第39卷第6期　中国科学技术大学学报　Vol. 39, No. 6
2009年6月　JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA　Jun. 2009

Article ID: 0253-2778(2009)06-0583-05

Constacyclic codes over ring $F_q+uF_q+\cdots+u^{s-1}F_q$

SHI Min-jia[1], ZHU Shi-xin[2]

(1. *School of Mathematical Sciences*, *Anhui University*, *Hefei* 230039, *China*;
2. *School of Mathematics*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: The structure of cyclic and constacyclic codes of odd length n over ring $R=F_q+uF_q+\cdots+u^{s-1}F_q$ was established, where F_q denoted a finite field with q elements, $q=p^e$ for some prime p and positive integers s, e, $(n,p)=1$. Besides. It was shown that all ideals in R were principal ideals and provide alternative expression forms of the structures of cyclic and constacyclic codes over R. Moreover, the rank of constacyclic codes over the ring R and their minimal generating sets were also obtained.

Key words: cyclic code; ideal; rank; the minimal generating set

CLC number: TN911.22　　**Document code**: A

AMS Subject Classification (2000): Primary 94B05; Secondary 94B15

环 $F_q+uF_q+\cdots+u^{s-1}F_q$ 上的常循环码

施敏加[1],朱士信[2]

(1.安徽大学数学科学学院,安徽合肥 230039;2.合肥工业大学数学学院,安徽合肥 230009)

摘要:确立了环 $R=F_q+uF_q+\cdots+u^{s-1}F_q$ 上码长为奇数 n 的循环码与常循环码的结构,其中 F_q 为含有 q 个元素的有限域,$q=p^e$,p(即域 F_q的特征)为素数,s, e 为正整数,且$(n,p)=1$.证明了该环上所有的理想均是主理想,给出了该环上循环码与常循环码的结构的另一种表达形式,且给出了该环上常循环码的秩与极小生成元集.

关键词:循环码;理想;秩;极小生成元集

0 Introduction

Progress has been attained in the direction of determining the structural properties of codes over large families of rings. Pless et al investigated the generators of cyclic codes and quadratic residue over Z_4 in Ref. [1]. The structure of cyclic codes over ring Z_{p^m} was obtained in Ref. [2] and later on, with a different proof in Ref. [5]. Qian et al studied the structure of cyclic codes over ring $F_p+uF_p+\cdots+u^{k-1}F_p$ in Ref. [8]. Feng et al discussed constacyclic codes over the integers modulo p^{k+1} in Ref. [11]. Dougherty et al studied cyclic codes over Z_4 of even length in Ref. [4]. Tapia-Recillas

Received: 2008-10-13; **Revised**: 2009-03-10

Foundation item: Supported by Doctoral Fund in Institutions of Higher Learning (20080359003), Key Project of Educational Office of Anhui Province on Natural Sciences (KJ2008A140) and Natural Sciences Project of Hefei University (08KY036ZR).

Biography: SHI Min-jia (corresponding author), male, born in 1980, PhD. Research field: coding theory and cryptography.
E-mail: smjwcl.good@163.com

and Vega considered some constacyclic codes over Z_{2^a}[9]. In this paper, We first investigate the structure of cyclic and constacyclic codes of odd length n over ring $F_q+uF_q+\cdots+u^{s-1}F_q$, where F_q denotes a finite field with q elements, $q=p^e$ for some prime p and positive s, e, and then show that all ideals in $F_q+uF_q+\cdots+u^{s-1}F_q$ are principal ideals and provide an alternative expression form of the structure of constacyclic codes over $F_q+uF_q+\cdots+u^{s-1}F_q$. The rank and minimal generator sets of constacyclic codes are also obtained. We denote $R=F_q+uF_q+\cdots+u^{s-1}F_q$ for convenience.

1 The structure of cyclic codes over ring R

The quotient ring R is a local ring with its maximal ideal (u). The ideals of R form a chain $(0)\subset(u^{s-1})\subset\cdots\subset(u^2)\subset(u)\subset(1)=R$, u is nilpotent and its nilpotent index is s. The units of R are the elements $a\in R$ such that $a\neq 0(\mathrm{mod}\ u)$. A codeword $(c_0,\cdots,c_n)\in C$ can be viewed as a polynomial $c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in R[x]$. If for a given codeword $(c_0,\cdots,c_n)\in C$, its right cyclic shift $(c_1,\cdots,c_n,c_0)$ is also a codeword of C, then the linear code C is called a cyclic code. It is straightforward to show that a cyclic code C of length n by viewing its codewords as polynomials is an ideal in $R[x]$. The structure of cyclic codes over F_2+uF_2 is investigated in Ref. [1]. Further, the structure of cyclic codes over Z_{p^m} is investigated in Ref. [5] and the structure of cyclic codes over $F_p+uF_p+\cdots+u^{k-1}F_p$ is investigated in Ref. [8]. We will go over the structure of codes over R by a generalization of Refs. [7, 8, 11]. Because x^n-1 is a regular polynomial in $R[X]$[6], so a factorization of x^n-1 in $F_q[x]$ can be lifted uniquely to the same factorization in $R[x]$. Since $R[x]$ is a local ring[6], we have the following lemma:

Lemma 1.1[6] Let $x^n-1=f_1f_2\cdots f_r$, where $f_i(x)\in F_q[x]$, $i=1,2,\cdots,r$, are the irreducible monic polynomials. Then x^n-1 has the same factorization and irreducible polynomials in $R[x]$.

