AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(5): 12852–12869.
DOI: 10.3934/math.2024628
Received: 28 February 2024
Revised: 25 March 2024
Accepted: 29 March 2024
Published: 03 April 2024

Research article

On the construction of constacyclically permutable codes from constacyclic codes

Guanghui Zhang[1] **and Shuhua Liang**[2,*]

[1] Department of Mathematics, Suqian University, Suqian, Jiangsu, 223800, China
[2] School of Economics and Management, Suqian University, Suqian, Jiangsu, 223800, China

* **Correspondence:** Email: 22125@squ.edu.cn.

Abstract: In this paper, we propose a way to partition any constacyclic code over a finite field in its equivalence classes according to the algebraic structure of the code. Such a method gives the generalization of cyclically permutable codes (CPCs), which are called constacyclically permutable codes (CCPCs), and it is useful to derive a CCPC from a given constacyclic code. Moreover, we present an enumerative formula for the code size of such a CCPC, with all of the terms being positive integers, and we provide an algebraic method to produce such a CCPC.

Keywords: constacyclically permutable code; constacyclic code; primitive idempotent; group action
Mathematics Subject Classification: 94B15, 94B60

1. Introduction

Cyclically permutable codes (CPCs), originally introduced by Gilbert in the early 1960s [1], make up a binary block code of code length n such that each codeword has a cyclic order n and the codewords are cyclically distinct. CPCs have many applications in communication networks, for example, as protocol sequences [2,3], and in watermarking systems [4]. Additionally, non-binary CPCs have applications in direct sequence code division multiple access systems with asynchronous base stations [5], as well as in the construction of frequency-hopping sequence sets [6–9]. Therefore, they are the focus of great theoretical interest and have practical significance in the study and exploration of q-ary CPCs [5, 6, 10–14].

Cyclic codes are considered important in theoretical studies because they posses a very rich mathematical structure. So, it seems possible to provide a useful framework to generate CPCs by choosing the codewords that are cyclically distinct and have maximal cyclic order. More specifically, one has an equivalence relationship for any cyclic code C: Two codewords of C are said to be equivalent if one can be obtained from the other by applying the cyclic shift a certain number of times. The equivalence class whose elements have full cyclic order is called a *nonperiodic cyclic equivalence class* (see [15] or [8]). Picking up exactly one member from each of the nonperiodic cyclic equivalence classes of C yields a CPC, which is denoted by C'. Note that C' is certainly not unique by its very definition, and that C' is a CPC that is derived from C with the largest possible code size. There are two basic questions that are attractive for mathematical investigations and practical applications: Q1: how to determine the exact value of $|C'|$ for a given arbitrary cyclic code C where $|C'|$ denotes the size of C'; Q2: how to find a general construction scheme that produces C' for an arbitrary cyclic code C.

Making use of a combinatorial technique known as the Möbius inversion formula, a group of authors, first in [16] and consequently in [17], found enumerative formulas for the value of $|C'|$, where C is a binary simple-root cyclic code. Song et al. [8] also utilized the Möbius function to obtain an enumerative formula for the size of C', where C is a Reed-Solomon (RS) code. Combining the Möbius inversion formula with some elementary properties of cyclic codes, Xia and Fu [18] determined the value of $|C'|$, where C is a q-ary simple-root cyclic code.

Compared with Q1, it seems that the method for deriving CPCs from a general cyclic code is still a challenging problem, even for the binary case. Maracle and Wolverton [13] provided an efficient algorithm to generate cyclically inequivalent subsets. In [18], Xia and Fu presented several algebraic constructions of subcodes of C', where the codes C are particular classes of cyclic codes. Here, by using the check polynomial approach, Xia and Fu obtained subcodes of C' from special classes of cyclic codes C, all of which have code sizes that are strictly less than $|C'|$. Kuribayashi and Tanaka [19] first provided an efficient and systematic method to construct a C' from a binary cyclic code C when the code length n is a Mersenne prime, i.e., n is a prime number in the form $2^m - 1$ for some m. Lemos-Neto and da Rocha [12] gave a necessary and sufficient condition on the generator polynomial of a cyclic code C under which any nonzero codeword of C has full cyclic order; further, in the same paper [12], the authors continued to provide an effective method to find CPCs from C, where C is a cyclic code of length $n = q^m - 1$. Nguyen et al. [3] proposed a novel procedure to obtain CPCs from RS codes of lengths $p - 1$ and $p + 1$, respectively, where p is a prime number. Using the discrete Fourier transform, Yang et al. [20] developed an efficient algorithm to produce a CPC from a p-ary cyclic code, where p is a prime number. Extending the results of [3,20], Cho et al. [21] proposed an effective algorithm to generate CPCs from a prime-length cyclic code. Recently, Bastos and Lemos-Neto [22] presented a method to obtain a CPC from a simple-root cyclic code by using the x-cyclotomic coset. More specifically, the determinant of codewords of C' is dependent on that of the x-cyclotomic coset modulo $h(x)$, where $h(x)$ is a divisor of $x^n - 1$.

In this paper, we aim to give the generalization of CPCs, which are called constacyclically permutable codes (CCPCs), and to introduce a method to derive a CCPC from a given constacyclic code. More specifically, let C be a given λ-constacyclic code of length n over $\mathbb{F}$, where λ is a nonzero element of $\mathbb{F}$ with order t, and ϕ be the cyclic shift of C. Two codewords c_1, c_2 of C are said to be equivalent if there is an integer r such that $\phi^r(c_1) = c_2$. In other words, the cyclic subgroup $\langle\phi\rangle$ of the automorphism group of C generated by the cyclic shift ϕ acts naturally on the constacyclic code C; then, c_1 and c_2 are equivalent if and only if they are in the same orbit. For an element c of C, if the length of the orbit containing c is nt, that is, nt is the least positive integer satisfying that $\phi^{nt}(c) = c$, then we state that c has full constacyclic order. The orbit of size nt is called the nonperiodic constacyclic equivalence class. A CCPC generated from C is formed by taking exactly one element from each nonperiodic constacyclic equivalence class of C, denoted still as C'. Similar to the case of CPCs, we focus on solving the following problem: For a given arbitrary constacyclic code C, we want to determine the exact value of $|C'|$, where $|C'|$ denotes the size of C', and to find a general construction scheme that produces C'. To this end, we use the language of group actions to reinterpret that C' is merely a representative of the n-length orbits of $\langle\phi\rangle$ on C, where $\langle\phi\rangle$ is the cyclic subgroup of the automorphism group of C generated by the cyclic shift ϕ. One of the advantages of our new approach lies in that the codewords of C are presented in terms of the primitive idempotents of C. Based on this approach, we present a new enumerative formula for the code size of such a CCPC with all of the terms being positive integers. On the other hand, we provide an algebraic method to produce such a CCPC.

This paper is organized as follows. We provide the basic notation and some results about constacyclic codes in Section 2. An enumerative formula for the exact value of $|C'|$ is given in Section 3. Section 4 proposes an effective method to generate C', where C is any simple-root constacyclic code, and presents an example to illustrate our main results.

2. Preliminaries

Let q be a prime power and n be a positive integer that is coprime with q. Let $\mathbb{F}_q$ denote a finite field with q elements and $\mathbb{F}_q^{\times}$ denote the set of all nonzero elements of $\mathbb{F}_q$, that is, $\mathbb{F}_q^{\times} = \mathbb{F}_q\backslash\{0\}$. Let x be an indeterminate over $\mathbb{F}_q$ and $\mathbb{F}_q[x]$ be the polynomial ring in variable x with coefficients in $\mathbb{F}_q$. Let $\mathbb{Z}$ be the set of integers, $\mathbb{Z}^+$ be the set of the positive integers, and $\mathbb{N}$ be the set of non-negative integers. For $s \in \mathbb{N}$, let $[0, s]$ denote the set $\{0, 1, 2, \cdots, s\}$. For any finite number of integers $a_1, a_2, \cdots, a_v$ which are not all equal to 0, we denote their greatest common divisor by $\gcd(a_1, a_2, \cdots, a_v)$; for any finite number of integers $a_1, a_2, \cdots, a_v$, none of which is equal to 0, denote their least common multiple by $\mathrm{lcm}(a_1, a_2, \cdots, a_v)$, where $v \geq 2$ is a positive integer. We use the notation $H \leq G$ to indicate that H is a subgroup of G. For the set S, let $|S|$ denote the number of elements of S. For $a, b \in \mathbb{Z}$, we use $a|b$ to denote that a divides b.

