J Algebr Comb (2019) 49:135–146
https://doi.org/10.1007/s10801-018-0822-6

Improved lower bounds on the degree–diameter problem

Tao Zhang[1] · **Gennian Ge**[1]

Received: 27 December 2017 / Accepted: 8 March 2018 / Published online: 16 March 2018

Abstract Let $C(d, k)$ and $AC(d, k)$ be the largest order of a Cayley graph and a Cayley graph based on an abelian group, respectively, of degree d and diameter k. It is well known that $C(d, k) \leq 1+d+d(d-1)+\cdots+d(d-1)^{k-1}$ with equality satisfied if and only if the graph is a Moore graph. However, there is a much better upper bound for abelian Cayley graph. We have $AC(d, 2) \leq \frac{d^2}{2} + d + 1$ and $AC(d, k) \leq \frac{d^k}{k!} + O(d^{k-1})$. On the other hand, the best currently lower bounds are $C(d, 2) \geq 0.684d^2$, $AC(d, 2) \geq \frac{25}{64}d^2 - 2.1d^{1.525}$ and $AC(d, k) \geq (\frac{d}{k})^k + O(d^{k-1})$ for sufficiently large d. In this paper, we improve previous results on the degree–diameter problem. We show that $C(d, 2) \geq \frac{200}{289}d^2 - 5.4d^{1.525}$, $AC(d, 2) \geq \frac{27}{64}d^2 - 3.9d^{1.525}$ and $AC(d, k) \geq (\frac{3}{3k-1})^k d^k + O(d^{k-0.475})$ for sufficiently large d.

Keywords Degree–diameter problem · Cayley graph · Group

Mathematics Subject Classification 05C12 · 05C25

Gennian Ge: Research supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310, Beijing Scholars Program, Beijing Hundreds of Leading Talents Training Project of Science and Technology, and Beijing Municipal Natural Science Foundation.

✉ Tao Zhang
taozhang@gzhu.edu.cn

[1] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

1 Introduction

In a graph Γ, the distance $d(u, v)$ from vertex u to vertex v is the length of a shortest $u - v$ path in Γ. The largest distance between two vertices in Γ is the diameter of Γ. Let $\Gamma = (V, E)$ be a graph of maximum degree d and diameter k. According to the Moore bound, Γ has at most $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$ vertices. When the order of V equals $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$, the graph Γ is called a Moore graph. Except $k = 1$ or $d \leq 2$, Moore graphs are only possible for $d = 3, 7, 57$ and $k = 2$ [5,8]. The graphs corresponding to the first two degrees are the Petersen graph and the Hoffman–Singleton graph. The existence of a Moore graph with degree 57 and diameter 2 is still open. As there are very few Moore graphs, it is interesting to ask the following the so-called degree–diameter problem.

Problem 1 *Given positive integers d and k, find the largest possible number $N(d, k)$ of vertices in a graph with maximum degree d and diameter k.*

We refer to [11] for a recent survey on the degree–diameter problem.

The Moore bound for diameter two is $N(d, 2) \leq d^2 + 1$. In [7], Erdős et al. improved this bound by showing that $N(d, 2) \leq d^2 - 1$ for $d \geq 4$, $d \neq 7, 57$. An explicit lower bound $N(d, 2) \geq d^2 - d + i$ is given by Brown's graphs [4] for all d such that $d - 1$ is a prime power and $i = 2$ for $d - 1$ even and $i = 1$ for $d - 1$ odd. A modification of Brown's graphs constructed by Širáň et al. [15] gives the lower bound $N(d, 2) \geq d^2 - 2d^{1.525}$ for all sufficiently large d. Clearly, this bound asymptotically approaches the Moore bound.

Let G be a group and $S \subseteq G$ such that $S^{-1} = S$ and $e \notin S$. Here $S^{-1} = \{s^{-1} : s \in S\}$. The Cayley graph $\Gamma(G, S)$ has a vertex set G, and two distinct vertices g, h are adjacent if and only if $g^{-1}h \in S$. Here S is called the generating set. A Cayley graph is always vertex-transitive and regular, and its valency equals $|S|$. Then, it is easy to see that the diameter of a Cayley graph $\Gamma(G, S)$ is k if and only if k is the smallest integer such that all elements in G appear in $\{\Pi_{i=1}^{l} s_i : s_i \in S \text{ for } l = 1, 2, \ldots, k\}$.

Proposition 1.1 *The diameter of a Cayley graph $\Gamma(G, S)$ is k if and only if k is the smallest integer such that all elements in G appear in $\{\Pi_{i=1}^{k} s_i : s_i \in S \cup \{e\}\}$, where e is the identity of group G.*

Since neither the Brown's graphs nor their modifications are vertex-transitive, it is a natural question to ask what is the maximum number of vertices of a vertex-transitive graph or a Cayley graph of diameter k and degree d. We use $v(d, k)$, $C(d, k)$ and $AC(d, k)$ to denote the largest order of a vertex-transitive graph, a Cayley graph and an abelian Cayley graph, respectively, of degree d and diameter k. Then, we have $N(d, k) \geq v(d, k) \geq C(d, k) \geq AC(d, k)$.

Currently, the best known construction of vertex-transitive graphs is the McKay–Miller–Širáň graph [10], which gives $v(d, 2) \geq \frac{8}{9}(d + \frac{1}{2})^2$, for degrees $d = \frac{1}{2}(3q - 1)$ such that $q \equiv 1 \pmod 4$ is a prime power. In the same paper the authors have shown that all these graphs are non-Cayley.

