conditions that τ_1 must satisfy. First, by (5),

$$\tau_i^2+\tau_{i+1}-2n+2\equiv 0 \pmod p, \tag{8}$$

for $i=0,1,2$. Second, we calculate the coefficients of $a_{\bar{g}}$ by using the inversion formula (2). Let β be an element of order $v=7$ in $\mathbb{F}_{p^{v-1}}$. For $\bar{g}\in G/H$ with $\chi(\bar{g})\equiv\beta \pmod p$,

$$\begin{aligned}a_{\bar{g}}&=\frac{1}{7}\left((2n+1)+\sum_{i=1}^{6}\chi(\overline{T}^{(i)})\chi(\bar{g}^{-i})\right)\\&=\frac{1}{7}\left((2n+1)+\sum_{i=1}^{3}\chi(\overline{T}^{(i)})\left(\chi(\bar{g}^i)+\chi(\bar{g}^{-i})\right)\right)\\&\equiv\frac{1}{7}\left((2n+1)+\sum_{j=0}^{2}\tau_1^{p^j}(\beta^{p^j}+\beta^{-p^j})\right) \pmod p.\end{aligned} \tag{9}$$

It is obvious that $a_{\bar{g}} \pmod p$ must correspond to an element in $\mathbb{F}_p$. In addition, since the size of $\overline{T}$ is $2n+1$, all $a_{\bar{g}}$'s also satisfy that

$$\sum_{\bar{g}\in G/H}a_{\bar{g}}\equiv 2n+1 \pmod p. \tag{10}$$

Based on all the previous necessary conditions, now we provide a method to exclude the existence of $\overline{T}$ satisfying Conditions (b') and (c'). First we choose a prime p. Then, depending on the value of n modulo p, we divide the calculations into p different cases. In each case, $\bar{l}$ is a concrete polynomial. To check the necessary conditions, we calculate all the roots of $\bar{l}$ in $\mathbb{F}_p^3=\mathbb{F}_p^{\frac{v-1}{2}}$ and then for each root τ_1,

(i) plug it into (7) to get τ_i;

(ii) check whether (8) holds for each i;

(iii) derive $a_{\bar{g}}$ from (9);

(iv) check whether $a_{\bar{g}}$ satisfies $a_{\bar{g}} \pmod p\in\mathbb{F}_p$ and (10).

By our MAGMA program, taking $p=101$, for each possible value of n modulo p, we can always find at least one of the necessary conditions not satisfied. Hence there is no $\overline{T}$ such that Conditions (b') and (c') hold. □

In the proof of Theorem 3.2, we need to raise $\overline{T}$ to $\overline{T}^{(2)}$ in $\overline{T}^2\equiv-\overline{T}^{(2)}+2n-2 \pmod{G/H}$ which is true only if 2 is a generator in $C_v\cong G/H$. Thus, we cannot apply this approach to G/H whose order is even. For $|G/H|=\prod_{i=1}^k p_i$ where p_i are prime numbers, if we can show the non-existence of $\overline{T}$ in G/H' which is of order p_i for some $i\in\{1,\ldots,k\}$, then we

also have the non-existence result for G/H. Hence we only concentrate on the case in which $|G/H|$ is an odd prime. As n^2+n+1 is an odd number for all $n \in \mathbb{Z}$, $v \mid 2(n^2+n+1)$ implies $v \mid n^2+n+1$ for every odd prime v.

The approach used in the proof of Theorem 3.2 can be further applied for larger G/H. The next 5 possible values of a prime dividing n^2+n+1 is 13, 19, 31, 37 and 43. Our MAGMA program shows that for $G/H \cong C_{13}$, $G/H \cong C_{19}$ and $G/H \cong C_{31}$, we can choose $p = 227$, $p = 241$ and $p = 881$ respectively and follows the steps in Theorem 3.2 to prove that there is no $\overline{T}$ satisfying Conditions (b') and (c'). For the next odd prime 37 dividing the order of G, our computer is not powerful enough to provide us the univariate polynomial with the variable $\overline{T}$ by calculating the resultants of 18 pairs of polynomials. Hence, we cannot provide any non-existence result for $v = 37$ or any larger prime numbers. As the process is more or less the same, we omit it here and present the results directly as follows:

Corollary 3.1. *Let G be an Abelian group of order $2n^2+2n+2$. Suppose that $8n-7$ is not a square in $\mathbb{Z}$. Assume that one collection of the following conditions holds*

(1) 3, 7, 19 *or* 31 *divides* n^2+n+1*;*

(2) $13 \mid n^2+n+1$, $8n-11 \notin \{13k^2 : k \in \mathbb{Z}\}$.