Let us review the definition of a constacyclic code. Let λ be a nonzero element of $\mathbb{F}_q$, that is, $\lambda \in \mathbb{F}_q^{\times}$. Let ϕ be the cyclic shift, as follows:

$$c = (c_0, c_1, \cdots, c_{n-1}) \mapsto \phi(c) = (\lambda c_{n-1}, c_0, \cdots, c_{n-2}).$$

A linear code C is λ-constacyclic if $c \in C$ implies that $\phi(c) \in C$. When $\lambda = 1$, the λ-constacyclic code is the usual cyclic code. Since we may associate each codeword $(c_0, c_1, \cdots, c_{n-1})$ in C with a polynomial $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ in the quotient ring $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$, a λ-constacyclic code of length n over $\mathbb{F}_q$ is an ideal of the quotient ring $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$. Write $\mathcal{R} = \mathbb{F}_q[x]/\langle x^n - \lambda\rangle$. If $c = (c_0, c_1, \cdots, c_{n-1})$ is regarded as a polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, then $\phi(c) = \phi(c(x)) = xc(x)$ in $\mathcal{R}$. Note that $\mathcal{R}$ is a principal ideal domain. Hence there is a unique monic polynomial $g(x)$ of minimum degree in the constacyclic code C. This polynomial generates C, that is, $C = \langle g(x)\rangle$, and it is called the generator polynomial for C (e.g., see [23, 24]).

In this section, we explore another approach to describe constacyclic codes, involving a different type of generating polynomial other than the generator polynomial. A polynomial $e(x) \in \mathcal{R}$ is said to be idempotent in $\mathcal{R}$ if $e^2(x) = e(x)$. Since $\gcd(n, q) = 1$, any constacyclic code C is generated by an idempotent, that is, there exists an idempotent $e(x)$ in $\mathcal{R}$ such that $C = \langle e(x)\rangle = \mathcal{R}e(x)$ (see [23]). Two idempotents $e(x)$ and $f(x)$ are called orthogonal if $e(x)f(x) = 0$ in $\mathcal{R}$. A nonzero idempotent $e(x)$ in $\mathcal{R}$ is called primitive if it cannot be written as the sum of two nonzero orthogonal idempotents in $\mathcal{R}$.

Let t be the multiplication order of λ. Then, $t|(q-1)$, which implies that $\gcd(q,t)=1$. Noting that $\gcd(q,n)=1$, we have that $\gcd(q,nt)=1$. Let m be the least integer such that $(nt)|(q^m-1)$ and $\mathbb{F}_{q^m}$ be the finite field with q^m elements. Then, there exists a primitive (nt)th root η of unity in $\mathbb{F}_{q^m}^{\times}$ such that $\lambda=\eta^n$. Thus, $x^n-\lambda=\prod\limits_{j=0}^{n-1}(x-\eta^{1+tj})$. Let

$$\begin{aligned}
C_0 &= \{(1+t\cdot i_0)q^j \big| j\in\mathbb{Z}\} = \{1,q,q^2,\cdots,q^{k_0-1}\};\\
C_1 &= \{(1+t\cdot i_1)q^j \big| j\in\mathbb{Z}\} = \{1+ti_1,(1+ti_1)q,(1+ti_1)q^2,\cdots,(1+ti_1)q^{k_1-1}\};\\
&\vdots\\
C_s &= \{(1+t\cdot i_s)q^j \big| j\in\mathbb{Z}\} = \{1+ti_s,(1+ti_s)q,(1+ti_s)q^2,\cdots,(1+ti_s)q^{k_s-1}\},
\end{aligned}$$

where $0=i_0<i_1<i_2<\cdots<i_s\le n-1$ and k_j is the smallest positive integer such that $1+t\cdot i_j\equiv(1+t\cdot i_j)q^{k_j} \pmod{nt}$ for $0\le j\le s$. Therefore, $C_0,C_1,\cdots,C_s$ are all distinct q-cyclotomic cosets modulo nt and form a partition of the set $\{1+ti|i=0,1,\cdots,n-1\}$. Clearly, $|C_j|=q^{k_j}$, $j=0,1,\cdots,s$.

Now, consider the factorization

$$x^n-\lambda=\prod_{v=0}^{s} m_v(x)$$

of $x^n-\lambda$ as irreducible factors over $\mathbb{F}_q$, where for $v=0,1,\cdots,s$,

$$m_v(x)=\prod_{j\in C_v}(x-\eta^j).$$

According to the Chinese remainder theorem, we have that

$$\mathcal{R}\cong\mathbb{F}_q[x]/\langle m_0(x)\rangle\oplus\mathbb{F}_q[x]/\langle m_1(x)\rangle\oplus\cdots\oplus\mathbb{F}_q[x]/\langle m_s(x)\rangle.$$

For $v=0,1,\cdots,s$, we let $M_v(x)=\frac{x^n-\lambda}{m_v(x)}$ and $I_v=\mathbb{F}_q[x]/\langle m_v(x)\rangle$. Then,

$$I_v=\mathbb{F}_q[x]/\langle m_v(x)\rangle\cong\langle M_v(x)\rangle, v=0,1,\cdots,s.$$

Hence, I_v is a minimal code in $\mathcal{R}$ with the generator polynomial $M_v(x)$, as well as a finite field with q^{k_v} elements for $v=0,1,\cdots,s$.

Let $\theta_0(x),\theta_1(x),\cdots,\theta_s(x)$ be all primitive idempotents in $\mathcal{R}$ (see, for example, [25]). In fact, $\theta_v(x)$ is the generating idempotent of minimal code I_v, that is, $I_v=\langle\theta_v(x)\rangle=\mathcal{R}\theta_v(x)$. All of the primitive idempotents in $\mathcal{R}$ have the following property: For $0\le i,j\le s$,

$$\theta_i(x)\theta_j(x)=\begin{cases}\theta_i(x), & i=j;\\ 0, & i\neq j.\end{cases}$$

Let $f(x)=\sum\limits_{i=0}^{n-1}a_ix^i\in\mathcal{R}$, and let

$$f(x)=m_v(x)\psi(x)+r(x),$$

where $\deg(r(x))<k_v$ and $0\le v\le s$. Then since there exists a polynomial $\varphi(x)$ such that $\theta_v(x)=\varphi(x)M_v(x)$ (please see [26, Theorem 7.4.9]), we obtain that

$$f(x)\theta_v(x) = m_v(x)\theta_v(x)\psi(x)+r(x)\theta_v(x)$$

$$
\begin{aligned}
&= m_v(x)\varphi(x)M_v(x)\psi(x) + r(x)\theta_v(x) \\
&= (x^n - \lambda)\varphi(x)\psi(x) + r(x)\theta_v(x) \\
&= r(x)\theta_v(x).
\end{aligned}
$$

Hence, for $v = 0, 1, \cdots, s$,

$$
I_v = \mathcal{R}\theta_v(x) = \Big\{ f(x)\theta_v(x) | f(x) \in \mathcal{R} \Big\} = \Big\{ \sum_{j=0}^{k_v-1} a_j x^j \theta_v(x) | a_j \in \mathbb{F}_q \Big\}. \tag{2.1}
$$

In addition, the representation of each element in I_v is unique; thus $|I_v| = q^{k_v}$.