For Cayley graphs, we have the following results. In [14], Šiagiová and Širáň gave a construction of Cayley graphs of diameter two and of order $d^2 - O(d^{\frac{3}{2}})$

for an infinite set of degrees d. Hence, their result for Cayley graphs asymptotically approaches the Moore bound $d^2 + 1$. Šiagiová and Širáň [13] constructed Cayley graphs of diameter two and of order $\frac{1}{2}(d + 1)^2$ for all degrees $d = 2q - 1$ where q is an odd prime power. In [1], Abas proved that $C(d, 2) \geq \frac{1}{2}d^2 - t$ for $d \geq 4$ even and $C(d, 2) \geq \frac{1}{2}(d^2 + d) - t$ for $d \geq 4$ odd, where $0 \leq t \leq 8$ is an integer depending on the congruence class of d modulo 8. Recently, Abas [2] showed that $C(d, 2) > 0.684d^2$ for every integer $d \geq 360756$. In this paper, we improve Abas's result and show that $C(d, 2) \geq \frac{200}{289}d^2 - 5.4d^{1.525}$ for sufficiently large d.

For Abelian Cayley graphs, we have $AC(d, k) \leq \frac{d^k}{k!} + O(d^{k-1})$ for $d \to \infty$ and fixed k [16]. In [6], Dougherty and Faber showed that $AC(d, k) \geq (\frac{d}{k})^k + O(d^{k-1})$ and asked whether the constant $1/k^k$ can be improved. In this paper, we give an affirmative answer to this question by showing that $AC(d, k) \geq (\frac{3}{3k-1})^k d^k + O(d^{k-0.475})$ for sufficiently large d. For small diameters, we have better results. Macbeth et al. [9] showed that $AC(d, 2) \geq \frac{3}{8}(d^2 - 4)$ for $d = 4q - 2$, where q is an odd prime. This result was generalized in [15], where it is proved that $AC(d, 2) \geq \frac{3}{8}d^2 - 1.45d^{1.525}$ for any sufficiently large d. Later, Pott and Zhou [12] gave a construction of abelian Cayley graphs of diameter two and of order $\frac{25}{64}d^2 - 2.1d^{1.525}$ for sufficiently large d from generalized difference sets. In this paper, we improve their result and show that $AC(d, 2) \geq \frac{27}{64}d^2 - 3.9d^{1.525}$ for sufficiently large d. Other researchers also considered the largest order of a Cayley graph based on cyclic group and metacyclic group, see [9,17].

This paper is organized as follows. In Sect. 2, we give a lower bound for $C(d, 2)$. In Sect. 3, we show lower bounds for $AC(d, 2)$ and $AC(d, k)$.

2 Lower bound for $C(d, 2)$

The following lemma can be found in [2], which will be used later.

Lemma 2.1 [2] *The equations*

$$a_1x + b_1y = c_1,$$
$$a_2x + b_2y = c_2$$

over $\mathbb{Z}_n$ have a unique solution in $\mathbb{Z}_n$ if and only if the determinant $D = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$ is coprime with n.

Now we state our main result.

Theorem 2.2 *Let $n = 2m$, where m is an odd integer. Let $G = \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_2$ be a group with multiplication $(i_0, i_1, i) \cdot (j_0, j_1, j) = (i_0 + j_i, i_1 + j_{1-i}, i + j)$, where $(i_0, i_1, i), (j_0, j_1, j) \in \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_2$. If there exists a subset $T \subseteq G$ such that*

(1) *at least one of* $\{(m, 0, 0), (0, m, 0)\}$ *is contained in* T*;*
(2) *if* $(i, j, 0) \in T$*, then* $i + j \equiv 1 \pmod 2$*;*
(3) $(T \cup T^{-1}) \cdot (T \cup T^{-1}) \supseteq G$*,*

then for any odd prime $p > 4|T|$*, there exists a Cayley graph of diameter two, degree* $(2|T|+1-\epsilon-\rho)p-1$*, and of order* $2p^2n^2$*, where* $\epsilon = |T \cap \{(m,0,0),(0,m,0)\}|$ *and* $\rho = \min\{1, |T \cap \{(i, n-i, 1) : i \in [0, n-1]\}|\}$.

Proof Let p be an odd prime with $p > 4|T|$. Let $H = \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_2$ be a group with multiplication $(x_0, x_1, i_0, i_1, i) \cdot (y_0, y_1, j_0, j_1, j) = (x_0 + (-1)^{i_0} y_i, x_1 + (-1)^{i_1} y_{1-i}, i_0 + j_i, i_1 + j_{1-i}, i + j)$, where $(x_0, x_1, i_0, i_1, i), (y_0, y_1, j_0, j_1, j) \in \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_2$.

