Chin. Ann. Math. Ser. B
42(5), 2021, 791–800
DOI: 10.1007/s11401-021-0291-4

Chinese Annals of Mathematics, Series B

LCD Codes and Self-orthogonal Codes in Finite Dihedral Group Algebras*

Yanyan GAO[1] Qin YUE[2] Yansheng WU[3]

Abstract Let $\mathbb{F}_q$ be a finite field with order q and D_{2n} be the dihedral group with $2n$ elements, and $\gcd(q, 2n) = 1$. In this article, the authors give precise descriptions and enumerations of linear complementary dual (LCD) codes and self-orthogonal codes in the finite dihedral group algebras $\mathbb{F}_q[D_{2n}]$. Some numerical examples are also presented to illustrate the main results.

Keywords Group algebra, Dihedral group, LCD codes, Self-orthogonal codes
2000 MR Subject Classification 11T71, 11T30

1 Introduction

Group algebra is one of the important sources of constructing linear codes. We call $\mathcal{C}$ a group code if $\mathcal{C}$ is just a right ideal in a group ring $R[G]$, where R is a commutative ring and G is a finite group. In particular, if G is abelian, then $\mathcal{C}$ is an abelian code. A brief survey on group codes of some recent results is provided as follows.

(1) Ferraz et al. [10] determined the number of simple components of a semisimple finite abelian group algebra, in term of the number of q-cyclotomic classes.

(2) Brochero Martínez et al. [3] determined an explicit expression for the primitive idempotents of $\mathbb{F}_q[G]$, where $\mathbb{F}_q$ is a finite field, G is a finite cyclic group of order p^k, and p is an odd prime with $\gcd(q, p) = 1$. Brochero Martínez [2] also showed explicitly all central irreducible idempotents and their Wedderburn decomposition of the dihedral group algebra $\mathbb{F}_q[D_{2n}]$ if every prime divisor of n divides $q - 1$.

(3) Polcino Milies et al. [17] calculated the minimum distances and the dimensions of all cyclic codes of length p^n over a finite field $\mathbb{F}_q$. If p is an odd prime, $\mathbb{F}_q$ is a finite field with

Manuscript received January 17, 2019. Revised March 2, 2021.
[1]Department of Mathematics and Physics, Nanjing Institute of Technology, Nanjing 211167, China; State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China. E-mail: gyy_318@163.com
[2]Corresponding author. Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China; State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China. E-mail: yueqin@nuaa.edu.cn
[3]School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China. E-mail: wysasd@163.com.
*This work was supported by the National Natural Science Foundation of China (Nos. 61772015, 11971321, 12101326), Foundation of Nanjing Institute of Technology (No. CKJB202007), the NUPTSF (No. NY220137), the Guangxi Natural Science Foundation (No. 2020GXNSFAA159053), the National Key Research and Development Program of China (No. 2018YFA0704703), Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-17-010), the Open Project of Shanghai Key Laboratory of Trustworthy Computing (No. OP202101).

q elements, and q generates the group of invertible elements of the residue ring module p^n, denoted by $\mathbb{Z}_{p^n}$.

(4) Jitman et al. [12] gave a characterization and an enumeration of Euclidean self-dual and Euclidean self-orthogonal abelian codes in principal ideal group algebras. Then Jitman et al. continued this work and studied the Hermitian self-dual abelian codes in a group ring $\mathbb{F}_{q^2}[G]$ in [13].

(5) Choosuwan et al. [6] gave the complete enumeration of self-dual abelian codes in non-principal ideal group algebras $\mathbb{F}_{2^k}[A\times\mathbb{Z}\times\mathbb{Z}_{2^s}]$ with respect to both the Euclidean and Hermitian inner products, where k and s are positive and A is an abelian group of odd order.

(6) In 2017, Boripan et al. [1] studied a family of abelian codes with complementary dual in a group algebra $\mathbb{F}_{p^v}[G]$ in the two cases of Euclidean and Hermitian inner products, where p is a prime, v is a positive integer, and G is an arbitrary finite abelian group.

(7) Cao et al. [7] proved that any left D_{2n}-code (left ideal of the group algebra $\mathbb{F}_q[D_{2n}]$ with $\gcd(q,2n)=1$) is a direct sum of concatenated codes with inner codes A_i and outer codes C_i, where A_i is a minimal self-reciprocal cyclic code over $\mathbb{F}_q$ of length n and C_i is a skew cyclic code of length 2 over an extension field or principal ideal ring of $\mathbb{F}_q$. Cao et al. also extended the results of [7] to the left dihedral codes over Galois rings $GR(p^2,n)$ in [8].