For the quotient ring $\mathbb{F}_{q^m}[x]/\langle x^n - \lambda\rangle$, there are n primitive idempotents (see, for example, [25]):

$$
e_{1+tj}(x) = \frac{1}{n}\sum_{u=0}^{n-1} \eta^{-u(1+tj)} x^u,\ j = 0, 1, \cdots, n-1. \tag{2.2}
$$

Then, for every u with $0 \le u \le n-1$,

$$
\begin{aligned}
\sum_{j=0}^{n-1} \eta^{u(1+tj)} e_{1+tj}(x) &= \sum_{j=0}^{n-1} \eta^{u(1+tj)} \cdot \frac{1}{n} \sum_{v=0}^{n-1} \eta^{-v(1+tj)} x^v \\
&= \frac{1}{n} \sum_{j=0}^{n-1} \sum_{v=0}^{n-1} \eta^{(u-v)(1+tj)} x^v \\
&= x^u.
\end{aligned}
$$

This shows that

$$
x^u = \sum_{j=0}^{n-1} \eta^{u(1+tj)} e_{1+tj}(x). \tag{2.3}
$$

In what follows, we determine the explicit formula for the primitive idempotents $\theta_v(x)'s$. Assume that $\theta_v(x) = \sum\limits_{u=0}^{n-1} b_u x^u$. Then,

$$
\begin{aligned}
\frac{1}{n}\sum_{j=0}^{n-1} \theta_v(\eta^{1+tj})\eta^{-u(1+tj)} &= \frac{1}{n}\sum_{j=0}^{n-1}\sum_{\kappa=0}^{n-1} b_\kappa \eta^{(1+tj)\kappa}\eta^{-u(1+tj)} \\
&= \frac{1}{n}\sum_{j=0}^{n-1}\sum_{\kappa=0}^{n-1} b_\kappa \eta^{(1+tj)(u-\kappa)} \\
&= \frac{1}{n}\sum_{\kappa=0}^{n-1} b_\kappa \sum_{j=0}^{n-1} \eta^{(1+tj)(\kappa-u)} = b_u.
\end{aligned}
$$

That is to say,

$$
b_u = \frac{1}{n}\sum_{j=0}^{n-1} \theta_v(\eta^{1+tj})\eta^{-u(1+tj)}. \tag{2.4}
$$

On the other hand, since $\theta_v(x)$ is idempotent, we have that $\theta_v^2(x) = \theta_v(x)$ in $\mathcal{R}$; thus $\theta_v^2(\eta^j) = \theta_v(\eta^j)$ for $j \geq 1$. Therefore, $\theta_v(\eta^j) = 0$ or 1. But, according to [26, Theorem 7.4.12], $\theta_v(x)$ and $M_v(x)$ have the same zeros among the n-th roots of λ; thus

$$\theta_v(\eta^j) = \begin{cases} 0, & \text{if } j \notin C_v; \\ 1, & \text{if } j \in C_v. \end{cases}$$

Therefore,

$$b_u = \frac{1}{n} \sum_{j \in C_v} \eta^{-uj}. \tag{2.5}$$

Thus, by (2.2) and (2.5), we deduce that

$$\theta_v(x) = \sum_{u=0}^{n-1} b_u x^u = \frac{1}{n} \sum_{u=0}^{n-1} \sum_{j \in C_v} \eta^{-uj} x^u = \sum_{j \in C_v} e_j(x). \tag{2.6}$$

Hence, we can use $\theta_v(x)$ to determine all of the elements of I_v in (2.1), as follows:

$$\begin{aligned}
\sum_{j=0}^{k_v-1} a_j x^j \theta_v(x) &= \sum_{j=0}^{k_v-1} a_j \sum_{\kappa=0}^{n-1} \eta^{j(1+t\kappa)} e_{1+t\kappa}(x) \sum_{u \in C_v} e_u(x) \\
&= \sum_{j=0}^{k_v-1} a_j \sum_{\ell=0}^{s} \sum_{\kappa \in C_\ell} \eta^{j\kappa} e_\kappa(x) \sum_{u \in C_v} e_u(x) \\
&= \sum_{j=0}^{k_v-1} a_j \sum_{\ell=0}^{s} \sum_{\kappa \in C_\ell} \eta^{j\kappa} \sum_{u \in C_v} e_\kappa(x) e_u(x) \\
&= \sum_{j=0}^{k_v-1} a_j \sum_{\kappa \in C_v} \eta^{j\kappa} e_\kappa(x) \\
&= \sum_{j=0}^{k_v-1} a_j \sum_{u=0}^{k_v-1} \eta^{j(1+ti_v)q^u} e_{(1+ti_v)q^u}(x) \\
&= \sum_{j=0}^{k_v-1} \sum_{u=0}^{k_v-1} a_j \eta^{j(1+ti_v)q^u} e_{(1+ti_v)q^u}(x).
\end{aligned}$$

Therefore, we get that

$$\mathcal{R} = \mathcal{R}\theta_0(x) \oplus \mathcal{R}\theta_1(x) \oplus \cdots \oplus \mathcal{R}\theta_s(x), \tag{2.7}$$

where

$$\mathcal{R}\theta_v(x) = \left\{ \sum_{j=0}^{k_v-1} \sum_{u=0}^{k_v-1} a_j \eta^{j(1+ti_v)q^u} e_{(1+ti_v)q^u}(x) | a_j \in \mathbb{F}_q \right\}, \tag{2.8}$$

for $v = 0, 1, \cdots, s$.

Let C be a λ-constacyclic code. Then, we can write

$$C = \bigoplus_{j \in J} \mathcal{R}\theta_j(x), \tag{2.9}$$

where J is a nonempty subset of $[0, s]$, and further denote the following:

$$C^\sharp = \bigoplus_{j\in J} \mathcal{R}\theta_j(x)\backslash\{0\}. \tag{2.10}$$

3. An enumerative formula for CCPCs

In this section, we aim to obtain a closed formula for the exact value of $|C'|$ for a given constacyclic code C. To this end, we explore the characterization of codewords of C with full constacyclic orders.

Lemma 3.1. *Let $a, b, i_v, u \in \mathbb{N}$ and $a \equiv b \pmod n$. Then, as two elements of $\mathcal{R}$ we have*

$$\eta^{-a(1+ti_v)q^u} x^a = \eta^{-b(1+ti_v)q^u} x^b.$$

Proof. Assume that $b = ns + a (s \in \mathbb{Z})$. Then,

$$\begin{aligned} \eta^{-b(1+ti_v)q^u} x^b &= \eta^{-(ns+a)(1+ti_v)q^u} x^{ns+a} \\ &= \eta^{-a(1+ti_v)q^u} x^a \cdot \eta^{-ns(1+ti_v)q^u} x^{ns}. \end{aligned}$$

Notice that $x^n = \lambda = \eta^n$ and λ is an element of order t; we have

$$\eta^{-ns(1+ti_v)q^u} x^{ns} = \eta^{-ns(1+ti_v)q^u} \eta^{ns} = \eta^{-nsti_vq^u} = \lambda^{-ti_vq^u} = 1.$$

This proves the result. □

Lemma 3.2. *Assume that r is a positive integer and $v \in [0, s]$. Let*

$$a(x) = \sum_{j=0}^{k_v-1} \sum_{u=0}^{k_v-1} a_j \eta^{j(1+ti_v)q^u} e_{(1+ti_v)q^u}(x) \in \mathcal{R}\theta_v(x),$$

where $a_j \in \mathbb{F}_q$ for $0 \le j \le k_v - 1$. Then,

(1) $\phi^r(e_{(1+ti_v)q^u}(x)) = \eta^{r(1+ti_v)q^u} e_{(1+ti_v)q^u}(x)$;

(2) $\phi^r(a(x)) = \sum_{j=0}^{k_v-1} \sum_{u=0}^{k_v-1} a_j \eta^{(j+r)(1+ti_v)q^u} e_{(1+ti_v)q^u}(x)$;

(3) $\phi^r(a(x)) = a(x)$ *if and only if* $\frac{nt}{\gcd(n,1+ti_v)} \Big| r$.

Proof. (1) By (2.2) and Lemma 3.1, we have

$$\begin{aligned} \phi^r(e_{(1+ti_v)q^u}(x)) &= x^r e_{(1+ti_v)q^u}(x) \\ &= x^r \cdot \frac{1}{n} \sum_{j=0}^{n-1} \eta^{-j(1+ti_v)q^u} x^j \\ &= \eta^{r(1+ti_v)q^u} \cdot \frac{1}{n} \sum_{j=0}^{n-1} \eta^{-(j+r)(1+ti_v)q^u} x^{j+r} \\ &= \eta^{r(1+ti_v)q^u} e_{(1+ti_v)q^u}(x). \end{aligned}$$

This proves part (1).

(2) From (1) above, it follows that

$$\begin{aligned}\phi^r(a(x)) &= \sum_{j=0}^{k_v-1}\sum_{u=0}^{k_v-1} a_j\eta^{j(1+ti_v)q^u}\phi^r(e_{(1+ti_v)q^u}(x))\\ &= \sum_{j=0}^{k_v-1}\sum_{u=0}^{k_v-1} a_j\eta^{j(1+ti_v)q^u}\cdot\eta^{r(1+ti_v)q^u}e_{(1+ti_v)q^u}(x)\\ &= \sum_{j=0}^{k_v-1}\sum_{u=0}^{k_v-1} a_j\eta^{(j+r)(1+ti_v)q^u}e_{(1+ti_v)q^u}(x).\end{aligned}$$

This proves part (2).