Let ω be a primitive element of $\mathbb{F}_p$ and $a_i = \omega^i$. Since at least one of $\{(m,0,0),(0,m,0)\}$ is contained in T, without loss of generality, we assume $(m,0,0) \in T$. If $\rho = 1$, then suppose $(i_z, n-i_z, 1) \in T$. We divide T into five subsets: $T = T_1 \cup T_2 \cup T_3 \cup T_4 \cup T_5$, where

$$T_1 = \{(m,0,0)\},$$
$$T_2 = \{(i_z, n-i_z, 1)\},$$
$$T_3 = \{(0,m,0)\} \cap T,$$
$$T_4 = \{(i,j,0) : (i,j,0) \in T, (i,j,0) \neq (m,0,0),(0,m,0)\} = \{(t_i, s_i, 0) : i \in [1,l]\},$$
$$T_5 = \{(i,j,1) : (i,j,1) \in T, (i,j,1) \neq (i_z, n-i_z, 1)\} = \{(u_i, v_i, 1) : i \in [1,k]\}.$$

Define

$$X_1 = \{A(x) = (x, a_1 x, m, 0, 0) : x \in \mathbb{F}_p\},$$
$$X_2 = \{B(x) = (x, -x, i_z, n-i_z, 1) : x \in \mathbb{F}_p\},$$
$$X_3 = \{C(x) = (x, 0, 0, m, 0) : (0,m,0) \in T, x \in \mathbb{F}_p\},$$
$$X_4 = \{D_i(x) = (x, a_{i+1} x, t_i, s_i, 0) : x \in \mathbb{F}_p, i \in [1,l]\},$$
$$X_5 = \{E_i(x) = (x, a_{i+l+1} x, u_i, v_i, 1) : x \in \mathbb{F}_p, i \in [1,k]\},$$
$$X = X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5.$$

Note that $t_i + s_i \equiv 1 \pmod 2$ and m is odd, then we can compute to get that

$$X_1^{-1} = \{A(x)^{-1} = (x, -a_1 x, m, 0, 0) : x \in \mathbb{F}_p\},$$
$$X_2^{-1} = X_2,$$
$$X_3^{-1} = X_3,$$
$$X_4^{-1} = \{D_i(x)^{-1} = ((-1)^{t_i+1} x, (-1)^{t_i} a_{i+1} x, -t_i, -s_i, 0) : x \in \mathbb{F}_p, i \in [1,l]\},$$
$$X_5^{-1} = \{E_i(x)^{-1} = ((-1)^{v_i+1} a_{l+i+1} x, (-1)^{u_i+1} x, -v_i, -u_i, 1) : x \in \mathbb{F}_p, i \in [1,k]\}.$$

Note that $(0, a_1 \cdot 0, m, 0, 0) = (0, -a_1 \cdot 0, m, 0, 0)$, then $|X \cup X^{-1}| = (2|T| + 1 - \epsilon - \rho)p - 1$.

We can compute to get that $A(x) \cdot A(y) = (x - y, a_1 x + a_1 y, 0, 0, 0)$. Since the determinant $\begin{vmatrix} 1 & -1 \\ a_1 & a_1 \end{vmatrix} = 2a_1$ is coprime with p, then for any $(u, v) \in \mathbb{F}_p \times \mathbb{F}_p$, there is $x, y \in \mathbb{F}_p \times \mathbb{F}_p$ such that $(x - y, a_1 x + a_1 y) = (u, v)$.

We can also compute to get the following equations.

$$
\begin{aligned}
A(x)\cdot B(y) &= (x-y, a_1x-y, m+i_z, n-i_z, 1),\\
A(x)\cdot C(y) &= (x-y, a_1x, m, m, 0),\\
A(x)\cdot D_i(y) &= (x-y, a_1x+a_{i+1}y, m+t_i, s_i, 0),\\
A(x)\cdot E_i(y) &= (x-y, a_1x+a_{i+l+1}y, m+u_i, v_i, 1),\\
A(x)\cdot D_i(y)^{-1} &= (x-(-1)^{t_i+1}y, a_1x\\
&\quad +(-1)^{t_i}a_{i+1}y, m-t_i, -s_i, 0),\\
A(x)\cdot E_i(y)^{-1} &= (x-(-1)^{v_i+1}a_{l+i+1}y, a_1x\\
&\quad +(-1)^{u_i+1}y, m-v_i, -u_i, 1),\\
B(x)\cdot A(y) &= (x+(-1)^{i_z}a_1y, -x\\
&\quad +(-1)^{n-i_z}y, i_z, m+n-i_z, 1),\\
B(x)\cdot C(y) &= (x, -x+(-1)^{n-i_z}y, i_z+m, n-i_z, 1),\\
B(x)\cdot D_i(y) &= (x+(-1)^{i_z}a_{i+1}y, -x+(-1)^{n-i_z}y, i_z\\
&\quad +s_i, n-i_z+t_i, 1),\\
B(x)\cdot E_i(y) &= (x+(-1)^{i_z}a_{i+l+1}y, -x+(-1)^{n-i_z}y, i_z\\
&\quad +v_i, n-i_z+u_i, 0),\\
B(x)\cdot D_i(y)^{-1} &= (x+(-1)^{i_z+t_i}a_{i+1}y, -x\\
&\quad +(-1)^{n-i_z+t_i+1}y, i_z-s_i, n-i_z-t_i, 1),\\
B(x)\cdot E_i(y)^{-1} &= (x+(-1)^{i_z+u_i+1}y, -x\\
&\quad +(-1)^{n-i_z+v_i+1}a_{l+i+1}y, i_z-u_i, n-i_z-v_i, 0),\\
C(x)\cdot B(y) &= (x+y, y, i_z, m+n-i_z, 1),\\
C(x)\cdot D_i(y) &= (x+y, -a_{i+1}y, t_i, m+s_i, 0),\\
C(x)\cdot E_i(y) &= (x+y, -a_{i+l+1}y, u_i, m+v_i, 1),\\
C(x)\cdot D_i(y)^{-1} &= (x+(-1)^{t_i+1}y, (-1)^{t_i+1}a_{i+1}y,\\
&\quad -t_i, m-s_i, 0),\\
C(x)\cdot E_i(y)^{-1} &= (x+(-1)^{v_i+1}a_{l+i+1}y,\\
&\quad (-1)^{u_i}y, -v_i, m-u_i, 1),\\
D_i(x)\cdot B(y) &= (x+(-1)^{t_i}y, a_{i+1}x+(-1)^{s_i}(-y), t_i\\
&\quad +i_z, s_i+n-i_z, 1),\\
D_i(x)\cdot D_j(y) &= (x+(-1)^{t_i}y, a_{i+1}x\\
&\quad +(-1)^{s_i}a_{j+1}y, t_i+t_j, s_i+s_j, 0),\\
D_i(x)\cdot E_j(y) &= (x+(-1)^{t_i}y, a_{i+1}x\\
&\quad +(-1)^{s_i}a_{j+l+1}y, t_i+u_j, s_i+v_j, 1),
\end{aligned}
$$

