Palestine Journal of Mathematics

Vol 15(2)(2026) , 313–327

Generalised cyclotomic cosets and its application on LCD group codes

Ankan Shaw and Satya Bagchi

Communicated by: N. Abhilash

MSC 2020 Classifications: Primary 94B05; Secondary 20C05.

Keywords and phrases: Cyclotomic cosets, group code, LCD code, cyclic code.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

The first author would like to thank the Ministry of Education (MoE), Government of India, for financial support to carry out his research. This work is also supported by Science and Engineering Research Board (SERB), DST, India, Grant No. MTR/2021/000611.

Corresponding Author: Ankan Shaw

Abstract We investigate some new properties of p-cyclotomic cosets modulo n using a group-theoretic approach, where we remove all restrictions on n except $(n, p) = 1$. We introduce the notion of p-generalised cyclotomic cosets. A complete enumeration principle for p-generalised cyclotomic cosets is proposed. Using these results, we precisely calculate the number of binary finite abelian LCD group codes.

1 Introduction

The purpose of the present work is to investigate generalized cyclotomic cosets and to explore their applications to LCD (linear complementary dual) group codes. The initiation of such a study can be traced back to the fundamental work by Shannon [22]. LCD codes, originally introduced by Massey [19] and later revitalized through their relevance to cryptographic countermeasures and error correction, have been shown to possess important advantages in communication theory and information security. In particular, LCD codes play a central role in side–channel attack resistance [7] and admit rich algebraic characterizations and parametrizations [8]. Recent developments also demonstrate the significance of LCD structures in algebraic geometry codes [20] and in group codes with complementary duals [9].

Group codes themselves form a classical and evolving subject at the intersection of coding theory and computational group theory, with recent contributions addressing their performance [5], decoding algorithms [18], and structural analysis via coset enumeration techniques [10], [25], [33]. Over the past few years, several mathematicians have utilized cyclotomic cosets to study cyclic codes; see [35], [26], [30], [31], [32]. The explicit description of all q-cyclotomic cosets modulo p^n was obtained in [3, 23]. All q-cyclotomic cosets modulo p^m play a vital role in computing the weight distribution of various irreducible cyclic codes [24]. In order to determine the size and lower bounds for the minimum distance of cyclic codes, the properties of cyclotomic cosets have been extensively studied in the literature; see [10], [11], [34], [35], [17], [23], [28], [25]. In fact, these properties are useful in deriving efficient quantum codes [1], [2], [4], [6], [11], [13], [16], [27], [29]. To determine which binary cyclotomic cosets contain two consecutive integers, Mandelbaum [17] investigated the properties of these cosets. In [11], [23], [28], the authors studied the q-cyclotomic cosets (q-cosets for short) modulo $q^m - 1$. To determine the exact dimension of BCH codes with small designed distances, the authors in [1], [2] established conditions on q-cosets modulo n, where $n = q^m - 1$. This led to the construction of new families of quantum codes. They also used these properties to derive necessary and sufficient conditions for dual-containing (Euclidean and Hermitian) BCH codes. To construct

various new families of efficient quantum BCH codes, the authors in [13], [14], [15] studied the properties of both q-cosets and q^2-cosets. Cyclotomic cosets modulo the sum of two distinct prime powers were investigated in [21].

Motivated by these developments, our work introduces a generalized framework for cyclotomic cosets over direct products of cyclic groups and applies this framework to the construction and classification of LCD abelian group codes. The resulting theory extends classical cyclotomic methods (cf. [17], [28], [23]) and provides new structural insights into idempotent-based constructions of group codes. In this work, we study the p-cyclotomic cosets modulo n. Here, we remove all restrictions on n except the condition $(n, p) = 1$. We introduce the notion of generalized cyclotomic cosets and provide an enumeration of p-generalized cyclotomic cosets modulo n. These results are then applied to the study of abelian LCD group codes, in particular binary LCD group codes.

Throughout the text, the letter p signifies a prime, and n a positive integer with $\gcd(p, n) = 1$. The p-cyclotomic coset modulo n containing i is defined by

$$C_i = \{\, ip^j \pmod{n} \in \mathbb{Z}_n : j = 0, 1, 2, \dots \}.$$

A subset $\{i_1, \dots, i_t\}$ of $\mathbb{Z}_n$ is called a complete set of representatives of p-cyclotomic cosets modulo n if $C_{i_1}, C_{i_2}, \dots, C_{i_t}$ are distinct and

$$\bigcup_{j=1}^{t} C_{i_j} = \mathbb{Z}_n.$$

Furthermore, any two cyclotomic cosets are either equal or disjoint. Hence, $\{C_{i_1}, C_{i_2}, \dots, C_{i_t}\}$ forms a partition of $\mathbb{Z}_n$.

A linear code C of length n is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_p^n$. A linear code C of length n over $\mathbb{F}_p$ is said to be cyclic if a cyclic right shift of the components of a codeword in C is again a codeword in C. A linear code C is called a linear complementary dual (LCD) code if

$$C \cap C^{\perp} = \{\theta\}.$$

Let $\mathcal{G}$ be a finite group of order n with identity element $1_{\mathcal{G}}$. The group algebra $\mathbb{F}_p\mathcal{G}$ is the collection of all formal sums of the form

$$\mathbb{F}_p\mathcal{G} = \left\{ \sum_{g \in \mathcal{G}} a_g g : a_g \in \mathbb{F}_p \right\},$$

endowed with the binary operations $+$ and $*$. For $a = \sum_{g\in\mathcal{G}} a_g g$ and $b = \sum_{g\in\mathcal{G}} b_g g$ in $\mathbb{F}_p\mathcal{G}$, these operations are defined by

$$a + b = \sum_{g\in\mathcal{G}} (a_g + b_g) g \quad \text{and} \quad a * b = ab = \sum_{g,h\in\mathcal{G}} a_g b_h \, gh,$$

respectively. The support of an element $a \in \mathbb{F}_p\mathcal{G}$ is defined as

$$\mathrm{Supp}(a) = \{\, g \in \mathcal{G} \mid a_g \neq 0 \,\}.$$

Under these operations, $\mathbb{F}_p\mathcal{G}$ becomes an $\mathbb{F}_p$-vector space with the elements of $\mathcal{G}$ as a basis. In fact, $(\mathbb{F}_p\mathcal{G}, +, *)$ is a ring with identity. Therefore, $\mathbb{F}_p\mathcal{G}$ is an $\mathbb{F}_p$-algebra.

After ordering the elements of $\mathcal{G}$ as $g_0, g_1, \dots, g_{n-1}$, we define a map

$$\Phi : \mathbb{F}_p\mathcal{G} \to \mathbb{F}_p^n \quad \text{by} \quad \Phi(g_i) = e_{i+1}, \tag{1.1}$$

where $\{e_1, e_2, \dots, e_n\}$ is the standard basis of $\mathbb{F}_p^n$. Then Φ is an $\mathbb{F}_p$-vector space isomorphism. Hence, the group algebra $\mathbb{F}_p\mathcal{G}$ is isomorphic to $\mathbb{F}_p^n$ as an $\mathbb{F}_p$-vector space, allowing us to transfer many coding-theoretic properties from $\mathbb{F}_p^n$ to $\mathbb{F}_p\mathcal{G}$.

We extend Φ $\mathbb{F}_p$-linearly by

$$\Phi\left(\sum_{i=0}^{n-1} a_i g_i \right) = (a_0, a_1, \dots, a_{n-1}).$$

Note that the isomorphism Φ is not canonical, since it depends on the ordering of the elements of $\mathcal{G}$. Different orderings lead only to permutations of the coordinates; hence the corresponding codes are permutation equivalent.
A *right group code* $\mathcal{C}$ is a right ideal of the group algebra $\mathbb{F}_p\mathcal{G}$. If $\mathcal{G}$ is abelian (respectively, cyclic), then $\mathcal{C}$ is called an *abelian* (respectively, *cyclic*) group code. For an element $a = \sum_{g\in\mathcal{G}} a_g g \in \mathbb{F}_p\mathcal{G}$, we define its *adjoint* by

$$\widehat{a} := \sum_{g\in\mathcal{G}} a_g\, g^{-1}.$$

When $\mathcal{G} = \{g_0, g_1, \ldots, g_{n-1}\}$ and $a = \sum_{i=0}^{n-1} a_i g_i \in \mathbb{F}_p\mathcal{G}$, the scalars $a_i \in \mathbb{F}_p$ are called the coefficients of a, and the elements g_i are its group components.
Throughout this article, we assume that $\mathcal{G}$ is an abelian group and that $\mathcal{C} = e\,\mathbb{F}_p\mathcal{G}$ is an LCD group code.
In the next section, we present the counting principle for cyclotomic cosets and its properties. In Section 3, the case of binary cyclic LCD group codes is considered. We emphasize the notion of generalized cyclotomic cosets and their enumeration in Section 4. In Section 5, we compute binary LCD abelian group codes using generalized cyclotomic cosets. Finally, we provide several examples illustrating our results in Section 6. We conclude with some promising directions for future work.