(3) By part (2), we see that $\phi^r(a(x)) = a(x)$ if and only if $\eta^{r(1+ti_v)q^u} = 1$. Notice that $\gcd(nt, q^u) = 1$, $\gcd(t, 1 + ti_v) = 1$, and $\gcd\left(\frac{nt}{\gcd(nt,1+ti_v)}, \frac{1+ti_v}{\gcd(nt,1+ti_v)}\right) = 1$. It follows that

$$\begin{aligned}\phi^r(a(x)) = a(x) &\Leftrightarrow (nt)|r(1+ti_v)q^u\\ &\Leftrightarrow (nt)|r(1+ti_v)\\ &\Leftrightarrow \frac{nt}{\gcd(nt,1+ti_v)}\Big|r\frac{1+ti_v}{\gcd(nt,1+ti_v)}\\ &\Leftrightarrow \frac{nt}{\gcd(n,1+ti_v)}\Big|r.\end{aligned}$$

This concludes the proof. □

Based on the preliminaries above, the next two results can be used to characterize the codewords with full constacyclic order for a given constacyclic code, which are discussed for the irreducible and reducible cases. These can be attributed to some number theory conditions.

Lemma 3.3. *Let $v \in [0, s]$ and $C = \mathcal{R}\theta_v(x)$ be an irreducible constacyclic code generated by the primitive idempotent $\theta_v(x)$ as shown in (2.8). Then, we have the following:*

(1) *If $\gcd(n, 1 + ti_v) = 1$, then every nonzero element of C has full constacyclic order.*

(2) *If $\gcd(n, 1 + ti_v) \neq 1$, then none of the nonzero elements of C has full constacyclic order.*

Proof. (1) Suppose that $\gcd(n, 1 + ti_v) = 1$. Let $a(x)$ be an arbitrary element in C and r_0 be the least positive integer such that $\phi^{r_0}(a(x)) = a(x)$. Since $\phi^{nt}(a(x)) = a(x)$, we have that $r_0|(nt)$. On the other hand, by Lemma 3.2(3), we get that $(nt)|r_0$. Therefore, $r_0 = nt$, i.e., every nonzero element of C has full constacyclic order.

(2) Suppose that $\gcd(n, 1 + ti_v) \neq 1$. Set $r_0' = \frac{nt}{\gcd(nt,1+ti_v)}$. Then, $r_0' < nt$ and, by Lemma 3.2(3), it follows that $\phi^{r_0'}(a(x)) = a(x)$ for every nonzero element $a(x)$, which implies that none of the nonzero elements of C has full constacyclic order. □

Lemma 3.4. *Let $u \geq 2$ be an integer, and let $J = \{j_1, j_2, \cdots, j_u\} \subseteq [0, s]$ with $0 \leq j_1 < j_2 < \cdots < j_u \leq s$. Let C be a constacyclic code, as shown in (2.9), and $C^\sharp$ be as in (2.10). Then, we have the following:*

(1) *If $\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u}) = 1$, then every nonzero element of $C^\sharp$ has full constacyclic order.*

(2) *If $\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u}) \neq 1$, then none of the nonzero elements of $C^\sharp$ has full constacyclic order.*

Proof. Let $a(x) = a_1(x) + a_2(x) + \cdots + a_u(x)$ be an arbitrary element in $C^\sharp$, where $a_\ell(x) \in \mathcal{R}\theta_{j_\ell}(x)$ for $\ell = 0, 1, \cdots, u$, and s_0 be the least positive integer such that $\phi^{s_0}(a(x)) = a(x)$. Since $\phi^{nt}(a(x)) = a(x)$, we have that $s_0|(nt)$. On the other hand, we see that $\phi^{s_0}(a(x)) = a(x)$ if and only if $\phi^{s_0}(a_\ell(x)) = a_\ell(x)$ for $\ell = 0, 1, \cdots, u$. By Lemma 3.2(3), we get that $\phi^{s_0}(a_\ell(x)) = a_\ell(x)$ for $\ell = 0, 1, \cdots, u$ if and only if

$$\frac{nt}{\gcd(nt, 1 + ti_{j_\ell})}\Big| s_0,$$

for $\ell = 0, 1, \cdots, u$. Further, $\frac{nt}{\gcd(nt,1+ti_{j_\ell})}\Big|s_0$ for $\ell = 0, 1, \cdots, u$ if and only if

$$\mathrm{lcm}\Big(\frac{nt}{\gcd(nt, 1 + ti_{j_1})}, \frac{nt}{\gcd(nt, 1 + ti_{j_2})}, \cdots, \frac{nt}{\gcd(nt, 1 + ti_{j_u})}\Big)\Big| s_0.$$

By induction on u, we can easily prove the equality, as follows:

$$\mathrm{lcm}\Big(\frac{nt}{\gcd(nt, 1 + ti_{j_1})}, \frac{nt}{\gcd(nt, 1 + ti_{j_2})}, \cdots, \frac{nt}{\gcd(nt, 1 + ti_{j_u})}\Big) = \frac{nt}{\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u})}.$$

Therefore, $\frac{nt}{\gcd(nt,1+ti_{j_\ell})}\Big|s_0$ for $\ell = 0, 1, \cdots, u$ if and only if

$$\frac{nt}{\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u})}\Big| s_0.$$

(1) Suppose that $\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u}) = 1$. Then, we get $(nt)|s_0$. Hence, $s_0 = nt$. Therefore, every nonzero element of $C^\sharp$ has full constacyclic order.

(2) Suppose that $\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u}) \neq 1$. Set

$$s'_0 = \frac{nt}{\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u})}.$$

Then, $s'_0 < nt$. According to the above proof, we can see that $\phi^r(a(x)) = a(x)$ for $a(x) \in C^\sharp$ if and only if

$$\frac{nt}{\gcd(n, 1 + ti_{j_1}, 1 + ti_{j_2}, \cdots, 1 + ti_{j_u})}\Big| r.$$

So $\phi^{s'_0}(a(x)) = a(x)$. Since $s'_0 < nt$, $a(x)$ has no full constacyclic order. $a(x)$ is arbitrary, implying that none of the nonzero elements of $C^\sharp$ has full constacyclic order. □

Let C be a constacyclic code, as shown in (2.9) with $J = \{j_1, j_2, \cdots, j_u\} \subseteq [0, s]$, where $0 \leq j_1 < j_2 < \cdots < j_u \leq s$. That is,

$$C = \mathcal{R}\theta_{j_1}(x) \oplus \mathcal{R}\theta_{j_2}(x) \oplus \cdots \oplus \mathcal{R}\theta_{j_u}(x). \tag{3.1}$$

Then,

$$C^\sharp = \mathcal{R}\theta_{j_1}(x)\backslash\{0\} \oplus \mathcal{R}\theta_{j_2}(x)\backslash\{0\} \oplus \cdots \oplus \mathcal{R}\theta_{j_u}(x)\backslash\{0\}. \tag{3.2}$$

For $1 \leq v \leq u$, let

$$\Theta_v = \Big\{\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\}\Big| 1 \leq \ell_1 < \ell_2 < \cdots < \ell_v \leq u, \gcd(n, 1 + ti_{j_{\ell_1}}, 1 + ti_{j_{\ell_2}}, \cdots, 1 + ti_{j_{\ell_v}}) = 1\Big\}. \tag{3.3}$$

For $\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\} \in \Theta_v$, set

$$C^{\sharp}_{\ell_1,\ell_2,\cdots,\ell_v} = \mathcal{R}\theta_{j_{\ell_1}}(x)\backslash\{0\} \oplus \mathcal{R}\theta_{j_{\ell_2}}(x)\backslash\{0\} \oplus \cdots \oplus \mathcal{R}\theta_{j_{\ell_v}}(x)\backslash\{0\}. \tag{3.4}$$

Thus according to the characterization conditions above about the codewords with full constacyclic order, the following result is easily obtained, which determines the exact value of $|C'|$ for a given arbitrary constacyclic code C.

