Journal of Algebraic Combinatorics
https://doi.org/10.1007/s10801-022-01190-7

# Algebraic degree of Cayley graphs over abelian groups and dihedral groups

**Lu Lu[1] · Katja Mönius[2]**

Received: 12 August 2022 / Accepted: 7 November 2022


**Abstract**
For a graph $\Gamma$, let $K$ be the smallest field containing all eigenvalues of the adjacency matrix of $\Gamma$. The algebraic degree $\deg(\Gamma)$ is the extension degree $[K : \mathbb{Q}]$. In this paper, we completely determine the algebraic degrees of Cayley graphs over abelian groups and dihedral groups.

**Keywords** Cayley graph · Integral graph · Algebraic degree

**Mathematics Subject Classification** 05C50

## 1 Introduction

The *algebraic degree* of a graph was defined in [10] in order to generalize the concept of integral graphs. The *spectrum* of a graph $\Gamma$ is defined as the multiset of eigenvalues of the adjacency matrix of $\Gamma$. In particular, those eigenvalues are the roots of the monic characteristic polynomial of the adjacency matrix associated with $\Gamma$. Therefore, every eigenvalue of $\Gamma$ is an algebraic integer in some algebraic extension $K$ of the rationals, where $K$ is called the *splitting field* of $\Gamma$. The *algebraic degree* $\deg(\Gamma)$ is defined as the degree $[K : \mathbb{Q}]$. In particular, $\Gamma$ is called *integral* if $\deg(\Gamma) = 1$.

The *Cayley graph* $\mathrm{Cay}(G, S)$ is defined as the graph with vertex set $G$, where $G$ denotes a finite group and $S \subseteq G$, and edges from $g \in G$ to $h \in G$ whenever $gh^{-1} \in S$. Note that $\mathrm{Cay}(G, S)$ is an undirected graph if and only if $S = S^{-1}$, and has loops if and only if $e \in S$. If $S \neq S^{-1}$, then $\mathrm{Cay}(G, S)$ is also called *Cayley digraph*.

✉ Katja Mönius
katja.moenius@mathematik.uni-wuerzburg.de

Lu Lu
lulumath@csu.edu.cn

[1] School of Mathematics and Statistics, Central South University, Changsha 410083, Hunan, China

[2] Institute of Mathematics, Würzburg University, Emil-Fischer-Str. 40, 97074 Würzburg, Germany

Published online: 18 November 2022

In [8] and [9], Mönius precisely determined the algebraic degree of circulant digraphs, i.e. Cayley digraphs over cyclic groups. Moreover, integral Cayley graphs were studied intensively by several authors, e.g. Lu [7], Klotz and Sander [5, 6] and Ahmady et al. [1].

In this paper, we completely determine the splitting fields of Cayley graphs over abelian and dihedral groups. In particular, we precisely compute the algebraic degree of Cayley graphs and digraphs over abelian groups. We also give an upper bound for the algebraic degree of Cayley graphs and digraphs over dihedral groups, as well as a lower bound for the algebraic degree of Cayley graphs over dihedral groups.

## 2 Cayley graphs and digraphs over abelian groups

Let $G$ be an abelian group of order $n$ and let $S \subseteq G$ be a subset of $G$. Denote by $\Gamma = \mathrm{Cay}(G, S)$ the respective Cayley (di)graph, and let $K$ be the splitting field of $\Gamma$, i.e. the minimum field containing all eigenvalues of $\Gamma$. Without loss of generality, assume that $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$, where $n = n_1 n_2 \cdots n_r$. Therefore, each element $g \in G$ can be expressed as $g = (g_1, g_2, \ldots, g_r)$. For a positive integer $m$, denote by $\zeta_m = e^{2\pi \mathbf{i}/m}$ the primitive $m$-th root of unity, where $\mathbf{i} = \sqrt{-1}$. The eigenvalues of $\Gamma$ were obtained by Babai [3]:

**Lemma 1** ([3]) *The eigenvalues $\lambda_g$ of $\Gamma$ are given by $\lambda_g = \sum_{s \in S} \prod_{i=1}^{r} \zeta_{n_i}^{g_i s_i}$, for $g \in G$.*

