第46卷第2期 中国科学技术大学学报 Vol. 46, No. 2
2016年2月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Feb. 2016

Article ID:0253-2778(2016)02-0148-08

The minimal spanning sets of constacyclic codes over polynomial residue rings

LI Hongju[1], DING Jian[1,2]

(1. *Department of Common Course, Anhui Xinhua University, Hefei* 230088, *China*;
2. *School of Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: The minimal spanning sets and ranks of $(1+\lambda u)$ constacyclic codes with an arbitrary length $N=p^e n$ over $R=F_{p^m}[u]/\langle u^k\rangle$ were investigated, where $u^k=0$ and λ is a unit of R. Specifically, the case with $k=2$ and $\lambda=1$ was given, while a small mistake about the minimal spanning sets in [Abular T, Siap I. Constacyclic codes over F_2+uF_2. Journal of the Franklin Institute, 2009, 345: 520-529] was pointed out. Furthermore, based on the analysis of the equivalence between cyclic codes and constacyclic codes over R, the generator polynomials and minimal spanning sets of some other constacyclic codes over R were obtained. As a consequence, the generator polynomials and minimal spanning sets of $(1+\zeta u^2)$ constacyclic codes with odd length and length $N\equiv 2 \pmod 4$ over $F_{2^m}[u]/\langle u^3\rangle$ were given for any $\zeta\in F_{2^m}^*$.

Key words: constacyclic code; rank; the minimal spanning set; generator polynomial

CLC number: TN911.22 **Document code**: A doi:10.3969/j.issn.0253-2778.2016.02.00

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

Citation: Li Hongju, Ding Jian. The minimal spanning sets of constacyclic codes over polynomial residue rings [J]. Journal of University of Science and Technology of China, 2016,46(2):148-155,164.

多项式剩余类环上常循环码的极小生成元集

李红菊[1],丁 健[1,2]

(1.安徽新华学院公课部,安徽合肥 230088;2.合肥工业大学数学学院,安徽合肥 230009)

摘要:讨论了环 $R=F_{p^m}[u]/\langle u^k\rangle$ 上码长为任意长度 $N=p^e n$ 的$(1+\lambda u)$常循环码的极小生成元集和秩,其中 $u^k=0$,λ 是 R 上的单位.特别地给出了 $k=2$ 且 $\lambda=1$ 的情形,从而指出了文献[Abular T, Siap I. Constacyclic codes over F_2+uF_2. Journal of the Franklin Institute, 2009, 345: 520-529]中关于极小生成元集的一个小错误.此外,基于环 R 上循环码和常循环码的置换等价性的分析,得到了环 R 上其他一些常循环码的生成多项式和极小生成元集.特别地给出了环 $F_{2^m}[u]/\langle u^3\rangle$ 上码长 N 为奇数和码长 $N\equiv 2 \pmod 4$ 时$(1+\zeta u^2)$常循环码的生成多项式和极小生成元集,其中 $\zeta\in F_{2^m}^*$.

关键词:常循环码;秩;极小生成元集;生成多项式

Received:2015-07-13;**Revised**:2016-02-25

Foundation item: Supported by Anhui Province Natural Science Research (KJ2015A308, KJ2016A307), Anhui Province Colleges Outstanding Young Talents Program (gxyqZD2016389), Natural Science Project of AnHui Xinhua University (2014Zr009).

Biography: LI Hongju, female, born in 1982, lecturer. Research field: algebraic coding. E-mail: zhenxidj.happy@163.com

Corresponding author: DING Jian, master/associate professor. E-mail: dingjian_happy@163.com

0 Introduction

In 2006, $(1+u)$ constacyclic codes over F_2+uF_2 were first introduced by Qian et al in Ref. [2], where it was proved that the Gray image of a linear simple-root $(1+u)$ constacyclic code over F_2+uF_2 is a binary distance invariant linear cyclic code. From then on, codes over this family of rings have been a topic of study. Abular et al[3] discussed the minimal spanning sets of repeated-root cyclic codes over F_2+uF_2 and $F_2+uF_2+u^2F_2$, and it was extended to $F_q[u]/\langle u^k\rangle$ by Al-Ashke et al[4] where $q=p^m$ for prime number p and positive integer m. Shi et al[5] determined the minimal spanning sets of $(1+u)$ constacyclic codes with length 2^e over F_2+uF_2, which was extended to constacyclic codes of arbitrary length over F_2+uF_2 by Abular et al[1]. Zhu et al[6] studied the minimal spanning sets of simple-root cyclic and negacyclic codes over $F_q[u]/\langle u^k\rangle$. Shi et al[7] determined the structure and minimal generating sets of simple-root α constacyclic codes over $F_q[u]/\langle u^k\rangle$, which are based on the factorization of $(x^N-\alpha)$ in $F_q[u]/\langle u^k\rangle$. Kai et al[8] determined the structure and generator polynomials of repeated-root $(1+\lambda u)$ constacyclic codes over $F_p[u]/\langle u^k\rangle$, which was extended to $F_q[u]/\langle u^k\rangle$ by Li et al[9].

The sturctures of simple-root constacyclic codes and repeated-root $(1+\lambda u)$ constacyclic codes over $F_q[u]/\langle u^k\rangle$ have been determined, but the structures of other repeated-root constacyclic codes aren't clear. Besides, the minimal spanning sets of simple-root α constacyclic codes over $F_q[u]/\langle u^k\rangle$ in Ref. [7] are based on the factorization of $(x^N-\alpha)$ in $F_q[u]/\langle u^k\rangle$, which is not conducive to decoding and determining the distance distribution of constacyclic codes. In this paper, we determine the minimal spanning sets of $(1+\lambda u)$ constacyclic codes with an arbitrary length $N=p^en$ over R, as well as $\alpha_0^{p^m-t_0-1}(1+\lambda u)\alpha^\delta$ constacyclic codes and $\alpha_0^{p^m-t_0-1}\alpha^\delta$ constacyclic codes with length $N\equiv(p^t-\delta)\bmod p^t$ over R, where $p^{t-1}+1\leqslant k\leqslant p^t$ and $0\leqslant\delta\leqslant p^t-1$ for non-negative integer t. As a consequence, the generator polynomials and minimal spanning sets of $(1+\zeta u^2)$ constacyclic codes with odd length and length $N\equiv 2\pmod 4$ over $F_{2^m}[u]/\langle u^3\rangle$ are determined for any $\zeta\in F_{2^m}^*$.