2 Cyclotomic cosets

In this section we derive the cyclotomic coset with group theoretic approach. Throughout this section p, q are distinct primes, and $o(g)$ denotes the order of an element g in the group $\mathcal{G} = \mathbb{Z}_{q^l}$ for $l \in \mathbb{N}$. In this regard, we require the following lemma to serve our purpose.

Lemma 2.1. *Let s_i be the number of elements of order q^i in $\mathbb{Z}_{q^l}$ and let m_i be the smallest positive integer such that $q^i|(p^{m_i}+1)$ for $1 \le i \le l$. Then s_i is divisible by $2m_i$.*

Proof. We define $O_{q^i} = \{g \in \mathbb{Z}_{q^l} : o(g) = q^i\}$ for $0 \le i \le l$. Then $\mathbb{Z}_{q^l}$ forms partitions as follows:

$$\mathbb{Z}_{q^l} = O_1 \sqcup O_q \sqcup \cdots \sqcup O_{q^l}.$$

Here $|O_1| = 1$ and $|O_{q^i}| = s_i$ for $1 \le i \le l$. For $i \in \{1, 2, \ldots, l\}$ fixed, we define

$$O^1_{q^i} = \{x_1 \cdot q^{l-i}p^k \pmod{q^l} : k = 0, 1, \ldots, 2m_i - 1\}$$

with $x_1 = 1$. First, we prove that $O^1_{q^i} \subseteq O_{q^i}$. It is easy to see that

$$q^i\left(1 \cdot q^{l-i}p^k \pmod{q^l}\right) = q^l p^k \pmod{q^l} = 0 \pmod{q^l}. \tag{2.1}$$

Since $\gcd(p, q) = 1$, the integer q^i is the smallest integer that satisfies Equation (2.1). Otherwise, there would exist $1 \le j < i \le l$ such that

$$l - i + j \equiv 0 \pmod{l},$$

and hence

$$i \equiv j \pmod{l},$$

which is impossible because $i \ne j$ and $1 \le j < i \le l$. Consequently,

$$o\big(x_1\, q^{\,l-i}p^k\big) = q^i \text{ in } \mathbb{Z}_{q^l} \text{ for } k \in \{0, 1, \ldots, 2m_i - 1\}.$$

Hence, $O^1_{q^i} \subseteq O_{q^i}$.

Suppose there exist $k_1,\ k_2 \in \{0, 1, \ldots, 2m_i - 1\}$ such that $x_1 \cdot q^{l-i}p^{k_1} \pmod{q^l} = x_1 \cdot q^{l-i}p^{k_2} \pmod{q^l}$ with $k_1 > k_2$. Then $q^{l-i}(p^{k_1-k_2} - 1) \equiv 0 \pmod{q^l}$. Since $i \le l$, therefore, $p^{k_1-k_2} \equiv 1 \pmod{q^i}$. It implies that $-p^{k_1-k_2} \equiv p^{m_i} \pmod{q^i}$ as $q^i|(p^{m_i}+1)$. Consequently, $m_1 \ne k_1 - k_2$. Without loss of generality, let $m_i < k_1 - k_2$. Since $k_1,\ k_2 \in \{0, 1 \ldots 2m_i - 1\}$ and $m_1 \ne$

$k_1 - k_2$, therefore, $k_1 - k_2 - m_i < m_i$. Then $p^{m_i}(p^{k_1-k_2-m_i}+1) \equiv 0 \pmod{p^i}$. Consequently, $(p^{k_1-k_2-m_i}+1) \equiv 0 \pmod{p^i}$ as $\gcd(p,q) = 1$. Then we arrive at a contradiction as m_i be the smallest positive integer such that $q^i|(p^{m_i}+1)$ for $1 \leq i \leq l$. Hence, $|O^1_{q^i}| = 2m_i$. If $O_{q^i} \setminus O^1_{q^i} \neq \phi$, taking $x_2 \in O_{q^i} \setminus O^1_{q^i}$, we define

$$O^2_{q^i} = \{x_2 \cdot q^{l-i}p^k \pmod{q^l} \colon k = 0, 1, \ldots, 2m_i - 1\}.$$

Similarly, we get $O^2_{q^i} \subseteq O_{q^i}$. We claim that $O^1_{q^i} \cap O^2_{q^i} = \phi$. Suppose $y \in O^1_{q^i} \cap O^2_{q^i}$. Then, there exist some $k_1, k_2 \in \{0, 1, \ldots, 2m_i - 1\}$ such that $y = 1 \cdot q^{l-i}p^{k_1} \pmod{q^l}$ and $y = x_2 \cdot q^{l-i}p^{k_2} \pmod{q^l}$. This implies

$$x_2 = 1 \cdot p^{k_1-k_2} \pmod{q^l}.$$

Hence, $o(x_2) = q^l$. This concludes $x_2 \notin O_{q^i}$ when $i < l$; and $x_2 \in O^1_{q^i}$ when $i = l$, which are contradictions.
We observe that $|O^2_{q^i}| = 2m_i$. Similarly, choosing $x_j \in O_{q^i} \setminus (\sqcup_{t_i=1}^{j-1} O^{t_i}_{q^i})$ if $O_{q^i} \setminus (\sqcup_{t_i=1}^{j-1} O^{t_i}_{q^i}) \neq \phi$ and do the same process. In this way, we construct partitions $O^1_{q^i}, \ldots, O^{t_i}_{q^i}$ of O_{q^i}. Each $O^j_{q^i}$ has the same number of elements and $O_{q^i} = \sqcup_{j=1}^{t_i} O^j_{q^i}$. Therefore, $2m_it_i = s_i$ and this completes the proof. □

Lemma 2.2. *Let p and q be coprime positive integers, and let l be a positive integer. Let C_i be the p-cyclotomic coset modulo q^l containing i, defined by*

$$C_i = \left\{i \cdot p^k \bmod q^l : k = 0, 1, 2, \ldots\right\}.$$

Then every element of C_i has the same order in the additive group $\mathbb{Z}_{q^l}$.

Proof. Let $x \in C_i$ have order t in $\mathbb{Z}_{q^l}$, meaning t is the smallest positive integer such that

$$t \cdot x \equiv 0 \pmod{q^l}.$$

Since $x \in C_i$, there exists some $k_1 \in \mathbb{N} \cup \{0\}$ such that

$$x \equiv i \cdot p^{k_1} \pmod{q^l}.$$

Substituting this into the order condition yields

$$t \cdot i \cdot p^{k_1} \equiv 0 \pmod{q^l}.$$

As $\gcd(p,q) = 1$, the element p^{k_1} is invertible modulo q^l. Multiplying both sides by the inverse of p^{k_1} gives

$$t \cdot i \equiv 0 \pmod{q^l}.$$

Thus, t is the smallest positive integer satisfying $q^l \mid t \cdot i$, which depends only on i and q^l.

Now consider any other element $y \in C_i$, say $y \equiv i \cdot p^j \pmod{q^l}$ for some $j \geq 0$. Let t' be the order of y. Then

$$t' \cdot i \cdot p^j \equiv 0 \pmod{q^l}.$$

Again, since p^j is invertible modulo q^l, we obtain

$$t' \cdot i \equiv 0 \pmod{q^l}.$$

Hence, $t' \geq t$. Conversely, since $t \cdot i \equiv 0 \pmod{q^l}$, we have

$$t \cdot y = t \cdot i \cdot p^j \equiv 0 \pmod{q^l},$$

which implies $t' \mid t$, so $t' \leq t$. Therefore, $t' = t$, and all elements of C_i have the same order t. □

Theorem 2.3. *Let m_i be the smallest positive integer such that $q^i \mid (p^{m_i}+1)$ for $i \in \{1, 2, \ldots, l\}$. Then the number of p-cyclotomic cosets modulo q^l is*

$$1 + \sum_{i=1}^{l} \frac{s_i}{2m_i}.$$

Proof. It follows from the proof of Lemma 2.1, we get

$$\mathbb{Z}_{q^l} = O_1 \sqcup \left(\sqcup_{i=1}^{l} \sqcup_{j=1}^{t_i} O_{q^i}^j \right). \tag{2.2}$$

