Construction of Cyclically Permutable Codes From Prime Length Cyclic Codes

Keng Pei Cho, Chun-Long Lin, Houshou Chen, and Ting-Ya Yang
Dept. of Electrical Engineering and Graduate Institute of Communication Engineering
National Chung Hsing University, 145, Xingda Rd., Taichung 402, Taiwan
E-mail: houshou@dragon.nchu.edu.tw Tel/Fax: +886-22840688

***Abstract*—This paper proposes a novel algorithm to find the cyclically permutable codes (CPCs) from a cyclic code. In recent years, the CPCs are increasingly important, and have been applied in the communication network and optical communication. A CPC is a block code such that each codeword has full cyclic order and all codewords are cyclically distinct. In this paper, we use the characteristics of finite fields to develop an efficient algorithm to find a CPC from a q-ary cyclic code with prime length. More precisely, we propose an effective methods to find all codewords with full cyclic order from a cyclic code for prime-primitive length and prime-nonprimitive length respectively.**

I. Introduction

A cyclic code is a liner codes such that any cyclic shift of a codeword is another codeword. Gilbert [1] defined a cyclically permutable code as a block code of length n, such that each codeword has cyclic order n and any cyclic shift of all codewords are distinct, i.e., no codeword in CPC can be obtained by any cyclic shift of another codeword.

The cyclically permutable codes have been applied in the communication network, optical communication, and image processing. The applications of CPC include multiple access collision channel without feedback [2], [3], frequency-hopping spread spectrum communication channels [4], [5], optical orthogonal codes, and digital watermarking [6], [7]. Q. A. Nguyen, L. Gyorfi, and J. L. Massey [8] processed an encoding procedure for obtaining CPC from a Reed-Solomon (RS) code of length $p-1$ or of length $p+1$. In [9], the authors proposed an algebraic approach that selects a large subset of codewords with a full cyclic order to construct a constant-weight CPC for prime and primitive length. In [10], on the basis of the combinatorial design of a difference family, several constructions for constant-weight CPC are presented. However there have been no efficient methods proposed so far to find a CPC for non-primitive length.

Fourier transforms exist in the Galois field $GF(q^m)$, which is important in the study and processing of cyclic codes. As opposed to [9], [11], [12], which used the generator polynomial to find a CPC, this study proposes the use of the Galois field Fourier transform (GFFT) as an efficient method to find many CPCs from cyclic codes. This paper is the extension of the results in [8] and [13]. More precisely, this study extends the results of [8] and [13] in twofold advantages. First, for a cyclic code of non-primitive length $n=(p^m-1)/s$, $s>1$, and dimension k, we can construct a CPC with $s\cdot p^{k-m}$ codewords. The CPC constructed here has s times more codewords compared to the CPC constructed in [8]. Secondly, let $\alpha^i, i>1$, be a nonzero element for a RS code of primitive length $p-1$ and assume i and $p-1$ are relative prime, we can then construct a CPC which has more than p^{k-1} codewords for $s=1$, namely $n=p^m-1$.

The remainder of this paper is organized as follows. In Section II, we review some basic properties of cyclic codes and Galois field Fourier transform, such as the conjugate and cyclic shift properties. Section III uses these two properties to find the CPC from a cyclic code and provide the CPC examples for code length equal to prime-primitive and prime-nonprimitive. Finally, Section IV presents the conclusion.

II. Cyclic codes and Galois field Fourier transform

A linear code $C[n,k,d]$ over F_q is a k-dimensional subspace of F_q^n such that the minimum distance of C is d. An encoding of $C[n,k]$ refers to any linear bijection from F_q^k to F_q^n. More precisely, a $k\times n$ matrix G that has a basis of the code C as its row vector is called a generator matrix of C. Usually, we denote a linear code with a generator matrix G by $C=\langle G\rangle$.

