Complementary dual abelian codes in group algebras of some finite abelian groups

Somphong Jitman[1,*]

[1]Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom, 73000, Thailand

Abstract. Linear complementary dual codes have become an interesting subfamily of linear codes over finite fields since they can be practically applied in various fields such as cryptography and quantum error-correction. Recently, properties of complementary dual abelian codes were established in group algebras of arbitrary finite abelian groups. However, the enumeration formulas were given mostly based on number-theoretical characteristic functions. In this article, complementary dual abelian codes determined by some finite abelian groups are revisited. Specifically, the characterization of cyclotomic classes of an abelian group and the enumeration of complementary dual abelian codes are presented, where the group is a finite abelian p-group, a finite abelian 2-group, and a product of a finite abelian p-group and a finite abelian 2-group for some odd prime number p different from the characteristic of the alphabet filed. The enumeration formula for such complementary dual codes is given explicitly in a more precise form without characteristic functions. Some illustrative examples are given as well.

1 Introduction

A *linear complementary dual (LCD) code* is defined to be a linear code that meets its dual trivially. LCD codes have been first introduced together with their characterization and applications in [14]. A family of LCD codes has been shown to be good in [17] and asymptotically good in [14]. Later, various applications of LCD codes have been presented such as in information protection from hardware Trojan horses and side-channel attacks (see, for example, [5], [8], and [10]) and in constructions of quantum codes with good parameters (see, for example, [4] and [9]).

Cyclic codes over finite fields are algebraic structured codes that can be efficiently implemented using shift registers. Cyclic codes with complementary duality have been characterized in [18]. An abelian code over finite fields is one of the generalizations of cyclic codes defined as an ideal in a group algebra. Due to the theoretical and practical reasons, abelian codes form another interesting family of linear codes. The family of abelian codes have extensively studied in various directions (see, for example, [3], [6], [7], [12], and [16]). In [3], complementary dual abelian (CDA) codes were studied. The algebraic structures of such codes were established together with their enumeration results. However, the enumeration formulas were given mostly based on number-theoretical characteristic functions.

*e-mail: sjitman@gmail.com

In this article, CDA codes over a finite field $\mathbb{F}_{q^\nu}$ are revisited for some specific abelian groups, for all prime numbers q, and for all natural numbers ν. Precisely, for an odd prime number p different from q, we focus on CDA codes in a group algebra of an abelian group $B \times A$, where B is a finite 2-group and A is a finite p-group. The enumeration formulas for such CDA codes are given in a more precise form without the characteristic functions.

Some basic definitions, concepts, notations, and general results on CDA codes in [3] are recalled in Section 2. The key characterization and enumeration results in this article are presented in Section 3 and Section 4. The enumeration and characterization of CDA codes determined by a finite abelian p-group are presented in Section 3. Later, in Section 4, the number of CDA codes determined by a finite abelian 2-group is given as well as applications in the enumeration of CDA codes determined by a finite abelian group which is a product of a p-group and a 2-group. In Section 5, discussion and summary are given together with some open problems.

2 Preliminaries

Necessary notations and algebraic structures of group algebras of finite abelian groups over finite fields are provided as well as general results on CDA codes. The reader may refer to [3] and [12] for more information.

Throughout let ν be a natural number and let q be a prime number. Denote by $\mathbb{F}_{q^\nu}$ the finite field of q^ν elements. In this case, the characteristic of $\mathbb{F}_{q^\nu}$ is q.

2.1 Abelian Codes

For natural numbers i and j, we write $i|j$ if i is a divisor of j, and $i \nmid j$ otherwise. The notation $2^\gamma \| j$ refers to the situation where $2^\gamma | j$ and $2^{\gamma+1} \nmid j$. For integers a and b, we write $a \equiv b \pmod{i}$ if $i|(a-b)$. In the case where $\gcd(i, j) = 1$, denote by $\mathrm{ord}_j(i)$ the smallest natural number k satisfying $i^k \equiv 1 \pmod{j}$. For a natural number n, let G be an abelian group of order n. For convenience, the operation in G is written additively and the order of an element $g \in G$ is denote by $\mathrm{ord}(g)$. For a natural number d, let $\mathcal{N}_G(d)$ be the number of elements in the group G whose order is d. We note that $\mathcal{N}_G(d)$ can be zero or a natural number.

