

## The Gray Image of A Class of Constacyclic Codes Over the ring $F_{p^m}[u]/\langle u^k \rangle$

DING Jian, LI Hongju

(Department of Common Courses, Anhui Xinhua University, Hefei 230088, Anhui, PR China)

**Abstract:** Let  $R_{(p^m, k)} = F_{p^m}[u]/\langle u^k \rangle$ , where  $p^{j-1} + 1 \leq k \leq p^j$  and  $u^k = 0$  for some positive prime number  $p$  and positive integer  $j$ . A new Gray map from  $R_{(p^m, k)}$  to  $F_{p^m}^{p^j}$  is defined. It is proved that the Gray image of a linear  $(1 + u + \dots + u^{k-1})$  constacyclic code of an arbitrary length  $N$  over  $R_{(p^m, k)}$  is a distance invariant linear cyclic code of length  $p^j N$  over  $F_{p^m}$ . Moreover, the generator polynomial of the Gray image of such a constacyclic code is determined, and some optimal linear cyclic codes over  $F_3$ ,  $F_5$  and  $F_7$  are constructed via the Gray map.

**Key words:** linear code; cyclic code; constacyclic code; Gray map; optimal code

**CLC number:** TN911.22      **Document code:** A      doi:10.3969/j.issn.0253-2778.2017.07.009

**2010 Mathematics Subject Classification:** Primary 94B05; Secondary 94B15

**Citation:** DING Jian, LI Hongju. The Gray Image of A Class of Constacyclic Codes Over the ring  $F_{p^m}[u]/\langle u^k \rangle$ [J]. Journal of University of Science and Technology of China, 2017, 47(7):315-322.

丁健,李红菊. 环  $F_{p^m}[u]/\langle u^k \rangle$  上一类常循环码的 Gray 像[J]. 中国科学技术大学学报, 2017, 47(7):315-322.

## 环 $F_{p^m}[u]/\langle u^k \rangle$ 上一类常循环码的 Gray 像

丁 健,李红菊

(安徽新华学院公课部,安徽合肥 230088)

**摘要:** 令  $R_{(p^m, k)} = F_{p^m}[u]/\langle u^k \rangle$ , 其中  $p^{j-1} + 1 \leq k \leq p^j$ 、 $u^k = 0$ 、 $p$  为正素数、 $j$  为正整数. 定义了从  $R_{(p^m, k)}$  到  $F_{p^m}^{p^j}$  的一个新的 Gray 映射, 得到了环  $R_{(p^m, k)}$  上码长为任意长度  $N$  的线性  $(1 + u + \dots + u^{k-1})$  常循环码的 Gray 像是  $F_{p^m}$  上长为  $p^j N$  的保距线性循环码, 并给出了 Gray 像的生成多项式, 构造了  $F_3$ 、 $F_5$  和  $F_7$  上的一些最优线性循环码.

**关键词:** 线性码; 循环码; 常循环码; Gray 映射; 最优码

### 0 Introduction

It is well-known that constacyclic codes have rigorous algebraic structure and their error-

correcting performance is easy to be analyzed. The codes used in practice like BCH codes and quadratic residue codes can all be attributed to constacyclic codes. In addition, their encoding and decoding

**Received:** 2015-10-27; **Revised:** 2016-05-24

**Foundation item:** Supported by National Natural Science Foundation of China(61370089), Anhui Province Natural Science Research(KJ2015A308, KJ2016A307, KJ2017A623) and Anhui Province Colleges Outstanding Young Talents Program(gxyqZD2016389).

**Biography:** DING Jian, male, born in 1982, Master/Associate Professor. Research field: Algebraic coding. E-mail: dingjian\_happy@163.com.

**Corresponding author:** LI Hongju, Master/Lecture. E-mail: zhenxidj.happy@163.com.

circuits, especially encoding circuits, are easy to be designed. So constacyclic codes are a kind of important class of linear codes from both a theoretical and a practical perspective. The ring  $F_2 + uF_2$  is interesting because it shares some good properties of both the ring  $Z_4$  and the Galois field  $F_4$ . In 2006, Qian et al defined the  $(1 + u)$  constacyclic codes over  $F_2 + uF_2$  in Ref. [1] and obtained that the Gray image of a linear single-root  $(1 + u)$  constacyclic code over this ring was a binary distance invariant linear cyclic code. From then on, the construction of the Gray map over such rings have been a topic of study. Amarra et al<sup>[2]</sup> discussed the Gray image of a single-root  $(1 - u)$  constacyclic code over  $F_{p^k} + uF_{p^k}$ , which was a quasi-cyclic code over  $F_{p^k}$ . Sobhani et al<sup>[3]</sup> studied the Gray image of a single-root  $(1 + u^t)$  constacyclic codes over  $F_q[u]/\langle u^{t+1} \rangle$ , which was a quasi-cyclic code over  $F_q$ . Abular et al<sup>[4]</sup> showed that the Gray image of a linear  $(1 + u)$  constacyclic code of an arbitrary length over  $F_2 + uF_2$  was a binary distance invariant linear cyclic code and got the generator polynomial of the Gray image. Later, the results in Ref. [4] was extended to  $(1 + u)$  and  $(1 + u + \dots + u^{k-1})$  constacyclic codes over  $F_{2^m}[u]/\langle u^k \rangle$  in Refs. [5] and [6], while some optimal codes over  $F_2$  and  $F_4$  were constructed. Kai et al<sup>[7]</sup> and Ding et al<sup>[8]</sup> showed that the Gray image of a linear  $(1 + \lambda u)$  constacyclic code with an arbitrary length over  $F_p + uF_p$  was a distance invariant linear code over  $F_p$ , but the generator polynomials of the corresponding Gray images were not acquired.

In this paper, we study the Gray image of a  $(1 + u + \dots + u^{k-1})$  constacyclic code of an arbitrary length over  $R_{(p^m, k)}$  and obtain the generator polynomials of the corresponding Gray images. Furthermore, some optimal codes are given. This paper is organized as follows. Section 2 gives some results about constacyclic codes over the ring  $R_{(p^m, k)}$  and some operations mod  $p$ . In Section 3, we investigate the properties of a kind of matrix

$A_{p^j}$  over  $F_{p^m}$ . In Section 4, using the matrix in Section 3, we define a new distance-preserving map from  $(R_{(p^m, k)}[x], \text{Lee distance})$  to  $(F_{p^m}[x], \text{Hamming distance})$ . In Section 5, we study the structure and generator polynomial of the Gray image of a  $(1 + u + \dots + u^{k-1})$  constacyclic code over  $R_{(p^m, k)}$ . Besides, some optimal linear cyclic codes over  $F_3, F_5$  and  $F_7$  are constructed by means of this Gray map in Section 6.