We claim, except O_1, each p-cyclotomic coset modulo q^l is of the form $O_{q^i}^j$ for some $i \in \{1, 2, \ldots, l\}$, $j \in \{1, 2, \ldots, t_i\}$. We know that each p-cyclotomic coset modulo q^l is of the form

$$C_i = \left\{ i \cdot p^k \pmod{q^l} \colon k = 0, 1, 2, \ldots \right\}.$$

We can easily see that $C_0 = O_1$. Since $(p, q) = 1$, therefore, it follows from the Lemma 2.2 that each element in C_i has the same order in $\mathbb{Z}_{q^l}$. Hence, there exists $j \in \{1, 2, \ldots, l\}$ such that $o(w) = q^j$ in $\mathbb{Z}_{q^l}$ for $w \in C_i$. Consequently, $C_i \subset O_{q^j}$ as O_{q^j} contains all elements of $\mathbb{Z}_{q^l}$ with order q^i. It follows from the proof of the Lemma 2.1 that $O_{q^i} = \sqcup_{j=1}^{t_i} O_{q^i}^j$. This implies that there exists $l_1 \in \mathbb{N}$ such that $C_i \cap O_{q^j}^{l_1} \neq \phi$.
Suppose $C_i \cap O_{q^j}^t$ and $C_i \cap O_{q^j}^k$ are non-empty for $t \neq k$. Then

$$x_t q^{l-j} p^{k_1} \equiv i \cdot p^{k_2} \pmod{q^l} \quad \text{and} \quad x_k q^{l-j} p^{k_3} \equiv i \cdot p^{k_4} \pmod{q^l}.$$

Consequently,

$$x_t q^{l-j} p^{k_1+k_4-k_2} \equiv x_k q^{l-j} p^{k_3} \pmod{q^l},$$

which shows that $O_{q^j}^t \cap O_{q^j}^k \neq \phi$ for $t \neq k$. Thus, we arrive at a contradiction. Hence, either $C_i \cap O_{q^j}^t = \emptyset$ or $C_i \cap O_{q^j}^k = \emptyset$ but not both. Without loss of generality, let $C_i \cap O_{q^j}^t \neq \emptyset$ for some $t \in \{1, 2, \ldots, t_j\}$. Since $C_i \subset O_{q^j}$, therefore, $C_i \subset O_{q^j}^t$. Let $u \in C_i$. Then $u \in O_{q^j}^t$. We know that u repeats after a cycle length $2m_j$ and all elements of C_i are of the same order in $\mathbb{Z}_{q^l}$. Hence, $C_i = O_{q^j}^t$. The remaining part of the proof follows from Lemma 2.1 and Equation (2.2). □

Remark 2.4. In light of the above facts, one can infer the cardinality of each cyclotomic coset from the proof of the theorem. Therefore, for any p-cyclotomic coset C_i, we have

$$|C_i| \in \{1, 2m_1, \ldots, 2m_l\}.$$

Applying Theorem 2.3, we have the following corollary.

Corollary 2.5. *Each $O_{q^i}^j$ is closed under inverses in $\mathbb{Z}_{q^l}$, i.e., each $O_{q^i}^j$ is closed under multiplication by $-1 \pmod{q^l}$.*

Proof. We have $O_{q^i}^j = \{x_j \cdot q^{l-i} p^k \pmod{q^l} \colon k = 0, 1, \ldots, 2m_i - 1\}$. It is easy to see that $x_j \cdot q^{l-i} p^{k_1+m_i} \pmod{q^l} \in O_{q^i}^j$ for $0 \leq k_1 \leq m_i - 1$. Now,

$$\begin{aligned} p^{m_i} &\equiv -1 \pmod{q^i} \\ \Rightarrow q^{l-i} p^{m_i} &\equiv -q^{l-i} \pmod{q^l} \\ \Rightarrow x_j q^{l-i} p^{m_i} p^{k_1} &\equiv -x_j q^{l-i} p^{k_1} \pmod{q^l}. \end{aligned}$$

This shows that $O_{q^i}^j = \{x_j \cdot q^{l-i} p^k \pmod{q^l} \colon k = 0, 1, \ldots, m_i - 1\} \cup \{x_j \cdot q^{l-i} p^{m_1+k} \pmod{q^l} \colon k = 0, 1, \ldots, m_i - 1\}$ and the result follows. □

Theorem 2.6. *(Euler's theorem) Suppose a and n are co-prime integers, and $\varphi(n)$ is a Euler's phi function. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Since $(p, q) = 1$ therefore, there exists the smallest $m_i \in \mathbb{N}$ such that $q^i | (p^{m_i} - 1)$ for $i \in \{1, 2, \ldots, l\}$ due to Euler's theorem.

Lemma 2.7. *Let s_i denote the number of elements of order q^i in $\mathbb{Z}_{q^l}$, and let m_i be the smallest positive integer such that $q^i \mid (p^{m_i} - 1)$ for $i \in \{1, 2, \ldots, l\}$. Then $m_i \mid s_i$.*

Proof. We define $O_{q^i} = \{g \in \mathbb{Z}_{q^l} : o(g) = q^i\}$ for $0 \leq i \leq l$. Then $\mathbb{Z}_{q^l}$ forms partitions as follows:

$$\mathbb{Z}_{q^l} = O_1 \sqcup O_q \sqcup \cdots \sqcup O_{q^l}.$$

Here $|O_1| = 1$ and $|O_{q^i}| = s_i$ for $1 \leq i \leq l$. For a fixed $i \in \{1, 2, \ldots, l\}$, we define

$$O^1_{q^i} = \{x_1 \cdot q^{l-i}p^k \pmod{q^l} : k = 0, 1, \ldots, m_i - 1\}$$

with $x_1 = 1$. First, we prove that $O^1_{q^i} \subseteq O_{q^i}$. It is easy to see that

$$q^i \left(1 \cdot q^{l-i}p^k \pmod{q^l}\right) = q^l p^k \pmod{q^l} = 0 \pmod{q^l}. \tag{2.3}$$

Since i is the smallest integer that satisfies Equation (2.3) and $\gcd(p, q) = 1$, therefore, $O^1_{q^i} \subseteq O_{q^i}$ and $|O^1_{q^i}| = m_i$. If $O_{q^i} \setminus O^1_{q^i} \neq \phi$, taking $x_2 \in O_{q^i} \setminus O^1_{q^i}$, we define

$$O^2_{q^i} = \{x_2 \cdot q^{l-i}p^k \pmod{q^l} : k = 0, 1, \ldots, m_i - 1\}.$$

Similarly, we can show that $O^2_{q^i} \subseteq O_{q^i}$. We claim that $O^1_{q^i} \cap O^2_{q^i} = \phi$. Suppose $y \in O^1_{q^i} \cap O^2_{q^i}$. Then, there exist some $k_1, k_2 \in \{0, 1, \ldots, m_i - 1\}$ such that $y = 1 \cdot q^{l-i}p^{k_1} \pmod{q^l}$ and $y = x_2 \cdot q^{l-i}p^{k_2} \pmod{q^l}$. This implies

$$x_2 = 1 \cdot p^{k_1 - k_2} \pmod{q^l}.$$

Hence, $o(x_2) = q^l$. This concludes that $x_2 \notin O_{q^i}$ when $i < l$; and $x_2 \in O^1_{q^i}$ when $i = l$, which are contradictions.
We observe that $|O^2_{q^i}| = m_i$. Similarly, choosing $x_j \in O_{q^i} \setminus (\sqcup_{t_i=1}^{j-1} O^{t_i}_{q^i})$, we construct partitions $O^3_{q^i}, O^4_{q^i}, \ldots, O^{t_i}_{q^i}$ of O_{q^i}. Each $O^j_{q^i}$ has the same number of elements and

$$O_{q^i} = \sqcup_{j=1}^{t_i} O^j_{q^i}.$$

Therefore, $m_i t_i = s_i$ and this completes the proof. □

As an application of Lemma 2.7, we get the following theorem.

Theorem 2.8. *Let s_i denote the number of elements of order q^i in $\mathbb{Z}_{q^l}$, and let m_i be the smallest positive integer such that $q^i \mid (p^{m_i} - 1)$ for $i \in \{1, 2, \ldots, l\}$. Then the number of p-cyclotomic cosets modulo q^l is*

$$1 + \sum_{i=1}^{l} \frac{s_i}{m_i}.$$

Proof. It follows from Lemma 2.7 that $s_i \mid m_i$. We have the partition of $\mathbb{Z}_{q^l}$ as follows:

$$\mathbb{Z}_{q^l} = O_1 \sqcup (\sqcup_{i=1}^{l} \sqcup_{j=1}^{t_i} O^j_{q^i}). \tag{2.4}$$

