Construction of Cyclically Permutable Codes From Cyclic Codes

Ting-Ya Yang¹, Houshou Chen² *, Kuo-Cheng Chung³

¹Dept. of Electrical Engineering and Graduate Institute of Communication Engineering
National Chung Hsing University, 250, Kuo Kuang Rd., Taichung 402, Taiwan

*Corresponding Author: houshou@dragon.nchu.edu.tw

Abstract

Cyclically permutable codes (CPCs) are important to communication networks, e.g., multiple access collision channels without feedback and frequency-hopping spread spectrum communication channels. A CPC is a block code of length n such that each codeword has full cyclic order n and all codewords are cyclically distinct. This study investigates the characteristics of finite fields to develop an efficient algorithm to find a CPC from a p-ary cyclic code, where p is a prime number. In this paper, the Galois field Fourier transform technique is used to generate a CPC of either primitive or non-primitive length.

Keywords: Cyclic codes, finite field, cyclically permutable codes, BCH codes, Reed-Solomon codes.

1. Introduction

For the past few years, cyclically permutable codes and their applications in communication networks, e.g. multiple access collision channel without feedback (1) and frequency-hopping spread spectrum communications channels (2), (3), and digital waterarking (4), (5) have become increasingly important. A cyclic code (6) is defined as a linear block code such that any cyclic shift of every codeword yields another codeword. Gilbert (7) defined a cyclically permutable code (CPC) as a block code of length n, such that each codeword has cyclic order $n\mathbb{Z}$ 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. Maracle and Wolverton (8) proposed an algorithm for constructing the cyclically inequivalent subset. However, an existing p-ary cyclic codes usually do not enable this efficient construction.

A cyclically permutable code of length $n$ can be obtained directly from a cyclic code by partitioning this cyclic code into cyclically equivalent subsets, each consisting of all cyclic shift of a codewords, and then choosing any one codeword from those subsets of size $n\mathbb{Z}$. However, it is required that the CPC must be effectively constructed from this cyclic code. N. Q. A. L. Gyorfi and J. L. Massey (9) proposed an encoding procedure for obtaining cyclically equivalent subsets and formed a CPC from a maximum-distance-separable (MDS) code, such as abReed-Solomon (RS) code of length $p-1$ or a generalized Berlekamop-Justesen (BJ) code of length $p+1$, both with dimension $k$ and over $F_p$. More precisely, they constructed a CPC with $p^{k-1}$ codewords from a RS code or a CPC with $p^{k-2}$ codewords from a BJ code.

The design of a difference family and several constructions of constant-weight CPCs are presented in (10) where the authors proposed combinatorial constructions to construct a CPC that have other coding applications. In (11), the authors proposed the use of algebraic property of a binary cyclic code, such as the generator polynomial in time-domain, for an efficient and systematic construction of a CPC from this binary cyclic code.

In this paper, we use the Galois field Fourier transform method to form a CPC from a p-ary cyclic code of length $n$ where $n$ is a divisor of $p^{m-1}$. Let $\alpha$ be an element with multiplication order $n$. This study extends the results of (9) 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 $s \cdot p^{k-1}$ codewords. The CPC constructed here has $s$ times more codewords compared to the CPC constructed in (9). Secondly, let $\alpha^i$, $i>1$, be a nonzero of 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. The remainder of this paper is organized as follows. In Section, we describe the Galois Field Fourier transforms for a p-ary cyclic code. Section III proposes an efficient construction for a CPC from the cyclic codes and provides some CPC examples with
The GFFT can also be written as

\[ v_j = n^{-1} \sum_{j=0}^{n-1} \alpha^{-ij} V_j \]  

(2)

where \( \alpha^{-1} \) is the vector multiplicative inverse of \( n \). The spectrum of the polynomial \( v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1} \) is the GFFT of \( v = (v_0, v_1, \ldots, v_{n-1}) \), and the vector \( v \) is in the time domain, and its corresponding transform \( V \) is in the frequency domain. Given a polynomial \( v(x) \), we can show that

\[ V_j = \sum_{i=0}^{n-1} v_j (\alpha^{-i})^j = v(\alpha^j) \]  

(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

\[ v_i = \frac{1}{n} \sum_{j=0}^{n-1} V_j (\alpha^{-i})^j = \frac{1}{n} V(\alpha^{-i}) \]  

(4)

Then, \( \alpha^{-i} \) is a zero of \( V(x) \) if and only if the \( i \)-th frequency component \( v_i \) of the inverse transform of \( V \) equals zero. When the zeros of a cyclic code are \( \{ \alpha^1, \alpha^2, \ldots, \alpha^{n-1} \} \), then the inverse of nonzeros are

\[ \{ \alpha^{-(n-k+1)}, \alpha^{-(n-k+2)}, \ldots, \alpha^{-(n-1)} \} = \{ \alpha^{k-1}, \alpha^{k-2}, \ldots, \alpha^{n-k} \} \]