## 1 Preliminaries

Let  $R_{(p^m, k)}$  denote the polynomial residue ring  $F_{p^m}[u]/\langle u^k \rangle$ , where  $p^{j-1} + 1 \leq k \leq p^j$  and  $u^k = 0$  for some positive prime number  $p$  and positive integer  $j$ . Let  $n$  and  $p$  be relatively prime, if  $x^n - 1 = f_1 f_2 \dots f_w$  is the factorization of  $(x^n - 1)$  into a product of monic basic irreducible pairwise coprime polynomials in  $F_{p^m}[x]$ , then this factorization is unique and can be directly carried over  $R_{(p^m, k)}$  from over  $F_{p^m}$ . Let  $C$  be a code of length  $N = p^e n$  over  $R_{(p^m, k)}$ , where  $e$  is a non-negative integer. For some fixed unit  $\alpha$  of  $R_{(p^m, k)}$ , the  $\alpha$  constacyclic shift  $\tau_\alpha$  on  $R_{(p^m, k)}^N$  is the shift  $\tau_\alpha(c_0, c_1, \dots, c_{N-1}) = (\alpha c_{N-1}, c_0, c_1, \dots, c_{N-2})$ . The code  $C$  is said to be an  $\alpha$  constacyclic code if  $\tau_\alpha(C) = C$ . Now, we identify a codeword  $c = (c_0, c_1, \dots, c_{n-1})$  with its polynomial representation  $c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$ , then  $xc(x)$  corresponds to an  $\alpha$  constacyclic shift of  $c(x)$  in the ring  $R_{(p^m, k)}[x]/\langle x^n - \alpha \rangle$ . Thus  $\alpha$  constacyclic codes of length  $N$  over  $R_{(p^m, k)}$  can be identified as ideals in the ring  $R_{(p^m, k)}[x]/\langle x^N - \alpha \rangle$ . In the following, we let  $p^{j-1} + 1 \leq k \leq p^j$  for some positive prime number  $p$  and positive integer  $j$ .

Let  $C_r^s = \frac{r!}{s!(r-s)!}$  for some positive integer  $0 \leq s \leq r$ , then we have the following propositions.

**Proposition 1.1**  $C_{p-1}^s \not\equiv 0 \pmod{p}$ .

**Proof**  $C_{p-1}^s = \frac{(p-1)!}{s!(p-s-1)!} \not\equiv 0 \pmod{p}$ .

**Proposition 1.2**  $C_p^s \equiv 0 \pmod{p}$  for positive

integer  $1 \leq s \leq p-1$ .

**Proof**  $C_p^s = \frac{p!}{s!(p-s)!} = p \cdot \frac{(p-1)!}{s!(p-s)!} \equiv 0 \pmod{p}$ .

**Proposition 1.3**  $C_{r+1}^s - C_r^{s-1} = C_r^s$  for positive integer  $1 \leq s \leq r$ .

**Proof** If  $1 \leq s \leq r$ , then

$$C_{r+1}^s - C_r^{s-1} = \frac{(r+1)!}{s!(r-s+1)!} - \frac{r!}{(s-1)!(r-s+1)!} = \frac{r!}{s!(r-s+1)!}(r+1-s) = \frac{r!}{s!(r-s)!} = C_r^s.$$

**Proposition 1.4**  $C_{r+1}^s = \sum_{l=0}^s C_{r-l}^{s-l}$  for positive integer  $0 \leq s \leq r$  and  $r \geq 1$ .

**Proof** If  $s = 0$  and  $r \geq 1$ , then the result is straightforward.

If  $1 \leq s \leq r$ , by Proposition 1.3,

$$\begin{aligned} \sum_{l=0}^s C_{r-l}^{s-l} &= C_{r-s}^0 + \sum_{l=0}^{s-1} C_{r-l}^{s-l} = C_{r-s}^0 + \sum_{l=0}^{s-1} (C_{r-l+1}^{s-l} - C_{r-l}^{s-l-1}) = \\ &C_{r-s}^0 + \sum_{l=0}^{s-1} C_{r-l+1}^{s-l} - \sum_{l=0}^{s-1} C_{r-l}^{s-l-1} = C_{r-s}^0 + \sum_{l=0}^{s-1} C_{r-l+1}^{s-l} - \sum_{l=1}^s C_{r-l+1}^{s-l} = \\ &C_{r-s}^0 + C_{r+1}^s - C_{r-s+1}^0 = C_{r+1}^s. \end{aligned}$$

## 2 A kind of matrix $A_{p^j}$ over $F_{p^m}$

**Definition 2.1** If  $j = 1$ , then  $A_{p^j} = A_p =$

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & C_{p-1}^{p-1} \\ 0 & 0 & \cdots & C_{p-1}^{p-2} & C_{p-2}^{p-2} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & C_{p-1}^1 & \cdots & C_2^1 & C_1^1 \\ C_{p-1}^0 & C_{p-2}^0 & \cdots & C_1^0 & 1 \end{pmatrix}. \text{ If } j \geq 2, \text{ then}$$

$$A_{p^j} =$$

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & C_{p-1}^{p-1} A_{p^{j-1}} \\ 0 & 0 & \cdots & C_{p-1}^{p-2} A_{p^{j-1}} & C_{p-2}^{p-2} A_{p^{j-1}} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & C_{p-1}^1 A_{p^{j-1}} & \cdots & C_2^1 A_{p^{j-1}} & C_1^1 A_{p^{j-1}} \\ C_{p-1}^0 A_{p^{j-1}} & C_{p-2}^0 A_{p^{j-1}} & \cdots & C_1^0 A_{p^{j-1}} & A_{p^{j-1}} \end{pmatrix}.$$

From the definition of matrix  $A_{p^j}$ , we see that  $A_{p^j}$  is a  $p^j \times p^j$  matrix. Let  $A_{p^j}[R(i)]$  and  $A_{p^j}(i)$  be the  $i$ th row and the  $i$ th column of  $A_{p^j}$  for  $1 \leq i \leq p^j$  respectively, then  $A_{p^j}[R(1)] = (\underbrace{0, \dots, 0}_{(p^j-1) \text{ zeros}}, 1)$  and  $A_{p^j}(p^j) = (\underbrace{1, \dots, 1}_{p^j \text{ ones}})^T$ .

**Lemma 2.1**  $A_{p^j}$  is an invertible matrix in  $F_{p^m}$ .

**Proof** From Definition 2.1 and Proposition 1.1, we see that  $A_p$  is a lower triangular matrix and each element of its secondary diagonal is not zero mod  $p$ , so  $A_p$  is invertible in  $F_{p^m}$ . Suppose  $A_{p^{j_1}}$  is an invertible matrix for some positive integer  $j_1$  in  $F_{p^m}$ , then  $C_{p-1}^s A_{p^{j_1}}$  is also invertible in  $F_{p^m}$  for positive integer  $0 \leq s \leq p-1$ , so  $A_{p^{j_1+1}}$  is invertible in  $F_{p^m}$ , which gives the proof.

**Lemma 2.2** Let  $B_{p^j} = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \vdots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$  be a  $p^j \times p^j$  matrix, where each element of  $B_{p^j}$  is one, then  $B_{p^j} A_{p^j} = (A_{p^j}(p^j), \underbrace{0, \dots, 0}_{(p^j-1) \text{ zeros}})$  in  $F_{p^m}$ .

**Proof** By Proposition 1.4,  $B_p[R(1)]A_p = (C_{p-1}^0, \sum_{l=0}^1 C_{p-l-1}^{1-l}, \sum_{l=0}^2 C_{p-l-1}^{2-l}, \dots, \sum_{l=0}^{p-1} C_{p-l-1}^{p-1-l}) = (1, C_p^1, C_p^2, \dots, C_p^{p-1})$ . According to Proposition 1.2,  $B_p[R(1)]A_p = (1, \underbrace{0, \dots, 0}_{(p-1) \text{ zeros}})$  in  $F_{p^m}$ , so  $B_p A_p = (A_p(p), \underbrace{0, \dots, 0}_{(p-1) \text{ zeros}})$ . Suppose  $B_{p^{j_1}} A_{p^{j_1}} = (A_{p^{j_1}}(p^{j_1}), \underbrace{0, \dots, 0}_{(p^{j_1}-1) \text{ zeros}})$  in  $F_{p^m}$  for some positive integer  $j_1$ . By Propositions 1.2 and 1.4, we have