1 Preliminaries

Let R denote the polynomial residue ring $F_{p^m}[u]/\langle u^k\rangle$ for positive prime number p and positive integer $k\geqslant 2$. 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 from over F_{p^m}. Let C be a code of length $N=p^en$ over R, where e is a non-negative integer. For some fixed unit α of R, the α constacyclic shift V_α on R^N is the shift $V_\alpha(c_0,c_1,\cdots,c_{N-1})=(\alpha c_{N-1},c_0,c_1,\cdots,c_{N-2})$. The code C is said to be an α constacyclic code if $V_\alpha(C)=C$. 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 $R[x]/\langle x^N-\alpha\rangle$. Thus α constacyclic codes of length N over R can be identified as ideals in $R[x]/\langle x^N-\alpha\rangle$. The number of elements in a minimal spanning set of a constacyclic code C is defined as the rank of C, which is denoted by rank(C).

2 $(1+\lambda u)$ constacyclic codes of arbitrary length over R

Let λ be a unit of R, then the following lemma is straightforward from Theorem 4 and Lemma 3 of Ref. [9].

Lemma 2.1 Let C be a $(1+\lambda u)$ constacyclic code of length $N=p^en$ over R, then

$$C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle,$$

where non-negative integer $0\leqslant k_i\leqslant kp^e$ for $1\leqslant i\leqslant j$. Furthermore, $|C|=p^{m(kN-\varepsilon)}$, where $\varepsilon=\sum_{i=1}^{j}k_i\deg(f_i)$.

In $R[x]/\langle x^N-(1+\lambda u)\rangle$, if $\max\{k_1,k_2,\cdots,$

$k_j\}=0$, then $C=\langle 1\rangle$.

If $\min\{k_1,k_2,\cdots,k_j\}=kp^e$, then $C=\langle(x^N-1)^k\rangle=\langle(\lambda u)^k\rangle=\langle 0\rangle$.

If $\max\{k_1,k_2,\cdots,k_j\}=\min\{k_1,k_2,\cdots,k_j\}=sp^e$ for $1\leqslant s\leqslant k-1$, then $C=\langle(x^N-1)^s\rangle=\langle(\lambda u)^s\rangle=\langle u^s\rangle$.

Suppose $\min\{k_1,k_2,\cdots,k_j\}<p^e$ and $\max\{k_1,k_2,\cdots,k_j\}\neq 0$. If $k_1\leqslant p^e$, then we put $f_1^{k_1}$ as a factor of polynomial G_1. If $sp^e<k_1\leqslant(s+1)p^e$ for $1\leqslant s\leqslant k-1$, then we put $f_1^{p^e}$ and $f_1^{k_1-sp^e}$ as a factor of polynomials G_l for $1\leqslant l\leqslant s$ and G_{s+1} respectively. By the analysis of k_i for $1\leqslant i\leqslant j$, we get $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=G_1G_2\cdots G_t$, where G_ω is a monic polynomial over F_{p^m} and $1\leqslant\deg(G_\omega)\leqslant N-1$ for $1\leqslant\omega\leqslant t$. Furthermore, $G_t\mid G_{t-1}\mid\cdots\mid G_2\mid G_1\mid(x^N-1)$. So $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}$, where H_w is a monic polynomial over F_{p^m} and $1\leqslant l_w\leqslant k$ for $1\leqslant w\leqslant i$. Besides, $l_1+l_2+\cdots+l_i\leqslant k$ and $H_i\mid H_{i-1}\mid\cdots\mid H_2\mid H_1\mid(x^N-1)$. If we let $\deg(H_w)=d_w$, then $1\leqslant d_i<d_{i-1}<\cdots<d_2<d_1<N$.

Suppose $sp^e\leqslant\min\{k_1,k_2,\cdots,k_j\}<(s+1)p^e$ and $\max\{k_1,k_2,\cdots,k_j\}\neq sp^e$ for $1\leqslant s\leqslant k-1$. By the ananysis of k_i for $1\leqslant i\leqslant j$, we get $f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}=(x^N-1)^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}$, where H_w is a monic polynomial over F_{p^m} and $1\leqslant l_w\leqslant k-s$ for $1\leqslant w\leqslant i$. Besides, $l_1+l_2+\cdots+l_i\leqslant k-s$ and $H_i\mid H_{i-1}\mid\cdots\mid H_2\mid H_1\mid(x^N-1)$. If we let $\deg(H_w)=d_w$, then $1\leqslant d_i<d_{i-1}<\cdots<d_2<d_1<N$.

From the construction of H_w for $1\leqslant w\leqslant i$ and the above discussion, we have the following lemma and theorem.

Lemma 2.2 In $F_{p^m}[x]$, we have the following results:

(Ⅰ) $\gcd\left(\frac{x^N-1}{H_1},H_1^{l_1-1}\right)=1$.

(Ⅱ) $\gcd\left(\frac{x^N-1}{H_1},H_l\right)=1$ for $2\leqslant l\leqslant i$ and $\gcd\left(\frac{H_w}{H_{w+1}},H_{w+1}^{l_{w+1}-1}\right)=1$ for $1\leqslant w\leqslant i-1$.

(Ⅲ) $\gcd\left(\frac{H_w}{H_{w+1}},H_l\right)=1$ for $1\leqslant w<l-1\leqslant i-1$.

