第45卷第7期 中国科学技术大学学报 Vol. 45, No. 7
2015年7月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jul. 2015

Article ID: 0253-2778(2015)07-0588-06

Construction of optimal codes with Homogeneous distance

DING Jian, LI Hongju

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

Abstract: Based on the torsion codes of a $(1+\lambda u)$ constacyclic code with arbitrary length over $R_{(p^m,k)}=F_{p^m}[u]/<u^k>$, a bound for the homogeneous distance of a $(1+\lambda u)$ constacyclic code with an arbitrary length over $R_{(p^m,k)}$ is obtained and the exact homogeneous distances of some $(1+\lambda u)$ constacyclic codes over $R_{(p^m,k)}$ are determined, where λ is a unit of $R_{(p^m,k)}$. Furthermore, a new distance-preserving Gray map from $R^N_{(p^m,k)}$ (Homogeneous distance) to $F_{p^m}^{p^{m(k-1)}N}$ (Hamming distance) is defined. It is proved that the Gray image of a linear $(1+\lambda u)$ constacyclic code of arbitrary length over $R_{(p^m,k)}$ is a linear code over F_{p^m}, and some optimal linear codes over F_2, F_3, and F_4 are constructed under this Gray map.

Key words: Optimal code; Constacyclic code; Homogeneous distance; Gray map

CLC number: TN911.22 **Document code**: A doi: 10.3969/j.issn.0253-2778.2015.07.013

Citation: DING Jian, LI Hongju. Construction of optimal codes with Homogeneous distance[J]. Journal of University of Science and Technology of China, 2015,45(7): 588-593.

利用齐次距离构造最优码

丁 健,李红菊

(安徽新华学院公课部,安徽合肥,230088)

摘要:利用 $R_{(p^m,k)}=F_{p^m}[u]/<u^k>$ 上任意长度的 $(1+\lambda u)$ 常循环码的挠码得到了 $R_{(p^m,k)}$ 上任意长度的 $(1+\lambda u)$ 常循环码的齐次距离的界,并确定了 $R_{(p^m,k)}$ 上某些 $(1+\lambda u)$ 常循环码的齐次距离的准确值,其中 λ 是 $R_{(p^m,k)}$ 上的单位. 此外,定义了从 $R^N_{(p^m,k)}$ (Homogeneous 距离)到 $F_{p^m}^{p^{m(k-1)}N}$ (Hamming 距离)的一个新的保距 Gray 映射,得到 $R_{(p^m,k)}$ 上任意长度的线性 $(1+\lambda u)$ 常循环码的 Gray 像是 F_{p^m} 上的线性码,构造了 F_2、F_3 和 F_4 上的一些最优线性码.

关键词:最优码;常循环码;Homogeneous 距离;Gray 映射

0 Introduction

Distance is a very important indicator of the quality of a code, and has thus been attracted much attention. In Ref. [1], the distributions of the Hamming distances, Lee distances and Euclidean distances of a $(1+u)$ constacyclic code with length 2^s over F_2+uF_2 were determined by Deng et al. In Ref. [2], Shi et al investigated the Homogeneous

Received: 2015-01-28; **Revised**: 2015-06-10

Foundation item: Supported by National Natural Science Foundation of China (61370089), Anhui Province Natural Science Research (KJ2015A308) and Natural Science Project of AnHui Xinhua University (2014Zr009).

Biography: DING Jian (corresponding author), male, born in 1982, Master/lecture. Research field: Algebraic coding.
Email: dingjian_happy@163.com