$$B_{p^{j_1+1}}[R(1)]A_{p^{j_1+1}} = (\underbrace{1, \dots, 1}_{p^{j_1+1} \text{ ones}}, \underbrace{1, \dots, 1}_{p^{j_1+1} \text{ ones}}, \dots, \underbrace{1, \dots, 1}_{p^{j_1+1} \text{ ones}}) \begin{pmatrix} 0 & 0 & \cdots & 0 & C_{p-1}^{p-1} A_{p^{j_1}} \\ 0 & 0 & \cdots & C_{p-1}^{p-2} A_{p^{j_1}} & C_{p-2}^{p-2} A_{p^{j_1}} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & C_{p-1}^1 A_{p^{j_1}} & \cdots & C_2^1 A_{p^{j_1}} & C_1^1 A_{p^{j_1}} \\ C_{p-1}^0 A_{p^{j_1}} & C_{p-2}^0 A_{p^{j_1}} & \cdots & C_1^0 A_{p^{j_1}} & A_{p^{j_1}} \end{pmatrix} =$$

$$(1, \underbrace{0, \dots, 0}_{(p^{j_1}-1) \text{ zeros}}, C_p^1(\underbrace{1, 0, \dots, 0}_{(p^{j_1}-1) \text{ zeros}}), C_p^2(\underbrace{1, 0, \dots, 0}_{(p^{j_1}-1) \text{ zeros}}), \dots, C_p^{p-1}(\underbrace{1, 0, \dots, 0}_{(p^{j_1}-1) \text{ zeros}})) = (1, \underbrace{0, \dots, 0}_{(p^{j_1+1}-1) \text{ zeros}}),$$

so  $B_{p^{j_1+1}}A_{p^{j_1+1}} = (A_{p^{j_1+1}}(\underbrace{p^{j_1+1}}_{(p^{j_1+1}-1) \text{ zeros}}), \underbrace{0, \dots, 0}_{(p^{j_1+1}-1) \text{ zeros}})$ . By induction, the desired result follows.

**Theorem 2.1** Let  $H_{p^j} =$

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \vdots & 0 & 1 \end{pmatrix} \text{ and}$$

$$D_{p^j} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \text{ where } H_{p^j} \text{ and } D_{p^j}$$

are both  $p^j \times p^j$  matrices, then  $H_{p^j}A_{p^j} = A_{p^j}D_{p^j}$  in  $F_{p^m}$ .

**Proof** We prove the result by induction on  $j$

in  $F_{p^m}$ . According to Propositions 1.2 and 1.4, if  $2 \leq i \leq p$ , then

$$H_p A_p(i) = H_p (0, \dots, 0, \underbrace{C_{p-1}^{i-1}, C_{p-2}^{i-2}, \dots, C_{p-i+1}^1, C_{p-i}^0}_{(p-i) \text{ zeros}})^T = \underbrace{(C_p^{i-1}, \dots, C_p^{i-1}, C_{p-1}^{i-2}, \dots, C_{p-i+2}^1, C_{p-i}^0)}_{p-i+1}^T = (0, \dots, 0, \underbrace{C_{p-1}^{i-2}, \dots, C_{p-i+2}^1, C_{p-i+1}^0}_{p-i+1})^T = A_p(i-1).$$

Besides,  $H_p A_p(1) = (\underbrace{1, \dots, 1}_{p \text{ ones}})^T = A_p(p)$ , So

$$H_p A_p = (A_p(p), \underbrace{A_p(1), A_p(2), \dots, A_p(p-1)}_{p \text{ ones}}) = A_p D_p.$$

Suppose  $H_{p^{j_1}}A_{p^{j_1}} = A_{p^{j_1}}D_{p^{j_1}}$  for some positive integer  $j_1$  in  $F_{p^m}$ , then

$$H_{p^{j_1}}A_{p^{j_1}} = (A_{p^{j_1}}(p^{j_1}), A_{p^{j_1}}(1), A_{p^{j_1}}(2), \dots, A_{p^{j_1}}(p^{j_1}-1))$$

and

$$H_{p^{j_1+1}}A_{p^{j_1+1}} = \begin{pmatrix} H_{p^{j_1}} & B_{p^{j_1}} & \cdots & B_{p^{j_1}} & B_{p^{j_1}} \\ 0 & H_{p^{j_1}} & \cdots & B_{p^{j_1}} & B_{p^{j_1}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & H_{p^{j_1}} & B_{p^{j_1}} \\ 0 & 0 & \vdots & 0 & H_{p^{j_1}} \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 0 & C_{p-1}^{p-1}A_{p^{j_1}} \\ 0 & 0 & \cdots & C_{p-1}^{p-2}A_{p^{j_1}} & C_{p-2}^{p-2}A_{p^{j_1}} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & C_{p-1}^1A_{p^{j_1}} & \cdots & C_2^1A_{p^{j_1}} & C_1^1A_{p^{j_1}} \\ C_{p-1}^0A_{p^{j_1}} & C_{p-2}^0A_{p^{j_1}} & \cdots & C_1^0A_{p^{j_1}} & A_{p^{j_1}} \end{pmatrix}.$$

By Lemma 2.2,

$$H_{p^{j_1+1}} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ C_{p-1}^0A_{p^{j_1}} \end{pmatrix} = \begin{pmatrix} B_{p^{j_1}}A_{p^{j_1}} \\ \vdots \\ B_{p^{j_1}}A_{p^{j_1}} \\ H_{p^{j_1}}A_{p^{j_1}} \end{pmatrix} = \begin{pmatrix} A_{p^{j_1}}(p^{j_1}) & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{p^{j_1}}(p^{j_1}) & 0 & 0 & \cdots & 0 \\ A_{p^{j_1}}(p^{j_1})A_{p^{j_1}}(1) & A_{p^{j_1}}(2) & \cdots & A_{p^{j_1}}(p^{j_1}-1) \end{pmatrix} = (A_{p^{j_1+1}}(\underbrace{p^{j_1+1}}_{(p^{j_1+1}-1) \text{ zeros}}), A_{p^{j_1+1}}(1), A_{p^{j_1+1}}(2), \dots, A_{p^{j_1+1}}(p^{j_1}-1)).$$

According to Propositions 1.2 to 1.4, if  $2 \leq i \leq p$ , then

$$H_{p^{j_1+1}} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ C_{p-1}^{i-1}A_{p^{j_1}} \\ C_{p-2}^{i-2}A_{p^{j_1}} \\ \vdots \\ C_{p-i+1}^1A_{p^{j_1}} \\ C_{p-i}^0A_{p^{j_1}} \end{pmatrix} = \begin{pmatrix} C_p^{i-1}B_{p^{j_1}}A_{p^{j_1}} \\ \vdots \\ C_p^{i-1}B_{p^{j_1}}A_{p^{j_1}} \\ C_{p-1}^{i-1}H_{p^{j_1}}A_{p^{j_1}} + C_{p-1}^{i-2}B_{p^{j_1}}A_{p^{j_1}} \\ C_{p-2}^{i-2}H_{p^{j_1}}A_{p^{j_1}} + C_{p-2}^{i-3}B_{p^{j_1}}A_{p^{j_1}} \\ \vdots \\ C_{p-i+1}^1H_{p^{j_1}}A_{p^{j_1}} + C_{p-i+1}^0B_{p^{j_1}}A_{p^{j_1}} \\ C_{p-i+1}^0H_{p^{j_1}}A_{p^{j_1}} \end{pmatrix} =$$