There is no $T \subseteq G$ viewed as an element in $\mathbb{Z}[G]$ satisfying Conditions (a), (b) and (c).

In Table 1, we list the cardinalities of n excluded by Corollary 3.1 and Theorem 3.1, respectively and the last row indicates the numbers of n to which Corollary 3.1 or Theorem 3.1 can be applied.

Table 1: The numbers of n to which Corollary 3.1 and Theorem 3.1 can be applied, where $v = |G/H|$.

Conditions	10	10^2	10^3	10^4	10^5
$3 \mid n^2+n+1$	1	25	304	3240	33036
$7 \mid n^2+n+1$	1	21	260	2778	28316
$13 \mid n^2+n+1$	1	10	133	1469	15161
$19 \mid n^2+n+1$	0	8	96	1022	10432
$31 \mid n^2+n+1$	1	5	59	627	6394
Corollary 3.1	3	52	620	6486	65826
Theorem 3.1	3	29	186	1407	10748
Total	5	80	805	7892	76573

Acknowledgment

This work is supported by the Natural Science Foundation of Hunan Province (through grant no. 2019RS2031), the Fund for NUDT Young Innovator Awards and the Hunan Provincial Natural Science Foundation of China (through grant no. 2020JJ5612).

References

[1] E. Bannai, T. Ito, On finite Moore graphs, *J. Faculty Sci. Univ. Tokyo Sect. A Math.* **20** (1973) 191–208.
[2] E. Bannai, T. Ito, Regular graphs with excess one, *Discrete Math.* **37** (1981) 147–158.
[3] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Vol. I, Cambridge Univ. Press, Cambridge, 1999.
[4] D. I. Bevan, G. Erskine, R. Lewis, Large circulant graphs of fixed diameter and arbitrary degree, *Ars Math. Contemp.* **13** (2017) 275–291.
[5] W. Bosma, J. Cannon, C. Playoust, The Magma algebra aystem I: The user language, *J. Symbolic Comput.* **24** (1997) 235–265.
[6] R. M. Damerell, On Moore graphs, *Math. Proc. Cambridge Philos. Soc.* **74** (1973) 227–236.
[7] R. Dougherty, V. Faber, The degree-diameter problem for several varieties of Cayley graphs I: The Abelian case, *SIAM J. Discrete Math.* **17** (2004) 478–519.
[8] A. J. Hoffman, R. R. Singleton, On Moore graphs with diameters 2 and 3, *IBM J. Res. Dev.* **4** (1960) 497–504.
[9] D. Kim, Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions, *European J. Combin.* **63** (2017) 1–5.
[10] K. H. Leung, Y. Zhou, No lattice tiling of $\mathbb{Z}^n$ by Lee sphere of radius 2, *J. Combin. Theory Ser. A* **171** (2020) Art# 105157.
[11] R. Lewis, The degree-diameter problem for circulant graphs of degree 8 and 9, *Electron. J. Combin.* **21** (2014) Art# P4.50.
[12] R. Lewis. The degree-diameter problem for circulant graphs of degrees 10 and 11, *Discrete Math.* **341** (2018) 2553–2566.
[13] H. Macbeth, J. Šiagiová, J. Širáň, Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups, *Discrete Math.* **312** (2012) 94–99.
[14] M. Miller, J. Širáň, Moore graphs and beyond: A survey of the degree/diameter problem, *Electron. J. Combin.* **20** (2013) Art# DS14.
[15] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.
[16] A. Pott, *Finite Geometry and Character Theory*, Springer-Verlag, Berlin, 1995.
[17] A. Pott, Y. Zhou, Cayley graphs of diameter two from difference sets, *J. Graph Theory* **85** (2016) 533–544.
[18] J. Širáň, J. Šiagiová, M. Ždímalová, *Large Graphs of Diameter Two and Given Degree*, Proc. IWONT 2010, Univ. Politecnica de Catalunya, 2011, pp. 347–359.
[19] E. Weiss, *Algebraic Number Theory*, Dover Publications, New York, 1998.
[20] T. Zhang, Y. Zhou, On the nonexistence of lattice tilings of $\mathbb{Z}^n$ by Lee spheres, *J. Combin. Theory Ser. A* **165** (2019) 225–257.