distance of a $(1+u)$ constacyclic code with length 2^s over $F_{p^m}[u]/<u^k>$, which was extented to $(1+\lambda u)$ constacyclic codes with length p^s over $R_{(p^m,k)}$ by Liu et al in Ref. [3] for any unit $\lambda\in R_{(p^m,k)}$. Zhu et al[4] discussed the the Homogeneous distance of a $(1+u)$ constacyclic code with an arbitrary length over $R_{(p^m,k)}$. Besides, Gray map is a bridge that connects a code over a ring with a code over finite field. In Ref. [5], a distance-preserving Gray map from $(F_2+uF_2)^N$ (Lee distance) to F_2^{2N} (Hamming distance) was defined by Qian et al, and the resulting Gray image of a single-root $(1+u)$-constacyclic code over F_2+uF_2 is a binary linear cyclic code, based on which several binary optimal linear codes were constructed under the Gray map. It was extended to $F_{2^m}[u]/<u^k>$ by Jian et al[6-7]. Kai et al [8] showed that the Gray image of a linear $(1+\lambda u)$ constacyclic code (Gray distance) of an arbitrary length over F_p+uF_p was a distance invariant linear code (Hamming distance) over F_p. In Ref. [9], Amarra et al derived that the Gray image of a single－root $(1-u)$ constacyclic code (Homogeneous distance) over $F_{p^m}+uF_{p^m}$ was a quasi-cyclic code (Hamming distance) over F_{p^m}. Furthermore, two optimal codes over F_4 were constructed. Later, the result of Ref. [9] was extended to single-root $(1+u^{k-1})$ constacyclic codes and single-root $(1-u^{k-1})$ constacyclic codes over $R_{(p^m,k)}$ in Refs. [10-11] respectively, but optimal codes were not given.

In this paper, we give a bound for the homogeneous distance of a $(1+\lambda u)$ constacyclic code of an arbitrary length over $R_{(p^m,k)}$ and the exact homogeneous distances of some $(1+\lambda u)$ constacyclic codes over $R_{(p^m,k)}$ are determined, where λ is a unit of $R_{(p^m,k)}$. Furthermore, a new distance-preserving Gray map from $R^N_{(p^m,k)}$ (Homogeneous distance) to $F_{p^m}^{p^{m(k-1)}N}$ (Hamming distance) is defined, and some optimal linear codes over F_2, F_3 and F_4 are constructed via the Gray map.

1 Preliminaries

Let $R_{(p^m,k)}$ denote the polynomial residue ring $F_{p^m}[u]/<u^k>$, where positive integer $k\geqslant 2$, p is a positive prime number and $u^k=0$. Let n and p be relatively prime, if $x^n-1=f_1f_2\cdots f_j$ 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 $R^N_{(p^m,k)}$ 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 Ref. [12], the notion of homogeneous weight on arbitrary finite chain rings was defined. The homogeneous weight of $a\in R_{(p^m,k)}$ is given by

$$w_{\hom}(a)=\begin{cases}p^{m(k-1)}, & a\in u^{k-1}R_{(p^m,k)}\backslash\{0\}\\ p^{m(k-1)}(p^m-1), & a\in R_{(p^m,k)}\backslash u^{k-1}R_{(p^m,k)}.\\ 0, & a=0\end{cases}$$

This extends to a weight function on $R^N_{(p^m,k)}$. For $c=(c_0, c_1, \cdots, c_{N-1})\in R^N_{(p^m,k)}$, we define $w_{\hom}(c)=\sum_{i=0}^{N-1}w_{\hom}(c_i)$. The homogeneous distance $d_{\hom}(X,Y)$ between any two distinct vectors $X,Y\in R^N_{(p^m,k)}$ is defined to be $w_{\hom}(X-Y)$. The minimum homogeneous distance of any two distinct codewords of C is called the homogeneous distance of C, which is denoted by $d_{\hom}(C)$.

Any $a\in r_{(p^m,k)}$, it can be written uniquely as $a=\sum_{i=0}^{k-1}u^ir_i(a)$, where $r_i(a)\in F_{p^m}$ for $0\leqslant i\leqslant k-1$. Let $\bar{a}=R_0(a)$ and $(C:u^\eta)=\{c\in R^N_{(p^m,k)}\mid u^\eta c\in C\}$ for $0\leqslant\eta\leqslant k-1$. If C is a $(1+\lambda u)$ constacyclic code of length N over $R_{(p^m,k)}$, then $(C:u^\eta)$ is also a

$(1+\lambda u)$ constacyclic code of length N over $R_{(p^m,k)}$ and $(C: u^i) \subseteq (C: u^{i+1})$ for $0 \leqslant i \leqslant k-1$. Besides, $\overline{(C: u^\eta)}$ is called the ηth-torsion code of C, which is denoted by $\mathrm{Tor}_\eta(C)$. Obviously, $\mathrm{Tor}_\eta(C)$ is a cyclic code over F_{p^m} of length N.