Linear complementary dual (LCD for short) codes are a class of linear codes introduced by Massey [14] in 1964. LCD codes have been extensively studied in literature recently. Carlet et al. [5] introduced a general construction of LCD codes from linear codes. Mesnager et al. [15] provided a construction scheme for obtaining LCD codes from any algebraic curve. Carlet et. al [4] investigated several constructions of new Euclidean and Hermitian LCD maximum distance separable (MDS for short) code using some linear codes with small dimension or codimension, self-orthogonal codes and generalized Reed-Solomon codes.

In this paper, we give precise descriptions and enumerations of LCD codes and self-orthogonal codes in the finite dihedral group algebras $\mathbb{F}_q[D_{2n}]$ if $\gcd(q,2n)=1$. Some numerical examples are also presented to illustrate our main results.

The present paper is organized as follows. In Section 2, we give a review of some properties of group algebras and some other preliminaries. In Section 3, we prove our main results. In Section 4, as examples, we count the numbers of all LCD and self-orthgonal codes for the following dihedral group algebras: (i) for $q=3$, $\mathbb{F}_3[D_{14}],\mathbb{F}_3[D_{16}],\mathbb{F}_3[D_{26}]$; (ii) for $q=5$, $\mathbb{F}_5[D_{16}],\mathbb{F}_5[D_{26}]$.

2 Preliminaries

2.1 Group algebras

Let $\mathbb{F}_q$ be a finite field and G a finite group. The group algebra $\mathbb{F}_q[G]$ is defined as the vector over $\mathbb{F}_q$ with basis G, and it has scalar, additive and multiplicative operators as follows: For $c,a_g,b_g\in\mathbb{F}_q$ and $g\in G$,

$$c\Big(\sum_{g\in G}a_g g\Big)=\sum_{g\in G}ca_g g,$$

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)g,$$
$$\Big(\sum_{g\in G} a_g g\Big)\Big(\sum_{h\in G} b_h h\Big) = \sum_{g\in G}\Big(\sum_{uv=g} a_u b_v\Big)g.$$

Then $\mathbb{F}_q[G]$ is an associative $\mathbb{F}_q$-algebra with the identity $1 = 1_{\mathbb{F}_q}1_G$, where $1_{\mathbb{F}_q}$ and 1_G are the identity elements of $\mathbb{F}_q$ and G, respectively. Readers are referred to [16, 18] for more details on group ring or group algebra.

Define the (standard) inner product on $\mathbb{F}_q[G]$ as follows: For $\alpha = \sum\limits_{g\in G} a_g g, \beta = \sum\limits_{g\in G} b_g g \in \mathbb{F}_q[G]$,

$$\langle \alpha, \beta\rangle = \sum_{g\in G} a_g b_g.$$

If $\mathcal{C}$ is a right ideal of $\mathbb{F}_q[G]$, then $\mathcal{C}$ is a linear code over $\mathbb{F}_q$. Hence the dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp} = \{\alpha \in \mathbb{F}_q[G] \mid \langle \alpha, \beta\rangle = 0 \text{ for every } \beta \in \mathcal{C}\}.$$

If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called a self-orthogonal code. If $\mathcal{C}\bigcap\mathcal{C}^{\perp} = 0$, then $\mathcal{C}$ is called a linear complementary dual code, or shortly an LCD code. One has the following simple fact: If $g, h \in G$, then

$$\langle g, h\rangle = \begin{cases} 1, & \text{if } g = h, \\ 0, & \text{otherwise.} \end{cases}$$

Suppose that $\alpha, \beta \in \mathbb{F}_q[G]$ and $g \in G$. Then

$$\langle \alpha g, \beta g\rangle = \langle \alpha, \beta\rangle,$$

which is called G-invariance. Suppose that $\alpha = \sum\limits_{g\in G} a_g g \in \mathbb{F}_q[G]$. Then $wt(\alpha) = |\{a_g \neq 0 | \, g \in G\}|$ is called the Hamming weight of α.