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 \\ C_{p-1}^{i-1} A_{pj1}(p^{j1}) & C_{p-1}^{i-1} A_{pj1}(1) & C_{p-1}^{i-1} A_{pj1}(2) & \dots & C_{p-1}^{i-1} A_{pj1}(p^{j1}-1) \\ C_{p-1}^{i-2} A_{pj1}(p^{j1}) & C_{p-1}^{i-2} A_{pj1}(1) & C_{p-1}^{i-2} A_{pj1}(2) & \dots & C_{p-1}^{i-2} A_{pj1}(p^{j1}-1) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ C_{p-i+2}^1 A_{pj1}(p^{j1}) & C_{p-i+1}^1 A_{pj1}(1) & C_{p-i+1}^1 A_{pj1}(2) & \dots & C_{p-i+1}^1 A_{pj1}(p^{j1}-1) \\ C_{p-i+1}^0 A_{pj1}(p^{j1}) & C_{p-i+1}^0 A_{pj1}(1) & C_{p-i+1}^0 A_{pj1}(2) & \dots & C_{p-i+1}^0 A_{pj1}(p^{j1}-1) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 \\ 0 & C_{p-1}^{i-1} A_{pj1}(1) & C_{p-1}^{i-1} A_{pj1}(2) & \dots & C_{p-1}^{i-1} A_{pj1}(p^{j1}-1) \\ C_{p-1}^{i-2} A_{pj1}(p^{j1}) & C_{p-1}^{i-2} A_{pj1}(1) & C_{p-1}^{i-2} A_{pj1}(2) & \dots & C_{p-1}^{i-2} A_{pj1}(p^{j1}-1) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ C_{p-i+2}^1 A_{pj1}(p^{j1}) & C_{p-i+1}^1 A_{pj1}(1) & C_{p-i+1}^1 A_{pj1}(2) & \dots & C_{p-i+1}^1 A_{pj1}(p^{j1}-1) \\ C_{p-i+1}^0 A_{pj1}(p^{j1}) & C_{p-i+1}^0 A_{pj1}(1) & C_{p-i+1}^0 A_{pj1}(2) & \dots & C_{p-i+1}^0 A_{pj1}(p^{j1}-1) \end{pmatrix} = (A_{pj1+1}((i-1)p^{j1}), A_{pj1+1}((i-1)p^{j1}+1), A_{pj1+1}((i-1)p^{j1}+2), \dots, A_{pj1+1}(ip^{j1}-1)).$$

So  $H_{pj1+1} A_{pj1+1} = A_{pj1+1} D_{pj1+1}$ , this gives the proof.

### 3 A new Gray map

Let  $a, b$  be two elements in  $R_{(pm,k)}$ , then  $a, b$  can be written as  $a = \sum_{i=0}^{k-1} u^i r_i(a)$  and  $b = \sum_{i=0}^{k-1} u^i r_i(b)$  respectively, where  $r_i(a), r_i(b) \in F_{pm}$  for positive integer  $0 \leq i \leq k-1$ . It is easy to check that  $r_i(a+b) = r_i(a) + r_i(b)$  for  $0 \leq i \leq k-1$ .

**Definition 3.1** For an arbitrary element  $a$  in  $R_{(pm,k)}$ , a new Gray map  $\Phi_{(pm,k)}$  from  $R_{(pm,k)}$  to  $F_{pm}^{pj}$  is defined as follows:  $\Phi_{(pm,k)}(a) = (\underbrace{0, \dots, 0}_{(pj-k) \text{ zeros}}, r_0(a), r_1(a), \dots, r_{k-1}(a)) A_{pj}$ .

Note that  $\Phi_{(pm,k)}$  is linear, since

$$\begin{aligned} \Phi_{(pm,k)}(a+b) &= (\underbrace{0, \dots, 0}_{(pj-k) \text{ zeros}}, r_0(a+b), \\ & r_1(a+b), \dots, r_{k-1}(a+b)) A_{pj} = \\ & [(\underbrace{0, \dots, 0}_{(pj-k) \text{ zeros}}, r_0(a), r_1(a), \dots, r_{k-1}(a)) + \\ & (\underbrace{0, \dots, 0}_{(pj-k) \text{ zeros}}, r_0(b), r_1(b), \dots, r_{k-1}(b))] A_{pj} = \\ & \Phi_{(pm,k)}(a) + \Phi_{(pm,k)}(b). \end{aligned}$$

Furthermore,  $\Phi_{(pm,k)}$  is a bijection from  $R_{(pm,k)}$  to  $F_{pm}^{pj}$  because of the invertibility of  $A_{pj}$

by Lemma 2.1, we identify a codeword  $c = (c_0, c_1, \dots, c_{N-1}) \in R_{(pm,k)}^N$  with its polynomial representation  $c(x) = c_0 + c_1 x + \dots + c_{N-1} x^{N-1}$  and denote  $P_i[c(x)] = \sum_{l=0}^{N-1} r_l(c_l) x^l$  for positive integer  $0 \leq i \leq k-1$ , then  $c(x) = \sum_{i=0}^{k-1} u_i P_i[c(x)]$ . Thus, the Gray map  $\Phi_{(pm,k)}$  can be extended to  $R_{(pm,k)}[x]$  in an obvious way.

**Definition 3.2** For an arbitrary codeword  $c = (c_0, c_1, \dots, c_{N-1}) \in R_{(pm,k)}^N$ , its polynomial representation is  $c(x) = c_0 + c_1 x + \dots + c_{N-1} x^{N-1} \in R_{(pm,k)}[x]$ . The polynomial Gray map  $\Phi_{(pm,k)}$  from  $R_{(pm,k)}[x]$  to  $F_{pm}[x]$  is defined as follows:

$$\Phi_{(pm,k)}[c(x)] = (\underbrace{0, \dots, 0}_{(pj-k) \text{ zeros}}, P_0[c(x)],$$

$$P_1[c(x)], \dots, P_{k-1}[c(x)] A_{pj} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(pj-1)N} \end{pmatrix}.$$

Obviously,  $\Phi_{(pm,k)}$  is not only linear, but also a bijection from  $R_{(pm,k)}[x]$  to  $F_{pm}[x]$ .

**Definition 3.3** Let  $W_L$  be the Lee weight of the element of  $R_{(pm,k)}$  and  $W_H$  be the Hamming weight of the element of  $F_{pm}^{pj}$ . We define that  $W_L(a) = W_H[\Phi_{(pm,k)}(a)]$  for an arbitrary element

$a$  in  $R_{(p^m, k)}$ . The Lee weight of a codeword in  $R_{(p^m, k)}[x]$  is the rational integer sum of the Lee weight of its coefficients. The Lee distance between two codewords  $c$  and  $c'$  is defined as the Lee weight of  $(c - c')$ .

**Theorem 3.1** The polynomial Gray map  $\Phi_{(p^m, k)}$  is not only a linear bijection from  $R_{(p^m, k)}[x]$  to  $F_{p^m}[x]$ , but also a distance-preserving map from  $(R_{(p^m, k)}[x], \text{Lee distance})$  to  $(F_{p^m}[x], \text{Hamming distance})$ .

**4 The Gray image of a  $(1 + u + \dots + u^{k-1})$  constacyclic code over  $R_{(p^m, k)}$**

**Lemma 4.1** In  $R_{(p^m, k)}[x]/\langle x^N - (1 + u + \dots + u^{k-1}) \rangle$ ,  $x^{p^j N} = 1$  and  $u = x^{(p^j - 1)N} (x^N - 1)$ .

**Proof** In  $R_{(p^m, k)}[x]/\langle x^N - (1 + u + \dots + u^{k-1}) \rangle$ ,  $x^N = 1 + u + \dots + u^{k-1}$ ,  $u^k = 0$  and  $p^{j-1} + 1 \leq k \leq p^j$ , so  $u^{p^j} = 0$  and  $x^{p^j N} = (1 + u + \dots + u^{k-1})^{p^j} = 1$ . Since  $(1 - u)x^N = 1 - u^k = 1 = x^{p^j N}$ , then  $u = 1 - x^{(p^j - 1)N} = x^{(p^j - 1)N} (x^N - 1)$ .