A. Cyclic codes

A linear code C of length n is a cyclic code if every codeword of C is invariant under a cyclic shift, i.e., if

$$c=(c_0,c_1,c_2,\cdots,c_{n-2},c_{n-1})\in C$$

then

$$(c_{n-1},c_0,c_1,\cdots,c_{n-3},c_{n-2})\in C.$$

We will also use $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ to refer the codeword c. Clearly, it can be shown that cyclic shift of any positions of a codeword in C is also another codeword [14]. The element in finite field $GF(q^m)$ are represented by $\{0,\alpha^0,\alpha^1,\alpha^2,\cdots,\alpha^{n-1}\}$, where $n=q^m-1$ and α denotes a root of a primitive polynomial of degree m, and each nonzero element is the root of $x^{n-1}-1$.

Let $S=\{\alpha^0,\alpha^1,\cdots,\alpha^{n-1}\}$ and $Z=\{\alpha^{i_1},\alpha^{i_2},\cdots,\alpha^{i_{n-k}}\}\subset S$. A cyclic code $C[n,k]$ with Z as nonzeros of the code can be described by a polynomial $g(x)=$

$$(x-\alpha^{i_1})(x-\alpha^{i_2})\cdots(x-\alpha^{i_{n-k}})=g_0+g_1x+\cdots+g_{n-k}x^{n-k}.$$

This minimum degree polynomial $g(x)$ generates C, i.e., $C=\langle g(x)\rangle=\{a(x)g(x):\deg a(x)<k\}$, and $g(x)$

is called the generator polynomial of C. The polynomial $h(x) = (x^n - 1)/g(x)$ is called the check polynomial of C. The roots of $g(x)$ and $h(x)$ are called the nonzeros and zeros of the code respectively. Moreover, the codeword of $C = (c_0, c_1, \cdots, c_{n-1})$ can be generated as follow:

$$C = u \cdot \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ & \vdots & & \vdots & & \vdots & 0 \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}.$$

Where $u = u_0, u_1, \cdots, u_{k-1}$.

B. Galois field Fourier transform

Cyclic codes can also be defined as codes whose codewords have certain specified spectral components that are equal to zeros [14], [15]. Let $v = (v_0, v_1, \cdots, v_{n-1})$ be a vector of length n over $GF(q^m)$, and let α be an element of $GF(q^m)$ of order n, where n is a divisor of $q^m - 1$ for some positive number. The Galois field Fourier transform (GFFT) of the vector v in time-domain is $v = (v_0, v_1, \cdots, v_{n-1})$ in frequency-domain defined as

$$\begin{pmatrix} V_0 \\ V_1 \\ \vdots \\ V_{n-1} \end{pmatrix} = \begin{pmatrix} (\alpha^0)^0 & \cdots & (\alpha^0)^{n-1} \\ (\alpha^1)^0 & \cdots & (\alpha^1)^{n-1} \\ \vdots & \cdots & \vdots \\ (\alpha^{n-1})^0 & \cdots & (\alpha^{n-1})^{n-1} \end{pmatrix} \cdot \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix}.$$

The GFFT can be also written by the formula

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i, \qquad j = 0, 1, \cdots, n-1. \tag{1}$$

We will use $v \leftrightarrow V$ to denote the GFFT relationship between v and V. Similarly, the inverse GFFT can also be written as

$$v_i = n^{-1} \sum_{j=0}^{n-1} \alpha^{-ij} V_j, \qquad i = 0, 1, \cdots, n-1. \tag{2}$$

where n^{-1} is the vector multiplicative inverse of n.

We can represent a vector $v = (v_0, v_1, \cdots, v_{n-1})$ by a polynomial $v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ and $V = (V_0, V_1, \cdots, V_{n-1})$ by a polynomial $V(x) = V_0 + V_1 x + \cdots + V_{n-1} x^{n-1}$. Given a polynomial $v(x)$, we can show that

$$V_j = \sum_{i=0}^{n-1} v_i (\alpha^j)^i = v(\alpha^j). \tag{3}$$

The j-th component of the GFFT of v is obtained by evaluating $v(x)$ at $x = \alpha^j$. Similarly, we can write the i-th component of v as

$$v_i = \frac{1}{n} \sum_{j=0}^{n-1} V_j (\alpha^{-i})^j = \frac{1}{n} V(\alpha^{-i}). \tag{4}$$

In other words, α^{-i} is a zero of $V(x)$ if and only if $v_i = 0$.