2 Homogeneous distance

In the following, we suppose $x^n-1=f_1 f_2 \cdots f_j$ is the factorization of (x^n-1) into a product of monic basic irreducible pairwise coprime polynomials in $F_{p^m}[x]$, then the following lemmas is straight forward from Theorem 4 and Lemma 3 of Ref. [13].

Lemma 2.1[13] Let C be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$ for any unit $\lambda \in R_{(p^m,k)}$, then $C=<\prod_{i=1}^{j} f_i^{k_i}>$, where non-negative integer $0 \leqslant k_i \leqslant kp^e$ for $0 \leqslant i \leqslant j$. Furthermore, $|C|=p^{m(kN-\varepsilon)}$, where $\varepsilon=\sum_{i=1}^{j} k_i \deg(f_i)$.

Lemma 2.2 Let $C=<\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}>$ be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$, then $<\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}> \subseteq (C: u^\eta)$, where $<\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}>$ is a $(1+\lambda u)$ constacyclic code over $R_{(p^m,k)}$ of length N for $0 \leqslant \eta \leqslant k-1$ and $\theta_i^{(\eta)}=k_i-\min\{p^e\eta, k_i\}$.

Proof For any $h(x) \in <\prod_{i=1}^{j} f_i^{k_i}>$, there exsits $g(x) \in R_{(p^m,k)}[x]/<x^N-(1+\lambda u)>$ such that $h(x)=g(x)\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}$. Thus,

$$u^\eta h(x)=[\lambda^{-1}(x^N-1)]^\eta g(x)\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}=$$

$$\lambda^{-\eta}(x^n-1)^{p^e\eta} g(x)\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}=\lambda^{-\eta} g(x)\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}+p^e\eta}=$$

$$\lambda^{-\eta} g(x)\prod_{i=1}^{j} f_i^{k_i+p^e\eta-\min\{p^e\eta, k_i\}} \in C,$$

this gives the proof.

Lemma 2.3 Let $f(x)$ be a monic divisor of (x^n-1) in $F_{p^m}[x]$. Then, for any positive integer l, $<f^{p^e+l}(x)>=<f^{p^e}(x)>$ in $F_{p^m}[x]/<(x^N-1)>$.

Proof Let $\hat{f}(x)=(x^n-1)/f(x)$. Since $f(x)$ and $\hat{f}(x)$ are coprime in $F_{p^m}[x]$, it follows that $f^l(x)$ and $\hat{f}(x)$ are coprime in $F_{p^m}[x]$. Hence, there exist $\mu(x)$, $\nu(x) \in F_{p^m}[x]$ such that $\mu(x) f^l(x)+\nu(x)\hat{f}^{p^e}(x)=1$. Computing in $F_{p^m}[x]/<(x^N-1)>$, we have

$$\mu(x) f^{p^e+l}(x)=[1-\nu(x)\hat{f}^{p^e}(x)]\hat{f}^{p^e+l}(x)=f^{p^e}(x),$$

this gives the proof.

The following lemma is from Theorem 1 of Ref. [14].

Lemma 2.4 If C is a linear code over $R_{(p^m,k)}$, then $|C|=\prod_{\eta=0}^{k-1}|\mathrm{Tor}_\eta(C)|$.

Theorem 2.1 Let $C=<\prod_{i=1}^{j} f_i^{k_i}>$ be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$, then $\mathrm{Tor}_\eta(C)=<\prod_{i=1}^{j} f_i^{\tau_i^{(\eta)}}>$ is a cyclic code over F_{p^m} of length N, where $\tau_i^{(\eta)}=\min\{p^e(\eta+1), k_i\}-\min\{p^e\eta, k_i\}$ for $0 \leqslant \eta \leqslant k-1$ and $1 \leqslant i \leqslant j$.