**Theorem 4.1** If  $C$  is a  $(1 + u + \dots + u^{k-1})$  constacyclic code of length  $N$  over  $R_{(p^m, k)}$ , then  $\Phi_{(p^m, k)}(C)$  is a linear cyclic code of length  $p^j N$  over  $F_{p^m}$ .

**Proof** One only needs to prove  $\Phi_{(p^m, k)}[xc(x)] = x\Phi_{(p^m, k)}[c(x)]$  for an arbitrary codeword  $c(x)$  of  $C$ . In fact,  $x^N = 1 + u + \dots + u^{k-1}$  and  $x^{p^j N} = 1$  in  $R_{(p^m, k)}[x]/\langle x^N - (1 + u + \dots + u^{k-1}) \rangle$  by Lemma 5.1. For an arbitrary codeword  $c(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{N-1} x^{N-1} \in C$ , it can be written

in the form  $c(x) = \sum_{i=0}^{k-1} u^i P_i[c(x)]$ . Then, we have  $xc(x) = (1 + u + \dots + u^{k-1})c_{N-1} + c_0 x + c_1 x^2 + \dots + c_{N-2} x^{N-1} = \sum_{i=0}^{k-1} u^i P_i[xc(x)]$ , where

$$P_i[xc(x)] = r_i[(1 + u + \dots + u^{k-1})c_{N-1}] + \sum_{l=0}^{N-2} r_i(c_l)x^{l+1} = [r_0(c_{N-1}) + r_1(c_{N-1}) + \dots + r_i(c_{N-1})] + xP_i[c(x)] - x^N r_i(c_{N-1})$$

and  $i = 0, 1, \dots, k - 1$ . Therefore

$$\begin{aligned} \Phi_{(p^m, k)}[xc(x)] &= (\underbrace{0, \dots, 0}_{(p^j - k) \text{ zeros}}, P_0[xc(x)], P_1[xc(x)], \dots, P_{k-1}[xc(x)]) A_{p^j} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(p^j - 1)N} \end{pmatrix} = \\ &= (\underbrace{0, \dots, 0}_{(p^j - k) \text{ zeros}}, r_0(c_{N-1}), \sum_{i=0}^1 r_i(c_{N-1}), \dots, \sum_{i=0}^{k-1} r_i(c_{N-1})) A_{p^j} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(p^j - 1)N} \end{pmatrix} - \\ &= (\underbrace{0, \dots, 0}_{(p^j - k) \text{ zeros}}, x^N r_0(c_{N-1}), x^N r_1(c_{N-1}), \dots, x^N r_{k-1}(c_{N-1})) A_{p^j} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(p^j - 1)N} \end{pmatrix} + \\ &= (\underbrace{0, \dots, 0}_{(p^j - k) \text{ zeros}}, xP_0[c(x)], xP_1[c(x)], \dots, xP_{k-1}[c(x)]) A_{p^j} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(p^j - 1)N} \end{pmatrix} = \\ &= (\underbrace{0, \dots, 0}_{(p^j - k) \text{ zeros}}, r_0(c_{N-1}), r_1(c_{N-1}), \dots, r_{k-1}(c_{N-1})) (H_{p^j} A_{p^j} - A_{p^j} D_{p^j}) \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(p^j - 1)N} \end{pmatrix} + x\Phi_k[c(x)]. \end{aligned}$$

By Theorem 2. 1,  $\Phi_{(pm,k)}[xc(x)] = x\Phi_{(pm,k)}[c(x)]$ .

**Lemma 4. 2** In  $F_{pm}[x]$ ,  $(x^N - 1)^{p^t} = \sum_{i=1}^{t+1} C_{p-i}^{p-t-1} x^{(i-1)p^t N}$  for non-negative integer  $t$  and  $0 \leq l \leq p - 2$ .

**Proof** In  $F_{pm}[x]$ , if  $l = 0$ , the result is straightforward.

If  $l = 1$ , then  $\sum_{i=1}^{l+1} C_{p-i}^{p-l-1} x^{(i-1)p^t N} = \sum_{i=1}^2 C_{p-i}^{p-2} x^{(i-1)p^t N} = C_{p-2}^{p-2} + C_{p-2}^{p-2} x^{p^t N} = x^{p^t N} + p - 1 = x^{p^t N} - 1 = (x^N - 1)^{p^t}$ .

Suppose  $(x^N - 1)^{p^{l_1}} = \sum_{i=1}^{l_1+1} C_{p-i}^{p-l_1-1} x^{(i-1)p^{l_1} N}$  for some positive integer  $0 \leq l_1 \leq p - 3$ . By Propositions 1.2 and 1.3,

$$\begin{aligned} (x^N - 1)^{p^{l_1+1}} &= (x^N - 1)^{p^{l_1}} \sum_{i=1}^{l_1+1} C_{p-i}^{p-l_1-1} x^{(i-1)p^{l_1} N} = \\ (x^{p^{l_1} N} - 1) \sum_{i=1}^{l_1+1} C_{p-i}^{p-l_1-1} x^{(i-1)p^{l_1} N} &= \sum_{i=1}^{l_1+1} C_{p-i}^{p-l_1-1} x^{ip^{l_1} N} - \\ \sum_{i=1}^{l_1+1} C_{p-i}^{p-l_1-1} x^{(i-1)p^{l_1} N} &= \sum_{i=2}^{l_1+2} C_{p-i}^{p-l_1-1} x^{(i-1)p^{l_1} N} - \\ \sum_{i=1}^{l_1+1} C_{p-i}^{p-l_1-1} x^{(i-1)p^{l_1} N} &= C_{p-l_1-1}^{p-l_1-1} x^{(l_1+1)p^{l_1} N} - \\ C_{p-1}^{p-l_1-1} + \sum_{i=2}^{l_1+1} (C_{p-i}^{p-l_1-1} - C_{p-i-1}^{p-l_1-1}) x^{(i-1)p^{l_1} N} &= \\ C_{p-l_1-2}^{p-l_1-2} x^{(l_1+1)p^{l_1} N} - (C_{p-l_1-1}^{p-l_1-1} - C_{p-1}^{p-l_1-2}) + \\ \sum_{i=2}^{l_1+1} C_{p-i}^{p-l_1-2} x^{(i-1)p^{l_1} N} &= C_{p-l_1-2}^{p-l_1-2} x^{(l_1+1)p^{l_1} N} + \\ C_{p-1}^{p-l_1-2} + \sum_{i=2}^{l_1+1} C_{p-i}^{p-l_1-2} x^{(i-1)p^{l_1} N} &= \sum_{i=1}^{l_1+2} C_{p-i}^{p-l_1-2} x^{(i-1)p^{l_1} N}. \end{aligned}$$

This gives the proof.