C. Cyclic shift and conjugate property

The cyclic shift property of GFFT is known as follows.

$$\begin{gathered} v = (v_0, \cdots, v_t, \cdots, v_{n-1}) = (v_l)_{l=0\sim n-1} \\ \updownarrow \\ V = (V_0, \cdots, V_t, \cdots V_{n-1}) = (V_l)_{l=0\sim n-1} \end{gathered}$$

$$\begin{gathered} (v_{n-t}, \cdots, v_0, \cdots, v_{n-1-t}) \\ \updownarrow \\ (V_0(\alpha^{-0} \cdot \alpha^{-t}), \cdots, V_t(\alpha^{-t} \cdot \alpha^{-t}), \\ \cdots, V_{n-1}(\alpha^{-(n-1)} \cdot \alpha^{-t})). \end{gathered}$$

When v_0 cyclic shifts t units, the original V_0 will multiplied by α^{-t}. Because α is in finite field $GF(q^m)$, α must satisfy the conjugate property, namely,

$$\{(\alpha^l)^{q^b}\}_{b=0\sim m-1}.$$

The index of α is defined by mod n, and the group of repetitions is the same group.

Let a code is a cyclic code $C[n, k, d]$. So we have to choose $d-1$ consecutive roots. The degree of $g(x)$ is equal to $n-k$. Let $\{(\alpha^x)^{q^b}\}_{x=1\sim d-1}$ are zeros, and the remaining elements are nonzeros defined as

$$\{(\alpha^l)^{q^b}\}_{b=0\sim m-1} = \begin{cases} \{(\alpha^x)^{q^b}\}_{x=1\sim d-1}, & if \quad zeros. \\ \{(\alpha^l)^{q^b}\}/\{(\alpha^x)^{q^b}\}, & if \quad nonzeros. \end{cases}$$

The inverse of nonzeros of C is defined as

$$\{(\alpha^{-h})\}_{h=\{lq^b\}-\{xq^b\}}.$$

Then we can use the inverse of the nonzeros of a cyclic code to form the generator matrix G as

$$G = \{(\alpha^{-h})^{\mathrm{T}}\}^j = \begin{pmatrix} (\alpha^0)^j \\ (\alpha^{-dq^0})^j \\ (\alpha^{-dq^1})^j \\ \vdots \\ (\alpha^{-dq^{m-1}})^j \\ \vdots \\ (\alpha^{-(n-1)q^0})^j \\ (\alpha^{-(n-1)q^1})^j \\ \vdots \\ (\alpha^{-(n-1)q^{m-1}})^j \end{pmatrix}_{k \times n} \tag{5}$$

where $j = 0 \sim n-1$.

With the conjugate property and cyclic shift property of GFFT, we propose the concept using G matrix in (5) to obtain the CPC as follows. Let $C[n, k, d]$ be a cyclic code over $GF(q^m)$, where n is a divisor of $q^m - 1$. From the G matrix

in (5), the codewords of C can be obtained by

$$C = u \cdot \begin{pmatrix} (\alpha^0)^j \\ (\alpha^{-dq^0})^j \\ (\alpha^{-dq^1})^j \\ \vdots \\ (\alpha^{-dq^{m-1}})^j \\ \vdots \\ (\alpha^{-(n-1)q^0})^j \\ (\alpha^{-(n-1)q^1})^j \\ \vdots \\ (\alpha^{-(n-1)q^{m-1}})^j \end{pmatrix}_{k\times n}, \quad j = 0 \sim (n-1)$$

where $u = (u_0, u_{-dq^0}, \cdots, u_{-dq^{m-1}}, \cdots, u_{-(n-1)q^0}, \cdots, u_{-(n-1)q^{m-1}}) = (u_{(-h)})$. There are a total of k. Let u of index be L, namely, $(-h) = L$.