It is clear that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^*$. Let $\eta$: $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}_n^*$ be the isomorphism defined by $\eta(\sigma) = k$ for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, where $k \in \mathbb{Z}_n^*$ is the integer such that $\sigma(\zeta_n) = \zeta_n^k$. Let $\mathbb{Z}_n^*$ act on $G$ by $ag = a(g_1, g_2, \ldots, g_r) = (ag_1, ag_2, \ldots, ag_r)$ for any $a \in \mathbb{Z}_n^*$ and $g \in G$. This leads to $\sigma(\zeta_{n_i}^k) = \sigma(\zeta_n^{kn/n_i}) = \zeta_n^{\eta(\sigma)kn/n_i} = \zeta_{n_i}^{\eta(\sigma)k}$. Therefore, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $g \in G$, we have

$$\sigma(\lambda_g) = \sigma\left(\sum_{s \in S} \prod_{i=1}^{r} \zeta_{n_i}^{g_i s_i}\right) = \sum_{s \in S} \prod_{i=1}^{r} \sigma(\zeta_{n_i}^{g_i s_i}) = \sum_{s \in S} \prod_{i=1}^{r} \zeta_{n_i}^{\eta(\sigma) g_i s_i}. \tag{1}$$

Let $S = \{(s_1, \ldots, s_r) \mid s_i \in \mathbb{Z}_{n_i}\}$. We say that a subgroup $H \subseteq \mathbb{Z}_n^*$ is fixing $S$ if and only if $hS = \{(hs_1 \bmod n_1, \ldots, hs_r \bmod n_r) \mid s_i \in \mathbb{Z}_{n_i}\} = S$ for all $h \in H$.

Subsequently, let $H = \eta(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K))$. According to (1), Li [4] showed the following result:

**Lemma 2** ([4]) *For all $g \in G$, the eigenvalue $\lambda_g$ is contained in $K$ if and only if $S$ is a union of some orbits $Hx$ for $x \in G$.*

Note that $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : K][K : \mathbb{Q}]$. From Lemma 2, we immediately get the following result:

**Theorem 1** *Let $\mathcal{H} = \{h \in \mathbb{Z}_n^* \mid hS = S\}$ be the largest subgroup of $\mathbb{Z}_n^*$ fixing S. Then, the splitting field of $\Gamma$ is given by*

$$K = \mathbb{Q}(\zeta_n)^{\eta^{-1}(\mathcal{H})} = \{x \in \mathbb{Q}(\zeta_n) \mid \sigma x = x, \forall \sigma \in \eta^{-1}(\mathcal{H})\}.$$

*Therefore, $\mathcal{H} = H$ and the algebraic degree of $\Gamma$ is*

$$\deg(\Gamma) = \frac{\varphi(n)}{|H|}.$$

***Proof*** Since $\mathcal{H}$ is a subgroup fixing $S$, we see that $S$ is a union of some orbits and, therefore, by Lemma 2, all eigenvalues of $\Gamma$ belong to $\mathbb{Q}(\zeta_n)^{\eta^{-1}(\mathcal{H})}$. Now, let $L$ be a field containing all eigenvalues of $\Gamma$, then, again by Lemma 2, $S$ is a union of some orbits $\eta(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)x$ for $x \in G$. This means that $\eta(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$ fixes $S$. Since $\mathcal{H}$ is the largest subgroup of $\mathbb{Z}_n^*$ fixing $S$, we have that $\eta(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L) \leq \mathcal{H}$ and, thus, $\mathbb{Q}(\zeta_n)^{\eta^{-1}(\mathcal{H})} \subseteq L$. Therefore, $\mathbb{Q}(\zeta_n)^{\eta^{-1}(\mathcal{H})}$ must be the smallest field containing all eigenvalues of $\Gamma$, i.e. $K = \mathbb{Q}(\zeta_n)^{\eta^{-1}(\mathcal{H})}$ and $\mathcal{H} = H$. □

***Example 1*** (Integral Cayley graph over abelian group) Let $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ and $S = \{(0, 1), (1, 0), (0, -1)\}$. Note that $\mathbb{Z}_8^* = \{1, 3, -3, -1\}$, and

$$3S = -3S = \{(0, -1), (1, 0), (0, 1)\} = S = -S.$$

Therefore, $H = \mathbb{Z}_8^*$ and $\deg(\Gamma) = 1$, i.e., $\Gamma$ is integral. In fact, the spectrum of $\Gamma$ is $\left\{\pm 3, [\pm 1]^3\right\}$.