**Lemma 4.3** In  $F_{pm}[x]$ ,

$$A_{pj} \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{(pj-1)N} \\ x^{pjN} \end{pmatrix} = \begin{pmatrix} x^{pjN} \\ x^{(pj-1)N} (x^N - 1) \\ \vdots \\ x^{2N} (x^N - 1)^{pj-2} \\ x^N (x^N - 1)^{pj-1} \end{pmatrix}.$$

**Proof** In  $F_{pm}[x]$ , according to Lemma 4.2,

$$A_p \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{(p-1)N} \\ x^{pN} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & C_{p-1}^{p-1} \\ 0 & 0 & \cdots & C_{p-1}^{p-2} & C_{p-2}^{p-2} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & C_{p-1}^1 & \cdots & C_2^1 & C_1^1 \\ (C_{p-1}^0 & C_{p-2}^0 & \cdots & C_1^0 & 1) \end{pmatrix} \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{(p-1)N} \\ x^{pN} \end{pmatrix} = \begin{pmatrix} C_{p-1}^{p-1} x^{pN} \\ \sum_{i=1}^2 C_{p-i}^{p-2} x^{(p+i-2)N} \\ \vdots \\ \sum_{i=1}^{p-1} C_{p-i}^1 x^{[p+i-(p-1)]N} \\ \sum_{i=1}^p x^{iN} \end{pmatrix} = \begin{pmatrix} x^{pN} \\ x^{(p-1)N} (x^N - 1) \\ \vdots \\ x^{2N} (x^N - 1)^{p-2} \\ x^N (x^N - 1)^{p-1} \end{pmatrix}.$$

Let  $L_{pj_1} = \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{(pj_1-1)N} \\ x^{pj_1N} \end{pmatrix}$  and suppose  $A_{pj_1} L_{pj_1} =$

$$\begin{pmatrix} x^{pj_1N} \\ x^{(pj_1-1)N} (x^N - 1) \\ \vdots \\ x^{2N} (x^N - 1)^{pj_1-2} \\ x^N (x^N - 1)^{pj_1-1} \end{pmatrix}$$

in  $F_{pm}[x]$ , where  $j_1$  is a positive integer. By Lemma 4.2, we have

$$A_{pj_1+1} \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{(pj_1+1-1)N} \\ x^{pj_1+1N} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & C_{p-1}^{p-1} A_{pj_1} \\ 0 & 0 & \cdots & C_{p-1}^{p-2} A_{pj_1} & C_{p-2}^{p-2} A_{pj_1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & C_{p-1}^1 A_{pj_1} & \cdots & C_2^1 A_{pj_1} & C_1^1 A_{pj_1} \\ (C_{p-1}^0 A_{pj_1} & C_{p-2}^0 A_{pj_1} & \cdots & C_1^0 A_{pj_1} & A_{pj_1}) \end{pmatrix} \begin{pmatrix} L_{pj_1} \\ x^{pj_1N} L_{pj_1} \\ \vdots \\ x^{(p-2)pj_1N} L_{pj_1} \\ x^{(p-1)pj_1N} L_{pj_1} \end{pmatrix} =$$

$$\begin{pmatrix} A_{\rho j 1} L_{\rho j 1} C_{\rho-1}^{\rho-1} x^{(\rho-1)\rho j 1 N} \\ A_{\rho j 1} L_{\rho j 1} \sum_{i=1}^2 C_{\rho-i}^{\rho-2} x^{(\rho+i-3)\rho j 1 N} \\ \vdots \\ A_{\rho j 1} L_{\rho j 1} \sum_{i=1}^{\rho-1} C_{\rho-i}^1 x^{[\rho+i-(\rho-1)-1]\rho j 1 N} \\ A_{\rho j 1} L_{\rho j 1} \sum_{i=1}^{\rho} x^{(i-1)\rho j 1 N} \end{pmatrix} = \begin{pmatrix} x^{(\rho-1)\rho j 1 N} A_{\rho j 1} L_{\rho j 1} \\ x^{(\rho-2)\rho j 1 N} A_{\rho j 1} L_{\rho j 1} \sum_{i=1}^2 C_{\rho-i}^{\rho-2} x^{(i-1)\rho j 1 N} \\ \vdots \\ x^{\rho j 1 N} A_{\rho j 1} L_{\rho j 1} \sum_{i=1}^{\rho-1} C_{\rho-i}^1 x^{(i-1)\rho j 1 N} \\ A_{\rho j 1} L_{\rho j 1} \sum_{i=1}^{\rho} x^{(i-1)\rho j 1 N} \end{pmatrix} = \begin{pmatrix} x^{(\rho-1)\rho j 1 N} A_{\rho j 1} L_{\rho j 1} \\ x^{(\rho-2)\rho j 1 N} (x^N - 1)^{\rho j 1} A_{\rho j 1} L_{\rho j 1} \\ \vdots \\ x^{\rho j 1 N} (x^N - 1)^{\rho j 1 (\rho-2)} A_{\rho j 1} L_{\rho j 1} \\ (x^N - 1)^{\rho j 1 (\rho-1)} A_{\rho j 1} L_{\rho j 1} \end{pmatrix} = \begin{pmatrix} x^{\rho j 1+1 N} \\ x^{(\rho j 1+1)N} (x^N - 1) \\ x^{(\rho j 1+2)N} (x^N - 1)^2 \\ \vdots \\ x^N (x^N - 1)^{\rho j 1+1} \end{pmatrix}.$$

By induction, the desired result follows.

$(x^N - 1)^i \in F_{pm}[x]/\langle x^{\rho j N} - 1 \rangle$  for  $0 \leq \deg(E_i(x)) \leq N - 1$ , then

**Lemma 4.4** If  $c(x) = \sum_{i=0}^{k-1} E_i(x)x^{(\rho j-i)N}$

$$\left( \underbrace{0, \dots, 0}_{(\rho j-k) \text{ zeros}}, E_0(x), E_1(x), \dots, E_{k-1}(x) \right) A_{\rho j} \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{\rho j N} \end{pmatrix} = x^{kN} (x^N - 1)^{\rho j-k} c(x).$$

**Proof** In  $F_{pm}[x]/\langle x^{\rho j N} - 1 \rangle$ ,  $x^{\rho j N} = 1$ . By Lemma 4.3,

$$\begin{aligned} & \left( \underbrace{0, \dots, 0}_{(\rho j-k) \text{ zeros}}, E_0(x), E_1(x), \dots, E_{k-1}(x) \right) A_{\rho j} \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{\rho j N} \end{pmatrix} = \\ & \left( \underbrace{0, \dots, 0}_{(\rho j-k) \text{ zeros}}, E_0(x), E_1(x), \dots, E_{k-1}(x) \right) \begin{pmatrix} x^{\rho j N} \\ x^{(\rho j-1)N} (x^N - 1) \\ x^{(\rho j-2)N} (x^N - 1)^2 \\ \vdots \\ x^N (x^N - 1)^{\rho j-1} \end{pmatrix} = \\ & (E_0(x), E_1(x), \dots, E_{k-1}(x)) \begin{pmatrix} x^{kN} (x^N - 1)^{\rho j-k} \\ x^{(k-1)N} (x^N - 1)^{\rho j-k+1} \\ \vdots \\ x^N (x^N - 1)^{\rho j-1} \end{pmatrix} = \\ & x^{kN} (x^N - 1)^{\rho j-k} (E_0(x), E_1(x), \dots, E_{k-1}(x)) \begin{pmatrix} x^{\rho j N} \\ x^{(\rho j-1)N} (x^N - 1) \\ \vdots \\ x^{(\rho j-k+1)N} (x^N - 1)^{k-1} \end{pmatrix} = x^{kN} (x^N - 1)^{\rho j-k} c(x). \end{aligned}$$



Let  $n$  and  $p$  be relatively prime, if  $x^n - 1 = f_1 f_2 \cdots f_w$  be the factorization of  $(x^n - 1)$  into a product of monic basic irreducible pairwise coprime polynomials in  $F_{p^m}[x]$ , then the following lemma is straightforward from Theorem 4 and Lemma 3 of Ref. [9].

**Lemma 4.5** Let  $C$  be a  $(1 + u + \cdots + u^{k-1})$  constacyclic code of length  $N = p^e n$  over  $R_{(p^m, k)}$ , then  $C = \langle f_1^{k_1} f_2^{k_2} \cdots f_w^{k_w} \rangle$ , where  $e$  is a non-negative integer and  $0 \leq k_i \leq p^e k$  for positive integer  $1 \leq i \leq w$ . Furthermore,  $|C| = p^{m(kN - \eta)}$ , where  $\eta = \sum_{i=1}^w k_i \deg(f_i)$ .