We can then use the zeros and the inverse of the nonzeros of a cyclic code to form the parity check matrix \( H \) and the generator matrix \( G \) as

\[ H = \begin{pmatrix} (\alpha^1)^j \\ (\alpha^2)^j \\ \vdots \\ (\alpha^{n-k})^j \end{pmatrix}, \quad G = \begin{pmatrix} (\alpha^0)^j \\ (\alpha^1)^j \\ \vdots \\ (\alpha^{n-1})^j \end{pmatrix} \]

where \( j = 0, 1, \ldots, n-1 \).
3. Construction of Cyclically Permutable Codes

CPCs are based on the characteristics of cyclic codes, where the cyclically shifted codewords occupy the same subspace, with each CPC codeword belonging to each subspace. Gillbert (3) defined a CPC as a binary block code, the codewords of which are cyclically distinct and have full order. This study proposes efficient methods that can be used to find the CPC, and propose the construction of CPCs using $p$-ary linear cyclic $(n, k, d)$ codes, where $n$, $k$ and $d$ are the block length, dimension and minimum Hamming distance, respectively, and those codes with code digits in $GF(q)$ and $p$ can be a prime number. Moreover, this paper presents a cyclic code that can be used to find more CPCs compared with (6), and $n$ can have both primitive and non-primitive lengths.

3.1 $\alpha^{-i}$ is a $(n,k)$ cyclic code zero root, then $gcd(n, i)=1$

Lemma: A Consider the binary $(n, k, d)$ BCH code, where $n$ is prime and has primitive length, and where $n=2^m-1$, and has $2^{k-2}$ codewords with full order; then, we can obtain a CPC using $(2^k-2)/n$.

Proof: Let $\{\alpha^n, \alpha^{2n}, \ldots, \alpha^{kn}\}$ be a zero root and all its cyclotomic cosets, and the non-zero inverse be $\{\alpha^{n-1}, \alpha^{2n-1}, \ldots, \alpha^{kn-1}\}$, where $\alpha^n=\alpha^{kn}$. Let $k=1+r. m$ be the binary $(n, k, d)$ BCH code, where the codewords have $2^k=2.2^{m-1}$. Substituting a non-zero inverse into (3) to generate the matrix, we have

$$G = \begin{pmatrix}
\alpha^0 \\
\alpha^1 \\
\vdots \\
\alpha^{2m-k} \\
\vdots \\
\alpha^{2m-1} \\
\vdots \\
\alpha^{r. m} \\
\vdots \\
\end{pmatrix} = c = (u_0, u_1, u_2, \ldots, u_r) \cdot G$$

where $u_0 \in F_2$ and $u_i \in F_2^n$, and $x=1, \ldots, r$; then, we can find the CPC. First, let $u_0=1$ belong to $F_2^n$ arbitrary value. We have a $2^{k-m}(2^m-1)=2^{k-1}.2 \cdot (2^m-1)$ codeword with full order, and the CPC number is $(2^m-1).2$. The next set of $u_0=0$ and $u_1=1$ and another still belongs to the arbitrary value $F_2^n$. Similarly, we can calculate $(2^m-2) \cdot 2 \cdot (2^m-1)$ full order codewords, and these CPC numbers are $(2^m-2) \cdot 2$. If the CPC of the sequence obtained from $u_0, \ldots, u_c$ are zeros and $u_c=1$, then the CPC number is $(2^m)^{c-1} \cdot 2=2$. Finally, there are total CPC induction formula components of $2[(2^m)^{c-1}+(2^m)^{c-2}]^2=(2^m)^{c-1}+(2^m)^{c-2}]^2 = 2 \cdot (2^m-1)$, and the total CPC number is $(2^m)^{c-1} \cdot 2=2$. We obtained the desired result when $n$ is prime and has primitive length, and where the total CPC number is $(2^k-2)/n$.

EXAMPLE 1: Consider a $(31,16,7)$ BCH code over $F_2$. We can extend it to $F_2^5(F_2[x]/(x^3+x^2+1))$, where the degree is $m=5$ and where $n=2^5-1$ is primitive and has primitive length. The cyclotomic coset is

$$G = \begin{pmatrix}
\alpha^0 \\
\alpha^1 \\
\vdots \\
\alpha^3 \\
\vdots \\
\end{pmatrix} = c = (u_0, u_1, u_2, u_3, \ldots) \cdot G$$

where $u_0 \in F_2$ and $u_i \in F_2^n$. First, let $u_0=1$ and $u_1, u_2 \in F_2$. Second, let $u_0=0$, $u_1=1$ and $u_2 \in F_2^n$, which is another element. The CPC code is $2^{k-2m}=2^{16-10}=2^6$. Then, let $u_0=0$, $u_1=0$ and $u_2=1$, and the number of $2^{k-2m}=2^{16-15}=2^1$ with CPCs. We obtain a total CPC number of $(2^k-2)/n=27$. Similarly, the same characteristics of in $p$-ary exist.