Let $\mathbb{F}_{q^\nu}[G]$ be the group algebra of the finite abelian group G over $\mathbb{F}_{q^\nu}$. An element in the group algebra $\mathbb{F}_{q^\nu}[G]$ is presented as the usual sum $\sum_{g \in G} \alpha_g Y^g$, where $\alpha_g \in \mathbb{F}_{q^\nu}$. In the group algebra $\mathbb{F}_{q^\nu}[G]$, the calculation can be done as in the ring $\mathbb{F}_{q^\nu}[Y]$ of polynomials, where the subscripts and superscripts are operated in G. An *abelian code* is a generalization of a cyclic code over $\mathbb{F}_{q^\nu}$ defined as an ideal in $\mathbb{F}_{q^\nu}[G]$. Equivalently, an abelian code in $\mathbb{F}_{q^\nu}[G]$ can be represented as a subspace of $\mathbb{F}_{q^\nu}^n$ embedded as an ideal in $\mathbb{F}_{q^\nu}[G]$ (see [12] and [13]).

The *inner product* between $u = \sum_{g \in G} u_g Y^g$ and $v = \sum_{g \in G} v_g Y^g$ in $\mathbb{F}_{q^\nu}[G]$ is given to be the form $\langle u, v \rangle := \sum_{g \in G} u_g v_g$. The *dual* of an abelian code C in the group algebra $\mathbb{F}_{q^\nu}[G]$ is given to be the set

$$C^\perp := \{v \in \mathbb{F}_{q^\nu}[G] \mid \langle c, v \rangle = 0 \text{ for all } c \in C\}.$$

For an abelian code C in $\mathbb{F}_{q^\nu}[G]$, we note that $C^\perp$ and $C \cap C^\perp$ are also abelian codes. In [3], an abelian code C is called a *CDA code* if $C \cap C^\perp = \{0\}$.

Let Q denote the Sylow q-subgroup of G. It follows that the abelian group G can be viewed in the form of $G \cong A \times Q$ for some subgroup A of G with $|A| = [G : Q]$ and $q \nmid |A|$. Clearly, the group algebra $\mathcal{R} := \mathbb{F}_{q^\nu}[A]$ is semi-simple. In [2] and [12], the semi-simple group algebra $\mathcal{R} := \mathbb{F}_{q^\nu}[A]$ studied and its decomposition is given using the discrete Fourier transform. For completeness, necessary results are recalled.

The q^ν-*cyclotomic class* of the finite abelian group A containing $a \in A$ is given as

$$S_{q^\nu}(a) := \{q^{\nu i} \cdot a \mid i = 0, 1, \dots\}.$$

It is not difficult to see that $S_{q^\nu}(a) = \{q^{\nu i} \cdot a \mid 0 \le i < \mathrm{ord}_{\mathrm{ord}(a)}(q^\nu)\}$.

Each element e in $\mathcal{R}$ is called an *idempotent* if e is non-zero and $e^2 = e$. In addition, if an idempotent e satisfies either $ef = 0$ or $ef = e$ for every other idempotent in $\mathcal{R}$, it is said to be *primitive* From [7, Proposition II.4], there are one-to-one correspondence between the q^ν-cyclotomic classes of A and the primitive idempotents in $\mathcal{R}$. Precisely, each q^ν-cyclotomic class of A induces a primitive idempotent in $\mathcal{R}$.

Let $\{S_{p^\nu}(a_i) \mid i = 1, 2, \dots, k\}$ denote the set of all q^ν-cyclotomic classes of A. For each $i \in \{1, 2, \dots, k\}$, denote by e_i the primitive idempotent in the group algebra $\mathcal{R}$ determined by $S_{p^\nu}(a_i)$. In [3], the decomposition of $\mathcal{R}$ is given as follows

$$\mathcal{R} = \bigoplus_{i=1}^{k} \mathcal{R}e_i \cong \prod_{i=1}^{k} \mathbb{F}_{q^{\nu s_i}}, \tag{1}$$

where $\mathcal{R}e_i \cong \mathbb{F}_{q^{\nu s_i}}$ and $s_i = |S_{q^\nu}(a_i)| = \mathrm{ord}_{\mathrm{ord}(a_i)}(q^\nu)$. Consequently,

$$\mathbb{F}_{q^\nu}[G] = \mathcal{R}[Q] = \bigoplus_{i=1}^{k} (\mathcal{R}e_i)[Q] \cong \prod_{i=1}^{k} \mathbb{F}_{q^{\nu s_i}}[Q]. \tag{2}$$

2.2 Complementary Dual Abelian Codes

General results on CDA codes over finite field have been presented in [3] using a number-theoretical characteristic function summarized.