**Theorem 4.2** Let  $C = \langle f_1^{k_1} f_2^{k_2} \cdots f_w^{k_w} \rangle$  be a  $(1 + u + \cdots + u^{k-1})$  constacyclic code of length  $N = p^e n$  over  $R_{(p^m, k)}$ , where  $e$  is a non-negative integer and  $0 \leq k_i \leq p^e \cdot k$  for positive integer  $1 \leq i \leq w$ . Then the Gray image  $\Phi_{(p^m, k)}(C)$  is a linear cyclic code of length  $p^j N$  over  $F_{p^m}$  and  $\Phi_{(p^m, k)}(C) = \langle (x^N - 1)^{p^j - k} f_1^{k_1} f_2^{k_2} \cdots f_w^{k_w} \rangle$ .

**Proof** By Theorem 4.1,  $\Phi_{(p^m, k)}(C)$  is a linear cyclic code of length  $p^j N$  over  $F_{p^m}$ . So, we only need to prove  $\Phi_{(p^m, k)}(C) = \langle (x^N - 1)^{p^j - k} f_1^{k_1} f_2^{k_2} \cdots f_w^{k_w} \rangle$ . By Lemma 4.1,  $x^{p^j N} = 1$  and  $u = x^{(p^j - 1)N} (x^N - 1)$  in  $R_{(p^m, k)}[x] / \langle x^N - (1 + u + \cdots + u^{k-1}) \rangle$ , so  $u^i = x^{(p^j - i)N} (x^N - 1)^i$ , where  $i = 0, 1, \dots, k-1$ . Let  $c(x) = f_1^{k_1} f_2^{k_2} \cdots f_w^{k_w} \in C$ , then  $c(x) = \sum_{i=0}^{k-1} u^i P_i[c(x)] = \sum_{i=0}^{k-1} P_i[c(x)] x^{(p^j - i)N} (x^N - 1)^i$  and  $x^{(p^j - k + 1)N} c(x) \in C$ . By Lemma 4.4 and the proof of Theorem 4.1,

$$\Phi_{(p^m, k)}[x^{(p^j - k + 1)N} c(x)] = x^{(p^j - k + 1)N} \Phi_{(p^m, k)}[c(x)] = x^{(p^j - k)N} (\underbrace{0, \dots, 0}_{(p^j - k) \text{ zeros}}, P_0[c(x)]),$$

$$P_1[c(x)], \dots, P_{k-1}[c(x)] A_{p^j} \begin{pmatrix} x^N \\ x^{2N} \\ \vdots \\ x^{p^j N} \end{pmatrix} =$$

$$x^{(p^j - k)N} x^{kN} (x^N - 1)^{p^j - k} c(x) = (x^N - 1)^{p^j - k} c(x) \in \Phi_{(p^m, k)}(C).$$

So  $\langle (x^N - 1)^{p^j - k} f_1^{k_1} f_2^{k_2} \cdots f_w^{k_w} \rangle \subseteq \Phi_{(p^m, k)}(C)$ . Comparing the numbers of codewords

by Lemma 4.5, we have  $\Phi_{(p^m, k)}(C) = \langle (x^N - 1)^{p^j - k} f_1^{k_1} f_2^{k_2} \cdots f_w^{k_w} \rangle$ .

## 5 Examples

**Example 1** Let  $p = k = 3$  in Definition 3.2 and Theorem 4.2, we can get some other optimal codes unattainable from Refs. [5] and [6]. Let  $g_1 = x + 2$ ,  $g_2 = x^3 + 2x + 2$ ,  $g_3 = x^3 + x^2 + 2$ ,  $g_4 = x^3 + x^2 + x + 2$  and  $g_5 = x^3 + 2x^2 + 2x + 2$ , then  $x^{13} - 1 = \prod_{i=1}^5 g_i$  in  $F_3[x]$ . Tab. 1 presents several optimal linear cyclic codes over  $F_3$  obtained from  $(1 + u + u^2)$  constacyclic codes over  $F_3[u] / \langle u^3 \rangle$  of length  $N = 13$ .

**Tab.1 Optimal linear cyclic codes over  $F_3$  obtained from  $(1 + u + u^2)$  constacyclic codes over  $F_3[u] / \langle u^3 \rangle$**

Length	Generator polynomial	Gray image
13	$g_1^2 g_2$	[39, 34, 3]
13	$g_1^2 g_3$	[39, 34, 3]
13	$g_1^2 g_4$	[39, 34, 3]
13	$g_1^2 g_5$	[39, 34, 3]
13	$g_1^3 g_4 g_5^2$	[39, 27, 6]
13	$g_1^3 g_1^2 g_5$	[39, 27, 6]
13	$g_1^3 g_3 g_5^2$	[39, 27, 6]
13	$g_1^3 g_3^2 g_5$	[39, 27, 6]
13	$g_1^3 g_3 g_1^2$	[39, 27, 6]
13	$g_1^3 g_3^2 g_4$	[39, 27, 6]
13	$g_1^3 g_2 g_5^2$	[39, 27, 6]
13	$g_1^3 g_2^2 g_5$	[39, 27, 6]
13	$g_1^3 g_2 g_1^2$	[39, 27, 6]
13	$g_1^3 g_2^2 g_4$	[39, 27, 6]
13	$g_1^3 g_2 g_5^2$	[39, 27, 6]
13	$g_1^3 g_2^2 g_3$	[39, 27, 6]

**Example 2** Let  $G_1 = x + 1$ ,  $G_2 = x + 2$ ,  $G_3 = x + 3$  and  $G_4 = x + 4$ , then  $x^4 - 1 = G_1 G_2 G_3 G_4$  in  $F_5[x]$ . Tab. 2 presents several optimal linear cyclic codes over  $F_5$  obtained from  $(1 + u + u^2 + u^3 + u^4)$  constacyclic codes over  $F_5[u] / \langle u^5 \rangle$  of length  $N = 4$ .

**Tab.2 Optimal linear cyclic codes over  $F_5$  obtained from  $(1+u+u^2+u^3+u^4)$  constacyclic codes over  $F_5[u]/\langle u^5 \rangle$**

Length	Generator polynomial	Gray image
4	$G_1 G_2^2$	[20, 17, 3]
4	$G_1^2 G_2$	[20, 17, 3]
4	$G_1 G_3^2$	[20, 17, 3]
4	$G_1^2 G_3$	[20, 17, 3]
4	$G_2 G_4^2$	[20, 17, 3]
4	$G_2^2 G_4$	[20, 17, 3]
4	$G_3 G_4^2$	[20, 17, 3]
4	$G_3^2 G_4$	[20, 17, 3]
4	$G_2 G_3 G_4^3$	[20, 15, 4]
4	$G_2 G_3^3 G_4$	[20, 15, 4]
4	$G_2^3 G_3 G_4$	[20, 15, 4]
4	$G_1 G_3 G_4^3$	[20, 15, 4]
4	$G_1 G_3^3 G_4$	[20, 15, 4]
4	$G_1^3 G_3 G_4$	[20, 15, 4]
4	$G_1 G_2 G_4^3$	[20, 15, 4]
4	$G_1^3 G_2 G_4$	[20, 15, 4]
4	$G_1 G_2 G_3^3$	[20, 15, 4]
4	$G_1 G_2^3 G_3$	[20, 15, 4]
4	$G_1^3 G_2 G_3$	[20, 15, 4]

**Example 3** Let  $Q_1 = x + 1, Q_2 = x + 2, Q_3 = x + 3, Q_4 = x + 4, Q_5 = x + 5$  and  $Q_6 = x + 6$ , then  $x^6 - 1 = \prod_{i=1}^6 Q_i$  in  $F_7[x]$ . Tab. 3 presents several optimal linear cyclic codes over  $F_7$  obtained from  $(1 + u + u^2 + u^3 + u^4 + u^5 + u^6)$  constacyclic codes over  $F_7[u]/\langle u^7 \rangle$  of length  $N = 6$ .

