文章编号:0253-2778(2017)7-0315-08

The Gray Image of A Class of Constacyclic Codes Over the ring $F_{p^m}[u]/<u^k>$

DING Jian, LI Hongju

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

Abstract: Let $R_{(p^m,k)}=F_{p^m}[u]/<u^k>$, where $p^{j-1}+1\leqslant k\leqslant p^j$ 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 $(1+u+\cdots+u^{k-1})$ constacyclic code of an arbitrary length N over $R_{(p^m,k)}$ is a distance invariant linear cyclic code of length p^jN 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 $F_{pm}[u]/<u^k>$[J]. Journal of University of Science and Technology of China, 2017,47(7):315-322.
丁健,李红菊. 环 $F_{pm}[u]/<u^k>$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 $F_{p^m}[u]/<u^k>$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 $R_{(p^m,k)}=F_{p^m}[u]/<u^k>$,其中 $p^{j-1}+1\leqslant k\leqslant p^j$、$u^k=0$、$p$ 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 $(1+u+\cdots+u^{k-1})$ 常循环码的 Gray 像是 F_{p^m} 上长为 p^jN 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[2] 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[3] studied the Gray image of a single-root $(1+u^t)$ constacyclic codes over $F_q[u]/<u^{t+1}>$, which was a quasi-cyclic code over F_q. Abular et al[4] 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 $(1+u+\cdots+u^{k-1})$ constacyclic codes over $F_{2^m}[u]/<u^k>$ in Refs. [5] and [6], while some optimal codes over F_2 and F_4 were constructed. Kai et al[7] and Ding et al[8] 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 $(1+u+\cdots+u^{k-1})$ 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 $(R_{(p^m,k)}[x]$, Lee distance$)$ to $(F_{p^m}[x]$, Hamming distance$)$. In Section 5, we study the structure and generator polynomial of the Gray image of a $(1+u+\cdots+u^{k-1})$ constacyclic code over $R_{(p^m,k)}$. Besides, some optimal linear cyclic codes over F_3, F_5 and F_7 are constructed by meuns of this Gray map in Section 6.

1 Preliminaries

Let $R_{(p^m,k)}$ denote the polynomial residue ring $F_{p^m}[u]/<u^k>$, where $p^{j-1}+1\leqslant k\leqslant p^j$ and $u^k=0$ for some positive prime number p and positive integer j. Let n and p be relatively prime, if $x^n-1=f_1f_2\cdots f_w$ 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 $N=p^en$ over $R_{(p^m,k)}$, where e is a non-negative integer. For some fixed unit α of $R_{(p^m,k)}$, the α constacyclic shift τ_α on $R_{(p^m,k)}{}^N$ is the shift $\tau_\alpha(c_0,c_1,\cdots,c_{N-1})=(\alpha c_{N-1},c_0,c_1,\cdots,c_{N-2})$. The code C is said to be an α constacyclic code if $\tau_\alpha(C)=C$. Now, we identify a codeword $c=(c_0,c_1,\cdots,c_{n-1})$ with its polynomial representation $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}$, then $xc(x)$ corresponds to an α constacyclic shift of $c(x)$ in the ring $R_{(p^m,k)}[x]/<x^N-\alpha>$. Thus α constacyclic codes of length N over $R_{(p^m,k)}$ can be identified as ideals in the ring $R_{(p^m,k)}[x]/<x^N-\alpha>$. In the following, we let $p^{j-1}+1\leqslant k\leqslant p^j$ for some positive prime number p and positive integer j.

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

Proposition 1.1 $C_{p-1}^s\neq 0(\bmod p)$.

Proof $C_{p-1}^s=\dfrac{(p-1)!}{s!\,(p-s-1)!}\neq 0(\bmod p)$.

Proposition 1.2 $C_p^s\equiv 0(\bmod p)$ for positive integer $1\leqslant s\leqslant p-1$.

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

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

Proof If $1\leqslant s\leqslant r$, 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 $0\leqslant s\leqslant r$ and $r\geqslant 1$.