3.2 $(n, k)$ cyclic codes with non-primitive length $s \neq 1$

We use GFFT for RS codes defined as

$$\left(c_0, \ldots, c_{n-1}\right) = \left(u_0, \ldots, u_{k-1}\right) \cdot \begin{pmatrix}
\alpha^0 \\
\vdots \\
\alpha^{s-1} \\
\end{pmatrix}$$

(5)

We consider the codes with zeros $\{\alpha^1, \alpha^2, \ldots, \alpha^{s-1}\}$, then, we evaluate $\nu(\alpha^i)=\nu(\alpha^j)=\cdots=\nu(\alpha^{s-1})$ and $V_1=V_2=\cdots=V_{n-1}=0$. We use the definition in (2) as
\[
\begin{pmatrix}
0
\vdots
V_0
\vdots
V_n-1
\end{pmatrix}
\]}
\[
\begin{pmatrix}
\cdots
\vdots
\frac{1}{n} (\alpha^{-i})
\vdots
\vdots
\frac{1}{n} (\alpha^{-i})
\end{pmatrix}
\]

\[
\Rightarrow \begin{pmatrix}
0
\vdots
V_0
\vdots
V_n-1
\end{pmatrix}
\begin{pmatrix}
\frac{1}{n} V_n-k
\vdots
\frac{1}{n} V_{n-k+1}
\end{pmatrix}
\begin{pmatrix}
\alpha \cdot \beta
\vdots
\alpha \cdot \beta
\vdots
\alpha \cdot \beta
\end{pmatrix}
\]

for \(1 \leq i \leq n-k\) and \(j=0, n-k+1, \ldots, n-1\). Let \(u_0=(1/n) \cdot V_0, u_1=(1/n) \cdot V_1, \ldots, u_{k-1}=(1/n) \cdot V_{n-k+1}\) then we can obtain

\[
u_j = \frac{1}{n} V_n-j = \frac{1}{n} V_j = \frac{1}{n} v(\alpha^{-j}) = \frac{1}{n} \varepsilon(\alpha^{-j})
\]

(6)

Consider \(\epsilon^0(x)\) as the right shift of \(\epsilon(x)\) component of

\[
u_j(\alpha)=\frac{1}{n} \epsilon(\alpha^{-j}) = \frac{1}{n} \alpha^{-\beta} \cdot \varepsilon(\alpha^{-j}) = \frac{1}{n} \alpha^{-\beta} \cdot \frac{1}{n} \varepsilon(\alpha^{-j})
\]

Finally, we have

\[
u_j(\alpha) = \alpha^{-\beta} \cdot \nu_j
\]

(7)

Consider \((p+1, k, p+2-k)\) RS code over \(F_p\), where \(n=p+1\) is

of non-primitive length. Let \(n=p+1\) and \(s=(p^2-1)/(p+1)=p-1\); then, \(\omega(\beta) = p^2-1\) and \(\omega(\alpha) = p + 1\), and we can obtain

\[
\alpha = \beta^{p+1} = \beta^s \cdot \beta^t. \text{ Using (3), we obtain } u_1(\alpha) = (\alpha^{-1}) u_1 = (\beta^{p+1} - \beta) \cdot u_1 = (\beta^{p+1} - \beta^t)
\]

\[
u_1(\alpha) = \alpha^{p+1} = \beta^s \cdot \beta^t
\]

\[
u_1(\alpha) = \frac{1}{n} \epsilon(\alpha^{-j}) = \frac{1}{n} \alpha^{-\beta} \cdot \varepsilon(\alpha^{-j}) = \frac{1}{n} \alpha^{-\beta} \cdot \frac{1}{n} \varepsilon(\alpha^{-j})
\]

Finally, we have

\[
u_j(\alpha) = \alpha^{-\beta} \cdot \nu_j
\]

(7)

In this study, we generate \([(p^2-1)/(p+1)] \cdot p^{k-2} \equiv s \cdot p^{k-2}\).

Comparing CPCs with [6] only have \(p^{k-2}\) CPCs, and we obtain additional CPCs. Further, in [6], the code length is only primitive length.