Proof From Lemmas 2.2 and 2.3, we get

$$\mathrm{Tor}_\eta(C)=\overline{(C: u^\eta)} \supseteq \overline{<\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}>}=<\prod_{i=1}^{j} \overline{f}_i^{\theta_i^{(\eta)}}>.$$

So, in $F_{p^m}[x]/(x^N-1)$, $\mathrm{Tor}_\eta(C) \supseteq <\prod_{i=1}^{j} f_i^{\theta_i^{(\eta)}}>=<\prod_{i=1}^{j} f_i^{\min\{p^e, \theta_i^{(\eta)}\}}>=<\prod_{i=1}^{j} f_i^{\tau_i^{(\eta)}}>$.

Since $|<\prod_{i=1}^{j} f_i^{\tau_i^{(\eta)}}>|=p^{m[N-\sum_{i=1}^{j}\tau_i^{(\eta)}\deg(f_i)]}$, then $\prod_{\eta=0}^{k-1}|\mathrm{Tor}_\eta(C)| \geqslant$

$$p^{m\sum_{\eta=0}^{k-1}[N-\sum_{i=1}^{j}\tau_i^{(\eta)}\deg(f_i)]}=p^{m[kN-\sum_{i=1}^{j}k_i\deg(f_i)]}.$$

From Lemmas 2.1 and 2.4, the result follows.

Let $d_H(C)$ and d_η be the Hamming distance of C and $\mathrm{Tor}_\eta(C)$ respectively. The following lemma is from Theorem 4.2 of Ref. [15].

Lemma 2.5[15] Let C be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$, then $d_{\mathrm{hom}}(C)=p^{m(k-1)} d_{k-1}$ for $0 \leqslant \eta \leqslant k-1$.

Theorem 2.2 Let C be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$, then $p^{m(k-2)}\min\{(p^m-1)d_{k-2}, p^m d_{k-1}\} \leqslant d_{\mathrm{hom}}(C) \leqslant p^{m(k-1)} d_{k-1}$.

Proof The proof is similar to that of Theorem 5 of Ref. [4].

From Theorem 2.2, we can get the following corollary.

Corollary 2.1 Let C be a $(1+\lambda u)$

constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$. If $(p^m-1)d_{k-2}\geqslant p^m d_{k-1}$, then $d_{\hom}(C)=p^{m(k-1)}d_{k-1}$.

Corollary 2.2 Let $C=\langle\prod_{i=1}^{j} f_i^{k_i}\rangle$ be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$. If $\min\{k_1, k_2, \cdots, k_j\}\geqslant p^e(k-1)$, then $d_{\hom}(C)=p^{m(k-1)}d_{k-1}$.

Proof If $\min\{k_1, k_2, \cdots, k_j\}\geqslant p^e(k-1)$, then

$$C=\langle\prod_{i=1}^{j} f_i^{k_i}\rangle=\langle(x^n-1)^{p^e(k-1)}\prod_{i=1}^{j} f_i^{k_i-p^e(k-1)}\rangle=$$

$$\langle u^{k-1}\lambda^{k-1}\prod_{i=1}^{j} f_i^{k_i-p^e(k-1)}\rangle.$$

From Definition of Homogeneous weight and Lemma 2.5, we get $d_{\hom}(C)=p^{m(k-1)}d_{k-1}$.

Corollary 2.3 Let $C=\langle\prod_{i=1}^{j} f_i^{k_i}\rangle$ be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$ and $\sigma=\max\{k_1, k_2, \cdots, k_j\}$.

(1) If $1\leqslant\sigma\leqslant p^e(k-2)$, then $d_{\hom}(C)=p^{m(k-2)}(p^m-1)$.

(2) If $p^e(k-2)+1\leqslant\sigma\leqslant p^e(k-1)$, then $d_{\hom}(C)=p^{m(k-1)}$.

Proof The proof is similar to that of Corollary 2 of Ref.[4].