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

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

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

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

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

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

. If $j\geqslant 2$, then $A_{p^j}=$

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

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 $1\leqslant i\leqslant p^j$ respectively, then $A_{p^j}[R(1)]=(\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}},1)$ and $A_{p^j}(p^j)=(\underbrace{1,\cdots,1}_{p^j\text{ ones}})^T$.

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 $C_{p-1}^sA_{p^{j_1}}$ is also invertible in F_{p^m} for positive integer $0\leqslant s\leqslant p-1$, 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 $B_{p^j}A_{p^j}=(A_{p^j}(p^j),\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}})$ in F_{p^m}.

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

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

$$(1,\ \underbrace{0,\cdots,0}_{(pj1-1)\text{ zeros}},C_p^1(1,\ \underbrace{0,\cdots,0}_{(pj1-1)\text{ zeros}}),C_p^2(1,\ \underbrace{0,\cdots,0}_{(pj1-1)\text{ zeros}})\cdots,C_p^{p-1}(1,\ \underbrace{0,\cdots,0}_{(pj1-1)\text{ zeros}}))=(1,\ \underbrace{0,\cdots,0}_{(pj1+1-1)\text{ zeros}}),$$

so $B_{pj1+1}A_{pj1+1}=(A_{pj1+1}(p^{j1+1}),\ \underbrace{0,\cdots,0}_{(pj1+1-1)\text{ zeros}})$. By induction, the desired result follows.

Theorem 2.1 Let $H_{pj}=\begin{pmatrix}1&1&\cdots&1&1\\0&1&\cdots&1&1\\\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&1&1\\0&0&\vdots&0&1\end{pmatrix}$ and

$$D_{pj}=\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&0&\cdots&1\\1&0&0&\cdots&0\end{pmatrix},$$ where H_{pj} and D_{pj} are both $p^j\times p^j$ matrices, then $H_{pj}A_{pj}=A_{pj}D_{pj}$ in F_{pm}.

Proof We prove the result by induction on j in F_{pm}. According to Propositions 1.2 and 1.4, if $2\leqslant i\leqslant p$, then

$$H_pA_p(i)=H_p(\underbrace{0,\cdots,0}_{(p-i)\text{ zcros}},C_{p-1}^{i-1},C_{p-2}^{i-2},\cdots,C_{p-i+1}^{1},C_{p-i}^{0})^T=$$

$$(\underbrace{C_p^{i-1},\cdots,C_p^{i-1}}_{p-i+1},C_{p-1}^{i-2},\cdots,C_{p-i+2}^{1},C_{p-i}^{0})^T=$$

$$(\underbrace{0,\cdots,0}_{p-i+1},C_{p-1}^{i-2},\cdots,C_{p-i+2}^{1},C_{p-i+1}^{0})^T=A_p(i-1).$$

Besides, $H_pA_p(1)=(\underbrace{1,\cdots,1}_{p\ ones})^T=A_p(p)$, So $H_pA_p=(A_p(p),A_p(1),A_p(2),\cdots,A_p(p-1)=A_pD_p)$.

Suppose $H_{pj1}A_{pj1}=A_{pj1}D_{pj1}$ for some positive integer j_1 in F_{pm}, then

$$H_{pj1}A_{pj1}=(A_{pj1}(p^{j1}),A_{pj1}(1),$$
$$A_{pj1}(2),\cdots,A_{pj1}(p^{j1}-1))$$

and

$$H_{pj1+1}A_{pj1+1}=\begin{pmatrix}H_{pj1}&B_{pj1}&\cdots&B_{pj1}&B_{pj1}\\0&H_{pj1}&\cdots&B_{pj1}&B_{pj1}\\\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&H_{pj1}&B_{pj1}\\0&0&\vdots&0&H_{pj1}\end{pmatrix}\begin{pmatrix}0&0&\cdots&0&C_{p-1}^{p-1}A_{pj1}\\0&0&\cdots&C_{p-1}^{p-2}A_{pj1}&C_{p-2}^{p-2}A_{pj1}\\\vdots&\vdots&\cdots&\vdots&\vdots\\0&C_{p-1}^{1}A_{pj1}&\cdots&C_{2}^{1}A_{pj1}&C_{1}^{1}A_{pj1}\\C_{p-1}^{0}A_{pj1}&C_{p-2}^{0}A_{pj1}&\cdots&C_{1}^{0}A_{pj1}&A_{pj1}\end{pmatrix}.$$