Let a be an element in A. A q^ν-cyclotomic class $S_{q^\nu}(a)$ is said to be of *type I* if $S_{q^\nu}(a) = S_{q^\nu}(-a)$ and it is said to be of *type II* otherwise. By rearranging the set $\{S_{p^\nu}(a_i) \mid i = 1, 2, \dots, k\}$, it can be assumed that $\{S_{q^\nu}(a_j) | j = 1, 2, \dots, r_I\}$ is the set of all q^ν-cyclotomic classes of type I and $\{S_{q^\nu}(a_{r_I+l}) \mid l = 1, 2, \dots, r_{II}\} \cup \{S_{q^\nu}(a_{r_I+r_{II}+l}) = S_{q^\nu}(-a_{r_I+l}) \mid l = 1, 2, \dots, r_{II}\}$ is the set of all q^ν-cyclotomic classes of type *II*. In this case, $k = r_I + 2r_{II}$.

By rearranging the terms in (2) (see [3]), it follows that

$$\mathbb{F}_{q^\nu}[A \times Q] \cong \left(\prod_{j=1}^{r_I} \mathbb{K}_j[Q]\right) \times \left(\prod_{l=1}^{r_{II}} (\mathbb{L}_l[Q] \times \mathbb{L}_l[Q])\right), \tag{3}$$

where $\mathbb{K}_j \cong \mathbb{F}_{q^{\nu s_j}}$ and $\mathbb{L}_l \cong \mathbb{F}_{p^{\nu s_{r_I+l}}}$ for all integers $j = 1, 2, \dots, r_I$ and $l = 1, 2, \dots, r_{II}$. Consequently, each abelian code C in $\mathbb{F}_{q^\nu}[A \times Q]$ is of the form

$$C \cong \left(\prod_{j=1}^{r_I} C_j\right) \times \left(\prod_{l=1}^{r_{II}} \left(D_l \times D_l'\right)\right), \tag{4}$$

for some abelian codes $C_j \subseteq \mathbb{K}_j[Q]$, $D_l \subseteq \mathbb{L}_l[Q]$, and $D_l' \subseteq \mathbb{L}_l[Q]$.

In [3], the characterization of CDA codes in $\mathbb{F}_{q^\nu}[A \times Q]$ has been given.

Proposition 1 ([3, Corollary 4]) *Let q be a prime number and let ν be a positive integer. Let A be finite abelian group such that $q \nmid |A|$ and let Q be a finite abelian q-group. Then an abelian code C in $\mathbb{F}_{q^\nu}[A \times Q]$ decomposed as in* (4) *is CDA if and only if the following statements hold.*

1) $C_j \in \{\{0\}, \mathbb{K}_j[Q]\}$ *for all* $1 \le j \le r_I$.

2) $(D_l, D_l') \in \{(\{0\}, \mathbb{L}_j[Q]), (\mathbb{L}_j[Q], \{0\})\}$ *for all* $1 \le l \le r_{II}$.

Moreover, in [3, Corollary 5], the enumeration formula of CDA codes in $\mathbb{F}_{q^\nu}[A \times Q]$ has been shown to be independent of the choices of Q.

Proposition 2 ([3, Corollary 5]) *Let q be a prime number and let ν be a natural number. Let A be finite abelian group such that $q \nmid |A|$ and let Q be a finite abelian q-group. If $\mathbb{F}_{q^\nu}[A \times Q]$ decomposed as in* (3)*, then the number of CDA codes in $\mathbb{F}_{q^\nu}[A \times Q]$ is $2^{r_I + r_{II}}$.*

In [3], the numbers r_I and r_{II} have been presented via the characteristic function

$$\chi(d, q^\nu) = \begin{cases} 1 & \text{if } d|(q^{\nu i} + 1) \text{ for some natural number } i, \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

for all natural numbers d.

Proposition 3 ([3, Proposition 5]) *Let q be a prime and let ν be a natural number. Let A be a finite abelian group of exponent M. If $q \nmid M$, then*

$$r_I = \sum_{d|M} \chi(d, q^\nu) \frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(q^\nu)} \quad \text{and} \quad r_{II} = \frac{1}{2} \sum_{d|M} (1 - \chi(d, q^\nu)) \frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(q^\nu)}.$$

We note that $\mathcal{N}_A(d)$ is given in [1].