We claim that each p-cyclotomic coset modulo n is of the form O_1 or $O^j_{q^i}$ for some $i \in \{1, 2, \ldots l\}$, $j \in \{1, 2, \ldots t_i\}$. Now, each p-cyclotomic coset modulo n is of the form

$$C_i = \left\{i \cdot p^k \pmod{q^l} : k = 0, 1, \ldots\right\}.$$

It is straightforward that $C_0 = O_1$. Since $(p, q) = 1$, therefore, each element in C_i is of the same order in $\mathbb{Z}_{q^l}$. Thus, there exists $j \in \{1, 2, \ldots, l\}$ such that $C_i \subset O_{q^j}$. Hence, there exits $l_1 \in \mathbb{N}$ such that $C_i \cap O^{l_1}_{q^j} \neq \phi$.
Suppose $C_i \cap O^t_{q^j}$ and $C_i \cap O^k_{q^j}$ are non-empty for $t \neq k$. Then $x_t q^{l-j}p^{k_1} \pmod{q^l} = i \cdot p^{k_2} \pmod{q^l}$ and $x_k q^{l-j}p^{k_3} \pmod{q^l} = i \cdot p^{k_4} \pmod{q^l}$. Now,

$$\begin{aligned} x_t q^{l-j}p^{k_1-k_2+k_4} &\equiv i \cdot p^{k_4} \pmod{q^l} \\ \Rightarrow x_t q^{l-j}p^{k_1+k_4-k_2} &\equiv x_k q^{l-j}p^{k_3} \pmod{q^l}, \end{aligned}$$

which shows that $O^t_{q^j} \cap O^k_{q^j} \neq \phi$ for $t \neq k$. Hence, we arrive at a contradiction. Therefore, $C_i \subset O^t_{q^j}$ for some $t \in \{1, 2, \ldots, t_j\}$.
Let $u \in C_i$. Then $u \in O^t_{q^j}$. We know that u will come after a cycle of length m_i and all elements of C_i are of the same order. Hence, $C_i = O^t_{q^j}$. The remaining part of the proof follows from Lemma 2.7 and Equation (2.4). □

Remark 2.9. The proof of the aforementioned theorem can be used to find the cardinality of each cyclotomic coset under the aforementioned conditions. Therefore, for any p-cyclotomic coset C_i, $|C_i| \in \{1, m_1, \ldots, m_l\}$.

Corollary 2.10. *Suppose that $q^l \nmid (p^m + 1)$ for $m \in \mathbb{N}$. Then the inverse of any element of the subset $O^j_{q^i}$ of the group $\mathbb{Z}_{q^l}$ does not belong to $O^j_{q^i}$.*

Proof. We have $O^j_{q^i} = \{x_j \cdot q^{l-i}p^k \pmod{q^l} \colon k = 0, 1, \ldots, m_i - 1\}$. Suppose $x_j q^{l-i}p^{k_1} \pmod{q^l}$ has an inverse element of $\mathbb{Z}_{q^l}$ in $O^j_{q^i}$. Therefore, there exists $k_2 \in \mathbb{N}$ such that

$$\begin{aligned} x_j q^{l-i}p^{k_2} &\equiv -x_j q^{l-i}p^{k_1} \pmod{q^l} \\ \Rightarrow x_j q^{l-i}p^{k_1}(p^{k_2-k_1} + 1) &\equiv 0 \pmod{q^l}. \end{aligned}$$

This shows that $q^i \mid (p^{m_i} + 1)$ for some $m_i \in \mathbb{N}$, which is a contradiction. This completes the proof. □

3 Enumeration of binary cyclic LCD group codes via cyclotomic cosets

In this section, we give a counting principle for cyclic LCD group codes using cyclotomic cosets. Throughout this section, we consider $\mathcal{G}$ to be a finite cyclic group of odd order n generated by g, and $\mathcal{C} = e\mathbb{F}_2\mathcal{G}$ to be an LCD group code in $\mathbb{F}_2\mathcal{G}$. Suppose that $\mathcal{S} = \{C_{r_1}, C_{r_2}, \ldots, C_{r_t}\}$ is the complete set of t distinct 2-cyclotomic cosets modulo n. Now, we partition $\mathcal{G}$ into t parts such that

$$\mathcal{G} = \bigcup_{i=1}^{t} P_i,$$

where $P_i = \{g^j \colon j \in C_{r_i}\}$.

Suppose C_i is a 2-cyclotomic coset modulo n such that its elements are not closed under multiplication by $-1 \pmod{n}$. If the inverse of $a = i2^{k_1} \pmod{n} \in C_i$ is $b = j2^{k_2} \pmod{n} \in C_j$, then the inverse of $2a = i2^{k_1+1} \pmod{n} \in C_i$ is $2b = j2^{k_2+1} \pmod{n} \in C_j$. Therefore, for each C_i with cardinality m, there exists a C_j with the same cardinality such that $C_i \sqcup C_j$ is closed under multiplication by $-1 \pmod{n}$.
Before we proceed further, we would like to state a useful result from [9] that plays an important role in what follows.

Theorem 3.1. *[9, Theorem 3.1] Let $\mathcal{C}$ be a right ideal in $\mathbb{F}_p\mathcal{G}$. Then the following conditions are equivalent:*

(i) $\mathcal{C}$ is an LCD group code,

(ii) $\mathcal{C} = e\,\mathbb{F}_p\mathcal{G}$, where $e^2 = e = \hat{e}$.

Here, $\hat{e}$ denotes the adjoint of e in $\mathbb{F}_p\mathcal{G}$.

From this point onward, throughout the entire section, we assume that $\gcd(2, n) = 1$. We begin with the following lemma.

Lemma 3.2. *If $P_i \cap Supp(e) \neq \phi$, then $P_i \subseteq Supp(e)$.*

Proof. Suppose $h \in P_i \cap Supp(e)$. Therefore, there exists $l \in \mathbb{N} \cup \{0\}$ such that $h = g^{i2^l \pmod{n}} \in Supp(e)$. Then by the definition of P_i, we get $g^{i2^{l+j} \pmod{n}} \in P_i$ for all $j \in \mathbb{N} \cup \{0\}$. Since $e^2 = e$, therefore, $g^{i2^{l+j} \pmod{n}} \in Supp(e)$ and this completes the proof. □

We use this lemma to establish almost every result in this section.

Theorem 3.3. *Suppose $\mathcal{G}$ is a cyclic group of order n and $n \mid (2^j + 1)$ for some $j \in \mathbb{N}$. Then the number of non-zero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^t - 1$.*

Proof. It follows from Lemma 3.2, if $P_i \cap Supp(e) \neq \phi$, then $P_i \subseteq Supp(e)$ for all $i \in \{1, 2, \ldots, t\}$.

We observe that each P_i is closed under square. We will now show that each P_i is closed under inverses. Let $h \in P_i$. Then there exists $l \in \mathbb{N} \cup \{0\}$ such that $h = g^{i2^l \pmod n}$. Since $n \mid (2^j + 1)$ for some $j \in \mathbb{N}$, therefore, $2^j \equiv -1 \pmod n$. Then $g^{i2^{l+j} \pmod n}$ is the inverse of h, which belongs to P_i. Thus, P_i is closed under inverses. If we choose $Supp(e)$ as a union of any number of elements of $\mathcal{P} = \{P_1, P_2, \ldots, P_t\}$, then e satisfies the condition $e^2 = e = \hat{e}$. Since

$$\mathcal{G} = \bigcup_{i=1}^{t} P_i$$

consequently, we get total 2^t such $Supp(e)$. Thus, for each such $Supp(e)$, we can construct exactly one LCD group code in $\mathbb{F}_2\mathcal{G}$. Hence, the total number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $(2^t - 1)$. □

By the hypothesis and the structure of cyclotomic cosets, for each cyclotomic coset C_{r_i} with $|C_{r_i}| > 1$, there exists a distinct cyclotomic coset C_{r_j} with $|C_{r_j}| = |C_{r_i}|$ such that the union $C_{r_i} \cup C_{r_j}$ is closed under multiplication by 2 and under the inverse map. Consequently, the corresponding set $P_i \cup P_j$ in $\mathcal{G}$ is closed under squaring and taking inverses. This leads to the following lemma.

Lemma 3.4. *Suppose that $n \nmid (2^m + 1)$ for all $m \in \mathbb{N}$. Then every non-inverse-closed 2-cyclotomic coset occurs in a unique inverse pair.*

Theorem 3.5. *Suppose $\mathcal{G}$ is a cyclic group of order $n = p^s$ for any prime p and $n \nmid (2^m + 1)$ for all $m \in \mathbb{N}$. Then the number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^{\frac{t+1}{2}} - 1$.*

Proof. From Lemma 3.2, if $P_i \cap Supp(e) \neq \phi$, then $P_i \subseteq Supp(e)$ for all $i \in \{1, 2, \ldots, t\}$. It is easy to see that, each P_i is closed under square.
Next, we will show that any P_i with $|P_i| > 1$, $h^{-1} \notin P_i$ for all $h \in P_i$. Suppose there exists $m_1 \in \mathbb{N} \cup \{0\}$ such that $h_1 = g^{i2^{m_1} \pmod n} \in P_i$ has the inverse in P_i. Then there exists $m_2 \in \mathbb{N} \cup \{0\}$ with $h_2 = g^{i2^{m_2} \pmod n} \in P_i$ such that $h_1 h_2 = 1_{\mathcal{G}}$. This shows that

$$(2^{m_1} + 2^{m_2}) \equiv 0 \pmod n.$$

Since $(2, n) = 1$, therefore, from above we get $n \mid (2^{m_3} + 1)$ for some $m_3 \in \mathbb{N}$, which is a contradiction.
Since $n \nmid (2^m + 1)$ for all $m \in \mathbb{N}$, therefore, we get $P_i \cup P_j$ in $\mathcal{G}$, that is closed under square and inverses due to the Lemma 3.4.