For example, the double-error correcting BCH code $C[15, 7, 5]$ has zeros $\{\alpha^1, \alpha^2, \alpha^4, \alpha^8\} \cup \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$. The nonzeros are $\{\alpha^0\} \cup \{\alpha^5, \alpha^{10}\} \cup \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$. Then we can use the inverse of the nonzeros to get the generator matrix G as

$$G = \left(\begin{array}{cccc} (\alpha^0)^0 & (\alpha^0)^1 & \cdots & (\alpha^0)^{14} \\ \hline (\alpha^1)^0 & (\alpha^1)^1 & \cdots & (\alpha^1)^{14} \\ (\alpha^2)^0 & (\alpha^2)^1 & \cdots & (\alpha^2)^{14} \\ (\alpha^4)^0 & (\alpha^4)^1 & \cdots & (\alpha^4)^{14} \\ (\alpha^8)^0 & (\alpha^8)^1 & \cdots & (\alpha^8)^{14} \\ \hline (\alpha^5)^0 & (\alpha^5)^1 & \cdots & (\alpha^5)^{14} \\ (\alpha^{10})^0 & (\alpha^{10})^1 & \cdots & (\alpha^{10})^{14} \end{array}\right)$$

The codewords of $C = (c_0, c_1, \cdots, c_{14})$ are obtained by

$$C = u \cdot G = (u_0, u_1u_2u_4u_8, u_5u_{10}) \cdot G$$

where $u_0 \in GF(2)$, $u_1 \in GF(2^4)$, and $u_5 \in GF(2^2)$. $u_1u_2u_4u_8$ is the same conjugate group, so u_1 is determined, $u_2u_4u_8$ will follow u_1. The same is true for u_5u_{10}. There are $2^1 \cdot 2^4 \cdot 2^2 = 2^7$ codewords.

Let $c(x)$ be a codeword of a cyclic code C. The cyclic shift subset of $c(x)$ is defined as $\langle c(x)\rangle = \{c(x), xc(x), \cdots, x^{e-1}c(x)\}$, when e is the smallest number such that $x^e c(x) = c(x)$. We call e the cyclic order of the codeword $c(x)$. To form a CPC from a cyclic code $C[n, k]$, we first find those codewords $c(x)$ in C with cyclic order equal to n, and then use the cyclic shift property of GFFT to find one codeword from the cyclic shift subset $\langle c(x)\rangle$.

If $gcd(n, L) = 1$, then the order of the element α^L is n and we can use any nonzeros frequency index V_L to find codewords of CPC. For example, let $u_1 = \alpha^0$, the codewords of CPC from $C[15, 7, 5]$ are obtained by

$$C = (u_0, \underbrace{u_1}_{=\alpha^0} u_2u_4u_8, u_5u_{10}) \cdot G$$

where $u_0 \in GF(2)$ and $u_5 \in GF(2^2)$. The number of codewords of CPC from $[15, 7, 5]$ is $2^1 \cdot 1 \cdot 2^2 = 8$.

III. CONSTRUCTIONS OF CYCLICALLY PERMUTABLE CODES

A CPC is a binary block code whose codewords are cyclically distinct and have full order. In this section, we use the conjugate and cyclic shift properties to find the CPC from a cyclic code and provide the CPC examples for code length n equal to prime and non-primitive. Let $c(x)$ be a codeword of a cyclic code C. The cyclic shift subset of $c(x)$ is defined as $\langle c(x)\rangle = \{c(x), xc(x), \cdots, x^{e-1}c(x)\}$, when e is the smallest number such that $x^e c(x) = c(x)$. We call e the cyclic order of the codeword $c(x)$. To form a CPC from a cyclic code $C[n, k]$, we first find those codewords $c(x)$ in C with cyclic order equal to n, and then use the cyclic shift property of GFFT to find one codeword from the cyclic shift subset $\langle c(x)\rangle$.

A. Prime and primitive length

When length n is primitive and prime, then $gcd(n, L) = 1$, the order of the element α^L is n and we can use any nonzero frequency index $V_L = u_L$ to find codewords of CPC. For example a [7,4,3] BCH code over F_2. Where the degree is $m = 3$ and where $n = 2^3 - 1$ is prime and has primitive length. The cyclotomic coset is $\{\alpha^0\}$, $\{\alpha^1, \alpha^2, \alpha^4\}$ and $\{\alpha^3, \alpha^6, \alpha^5\}$. Select zeros roots are $\{\alpha^1, \alpha^2, \alpha^4\}$. So nonzeros roots are $\{\alpha^0\}$ and $\{\alpha^3, \alpha^6, \alpha^5\}$. Then we can obtain the generated matrix through the nonzeros inverse roots and encoding of $C = (c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ in frequency-domain by