Theorem 2.3 Let $C=\langle f_1^{k_1}f_2^{k_2}\cdots f_j^{k_j}\rangle$ be any $(1+\lambda u)$ constacyclic codes over R of length $N=p^en$ and $\gcd(n,p)=1$. Then, C has one of the following forms:

① $C=\langle 0\rangle$. Or,

② $C=\langle 1\rangle$. Or,

③ $C=\langle(x^N-1)^s\rangle=\langle u^s\rangle$ where $1\leqslant s\leqslant k-1$. Or,

④ $C=\langle H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle$, where $H_i\mid H_{i-1}\mid\cdots\mid H_2\mid H_1\mid(x^N-1)$ over F_{p^m} and $1\leqslant l_w\leqslant k$ for $1\leqslant w\leqslant i\leqslant k$. Furthermore, $l_1+l_2+\cdots+l_i\leqslant k$ and $1\leqslant d_i<d_{i-1}<\cdots<d_2<d_1<N$ where $\deg(H_w)=d_w$ for $1\leqslant w\leqslant i$. Or,

⑤ $C=\langle(x^N-1)^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle=\langle u^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle$, where $H_i\mid H_{i-1}\mid\cdots\mid H_2\mid H_1\mid(x^N-1)$ and $1\leqslant l_w\leqslant k-s<k$ for $1\leqslant w\leqslant i\leqslant k-s$. Furthermore, $l_1+l_2+\cdots+l_i\leqslant k-s$ and $1\leqslant d_i<d_{i-1}<\cdots<d_2<d_1<N$ where $d_w=\deg(H_w)$ for $1\leqslant w\leqslant i$.

Definition 2.4 Let b be a non-negative integer and $a_{l(b-1)r}\in F_{p^m}$. If $0\leqslant b<l_1$, then

$$g_b(x)=H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\sum_{r=0}^{N-d_1-1}a_{0br}x^r.$$

If $l_1+l_2\cdots+l_t\leqslant b<l_1+l_2\cdots+l_{t+1}$ for $1\leqslant t\leqslant i-1$, then

$$g_b(x)=H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\sum_{r=0}^{N-d_1-1}a_{0br}x^r+H_2^{l_2}\cdots H_i^{l_i}\sum_{r=0}^{d_1-d_2-1}a_{l_1(b-l_1)r}x^r+\cdots+H_{t+1}^{l_{t+1}}\cdots H_i^{l_i}\sum_{r=0}^{d_t-d_{t+1}-1}a_{(l_1+l_2\cdots+l_t)(b-l_1-\cdots-l_t)r}x^r.$$

If $l_1+l_2\cdots+l_i\leqslant b<k$, then

$$g_b(x)=H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\sum_{r=0}^{N-d_1-1}a_{0br}x^r+H_2^{l_2}\cdots H_i^{l_i}\sum_{r=0}^{d_1-d_2-1}a_{l_1(b-l_1)r}x^r+\cdots+H_i^{l_i}\sum_{r=0}^{d_{i-1}-d_i-1}a_{(l_1+l_2\cdots+l_{i-1})(b-l_1-\cdots-l_{i-1})r}x^r+\sum_{r=0}^{d_i-1}a_{(l_1+l_2\cdots+l_i)(b-l_1-\cdots-l_i)r}x^r.$$

Lemma 2.5 In $R[x]/\langle x^N-(1+\lambda u)\rangle$, if $u\mid g_b(x)$, then $a_{l(b-1)r}=0$.

Proof In $R[x]/\langle x^N-(1+\lambda u)\rangle$, $x^N-(1+\lambda u)=0$, so $u=\lambda^{-1}(x^N-1)$. Thus, $H_i\mid H_{i-1}\mid\cdots\mid$

$H_2 \mid H_1 \mid (x^N-1) \mid u$.

If $0 \leqslant b < l_1$, then

$$u \mid H_1^{l_1} H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{N-d_1-1} a_{0br} x^r,$$

which implies

$$\frac{x^N-1}{H_1} \Big| H_1^{l_1-1} H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{N-d_1-1} a_{0br} x^r.$$

By Lemma 2.2, we have

$$\frac{x^N-1}{H_1} \Big| \sum_{r=0}^{N-d_1-1} a_{0br} x^r.$$

Since

$$N-d_1-1 < N-d_1 = \deg\left(\frac{x^N-1}{H_1}\right) < N,$$

then $a_{0br}=0$ for $0 \leqslant b < l_1$.

If $l_1+l_2\cdots+l_t \leqslant b < l_1+l_2\cdots+l_{t+1}$ for $1 \leqslant t < i-1$, then

$$u \mid [H_1^{l_1} H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{N-d_1-1} a_{0br} x^r + H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{d_1-d_2-1} a_{l_1(b-l_1)r} x^r + \cdots + H_{t+1}^{l_{t+1}} \cdots H_i^{l_i} \sum_{r=0}^{d_t-d_{t+1}-1} a_{(l_1+l_2+\cdots+l_t)(b-l_1-\cdots-l_t)r} x^r].$$

Since $H_t \mid u$, then

$$H_t \mid H_{t+1}^{l_{t+1}} \cdots H_i^{l_i} \sum_{r=0}^{d_t-d_{t+1}-1} a_{(l_1+l_2+\cdots+l_t)(b-l_1-\cdots-l_t)r} x^r$$

which implies

$$\frac{H_t}{H_{t+1}} \Big| H_{t+1}^{l_{t+1}} \cdots H_i^{l_i} \sum_{r=0}^{d_t-d_{t+1}-1} a_{(l_1+l_2+\cdots+l_t)(b-l_1-\cdots-l_t)r} x^r.$$

By Lemma 2.2, we have

$$\frac{H_t}{H_{t+1}} \Big| \sum_{r=0}^{d_t-d_{t+1}-1} a_{(l_1+l_2+\cdots+l_t)(b-l_1-\cdots-l_t)r} x^r.$$

Since

$$d_t-d_{t+1}-1 < d_t-d_{t+1} = \deg\left(\frac{H_t}{H_{t+1}}\right) < N,$$

then $a_{(l_1+l_2+\cdots+l_t)(b-l_1-\cdots-l_t)r}=0$ where $l_1+l_2\cdots+l_t \leqslant b < l_1+l_2\cdots+l_{t+1}$ for $1 \leqslant t < i-1$. Thus,

$$u \mid [H_1^{l_1} H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{N-d_1-1} a_{0br} x^r + H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{d_1-d_2-1} a_{l_1(b-l_1)r} x^r + H_t^{l_t} \cdots H_i^{l_i} \sum_{r=0}^{d_{t-1}-d_t-1} a_{(l_1+l_2+\cdots+l_{t-1})(b-l_1-\cdots-l_{t-1})r} x^r].$$

Similarly, we can get

$$a_{0br} = a_{l_1(b-l_1)r} = \cdots = a_{(l_1+l_2+\cdots+l_t)(b-l_1-\cdots-l_t)r} = 0$$

where $l_1+l_2\cdots+l_t \leqslant b < l_1+l_2\cdots+l_{t+1}$ for $1 \leqslant t < i-1$.