2.2 Some lemmas

Lemma 2.1 (see Maschke's Theorem [18]) *Let R be a ring and G be a group. Then the group ring $R[G]$ is semisimple if and only if the following conditions hold.*

(i) *R is a semisimple ring.*

(ii) *G is finite.*

(iii) *$|G|$ is invertible in R.*

By Lemma 2.1, it is easy to verify that $\mathbb{F}_q[G]$ is semisimple if and only if G is a finite group and $\mathrm{char}(\mathbb{F}_q) \nmid |G|$. By the Wedderburn-Artin theorem, $\mathbb{F}_q[G]$ is isomorphic to a direct sum of matrix algebras over division rings, such that each division algebra is a finite algebra over $\mathbb{F}_q$, i.e., there is an isomorphism of $\mathbb{F}_q$-algebra:

$$\rho : \mathbb{F}_q[G] \cong M_{l_1}(D_1) \bigoplus M_{l_2}(D_2) \bigoplus \cdots \bigoplus M_{l_t}(D_t),$$

where D_j are fields such that $|G| = \sum_{j=1}^{t} l_j^2[D_j : \mathbb{F}_q]$. Hence, every right ideal of $\mathbb{F}_q[G]$ is generated by an idempotent of $\mathbb{F}_q[G]$. Observe that $\mathbb{F}_q[G]$ has t central irreducible idempotents, each one of the form

$$e_i = \rho^{-1}(0, \cdots, 0, I_i, 0, \cdots, 0),$$

where I_i are the identity matrices of the component $M_{l_i}(D_i)$ for $1 \le i \le t$.

Let $\mathbb{F}_q$ be a finite field of order q and n be a positive integer with $\gcd(2n, q) = 1$. For any monic polynomial $g(x) \in \mathbb{F}_q[x]$ with $g(0) = a_0 \neq 0$, $g^*(x)$ denotes the reciprocal polynomial of $g(x)$, i.e., $g^*(x) = a_0^{-1}x^{\deg(g)}g(\frac{1}{x})$. We say that $g(x)$ is a self-reciprocal polynomial if $g(x) = g^*(x)$. Suppose that there is an irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$ as follows:

$$x^n - 1 = f_1(x)f_2(x)\cdots f_r(x)f_{r+1}(x)f_{r+1}^*(x)\cdots f_{r+s}(x)f_{r+s}^*(x),$$

where $f_i(x) = f_i^*(x), 1 \le i \le r$. For convenience, we set $f_1(x) = x - 1$ and $f_2(x) = x + 1$ if n is even; and $f_1(x) = x - 1$ if n is odd.

Let C_n be a cyclic group of order n. It is well known that $\mathbb{F}_q[C_n] \cong \mathbb{F}_q[x]/\langle x^n - 1\rangle$. By the Chinese remainder theorem,

$$\mathbb{F}_q[x]/\langle x^n - 1\rangle \cong \Big(\bigoplus_{j=1}^{r+s} \mathbb{F}_q[x]/\langle f_j(x)\rangle\Big) \oplus \Big(\bigoplus_{j=r+1}^{r+s} \mathbb{F}_q[x]/\langle f_j^*(x)\rangle\Big).$$

Lemma 2.2 (see [3]) *Let I be an ideal of $\mathbb{F}_q[C_n]$ generated by the monic polynomial $g(x)$, which is a divisor of $x^n - 1$. Set $f(x) = \frac{x^n-1}{g(x)}$. Then the principal idempotent of I is*

$$e_f = -\frac{((f^*(x))')^*}{n} \cdot \frac{x^n - 1}{f(x)}.$$

Lemma 2.3 (see [2]) *Let $\mathbb{F}_q$ be a finite field with order q and $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, yxy = x^{-1}\rangle$ be the dihedral group with $2n$ elements. Then the group algebra $\mathbb{F}_q[D_{2n}]$ has the Wedderburn decomposition of the form*

$$\mathbb{F}_q[D_{2n}] \cong \bigoplus_{j=1}^{r+s} A_j,$$

where

$$A_j = \begin{cases} \mathbb{F}_q \bigoplus \mathbb{F}_q, & j \le \delta, \\ M_2(\mathbb{F}_q(\alpha_j + \alpha_j^{-1})), & \delta + 1 \le j \le r + s, \end{cases} \qquad \delta = \begin{cases} 1, & \text{if } n \text{ is odd}, \\ 2, & \text{if } n \text{ is even}. \end{cases}$$

Observe that, if $r + 1 \le j \le r + s$, then $M_2(\mathbb{F}_q(\alpha_j + \alpha_j^{-1})) = M_2(\mathbb{F}_q(\alpha_j))$.