$$c = (u_0, u_1u_2u_4) \cdot \left(\begin{array}{cccc} (\alpha^0)^0 & (\alpha^0)^1 & \cdots & (\alpha^0)^{n-1} \\ \hline (\alpha^1)^0 & (\alpha^1)^1 & \cdots & (\alpha^1)^{n-1} \\ (\alpha^2)^0 & (\alpha^2)^1 & \cdots & (\alpha^2)^{n-1} \\ (\alpha^4)^0 & (\alpha^4)^1 & \cdots & (\alpha^4)^{n-1} \end{array}\right).$$

The information bits $(u_1u_2u_4)$ is conjugate roots for binary codes. Then $u_0 \in GF(2)$ and $u_1 \in GF(2^3)$, there are $2^1 \cdot 2^3 = 2^4$ codewords. For the CPC desired use the **cyclic shift property**, and first let $(u_1u_2u_4) = (\alpha^0\alpha^0\alpha^0)$ and $u_0 \in GF(2)$ may by 0 or α^0. As shown in Tab. I, t is cyclic shift in this table. Therefore, $u_1 = \alpha^0 \sim \alpha^{-6}$ do cyclic shifts for the same cyclic code, so α^0 is taken as a representative. Respectively, we obtain a total CPC number of $p^{k-m} = 2^{4-3} = 2$ that the order is $n = 7$. The result is shown in Fig. 1.

TABLE I
CPC SCHEMATIC OF PRIMITIVE BY ONE INDEX.

$t=0$	$t=1$	$t=2$	$t=3$	$t=4$	$t=5$	$t=6$
α^0	α^{-1}	α^{-2}	α^{-3}	α^{-4}	α^{-5}	α^{-6}

B. Prime and nonprimitive length

Lemma 1: For every non-primitive length n, which that $n \neq p^m - 1$, we can obtain more s times of CPC with full cyclic order n.

Proof: For a (n, k) cyclic code over F_p, there exist p^k codewords. Further, based on Lemma 1, when n is non-primitive length, $o(\alpha) = n$ and $n|p^m - 1$. Let $\beta \in F_{p^m}$

primitive element, and $O(\beta) = p^m - 1$, at the same time we can find that $\alpha = \beta^{\frac{p^m-1}{n}} = \beta^s$. We obtain to the following formula

$$u_1^{(t)} = (\alpha^{-t})u_1 = (\beta^{-\frac{p^{m-1}}{n}\cdot t})u_1 = (\beta^{-s\cdot t})u_1 \tag{6}$$

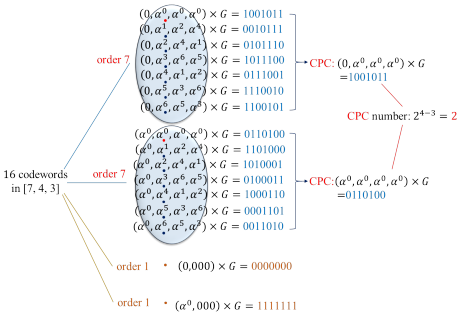

Fig. 1. CPCs constructed by [7,4,3] cyclic code.

where u_1 cyclic shift t units is $u_1^{(t)}$. Which shown in the following Tab. II.

TABLE II
CPC SCHEMATIC OF NON-PRIMITIVE BY ONE INDEX.

$\alpha^0 = \beta^0$	$\alpha^{-1} = \beta^{-s}$	$\alpha^{-2} = \beta^{-2s}$	$\cdots$	$\alpha^{-(n-1)} = \beta^{-(n-1)s}$
β^{-1}	$\beta^{-(s+1)}$	$\beta^{-(2s+1)}$	$\cdots$	$\beta^{-((n-1)s+1)}$
β^{-2}	$\beta^{-(s+2)}$	$\beta^{-(2s+2)}$	$\cdots$	$\beta^{-((n-1)s+2)}$
β^{-3}	$\beta^{-(s+3)}$	$\beta^{-(2s+3)}$	$\cdots$	$\beta^{-((n-1)s+3)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\beta^{-(s-1)}$	$\beta^{-(2s-1)}$	$\beta^{-(3s-1)}$	$\cdots$	$\beta^{-(ns-1)}$