Therefore, we have total $\frac{t-1}{2} + 1$ sets in $\mathcal{G}$ that are closed under square and inverses. As a result, there are $2^{\frac{t+1}{2}}$ such $Supp(e)$. For each $Supp(e)$, we obtain a uniquely determined LCD group code in $\mathbb{F}_2\mathcal{G}$. Hence, the total number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^{\frac{t+1}{2}} - 1$. □

Theorem 3.6. *Suppose that $\mathcal{G}$ is a cyclic group of order $n = q_1 q_2$, where q_1 and q_2 are primes, and $n \nmid (2^l + 1)$ for all $l \in \mathbb{N}$. If $q_2 \nmid (2^l + 1)$ for all $l \in \mathbb{N}$ and $q_1 \mid (2^m + 1)$ for some $m \in \mathbb{N}$, then the cyclotomic coset C_{q_2} is closed under inverses, whereas C_{q_1} is not.*

Proof. Let $x \in C_{q_2}$. Then there exists $l \in \mathbb{N} \cup \{0\}$ such that $x = q_2 2^l \pmod n$. Since $(n, 2) = 1$ and $q_1 \mid (2^m + 1)$ for some $m \in \mathbb{N}$, therefore, there exists $i \in \mathbb{N}$ such that $q_2 2^{l+i} \pmod n = -x \in C_{q_2}$. Hence, C_{q_2} is closed under inverses.
Let $l_1, l_2, l_3 \in \mathbb{N} \cup \{0\}$. To prove C_{q_1} is not closed under inverse, we suppose that $x = q_1 2^{l_1} \pmod n$ has the inverse in C_{q_1}. Then there exists $y = q_1 2^{l_2} \pmod n$ in C_{q_1} for some l_2 such that

$$x + y \equiv 0 \pmod n.$$

Consequently, $q_2 \mid (2^{l_3} + 1)$ for some $l_3 \in \mathbb{N}$, which is a contradiction. This completes the proof. □

Theorem 3.7. *Suppose $\mathcal{G}$ is a cyclic group of order $n = q_1q_2$, where q_1 and q_2 are odd primes, and $n \nmid (2^l + 1)$ for all $l \in \mathbb{N}$. If $q_1 \nmid (2^l + 1)$ and $q_2 \nmid (2^l + 1)$ for all $l \in \mathbb{N}$, then the cyclotomic cosets C_{q_1} and C_{q_2} are not closed under taking inverses.*

Proof. This proof follows from the last part of the proof of Theorem 3.6. □

Theorem 3.8. *Suppose that $\mathcal{G}$ is a cyclic group of order $n = q_1q_2$, where q_1 and q_2 are two odd primes and $n \nmid (2^l + 1)$ for all $l \in \mathbb{N}$. If $q_1 \mid (2^l + 1)$ for some $l \in \mathbb{N}$ and $q_2 \nmid (2^m + 1)$ for all $m \in \mathbb{N}$, then the number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^{\frac{t}{2}+1} - 1$.*

Proof. It follows from Lemma 3.2 that, if $P_i \cap Supp(e) \neq \phi$, then $P_i \subseteq Supp(e)$ for all $i \in \{1, 2, \ldots, t\}$. It is easy to see that, each P_i is closed under square. Now, P_{q_2} is closed under inverses due to Theorem 3.6. With similar arguments of Theorem 3.5, we conclude that, for any $P_i (\neq P_{q_2})$ with $| P_i | > 1$, $h^{-1} \notin P_i$ for all $h \in P_i$.
Since $n \nmid (2^l + 1)$ for all $l \in \mathbb{N}$, therefore, we get $P_i \cup P_j$ in $\mathcal{G}$, that is closed under square and inverses due to the Lemma 3.4.
Therefore, we have total

$$\frac{t-2}{2} + 2 = \frac{t}{2} + 1$$

sets in $\mathcal{G}$, that are closed under square and inverses. As a result, there are $2^{\frac{t}{2}+1}$ such $Supp(e)$. Each support Supp(e) determines exactly one LCD group code in $\mathbb{F}_2\mathcal{G}$. Hence, the total number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^{\frac{t+2}{2}} - 1$. □

Theorem 3.9. *Suppose that $\mathcal{G}$ is a cyclic group of order $n = q_1q_2$, where q_1 and q_2 are primes, and $n \nmid (2^m + 1)$ for all $m \in \mathbb{N}$. If $q_1 \nmid (2^m + 1)$ and $q_2 \nmid (2^m + 1)$ for all $m \in \mathbb{N}$, then the number of non-zero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^{\frac{t+1}{2}} - 1$.*

Proof. The proof follows from Theorem 3.7 and Theorem 3.8. □

The next theorem, in some sense, assimilates the above results. We need the following notations to serve our purpose. Now, consider the set

$$\mathcal{S}' = \{C_i : i \in U\},$$

where U is defined by

$$U = \left\{d_1 \in \mathbb{N} : n = d_1d_2,\ \ d_1 \nmid (2^l + 1) \ \text{ for all } \ l \in \mathbb{N},\ \ d_2 \mid (2^m + 1) \ \text{ some } \ m \in \mathbb{N} \ \text{ and } \ d_2 \in \mathbb{N}\right\}$$

It is clear that U serves as an indexing set for $\mathcal{S}'$, where $\mathcal{S}'$ is the collection of some cyclotomic cosets of $\mathcal{G}$ defined above.

Theorem 3.10. *Suppose $\mathcal{G}$ is a cyclic group of order n and $n \nmid (2^m + 1)$ for all $m \in \mathbb{N}$. Let t_1 be the cardinality of $\mathcal{S}'$. Then the number of nonzero cyclic LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^{\frac{t+t_1}{2}} - 1$.*

Proof. It follows from Lemma 3.2 that, if $P_i \cap Supp(e) \neq \phi$, then $P_i \subseteq Supp(e)$ for all $i \in \{1, 2, \ldots, t\}$. It is easy to see that, each P_i is closed under square. Consequently, each element in $\mathcal{S}$ is closed under multiplication by 2. Now, from the similar arguments of Theorem 3.6, each element in $\mathcal{S}'$ is closed under multiplication by -1 and 2. By the similar arguments of Theorem 3.7, each element in $\mathcal{S} \setminus \mathcal{S}'$ is not closed under multiplication by -1. Therefore, by the definition of the cyclotomic coset for each $C_j \in \mathcal{S} \setminus \mathcal{S}'$, there exists a coset $C_i \in \mathcal{S} \setminus \mathcal{S}'$ with the same cardinality of C_j such that $C_i \cup C_j$ is closed under multiplication by -1.
It is easy to see that the cardinality of $\mathcal{S} \setminus \mathcal{S}'$ is $t - t_1$. Thus, we get total

$$\frac{t-t_1}{2} + t_1 = \frac{t+t_1}{2}$$

number of sets containing elements of $\mathcal{G}$, which are closed under square and inverses. Therefore, we have total $2^{\frac{t+t_1}{2}}$ such $Supp(e)$, for which each $Supp(e)$ contributes exactly one LCD group code in $\mathbb{F}_2\mathcal{G}$. Hence, the total number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^{\frac{t+t_1}{2}} - 1$. □

4 Generalised cyclotomic cosets

In this section, we explore the structure of p-generalised cyclotomic cosets in order to obtain new properties of them. It is convenient to mention some notations to serve our purpose.
Suppose $\mathcal{G} := \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_s}$, and p-cyclotomic cosets modulo m_k is $C_i^k = \{i \cdot p^j \pmod{m_k} : j = 0, 1, 2, \ldots\}$, where $\gcd(m_k, p) = 1$ for all $k \in \{1, 2, \ldots, s\}$ with a prime p. Let us define the p-generalised cyclotomic cosets in $\mathcal{G}$ by

$$C_{i_1,i_2,\cdots,i_s} = \left\{\left(i_1 \cdot p^k \pmod{m_1}, \cdots, i_s \cdot p^k \pmod{m_s}\right) : k = 0, 1, 2, \ldots\right\}.$$

Throughout what follows, we occasionally denote cyclotomic cosets by C_i and C'_j, and their meaning is always specified when used. We also fix particular values of indices such as i_1 and i_2 when required for certain results.