$$\begin{aligned}
D_i(x)\cdot D_j(y)^{-1} &= (x+(-1)^{t_i+t_j+1}y, a_{i+1}x\\
&\quad +(-1)^{s_i+t_j}a_{j+1}y, t_i-t_j, s_i-s_j, 0),\ i\neq j,\\
D_i(x)\cdot E_j(y)^{-1} &= (x+(-1)^{t_i+v_j+1}a_{l+i+1}y, a_{i+1}x\\
&\quad +(-1)^{s_i+u_j+1}y, t_i-v_j, s_i-u_j, 1),\\
E_i(x)\cdot A(y) &= (x+(-1)^{u_i}a_1y, a_{i+l+1}x\\
&\quad +(-1)^{v_i}y, u_i, v_i+m, 1),\\
E_i(x)\cdot B(y) &= (x+(-1)^{u_i}(-y), a_{i+l+1}x+(-1)^{v_i}y, u_i\\
&\quad +n-i_z, v_i+i_z, 0),\\
E_i(x)\cdot C(y) &= (x, a_{i+l+1}x+(-1)^{v_i}y, u_i+m, v_i, 1),\\
E_i(x)\cdot D_j(y) &= (x+(-1)^{u_i}a_{j+1}y, a_{i+l+1}x\\
&\quad +(-1)^{v_i}y, u_i+s_j, v_i+t_j, 1),\\
E_i(x)\cdot E_j(y) &= (x+(-1)^{u_i}a_{j+l+1}y, a_{i+l+1}x\\
&\quad +(-1)^{v_i}y, u_i+v_j, v_i+u_j, 0),\\
E_i(x)\cdot D_j(y)^{-1} &= (x+(-1)^{u_i+t_j}a_{j+1}y, a_{i+l+1}x\\
&\quad +(-1)^{v_i+t_j+1}y, u_i-s_j, v_i-t_j, 1),\\
E_i(x)\cdot E_j(y)^{-1} &= (x+(-1)^{u_i+u_j+1}y, a_{i+l+1}x\\
&\quad +(-1)^{v_i+v_j+1}a_{l+j+1}y, u_i-u_j, v_i-v_j, 0),\ i\neq j,\\
D_i(x)^{-1}\cdot B(y) &= ((-1)^{t_i+1}x+(-1)^{t_i}y, (-1)^{t_i}a_{i+1}x\\
&\quad +(-1)^{s_i}(-y), -t_i+i_z, -s_i+n-i_z, 1),\\
D_i(x)^{-1}\cdot E_j(y) &= ((-1)^{t_i+1}x+(-1)^{t_i}y, (-1)^{t_i}a_{i+1}x\\
&\quad +(-1)^{s_i}a_{j+l+1}y, -t_i+u_j, -s_i+v_j, 1),
\end{aligned}$$

$$\begin{aligned}
D_i(x)^{-1}\cdot D_j(y)^{-1} &= ((-1)^{t_i+1}x+(-1)^{t_i+t_j+1}y, (-1)^{t_i}a_{i+1}x\\
&\quad +(-1)^{s_i+t_j}a_{j+1}y, -t_i-t_j, -s_i-s_j, 0),\\
D_i(x)^{-1}\cdot E_j(y)^{-1} &= ((-1)^{t_i+1}x\\
&\quad +(-1)^{t_i+v_j+1}a_{l+j+1}y, (-1)^{t_i}a_{i+1}x\\
&\quad +(-1)^{s_i+u_j+1}y, -t_i-v_j, -s_i-u_j, 1),\\
E_i(x)^{-1}\cdot A(y) &= ((-1)^{v_i+1}a_{l+i+1}x\\
&\quad +(-1)^{v_i}a_1y, (-1)^{u_i+1}x+(-1)^{u_i}y, -v_i,\\
&\quad -u_i+m, 1),\\
E_i(x)^{-1}\cdot B(y) &= ((-1)^{v_i+1}a_{l+i+1}x\\
&\quad +(-1)^{v_i}(-y), (-1)^{u_i+1}x\\
&\quad +(-1)^{u_i}y, -v_i+n-i_z, -u_i+i_z, 0),\\
E_i(x)^{-1}\cdot C(y) &= ((-1)^{v_i+1}a_{l+i+1}x, (-1)^{u_i+1}x\\
&\quad +(-1)^{u_i}y, -v_i+m, -u_i, 1),
\end{aligned}$$