3 A new Gray map

Any $a, b\in R_{(p^m,k)}$ can be written uniquely as $a=\sum_{i=0}^{k-1}u^i r_i(a)$ and $b=\sum_{i=0}^{k-1}u^i r_i(b)$, where $r_i(a)$, $r_i(b)\in F_{p^m}$ and $r_i(a+b)=r_i(a)+r_i(b)$ for $0\leqslant i\leqslant k-1$.

Definition 3.1 For any element a in $R_{(p^m,k)}$, the Gray map $\Phi_{(p^m,k)}: R_{(p^m,k)}\to F_{p^m}^{p^{m(k-1)}}$ is defined as $\Phi_{(p^m,k)}(a)=(A_1(a), A_2(a), \cdots, A_{p^{m(k-1)}}(a))$, where $A_l(a)\in\{r_{k-1}(a)+\sum_{i=0}^{k-2}\xi_i r_i(a)\mid\xi_i\in F_{p^m}\}$ and pairwise inequal for $1\leqslant l\leqslant p^{m(k-1)}$. Naturally, the Gray map can be extended as follows:

$\Phi_{(p^m,k)}: R_{(p^m,k)}^N\to F_{p^m}^{p^{m(k-1)}N}$,

$(c_0, c_1, \cdots, c_{N-1})\to$

$(\Phi_{(p^m,k)}(c_0), \Phi_{(p^m,k)}(c_1), \cdots, \Phi_{(p^m,k)}(c_{N-1}))$.

Lemma 3.1 The Gray map $\Phi_{(p^m,k)}$ is a distance-preserving map from $R_{(p^m,k)}^N$ (Homogeneous distance) to $F_{p^m}^{p^{m(k-1)}N}$ (Hamming distance).

Proof Let $a\in R_{(p^m,k)}$ and $w_{\mathrm{Ham}}[\Phi_{(p^m,k)}(a)]$ be the Hamming weight of $\Phi_{(p^m,k)}(a)$.

If $a=0$, then $r_i(0)=0$ for $0\leqslant i\leqslant k-1$. Thus $r_{k-1}(0)+\sum_{i=0}^{k-2}\xi_i r_i(0)=0$ for arbitrary $\xi_i\in F_{p^m}$, which implies $A_l(0)=0$ for $1\leqslant l\leqslant p^{m(k-1)}$. So

$$w_{\mathrm{Ham}}[\Phi_{(p^m,k)}(0)]=0.$$

If $a\in u^{k-1}R_{(p^m,k)}\backslash\{0\}$, then $r_{k-1}(a)\neq 0$ and $r_i(a)=0$ for $0\leqslant i\leqslant k-2$. So $r_{k-1}(a)+\sum_{i=0}^{k-2}\xi_i r_i(a)\neq 0$ for arbitrary $\xi_i\in F_{p^m}$, which implies $A_l(a)\neq 0$ for $1\leqslant l\leqslant p^{m(k-1)}$. Thus

$$w_{\mathrm{Ham}}[\Phi_{(p^m,k)}(a)]=p^{m(k-1)}\text{ for } a\in u^{k-1}R_{(p^m,k)}\backslash\{0\}.$$

If $a\in R_{(p^m,k)}\backslash u^{k-1}R_{(p^m,k)}$, there exists $r_s(a)\neq 0$ where $0\leqslant s\leqslant k-2$. So, there were $p^{m(k-1)}(p^m-1)$ non-zero elements in $\{r_{k-1}(a)+\sum_{i=0}^{k-2}\xi_i r_i(a)\mid\xi_i\in F_{p^m}\}$, which implies $w_{\mathrm{Ham}}[\Phi_{(p^m,k)}(a)]=p^{m(k-2)}(p^m-1)$ for $a\in R_{(p^m,k)}\backslash u^{k-1}R_{(p^m,k)}$.

So $w_{\mathrm{Ham}}[\Phi_{(p^m,k)}(a)]=w_{Ham}(a)$ for any $a\in R_{(p^m,k)}$, this gives the proof.