By Lemma 2.2,

$$H_{pj1+1}\begin{pmatrix}0\\\vdots\\0\\C_{p-1}^{0}A_{pj1}\end{pmatrix}=\begin{pmatrix}B_{pj1}A_{pj1}\\\vdots\\B_{pj1}A_{pj1}\\H_{pj1}A_{pj1}\end{pmatrix}=\begin{pmatrix}A_{pj1}(p^{j1})&0&0&\cdots&0\\\vdots&\vdots&\vdots&\vdots&\vdots\\A_{pj1}(p^{j1})&0&0&\cdots&0\\A_{pj1}(p^{j1})&A_{pj1}(1)&A_{pj1}(2)&\cdots&A_{pj1}(p^{j1}-1)\end{pmatrix}=$$

$$(A_{pj1+1}(p^{j1+1}),A_{pj1+1}(1),A_{pj1+1}(2),\cdots,A_{pj1+1}(p^{j1}-1)).$$

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

$$H_{pj1+1}\begin{pmatrix}0\\\vdots\\0\\C_{p-1}^{i-1}A_{pj1}\\C_{p-2}^{i-2}A_{pj1}\\\vdots\\C_{p-i+1}^{1}A_{pj1}\\C_{p-i}^{0}A_{pj1}\end{pmatrix}=\begin{pmatrix}C_p^{i-1}B_{pj1}A_{pj1}\\\vdots\\C_p^{i-1}B_{pj1}A_{pj1}\\C_{p-1}^{i-1}H_{pj1}A_{pj1}+C_{p-1}^{i-2}B_{pj1}A_{pj1}\\C_{p-2}^{i-2}H_{pj1}A_{pj1}+C_{p-2}^{i-3}B_{pj1}A_{pj1}\\\vdots\\C_{p-i+1}^{1}H_{pj1}A_{pj1}+C_{p-i+1}^{0}B_{pj1}A_{pj1}\\C_{p-i+1}^{0}H_{pj1}A_{pj1}\end{pmatrix}=$$

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

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

$$(A_{pj1+1}((i-1)p^{j1}), A_{pj1+1}((i-1)p^{j1}+1), A_{pj1+1}((i-1)p^{j1}+2), \cdots, A_{pj1+1}(ip^{j1}-1)).$$

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 $R_{(p^m,k)}$, 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 $r_i(a), r_i(b)\in F_{p^m}$ for positive integer $0\leqslant i\leqslant k-1$. It is easy to check that $r_i(a+b)=r_i(a)+r_i(b)$ for $0\leqslant i\leqslant k-1$.

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

Note that $\Phi_{(p^m,k)}$ is linear, since

$$\Phi_{(p^m,k)}(a+b)=(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}}, r_0(a+b),$$

$$r_1(a+b), \cdots, r_{k-1}(a+b))A_{pj}=$$

$$[(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}}, r_0(a), r_1(a), \cdots, r_{k-1}(a))+$$

$$(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}}, r_0(b), r_1(b), \cdots, r_{k-1}(b))]A_{pj}=$$

$$\Phi_{(p^m,k)}(a)+\Phi_{(p^m,k)}(b).$$

Furthermore, $\Phi_{(p^m,k)}$ is a bijection from $R_{(p^m,k)}$ to $F_{p^m}{}^{pj}$ because of the invertibility of A_{pj} by Lemma 2.1. we identify a codeword $c=(c_0,c_1,\cdots,c_{N-1})\in R_{(p^m,k)}{}^N$ with its polynomial representation $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}$ and denote $P_i[c(x)]=\sum_{l=0}^{N-1}r_i(c_l)x^l$ for positive integer $0\leqslant i\leqslant k-1$, then $c(x)=\sum_{i=0}^{k-1}u_iP_i[c(x)]$. Thus, the Gray map $\Phi_{(p^m,k)}$ can be extended to $R_{(p^m,k)}[x]$ in an obvious way.