In the following sections, we present the number of CDA codes in $\mathbb{F}_{q^\nu}[A \times Q]$, where A is a finite abelian group viewed as a product of a finite p-group and a finite 2-group for all odd prime numbers q with $p \neq q$. Since this number is independent of the Sylow q-subgroup Q, it is therefore enough to determined only r_I and r_{II} for $\mathbb{F}_{q^\nu}[A]$. Precisely, the numbers r_I and r_{II} will be given in a more precise from without the characteristic function χ.

3 CDA Codes: p-Groups

Let p be an odd prime number different form q. Throughout let A denote a finite abelian p-group of exponent p^s and order p^t for some integers $1 \le s \le t$. It is not difficult to see that $A \cong \prod_{i=1}^{s} \left(\mathbb{Z}_{p^i}\right)^{t_i}$, where $t_i \ge 0$ for all $i = 1, 2, \ldots, s-1$, $t_s \ge 1$, and $t = \sum_{i=1}^{s} i t_i$.

Lemma 1 ([1, Theorem 1]) *Let s be a natural number and let $A = \prod_{i=1}^{s} \left(\mathbb{Z}_{p^i}\right)^{t_i}$ be a finite abelian p-group with $t_s \ge 1$ and $t_i \ge 0$ for each $i = 1, 2, \ldots, s-1$. Then, for all $1 \le i \le s$, we have*

$$\mathcal{N}_A(p^i) = p^{m_i} - p^{m_{i-1}},$$

where $N := \sum_{i=1}^{s} t_i$, $m_0 := 0$, $m_1 := N$, and $m_i := iN + \sum_{j=1}^{i-1} (j - i)$ for all $2 \le i \le s$.

From [15, Theorem 3.6], for a natural number i, we have

$$\mathrm{ord}_{p^i}(q^\nu) = \begin{cases} \mathrm{ord}_p(q^\nu) & \text{if } i \le \beta, \\ p^{i-\beta} \, \mathrm{ord}_p(q^\nu) & \text{if } \beta < i, \end{cases} \tag{6}$$

where β is the largest integer such that $p^\beta | \left(q^{\nu \, \mathrm{ord}_p(q^\nu)} - 1\right)$.

In the rest of this subsection, some characterizations of an element in A and a q^ν-cyclotomic class of A are presented. Subsequently, the enumeration of CDA codes in a group algebra of A is presented. Theses are key to determine the numbers r_I and r_{II} in Proposition 5.

Proposition 4 *Let p be an odd prime number with $p \neq q$ and let A be a finite abelian p-group. Then TFAE.*

1) $\mathrm{ord}_p(q^\nu)$ *is even.*

2) $\mathrm{ord}_{p^i}(q^\nu)$ *is even for all natural numbers i.*

3) $\chi(p^i, q^\nu) = 1$ *for all integers $i \geq 0$.*

4) *Every q^ν-cyclotomic class of A is of type I.*

Proof. The statement "1) implies 2)" can be derived directly from (6).

Assume that $\mathrm{ord}_{p^i}(q^\nu)$ is even for all natural numbers i. Clearly, $\chi(p^0, q^\nu) = 1$. For $i \geq 1$, $\mathrm{ord}_{p^i}(q^\nu) = 2k$ for some natural number k. Precisely, $q^{2\nu k} \equiv 1 \pmod{p^i}$ and $q^{\nu k} \not\equiv 1 \pmod{p^i}$ which implies that $p^i | (q^{\nu k} - 1)(q^{\nu k} + 1)$ and $p^i \nmid (q^{\nu k} - 1)$. Consequently, we have $p^i | (q^{\nu k} + 1)$, and hence, $\chi(p^i, q^\nu) = 1$. This proves "2) implies 3)".

Assume that $\chi(p^i, q^\nu) = 1$ for all integers $i \geq 0$. Clearly, the q^ν-cyclotomic class $\{0\}$ is of type I. Let $a \in A \setminus \{0\}$. It follows that $\mathrm{ord}(a) = p^j$ for some integer $1 \leq j \leq s$. As $\chi(p^j, q^\nu) = 1$, we have $p^j | (q^{\nu k} + 1)$ for some integer $k \geq 1$. Consequently, $q^{\nu k} \equiv -1 \pmod{p^j}$ and $q^{\nu k} a = -a$, i.e., $-a \in S_{q^\nu}(a)$. Then $S_{q^\nu}(a) = S_{q^\nu}(-a)$. The statement "3) implies 4)" is completed.