Lemma 4.1. *Any p-generalised cyclotomic cosets $C_{i_1,i_2,\cdots,i_s}$ in $\mathcal{G}$ is closed under inverses if and only if all $C^1_{i_1}, C^2_{i_2}, \cdots, C^s_{i_s}$ are closed under inverses.*

Proof. Suppose $C_{i_1,i_2,\cdots,i_s}$ is closed under inverses. Therefore, for all $h \in C_{i_1,i_2,\cdots,i_k}$, $h^{-1} = -h \in C_{i_1,i_2,\cdots,i_k}$. Let $h = (h_1, h_2, \cdots, h_s) \in C_{i_1,i_2,\cdots,i_s}$. Then $h_j \in C^j_{i_j}$ for $j \in \{1, 2, \ldots, s\}$. Now, $-h \in C_{i_1,i_2,\cdots,i_s}$ and consequently $-h_j \in C^j_{i_j}$ for $j \in \{1, 2, \ldots, s\}$. Hence, $C_{i_1,i_2,\cdots,i_k}$ is closed under inverses. Converse part follows in the similar way. □

Lemma 4.2. *[34] Let m and n be two natural numbers. Then $mn = \gcd(m, n)\, lcm(m, n)$.*

Lemma 4.3. *Let $\mathcal{G} := \mathbb{Z}_n \times \mathbb{Z}_m$ for some $n, m \in \mathbb{N} \setminus p\mathbb{N}$ with $n, m > 1$. Suppose $\mathbb{Z}_n = C_{r_1} \sqcup C_{r_2} \sqcup \cdots \sqcup C_{r_k}$ and $\mathbb{Z}_m = C'_{s_1} \sqcup C'_{s_2} \sqcup \cdots \sqcup C'_{s_l}$ with $|C_{r_i}| = n_i$ and $|C'_{s_j}| = m_j$ for $i \in \{1, 2, \ldots, k\}$ and $j \in \{1, 2, \ldots, l\}$. Then*

$$nm = \sum_{i=1}^{k} \sum_{j=1}^{l} \gcd(n_i, m_j) lcm(n_i, m_j).$$

Proof. We have $\mathbb{Z}_n = \bigsqcup_{i=1}^{k} C_{r_i}$ and $\mathbb{Z}_m = \bigsqcup_{j=1}^{l} C'_{r_j}$. Then $n = \sum_{i=1}^{k} n_i$ and $m = \sum_{j=1}^{l} m_j$. Then

$$\begin{aligned} nm &= \Big(\sum_{n=1}^{k} n_i\Big)\Big(\sum_{n=1}^{l} m_j\Big) \\ &= \sum_{i=1}^{k} \sum_{j=1}^{l} n_i m_j \\ &= \sum_{i=1}^{k} \sum_{j=1}^{l} \gcd(n_i, m_j) lcm(n_i, m_j) \qquad \text{(by Lemma 4.2).} \end{aligned}$$

□

Now, we will consider group $\mathcal{G} = \mathbb{Z}_n \times \mathbb{Z}_m$, where p-generalised cyclotomic cosets in $\mathcal{G}$ by

$$C_{i_1,i_2} = \left\{\left(i_1 \cdot p^k \pmod{n}, i_2 \cdot p^k \pmod{m}\right) : k = 0, 1, 2, \ldots\right\}.$$

Lemma 4.4. *Suppose $C_r = \{r(= rp^k), rp, \ldots, rp^{k-1}\}$ in $\mathbb{Z}_n$ and $C'_s = \{s, sp, \ldots, sp^{l-1}\}$ in $\mathbb{Z}_m$. Let $t = \gcd(k, l)$ and $t_1 = lcm(k, l)$. Then $|C_{r,sp^i}| = t_1$ for all $1 \le i \le t$ and $\sqcup_{i=1}^{t} C_{r,sp^i} = \{(x, y) : x \in C_r, y \in C'_s\}$.*

Proof. We have $C_r = \{(rp^i \pmod{n}) : i = 0, 1, \cdots\} = \{r \pmod{n}, \cdots, rp^{k-1} \pmod{n}\}$ in $\mathbb{Z}_n$ and $C'_s = \{(sp^i \pmod{m}) : i = 0, 1, \cdots\} = \{s \pmod{m}, \cdots, sp^{l-1} \pmod{m}\}$ in $\mathbb{Z}_m$. It follows from the Lemma 4.2 that, $kl = \gcd(k, l) lcm(k, l)$. Now, $C_{r,p^i} = \{(rp^j \pmod{n}, sp^j \pmod{m}) : j = 0, 1, 2, \ldots\}$. Suppose $|C_{r,sp^i}| = t_2$. Therefore, $rp^{t_2} \pmod{n} = r \pmod{n}$ and $sp^{t_2} \pmod{m} = s \pmod{m}$. Consequently,

$$rp^{t_2} \equiv r \pmod{n} \quad \text{and} \quad sp^{t_2} \equiv s \pmod{m}.$$

This leads to conclude that $t_2 = lcm(k,l) = t_1$. Hence, $|C_{r,sp^i}| = lcm(k,l)$.
Next, we claim that $C_{r,sp^i} \cap C_{r,sp^j} = \emptyset$ for $i,j \in \{1,2,\ldots,t\}$ with $i \neq j$. Suppose $z \in (C_{r,sp^i} \cap C_{r,sp^j})$ for $i \neq j$. Therefore, there exist $k_2 \in \{0,1,\ldots,k-1\}$ and $k_3 \in \{0,1,\ldots,l-1\}$ such that $z = (rp^{k_2}, sp^i p^{k_2}) = (rp^{k_3}, sp^j p^{k_3})$. Consequently,

$$k_2 = k_3 \quad \text{and} \quad sp^i p^{k_2} = sp^j p^{k_3}.$$

Since $k_2 = k_3$, therefore, $i = j$ which contradicts that $i \neq j$. Hence, $C_{r,sp^i} \cap C_{r,sp^j} = \emptyset$ for $i \neq j$. Since $|C_{r,sp^i}| = t_1$ and $C_{r,sp^i} \subseteq (C_r \times C'_s)$ for all $i \in \{1,2,\ldots,t\}$, therefore, $tt_1 = kl$. Hence, $\sqcup_{i=1}^{t} C_{r,sp^i} = \{(x,y) \colon x \in C_r, y \in C'_s\}$. □

The preceding discussion demonstrates that if C_r is a p-cyclotomic coset in $\mathbb{Z}_n$ and C'_s is a p-cyclotomic coset in $\mathbb{Z}_m$, then their Cartesian product $C_r \times C'_s$ need not constitute a p-generalised cyclotomic coset in $\mathbb{Z}_n \times \mathbb{Z}_m$. In fact, the set $C_r \times C'_s$ admits a partition into p-generalised cyclotomic cosets of $\mathbb{Z}_n \times \mathbb{Z}_m$, yielding the decomposition

$$C_r \times C'_s = \bigsqcup_{i=1}^{t} C_{r,sp^i},$$

where each C_{r,sp^i} is a p-generalised cyclotomic coset in $\mathbb{Z}_n \times \mathbb{Z}_m$. The next result illustrates the utility of the above lemma.

Theorem 4.5. *Suppose $\mathbb{Z}_n = \bigsqcup_{i=1}^{k} C_{r_i}$ and $\mathbb{Z}_m = \bigsqcup_{j=1}^{l} C'_{s_j}$ are the decompositions into p-cyclotomic cosets with $|C_{r_i}| = n_i$ and $|C'_{s_j}| = m_j$. Then, for each pair (i,j), there exist exactly $\gcd(n_i, m_j)$ p-generalised cyclotomic cosets of $\mathbb{Z}_n \times \mathbb{Z}_m$ that partition $C_{r_i} \times C'_{s_j}$, and each of these cosets has cardinality $\operatorname{lcm}(n_i, m_j)$.*

Proof. Fix indices i and j with $1 \leq i \leq k$ and $1 \leq j \leq l$. Consider the p-cyclotomic coset C_{r_i} in $\mathbb{Z}_n$ of size n_i and the p-cyclotomic coset C'_{s_j} in $\mathbb{Z}_m$ of size m_j.
Apply Lemma 4.4 with the following parameters:

$$C_r = C_{r_i},\ C'_s = C'_{s_j},\ k = n_i,\ l = m_j.$$

Then by Lemma 4.4: $t = \gcd(n_i, m_j)$, $t_1 = \operatorname{lcm}(n_i, m_j)$. Now, it follows from the Lemma 4.4 that

(i) $C_{r_i} \times C'_{s_j}$ is partitioned into exactly $t = \gcd(n_i, m_j)$ distinct p-generalised cyclotomic cosets of the form $C_{r_i, s_j p^i}$ (for $i = 1,\ldots,t$).

(ii) Each of these cosets has cardinality $t_1 = \operatorname{lcm}(n_i, m_j)$.