Theorem 3.5. *Let the notation be as above. Let C be a constacyclic code, as shown in (3.1). Then, the following holds:*

(1) *The elements of C with full constacyclic order are given by*

$$\bigcup_{v=1}^{u} \bigcup_{\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\} \in \Theta_v} C^{\sharp}_{\ell_1,\ell_2,\cdots,\ell_v}.$$

(2) $|C'|$ *is given as follows:*

$$|C'| = \frac{1}{nt} \sum_{v=1}^{u} \sum_{\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\} \in \Theta_v} \prod_{\rho=1}^{v} (q^{k_{j_{\ell_\rho}}} - 1).$$

Proof. (1) It follows from Lemmas 3.3 and 3.4.

(2) According to the definition of C', and based on the result of (1), we have

$$(nt)|C'| = \sum_{v=1}^{u} \sum_{\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\} \in \Theta_v} \left|C^{\sharp}_{\ell_1,\ell_2,\cdots,\ell_v}\right|.$$

Since

$$\left|C^{\sharp}_{\ell_1,\ell_2,\cdots,\ell_v}\right| = \prod_{\rho=1}^{v} (q^{k_{j_{\ell_\rho}}} - 1),$$

we obtain the desired result.

4. Generation of CCPCs

In this section, we delve more deeply into the structure of CCPCs, paying particular attention to the elements of C' for a given constacyclic code C. First, we describe the observation. Recall that, for $v \in [0, s]$ the irreducible code $\mathcal{R}\theta_v(x)$ is given by

$$\mathcal{R}\theta_v(x) = \left\{ \sum_{j=0}^{k_v-1} \sum_{u=0}^{k_v-1} a_j \eta^{j(1+ti_v)q^u} e_{(1+ti_v)q^u}(x) \middle| a_j \in \mathbb{F}_q \right\}.$$

Notice the following fact about the element of $\mathcal{R}\theta_v(x)$:

$$\sum_{j=0}^{k_v-1} \sum_{u=0}^{k_v-1} a_j \eta^{j(1+ti_v)q^u} e_{(1+ti_v)q^u}(x) = \sum_{u=0}^{k_v-1} \Big(\sum_{j=0}^{k_v-1} a_j \eta^{j(1+ti_v)} \Big)^{q^u} e_{(1+ti_v)q^u}(x).$$

And, when a_j runs through $\mathbb{F}_q$, $\sum_{j=0}^{k_v-1} a_j\eta^{j(1+ti_v)}$ just runs through finite field $\mathbb{F}_{q^{k_v}}$. Then, $\mathcal{R}\theta_v(x)$ can be expressed, as follows:

$$\mathcal{R}\theta_v(x) = \left\{ \sum_{u=0}^{k_v-1} \omega^{q^u} e_{(1+ti_v)q^u}(x) \middle| \omega \in \mathbb{F}_{q^{k_v}} \right\}. \tag{4.1}$$

For every $v \in [0, s]$, $\mathcal{R}\theta_v(x) = \mathbb{F}_{q^{k_v}}$ is a finite field; we can denote its primitive element by γ_v, which generates the cyclic group $\mathbb{F}_{q^{k_v}}^\times = \mathbb{F}_{q^{k_v}}\backslash\{0\}$. If $\gcd(n, 1 + ti_v) = 1$, then there is the decomposition of the left cosets of $\langle\eta^{1+ti_v}\rangle = \langle\eta\rangle$ in $\mathbb{F}_{q^{k_v}}^\times = \mathbb{F}_{q^{k_v}}\backslash\{0\}$, as follows:

$$\mathbb{F}_{q^{k_v}}^\times = \langle\eta^{1+ti_v}\rangle \cup \gamma_v\langle\eta^{1+ti_v}\rangle \cup \cdots \gamma_v^{\frac{q^{k_v}-1}{nt}-1}\langle\eta^{1+ti_v}\rangle. \tag{4.2}$$

We first consider irreducible constacyclic codes.

Theorem 4.1. *Let $C = \mathcal{R}\theta_v(x)$ be an irreducible constacyclic code over $\mathbb{F}_q$, where $v \in [0, s]$. Suppose that $\gcd(n, 1 + ti_v) = 1$, and keep the notation as in (4.2). Then,*

$$C' = \left\{ \sum_{u=0}^{k_v-1} \gamma_v^{\ell q^u} e_{(1+ti_v)q^u}(x) \middle| 0 \le \ell \le \frac{q^{k_v} - 1}{nt} - 1 \right\}.$$

is a CCPC of size $\frac{q^{k_v}-1}{nt}$.

Proof. By Lemma 3.3, every nonzero element of C has full constacyclic order. Suppose that

$$a(x) = \sum_{u=0}^{k_v-1} \omega_1^{q^u} e_{(1+ti_v)q^u}(x) \in \mathcal{R}\theta_v(x)\backslash\{0\};$$

$$b(x) = \sum_{u=0}^{k_v-1} \omega_2^{q^u} e_{(1+ti_v)q^u}(x) \in \mathcal{R}\theta_v(x)\backslash\{0\},$$

where $\omega_1, \omega_2 \in \mathbb{F}_{q^{k_v}}$. If there exists r such that $\phi^r(a(x)) = b(x)$, then, by Lemma 3.2(2), we see that

$$\phi^r(a(x)) = \sum_{u=0}^{k_v-1} (\eta^{r(1+ti_v)}\omega_1)^{q^u} e_{(1+ti_v)q^u}(x) = b(x) = \sum_{u=0}^{k_v-1} \omega_2^{q^u} e_{(1+ti_v)q^u}(x).$$

Therefore, $\phi^r(a(x)) = b(x)$ if and only if $\eta^{r(1+ti_v)}\omega_1 = \omega_2$, which implies that ω_1 and ω_2 make up the same left coset of $\langle\eta^{1+ti_v}\rangle = \langle\eta\rangle$ in $\mathbb{F}_{q^{k_v}}^\times = \mathbb{F}_{q^{k_v}}\backslash\{0\}$. Therefore, according to (4.2), we obtain the desired result. □

In what follows, we consider the case when C is a reducible constacyclic code. Let C be as in (3.1), where $u \ge 2$. For simplicity, we write

$$\alpha_\kappa = j_{\ell_\kappa}, \kappa = 1, 2, \cdots, v.$$

$$m_\kappa = \frac{(q^{k_{\alpha_\kappa}} - 1)\gcd(n, 1 + ti_{\alpha_\kappa})}{nt}, \kappa = 1, 2, \cdots, v;$$

$$n_\kappa = \frac{nt\gcd(n, 1+ti_{\alpha_1}, 1+ti_{\alpha_2}, \cdots, 1+ti_{\alpha_\kappa})}{\gcd(n, 1+ti_{\alpha_1}, 1+ti_{\alpha_2}, \cdots, 1+ti_{\alpha_{\kappa-1}})\gcd(n, 1+ti_{\alpha_\kappa})}, \kappa = 2, 3, \cdots, v.$$

We set

$$\begin{aligned} G_1 &= \bigoplus_{\kappa=1}^{v} \mathcal{R}\theta_{\alpha_\kappa}(x)\backslash\{0\} = \bigoplus_{\kappa=1}^{v} \mathbb{F}_{q^{\alpha_\kappa}}\backslash\{0\} = \bigoplus_{\kappa=1}^{v} \mathbb{F}^{\times}_{q^{\alpha_\kappa}}. \\ G_2 &= \bigoplus_{\kappa=1}^{v} \langle \eta^{1+ti_{\alpha_\kappa}}\rangle = \langle \eta^{1+ti_{\alpha_1}}\rangle \oplus \langle \eta^{1+ti_{\alpha_2}}\rangle \oplus \cdots \oplus \langle \eta^{1+ti_{\alpha_v}}\rangle. \\ G_3 &= \Big\langle \sum_{\kappa=1}^{v} \eta^{1+ti_{\alpha_\kappa}} \Big\rangle = \langle \eta^{1+ti_{\alpha_1}} + \eta^{1+ti_{\alpha_2}} + \cdots + \eta^{1+ti_{\alpha_v}}\rangle. \end{aligned}$$

Then $G_3 \leq G_2 \leq G_1$.