Lemma 2.4 (see [2]) *The dihedral group algebra $\mathbb{F}_q[D_{2n}]$ has $\delta + r + s$ central irreducible idempotents*:

(1) *2δ idempotents of the form $\frac{1+y}{2}e_{f_j}$ and $\frac{1-y}{2}e_{f_j}$, where $j \le \delta$,*

(2) *$r - \delta$ idempotents e_{f_j}, where $j = \delta + 1, \cdots, r$, generated by the auto-reciprocals factor of $x^n - 1$,*

(3) *s idempotents $e_{f_j} + e_{f_j^*}$, where $j = r + 1, \cdots, r + s$.*

3 Main Results

The adjoint of an element $\alpha = \sum_{g\in G} a_g g \in \mathbb{F}_q[G]$ is defined by $\widehat{\alpha} = \sum_{g\in G} a_g g^{-1}$. Suppose that e is an idempotent of $\mathbb{F}_q[G]$. If $e\mathbb{F}_q[G]$ is an irreducible right ideal, e is called an irreducible idempotent. If there is a factorization of orthogonal irreducible idempotents: $1 = e_1 + \cdots + e_n$, then $\{e_1, \cdots, e_n\}$ is called a complete set of orthogonal idempotents. In fact, for each right ideal I of $\mathbb{F}_q[G]$, $I = \sum_{i\in S} e_i\mathbb{F}_q[G]$, where $S \subset \{1, \cdots, n\}$.

If $\widehat{e} = e$, then e is called a projective idempotent. If $\widehat{e}e = 0$, then e is called an isotropic idempotent.

Lemma 3.1 (see [9]) *If $\mathcal{C}$ is a right ideal of $\mathbb{F}_q[G]$, then the following statements are equivalent*:

(a) $\mathcal{C}$ *is an* LCD *code,*

(b) $\mathcal{C} = e\mathbb{F}_q[G]$, *where* $e^2 = e = \widehat{e}$.

In this section, we give the generators and enumerations of LCD codes and self-orthogonal codes in finite dihedral group algebra $\mathbb{F}_q[D_{2n}]$. In the following, we shall find a complete set of orthogonal idempotent with irreducible projective idempotents and irreducible isotropic idempotents by central irreducible idempotents of $\mathbb{F}_q[D_{2n}]$ by Lemma 2.4.

Theorem 3.1 *The dihedral group algebra $\mathbb{F}_q[D_{2n}]$ has a complete set of orthogonal idempotents with $2r$ irreducible projective idempotents and $2s$ irreducible isotropic idempotents.*

Proof (1) As in the proof of Lemma 2.3, let τ be the isomorphism of $\mathbb{F}_q$-algebra defined by $\sum_{j=1}^{r+s} \tau_j$. Note that

$$\begin{aligned}\tau_1 : \mathbb{F}_q[D_{2n}] &\to \mathbb{F}_q \bigoplus \mathbb{F}_q,\\ x &\mapsto (1,1),\ y \mapsto (1,-1),\end{aligned}$$

and if n is even, then

$$\begin{aligned}\tau_2 : \mathbb{F}_q[D_{2n}] &\to \mathbb{F}_q \bigoplus \mathbb{F}_q,\\ x &\mapsto (-1,-1),\ y \mapsto (1,-1).\end{aligned}$$

For $j \geq \delta + 1$,

$$\begin{aligned}\tau_j : \mathbb{F}_q[D_{2n}] &\to M_2(\mathbb{F}_q(\alpha_j)),\\ x &\mapsto \begin{pmatrix} \alpha_j & 0 \\ 0 & \alpha_j^{-1} \end{pmatrix},\ y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\end{aligned}$$

where α_j is a root of $f_j(x)$.

By Lemma 2.2, $e_{f_j} (1 \leq j \leq r)$ are center primitive idempotents of $\mathbb{F}_q[C_n]$. We proceed the proof with the following two cases:

Case 1. If $j \leq \delta$, then by Lemma 2.4, $\frac{1+y}{2}e_{f_j}$ and $\frac{1-y}{2}e_{f_j}$ are orthogonal irreducible idempotents of dihedral group algebra $\mathbb{F}_q[D_{2n}]$.