Assume that every q^ν-cyclotomic class of the group A is of type I. Let $a \in A$ be an elemnent of order p. Since $S_{q^\nu}(a)$ is of type I, we have $-a \in S_{q^\nu}(a)$. Consequently, $q^{\nu k} \equiv -1 \pmod{p}$ for some natural number k. Denote by ℓ the smallest natural number satisfying $q^{\nu \ell} \equiv -1 \pmod{p}$. Then $q^{2\nu \ell} \equiv 1 \pmod{p}$ and $q^{\nu \ell} \not\equiv 1 \pmod{p}$. It can be deduced that $\mathrm{ord}_p(q^\nu) = 2\ell$ is even. This proves "4) implies 1)". ∎

In the following corollary, we present the dual statement of Proposition 4.

Corollary 1 *Let p be an odd prime number with $p \neq q$ and let A be a finite abelian p-group. Then TFAE.*

1) $\mathrm{ord}_p(q^\nu)$ *is odd.*

2) $\mathrm{ord}_{p^i}(q^\nu)$ *is odd for all natural numbers i.*

3) $\chi(p^i, q^\nu) = 0$ *for all natural numbers i.*

4) $\{0\}$ *is the only q^ν-cyclotomic class of type I.*

For a finite abelian p-group A, it can be concluded that either every q^ν-cyclotomic class of A is of type I or $\{0\}$ is the unique q^ν-cyclotomic class of type I. The numbers r_I and r_{II} are given as follows.

Proposition 5 *Let p be an odd prime with $p \neq q$ and let A be a finite abelian p-group of exponent p^s.*

1) *If* $\mathrm{ord}_p(q^\nu)$ *is even, then*

$$r_I = 1 + \sum_{i=1}^{s} \frac{N_A(p^i)}{\mathrm{ord}_{p^i}(q^\nu)} \text{ and } r_{II} = 0.$$

2) *If* $\mathrm{ord}_p(q^\nu)$ *is odd, then*

$$r_I = 1 \text{ and } r_{II} = \sum_{i=1}^{s} \frac{N_A(p^i)}{2\mathrm{ord}_{p^i}(q^\nu)}.$$

Proof. First, we note that the orders of elements in A are of the form p^i for some integer i such that $0 \leq i \leq s$ and the set of all elements in A of order p^i can be viewed as a disjoint union of q^ν-cyclotomic classes of A of the same cardinality $\mathrm{ord}_{p^i}(q^\nu)$. Then the statements 1) and 2) follow from Proposition 4 and Corollary 1, respectively. ∎

Using (6), the simplification of the formulas in Proposition 5 is derived.

Corollary 2 *Let p be an odd prime number with $p \neq q$ and let A be a finite abelian p-group of exponent p^s. Let β be the largest integer such that $p^\beta | \left(q^{\nu \,\mathrm{ord}_p(q^\nu)} - 1\right)$.*

1) *If $\mathrm{ord}_p(q^\nu)$ is even, then*

$$r_I = 1 + \frac{1}{\mathrm{ord}_p(q^\nu)} \left(\sum_{i=1}^{\beta} \mathcal{N}_A(p^i) + \sum_{i=\beta+1}^{s} \frac{\mathcal{N}_A(p^i)}{p^{i-\beta}} \right) \text{ and } r_{II} = 0.$$

2) *If $\mathrm{ord}_p(q^\nu)$ is odd, then*

$$r_I = 1 \text{ and } r_{II} = \frac{1}{2\mathrm{ord}_p(q^\nu)} \left(\sum_{i=1}^{\beta} \mathcal{N}_A(p^i) + \sum_{i=\beta+1}^{s} \frac{\mathcal{N}_A(p^i)}{p^{i-\beta}} \right).$$

In the case where $\beta > s$, the empty sum will be referred to as zero.

Proof. From (6), we have

$$\mathrm{ord}_{p^i}(q^\nu) = \begin{cases} \mathrm{ord}_p(q^\nu) & \text{if } i \leq \beta, \\ p^{i-\beta}\,\mathrm{ord}_p(q^\nu) & \text{if } \beta < i. \end{cases}$$

The results can be derived directly from Proposition 5. ∎

Example 1 *Let $q = 7$, $\nu = 3$, and let $A := \mathbb{Z}_{11^2} \times \mathbb{Z}_{11}$. Then A has exponent 11^2 and order 11^3. Since $\mathrm{ord}_{11}(7^3) = 10$ is even, by Proposition 5, we have $r_{II} = 0$ and*

$$r_I = 1 + \sum_{i=1}^{2} \frac{\mathcal{N}_A(p^i)}{\mathrm{ord}_{p^i}(q^\nu)} = 1 + \frac{\mathcal{N}_A(11^1)}{\mathrm{ord}_{11}(7^3)} + \frac{\mathcal{N}_A(11^2)}{\mathrm{ord}_{11^2}(7^3)}.$$