Suppose that γ_{α_κ} is the primitive element of the finite field $\mathbb{F}_{q^{k\alpha_\kappa}} = \mathbb{F}_{q^{kj_{\ell_\kappa}}}$, that is to say, $\mathbb{F}^{\times}_{q^{k\alpha_\kappa}} = \langle \gamma_{\alpha_\kappa}\rangle$ for $\kappa = 1, 2, \cdots, v$.

Our goal now is to construct a coset decomposition of G_3 in G_1. First, for $\kappa = 1, 2, \cdots, v$,

$$\mathbb{F}^{\times}_{q^{k\alpha_\kappa}} = \bigcup_{\varepsilon_\kappa=0}^{m_\kappa-1} \gamma_{\alpha_\kappa}^{\varepsilon_\kappa}\langle \eta^{1+ti_{\alpha_\kappa}}\rangle.$$

Then, there exists a coset decomposition of the subgroup G_2 in G_1:

$$G_1 = \bigcup_{\varepsilon_1=0}^{m_1-1}\bigcup_{\varepsilon_2=0}^{m_2-1}\cdots\bigcup_{\varepsilon_v=0}^{m_v-1}\Big(\sum_{\kappa=1}^{v}\gamma_{\alpha_\kappa}^{\varepsilon_\kappa}\Big)G_2.$$

Next, the routine check shows that there is a coset decomposition of the subgroup G_3 in G_2:

$$\begin{aligned} G_2 &= \bigcup_{\sigma_2=0}^{n_2-1}\cdots\bigcup_{\sigma_v=0}^{n_v-1}\Big\{\Big(\theta^{1+ti_{\alpha_1}} + \theta^{\sigma_2(1+ti_{\alpha_2})} + \cdots + \theta^{\sigma_v(1+ti_{\alpha_v})}\Big)G_3\Big\} \\ &= \bigcup_{\sigma_2=0}^{n_2-1}\cdots\bigcup_{\sigma_v=0}^{n_v-1}\Big\{\Big(\sum_{j=1}^{v}\theta^{\sigma_j(1+ti_{\alpha_j})}\Big)G_3\Big\}, \end{aligned} \tag{4.3}$$

where $\sigma_1 = 1$.

Therefore, the coset decomposition of the subgroup G_3 in G_1 is given as follows:

$$\begin{aligned} G_1 &= \bigcup_{\varepsilon_1=0}^{m_1-1}\bigcup_{\varepsilon_2=0}^{m_2-1}\cdots\bigcup_{\varepsilon_v=0}^{m_v-1}\bigcup_{\sigma_2=0}^{n_2-1}\cdots\bigcup_{\sigma_v=0}^{n_v-1}\Big\{\Big(\sum_{\kappa=1}^{v}\gamma_{\alpha_\kappa}^{\varepsilon_\kappa}\Big)\Big(\sum_{j=0}^{v}\theta^{\sigma_j(1+ti_{\alpha_j})}\Big)G_3\Big\} \\ &= \bigcup_{\varepsilon_1=0}^{m_1-1}\bigcup_{\varepsilon_2=0}^{m_2-1}\cdots\bigcup_{\varepsilon_v=0}^{m_v-1}\bigcup_{\sigma_2=0}^{n_2-1}\cdots\bigcup_{\sigma_v=0}^{n_v-1}\Big\{\sum_{\kappa=1}^{v}\sum_{j=1}^{v}\Big(\gamma_{\alpha_\kappa}^{\varepsilon_\kappa}\cdot\theta^{\sigma_j(1+ti_{\alpha_j})}\Big)G_3\Big\}. \end{aligned} \tag{4.4}$$

We are now in a position to determine a CCPC from a given constacyclic code.

Theorem 4.2. *Apply the notation as above. Let C be a constacyclic code with the decomposition of the form as in (3.1). Then,*

$$\begin{aligned} C' = & \bigcup_{v=1}^{u} \bigcup_{\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\} \in \Theta_v} \bigcup_{\varepsilon_1=0}^{m_1-1} \bigcup_{\varepsilon_2=0}^{m_2-1} \cdots \bigcup_{\varepsilon_v=0}^{m_v-1} \bigcup_{\sigma_2=0}^{n_2-1} \cdots \bigcup_{\sigma_v=0}^{n_v-1} \\ & \left\{ \sum_{\epsilon=1}^{v} \sum_{\kappa=1}^{v} \sum_{j=1}^{v} \sum_{u=0}^{k_{\alpha_\epsilon}-1} \left(\gamma_{\alpha_\kappa}^{\varepsilon_\kappa} \cdot \theta^{\sigma_j (1+ti_{\alpha_j})} \right)^{q^u} e_{(1+ti_{\alpha_\epsilon})q^u}(x) \right\}. \end{aligned} \tag{4.5}$$

is a CCPC of size

$$\frac{1}{nt} \sum_{v=1}^{u} \sum_{\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\} \in \Theta_v} \prod_{\rho=1}^{v} (q^{k_{j_{\ell_\rho}}} - 1)$$

where Θ_v is as shown in (3.3).

Proof. Let $\{j_{\ell_1}, j_{\ell_2}, \cdots, j_{\ell_v}\} \in \Theta_v$, where $1 \le v \le u$. Now, we only need to consider the following subcode:

$$\mathcal{R}\theta_{j_{\ell_1}}(x) \oplus \mathcal{R}\theta_{j_{\ell_2}}(x) \oplus \cdots \oplus \mathcal{R}\theta_{j_{\ell_v}}(x).$$

Note that, for $1 \le \epsilon \le v$,

$$\mathcal{R}\theta_{\alpha_\epsilon}(x) = \mathcal{R}\theta_{j_{\ell_\epsilon}}(x) = \left\{ \sum_{u=0}^{k_{\alpha_\epsilon}-1} \omega^{q^u} e_{(1+ti_{\alpha_\epsilon})q^u}(x) \middle| \omega \in \mathbb{F}_{q^{k_{\alpha_\epsilon}}} \right\}.$$

Assume that

$$f(x) = \sum_{\epsilon=1}^{v} a_\epsilon(x) \in \bigoplus_{\epsilon=1}^{v} \mathcal{R}\theta_{\alpha_\epsilon}(x); g(x) = \sum_{\epsilon=1}^{v} b_\epsilon(x) \in \bigoplus_{\epsilon=1}^{v} \mathcal{R}\theta_{\alpha_\epsilon}(x),$$

where

$$a_\epsilon(x) = \sum_{u=0}^{k_{\alpha_\epsilon}-1} \omega_{1\epsilon}^{q^u} e_{(1+ti_{\alpha_\epsilon})q^u}(x) \in \mathcal{R}\theta_{\alpha_\epsilon}(x), \omega_{1\varepsilon} \in \mathbb{F}_{q^{k_{\alpha_\epsilon}}}, \forall\ 1 \le \epsilon \le v;$$

$$b_\epsilon(x) = \sum_{u=0}^{k_{\alpha_\epsilon}-1} \omega_{2\epsilon}^{q^u} e_{(1+ti_{\alpha_\epsilon})q^u}(x) \in \mathcal{R}\theta_{\alpha_\epsilon}(x), \omega_{2\varepsilon} \in \mathbb{F}_{q^{k_{\alpha_\epsilon}}}, \forall\ 1 \le \epsilon \le v.$$

Then, for any $r \in \mathbb{Z}^+$, $\phi^r(f(x)) = g(x)$ if and only if

$$\begin{aligned} g(x) &= \sum_{\epsilon=1}^{v} \sum_{u=0}^{k_{\alpha_\epsilon}-1} \omega_{2\varepsilon}^{q^u} e_{(1+ti_{\alpha_\epsilon})q^u}(x) \\ &= \phi^r(f(x)) = \sum_{\epsilon=1}^{v} \sum_{u=0}^{k_{\alpha_\epsilon}-1} (\eta^{r(1+ti_{\alpha_\epsilon})} \omega_{1\epsilon})^{q^u} e_{(1+ti_{\alpha_\epsilon})q^u}(x), \end{aligned}$$

which holds if and only if

$$\eta^{r(1+ti_{\alpha_\epsilon})} \omega_{1\epsilon} = \omega_{2\epsilon}, \epsilon = 1, 2, \cdots, v,$$

which shows that both $\sum_{\epsilon=1}^{v}\omega_{1\epsilon}$ and $\sum_{\epsilon=1}^{v}\omega_{2\epsilon}$ are in the same coset of

$$\Big\langle \sum_{\kappa=1}^{v} \eta^{1+ti_{\alpha_\kappa}} \Big\rangle = \langle \eta^{1+ti_{\alpha_1}} + \eta^{1+ti_{\alpha_2}} + \cdots + \eta^{1+ti_{\alpha_v}} \rangle = G_3$$

in the group

$$\bigoplus_{\kappa=1}^{v} \mathcal{R}\theta_{\alpha_\kappa}(x)\backslash\{0\} = \bigoplus_{\kappa=1}^{v} \mathbb{F}_{q^{\alpha_\kappa}}\backslash\{0\} = \bigoplus_{\kappa=1}^{v} \mathbb{F}_{q^{\alpha_\kappa}}^{\times} = G_1.$$

By virtue of the result shown in (4.4), we immediately obtain this theorem. □

At the end of this section, we present an example to illustrate our main results.