$$
\begin{aligned}
E_i(x)^{-1} \cdot D_j(y) = ((-1)^{v_i+1} a_{l+i+1} x \\
&+ (-1)^{v_i} a_{j+1} y, (-1)^{u_i+1} x \\
&+ (-1)^{u_i} y, -v_i + s_j, -u_i + t_j, 1), \\
E_i(x)^{-1} \cdot E_j(y) = ((-1)^{v_i+1} a_{l+i+1} x \\
&+ (-1)^{v_i} a_{j+l+1} y, (-1)^{u_i+1} x \\
&+ (-1)^{u_i} y, -v_i + v_j, -u_i + u_j, 0), \ i \neq j, \\
E_i(x)^{-1} \cdot D_j(y)^{-1} = ((-1)^{v_i+1} a_{l+i+1} x \\
&+ (-1)^{v_i+t_j} a_{j+1} y, (-1)^{u_i+1} x \\
&+ (-1)^{u_i+t_j+1} y, -v_i - s_j, -u_i - t_j, 1), \\
E_i(x)^{-1} \cdot E_j(y)^{-1} = ((-1)^{v_i+1} a_{l+i+1} x \\
&+ (-1)^{v_i+u_j+1} y, (-1)^{u_i+1} x \\
&+ (-1)^{u_i+v_j+1} a_{l+j+1} y, -v_i - u_j, -u_i - v_j, 0).
\end{aligned}
$$

Since $p > 4|T|$, then from the choice of a_i and Lemma 2.1, we have $(X \cup X^{-1}) \cdot (X \cup X^{-1}) \supseteq H$. Hence, the result follows. □

By taking a special group G and a set T in Theorem 2.2, we have the following corollary.

Corollary 2.3 *Let $p > 36$ be an odd prime and $d = 17p - 1$. Then, there exists a Cayley graph of diameter two, degree d, and of order $\frac{200}{289}(d+1)^2$.*

Proof Let $G = \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$ be a group with multiplication $(i_0, i_1, i) \cdot (j_0, j_1, j) = (i_0 + j_i, i_1 + j_{1-i}, i + j)$, where $(i_0, i_1, i), (j_0, j_1, j) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$. Let $T = \{(5, 0, 0), (0, 0, 1), (1, 0, 1), (5, 0, 1), (1, 3, 1), (1, 7, 1), (5, 2, 1), (3, 2, 0), (4, 1, 0)\}$. Then, it is easy to check that T satisfies the conditions in Theorem 2.2. Hence, for odd prime $p > 36$, there exists a Cayley graph of diameter two, degree $17p - 1$, and of order $200p^2$. □

Corollary 2.4 *For sufficiently large degree d,*

$$C(d, 2) \geq \frac{200}{289} d^2 - 5.4 d^{1.525}.$$

Proof Let $p > 36$ be an odd prime. Let T (H, resp.) be the defining set (group, resp.) of the Cayley graph in Corollary 2.3. Then, $|T| = 17p - 1$ and the graph has $200p^2$ vertices.

For any integer $d \in [17p - 1, 200p^2 - 1]$, we can choose and add $(d - |T|)$ elements in H to T to get a new set T' such that $|T'| = d$ and $T' = T'^{-1}$. Clearly the Cayley graph $\Gamma(H, T')$ is still of diameter 2.

Now we fix d, which is sufficiently large. Let $b = \frac{d}{17} + \frac{1}{17}$. By [3], there is a prime p such that $b - b^{0.525} \leq p \leq b$. Hence, we can take this p and construct the Cayley graph $\Gamma(H, T')$ such that $|T'| = d$ and

$$|H| = 200p^2 \geq 200(b - b^{0.525})^2$$

$$
\begin{aligned}
&> 200(b^2 - 2b^{1.525}) \\
&> 200\left(\frac{d^2}{289} - 2\left(\frac{d}{17}\right)^{1.525}\right) \\
&> \frac{200}{289}d^2 - 5.4d^{1.525}.
\end{aligned}
$$

□

3 Lower bounds for $AC(d, k)$

In this section, we consider abelian Cayley graphs. We will give two constructions of abelian Cayley graphs, which improve the lower bounds for $AC(d, 2)$ and $AC(d, k)$.

3.1 $AC(d, 2)$

Theorem 3.1 *Let q be a prime power with $q \geq 13$ and $d = 24q-2$. Then, $AC(d, 2) \geq \frac{27}{64}(d+2)^2$.*

Proof Let w be a primitive element in $\mathbb{F}_{243}$ and $T = \{w^{22i} : i \in [0, 10]\}$. Then, it is easy to check that

$$T \cup (-T) \cup \{\pm x \pm y : x, y \in T, x \neq y\} \cup \{0\} = \mathbb{F}_{243}.$$

Let $G = \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_{243}$ be an abelian group with multiplication $(x_0, x_1, i) \cdot (y_0, y_1, j) = (x_0 + y_0, x_1 + y_1, i + j)$, where $x_0, x_1, y_0, y_1 \in \mathbb{F}_q$ and $i, j \in \mathbb{F}_{243}$. For $a \in \mathbb{F}_q$, let $D_a = \{(x, ax) : x \in \mathbb{F}_q\}$. Then, $D_a + D_b = \mathbb{F}_q \times \mathbb{F}_q$ for $a \neq b$. Denote $T = \{t_1, t_2, \ldots, t_{11}\}$ and $\mathbb{F}_q = \{a_1, a_2, \ldots, a_q\}$. Define

$$D = \big((D_{a_{12}}, 0) \cup (D_{a_{13}}, 0)\big) \bigcup_{i=1}^{11} \big((D_{a_i}, t_i) \cup (D_{a_i}, -t_i)\big) \setminus \{(0, 0, 0)\}.$$

Then, we can compute to get the following equations.