Case 2. If $\delta+1 \le j \le r$, then we need to verify that $\tau_j(\frac{1+y}{2}e_{f_j})$ and $\tau_j(\frac{1-y}{2}e_{f_j})$ are idempotents of $M_2(\mathbb{F}_q(\alpha_j))$. Since $f_j(x)=f_j^*(x)$ and α_j is a root of $f_j(x)$,

$$\tau_j(e_{f_j})=\begin{pmatrix} e_{f_j}(\alpha_j) & 0 \\ 0 & e_{f_j}(\alpha_j)\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

Hence

$$\tau_j\Big(\frac{1+y}{2}e_{f_j}\Big)=\tau_j\Big(\frac{1+y}{2}\Big)\tau_j(e_{f_j})=\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix},$$
$$\tau_j\Big(\frac{1-y}{2}e_{f_j}\Big)=\tau_j\Big(\frac{1-y}{2}\Big)\tau_j(e_{f_j})=\frac{1}{2}\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1&-1\\-1&1\end{pmatrix}.$$

It is obvious that $\tau_j\big(\frac{1+y}{2}e_{f_j}\big)$ and $\tau_j\big(\frac{1-y}{2}e_{f_j}\big)$ are orthogonal irreducible idempotents of $M_2(\mathbb{F}_q(\alpha_j))$, and moreover,

$$\tau_j\Big(\frac{1+y}{2}e_{f_j}\Big)+\tau_j\Big(\frac{1-y}{2}e_{f_j}\Big)=I_2.$$

Therefore, $\frac{1+y}{2}e_{f_j}$ and $\frac{1-y}{2}e_{f_j}$ are orthogonal irreducible idempotents of $\mathbb{F}_q[D_{2n}]$.

Next we prove that $e_{f_j}=\widehat{e_{f_j}}$ by Lemma 3.1. In fact,

$$e_{f_j}=-\frac{((f_j^*(x))')^*}{n}\cdot\frac{x^n-1}{f_j(x)}=\sum_{i=1}^{k}u_{\lambda_{ji}},$$

where $f_j(x)=(x-\lambda_{j1})(x-\lambda_{j2})\cdots(x-\lambda_{jk})\in\mathbb{F}_{q^t}[x]$, $\mathbb{F}_q[x]/(f_j(x))\cong\mathbb{F}_{q^t}$ (for some positive integer t), and

$$u_{\lambda_{ji}}=\frac{1}{n}\sum_{l=0}^{n-1}\lambda_{ji}^{-l}x^l=\frac{1}{n}(1+\lambda_{ji}^{-1}x+\lambda_{ji}^{-2}x^2+\cdots+\lambda_{ji}^{1-n}x^{n-1}),\quad 1\le j\le k.$$

Then

$$\widehat{u_{\lambda_{ji}}}=\frac{1}{n}(1+\lambda_{ji}^{-1}x^{-1}+\lambda_{ji}^{-2}x^{-2}+\cdots+\lambda_{ji}^{n-l}x^{-(n-1)}).$$

Since $\lambda_{j1},\lambda_{j2},\cdots,\lambda_{jk}$ are all roots of $f_j(x)$, $\lambda_{j1}^{-1},\lambda_{j2}^{-1},\cdots,\lambda_{jk}^{-1}$ are also all roots of $f_j(x)$. Hence $\widehat{e_{f_j}}=e_{f_j}$.

Since $\widehat{y}=y^{-1}=y$, it is easy to get two orthogonal irreducible projective idempotents:

$$\widehat{\frac{1+y}{2}}e_{f_j}=\frac{1+y}{2}e_{f_j},\quad \widehat{\frac{1-y}{2}}e_{f_j}=\frac{1-y}{2}e_{f_j},$$

and $\tau_j\big(\frac{1+y}{2}e_{f_j}\big)+\tau_j\big(\frac{1-y}{2}e_{f_j}\big)=I_2$, $\delta+1\le j\le r$.

(2) Next, we need to check that $\widehat{e_{f_j}}e_{f_j}=0$ and $\widehat{e_{f_j^*}}e_{f_j^*}=0$ for all $j=r+1,\cdots,r+s$. In fact, $f_j(x)=(x-\lambda_{j1})(x-\lambda_{j2})\cdots(x-\lambda_{jk})\in\mathbb{F}_{q^t}[x]$, $\mathbb{F}_q[x]/(f_j(x))\cong\mathbb{F}_{q^t}$, and $e_{f_j}=-\frac{((f_j^*(x))')^*}{n}\cdot\frac{x^n-1}{f_j(x)}=\sum\limits_{i=1}^{k}u_{\lambda_{ji}}$, where $u_{\lambda_{ji}}=\frac{1}{n}\sum\limits_{l=0}^{n-1}\lambda_{ji}^{-l}x^l$, $1\le i\le k$. Then

$$\widehat{u_{\lambda_{ji}}}=\frac{1}{n}(1+\lambda_{ji}^{-1}x^{-1}+\lambda_{ji}^{-2}x^{-2}+\cdots+\lambda_{ji}^{n-l}x^{-(n-1)}).$$

Since $\lambda_{j1},\lambda_{j2},\cdots,\lambda_{jk}$ are all roots of $f_j(x)$, $\lambda_{j1}^{-1},\lambda_{j2}^{-1},\cdots,\lambda_{jk}^{-1}$ are also all roots of $f_j^*(x)$. Hence $\widehat{e_{f_j}}=e_{f_j^*}$.