Example1: Consider (17,9,5) of BCH code over $F_{2^8} = \frac{F_2[x]}{x^8+x^4+x^3+x^2+1}$, when $m = 8$ and $\alpha = \beta^{(p^m-1)/n} = \beta^{(2^8-1)/17} = \beta^{15}$, the distribution of cyclotomic coset is $\{\alpha^0\}$, $\{\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{15}, \alpha^{13}, \alpha^9\}$ and $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^7, \alpha^{14}, \alpha^{11}, \alpha^5, \alpha^{10}\}$. Select zeros roots are $\{\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{15}, \alpha^{13}, \alpha^9\}$. So non-zero roots are $\{\alpha^0\}$ and $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^7, \alpha^{14}, \alpha^{11}, \alpha^5, \alpha^{10}\}$. Then we can obtain the generated matrix through the non-zeros inverse roots. Form a generated matrix as following

$$G = \begin{pmatrix} (\alpha^0)^0 & (\alpha^0)^1 & \cdots & (\alpha^0)^{16} \\ \hline (\alpha^3)^0 & (\alpha^3)^1 & \cdots & (\alpha^3)^{16} \\ (\alpha^6)^0 & (\alpha^6)^1 & \cdots & (\alpha^6)^{16} \\ (\alpha^{12})^0 & (\alpha^{12})^1 & \cdots & (\alpha^{12})^{16} \\ (\alpha^7)^0 & (\alpha^7)^1 & \cdots & (\alpha^7)^{16} \\ (\alpha^{14})^0 & (\alpha^{14})^1 & \cdots & (\alpha^{14})^{16} \\ (\alpha^{11})^0 & (\alpha^{11})^1 & \cdots & (\alpha^{11})^{16} \\ (\alpha^5)^0 & (\alpha^5)^1 & \cdots & (\alpha^5)^{16} \\ (\alpha^{10})^0 & (\alpha^{10})^1 & \cdots & (\alpha^{10})^{16} \end{pmatrix}$$

$$= \begin{pmatrix} (\beta^0)^0 & (\beta^0)^1 & \cdots & (\beta^0)^{16} \\ \hline (\beta^{45})^0 & (\beta^{45})^1 & \cdots & (\beta^{45})^{16} \\ (\beta^{90})^0 & (\beta^{90})^1 & \cdots & (\beta^{90})^{16} \\ (\beta^{180})^0 & (\beta^{180})^1 & \cdots & (\beta^{180})^{16} \\ (\beta^{105})^0 & (\beta^{105})^1 & \cdots & (\beta^{105})^{16} \\ (\beta^{210})^0 & (\beta^{210})^1 & \cdots & (\beta^{210})^{16} \\ (\beta^{165})^0 & (\beta^{165})^1 & \cdots & (\beta^{165})^{16} \\ (\beta^{75})^0 & (\beta^{75})^1 & \cdots & (\beta^{75})^{16} \\ (\beta^{150})^0 & (\beta^{150})^1 & \cdots & (\beta^{150})^{16} \end{pmatrix}$$

The non-zeros inverse roots and encoding of C in frequency-domain by

$$(c_0, c_1, \cdots, c_{16}) = (u_0, u_3u_6u_{12}u_7u_{14}u_{11}u_5u_{10}) \cdot G.$$

First, from the theorem of pervious section, we have found $\alpha^L = \alpha^3$ of $gcd(17, 3) = 1$ namely n and L is relatively prime, the number of CPC with full cyclic order will be, let $u_0 \in F_2$ be 0 or 1 and $u_3 = \alpha^0$, then the number of CPC with full cyclic order will equal to $p^{k-m} = 2^{9-8} = 2$. Due to we proposed when $n \neq p^m - 1$ which n is non-primitive length in this section, may get more number of CPC with full cyclic order by $(s-1)$ times, so this example will show the number of CPC with full cyclic order is $s \cdot p^{k-m} = 15 \cdot 2^{9-8} = 30$. The distribution of β shown in the following Tab. III. Each column makes a CPC in this table. β are $(s-1)$ more CPC than α. The result is shown in Fig. 2.