$$
\begin{aligned}
&(D_{a_{12}}, 0) + (D_{a_{13}}, 0) = \mathbb{F}_q \times \mathbb{F}_q \times \{0\}, \\
&(D_{a_{12}}, 0) + (D_{a_i}, \pm t_i) = \mathbb{F}_q \times \mathbb{F}_q \times \{\pm t_i\}, \\
&(D_{a_i}, \pm t_i) + (D_{a_j}, \pm t_j) = \mathbb{F}_q \times \mathbb{F}_q \times \{\pm t_i \pm t_j\} \text{ for } i \neq j.
\end{aligned}
$$

Hence, $(D \cup \{(0, 0, 0)\}) + (D \cup \{(0, 0, 0)\})$ covers all the elements in G. Note that $|D| = 24q - 2$ and $|G| = 243q^2$. We have

$$AC(d, 2) \geq \frac{27}{64}(d+2)^2.$$

□

Corollary 3.2 *For sufficiently large degree d,*

$$AC(d,2) \geq \frac{27}{64}d^2 - 3.9d^{1.525}.$$

Proof Let $p \geq 13$ be an odd prime. Let T (G, resp.) be the defining set (group, resp.) of the Cayley graph in Theorem 3.1. Then, $|T| = 24p - 2$ and the graph has $243p^2$ vertices.

For any integer $d \in [24p-2, 243p^2-1]$, we can choose and add $(d - |T|)$ elements in G to T to get a new set T' such that $|T'| = d$ and $T' = T'^{-1}$. Clearly the Cayley graph $\Gamma(G, T')$ is still of diameter 2.

Now we fix d, which is sufficiently large. Let $b = \frac{d}{24} + \frac{1}{12}$. By [3], there is a prime p such that $b - b^{0.525} \leq p \leq b$. Hence, we can take this p and construct the Cayley graph $\Gamma(G, T')$ such that $|T'| = d$ and

$$\begin{aligned} |G| = 243p^2 &\geq 243(b - b^{0.525})^2 \\ &> 243(b^2 - 2b^{1.525}) \\ &> 243\left(\frac{d^2}{576} - 2\left(\frac{d}{24}\right)^{1.525}\right) \\ &> \frac{27}{64}d^2 - 3.9d^{1.525}. \end{aligned}$$

□

3.2 $AC(d,k)$

In this subsection, we consider the case $AC(d,k)$. We first prove a lower bound for $AC(d,4)$.

Theorem 3.3 *Let q be a prime power and $d = 11q - 5$. Then, $AC(d,4) \geq (\frac{3}{11})^4(d+5)^3(d-6)$.*

Proof Let $H = \mathbb{F}_q^* \times (\mathbb{F}_q)^3 \times (\mathbb{Z}_3)^4$ be an abelian group with multiplication $(x, x_0, x_1, x_2, i_0, i_1, i_2, i_3) \cdot (y, y_0, y_1, y_2, j_0, j_1, j_2, j_3) = (xy, x_0+y_0, x_1+y_1, x_2+y_2, i_0+j_0, i_1+j_1, i_2+j_2, i_3+j_3)$, where $x, y \in \mathbb{F}_q^*$, $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{F}_q$ and $i_0, i_1, i_2, i_3, j_0, j_1, j_2, j_3 \in \mathbb{Z}_3$. Let

$$\begin{aligned}
&A = \{a(x) = (x, x, 0, 0, 1, 0, 0, 0) : x \in \mathbb{F}_q^*\}, \ B = \{b(x) = (x, 0, x, 0, 0, 1, 0, 0) : x \in \mathbb{F}_q^*\}, \\
&C = \{c(x) = (x, 0, 0, x, 0, 0, 1, 0) : x \in \mathbb{F}_q^*\}, \ D = \{d(x) = (x, 0, 0, 0, 0, 0, 0, 1) : x \in \mathbb{F}_q^*\}, \\
&E = \{e(x) = (1, x, 0, 0, 0, 0, 0, 0) : x \in \mathbb{F}_q^*\}, \ F = \{f(x) = (1, 0, x, 0, 0, 0, 0, 0) : x \in \mathbb{F}_q^*\}, \\
&G = \{g(x) = (1, 0, 0, x, 0, 0, 0, 0) : x \in \mathbb{F}_q^*\}, \\
&a = (1, 0, 0, 0, 1, 0, 0, 0), \qquad b = (1, 0, 0, 0, 0, 1, 0, 0), \\
&c = (1, 0, 0, 0, 0, 0, 1, 0).
\end{aligned}$$

It can be computed to get that

$$A^{-1} = \{a(x)^{-1} = (x^{-1}, -x, 0, 0, -1, 0, 0, 0) : x \in \mathbb{F}_q^*\}, \quad B^{-1} = \{b(x)^{-1} = (x^{-1}, 0, -x, 0, 0, -1, 0, 0) : x \in \mathbb{F}_q^*\},$$
$$C^{-1} = \{c(x)^{-1} = (x^{-1}, 0, 0, -x, 0, 0, -1, 0) : x \in \mathbb{F}_q^*\}, \quad D^{-1} = \{d(x)^{-1} = (x^{-1}, 0, 0, 0, 0, 0, 0, -1) : x \in \mathbb{F}_q^*\},$$
$$E^{-1} = E, \quad F^{-1} = F,$$
$$G^{-1} = G,$$
$$a^{-1} = (1, 0, 0, 0, -1, 0, 0, 0), \quad b^{-1} = (1, 0, 0, 0, 0, -1, 0, 0),$$
$$c^{-1} = (1, 0, 0, 0, 0, 0, -1, 0).$$

Define $T' = A \cup B \cup C \cup D \cup E \cup F \cup G \cup \{a, b, c\}$ and $T = T' \cup T'^{-1}$. Then, $|T| = 11q - 5$.