***Example 2*** (Cayley graph over abelian group of algebraic degree 2) Let $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ and $S = \{(1, 1), (-1, -1), (0, 1), (0, -1)\}$. Note that $\mathbb{Z}_{24}^* = \{1, 5, 7, 11, -11, -7, -5, -1\}$, and

$$\begin{cases} 5S = -5S = 7S = -7S = \{(1, -1), (-1, 1), (0, -1), (0, 1)\} \neq S, \\ 11S = -11S = \{(-1, -1), (1, 1), (0, 1), (0, -1)\} = S = -S. \end{cases}$$

Therefore, $H = \{1, 11, -11, -1\}$ and $\deg(\Gamma) = 2$. In fact, the spectrum of $\Gamma$ is

$$\left\{\pm 4, [\pm 2]^4, [\pm 1 \pm \sqrt{3}]^2, [0]^6\right\}.$$

***Example 3*** (Cayley digraph over abelian group of algebraic degree 4) Let $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ and $S = \{(1, 1), (0, 1), (0, -1)\}$. We observe that

$$\begin{cases} -7S = 5S = \{(1, -1), (0, -1), (0, 1)\} \neq S, \\ 7S = -5S = \{(-1, 1), (0, 1), (0, -1)\} \neq S, \\ 11S = \{(-1, -1), (0, -1), (0, 1)\} \neq S, \\ -11S = \{(1, 1), (0, 1), (0, -1)\} = S. \end{cases}$$

Thus, $H = \{1, -1\}$ and $\deg(\Gamma) = 4$.

In [9], Mönius solved the Inverse Galois problem for circulant graphs showing that every finite abelian extension of the rationals is the splitting field of some circulant graph. A similar result can be obtained for (non-circulant) Cayley graphs over abelian groups: Let $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ be a non-cyclic abelian group, i.e. $n = n_1 n_2 \cdots n_r$ where each $n_i$ is a prime power. For any subgroup $H$ of $\mathbb{Z}_n^*$, let

$$S = (H \bmod n_1) \times (H \bmod n_2) \times \cdots \times (H \bmod n_r)$$

for $(H \bmod n_i) = \{h \bmod n_i \mid h \in H\}, i = 1, \ldots, r$. Then, $H$ is the largest subgroup of $\mathbb{Z}_n^*$ fixing $S$ and, therefore, the splitting field of $\Gamma = \mathrm{Cay}(G, S)$ equals $K = \mathbb{Q}(\zeta_n)^{\eta^{-1}(H)}$. Together with the well-known Kronecker–Weber theorem, we get the following result.

**Corollary 1** (Inverse Galois problem for Cayley graphs over abelian groups) *Every finite abelian extension $K$ of the rationals (of order $n$) is the splitting field of some Cayley graph over an abelian group. In particular, if $n$ has at least one prime divisor of order $\geq 2$, then there is a non-circulant Cayley graph over an abelian group with splitting field $K$.*

## 3 Cayley graphs over dihedral groups

In this section, we restrict our considerations to Cayley graphs over dihedral groups, i.e. we always assume that $G = D_n = C_n \rtimes C_2 = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$ and $S \subset G$ is a subset with $e \notin S$ and $S = S^{-1}$. Let $S = S_1 \cup S_2$, where $S_1 \subseteq \langle a \rangle$ and $S_2 \subseteq b\langle a \rangle$, and $I_1 = \{i \in \mathbb{Z}_n \mid a^i \in S_1\}$. It is clear that $I_1 = -I_1$ since $S = S^{-1}$. Moreover, let $\Gamma = \mathrm{Cay}(G, S)$ denote the respective Cayley graph and let $K$ be the minimum field containing all eigenvalues of $\Gamma$. Let $\chi_l$ be the irreducible characters of $D_n$ of degree 2 for $1 \leq l \leq \lfloor \frac{n-1}{2} \rfloor$, where $\chi_l(a^k) = 2\cos\frac{2\pi lk}{n}$ and $\chi_l(ba^k) = 0$. For a subset $A \subseteq G$, let $\chi_l(A) = \sum_{x \in A} \chi_l(x)$ and $\chi_l(A^2) = \sum_{x,y \in A} \chi_l(xy)$. The eigenvalues of $\Gamma$ were obtained by Babai [3] and were restated by Lu [7].