Hence

$$\tau_j(\widehat{e_{f_j}}e_{f_j}) = \tau_j(\widehat{e_{f_j}})\tau_j(e_{f_j}) = \begin{pmatrix} \widehat{e_{f_j}}(\alpha_j) & 0 \\ 0 & \widehat{e_{f_j}}(\alpha_j^{-1}) \end{pmatrix} \begin{pmatrix} e_{f_j}(\alpha_j) & 0 \\ 0 & e_{f_j}(\alpha_j^{-1}) \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 0.$$

Similarly, we can obtain $\tau_j(\widehat{e_{f_j^*}}e_{f_j^*}) = 0$. Therefore $\widehat{e_{f_j}}e_{f_j} = 0$, $\widehat{e_{f_j^*}}e_{f_j^*} = 0$, $e_{f_j} + e_{f_j^*} = I_2$.

This completes the proof.

For convenience of enumerations, we give the following sets:

$$\Delta_1 = \Big\{\frac{1+y}{2}e_{f_i}, \frac{1-y}{2}e_{f_i} : 1 \le i \le r\Big\},$$
$$\Delta_2 = \{e_{f_i}, e_{f_i^*} : r+1 \le i \le r+s\}.$$

Then $\Delta_1 \cup \Delta_2$ is a complete set of orthogonal idempotents in $\mathbb{F}_q[D_{2n}]$.

Theorem 3.2 *There are* 2^{2r+s} LCD *codes in the finite dihedral group algebra* $\mathbb{F}_q[D_{2n}]$.

Proof For a right ideal $\mathcal{C}$ of $\mathbb{F}_q[D_{2n}]$, by the Wedderburn-Artin theorem

$$\mathcal{C} = \Big(\sum_{i\in S} e_i\Big)\mathbb{F}_q[D_{2n}],$$

where $S \subset \Delta_1 \cup \Delta_2$. By Lemma 3.1, $\mathcal{C}$ is an LCD code if and only if $\widehat{\sum\limits_{i\in S} e_i} = \sum\limits_{i\in S} \widehat{e_i} = \sum\limits_{i\in S} e_i$.

It is easy to know that the idempotents of Δ_1 are irreducible projective idempotents. Set

$$\Delta_2' = \{e_{f_i} + e_{f_i^*} : r+1 \le i \le r+s\}.$$

Then $\Delta_1 \cup \Delta_2'$ consists of all irreducible projective idempotents.

Suppose that $\mathcal{C} = \sum\limits_{i\in S} e_i\mathbb{F}_q[D_{2n}]$ is an LCD code. Then $S \subset \Delta_1 \cup \Delta_2'$. The converse also holds. Moreover, from $|\Delta_1 \cup \Delta_2'| = 2s + r$, we obtain the result.

The proof is completed.

Lemma 3.2 *For any* $\alpha, \beta, \gamma \in \mathbb{F}_q[G]$, $\langle \alpha\beta, \gamma\rangle = \langle \alpha, \widehat{\beta}\gamma\rangle$.

Proof For $g \in G$, we only need to verify that $\langle g\beta, \gamma\rangle = \langle g, \widehat{\beta}\gamma\rangle$. Letting $\beta = \sum\limits_{h\in G} a_h h, \gamma = \sum\limits_{h\in G} b_h h$, we obtain that

$$\langle g\beta, \gamma\rangle = \Big\langle \sum_{h\in G} a_h gh, \sum_{h\in G} b_h h\Big\rangle = \sum_{h\in G} a_h b_h,$$
$$\langle g, \widehat{\beta}\gamma\rangle = \Big\langle g, \sum_{h\in G} a_h h^{-1} \sum_{h\in G} b_h h\Big\rangle = \Big\langle g, \sum_{h\in G} a_h h^{-1} \sum_{h\in G} b_h hg\Big\rangle = \sum_{h\in G} a_h b_h.$$

Therefore, we get $\langle g\beta, \gamma\rangle = \langle g, \widehat{\beta}\gamma\rangle$, and in general, we have $\langle \alpha\beta, \gamma\rangle = \langle \alpha, \widehat{\beta}\gamma\rangle$.