It is easy to compute to get that

$$\begin{aligned}
a(x)a(y)^{-1} f(z)g(w) &= (xy^{-1}, x - y, z, w, 0, 0, 0, 0),\\
d(x)d(y)^{-1} f(z)g(w) &= (xy^{-1}, 0, z, w, 0, 0, 0, 0),\\
e(x) f(y)g(z) &= (1, x, y, z, 0, 0, 0, 0),
\end{aligned}$$

and $\{(xy^{-1}, x - y, z, w, 0, 0, 0, 0) : x, y \in \mathbb{F}_q^*,\ z, w \in \mathbb{F}_q\} \cup \{(xy^{-1}, 0, z, w, 0, 0, 0, 0) : x, y \in \mathbb{F}_q^*,\ z, w \in \mathbb{F}_q\} \cup \{(1, x, y, z, 0, 0, 0, 0) : x, y, z \in \mathbb{F}_q\} = \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \times \{0\} \times \{0\} \times \{0\} \times \{0\}$.

We can do similar discussions, then $(T \cup \{(1, 0, 0, 0, 0, 0, 0, 0)\}) \cdot (T \cup \{(1, 0, 0, 0, 0, 0, 0, 0)\}) \cdot (T \cup \{(1, 0, 0, 0, 0, 0, 0, 0)\}) \cdot (T \cup \{(1, 0, 0, 0, 0, 0, 0, 0)\}) \supseteq H$ follows from the following equations and replace the elements of the left-hand side of equations to their inverse.

$$\begin{aligned}
&a(x)e(y) f(z)g(w) = (x, x + y, z, w, 1, 0, 0, 0), && b(x)e(y) f(z)g(w) = (x, y, x + z, w, 0, 1, 0, 0),\\
&c(x)e(y) f(z)g(w) = (x, y, z, x + w, 0, 0, 1, 0), && d(x)e(y) f(z)g(w) = (x, y, z, w, 0, 0, 0, 1),\\
&a(x)b(y)e(z)g(w) = (xy, x + z, y, w, 1, 1, 0, 0), && a(x)b \cdot e(y)g(z) = (x, x + y, 0, z, 1, 1, 0, 0),\\
&a(x)c(y) f(z)g(w) = (xy, x, z, y + w, 1, 0, 1, 0), && a \cdot c(x) f(y)g(z) = (x, 0, y, x + z, 1, 0, 1, 0),\\
&a(x)d(y) f(z)g(w) = (xy, x, z, w, 1, 0, 0, 1), && a \cdot d(x) f(y)g(z) = (x, 0, y, z, 1, 0, 0, 1),\\
&b(x)c(y)e(z)g(w) = (xy, z, x, y + w, 0, 1, 1, 0), && b \cdot c(x)e(y)g(z) = (x, y, 0, z, 0, 1, 1, 0),\\
&b(x)d(y)e(z)g(w) = (xy, z, x, w, 0, 1, 0, 1), && b \cdot d(x)e(y)g(z) = (x, y, 0, z, 0, 1, 0, 1),\\
&c(x)d(y)e(z) f(w) = (xy, z, w, x, 0, 0, 1, 1), && c \cdot d(x)e(y) f(z) = (x, y, z, 0, 0, 0, 1, 1),\\
&a(x)b(y)c(z)g(w) = (xyz, x, y, z + w, 1, 1, 1, 0), && a \cdot b(x)c(y)g(z) = (xy, 0, x, y + z, 1, 1, 1, 0),\\
&a(x)b \cdot c(y)g(z) = (xy, x, 0, y + z, 1, 1, 1, 0), && a \cdot b \cdot c(x)g(y) = (x, 0, 0, x + y, 1, 1, 1, 0),\\
&a(x)b(y)d(z)g(w) = (xyz, x, y, w, 1, 1, 0, 1), && a \cdot b(x)d(y)g(z) = (xy, 0, x, z, 1, 1, 0, 1),\\
&a(x)b \cdot d(y)g(z) = (xy, x, 0, z, 1, 1, 0, 1), && a \cdot b \cdot d(x)g(y) = (x, 0, 0, y, 1, 1, 0, 1),\\
&a(x)c(y)d(z) f(w) = (xyz, x, w, y, 1, 0, 1, 1), && a \cdot c(x)d(y) f(z) = (xy, 0, z, x, 1, 0, 1, 1),\\
&a(x)c \cdot d(y) f(z) = (xy, x, z, 0, 1, 0, 1, 1), && a \cdot c \cdot d(x) f(y) = (x, 0, y, 0, 1, 0, 1, 1),\\
&b(x)c(y)d(z)e(w) = (xyz, w, x, y, 0, 1, 1, 1), && b \cdot c(x)d(y)e(z) = (xy, z, 0, x, 0, 1, 1, 1),\\
&b(x)c \cdot d(y)e(z) = (xy, z, x, 0, 0, 1, 1, 1), && b \cdot c \cdot d(x)e(y) = (x, y, 0, 0, 0, 1, 1, 1),\\
&a(x)b(y)c(z)d(w) = (xyzw, x, y, z, 1, 1, 1, 1), && a \cdot b(x)c(y)d(z) = (xyz, 0, x, y, 1, 1, 1, 1),\\
&a(x)b \cdot c(y)d(z) = (xyz, x, 0, y, 1, 1, 1, 1), && a(x)b(y)c \cdot d(z) = (xyz, x, y, 0, 1, 1, 1, 1),\\
&a(x)b \cdot c \cdot d(y) = (xy, x, 0, 0, 1, 1, 1, 1), && a \cdot b(x)c \cdot d(y) = (xy, 0, x, 0, 1, 1, 1, 1),\\
&a \cdot b \cdot c(x)d(y) = (xy, 0, 0, x, 1, 1, 1, 1), && a \cdot b \cdot c \cdot d(x) = (x, 0, 0, 0, 1, 1, 1, 1).
\end{aligned}$$

□

The following theorem is a generalization of Theorem 3.3, and the discussion is similar as that of Theorem 3.3; we skip the proof.