**Lemma 3** ([3, 7]) *The eigenvalues of $\Gamma$ consist of some integers and the roots of*

$$f_l(x) = x^2 - \chi_l(S_1)x + \frac{1}{2}\left(\chi_l(S_1)^2 - \left(\chi_l(S_1^2) + \chi_l(S_2^2)\right)\right),$$

*for $1 \leq l \leq \lfloor \frac{n-1}{2} \rfloor$. In particular, all possibly non-integral eigenvalues are contained in the set*

$$\left\{ \frac{b_l \pm \sqrt{c_l}}{2} \mid 1 \leq l \leq \lfloor (n-1)/2 \rfloor \right\},$$

*where $b_l = \chi_l(S_1)$ and $c_l = 2(\chi_l(S_1^2) + \chi_l(S_2^2)) - (\chi_l(S_1))^2$.*

Since $I_1 = -I_1$, it is clear that

$$b_l = \chi_l(S_1) = \sum_{a^s \in S_1} 2\cos\frac{2\pi ls}{n} = 2\sum_{i \in I_1} \zeta_n^{li}$$

and $b_l, c_l \in \mathbb{Q}(\zeta_n)$. Let $K_0$ be a field such that $\mathbb{Q} \subseteq K_0 \subseteq \mathbb{Q}(\zeta_n)$. Therefore, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K_0)) \leq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^*$. Recall that $\eta$ is the isomorphism from $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ to $\mathbb{Z}_n^*$ such that $\sigma(\zeta_n) = \zeta_n^{\eta(\sigma)}$. In what follows, we always assume that $H = \eta(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K_0))$. We first get the following result:

**Lemma 4** *If $b_1, c_1 \in K_0$, then $b_l, c_l \in K_0$ for $1 \leq l \leq \lfloor \frac{n-1}{2} \rfloor$.*

***Proof*** For $1 \leq l \leq \lfloor \frac{n-1}{2} \rfloor$, let $\sigma_l \colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ be defined by $\sigma_l(\zeta_n) = \zeta_n^l$. It is clear that $\sigma_l$ is a homomorphism and $b_l = \sigma_l(b_1)$. Thus, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K_0)$, we have

$$\sigma(b_l) = \sigma(\sigma_l(b_1)) = \sigma\left(\sigma_l\left(2\sum_{i\in I_1}\zeta_n^i\right)\right) = 2\sum_{i\in I_1}\zeta_n^{\eta(\sigma)li} = \sigma_l(\sigma(b_1)) = \sigma_l(b_1) = b_l.$$

This leads to $b_l \in K_0$. Analogously, we also get $c_l \in K_0$. □

For a subset $A \subseteq \{1, \ldots, n\}$, denote by $\delta_A$ the *characteristic vector* of $A$, that is $\delta_A \in \mathbb{Q}^n$ with $\delta_A(i) = 1$ if $i \in A$ and 0 otherwise.

**Lemma 5** *The number $b_1$ is an element of $K_0$ if and only if $I_1$ is a union of some orbits $Hk$ for $k \in \mathbb{Z}_n$.*

***Proof*** To show the sufficiency, we only need to consider the case where $I_1$ is exactly one orbit. Suppose that $I_1 = Hk$. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K_0)$, we have

$$\begin{aligned}\sigma(b_1) &= \sigma\left(2\textstyle\sum_{i\in I_1}\zeta_n^i\right) = \sigma\left(2\sum_{hk\in Hk}\zeta_n^{hk}\right)\\ &= 2\textstyle\sum_{hk\in Hk}\sigma(\zeta_n^{hk}) = 2\sum_{hk\in Hk}\zeta_n^{\eta(\sigma)hk}\\ &= 2\textstyle\sum_{h'k\in\eta(\sigma)Hk}\zeta_n^{h'k} = 2\sum_{h'k\in Hk}\zeta_n^{h'k}\\ &= 2\textstyle\sum_{i\in I_1}\zeta_n^i = b_1.\end{aligned}$$

This leads to $b_1 \in K_0$.