If $l_1+l_2\cdots+l_i \leqslant b < k$, then

$$u \mid [H_1^{l_1} H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{N-d_1-1} a_{0br} x^r + H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{d_1-d_2-1} a_{l_1(b-l_1)r} x^r + \cdots + H_i^{l_i} \sum_{r=0}^{d_{i-1}-d_i-1} a_{(l_1+l_2+\cdots+l_{i-1})(b-l_1-\cdots-l_{i-1})r} x^r + \sum_{r=0}^{d_i-1} a_{(l_1+l_2+\cdots+l_i)(b-l_1-\cdots-l_i)r} x^r].$$

Since $H_i \mid u$, then

$$H_i \mid \sum_{r=0}^{d_i-1} a_{(l_1+l_2+\cdots+l_i)(b-l_1-\cdots-l_i)r} x^r.$$

Since $d_i - 1 < d_i = \deg(H_i) < N$, then $a_{(l_1+l_2+\cdots+l_i)(b-l_1-\cdots-l_i)r}=0$ where $l_1+l_2+\cdots+l_i \leqslant b \leqslant k-1$. Thus,

$$u \mid [H_1^{l_1} H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{N-d_1-1} a_{0br} x^r + H_2^{l_2} \cdots H_i^{l_i} \sum_{r=0}^{d_1-d_2-1} a_{l_1(b-l_1)r} x^r + \cdots + H_i^{l_i} \sum_{r=0}^{d_{i-1}-d_i-1} a_{(l_1+l_2+\cdots+l_{i-1})(b-l_1-\cdots-l_{i-1})r} x^r].$$

Similarly, we can get $a_{0br} = a_{l_1(b-l_1)r} = \cdots = a_{(l_1+l_2+\cdots+l_i)(b-l_1-\cdots-l_i)r}=0$ where $l_1+l_2+\cdots+l_i \leqslant b \leqslant k-1$. This gives the proof. □

Theorem 2.6　Let C be any $(1+\lambda u)$ constacyclic codes over $N=p^e n$ of length $N=p^e n$ and $\gcd(n,p)=1$, the constraints on the generator polynomials is the same as in Theorem 2.3.

(Ⅰ) If $C=\langle 1\rangle$, then $\mathrm{rank}(C)=N$ and C has a minimal spanning set over R given by $\chi_1=\{1, x, \cdots, x^{N-1}\}$.

(Ⅱ) If $C=\langle u^s\rangle$ where $1 \leqslant s \leqslant k-1$, then $\mathrm{rank}(C)=N$ and C has a minimal spanning set over R given by $\chi_2=\{u^s, u^s x, \cdots, u^s x^{N-1}\}$.

(Ⅲ) Let $C=\langle H_1^{l_1} H_2^{l_2} \cdots H_i^{l_i}\rangle$. If $l_1+l_2+\cdots+l_i \leqslant k-1$, then $\mathrm{rank}(C)=N$ and C has a minimal spanning set over R given by

$$\chi_3 = \{H_1^{l_1} H_2^{l_2} \cdots H_i^{l_i}, xH_1^{l_1} H_2^{l_2} \cdots H_i^{l_i}, \cdots,$$

$x^{N-d_1-1}H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}, u^{l_1}H_2^{l_2}\cdots H_i^{l_i},$
$xu^{l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,x^{d_1-d_2-1}u^{l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,$
$u^{l_1+l_2+\cdots+l_{i-1}}H_i^{l_i}, xu^{l_1+l_2+\cdots+l_{i-1}}H_i^{l_i},\cdots,$
$x^{d_{i-1}-d_i-1}u^{l_1+l_2+\cdots+l_{i-1}}H_i^{l_i},$
$u^{l_1+l_2+\cdots+l_i}, xu^{l_1+l_2+\cdots+l_i},\cdots,x^{d_i-1}u^{l_1+l_2+\cdots+l_i}\}.$

If $l_1+l_2+\cdots+l_i=k$, then rank(C)=N−d_i and C has a minimal spanning set over R given by

$\chi_4=\{H^{l_1}H_2^{l_2}\cdots H_i^{l_i}, xH^{l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,$
$x^{N-d_1-1}H^{l_1}H_2^{l_2}\cdots H_i^{l_i}, u^{l_1}H_2^{l_2}\cdots$
$H_i^{l_i}, xu^{l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,x^{d_1-d_2-1}u^{l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,$
$u^{l_1+l_2+\cdots+l_{i-1}}H_i^{l_i}, xu^{l_1+l_2+\cdots+l_{i-1}}H_i^{l_i},\cdots,$
$x^{d_{i-1}-d_i-1}u^{l_1+l_2+\cdots+l_{i-1}}H_i^{l_i}\}.$

(Ⅳ) Let C=$\langle u^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle$. If $l_1+l_2+\cdots+l_i\leqslant k-s-1$, then rank(C)=N and C has a minimal spanning set over R given by

$\chi_5=\{u^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}, xu^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,$
$x^{N-d_1-1}u^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}, u^{s+l_1}H_2^{l_2}\cdots H_i^{l_i},$
$xu^{s+l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,x^{d_1-d_2-1}u^{s+l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,$
$u^{s+l_1+l_2+\cdots+l_{i-1}}H_i^{l_i}, xu^{s+l_1+l_2+\cdots+l_{i-1}}H_i^{l_i},\cdots,$
$x^{d_{i-1}-d_i-1}u^{s+l_1+l_2+\cdots+l_{i-1}}H_i^{l_i},$
$u^{s+l_1+l_2+\cdots+l_i}, xu^{s+l_1+l_2+\cdots+l_i},\cdots,x^{d_i-1}u^{s+l_1+l_2+\cdots+l_i}\}.$