Theorem 3.4 *Let q be a prime power, k be an integer and $d = (3k-1)q - k - 1$. Then, $AC(d,k) \geq (\frac{3}{3k-1})^k (d+k+1)^{k-1}(d-2k+2)$.*

Corollary 3.5 *For sufficiently large degree d,*

$$AC(d,k) \geq \left(\frac{3}{3k-1}\right)^k d^k + O(d^{k-0.475}).$$

Proof Let p be an odd prime. Let T, (G, resp.) be the defining set (group, resp.) of the Cayley graph in Theorem 3.4. Then, $|T| = (3k-1)p - k - 1$ and the graph has $3^k p^{k-1}(p-1)$ vertices.

For any integer $d \in [(3k-1)p-k-1, 3^k p^{k-1}(p-1)-1]$, we can choose and add $(d - |T|)$ elements in G to T to get a new set T' such that $|T'| = d$ and $T' = T'^{-1}$. Clearly the Cayley graph $\Gamma(G, T')$ is still of diameter k.

Now we fix d, which is sufficiently large. Let $b = \frac{d}{3k-1} + \frac{k+1}{3k-1}$. By [3], there is a prime p such that $b - b^{0.525} \leq p \leq b$. Hence, we can take this p and construct the Cayley graph $\Gamma(G, T')$ such that $|T'| = d$ and

$$\begin{aligned} |G| = 3^k p^{k-1}(p-1) &\geq 3^k (b - b^{0.525})^{k-1}(b - b^{0.525} - 1) \\ &> 3^k b^k + O(b^{k-0.475}) \\ &> 3^k \left(\frac{d}{3k-1} + \frac{k+1}{3k-1}\right)^k \\ &\quad + O\left(\left(\frac{d}{3k-1} + \frac{k+1}{3k-1}\right)^{k-0.475}\right) \\ &> \left(\frac{3}{3k-1}\right)^k d^k + O(d^{k-0.475}). \end{aligned}$$

□

Acknowledgements The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper.

References

1. Abas, M.: Cayley graphs of diameter two and any degree with order half of the Moore bound. Discrete Appl. Math. **173**, 1–7 (2014)
2. Abas, M.: Cayley graphs of diameter two with order greater than 0.684 of the Moore bound for any degree. European J. Combin. **57**, 109–120 (2016)
3. Baker, R .C., Harman, G., Pintz, J.: The difference between consecutive primes. II. Proc. London Math. Soc. (3) **83**(3), 532–562 (2001)
4. Brown, W.G.: On graphs that do not contain a Thomsen graph. Can. Math. Bull. **9**, 281–285 (1966)
5. Damerell, R.M.: On Moore graphs. Proc. Cambridge Philos. Soc. **74**, 227–236 (1973)
6. Dougherty, R., Faber, V.: The degree–diameter problem for several varieties of Cayley graphs. I. The Abelian case. SIAM J. Discrete Math. **17**(3), 478–519 (2004)
7. Erdős, P., Fajtlowicz, S., Hoffman, A.J.: Maximum degree in graphs of diameter 2. Networks **10**(1), 87–90 (1980)

8. Hoffman, A.J., Singleton, R.R.: On Moore graphs with diameters 2 and 3. IBM J. Res. Dev. **4**, 497–504 (1960)
9. Macbeth, H., Šiagiová, J., Širáň, J.: Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups. Discrete Math. **312**(1), 94–99 (2012)
10. McKay, B.D., Miller, M., Širáň, J.: A note on large graphs of diameter two and given maximum degree. J. Combin. Theory Ser. B **74**(1), 110–118 (1998)
11. Miller, M., Širáň, J.: Moore graps and beyond: A survey of the degree/diameter problem. Electron. J. Combin. **1000**, 14 (2013)
12. Pott, A., Zhou, Y.: Cayley graphs of diameter two from difference sets. J. Graph Theory **85**(2), 533–544 (2017)
13. Šiagiová, J., Širáň, J.: A note on large Cayley graphs of diameter two and given degree. Discrete Math. **305**(1–3), 379–382 (2005)
14. Šiagiová, J., Širáň, J.: Approaching the Moore bound for diameter two by Cayley graphs. J. Combin. Theory Ser. B **102**(2), 470–473 (2012)
15. Širáň, J., Šiagiová, J., Zdimalova, M.: Large graphs of diameter two and given degree. In: Proceedings of the 3rd International Workshop on Optimal Network Topologies (IWONT), pp. 347–359. Universitat Politecnica de Catalunya (2010)
16. Stanton, R.G., Cowan, D.D.: Note on a square functional equation. SIAM Rev. **12**, 277–279 (1970)
17. Vetrík, T.: Abelian Cayley graphs of given degree and diameter 2 and 3. Graphs Combin. **30**(6), 1587–1591 (2014)