Conversely, assume that $A_1, A_2, \ldots, A_r$ have the form $A_i = Hk_i$ for some $k_i \in \mathbb{Z}_n$. Let $M$ be the $n \times n$ square matrix indexed by $\mathbb{Z}_n$ with $(i, j)$-entry being $\zeta_n^{ij}$. It is clear that $M$ is non-singular. Let $V, W$ be vector spaces over $K_0$ defined by $V = \{v \in K_0^n \mid Mv \in K_0^n\}$ and $W = \langle \delta_{A_1}, \ldots, \delta_{A_r} \rangle$, where $\langle \delta_{A_1}, \ldots, \delta_{A_r} \rangle$ denotes the span of the characteristic vectors $\delta_{A_1}, \ldots, \delta_{A_r}$ with $\delta_{A_i} \in K_0^n$. On the one hand, for any $v \in W$, we get $Mv \in K_0^n$ by the same arguments as above, which leads to $W \subseteq V$. On the other hand, if $s, t \in A_i = Hk_i$, then there exists $h \in H$ such that $t = hs$. Let $\sigma = \eta^{-1}(h)$, i.e. $\sigma(\zeta_n) = \zeta_n^h$, and $v \in V$. Since $\sigma \in K_0^{\eta^{-1}(H)}$, we have that $\sigma((Mv)_s) = (Mv)_s$ where $(Mv)_s$ denotes the $s$-th entry of the vector $Mv$. Moreover, we get

$$(Mv)_s = \sigma((Mv)_s) = \sigma\left(\sum_{x=0}^{n-1}\zeta_n^{sx}v(x)\right) = \sum_{x=0}^{n-1}\zeta_n^{hsx}v(x) = \sum_{x=0}^{n-1}\zeta_n^{tx}v(x) = (Mv)_t.$$

Thus, for all $v \in V$ we have $(Mv)_s = (Mv)_t$ whenever $s, t \in A_i$. Therefore, $Mv$ is a linear combination of $\delta_{A_1}, \ldots, \delta_{A_r}$, i.e. $Mv \in W$. Hence, $MV \subseteq W$ and, thus, $\dim V \leq \dim W$. Since $W \subseteq V$, we get $V = W$. Moreover, since $b_1 = 2(M\delta_{I_1})_1 \in K_0$, by Lemma 4, we have $b_l = 2(M\delta_{I_1})_l \in K_0$. Therefore, $M\delta_{I_1} \in K_0^n$ and, thus, $\delta_{I_1} \in V$ by definition of $V$. Since $V = W$, it follows that $I_1$ is the union of some orbits. □

**Lemma 6** *For $1 \leq l \leq \lfloor \frac{n-1}{2} \rfloor$, the number $c_l$ is equal to $2\chi_l(S_2^2)$.*

***Proof*** Since $I_1 = -I_1$, we have $b_l = \chi_l(S_1) = 2\sum_{i\in I_1} \zeta_n^{li}$. By simple calculations, we get

$$\begin{aligned}
2\chi_l(S_1^2) &= 2\sum_{a^i, a^j \in S_1} \chi_l(a^i a^j) = 2\sum_{i,j\in I_1} 2\cos\left(\tfrac{2\pi l(i+j)}{n}\right) \\
&= 2\sum_{i,j\in I_1} (\zeta_n^{l(i+j)} + \zeta_n^{-l(i+j)}) = 2\sum_{i\in I_1} \zeta_n^{li} \sum_{j\in I_1} \zeta_n^{lj} \\
&\quad +2\sum_{i\in I_1} \zeta_n^{-li} \sum_{j\in I_1} \zeta_n^{-lj} \\
&= \sum_{i\in I_1} \zeta_n^{li} b_l + \sum_{i\in I_1} \zeta_n^{-li} b_l = b_l(2\sum_{i\in I_1} \zeta_n^{i}) = b_l^2.
\end{aligned}$$

Therefore,

$$c_l = 2(\chi_l(S_1^2) + \chi_l(S_2^2)) - (\chi_l(S_1))^2 = 2\chi_l(S_2^2). \qquad \square$$