If $l_1+l_2+\cdots+l_i=k-s$, then rank(C)=N−d_i and C has a minimal spanning set over R given by

$\chi_6=\{u^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}, xu^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,$
$x^{N-d_1-1}u^sH_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}, u^{s+l_1}H_2^{l_2}\cdots H_i^{l_i},$
$xu^{s+l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,x^{d_1-d_2-1}u^{s+l_1}H_2^{l_2}\cdots H_i^{l_i},\cdots,$
$u^{s+l_1+l_2+\cdots+l_{i-1}}H_i^{l_i}, xu^{s+l_1+l_2+\cdots+l_{i-1}}H_i^{l_i},\cdots,$
$x^{d_{i-1}-d_i-1}u^{s+l_1+l_2+\cdots+l_{i-1}}H_i^{l_i}\}.$

Proof (Ⅰ) Suppose

$$\sum_{b=0}^{k-1}a_{0b}u^b+x\sum_{b=0}^{k-1}a_{1b}u^b+\cdots+x^{N-1}\sum_{b=0}^{k-1}a_{(N-1)b}u^b=0,$$

where $a_{rb}\in F_{p^m}$ for $0\leqslant r\leqslant N-1$ and $0\leqslant b\leqslant k-1$, then

$$\sum_{r=0}^{N-1}a_{r0}x^r+u\sum_{r=0}^{N-1}a_{r1}x^r+\cdots+u^{k-1}\sum_{r=0}^{N-1}a_{r(k-1)}x^r=0.$$

Thus, $u\mid\sum_{r=0}^{N-1}a_{r0}x^r$ which implies $(x^N-1)\mid\sum_{r=0}^{N-1}a_{r0}x^r$. So $a_{r0}=0$ for $0\leqslant r\leqslant N-1$.

Similarly, we can get $a_{rb}=0$ for $0\leqslant r\leqslant N-1$ and $0\leqslant b\leqslant k-1$. This implies that the χ_1 can linearly compose p^{kmN} different codewords over R, while the number is the same as |C| from Lemma 2.1 and the codewords from linear composition are all in C=$\langle 1\rangle$. Thus, C=$\langle 1\rangle$ has a minimal spanning set over R given by $\chi_1=\{1,x,\cdots,x^{N-1}\}$.

(Ⅱ) The proof is similar to Theorem 2.6 (Ⅰ).

(Ⅲ) Let C=$\langle H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle$. If $l_1+l_2+\cdots+l_i\leqslant k-1$, we suppose that there exist $a_{l(b-l)r}\in F_{p^m}$ such that

$$H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\sum_{r=0}^{N-d_1-1}\sum_{b=0}^{k-1}a_{0br}u^bx^r+u^{l_1}H_2^{l_2}\cdots H_i^{l_i}\sum_{r=0}^{d_1-d_2-1}\sum_{b=l_1}^{k-1}a_{l_1(b-l_1)r}u^{b-l_1}x^r+\cdots+$$
$$u^{l_1+l_2+\cdots+l_{i-1}}H_i^{l_i}\sum_{r=0}^{d_{i-1}-d_i-1}\sum_{b=l_1+l_2+\cdots+l_{i-1}}^{k-1}a_{(l_1+l_2+\cdots+l_{i-1})[b-(l_1+l_2+\cdots+l_{i-1})]r}u^{b-(l_1+l_2+\cdots+l_{i-1})}x^r+$$
$$u^{l_1+l_2+\cdots+l_i}\sum_{r=0}^{d_i-1}\sum_{b=l_1+l_2+\cdots+l_i}^{k-1}a_{(l_1+l_2+\cdots+l_i)[b-(l_1+l_2+\cdots+l_i)]r}u^{b-(l_1+l_2+\cdots+l_i)}x^r=0,$$

which implies $\sum_{b=0}^{k-1}u^bg_b(x)=0$. Thus, we have $g_0(x)=-\sum_{b=1}^{k-1}u^bg_b(x)$. This shows that $u\mid g_0(x)$. By Lemma 2.5, $g_0(x)=0=\sum_{b=1}^{k-1}u^bg_b(x)$. Similarly, we can get $u\mid g_b(x)$ for $0\leqslant b\leqslant k-1$. According to Lemma 2.5, $a_{l(b-l)r}=0$. This implies that χ_3 can linearly compose

$$p^{mk(N-d_1)}p^{m(k-l_1)(d_1-d_2)}\cdots p^{m[k-(l_1+l_2+\cdots+l_{i-1})](d_{i-1}-d_i)}\cdot p^{m[k-(l_1+l_2+\cdots+l_i)]d_i}=p^{m[kN-(l_1d_1+l_2d_2+\cdots+l_id_i)]}$$

different codewords over R, while the number is the same as |C| from Lemma 2.1 and the codewords from linear composition are all in C=$\langle H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle$. Thus, C=$\langle H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle$ has a

minimal spanning set over R given by χ_3.

Similarly, if $l_1+l_2+\cdots+l_i=k$, then $C=\langle H_1^{l_1}H_2^{l_2}\cdots H_i^{l_i}\rangle$ has a minimal spanning set over R given by χ_4.

(Ⅳ) The proof is similar to Theorem 2.6 (Ⅲ). □

Let $p=2$, $m=1$, $\lambda=1$, $k=2$ in Theorems 2.3 and 2.6, we have the following corollary.