By Lemma 1, we have $\mathcal{N}_A(11^1) = 120$ and $\mathcal{N}_A(11^2) = 1210$. Since $\mathrm{ord}_{11^2}(7^3) = 110$, it follows that

$$r_I = 1 + \frac{120}{10} + \frac{1210}{110} = 1 + 12 + 11 = 24.$$

Then $r_I + r_{II} = 24$ and the number of CDA codes in the group algebra $\mathbb{F}_{7^3}[\mathbb{Z}_{11^2} \times \mathbb{Z}_{11}]$ is 2^{24}.

4 CDA Codes: Products of 2-Groups and p-Groups

The enumeration of CDA codes is given in a more general setup. Precisely, we focus on a group algebra whose underlying abelian group is a product of a finite 2-group and a finite p-group.

4.1 CDA Codes: 2-Groups

We focus on CDA codes in a group algebra of a finite abelian 2-group. The characterization of such codes is presented together with their enumeration.

Proposition 6 *Let q be an odd prime number and let m be a natural number. Let B be a finite abelian 2-group of exponent 2^m. Let γ be the largest positive integer satisfying $2^\gamma|(q^\nu+1)$ and let $b \in B$. Then TFAE.*

1) $\mathrm{ord}(b) = 2^i$ *for some* $0 \le i \le \gamma$.

2) $S_{q^\nu}(b)$ *is a q^ν-cyclotomic class of type I.*

3) $\chi(\mathrm{ord}(b), q^\nu) = 1$.

In this case, $\mathrm{ord}(b) \in \{1, 2\}$ *or* $\mathrm{ord}_{\mathrm{ord}(b)}(q^\nu) = 2$.

Proof. Assume that $\mathrm{ord}(b) = 2^i$ for some $0 \le i \le \gamma$. Since $2^i|2^\gamma$ and $2^\gamma|(q^\nu+1)$, it follows that $\mathrm{ord}(b)|(q^\nu+1)$. Equivalently, $-b = q^\nu b$ which implies that $S_{q^\nu}(b) = S_{q^\nu}(-b)$ is of type I. This proves "1) implies 2)".

Assume that $S_{q^\nu}(b)$ is a q^ν-cyclotomic class of A of type I. It follows that $-b = q^{\nu k}b$ for some natural number k. Consequently, we have $\mathrm{ord}(b)|(q^{\nu k}+1)$. The statement "2) implies 3)" is proved.

Next, we prove the statement "3) implies 1)". Assume that $\chi(\mathrm{ord}(b), q^\nu) = 1$. Then $\mathrm{ord}(b)|(q^{\nu k}+1)$ for some natural number k. We write $\mathrm{ord}(b) = 2^i$ for some integer $i \ge 0$. If $i \in \{0, 1\}$, then $i \le \gamma$. Assume that $i \ge 2$. Then $2^2|(q^{\nu k}+1)$ which implies that k is odd. Since $q^{\nu k}+1 = (q^\nu+1)\sum_{j=0}^{k-1}(-q^\nu)^j$ and $\sum_{j=0}^{k-1}(-q^\nu)^j$ is odd, $2^i|(q^\nu+1)$. From the maximality of γ, we have $i \le \gamma$.

Finally, assume that $\mathrm{ord}(b) = 2^i$ for some $0 \le i \le \gamma$. If $i \in \{0, 1\}$, then $\mathrm{ord}(b) \in \{1, 2\}$. Assume that $\mathrm{ord}(b) = 2^i$ for some $2 \le i \le \gamma$. Then $2^2|(q^\nu+1)$ which implies that $2^2 \nmid (q^\nu-1)$. Hence, $2 = \mathrm{ord}_{2^2}(q^\nu) \le \mathrm{ord}_{2^i}(q^\nu) \le \mathrm{ord}_{2^\gamma}(q^\nu) = 2$. As desired, $\mathrm{ord}_{2^i}(q^\nu) = 2$. ∎

In the following corollary, we present the dual statement of Proposition 6.