A multiset $X$ is a collection of elements where an element may appear more than once. For $x \in X$, denote by $m_X(x)$ the multiplicity of $x$ in $X$. To avoid confusion, we use $[\cdot]$ to denote a multiset. For example, $X = [1, 1, 2, 3, 3]$ is a multiset and $m_X(1) = 2$. Given two multisets $X, Y$, their multiple $XY$ is a multiset, that is, $XY = [xy \mid x \in X, y \in Y]$, where $xy$ may occur more than once. The multi-union $X \sqcup Y$ is the multiset with $m_{X\sqcup Y}(z) = m_X(z) + m_Y(z)$ for any element $z$. For example, consider the two multisets of integers $X = [1, 1, -1]$, $Y = [1, 2]$, then $XY = [1, 2, 1, 2, -1, -2]$ and $X \sqcup Y = [1, 1, 1, -1, 2]$. Denote by $I_2 = [k \mid a^k \in S_2^2]$ the multiset of all indices $k$ such that $a^k \in S_2^2$. By Lemma 6, we get the following result. Since the proof is very similar to the one of Lemma 5, we omit it.

**Lemma 7** *The number $c_1$ is contained in $K_0$ if and only if $I_2$ is a multi-union of some orbits $Hk$ for $k \in \mathbb{Z}_n$.*

Combining Lemma 5 and Lemma 7, we get the following result. The proof is very similar to the one of Theorem 1 and, therefore, we omit it, too.

**Theorem 2** *Let $H = \{h \in \mathbb{Z}_n^* \mid hI_1 = I_1, hI_2 = I_2\}$ be the subgroup fixing both, $I_1$ and $I_2$. Then, $K = K_0(\sqrt{c_1}, \ldots, \sqrt{c_l})$, where $K_0 = \mathbb{Q}(\zeta_n)^{\eta^{-1}(H)} = \{x \in \mathbb{Q}(\zeta_n) \mid \sigma x = x, \forall \sigma \in \eta^{-1}(H)\}$.*

Assume that $\{k_1, \ldots, k_r\}$ is a maximum subset of $\mathbb{Z}_n$ such that all the orbits $Hk_1, Hk_2, \ldots, Hk_r$ are distinct. The set $R(H) = \{k_1, \ldots, k_r\}$ is called a *representative* of $H$. Suppose that $I_2 = m_1 \circ Hk_1 \sqcup m_2 \circ Hk_2 \sqcup \cdots \sqcup m_r \circ Hk_r$, where

$m_i \circ Hk_i$ indicates that the orbit $Hk_i$ appears $m_i$ times. By simple calculations, we immediately get

$$\chi_l(S_2^2) = 2\sum_{i=1}^{r} m_i \sum_{hk_i \in Hk_i} \zeta_n^{lhk_i}.$$

Note that, if $s, t \in Hk$, then there exists $h_0 \in H$ such that $h_0 s = t$. Let $\sigma = \eta^{-1}(h_0)$. We have

$$\sigma(\chi_s(S_2^2)) = \sigma\left(2\sum_{i=1}^{r} m_i \sum_{hk_i \in Hk_i} \zeta_n^{shk_i}\right) = 2\sum_{i=1}^{r} m_i \sum_{hk_i \in Hk_i} \zeta_n^{h_0 shk_i}$$
$$= 2\sum_{i=1}^{r} m_i \sum_{hk_i \in Hk_i} \zeta_n^{thk_i} = \chi_t(S_2^2).$$

Since $\chi_s(S_2^2) \in K_0$, we have $\chi_s(S_2^2) = \chi_t(S_2^2)$. Let $\mathcal{N} = \{k_i \mid \{1, 2, \ldots, \lfloor (n-1)/2 \rfloor\} \cap Hk_i \neq \emptyset\}$. Therefore, all possible values of $c_l$ are

$$c_{k_i} = 4\sum_{j=1}^{r} m_j \sum_{hk_j \in Hk_j} \zeta_n^{k_i hk_j},$$

for $k_i \in \mathcal{N}$. The following result is obtained:

**Corollary 2** *The algebraic degree of* $\Gamma$ *is bounded by*

$$\frac{\varphi(n)}{|H|} \leq \deg(\Gamma) \leq \frac{\varphi(n)}{|H|} 2^{|\mathcal{N}|}.$$