Corollary 2.7 Let C be any $(1+u)$ constacyclic codes over F_2+uF_2 of length $N=2^e n$ and $\gcd(2,n)=1$, then C has one of the following forms:

① $C=\langle 0\rangle$. Or,

② $C=\langle 1\rangle$ and $\mathrm{rank}(C)=N$. One of its minimal spanning sets over F_2+uF_2 is $\pi_1=\{1,x,\cdots,x^{N-1}\}$. Or,

③ $C=\langle u\rangle$ and $\mathrm{rank}(C)=N$. One of its minimal spanning sets over F_2+uF_2 is $\pi_2=\{u,ux,\cdots,ux^{N-1}\}$. Or,

④ $C=\langle H_1\rangle$, where $H_1\mid(x^N-1)$ over F_2 and $\deg(H_1)=d_1<N$. Then, $\mathrm{rank}(C)=N$ and C has a minimal spanning set over F_2+uF_2 given by $\pi_3=\{H_1,xH_1,\cdots,x^{N-d_1-1}H_1,u,ux,\cdots,ux^{d_1-1}\}$. Or,

⑤ $C=\langle H_1^2\rangle$, where $H_1\mid(x^N-1)$ over F_2 and $\deg(H_1)=d_1<N$. Then, $\mathrm{rank}(C)=N-d$ and C has a minimal spanning set over F_2+uF_2 given by $\pi_4=\{H_1^2,xH_1^2,\cdots,x^{N-d_1-1}H_1^2\}$. Or,

⑥ $C=\langle H_1H_2\rangle$, where $H_2\mid H_1\mid(x^N-1)$ over F_2. Let $\deg(H_w)=d_w$ for $w=1,2$, then $d_2<d_1<N$. So, $\mathrm{rank}(C)=N-d_2$ and C has a minimal spanning set over F_2+uF_2 given by $\pi_5=\{H_1H_2,xH_1H_2,\cdots,x^{N-d_1-1}H_1H_2,uH_2,uxH_2,\cdots,ux^{d_1-d_2-1}H_2\}$. Or,

⑦ $C=\langle uH_1\rangle$, where $H_1\mid(x^N-1)$ over F_2 and $\deg(H_1)=d_1<N$. Then, $\mathrm{rank}(C)=N-d_1$ and C has a minimal spanning set over F_2+uF_2 given by $\pi_7=\{uH_1,uxH_1,\cdots,ux^{N-d_1-1}H_1\}$.

Note The results of Abular and Siap in Ref. [1] about minimal spanning sets contain Corollary 2.7 ③, ④, ⑥ and ⑦, but Corollary 2.7 ② and ⑤ were not discussed.

3 Some other constacyclic codes over R

In the following, let $\alpha=\alpha_0+u\alpha_1$ for $\alpha_0\in F_{p^m}^*$ and $\alpha_1\in R$. Suppose $p^{t-1}+1\leqslant k\leqslant p^t$ and $p^t(l-1)+1\leqslant N\leqslant p^t l$ for non-negative integer t and l. Let $p^t l\equiv t_0 \bmod(p^m-1)$.

Theorem 3.1 A $(1+\lambda u)$ constacyclic code of length $N=p^t l-\delta$ over R is equivalent to an η_δ constacyclic code of length N over R, where $0\leqslant\delta\leqslant p^t-1$ and $\eta_\delta=\alpha_0^{p^m-t_0-1}(1+\lambda u)\alpha^\delta$.

Proof Let φ be the map

$$\varphi: R[x]/\langle x^N-(1+\lambda u)\rangle \to R[x]/\langle x^N-\eta_\delta\rangle,$$
$$r(x)\to r(\alpha x).$$

For any polynomials $r_1(x), r_2(x)\in R[x]$,

$$r_1(x)\equiv r_2(x)\bmod(x^N-(1+\lambda u))$$
$$\Leftrightarrow \text{There exists a polynomial } I(x)\in R[x] \text{ such that } r_1(x)-r_2(x)=I(x)[x^N-(1+\lambda u)]$$
$$\Leftrightarrow r_1(\alpha x)-r_2(\alpha x)=I(\alpha x)[\alpha^N x^N-(1+\lambda u)]$$
$$\Leftrightarrow r_1(\alpha x)-r_2(\alpha x)=\alpha^N I(\alpha x)\left(x^N-\frac{1+\lambda u}{\alpha^N}\right)$$
$$\Leftrightarrow r_1(\alpha x)-r_2(\alpha x)=\alpha^N I(\alpha x)\left[x^N-\frac{(1+\lambda u)\alpha^\delta}{\alpha_0^{t_0}}\right]$$
$$\Leftrightarrow r_1(\alpha x)-r_2(\alpha x)=\alpha^N I(\alpha x)(x^N-\eta_\delta)$$
$$\Leftrightarrow r_1(\alpha x)\equiv r_2(\alpha x)\bmod(x^N-\eta_\delta).$$

Therefore, φ is a one-to-one map. On the other hand,

$$\varphi(r_1(x)+r_2(x))=r_1(\alpha x)+r_2(\alpha x)=\varphi(r_1(x))+\varphi(r_2(x)),$$
$$\varphi(r_1(x)r_2(x))=r_1(\alpha x)r_2(\alpha x)=\varphi(r_1(x))\varphi(r_2(x)).$$

Thus φ is a ring isomorphism and this gives the proof. □

Corollary 3.2 A $(1+u)$ constacyclic code of length $N=4l-1$ over $F_{2^m}[u]/\langle u^3\rangle$ is equivalent to a $(1+\zeta u^2)$ constacyclic code of length $N=4l-1$ over $F_{2^m}[u]/\langle u^3\rangle$, where l is a non-negative integer and $\zeta\in F_{2^m}^*$.

Proof Let $\lambda=1$, $\delta=1$ and $\alpha=1+u[1+(\zeta+1)u]$ in Theorem 3.1, then

$$\eta_1=(1+u)[1+u+(\zeta+1)u^2]=1+\zeta u^2.$$

This gives the proof. □

From Theorems 2.3 and 2.6, Corollary 3.2, and Lemma 2.1, we get the following theorem.