Corollary 3 *Let q be an odd prime number and let m be a natural number. Let B be a finite abelian 2-group of exponent 2^m. Let γ be the largest positive integer such that $2^\gamma|(q^\nu+1)$ and let $b \in B$. Then TFAE.*

1) $\mathrm{ord}(b) = 2^i$ *for some* $\gamma < i \le m$.

2) $S_{q^\nu}(b)$ *is a q^ν-cyclotomic class of type II.*

3) $\chi(\mathrm{ord}(b), q^\nu) = 0$.

Using Proposition 6 and Corollary 3, the numbers r_I and r_{II} for a group algebra $\mathbb{F}_{q^\nu}[B]$ are presented.

Proposition 7 *Let q be an odd prime number and let m be a natural number. Let γ be the largest natural number satisfying $2^\gamma|(q^\nu+1)$ and let B be a finite abelian 2-group of exponent 2^m. Then*

$$r_I = \sum_{i=0}^{\gamma} \frac{\mathcal{N}_B(2^i)}{\mathrm{ord}_{2^i}(q^\nu)} = 1 + \mathcal{N}_B(2^1) + \sum_{i=2}^{\gamma} \frac{\mathcal{N}_B(2^i)}{2}$$

and

$$r_{II} = \sum_{i=\gamma+1}^{m} \frac{\mathcal{N}_B(2^i)}{2\mathrm{ord}_{2^i}(q^\nu)}.$$

In the case where $m < \gamma$, the empty sum will be regarded as zero.

Example 2 *Let $q = 7$, $\nu = 3$, and let $B := \mathbb{Z}_{2^4} \times \mathbb{Z}_{2^2}$. Then B has exponent 2^4 and order 2^6. Since $2^3 \| (7^3 + 1)$, we have $\gamma = 3$. By Proposition 7 and Lemma 1, it follows that*

$$r_I = \sum_{i=0}^{3} \frac{\mathcal{N}_B(2^i)}{\mathrm{ord}_{2^i}(7^3)} = 1 + \frac{3}{1} + \frac{12}{2} + \frac{16}{2} = 1 + 3 + 6 + 8 = 18$$

and

$$r_{II} = \sum_{i=4}^{4} \frac{\mathcal{N}_B(2^i)}{2\mathrm{ord}_{2^i}(7^3)} = \frac{32}{2 \cdot 2} = 8.$$

Then we have $r_I + r_{II} = 26$. Consequently, the number of CDA codes in the group algebra $\mathbb{F}_{7^3}[\mathbb{Z}_{2^4} \times \mathbb{Z}_{2^2}]$ is 2^{26}.

4.2 CDA Codes: Products of 2-Groups and p-Groups

We focus on CDA codes in $\mathbb{F}_{q^\nu}[B \times A]$ for all finite abelian p-groups A and for some finite abelian 2-group B of exponent 2^m. Precisely, the numbers r_I and r_{II} are presented for $m \leq \gamma$, where γ is the largest natural number satisfying $2^\gamma | (q^\nu + 1)$.

Proposition 8 *Let p be an odd prime number with $p \neq q$ and let m and s be natural numbers. Let γ be the largest natural number satisfying $2^\gamma | (q^\nu + 1)$. Let A be a finite abelian p-group of exponent p^s and let B be a finite abelian 2-group of exponent 2^m. If $m \leq \gamma$, then the following statements hold.*

1) *If $2 \| \mathrm{ord}_p(q^\nu)$, then*

$$r_I = \sum_{j=0}^{m} \sum_{i=0}^{s} \frac{\mathcal{N}_A(2^j p^i)}{\mathrm{ord}_{2^j p^i}(q^\nu)} \text{ and } r_{II} = 0.$$

2) *If $4 | \mathrm{ord}_p(q^\nu)$, then*

$$r_I = \sum_{i=0}^{s} \left(\frac{\mathcal{N}_A(p^i)}{\mathrm{ord}_{p^i}(q^\nu)} + \frac{\mathcal{N}_A(2p^i)}{\mathrm{ord}_{2p^i}(q^\nu)} \right) \text{ and } r_{II} = \sum_{j=2}^{m} \sum_{i=0}^{s} \frac{\mathcal{N}_A(2^j p^i)}{2\mathrm{ord}_{2^j p^i}(q^\nu)}.$$

3) *If $\mathrm{ord}_p(q^\nu)$ is odd, then*

$$r_I = \sum_{i=0}^{m} \frac{\mathcal{N}_B(2^i)}{\mathrm{ord}_{2^i}(q^\nu)} \text{ and } r_{II} = \sum_{j=1}^{m} \sum_{i=0}^{s} \frac{\mathcal{N}_A(2^j p^i)}{2\mathrm{ord}_{2^j p^i}(q^\nu)}.$$