Example 4.3. *Let $q = 5, n = 18$, and $\lambda = 4$. All 5-cyclotomic cosets are as follows:*

$$C_0 = \{1, 5, 25, 17, 13, 29\}, C_1 = \{3, 15\}, C_2 = \{7, 35, 31, 11, 19, 23\}, C_3 = \{9\}, C_4 = \{21, 33\}, C_5 = \{27\}.$$

Then, $t = 2$ and

$$i_0 = 0, i_1 = 1, i_2 = 3, i_3 = 4, i_4 = 10, i_5 = 13;$$

$$k_0 = 6, k_1 = 2, k_2 = 6, k_3 = 1, k_4 = 2, k_5 = 1.$$

Assume that five constacyclic codes C_1, C_2, C_3, C_4, C_5 are as follows:

$$C_1 = \mathcal{R}\theta_1(x);\ C_2 = \mathcal{R}\theta_2(x);\ C_3 = \mathcal{R}\theta_3(x) \oplus \mathcal{R}\theta_4(x);$$

$$C_4 = \mathcal{R}\theta_1(x) \oplus \mathcal{R}\theta_2(x);\ C_5 = \mathcal{R}\theta_0(x) \oplus \mathcal{R}\theta_2(x).$$

Set $\mathbb{F}_{5^2}^{\times} = \langle\gamma_1\rangle$ and $\mathbb{F}_{5^6}^{\times} = \langle\gamma_2\rangle$. Then, we have the following:

(1) *According to Lemma 3.3, since* $\gcd(n, 1+ti_1) = \gcd(18, 3) = 3 \neq 1$, *none of the nonzero elements of C_1 has full constacyclic order.*

(2) *According to Lemma 3.3, the fact that* $\gcd(n, 1 + ti_2) = \gcd(18, 7) = 1$ *shows that every nonzero element of C_2 has full constacyclic order; thus*

$$|C_2'| = \frac{q^{k_7} - 1}{nt} = \frac{5^6 - 1}{36} = 434.$$

By using Theorem 4.1, we get that

$$C_2' = \Big\{ \sum_{u=0}^{5} \gamma_1^{\ell \cdot 5^u} e_{7\cdot 5^u} \Big| 0 \leq \ell \leq 433 \Big\}.$$

(3) *According to Lemmas 3.3 and 3.4, since*

$$\gcd(n, 1 + ti_3) = \gcd(18, 9) = 9 \neq 1;$$

$$\gcd(n, 1 + ti_4) = \gcd(18, 21) = 3 \neq 1;$$

$$\gcd(n, 1 + ti_3, 1 + ti_4) = \gcd(18, 9, 21) = 3 \neq 1,$$

none of the nonzero elements of C_3 has full constacyclic order.

(4) *Since*

$$\gcd(n, 1+ti_1) = \gcd(18, 3) = 3 \neq 1;$$

$$\gcd(n, 1+ti_2) = \gcd(18, 7) = 1;$$

$$\gcd(n, 1+ti_1, 1+ti_2) = \gcd(18, 3, 7) = 1,$$

then,

$$\Theta_1 = \{\{2\}\}; \Theta_2 = \{\{1, 2\}\}.$$

By Theorem 3.5, we get that

$$|C_4'| = \frac{1}{nt}[(q^{k_2}-1)+(q^{k_1}-1)(q^{k_2}-1)] = \frac{1}{nt}q^{k_1}(q^{k_2}-1) = \frac{1}{36}\cdot 5^2 \cdot (5^6-1) = 10850.$$

In addition,

$$m_1 = \frac{(q^{k_1}-1)\gcd(n, 1+ti_1)}{nt} = \frac{(5^2-1)\gcd(18, 3)}{36} = 2.$$

$$m_2 = \frac{(q^{k_2}-1)}{nt} = \frac{5^6-1}{36} = 434.$$

$$n_2 = \frac{nt\gcd(n, 1+ti_1, 1+ti_2)}{\gcd(n, 1+ti_1)\gcd(n, 1+ti_2)} = \frac{36\gcd(18, 3, 7)}{\gcd(18, 3)\gcd(18, 7)} = 12.$$

By Theorem 4.2, we have that

$$\begin{aligned} C_4' &= \bigcup_{\varepsilon_2=0}^{433}\Big\{\sum_{u=0}^{24}(\gamma_1^{\varepsilon_2}\theta^{1+ti_2})^{q^u}e_{(1+ti_2)q^u}(x)\Big\}\bigcup \\ &\quad \bigcup_{\varepsilon_1=0}^{1}\bigcup_{\varepsilon_2=0}^{433}\bigcup_{\sigma_2=0}^{11}\Big\{\sum_{\epsilon=1}^{2}\sum_{\kappa=1}^{2}\sum_{j=1}^{2}\sum_{u=0}^{24}(\gamma_2^{\varepsilon_\kappa}\theta^{\sigma_j(1+ti_j)})^{q^u}e_{(1+ti_\epsilon)q^u}(x)\Big\} \\ &= \bigcup_{\varepsilon_2=0}^{433}\Big\{\sum_{u=0}^{24}(\gamma_1^{\varepsilon_2}\theta^{7})^{5^u}e_{7\cdot 5^u}(x)\Big\}\bigcup \\ &\quad \bigcup_{\varepsilon_1=0}^{1}\bigcup_{\varepsilon_2=0}^{433}\bigcup_{\sigma_2=0}^{11}\Big\{\sum_{\epsilon=1}^{2}\sum_{\kappa=1}^{2}\sum_{j=1}^{2}\sum_{u=0}^{24}(\gamma_2^{\varepsilon_\kappa}\theta^{\sigma_j(1+2i_j)})^{5^u}e_{(1+2i_\epsilon)5^u}(x)\Big\}. \end{aligned}$$

Here, from the formula of C_4', we can also get that

$$|C_4'| = 434 + 2\times 434\times 12 = 10850,$$

which is the same as the above result provided by Theorem 3.5.

(5) *Since*

$$\gcd(n, 1+ti_0) = \gcd(18, 1) = 1;$$

$$\gcd(n, 1+ti_2) = \gcd(18, 7) = 1;$$

$$\gcd(n, 1+ti_0, 1+ti_2) = \gcd(18, 1, 7) = 1,$$

then

$$\Theta_1 = \{\{0\},\{2\}\};\Theta_2 = \{\{0,2\}\}.$$

By Theorem 3.5, we get that

$$|C_5'| = \frac{1}{nt}[(q^{k_0}-1)+(q^{k_2}-1)+(q^{k_0}-1)(q^{k_2}-1)] = \frac{1}{36}[(5^6-1)+(5^6-1)+(5^6-1)(5^6-1)] = 6781684.$$

In addition,

$$\begin{aligned} m_1 &= \frac{(q^{k_0}-1)\gcd(n,1+ti_0)}{nt} = \frac{(5^6-1)\gcd(18,1)}{36} = 434.\\ m_2 &= \frac{(q^{k_2}-1)\gcd(n,1+ti_2)}{nt} = \frac{(5^6-1)\gcd(18,7)}{36} = 434.\\ n_2 &= \frac{nt\gcd(n,1+ti_0,1+ti_2)}{\gcd(n,1+ti_0)\gcd(n,1+ti_2)} = \frac{36\gcd(18,1,7)}{\gcd(18,1)\gcd(18,7)} = 36. \end{aligned}$$