Lemma 3.2 Let C is a linear code over $R_{(p^m,k)}$ of length N. Then $\Phi_{(p^m,k)}(C)$ is a linear code over F_{p^m} of length $p^{m(k-1)}N$.

Proof For any element $a, b\in R_{(p^m,k)}$, we have

$\Phi_{(p^m,k)}(a+b)=(A_1(a+b), A_2(a+b),\cdots,A_{p^{m(k-1)}}(a+b))=$

$(A_1(a)+A_1(b),A_2(a)+A_2(b),\cdots,A_{p^{m(k-1)}}(a)+A_{p^{m(k-1)}}(b))=$

$(A_1(a),A_2(a),\cdots,A_{p^{m(k-1)}}(a))+(A_1(b),A_2(b),\cdots,A_{p^{m(k-1)}}(b))=$

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

Besides, for any element $\beta\in F_{p^m}^*$, we have

$\Phi_{(p^m,k)}(\beta a)=$

$(A_1(\beta a), A_2(\beta a), \cdots, A_{p^{m(k-1)}}(\beta a))=$

$(\beta A_1(a), \beta A_2(a), \cdots, \beta A_{p^{m(k-1)}}(a))=$

$\beta\Phi_{(p^m,k)}(a)$

So, for any two codewords $c=(c_0, c_1, \cdots, c_{N-1})$ and $c'=(c'_0, c'_1, \cdots, c'_{N-1})$ of C, we have

$\Phi_{(p^m,k)}(c+c')=$

$(\Phi_{(p^m,k)}(c_0+c'_0),\Phi_{(p^m,k)}(c_1+c'_1),\cdots,\Phi_{(p^m,k)}(c_{N-1}+c'_{N-1}))=$

$\Phi_{(p^m,k)}(c)+\Phi_{(p^m,k)}(c')$.

Furthermore, $\Phi_{(p^m,k)}(\beta c)=(\Phi_{(p^m,k)}(\beta c_0), \Phi_{(p^m,k)}(\beta c_1), \cdots, \Phi_{(p^m,k)}(\beta c_{N-1}))=\beta\Phi_{(p^m,k)}(c)$.

Hence, $\Phi_{(p^m,k)}(C)$ is linear.

From Lemmas 2.1, 3.1 and 3.2, the following theorem is straightforward.

Theorem 3.1 Let $C=\langle\prod_{i=1}^{j} f_i^{k_i}\rangle$ be a $(1+\lambda u)$ constacyclic code of length $N=p^e n$ over $R_{(p^m,k)}$, *then* $\Phi_{(p^m,k)}(C)$ is a linear $[p^{m(k-1)}N, KN-\sum_{i=1}^{l}k_i\deg(f_i), d_{\hom}(C)]$ code over F_{p^m}.

We say that a linear code C over F_{p^m} is optimal if C has the maximal minimum distance for the given length and dimension. According to the minimum homogeneous distance of $(1+\lambda u)$ constacyclic codes and Theorem 3.1, we can obtain some optimal linear codes over F_{p^m}.

Example 3.1 In $F_2[x]$,

$$x^7-1=f_1(x)f_2(x)f_3(x),$$

where $f_1(x)=x+1$, $f_2(x)=x^3+x+1$, $f_3(x)=x^3+x^2+1$. Let $C=\langle f_1^2(x)f_2^2(x)f_3(x)\rangle$ be a $(1+u)$ constacyclic code over F_2+uF_2 of length 7. By Theorem 2.1, we get $\mathrm{Tor}_i(C)=\langle f_1(x)f_2(x)\rangle$, which is a [7,3,4] cyclic code over F_2. According to Corollary 2.2 and Theorem 3.1, $\Phi_{(2,2)}(C)$ is a [14,3,8] linear code over F_2, which is an optimal code. We list several binary optimal linear codes obtained from $(1+u)$ constacyclic codes over F_2+uF_2 in Tab. 1.