Definition 3.2 For an arbitrary codeword $c=(c_0,c_1,\cdots,c_{N-1})\in R_{(p^m,k)}{}^N$, its polynomial representation is $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}\in R_{(p^m,k)}[x]$. The polynomial Gray map $\Phi_{(p^m,k)}$ from $R_{(p^m,k)}[x]$ to $F_{p^m}[x]$ is defined as follows:

$$\Phi_{(p^m,k)}[c(x)]=(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}}, P_0[c(x)],$$

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

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

Definition 3.3 Let W_L be the Lee weight of the element of $R_{(p^m,k)}$ and W_H be the Hamming weight of the element of $F_{p^m}{}^{pj}$. We define that $W_L(a)=W_H[\Phi_{(p^m,k)}(a)]$ 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 ($R_{(p^m,k)}[x]$, Lee distance) to ($F_{p^m}[x]$, Hamming distance).

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

Lemma 4.1 In $R_{(p^m,k)}[x]/<x^N-(1+u+\cdots+u^{k-1})>$, $x^{pjN}=1$ and $u=x^{(pj-1)N}(x^N-1)$.

Proof In $R_{(p^m,k)}[x]/<x^N-(1+u+\cdots+u^{k-1})>$, $x^N=1+u+\cdots+u^{k-1}$, $u^k=0$ and $p^{j-1}+1\leqslant k\leqslant p^j$, so $u^{pj}=0$ and $x^{pjN}=(1+u+\cdots+u^{k-1})^{pj}=1$. Since $(1-u)x^N=1-u^k=1=x^{pjN}$, then $u=1-x^{(pj-1)N}=x^{(pj-1)N}(x^N-1)$.

Theorem 4.1 If C is a $(1+u+\cdots+u^{k-1})$ constacyclic code of length N over $R_{(p^m,k)}$, then $\Phi_{(p^m,k)}(C)$ is a linear cyclic code of length p^jN 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, $x^N=1+u+\cdots+u^{k-1}$ and $x^{pjN}=1$ in $R_{(p^m,k)}[x]/<x^N-(1+u+\cdots+u^{k-1})>$ by Lemma 5.1. For an arbitrary codeword $c(x)=c_0+c_1x+c_2x^2+\cdots+c_{N-1}x^{N-1}\in C$, it can be written in the form $c(x)=\sum_{i=0}^{k-1}u^iP_i[c(x)]$. Then, we have $xc(x)=(1+u+\cdots+u^{k-1})c_{N-1}+c_0x+c_1x^2+\cdots+c_{N-2}x^{N-1}=\sum_{i=0}^{k-1}u^iP_i[xc(x)]$, where

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

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

$$\Phi_{(p^m,k)}[xc(x)]=(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}},P_0[xc(x)],P_1[xc(x)],\cdots,P_{k-1}[xc(x)])A_{pj}\begin{pmatrix}1\\x^N\\\vdots\\x^{(pj-1)N}\end{pmatrix}=$$

$$(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}},r_0(c_{N-1}),\sum_{i=0}^{1}r_i(c_{N-1}),\cdots,\sum_{i=0}^{k-1}r_i(c_{N-1}))A_{pj}\begin{pmatrix}1\\x^N\\\vdots\\x^{(pj-1)N}\end{pmatrix}-$$

$$(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}},x^Nr_0(c_{N-1}),x^Nr_1(c_{N-1}),\cdots,x^Nr_{k-1}(c_{N-1}))A_{pj}\begin{pmatrix}1\\x^N\\\vdots\\x^{(pj-1)N}\end{pmatrix}+$$

$$(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}},xP_0[c(x)],xP_1[c(x)],\cdots,xP_{k-1}[c(x)])A_{pj}\begin{pmatrix}1\\x^N\\\vdots\\x^{(pj-1)N}\end{pmatrix}=$$

$$(\underbrace{0,\cdots,0}_{(pj-k)\text{ zeros}},r_0(c_{N-1}),r_1(c_{N-1}),\cdots,r_{k-1}(c_{N-1}))(H_{pj}A_{pj}-A_{pj}D_{pj})\begin{pmatrix}1\\x^N\\\vdots\\x^{(pj-1)N}\end{pmatrix}+x\Phi_k[c(x)].$$