TABLE III
CPC SCHEMATIC OF NON-PRIMITIVE N=17 BY ONE INDEX.

$\alpha^0 = \beta^0$	$\alpha^{-1} = \beta^{-15}$	$\alpha^{-2} = \beta^{-30}$	$\cdots$	$\alpha^{-16} = \beta^{-240}$
β^{-1}	β^{-16}	β^{-31}	$\cdots$	β^{-241}
β^{-2}	β^{-17}	β^{-32}	$\cdots$	β^{-242}
β^{-3}	β^{-18}	β^{-33}	$\cdots$	β^{-243}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
β^{-14}	β^{-29}	β^{-59}	$\cdots$	β^{-254}

Fig. 2. CPCs constructed by [17,9,5] cyclic code.

Example2: Consider a $(23, 12, 5)$, which is cyclic code over F_2 and $m = 11$, the code length n is non-primitive. We can calculate $s = (2^{11} - 1)/23 = 89$ and $o(\alpha) = 23$, $o(\beta) = 89$, the distribution of cyclotomic coset

is $\{\alpha^0\}$, $\{\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^9, \alpha^{18}, \alpha^{13}, \alpha^3, \alpha^6, \alpha^{12}\}$ and $\{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{17}, \alpha^{11}, \alpha^{22}, \alpha^{21}, \alpha^{19}, \alpha^{15}, \alpha^7, \alpha^{14}\}$. Let $\{\alpha^0\}$ and $\{\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^9, \alpha^{18}, \alpha^{13}, \alpha^3, \alpha^6, \alpha^{12}\}$ as inverse of nonzeros roots. The generated matrix component of

$$G = \begin{pmatrix} (\beta^0)^0 & (\beta^0)^1 & \cdots & (\beta^0)^{22} \\ \hline (\beta^{89})^0 & (\beta^{89})^1 & \cdots & (\beta^{89})^{22} \\ (\beta^{178})^0 & (\beta^{178})^1 & \cdots & (\beta^{178})^{22} \\ (\beta^{356})^0 & (\beta^{356})^1 & \cdots & (\beta^{356})^{22} \\ (\beta^{712})^0 & (\beta^{712})^1 & \cdots & (\beta^{712})^{22} \\ (\beta^{1424})^0 & (\beta^{1424})^1 & \cdots & (\beta^{1424})^{22} \\ (\beta^{801})^0 & (\beta^{801})^1 & \cdots & (\beta^{801})^{22} \\ (\beta^{1602})^0 & (\beta^{1602})^1 & \cdots & (\beta^{1602})^{22} \\ (\beta^{1157})^0 & (\beta^{1157})^1 & \cdots & (\beta^{1157})^{22} \\ (\beta^{267})^0 & (\beta^{267})^1 & \cdots & (\beta^{267})^{22} \\ (\beta^{534})^0 & (\beta^{534})^1 & \cdots & (\beta^{534})^{22} \\ (\beta^{1068})^0 & (\beta^{1068})^1 & \cdots & (\beta^{1068})^{22} \end{pmatrix}$$

The encoding of $C = (c_0, c_1, c_2, c_3, \cdots, c_{22})$ in frequency-domain by

$$c = (u_0, u_1 u_2 u_4 u_8 u_{16} u_9 u_{18} u_{13} u_3 u_6 u_{12}) \cdot G$$

where $u_0 \in F_2$ and $u_1 \in F_{2^{11}}$. When $u_1 = 1$, $u_2 \in F_{2^{11}}$ the CPC number is $s \cdot 2^{k-m} = 89 \cdot 2^{12-11}$. This example will show the number of CPC with full cyclic order is $s \cdot p^{k-m} = 89 \cdot 2^{12-11} = 178$. The distribution of β shown in the following Tab. IV. Each column makes a CPC in this table. β are $(s-1)$ more CPC than α. The result is shown in Fig. 3.

TABLE IV
CPC SCHEMATIC OF NON-PRIMITIVE N=23 BY ONE INDEX.