Example 3.2 In $F_3[x]$,

$$x^4-1=f_1(x)f_2(x)f_3(x),$$

Tab. 1 Optimal binary linear codes obtained from $(1+u)$ constacyclic codes over F_2+uF_2

Length of C	Generator polynomial of C	Gray image
3	$(x+1)^2(x^2+x+1)$	[6,2,4]
5	$(x+1)^2(x^4+x^3+x^2+x+1)$	[10,4,4]
6	$(x+1)^3(x^2+x+1)^2$	[12,5,4]
6	$(x+1)^4(x^2+x+1)^3$	[12,2,8]
6	$(x+1)^3(x^2+x+1)$	[12,7,4]
6	$(x+1)(x^2+x+1)^3$	[12,5,4]
6	$(x+1)^4(x^2+x+1)$	[12,6,4]
6	$(x+1)(x^2+x+1)^4$	[12,3,6]
7	$(x+1)^2(x^3+x+1)^2(x^3+x^2+1)$	[14,3,8]
7	$(x+1)^2(x^3+x+1)(x^3+x^2+1)^2$	[14,3,8]
7	$(x+1)^2(x^3+x+1)$	[14,9,4]
7	$(x+1)^2(x^3+x^2+1)$	[14,9,4]
9	$(x+1)^2(x^6+x^3+1)$	[18,10,4]
10	$(x+1)^3(x^4+x^3+x^2+x+1)$	[20,13,4]
10	$(x+1)^4(x^4+x^3+x^2+x+1)$	[20,12,4]

where $f_1(x)=x+1$, $f_2(x)=x+2$, $f_3(x)=x^2+1$. Let $C=\langle f_1^2(x)f_3(x)\rangle$ be a $(1+\lambda u)$ constacyclic code over F_3+uF_3 of length 4, where $\lambda=1$ or 2. By Theorem 2.1, we get $\mathrm{Tor}_0(C)=\langle f_1(x)f_3(x)\rangle$ and $\mathrm{Tor}_1(C)=\langle f_1(x)\rangle$, which are [4,1,4] and [4,3,2] cyclic code over F_3 respectively. According to Corollary 2.1 and Theorem 3.1, $\Phi_{(3,2)}(C)$ is a [12,4,6] linear code over F_3, which is an optimal code.

Let ω be a primitive element of F_4. Tabs. 2 and 3 present several optimal linear codes over F_4 and F_2 obtained from $(1+\lambda u)$ constacyclic codes over F_4+uF_4 and $F_2+uF_2+u^2F_2$ of some lengths respectively.

Tab. 2 Optimal linear codes over F_4 obtained from $(1+\lambda u)$ constacyclic codes over F_4+uF_4

Length of C	Generator polynomial of C	Gray image
3	$(x+1)^2(x+\omega)$	[12,3,8]
3	$(x+1)(x+\omega)^2$	[12,3,8]
3	$(x+1)^2(x+\omega^2)$	[12,3,8]
3	$(x+1)(x+\omega^2)^2$	[12,3,8]
3	$(x+\omega)^2(x+\omega^2)$	[12,3,8]
3	$(x+\omega)(x+\omega^2)^2$	[12,3,8]
5	$(x+1)^2(x^2+\omega x+1)^2(x^2+\omega^2x+1)$	[20,2,16]
5	$(x+1)^2(x^2+\omega x+1)(x^2+\omega^2x+1)^2$	[20,2,16]
5	$(x+1)(x^2+\omega x+1)^2$	[20,5,12]
5	$(x+1)(x^2+\omega^2x+1)^2$	[20,5,12]

Tab. 3 Optimal binary linear codes obtained from $(1+\lambda u)$ constacyclic codes over $F_2[u]/\langle u^3\rangle$

Length of C	Generator polynomial of C	Gray image
3	$(x+1)^2$	[12,7,4]
3	$(x^2+x+1)^2$	[12,5,4]
3	$(x+1)^2(x^2+x+1)$	[12,5,4]
3	$(x+1)^3(x^2+x+1)^2$	[12,2,8]
6	$(x+1)^3$	[24,15,4]
7	$(x+1)^2$	[28,19,4]
7	$(x+1)^3(x^3+x+1)^2$	[28,12,8]
7	$(x+1)^3(x^3+x^2+1)^2$	[28,12,8]
7	$(x^3+x+1)^2(x^3+x^2+1)^3$	[28,6,12]
7	$(x^3+x^2+1)^3(x^3+x^2+1)^2$	[28,6,12]

4 Conclusion

In this paper, we extended the result of Ref. [4] to $(1+\lambda u)$ constacyclic code of arbitrary length over $R_{(p^m,k)}$. Furthermore, some optimal linear code over F_2, F_3 and F_4 were constructed under a Gray map with the Homogeneous distance.