**Tab.3 Optimal linear cyclic codes over  $F_7$  obtained from  $(1+u+u^2+\dots+u^6)$  constacyclic codes over  $F_7[u]/\langle u^7 \rangle$**

Length	Generator polynomial	Gray image
6	$Q_1 Q_2^2$	[42, 39, 3]
6	$Q_1^2 Q_2$	[42, 39, 3]
6	$Q_1 Q_5^2$	[42, 39, 3]
6	$Q_1^2 Q_5$	[42, 39, 3]
6	$Q_2 Q_3^2$	[42, 39, 3]
6	$Q_2^2 Q_3$	[42, 39, 3]

6	$Q_2 Q_6^2$	[42, 39, 3]
6	$Q_2^2 Q_6$	[42, 39, 3]
6	$Q_4 Q_5^2$	[42, 39, 3]
6	$Q_4^2 Q_5$	[42, 39, 3]
6	$Q_4 Q_6^2$	[42, 39, 3]
6	$Q_4^2 Q_6$	[42, 39, 3]
6	$Q_1^3 Q_2 Q_3$	[42, 37, 4]
6	$Q_1 Q_2^3 Q_3$	[42, 37, 4]
6	$Q_1 Q_2 Q_3^3$	[42, 37, 4]
6	$Q_1^3 Q_3 Q_5$	[42, 37, 4]
6	$Q_1 Q_3^3 Q_5$	[42, 37, 4]
6	$Q_1 Q_3 Q_5^3$	[42, 37, 4]
6	$Q_1^3 Q_4 Q_5$	[42, 37, 4]
6	$Q_1 Q_4^3 Q_5$	[42, 37, 4]
6	$Q_1 Q_4 Q_5^3$	[42, 37, 4]
6	$Q_2^3 Q_3 Q_6$	[42, 37, 4]
6	$Q_2 Q_3^3 Q_6$	[42, 37, 4]
6	$Q_2 Q_3 Q_6^3$	[42, 37, 4]
6	$Q_2^3 Q_4 Q_6$	[42, 37, 4]
6	$Q_2 Q_4^3 Q_6$	[42, 37, 4]
6	$Q_2 Q_4 Q_6^3$	[42, 37, 4]
6	$Q_2^3 Q_5 Q_6$	[42, 37, 4]
6	$Q_2 Q_5^3 Q_6$	[42, 37, 4]
6	$Q_2 Q_5 Q_6^3$	[42, 37, 4]
6	$Q_4^3 Q_5 Q_6$	[42, 37, 4]
6	$Q_4 Q_5^3 Q_6$	[42, 37, 4]
6	$Q_4 Q_5 Q_6^3$	[42, 37, 4]
6	$Q_2^2 Q_3 Q_4 Q_5 Q_6^3$	[42, 32, 6]
6	$Q_2 Q_3^2 Q_4 Q_5^2 Q_6^3$	[42, 32, 6]
6	$Q_1 Q_3 Q_4^2 Q_5 Q_6^3$	[42, 32, 6]
6	$Q_1^2 Q_3 Q_4 Q_5^2 Q_6$	[42, 32, 6]
6	$Q_1^2 Q_5^2 Q_4 Q_5 Q_6$	[42, 32, 6]
6	$Q_1^2 Q_5^2 Q_4 Q_5 Q_6$	[42, 32, 6]
6	$Q_1^2 Q_3 Q_4 Q_5^2 Q_6$	[42, 32, 6]
6	$Q_1 Q_2^2 Q_4 Q_5 Q_6^3$	[42, 32, 6]
6	$Q_1 Q_2^2 Q_4 Q_5 Q_6^3$	[42, 32, 6]
6	$Q_1^2 Q_2 Q_4 Q_5^2 Q_6$	[42, 32, 6]
6	$Q_1 Q_2^2 Q_3 Q_5 Q_6^3$	[42, 32, 6]
6	$Q_1^2 Q_2 Q_3 Q_5^2 Q_6$	[42, 32, 6]

6	$Q_1^5 Q_2 Q_3^2 Q_5 Q_6$	[42,32,6]
6	$Q_1 Q_2 Q_3 Q_4^2 Q_5^2$	[42,32,6]
6	$Q_1 Q_2^2 Q_3 Q_4 Q_5^2$	[42,32,6]
6	$Q_1^2 Q_2 Q_3^2 Q_4 Q_5$	[42,32,6]
6	$Q_1^5 Q_2 Q_3^2 Q_4 Q_5$	[42,32,6]
6	$Q_1 Q_2 Q_3 Q_4^2 Q_5^2$	[42,32,6]
6	$Q_1^2 Q_2 Q_3 Q_4 Q_5^2$	[42,32,6]
6	$Q_1^2 Q_2 Q_3^2 Q_4 Q_5$	[42,32,6]
6	$Q_1^5 Q_2 Q_3^2 Q_4 Q_5$	[42,32,6]

## 6 Conclusion

In this paper, we extend the results of Ref. [6] about the Gray map to the polynomial residue ring  $F_{p^m}[u]/\langle u^k \rangle$ , where  $p^{j-1} + 1 \leq k \leq p^j$  and  $u^k = 0$  for some positive prime number  $p$  and positive integer  $j$ . Some optimal linear cyclic codes over  $F_3$ ,  $F_5$  and  $F_7$  are constructed via the Gray map. A natural problem is to find other Gray map over the ring  $F_{p^m}[u]/\langle u^k \rangle$ .

### References

- [1] QIAN J F, ZHANG L N, ZHU S X.  $(1+u)$ -constacyclic and cyclic codes over  $F_2 + uF_2$  [J]. Applied Mathematics Letters, 2006, 19 (8): 820-823.
- [2] AMARRA M C V, NEMENZO F R. On  $(1-u)$  cyclic codes over  $F_{p^k} + uF_{p^k}$  [J]. Applied Mathematics Letters, 2008, 21 (11): 1129-1133.
- [3] SOBHANI R, ESMAEILI E. Some constacyclic and cyclic codes over  $F_q[u]/\langle u^{t+1} \rangle$  [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, 93 (4): 808-813.
- [4] ABULAR T, SIAP I. Constacyclic codes over  $F_2 + uF_2$  [J]. Journal of the Franklin Institute, 2009, 346(5): 520-529.
- [5] DING J, LI H J. The gray images of  $(1+u)$  constacyclic codes over  $F_{2^m}[u]/\langle u^k \rangle$  [J]. Journal of Applied Mathematics and Computing, 2015, 49 (1): 1-13.
- [6] DING J, LI H J. The gray image of a class of constacyclic codes over polynomial residue rings [J]. Journal of the Franklin Institute, 2014, 351 (12): 5467 - 5479.
- [7] KAI X S, ZHU S X, LI P.  $(1+\lambda u)$ -constacyclic codes over  $F_p[u]/\langle u^k \rangle$ . Journal of the Franklin Institute, 2010, 347(5): 751-762.
- [8] DING J, LI H J. Construction of optimal codes with Homogeneous distance [J]. Journal of University of Science and Technology of China, 2015, 45 (7): 588-593.
- [9] 李岩, 朱士信. 环  $F_{p^m} + uF_{p^m} + \dots + u^{k-1}F_{p^m}$  上的一类常循环码 [J]. 合肥工业大学学报, 2013, 35 (3): 408-411.