Proof. Using Proposition 6, Proposition 7, and the number-theoretic property in [11, Proposition 2.3], the results are obtained. ∎

5 Conclusion and Remarks

In this article, CDA codes in group algebras have been revisited for some specific finite abelian groups. Additional algebraic properties of a group algebra of a finite abelian p-group and a group algebra of a finite abelian 2-group have been presented together the enumeration formula for their CDA codes. As applications, these results have been applied for the enumeration of CDA codes in a group algebra of an abelian group A which is a product of a finite p-group and a finite 2-group of exponent 2^m with $m \leq \gamma$, where γ is the largest natural number satisfying $2^\gamma | (q^\nu + 1)$. The enumeration formula for such CDA codes has been presented in a more precise form without any characteristic functions.

In general, it is of natural interest to extend the ideas in this article to cover the case where $m > \gamma$, or where the underlying abelian group is $A_1 \times A_2$ for some finite p_1-group A_1 and finite p_2-group A_2, where p_1 and p_2 are distinct odd prime numbers different from q.

Acknowledgements

The author would like to thank the anonymous referees for their helpful comments. This research was funded by National Research Council of Thailand and Silpakorn University under Research Grant N42A650381.

References

[1] Benson, S, Students ask the darnedest things: A result in elementary group theory, Math. Mag. **70**, 207–211 (1997).

[2] Berman, S. D, Semi-simple cyclic and abelian codes. Kibernetika **3**, 21–30 (1967).

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

[4] Carlet, C., Guilley, S, Complementary dual codes for countermeasures to side-channel attacks, Coding Theory and Applications **3**, 97–105 (2015).

[5] Carlet, C., Daif, A., Danger, J.L., Guilley, S., Najm, Z., Ngo, X.T., Portebouef, T., Tavernier, C, Optimized linear complementary codes implementation for hardware trojan prevention, In: Proceedings of European Conference on Circuit Theory and Design, 2015 August 24-26; Trondheim, Norway. Piscataway, USA: IEEE (2015).

[6] Chabanne, H, Permutation decoding of abelian codes, IEEE Trans. Inform. Theory **38**, 1826–1829 (1992).

[7] Ding, C., Kohel, D. R., Ling, S, Split group codes, IEEE Trans. Inform. Theory **46**, 485–495 (2000).

[8] Etesami, J., Hu, F., Henkel, W, LCD codes and iterative decoding by projections, a first step towards an intuitive description of iterative decoding, In: Proceedings of IEEE Globecom, 2011 December 5-9 ; Texas, USA. Piscataway, USA: IEEE (2011).

[9] Guenda, K., Jitman, S., Gulliver, T. A, Constructions of good entanglement-assisted quantum error correcting codes, Des. Codes Cryptogr. **86**, 121–136 (2018)

[10] Ishai, Y., Sahai, A., Wagner, D, Private circuits: securing hardware against probing attacks, In: *CRYPTO*, vol. 2729 of Lecture Notes in Computer Science, pages 463-481. Springer, August 1721 2003. Santa Barbara, CA, USA.

[11] Jitman, S., Correction to: Good integers and some applications in coding theory, Cryptography and Communications **10**, 1203–1203 (2018).

[12] Jitman, S., Ling, S., Liu, H., Xie, X, Abelian codes in principal ideal group algebras, IEEE Trans. Inform. Theory **59**, 3046–3058 (2013).

[13] Jitman, S., Ling, S., Solé, P, Hermitian self-dual Abelian codes. IEEE Trans. Inform. Theory **60**, 1496–1507 (2014).

[14] Massey, J.L, Linear codes with complementary duals, Discrete Mathematics **106/107** 337–342 (1992).

[15] Nathanson, M. B., *Elementary Methods in Number Theory*, (Springer, 2000).

[16] Rajan, B. S. , Siddiqi, M. U, Transform domain characterization of abelian codes, IEEE Trans. Inform. Theory **38**, 1817–1821 (1992).

[17] Sendrier, N, Linear codes with complementary duals meet the Gilber-Varshamov bound, Discrete Math **285**, 345–347 (2004).

[18] Yang, X., Massey, J.L, The condition for a cyclic code to have a complementary dual, Discrete Mathematics **126**, 391–393 (1994).