**EXAMPLE 2:** For \(35,25,4\) BCH codes over \(F_{12}^2\), the cyclotomic coset is

\[\{0\}\]
\[\{1, 2, 4, 8, 16, 32, 29, 23, 11, 22, 9, 18\}\]
\[\{3, 6, 12, 24, 13, 26, 17, 34, 33, 31, 27, 9\}\]
\[\{5, 10, 20\}\]
\[\{7, 14, 28, 21\}\]
\[\{15, 30, 25\}\]

First, we define \(s=(2^{u-1})/(n=2^{12-1})/35=4095/35=117\), \(\alpha=\beta^{s}=\beta^{117}\) and \(\omega(\alpha)=35\) and \(\omega(\beta)=2^{12-1}\). Consider the zeros as \(\{\alpha^5, \alpha^7, \alpha^{13}\}\), another is non-zero, where the non-zero inverse is \(\{\alpha^0, \alpha^3, \alpha^5\}\). The generated matrix component of

\[
G = \begin{pmatrix}
\alpha^0
\vdots
\alpha^3
\vdots
\alpha^5
\end{pmatrix}
\Rightarrow e = (u_0, u_1, u_5) \cdot G
\]

where \(u_0 \in F_2\) and \(u_1, u_5 \in F_{12}^2\). First, let \(u_1=1\) and \(u_3 \in F_{12}^2\) be another element in the codeword \(s \cdot 2^{k-2} \cdot (2^{12-1})/117 \cdot 2^{13} \cdot (2^{12-1})\) with full order.

Then, the CPC number is \(s \cdot 2^{k-2} \cdot 117 = 2^{k-2} \cdot 2^{12-1} \cdot 117 = 2^{13}\).

Second, set \(u_1=0\) and \(u_3=1\) in the codeword \(s \cdot 2^{k-2} \cdot (2^{12-1})=s \cdot 2^{k-2} \cdot (2^{12-1})\) with full order, then the CPC number is \(s \cdot 2^{k-2} \cdot (2^{12-1})=s \cdot 2^{k-2} \cdot 117 = 2\). Then, we obtain the total CPC number of \(s \cdot 2 \cdot 2^{k-2} = 2 \cdot 2^{12-1} = 2^{13+2}\).

**EXAMPLE 3:** Consider a \((6, k, d=n-k)\), which is RS code over \(F_3\) and \(m=2\), the code is non-prime and has primitive length. We can calculate \(s=(p^2-1)/(p+1)=5\cdot(5-1)/6=14\) and \(\omega(\alpha)=6, \omega(\beta)=p^2-1=5^2=24\). Next, we consider a \((6, 3, 4)\) RS code with \(\{\alpha^3, \alpha^7, \alpha^{13}\}\) as zeros and \(\{\alpha^0, \alpha^3, \alpha^5\}\) as non-zeros. The generated matrix component of

\[
G = \begin{pmatrix}
\alpha^0
\vdots
\alpha^3
\vdots
\alpha^5
\end{pmatrix}
\Rightarrow e = (u_0, u_1, u_5) \cdot G
\]

where \(u_0 \in F_3\) and \(u_1, u_5 \in F_{3}^2\). When \(u_1=1, u_5 \in F_{3}^2\) the CPC number is \((p-1) \cdot p^{k-1}=4 \cdot 5^{1}\). Also, when \(u_1=0, u_5=1\), the CPC number is \((p-1) \cdot (p^{k-2})=4 \cdot 5^{2}=20\). Finally, the total CPC number is \((p-1) \cdot (p^{k-1}+p^{k-2})=4 \cdot (5^{1}+5^{2})\). We can obtain \(u_1(\alpha) = (\alpha^{-1}) \cdot u_1 \Rightarrow (p^{k-2}) \cdot u_1 = \beta^{p+1}

\[
u_1(\alpha) = \frac{1}{n} \epsilon(\alpha^{-j}) = \frac{1}{n} \alpha^{-\beta} \cdot \varepsilon(\alpha^{-j}) = \frac{1}{n} \alpha^{-\beta} \cdot \frac{1}{n} \varepsilon(\alpha^{-j})
\]

4. **Conclusion and Discussion**

Cyclic codes are block codes in which a cyclic shift codeword generates another codeword belonging to the same subspace. With cyclically permutable codes (CPCs), the codewords are cyclically distinct and have full cyclic order. Although it is important to effectivley determine CPCs from cyclic codes, no approach has thus far been proposed. In this paper, we study the characteristics of finite fields and cyclic codes, and propose an efficient CPC construction procedure. The construction method proposed here is more efficient than the RS-based construction proposed in (5) and (6). In the first case, when \(gcd(n, i)=1\), we can obtain more CPCs.
Second, in (6), there is only the case where the CPC number comprises \( s = 1 \) multiples, and we can obtain more than \( s \geq 1 \) multiples of CPC. Moreover, as opposed to (5) which used the time domain, we proposed to use the frequency domain as an efficient method to find the CPC from cyclic code. We have shown the construction of CPCs based on the binary mapping of some \( p \)-ary linear cyclic codes, and we noted that the code can have primitive and non-primitive length.

References