Theorem 3.3 Let C be a $(1+\zeta u^2)$ constacyclic code of length $N=4l-1$ over $F_{2^m}[u]/\langle u^3\rangle$, where l is a non-negative integer and $\zeta\in$

$F_{2^m}^*$. Then

$$C=\langle f_1^{k_1}(\theta_1 x) f_2^{k_2}(\theta_1 x)\cdots f_j^{k_j}(\theta_1 x)\rangle,$$

where non-negative integer $0\leqslant k_i\leqslant 3$ for $1\leqslant i\leqslant j$ and $\theta_1=1+u+(\zeta+1)u^2$. Furthermore, $|C|=2^{m(3N-\varepsilon)}$, where

$$\varepsilon=\sum_{i=1}^{j} k_i\deg(f_i).$$

So C has one of the following forms:

① $C=\langle 0\rangle$. Or,

② If $C=\langle 1\rangle$, then $\mathrm{rank}(C)=N$ and C has a minimal spanning set over $F_{2^m}[u]/\langle u^3\rangle$ given by $\beta_1=\{1,x,\cdots,x^{N-1}\}$. Or,

③ If $C=\langle u^s\rangle$ where $1\leqslant s\leqslant 2$, then $\mathrm{rank}(C)=N$ and C has a minimal spanning set over $F_{2^m}[u]/\langle u^3\rangle$ given by $\beta_2=\{u^s,u^s x,\cdots,u^s x^{N-1}\}$.

④ $C=\langle H_1^{l_1}(\theta_1 x)\ H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x)\rangle$, where $H_i|H_{i-1}|\cdots|H_1|(x^N-1)$ over F_{2^m} and $1\leqslant l_w\leqslant 3$ for $1\leqslant w\leqslant i\leqslant 3$. Furthermore, $l_1+l_2+\cdots+l_i\leqslant 3$ and $1\leqslant d_i<d_{i-1}<\cdots<d_1<N$ where $\deg(H_w)=d_w$ for $1\leqslant w\leqslant i$. If $l_1+l_2+\cdots+l_i\leqslant 2$, then $\mathrm{rank}(C)=N$ and C has a minimal spanning set over $F_{2^m}[u]/\langle u^3\rangle$ given by

$$\begin{aligned}\beta_3=\{&H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &xH_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{N-d_1-1}H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &uH_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &xuH_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{d_1-d_2-1}uH_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &u^{l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),xu^{l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{d_{i-1}-d_i-1}u^{l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),u^{l_1+\cdots+l_i},\\ &xu^{l_1+\cdots+l_i},\cdots,x^{d_i-1}u^{l_1+\cdots+l_i}\}.\end{aligned}$$

If $l_1+\cdots+l_i=3$, then $\mathrm{rank}(C)=N-d_i$ and C has a minimal spanning set over $F_{2^m}[u]/\langle u^3\rangle$ given by

$$\begin{aligned}\beta_4=\{&H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &xH_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{N-d_1-1}H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &uH_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &xuH_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{d_1-d_2-1}uH_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &u^{l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),xu^{l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{d_{i-1}-d_i-1}u^{l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x)\}.\end{aligned}$$

Or,

⑤ $C=\langle u^s H_1^{l_1}(\theta_1 x)\ H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x)\rangle$, where $H_i|H_{i-1}|\cdots|H_1|(x^N-1)$ and $1\leqslant l_w\leqslant 3-s<3$ for $1\leqslant w\leqslant i\leqslant 3-s$. Furthermore, $l_1+\cdots+l_i\leqslant 3-s$ and $1\leqslant d_i<d_{i-1}<\cdots<d_1<N$ where $d_w=\deg(H_w)$ for $1\leqslant w\leqslant i$. If $l_1+\cdots+l_i\leqslant 2-s$, then $\mathrm{rank}(C)=N$ and C has a minimal spanning set over $F_{2^m}[u]/\langle u^3\rangle$ given by

$$\begin{aligned}\beta_5=\{&u^s H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &xu^s H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{N-d_1-1}u^s H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &u^{s+l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),xu^{s+l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{d_{i-1}-d_i-1}u^{s+l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),u^{s+l_1+\cdots+l_i},\\ &xu^{s+l_1+\cdots+l_i},\cdots,x^{d_i-1}u^{s+l_1+\cdots+l_i}\}.\end{aligned}$$

If $l_1+l_2+\cdots+l_i=3-s$, then $\mathrm{rank}(C)=N-d_i$ and C has a minimal spanning set over $F_{2^m}[u]/\langle u^3\rangle$ given by

$$\begin{aligned}\beta_6=\{&u^s H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\\ &xu^s H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{N-d_1-1}u^s H_1^{l_1}(\theta_1 x)H_2^{l_2}(\theta_1 x)\cdots H_i^{l_i}(\theta_1 x),\cdots,\\ &u^{s+l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),xu^{s+l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x),\cdots,\\ &x^{d_{i-1}-d_i-1}u^{s+l_1+\cdots+l_{i-1}}H_i^{l_i}(\theta_1 x)\}.\end{aligned}$$

Corollary 3.4 A $(1+u)$ constacyclic code of length $N=4l-3$ over $F_{2^m}[u]/\langle u^3\rangle$ is equivalent to a $(1+\zeta u^2)$ constacyclic code of length $N=4l-3$ over $F_{2^m}[u]/\langle u^3\rangle$, where l is a non-negative integer and $\zeta\in F_{2^m}^*$.

Proof Let $\lambda=1$, $\delta=3$ and $\alpha=1+u(1+\zeta u)$ in Theorem 3.1, then $\eta_\beta=(1+u)(1+u+\zeta u^2)^3=1+\zeta u^2$. This gives the proof. □

According to Corollary 3.3, we replace the θ_1 in Theorem 3.3 by $\theta_2=1+u(1+\zeta u)$, and get the generator polynomial and minimal spanning sets of a $(1+\zeta u^2)$ constacyclic code of length $N=4l-3$ over $F_{2^m}[u]/\langle u^3\rangle$, where l is a non-negative integer and $\zeta\in F_{2^m}^*$.

Theorem 3.5 A cyclic code of length $N=p^t l-\delta$ over R is equivalent to a τ_δ constacyclic code

of length N over R, where $0 \leqslant \delta \leqslant p^t - 1$ and $\tau_\delta = \alpha_0^{p^m - t_0 - 1} \alpha^\delta$.