This completes the proof for each fixed pair (i,j). Since the original groups decompose as disjoint unions of these cosets, the result holds globally. □

Theorem 4.6. *Let p be a prime and $m,n > 1$ be integers with $p \nmid m$ and $p \nmid n$. Consider the group $\mathcal{G} := \mathbb{Z}_n \times \mathbb{Z}_m$. Suppose we have partitions:*

$$\mathbb{Z}_m = C_{r_1} \sqcup C_{r_2} \sqcup \cdots \sqcup C_{r_k} \quad \text{and} \quad \mathbb{Z}_n = C'_{s_1} \sqcup C'_{s_2} \sqcup \cdots \sqcup C'_{s_l},$$

where $|C_{r_i}| = n_i$ for $i = 1,\ldots,k$ and $|C'_{s_j}| = m_j$ for $j = 1,\ldots,l$. Define $w_{ij} = \gcd(n_i, m_j)$ for each i,j. Then the group decomposes as:

$$\mathbb{Z}_n \times \mathbb{Z}_m = \bigsqcup_{i=1}^{k} \bigsqcup_{j=1}^{l} \bigsqcup_{t=0}^{w_{ij}-1} C_{r_i, s_j p^t}.$$

Proof. The proof follows from Lemma 4.4 and Theorem 4.5. □

Remark 4.7. Suppose $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2 \times \cdots \times \mathcal{G}_r$, where $\mathcal{G}_i = \mathbb{Z}_{n_i}$, $1 \leq i \leq r$. Let us define $H_1 = \mathcal{G}_1$, $H_i = H_{i-1} \times \mathcal{G}_i$ for $2 \leq i \leq r$. We can calculate the total number of p-generalised cyclotomic cosets of H_2 using Theorem 4.6. Applying Theorem 4.6 once more, we find the exact number of p-generalised cyclotomic cosets of H_3. Thus, in a similar way, we deduce the total number of p-generalised cyclotomic cosets of $H_r = \mathcal{G}$ due to Theorem 4.6. Moreover, we obtain an explicit description of all p-generalised cyclotomic cosets of $\mathcal{G}$. Thus, using Lemma 4.1, we can also get the p-generalised cyclotomic cosets that are closed under inverses.

5 Enumeration of binary LCD abelian group codes via generalised cyclotomic cosets

Let S be the complete set of p-generalised cyclotomic cosets in a finite abelian group $\mathcal{G}$ and let $|\mathcal{G}| = n$.

Theorem 5.1. *Let $\mathcal{G} := \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ be such that $n \mid (2^m + 1)$ for some $m \in \mathbb{N} \cup \{0\}$. Let t be the number of 2-generalised cyclotomic cosets in $\mathcal{G}$. Then the number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $2^t - 1$.*

Proof. It follows from Corollary 2.5 and Lemma 4.1 that each generalised p-modulo cyclotomic coset is closed under multiplication by 2 and -1. If we choose $Supp(e)$ as a union of any number of elements of 2-generalised cyclotomic cosets in $\mathcal{G}$, then e satisfies the condition $e^2 = e = \hat{e}$. Consequently, we get total 2^t such $Supp(e)$. Thus, for each such $Supp(e)$, we construct exactly one LCD group code in $\mathbb{F}_2\mathcal{G}$. Hence, the total number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is $(2^t - 1)$. □

Now we consider the case in which $n \nmid (2^m + 1)$ for all $m \in \mathbb{N} \cup \{0\}$. By Lemma 4.1, if any one of $C^1_{i_1}, C^2_{i_2}, \ldots, C^s_{i_s}$ fails to be closed under inversion, then $C_{i_1,i_2,\ldots,i_s}$ is not closed under inversion in $\mathcal{G}$. From the results of Section 3, we can determine which cyclotomic cosets are closed under inversion. Without loss of generality, assume that $C^1_{i_1}, C^2_{i_2}, \ldots, C^{s_1}_{i_{s_1}}$ are not closed under inversion, whereas $C^{s_1+1}_{i_{s_1+1}}, \ldots, C^s_{i_s}$ are closed under inversion.

Then there exist

$$C^1_{j_1},\ C^2_{j_2},\ \ldots,\ C^{s_1}_{j_{s_1}}$$

such that

$$C^1_{i_1} \sqcup C^1_{j_1},\ \ldots,\ C^{s_1}_{i_{s_1}} \sqcup C^{s_1}_{j_{s_1}}$$

are closed under inversion, by Lemma 3.4, where $1 \leq s_1 \leq s$. Therefore,

$$C_{i_1,i_2,\ldots,i_s} \ \sqcup\ C_{j_1,j_2,\ldots,j_{s_1},i_{s_1+1},\ldots,i_s}$$

is closed under inversion in $\mathcal{G}$.

Theorem 5.2. *Let $\mathcal{G} := \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ such that $n \nmid (2^m + 1)$ for all $m \in \mathbb{N} \cup \{0\}$. Let t be the total number of 2-generalised cyclotomic cosets in $\mathcal{G}$ and let t_1 be the number of 2-generalised cyclotomic cosets that are not closed under inverses. Then the number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is*

$$2^{\frac{2t-t_1}{2}} - 1.$$

Proof. The proof is analogous to that of Theorem 3.10, making use of Remark 4.7. □

6 Examples

In this section, we provide some examples of our concerning results.

Example 6.1. Let us consider $\mathcal{G} = \mathbb{Z}_9$. The order of $\mathcal{G}$ is 9, and we note that

$$9 \mid (2^3 + 1).$$

We now partition $\mathbb{Z}_9$ into its 2-cyclotomic cosets modulo 9. The three such cosets are

$$C_0 = \{0\}, \qquad C_1 = \{1, 2, 4, 5, 7, 8\}, \qquad C_3 = \{3, 6\}.$$

Since $2^3 \equiv -1 \pmod 9$, it follows that

$$2^4 \equiv -2 \equiv 7 \pmod 9, \qquad 2^5 \equiv -4 \equiv 5 \pmod 9, \qquad 2^6 \equiv -8 \equiv 1 \pmod 9.$$

Moreover,

$$3 \cdot 2^3 \equiv -3 \pmod 9,$$

which implies $6 \equiv -3 \pmod 9$. Hence the three 2-cyclotomic cosets modulo 9 may also be written as

$$C_0 = \{0\}, \qquad C_1 = \{1, 2, 4, -1, -2, -4\}, \qquad C_3 = \{3, -3\}.$$

Suppose that $\mathcal{G} = \langle g \rangle$. If we choose

$$\mathrm{Supp}(e) = \{g^i : i \in C_j\} \quad \text{for any } j \in \{0, 1, 3\},$$

then $e^2 = e = \widehat{e}$ in the group algebra $\mathbb{F}_2\mathcal{G}$. Hence the code $\mathcal{C} = e\,\mathbb{F}_2\mathcal{G}$ is an LCD group code. Similarly, if we choose

$$\mathrm{Supp}(e) = \{g^i : i \in C_j \cup C_k\} \quad \text{for any } j, k \in \{0, 1, 3\},$$

or

$$\mathrm{Supp}(e) = \{g^i : i \in C_0 \cup C_1 \cup C_3\},$$

then again $e^2 = e = \widehat{e}$ in $\mathbb{F}_2\mathcal{G}$. Thus, each such idempotent e produces an LCD group code. Therefore, the total number of nonzero LCD group codes in $\mathbb{F}_2\mathbb{Z}_9$ is

$$7 = 2^3 - 1.$$

Example 6.2. Suppose $\mathcal{G} = \mathbb{Z}_4 \times \mathbb{Z}_8$. We determine the number of generalised 3-cyclotomic cosets of $\mathcal{G}$.
First, we decompose the components

$$\mathbb{Z}_4 = C_0 \sqcup C_1 \sqcup C_2 = \{0\} \sqcup \{1, 3\} \sqcup \{2\},$$

$$\mathbb{Z}_8 = C'_0 \sqcup C'_1 \sqcup C'_2 \sqcup C'_4 \sqcup C'_5 = \{0\} \sqcup \{1, 3\} \sqcup \{2, 6\} \sqcup \{4\} \sqcup \{5, 7\}.$$

Cosets in $\mathbb{Z}_4$	Elements
C_0	$\{0\}$
C_1	$\{1, 3\}$
C_2	$\{2\}$

Cosets in $\mathbb{Z}_8$	Elements
C'_0	$\{0\}$
C'_1	$\{1, 3\}$
C'_2	$\{2, 6\}$
C'_4	$\{4\}$
C'_5	$\{5, 7\}$

Table 1. Cyclotomic cosets of $\mathbb{Z}_4$ and $\mathbb{Z}_8$ (base-3)

By Theorem 4.6, the generalised 3-cyclotomic cosets of $\mathcal{G} = \mathbb{Z}_4 \times \mathbb{Z}_8$ can be written as

$$\mathcal{G} = \bigsqcup_{i=1}^{k} \bigsqcup_{j=1}^{l} \bigsqcup_{t=0}^{w_{ij}-1} C_{r_i, 3^t s_j},$$

where $k = 3$ and $l = 4$. In particular,

$$\mathcal{G} = (C_{0,0} \sqcup C_{1,0} \sqcup C_{2,0} \sqcup C_{0,1} \sqcup C_{0,2} \sqcup C_{0,4} \sqcup C_{0,5} \sqcup C_{2,1} \sqcup C_{2,2} \sqcup C_{2,4} \sqcup C_{2,5}) \sqcup \bigsqcup_{i=1}^{7} C_{1,i}.$$

Thus, using Theorem 4.5 together with Table 6.2, the number of generalised 3-cyclotomic cosets of $\mathcal{G}$ is $2\,(\gcd(1,1) + \gcd(1,2) + \gcd(1,2) + \gcd(1,1) + \gcd(1,2)) + \gcd(2,1) + \gcd(2,2) + \gcd(2,2) + \gcd(2,1) + \gcd(2,2) = 18$. Hence, $\mathcal{G}$ has exactly 18 generalised 3-cyclotomic cosets.