***Example 4*** (Cayley graph over dihedral group of algebraic degree 2) Let $G = D_8$ and $S = \{a, a^7, b\}$. Then, $I_1 = \{1, -1\}$ and $I_2 = [0]$. Therefore, $H = \{1, -1\} \leq \mathbb{Z}_8^*$, the representative is $R(H) = \{0, 1, 2, 3, 4\}$ and $\mathcal{N} = \{1, 2, 3\}$. By simple calculations, we have $c_1 = c_2 = c_3 = 4$. Thus, $K = \mathbb{Q}(\zeta_8)^{\eta^{-1}(H)} = \mathbb{Q}(\sqrt{2})$ and $\deg(\Gamma) = 2 = \frac{\varphi(8)}{|H|}$.

***Example 5*** (Cayley graph over dihedral group of algebraic degree 4) Let $G = D_{12}$ and $S = \{a, a^{-1}, a^5, a^{-5}, b, ba, ba^5\}$. Then, $I_1 = \{1, -1, 5, -5\}$ and $I_2 = [0, 0, 0, 1, 4, 5, -1, -4, -5]$. Therefore, $H = \mathbb{Z}_{12}^*$, $R(H) = \{0, 1, 2, 3, 4, 6\}$ and $\mathcal{N} = \{1, 2, 3, 4\}$. By simple calculations, we get $c_1 = 8$, $c_2 = 16$, $c_3 = 20$ and $c_4 = 0$. Thus, $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ and $\deg(\Gamma) = 4$.

Though the field $K_0 = \mathbb{Q}^{\eta^{-1}(H)}$ is very clear, it is not easy to determine $K$. From the examples above, $K$ completely relies on the values $c_k$ for $k \in \mathcal{N}$. However, it seems that such values could not be described clearly since $H$ is just a subgroup of $\mathbb{Z}_n^*$. In what follows, we therefore consider a special case of $H$.

If $H = \mathbb{Z}_n^*$, then $K_0 = \mathbb{Q}$. Moreover, $R(H)\backslash\{0\}$ consists of all divisors of $n$ and, hence, $\mathcal{N} = \{1 \leq k \leq \lfloor (n-1)/2 \rfloor \mid k \mid n\}$. Furthermore, for each $d \mid n$, we have $Hd = \mathbb{Z}_{n/d}^* d$. Therefore, for any $k \in \mathcal{N}$, we have

$$c_k = 4\sum_{d|n} m_d \sum_{t\in\mathbb{Z}_{n/d}} \zeta_n^{ktd} = 4\sum_{d|n} m_d \sum_{t\in\mathbb{Z}_{n/d}} \zeta_{n/d}^{kt} = 4\sum_{d|n} m_d r_{n/d}(k),$$

where $r_q(m) = \sum_{1\leq j\leq q, gcd(j,q)=1} \zeta_q^{mj}$ is the famous Ramanujan sum. Note that

$$r_q(m) = \frac{\varphi(q)}{\varphi\left(\frac{q}{gcd(m,q)}\right)}\mu\left(\frac{q}{gcd(m,q)}\right),$$

where $\mu$ is the Möbius function. Thus, we have

$$c_k = 4\sum_{d|n} m_d \frac{\varphi(n/d)}{\varphi\left(\frac{n/d}{gcd(k,n/d)}\right)}\mu\left(\frac{n/d}{gcd(k,n/d)}\right)$$

and, in particular, $c_1 = 4\sum_{d|n} m_d \mu(n/d)$.

***Example 6*** (Integral Cayley graph over dihedral group) Let $G = D_8$ and $S = \{a, a^3, a^5, a^7, b, ba^4\}$. Then, $I_1 = \{1, 3, 5, 7\}$ and $I_2 = [0, 0, 4, -4]$. This leads to $H = \mathbb{Z}_8^*$ and $R(H) = \{0, 1, 2, 4\}$. Therefore, $\mathcal{N} = \{1, 2\}$. Since $I_2 = 2 \circ H8 \sqcup 2 \circ H4$, we get

$$c_1 = 4(2\mu(1) + 2\mu(2)) = 0, c_2 = 4(2\mu(1) + 2\frac{\varphi(2)}{\varphi(1)}\mu(1)) = 16.$$

Thus, $K = \mathbb{Q}$ and $\deg(\Gamma) = 1$.