参考文献(References)

[1] 邓林,朱士信,韩江洪. 环 F_2+uF_2 上长为 2^s 的 $(1+u)$常循环码的距离分布[J]. 中国科技大学学报,2008,38(10):1810-1814.
Deng L, Zhu S X, Han J H. The distribution of $(1+u)$ distances of constacyclic codes of length 2^s over F_2+uF_2 [J]. Journal of University of Science and Technology of China, 2008, 38(10): 1810-1814.

[2] 施敏加,杨善林,朱士信. 环 $F_2[u]/<u^k>$上长为 2^s 的$(1+u)$常循环码的距离分布[J]. 电子与信息学报,2010,32(1):112-116.
Shi M J, Yang S L, Zhu S X. The distributions of distances of $(1+u)$ constacyclic codes of length 2^s over $F_2[u]/<u^k>$ [J]. Journal of Electronics & Information Technology, 2010, 32(1): 112-116.

[3] 刘晓娟,朱士信. 环 $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上的长为 p^s 的$(1+\lambda u)$常循环码的距离分布[J]. 中国科学技术大学学报,2012,42(11):931-935.
Liu X J, Zhu S X. The distributions of distances of $(1+\lambda u)$ constacyclic codes of length p^s over $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$[J]. Journal of University of Science and Technology of China, 2012, 42(11): 931-935.

[4] 朱士信,黄素娟. 环 $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上$(1+u)$常循环码的齐次距离分布[J]. 电子与信息学报,2013,35(11):2579-2583.
Zhu S X, Huang S J. The distribution of homogeneous distance of $(1+u)$ constacyclic codes over $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ [J]. Journal of Electronics & Information Technology, 2013, 35(11): 2579-2583.

[5] 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.

[6] Ding J, Li H J. The Gray images of -constacyclic codes over $F_{2^m}[u]/<u^k>$[EB/OL]. http://link.springer.com/article/10.1007%2Fs12190-014-0847-5.

[7] 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.

[8] Kai X S, Zhu S X, Li P. $(1+\lambda u)$ constacyclic codes over $F_p[u]/<u^k>$[J]. Journal of the Franklin Institute, 2010, 347(5): 751-762.

[9] 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.

[10] Sobhani R, Esmaeili M. Some constacyclic and cyclic codes over $F_q[u]/<u^{t+1}>$[J]. IEICE Transactions on Foundamentals of Electronics, Communications and Computer Sciences, 2010, 93 (4): 808-813.

[11] Udomkavanich P, Jitman S. On the gray image of $(1+u^m)$ cyclic codes over $F_{p^k}+uF_{p^k}+\cdots+u^mF_{p^k}$[J]. International Journal of Contemporary Mathematical Sciences, 2009, 4 (25): 1265-1272.

[12] Greferath M, Schmidt S E. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code [J]. IEEE Transactions on Information Theory, 1999, 45(7): 2522-2524.

[13] 李岩,朱士信. 环 $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ 上的一类常循环码[J]. 合肥工业大学学报,2013,35(3):408-411.
Li Y, Zhu S X. A class of constacyclic codes over the ring $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$[J]. Journal of Hefei University of Technology, 2013, 35(3): 408−411.

[14] Han M, Ye Y P, Zhu S X, et al. Cyclic codes over $R=F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$ with p^sn length [J]. Information Science, 2011, 181(4): 926-934.

[15] Sălăgean A. Repeated-root cyclic and negacyclic codes over a finite chain ring [J]. Discrete Applied Mathematics, 2005, 154(2): 413-419.