This completes the proof.

Based on Lemma 3.2, we can get the following theorem.

Theorem 3.3 *Let $\mathcal{C} = e\mathbb{F}_q[G]$ be an right ideal of $\mathbb{F}_q[G]$, where e is an idempotent of $\mathbb{F}_q[G]$. Then $\mathcal{C}$ is a self-orthogonal code if and only if $\widehat{e}e = 0$.*

Proof For any $\alpha, \beta \in \mathbb{F}_q[G]$, we can easily get

$$0 = \langle e\alpha, e\beta\rangle = \langle \alpha, \widehat{e}e\beta\rangle.$$

Hence, we have $\widehat{e}e = 0$.

The proof is completed.

Theorem 3.4 *There are 3^s self-orthogonal codes in the finite dihedral group algebra $\mathbb{F}_q[D_{2n}]$.*

Proof For a right ideal $\mathcal{C}$ of $\mathbb{F}_q[D_{2n}]$, by the Wedderburn-Artin theorem

$$\mathcal{C} = \Big(\sum_{i\in S} e_i\Big)\mathbb{F}_q[D_{2n}],$$

where $S \subset \Delta_1 \cup \Delta_2$. By Theorem 3.3. $\mathcal{C}$ is a self-orthogonal code if and only if $\widehat{\sum\limits_{i\in S} e_i}\big(\sum\limits_{i\in S} e_i\big) = 0$.

Suppose that $\mathcal{C} = f\mathbb{F}_q[D_{2n}]$ is a right ideal of $\mathbb{F}_q[D_{2n}]$, where

$$f = \sum_{e_{f_i}+e_{f_i^*}\in\Delta_2'} (ae_{f_i} + be_{f_i^*}), \quad (a,b) \in \{(0,0),(0,1),(1,0)\}.$$

Then $\mathcal{C}$ is a self-orthogonal code. The converse also holds. Moreover, from $|\Delta_2'| = s$, we obtain the result.

The proof is completed.

4 Examples

In this section, we will give some examples to illustrate our main results.

Example 4.1 (i) Let $q = 3$ and $n = 7$. We consider the dihedral group algebra $\mathbb{F}_3[D_{14}]$. Here

$$x^7 - 1 = f_1(x)f_2(x),$$

where

$$f_1(x) = x - 1, \quad f_2(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

By Theorem 3.2, there are 2^4 LCD codes in $\mathbb{F}_3[D_{14}]$.

(ii) Let $q = 3$ and $n = 8$. We consider the dihedral group algebra $\mathbb{F}_3[D_{16}]$. Here

$$x^8 - 1 = f_1(x)f_2(x)f_3(x)f_4(x)f_4^*(x),$$

where

$$f_1(x) = x - 1, \quad f_2(x) = x + 1, \quad f_3(x) = x^2 + 1, \quad f_4(x) = x^2 + x + 2, \quad f_4^*(x) = x^2 + 2x + 2.$$

By Theorem 3.2, there are 2^7 LCD codes in $\mathbb{F}_3[D_{16}]$. By Theorem 3.4, there are 3 self-orthogonal codes in $\mathbb{F}_3[D_{16}]$.

(iii) Let $q = 3$ and $n = 13$. We consider the dihedral group algebra $\mathbb{F}_3[D_{26}]$. Here

$$x^{13} - 1 = f_1(x)f_2(x)f_2^*(x)f_3(x)f_3^*(x),$$

where

$$f_1(x) = x - 1, \quad f_2(x) = x^3 + 2x + 2, \quad f_2^*(x) = x^3 + x^2 + 2,$$
$$f_3(x) = x^3 + x^2 + x + 1, \quad f_4^*(x) = x^3 + 2x^2 + 2x + 2.$$

By Theorem 3.2, there are 2^4 LCD codes in $\mathbb{F}_3[D_{26}]$. By Theorem 3.4, there are 3^2 self-orthogonal codes in $\mathbb{F}_3[D_{26}]$.