By Theorem 4.2, we have that

$$\begin{aligned} C_5' \;&=\; \bigcup_{\varepsilon_1=0}^{433}\Big\{\sum_{u=0}^{15624}(\gamma_1^{\varepsilon_1}\theta^{1+ti_0})^{q^u}e_{(1+ti_0)q^u}(x)\Big\}\bigcup\bigcup_{\varepsilon_2=0}^{433}\Big\{\sum_{u=0}^{15624}(\gamma_2^{\varepsilon_2}\theta^{1+ti_2})^{q^u}e_{(1+ti_2)q^u}(x)\Big\}\bigcup\\ &\bigcup_{\varepsilon_1=0}^{433}\bigcup_{\varepsilon_2=0}^{433}\bigcup_{\sigma_2=0}^{35}\Big\{\sum_{\epsilon=1}^{2}\sum_{\kappa=1}^{2}\sum_{j=1}^{2}\sum_{u=0}^{15624}(\gamma_2^{\varepsilon_\kappa}\theta^{\sigma_j(1+ti_j)})^{q^u}e_{(1+ti_\epsilon)q^u}(x)\Big\}\\ &=\; \bigcup_{\varepsilon_1=0}^{433}\Big\{\sum_{u=0}^{15624}(\gamma_1^{\varepsilon_1}\theta)^{5^u}e_{1\cdot 5^u}(x)\Big\}\bigcup\bigcup_{\varepsilon_2=0}^{433}\Big\{\sum_{u=0}^{15624}(\gamma_2^{\varepsilon_2}\theta^7)^{5^u}e_{7\cdot 5^u}(x)\Big\}\bigcup\\ &\bigcup_{\varepsilon_1=0}^{433}\bigcup_{\varepsilon_2=0}^{433}\bigcup_{\sigma_2=0}^{35}\Big\{\sum_{\epsilon=1}^{2}\sum_{\kappa=1}^{2}\sum_{j=1}^{2}\sum_{u=0}^{15624}(\gamma_\kappa^{\varepsilon_\kappa}\theta^{\sigma_j(1+2i_j)})^{5^u}e_{(1+2i_\epsilon)5^u}(x)\Big\}. \end{aligned}$$

Here, from the formula of C_5', we can also get that

$$|C_5'| = 434 + 434 + 434\times 434\times 36 = 6781684,$$

which is the same as the above result provided by Theorem 3.5.

5. Conclusions

In this paper, we have introduced the definition of CCPCs and mainly focused on the construction of such a class of codes. First, we proposed a new and explicit enumerative formula for the code size of such CCPCs. Next, we provided an effective method to obtain such a CCPC by using an algebraic tool. A possible direction for future work is to consider the problem of constructing CCPCs with the largest possible code size from a given repeated-root constacyclic code.

Use of AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

We sincerely thank the Associate Editor and the anonymous referees for their carefully reading and helpful suggestions that led to the improvement of the paper.

G. Zhang was supported by the Guiding Science and Technology Plan Project of Suqian City in 2023.

Conflict of interest

The authors declare no conflicts of interest.

References

1. E. N. Gilbert, Cyclically permutable error-correcting codes, *IEEE T. Inform. Theory*, **9** (1963), 175–182. https://doi.org/10.1109/TIT.1963.1057840
2. L. Györfi, I. Vajda, Constructions of protocol sequence for multiple access collision channel without feedback, *IEEE T. Inform. Theory*, **39** (1993), 1762–1765. https://doi.org/10.1109/18.259673
3. Q. A. Nguyen, L. Györfi, J. L. Massey, Constructions of binary constant-weight cyclic codes and cyclically permutable codes, *IEEE T. Inform. Theory*, **38** (1992), 940–949. https://doi.org/10.1109/18.135636
4. S. Katzenbeisser, F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Norwood, MA: Artech House, 2000.
5. S. Sriram, S. Hosur, Cyclically permutable codes for rapid acquisition in DS-CDMA systems with asynchronous base stations, *IEEE J. Sel. Area. Comm.*, **19** (2001), 83–94. https://doi.org/10.1109/49.909611
6. B. Chen, L. Lin, S. Ling, H. Liu, Three new classes of optimal frequency-hopping sequence sets, *Design. Code. Cryptogr.*, **83** (2017), 219–232. https://doi.org/10.1007/s10623-016-0220-9
7. C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, M. Mishima, Sets of frequency hopping sequences: Bounds and optimal constructions, *IEEE T. Inform. Theory*, **55** (2009), 3297–3304. https://doi.org/10.1109/TIT.2009.2021366
8. H. Y. Song, I. S. Reed, S. W. Golomb, On the nonperiodic cyclic equivalence classes of Reed-Solomon codes, *IEEE T. Inform. Theory*, **39** (1993), 1431–1434. https://doi.org/10.1109/18.243465
9. S. B. Wicker, V. K. Bhargava, *Reed-Solomon codes and their applications*, IEEE Press, New York, 1994.
10. S. Bitan, T. Etzion, Constructions for optimal binary constant-weight cyclically permutable codes and difference families, *IEEE T. Inform. Theory*, **41** (1995), 77–87. https://doi.org/10.1109/18.370117
11. Q. A. Nguyen, L. Györfi, J. L. Massey, Constructions of binary constant-weight cyclic codes and cyclically permutable codes, *IEEE T. Inform. Theory*, **38** (1992), 940–949. https://doi.org/10.1109/18.135636

12. J. S. Lemos-Neto, V. C. da Rocha Jr., Cyclically permutable codes specified by roots of generator polynomial, *Electron. Lett.*, **50** (2014), 1202–1204. https://doi.org/10.1049/el.2014.0296
13. D. E. Maracle, C. T. Wolverton, Generating cyclically permutable codes, *IEEE T. Inform. Theory*, **20** (1974), 554–555. https://doi.org/10.1109/TIT.1974.1055243
14. D. H. Smith, S. Perkins, Cyclically permutable representations of cyclic codes, *Discrete Appl. Math.*, **156**, 76–81, 2008. https://doi.org/10.1016/j.dam.2007.08.038
15. F. Fu, S. Shen, On the nonperiodic cyclic equivalence classes of Hamming codes and BCH codes, *J. Stat. Plan. Infer.*, **140** (2001), 205–209. https://doi.org/10.1016/S0378-3758(00)00253-6
16. S. E. Tavares, P. E. Allard, S. G. S. Shiva, On decomposition of cyclic codes into cyclic classes, *Inf. Control*, **18** (1971), 342–354. https://doi.org/10.1016/S0019-9958(71)90446-3
17. P. E. Allard, S. G. S. Shiva, S. E. Tavares, A note on the decomposition of cyclic codes into cyclic classes, *Inf. Control*, **22** (1973), 100–106. https://doi.org/10.1016/S0019-9958(73)90518-4
18. S. Xia, F. Fu, *Nonperiodic cyclic equivalence classes of cyclic codes and algebraic constructions of cyclically permutable codes*, Proc. 12th Int. Symp. Applied Algebra, Algebraic Algorithms, Error-Correcting Codes, 1997, 341–352. https://doi.org/10.1007/3-540-63163-1_27
19. M. Kuribayashi, H. Tanaka, How to generate cyclically permutable codes from cyclic codes, *IEEE T. Inform. Theory*, **52** (2006), 4660–4663. https://doi.org/10.1109/TIT.2006.881834
20. T. Y. Yang, H. Chen, K. C. Chung, *Generation of cyclically permutable codes by Galois field Fourier transform*, Int. Conf. on Ubiquitous and Future Networks (ICUFN 2016), 2016, 322–325. https://doi.org/10.1109/ICUFN.2016.7537041
21. K. P. Cho, C. L. Lin, H. Chen, T. Y. Yang, *Construction of cyclically permutable codes from prime length cyclic codes*, 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Auckland, New Zealand, 2020, 1448–1452.
22. G. T. Bastos, J. S. de Lemos-Neto, On the cyclic order distribution and partitioning of linear cyclic codes, *São Paulo J. Math. Sci.*, **15** (2021), 404–418. https://doi.org/10.1007/s40863-020-00197-x
23. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003. https://doi.org/10.1017/CBO9780511807077
24. F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Company, 1997.
25. B. Chen, H. Liu, G. Zhang, Some minimal cyclic codes over finite fields, *Discrete Math.*, **331** (2014), 142–150. https://doi.org/10.1016/j.disc.2014.05.007
26. S. Roman, *Coding and information theory*, Springer-Verlag, 1992.