Proof Let ψ be the map

$$\psi: R[x]/\langle x^N - 1\rangle \to R[x]/\langle x^N - \tau_\delta\rangle,$$
$$r(x) \to r(\alpha x).$$

Similar to the proof of Theorem 3.1, ψ is a ring isomorphism, and the result follows. □

Corollary 3.6 A cyclic code of length $N = 4l-2$ over $F_{2^m}[u]/\langle u^3\rangle$ is equivalent to a $(1+\zeta u^2)$ constacyclic code of length $N=4l-2$ over $F_{2^m}[u]/\langle u^3\rangle$, where l is a non-negative integer and $\zeta \in F_{2^m}^*$.

Proof Since $\gcd(2, 2^m-1)=1$, then there exists $\gamma \in F_{2^m}^*$ such that $\gamma^2 = \zeta$. Let $\delta=2$, $\alpha = 1+\gamma u$ in Theorem 3.5, then $\tau_2 = (1+\beta u)^2 = 1+\zeta u^2$. This gives the proof. □

According to Theorems 2.6, 3.2 in Ref.[4] and Corollary 3.6, we can get the following theorem.

Theorem 3.7 Let C be a $(1+\zeta u^2)$ constacyclic code of length $N = 4l-2 = 2^e n$ over $F_{2^m}[u]/\langle u^3\rangle$ and $\theta_3 = 1+\gamma u$, where $\zeta \in F_{2^m}^*$ and $\gamma^2 = \zeta$. Then C has one of the following forms:

① $C = \langle g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x)\rangle$, where $(g + u p_1 + u^2 p_2) \mid (x^N - 1)$, $g \mid (x^N-1)$ and $\deg(p_2) < \deg(p_1)$ over $F_{2^m}[u]/\langle u^3\rangle$. Let $\deg(g) = r$, then $\operatorname{rank}(C) = N - r$. A minimal generating set of C over $F_{2^m}[u]/\langle u^3\rangle$ is

$$\Lambda_1 = \{g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x),$$
$$x[g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x)], \cdots,$$
$$x^{N-r-1}[g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x)]\}.$$

② $C = \langle g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x), u^2 a_2(\theta_3 x)\rangle$, where $a_2 \mid g \mid (x^N - 1)$, $(g + u p_1) \mid (x^N - 1)$ over $F_{2^m} + uF_{2^m}$ and $g \mid p_1\left(\frac{x^N-1}{g}\right)$, $a_2 \mid p_1\left(\frac{x^N-1}{g}\right)$, $a_2 \mid p_2\left(\frac{x^N-1}{g}\right)^2$, $\deg(p_2) < \deg(p_1)$. Let $\deg(g) = r$ and $\deg(a_2) = t$, then $\operatorname{rank}(C) = N - t$. A minimal generating set of Cover $F_{2^m}[u]/\langle u^3\rangle$ is

$$\Lambda_2 = \{g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x),$$
$$x[g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x)], \cdots,$$
$$x^{N-r-1}[g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x)],$$
$$u^2 a_2(\theta_3 x), xu^2 a_2(\theta_3 x), \cdots, x^{r-t-1} u^2 a_2(\theta_3 x)\}.$$

③ $C = \langle g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x), u a_1(\theta_3 x) + u^2 q_1(\theta_3 x), u^2 a_2(\theta_3 x)\rangle$, where $a_2 \mid a_1 \mid g \mid (x^N - 1)$, $a_1 \mid p_1\left(\frac{x^N-1}{g}\right)$, $a_2 \mid q_1\left(\frac{x^N-1}{a_1}\right)$, $a_2 \mid p_2\left(\frac{x^N-1}{g}\right)\left(\frac{x^N-1}{a_1}\right)$, $\deg(p_2) < \deg(a_2)$, $\deg(q_1) < \deg(a_2)$ and $\deg(p_1) < \deg(a_1)$ over F_{2^m}. Let $\deg(g) = r$, $\deg(a_1) = s$ and $\deg(a_2) = t$, then C has a minimal generating set over $F_{2^m}[u]/\langle u^3\rangle$ given by

$$\Lambda_3 = \{g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x),$$
$$x[g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x)], \cdots,$$
$$x^{N-r-1}[g(\theta_3 x) + u p_1(\theta_3 x) + u^2 p_2(\theta_3 x)],$$
$$u[a_1(\theta_3 x) + u q_1(\theta_3 x)],$$
$$xu[a_1(\theta_3 x) + u q_1(\theta_3 x)], \cdots,$$
$$x^{r-s-1} u[a_1(\theta_3 x) + u q_1(\theta_3 x)],$$
$$u^2 a_2(\theta_3 x), xu^2 a_2(\theta_3 x), \cdots, x^{s-t-1} u^2 a_2(\theta_3 x)\}.$$

4 Conclusion

In this paper, the generator polynomials and minimal generating sets of some constacyclic codes over $F_{p^m}[u]/\langle u^k\rangle$ have been investigated. In particular, the generator polynomials and minimal generating sets of $(1+\zeta u^2)$ constacyclic codes with odd length and $N \equiv 2 \pmod 4$ over $F_{2^m}[u]/\langle u^3\rangle$ have been obtained for any $\zeta \in F_{2^m}^*$. A natural problem is the determination of the generator polynomials and minimal generating sets of $(1+\zeta u^2)$ constacyclic codes with length $N \equiv 0 \pmod 4$ over $F_{2^m}[u]/\langle u^3\rangle$.

References

[1] Abualrub T, Siap I. Constacyclic codes over $F_2 + uF_2$ [J]. Journal of the Franklin Institute, 2009, 346: 520-529.

[2] Qian J F, Zhang L N, Zhu S X, et al. $(1+u)$ constacyclic and cyclic codes over $F_2 + uF_2$ [J]. Applied Mathematics Letters, 2006, 19(8): 820-823.

[3] Abualrub T, Siap I. Cyclic codes over the ring $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2 Z_2$ [J]. Designs Codes and Cryptography, 2007, 42(3): 273-287.

(下转第 164 页)