$\alpha^0 = \beta^0$	$\alpha^{-1} = \beta^{-89}$	$\alpha^{-2} = \beta^{-178}$	$\cdots$	$\alpha^{-22} = \beta^{-1958}$
β^{-1}	β^{-90}	β^{-179}	$\cdots$	β^{-1959}
β^{-2}	β^{-91}	β^{-180}	$\cdots$	β^{-1960}
β^{-3}	β^{-92}	β^{-181}	$\cdots$	β^{-1961}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
β^{-88}	β^{-177}	β^{-266}	$\cdots$	β^{-2046}

Fig. 3. CPCs constructed by [23,12,7] cyclic code.

IV. CONCLUSION AND DISCUSSION

We have proposed an efficient method which we could find out all codeword with full cyclic order in cyclic code to form the cyclically permutable codes.This paper has extended the results in [8] and [13] in twofold advantages by using the characteristics of finite fields to develop an efficient algorithm to find a CPC from a cyclic code of prime-primitive length and prime-nonprimitive length respectively.

ACKNOWLEDGMENT

This work was supported by the Ministry of Science and Technology of Republic of China under Grants MOST 107-2221-E-005-015-MY2.

REFERENCES

[1] E. N. Gillbert, "Cyclically permutable error-correcting codes," *IEEE Trans. Inform, Theory*, vol. 9, pp. 175–182, Jul. 1963.
[2] L. Gyorfi, I. Vajda. "Constructions of protocol sequence for multiple access collision channel without feedback," *IEEE Trans. Inform, Theory*, pp. 1762–1765, 1993.
[3] Y. Zhang, W. Shum, Wing Shing Wong, and Feng Shu. "Binary Sequences for Multiple Access Collision Channel:Identification and Synchronization," *IEEE Trans, on Commun*, vol. 62, no. 2, Feb. 2014.
[4] A. W. Lam and D. V. Sarwate. "Time-hopping and frequency-hopping multiple-access packet communications," *IEEE Tans, on Commun.*, pp. 875–888, 1990.
[5] I. Vajda and G. Einarsson. "Code acquisition for a frequency-hopping system," *IEEE Trans. Commun.*, 35(5):566-568, 1987.
[6] H. Inaba and H. Nakahara, "Notes on rotation-resistant digital watermark using radon transform," *in Proc. Int. Symp. Information Theory and Its Applications (ISITA 2004)*, Parma, Italy, pp. 310–315, Oct. 2004.
[7] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. San Mateo, CA: Morgan Kaufmann, 2007.
[8] Q. A. Nguyen, L. Gyorfi, and J. L. Massey, "Constructions of binary constantweight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform, Theory*, vol. 38, no. 3, pp. 940–949, May 1992.
[9] Kuribayashi and H. Tanaka, "How to Generate Cyclically Permutable Codes from Cyclic Codes," *IEEE Trans. Inform, Theory*, vol. 52, no. 10, pp. 4660–4663, oct. 2006.
[10] S. Bitan and T. Etzion, "Constructions for optimal constant weight cyclically permutable codes and difference families," *IEEE Trans. Inform, Theory*, vol. 41, no. 1, pp. 77–87, Jan. 1995.
[11] J.S. Lemos-Neto, V.C. da Rocha, "Cyclically permutable codes specified by roots of generator polynomial," *Electronics Letters*, vol. 50, no. 17, Aug. 2014.
[12] M. Kuribayashi, S. Suma, and N. Funabiki, "Efficient Decoding Algorithm for Cyclically Permutable Code," *IEEE Information Theory Workshop (ITW)*, Nov. 2018.
[13] Y. Ting Ya, C. Houshou, and C. Kuo Cheng, "Generation of cyclically permutable codes by Galois field Fourier transform," *Int. Conf. on Ubiquitous and Future Networks (ICUFN 2016)*, July. 2016.
[14] S. Lin and D. J. Costello Jr., *Error-Correcting Codes,* Prentice-Hall, New Jersey, 2004.
[15] T. K. Moon, *Error Correction Coding : Mathematical Methods And Algorithms*. Wiley Inter-science, pp. 269–276, 2005.