## 4 An upper bound for the algebraic degree of Cayley digraphs over dihedral groups

So far, we restricted our considerations to undirected Cayley graphs. If we omit the restrictions on $S$, then $I_1 = -I_1$ does not hold anymore in general. This makes the computation of the $c_l$'s and the field $K_0$ much more difficult. At least we could find an upper bound for the algebraic degree of Cayley digraphs over dihedral groups:

**Theorem 3** *Let $\Gamma$ denote a Cayley digraph over the dihedral group $D_n$, then*

$$\deg(\Gamma) \leq \frac{\varphi(n)}{|H|}2^{|\mathcal{N}|}.$$

***Proof*** Note that Lemma 3 still holds for digraphs. For $1 \leq l \leq \lfloor \frac{n-1}{2} \rfloor$, we now get $b_l = \chi_l(S_1) = \sum_{a^s\in S_1} 2\cos\frac{2\pi ls}{n} = \sum_{i\in I_1}(\zeta_n^{li} + \zeta_n^{-li}) = \sum_{i\in I_1\sqcup -I_1} \zeta_n^{li}$. Similar as in the proofs of Lemma 4 and Lemma 5, we can show that if $b_1, c_1 \in K_0$, then

$b_l, c_l \in K_0$, and that $b_1 \in K_0$ if and only if $I_1 \sqcup -I_1$ is a multi-union of some orbits $Hk$ for $k \in \mathbb{Z}_n$.

Again, let $I_2 = \{k \mid a^k \in S_2^2\}$. Note that $I_2 = -I_2$. With similar, but a bit more cumbersome computations as above, we now get

$$c_l = 2\chi_l(S_2^2) + b_l^2 - 4\sum_{i\in I_1}\zeta_n^{li}\sum_{j\in I_1}\zeta_n^{-lj}.$$

It is clear that with $I_1$ being a union of orbits $Hk$, so are $-I_1$ and $I_1 \sqcup -I_1$. Therefore, if $I_1$ is a union of orbits and $I_2$ is a multi-union of orbits, then $b_l, c_l \in K_0$ for all $l$. Thus, if $H$ denotes the subgroup fixing both, $I_1$ and $I_2$, then the splitting field $K$ of $\Gamma$ must be contained in the field $K_0(\sqrt{c_1}, \ldots, \sqrt{c_l})$ where $K_0 = \mathbb{Q}(\zeta_n)^{\eta^{-1}(H)}$. Hence, the statement follows. □

**Acknowledgements** This work is supported by NSFC (No. 12001544) and Natural Science Foundation of Hunan Province (Grant No. 2021JJ40707).

**Funding** Open Access funding enabled and organized by Projekt DEAL.

**Data availability** Data sharing is not applicable to this article as no new data were created or analyzed in this study.



## References

1. Ahmady, A., Bell, J., Mohar, B.: Integral Cayley graphs and groups. SIAM J. Discrete Math. **28**, 685–701 (2014)
2. Alprin, R.C., Peterson, B.L.: Integral sets and Cayley graphs of finite groups. Electron. J. Comb. **19**, P44 (2012)
3. Babai, L.: Spectra of Cayley graphs. J. Combin. Theory Ser. B **27**(2), 180–189 (1979)
4. Li, F.: A method to determine algebraically integral Cayley digraphs on finite abelian group. Contr. Discrete Math. **2**(15), 148–152 (2020)
5. Klotz, W., Sander, T.: Integral Cayley graphs defined by greatest common divisors. Electron. J. Comb. **18**, P94 (2011)
6. Klotz, W., Sander, T.: Integral Cayley graphs over abelian groups. Electron. J. Comb. **17**, R81 (2010)
7. Lu, L.: Integral Cayley graphs over dihedral groups. J. Algebr. Comb. **4**(47), 585–601 (2018)
8. Mönius, K.: The algebraic degree of spectra of circulant graphs. J. Number Theory **208**, 295–304 (2020)
9. Mönius, K.: Splitting fields of spectra of circulant graphs. J. Algebra **594**, 154–169 (2022)
10. Mönius, K., Steuding, J., Stumpf, P.: Which graphs have non-integral spectra? Graphs Comb. **34**(6), 1507–1518 (2018)