Example 6.3. Consider the non-cyclic abelian group

$$\mathcal{G} = \mathbb{Z}_7 \times \mathbb{Z}_7.$$

Since

$$\mathbb{Z}_7 = \{0\} \sqcup \{1, 2, 4\} \sqcup \{3, 6, 5\} = C_0 \sqcup C_1 \sqcup C_3,$$

the group $\mathcal{G}$ decomposes into the generalized 2-cyclotomic cosets

$$\mathcal{G} = (C_{0,0} \sqcup C_{0,1} \sqcup C_{0,3} \sqcup C_{1,0} \sqcup C_{3,0}) \sqcup_{i=1}^{6} C_{1,i} \sqcup_{i=1}^{6} C_{3,i}.$$

Therefore, the total number of generalized 2-cyclotomic cosets of $\mathcal{G}$ is 17. Applying Theorem 5.2, the number of self-adjoint idempotent elements in $\mathbb{Z}_2\mathcal{G}$ is

$$1 + \frac{(17-1)}{2} = 9,$$

and hence the number of nonzero LCD group codes in $\mathbb{F}_2\mathcal{G}$ is

$$2^9 - 1 = 511.$$

Using GAP, we compute the 2-cyclotomic cosets in each of the non-cyclic abelian groups $\mathcal{G}$ listed below. The computational results are fully consistent with the theoretical predictions established in the preceding section. The following table presents the number of 2-generalised cyclotomic cosets for several examples, listed according to the size of the underlying group.

Group $\mathcal{G}$	**Order $\lvert\mathcal{G}\rvert$**	**Number of 2-generalised cosets of $\mathcal{G}$**
$\mathbb{Z}_{17} \times \mathbb{Z}_{17}$	289	37
$\mathbb{Z}_{19} \times \mathbb{Z}_{57}$	1083	62
$\mathbb{Z}_{37} \times \mathbb{Z}_{37}$	1369	39
$\mathbb{Z}_{27} \times \mathbb{Z}_{54}$	1458	51
$\mathbb{Z}_{27} \times \mathbb{Z}_{81}$	2187	80

Table 2. Number of 2-generalised cosets sorted by group order.

7 Conclusion

In this paper, we present an enumeration of cyclotomic cosets and their properties. We illustrate that the cyclotomic cosets play a crucial role in calculating binary abelian LCD group codes. Our study culminates by introducing the notion of generalised cyclotomic cosets and their application to binary abelian LCD group codes. For every finite abelian group, we determine the precise number of binary LCD group codes. We furnish several examples and remarks concerning our results. A possible direction for future research is to consider our approach to enumerating all LCD group codes of $\mathbb{F}_{p^n}\mathcal{G}$, where $\mathcal{G}$ is any finite non-commutative group.

References

[1] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, *Primitive quantum BCH codes over finite fields*, in *Proc. Int. Symp. Inform. Theory (ISIT)*, 1114-1118, (2006).

[2] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, *On quantum and classical BCH codes*, IEEE Trans. Inform. Theory, **53(3)**, 1183-1188, (2007).

[3] S. Arora and S. Pruthi, *Minimal cyclic codes of length* $2p^n$, Finite Fields Appl., **5**, 177-187, (1999).

[4] A. Ashikhmin and E. Knill, *Non-binary quantum stabilizer codes*, IEEE Trans. Inform. Theory, **47(7)**, 3065–3072, (2001).

[5] M. Borello and W. Willems, *Group codes over fields are asymptotically good*, Finite Fields Appl., **68**, 101738, (2020).

[6] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, *Quantum error correction via codes over* $GF(4)$, IEEE Trans. Inform. Theory, **44(4)**, 1369-1387, (1998).

[7] C. Carlet and S. Guilley, *Complementary dual codes for counter-measures to side-channel attacks*, Advances Math. Commun., **10(1)**, 131-150, (2016).

[8] C. Carlet, S. Mesnager, C. Tang and Y. Qi, *New characterization and parametrization of LCD codes*, IEEE Trans. Inform. Theory, **65(1)**, 39-49, (2019).

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

[10] P. Diaconis and M. Simper, *Statistical enumeration of groups by double cosets*, J. Algebra, **607**, 214-246, (2022).

[11] D. Yue, Z. Hu, *On the dimension and minimum distance of BCH codes over $GF(q)$*, Chin. J. Electron., **18**, 263-269, (1996).

[12] L. Gálvez, J. L. Kim, N. Lee, Y. G. Roe, B. S. Won, *Some bounds on binary LCD codes*, Cryptography and Communications, **10(4)**, 719-728, (2018).

[13] G. G. L. Guardia, *New quantum MDS codes*, IEEE Trans. Inform. Theory, **57(8)**, 5551-5554, (2011).

[14] G. G. L. Guardia, *On the construction of nonbinary quantum BCH codes*, IEEE Trans. Inform. Theory, **60(3)**, 1528-1535, (2014).

[15] G. G. L. Guardia, R. Palazzo Jr., *Constructions of new families of nonbinary CSS codes*, Discrete Math., **310**, 2935-2945, (2010).

[16] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory, **52(11)**, 4892-4914, (2006).

[17] D. M. Mandelbaum, *Two applications of cyclotomic cosets to certain BCH codes*, IEEE Trans. Inform. Theory, **26**, 737-738, (1980).

[18] C. Martínez, F. Molina and A. Piñera-Nicolás, *Decoding algorithms in group codes*, Finite Fields Appl., **108**, 102692, (2025).

[19] J. L. Massey, *Linear codes with complementary duals*, Discrete Math., **106/107**, 337-342, (1992).

[20] S. Mesnager, C. Tang and Y. Qi, *Complementary dual algebraic geometry codes*, IEEE Trans. Inform. Theory, **64(4)**, 2390-2397, (2018).

[21] A. Sahni and P. T. Sehgal, *Cyclic codes of length $p^n q$*, Finite Fields Appl., **18**, 1017-1036, (2012).

[22] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J., **27**, 379-423, (1948).

[23] A. Sharma, G. K. Bakshi, V. C. Dumir and M. Raka, *Cyclotomic numbers and primitive idempotents in the ring $GF(q)/(x^{p^n}-1)$*, Finite Fields Appl., **10**, 653-673, (2004).

[24] K. Singh and S. Arora, *The primitive idempotents in $FC_{2^n} - I$*, Int. J. Algebra, **4**, 1231-1241, (2010).

[25] J. A. Todd and H. S. M. Coxeter, *A practical method for enumerating cosets of a finite abstract group*, Proc. Edinburgh Math. Soc., **5(1)**, 26-34, (1936).

[26] D. C. Wong and M. Ang, *Group codes defined over dihedral groups of small order*, Malaysian J. Math. Sci., **7**, 101-116, (2013).

[27] X. Li, *Quantum cyclic and constacyclic codes*, IEEE Trans. Inform. Theory, **50(3)**, 547-549, (2004).

[28] D.-W. Yue and G.-Z. Feng, *Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes*, IEEE Trans. Inform. Theory, **46(7)**, 2625-2628, (2000).

[29] C. Yu and S. Zhu, *New Binary Quantum Codes from Group Rings and Skew Group Rings*, Int. J. Theor. Phys., **63**, 27, (2024).

[30] M. Reza Alimoradi, *Decoding of cyclic codes over a class of finite rings*, Palestine Journal of Mathematics, **12(2)**, 321-328, (2023).

[31] K. Chatouh, *Linear skew cyclic codes over the ring $R = (B[v_1, v_2, v_3]) + \vartheta(B[v_1, v_2, v_3]) + \vartheta^2(B[v_1, v_2, v_3]) + \vartheta^3(B[v_1, v_2, v_3])$*, Palestine Journal of Mathematics, **13(4)**, 1213-1226, (2024).

[32] P. Rai, B. Singh, A. Ji Gupta, Skew cyclic codes over $F_q[u_1, u_2, \ldots, u_r] / \langle u_i^3 - u_i,\ u_i u_j - u_j u_i \rangle_{i,j=1}^{r}$. *Palestine Journal of Mathematics*, **13**, 216–229 (Special Issue III)(2024).

[33] D. F. Holt, B. Eick, E. A. O'Brien, *Handbook of Computational Group Theory*, Chapman & Hall/CRC, (2005).

[34] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, (1997).

[35] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, (1977).

Author information

Ankan Shaw, Department of Mathematics, National Institute of Technology Durgapur, India.
E-mail: ankanf22@gmail.com

Satya Bagchi, Department of Mathematics, National Institute of Technology Durgapur, India.
E-mail: sbagchi.maths@nitdgp.ac.in

Received: 2025-07-15
Accepted: 2025-12-18