Example 4.2 (i) Let $q = 5$ and $n = 8$. We consider the dihedral group algebra $\mathbb{F}_5[D_{16}]$. Here

$$x^8 - 1 = f_1(x)f_2(x)f_3(x)f_3^*(x)f_4(x)f_4^*(x),$$

where

$$f_1(x) = x - 1, \quad f_2(x) = x + 1, \quad f_3(x) = x + 2, \quad f_3^*(x) = x + 3,$$
$$f_4(x) = x^2 + 2, \quad f_4^*(x) = x^2 + 3.$$

By Theorem 3.2, there are 2^6 LCD codes in $\mathbb{F}_5[D_{16}]$. By Theorem 3.4, there are 3^2 self-orthogonal codes in $\mathbb{F}_5[D_{16}]$.

(ii) Let $q = 5$ and $n = 13$. We consider the dihedral group algebra $\mathbb{F}_5[D_{26}]$. Here

$$x^{13} - 1 = f_1(x)f_2(x)f_3(x)f_4(x),$$

where

$$f_1(x) = x - 1, \quad f_2(x) = x^4 + x^3 + 4x^2 + x + 1,$$
$$f_3(x) = x^4 + 2x^3 + x^2 + 2x + 1, \quad f_4(x) = x^4 + 3x^3 + 3x + 1.$$

By Theorem 3.4, there are 2^8 LCD codes in $\mathbb{F}_5[D_{26}]$.

Acknowledgement The authors are very grateful to the reviewers and the editor for their valuable comments and suggestions to improve the quality of this paper.

References

[1] Boripan, A., Jitman, S. and Udomkavanich, P., Characterization and enumeration of complementary dual abelian codes, *J. Appl. Math. Comput.*, **58**(1–2), 2018, 527–544.

[2] Brochero Martínez, F. E., Structure of finite dihedral group algebra, *Finite Fields Appl.*, **35**, 2015, 204–214.

[3] Brochero Martínez, F. E. and Giraldo Vergara, C. R., Explicit idempotents of finite group algebras, *Finite Fields Appl.*, **28**, 2014, 123–131.

[4] Carlet, C., Mesnager, S., Tang, C. and Qi, Y., Euclidean and Hermitian LCD MDS codes, *Des. Codes. Cryptogr.*, **86**(11), 2018, 2605–2618.

[5] Carlet, C., Mesnager, S., Tang, C., et al., Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, *IEEE Trans. Inf. Theory*, **64**(4), 2018, 3010–3017.

[6] Choosuwan, P., Jitman, S. and Udomkavanich, P., Self-abelian codes in some nonprincipal ideal group algebras, *Math. Probl. Eng.*, Article ID: 9020173, 12 pages, 2016.

[7] Cao, Y., Cao, Y. and Fu, F., Concatenated structure of left dihedral codes, *Finite Fields Appl.*, **38**, 2016, 93–115.

[8] Cao, Y., Cao, Y., Fu, F. and Wang, S., Left dihedral codes over Galois ring $GR(p^2, m)$, *Discrete Math.*, **341**, 2018, 1816–1834.

[9] Cruz, J. and Willems, W., On group codes with complementary duals, *Des. Codes. Cryptogr.*, **86**, 2018, 2065–2073,.

[10] Ferraz, R. A. and Polcino Milies, C., Idempotents in group algebras and minimal abelian codes, *Finite Fields Appl.*, **13**, 2007, 382–393.

[11] Griesmer, J. H., A bound for error correcting codes, *IBM J. Res. Der.*, **3**(5), 1960, 532–542.

[12] Jitman, S., Ling S., Liu, H. and Xie, X., Abelian codes in principal ideal group algebras, *IEEE Trans. Inf. Theory*, **59**, 2013, 3046–3057.

[13] Jitman, S., Ling, S. and Solé, P., Hermitian self-dual abelian codes, *IEEE Trans. Inf. Theory*, **60**, 2014, 1496–1507.

[14] Massey, J. L., Reversible codes, *Inf. Control*, **7**(3), 1964, 369–380.

[15] Mesnager, S., Tang, C. and Qi, Y., Complementary dual algebraic geometry codes, *IEEE Trans. Inf. Theory*, **64**, 2018, 2390–2397.

[16] Passman D. S., The Algebraic Structure of Group Rings, Wiley, New York, 1977.

[17] Polcino Milies, C. and Diniz de Melo, F., On cyclic and abelian codes, *IEEE Trans. Inf. Theory*, **59**, 2013, 7314–7319.

[18] Polcino Milies, C. and Sehgal, S. K., An Introduction to Group Rings, Dordrecht, The Notherlands: Kluwer, 2002.