The following theorem can be easily obtained by similar steps as Refs. [7,8].

Theorem 1.2 Assume that n is not divisible by p. There exist $F_i(0\leqslant i\leqslant s)$ basic irreducible and pairwise coprime polynomials where $x^n-1=F_0F_1\cdots F_s$ such that any ideal in $R[x]/(x^n-1)$ is a sum of ideals of the form $(\hat{F}_1)$, $(u\hat{F}_2)$, $\cdots$, $(u^{s-1}\hat{F}_s)$, i.e.

$$C=(\hat{F}_1,u\hat{F}_2,\cdots,u^{s-1}\hat{F}_s),$$

where $\hat{F}_i$ denotes the product of all F_j except F_i, $j\neq i$.

Remark Some generators in the result of Theorem 1.2 may be zero, if for some k, $1\leqslant k\leqslant s$, $F_k=1$, then

$$\hat{F}_k=F_1F_2\cdots F_{k-1}F_{k+1}\cdots F_s\equiv 0(\mathrm{mod}\ x^n-1).$$

The following theorem shows that all ideals in $R[x]/(x^n-1)$ are principal. In particular, it gives the structure of cyclic codes over R, which can also be found in Ref. [12]. Here we will give a detailed proof.

Theorem 1.3 Let C be a linear code of length n over R. Then $C=(g(x))$ for some $g(x)\in R[x]/(x^n-1)$.

Proof If C is a linear code of length n over R, then, by Theorem 1.2, $C=(\hat{F}_1,u\hat{F}_2,\cdots,u^{s-1}\hat{F}_s)$, where $x^n-1=F_0F_1\cdots F_s$ and polynomials F_i $(0\leqslant i\leqslant s)$ are pairwise coprime. If we take $g(x)=\hat{F}_1+u\hat{F}_2+\cdots+u^{s-1}\hat{F}_s$, Theorem 1.3 is proven. It is clear that

$$g(x)=\hat{F}_1+u\hat{F}_2+\cdots+u^{s-1}\hat{F}_s\subseteq C=(\hat{F}_1,u\hat{F}_2,\cdots,u^{s-1}\hat{F}_s).$$

To show the reverse, note that for any distinct $i,j\in\{0,1,\cdots,s\}$, we have $x^n-1|\hat{F}_i\hat{F}_j$, so $\hat{F}_i\hat{F}_j=0$ in $R[x]/(x^n-1)$. Moreover, for any i with $1\leqslant i\leqslant s$, $F_i,\hat{F}_i$ are coprime, hence, there exist $s_i(x)$, $t_i(x)\in R[x]$ such that $s_i(x)F_i+t_i(x)\hat{F}_i=1$. Thus, for any integer $j\in\{1,2,\cdots,s\}$, we have $\prod_{I=1}^{j}(s_iF_i+t_i\hat{F}_i)=1$. Multiplying the left-hand side of this equation out, we get that there exist polynomials $w_{j,0},\cdots,w_{j,j}$ such that

$$w_{j,0}F_1F_2\cdots F_j+w_{j,1}\hat{F}_1F_2\cdots F_j+w_{j,2}F_1\hat{F}_2\cdots F_j+\cdots+w_{j,j}F_1F_2\cdots F_{j-1}\hat{F}_j=1.$$

In particular, when $j=s-1$, we have

$$w_{s-1,0}F_1F_2\cdots F_{s-1}+w_{s-1,1}\hat{F}_1F_2\cdots F_{s-1}+w_{s-1,2}F_1\hat{F}_2\cdots F_{s-1}+\cdots+w_{s-1,s-1}F_1F_2\cdots F_{s-2}\hat{F}_{s-1}=1.$$

Multiplying both sides of the above equation by $u^{s-1}\hat{F}_s$ yields $u^{s-1}\hat{F}_sw_{s-1,0}F_1F_2\cdots F_{s-1}=u^{s-1}\hat{F}_s$. By hypothesis

$$g(x)=\hat{F}_1+u\hat{F}_2+\cdots+u^{s-1}\hat{F}_s,$$

which implies

$$g(x)F_1F_2\cdots F_{s-1}=u^{s-1}\hat{F}_sF_1F_2\cdots F_{s-1}.$$

Hence,

$$g(x)F_1F_2\cdots F_{s-1}w_{s-1,0}=u^{s-1}\hat{F}_sF_1F_2\cdots F_{s-1}w_{s-1,0}=u^{s-1}\hat{F}_s.$$

Therefore,

$$u^{s-1}\hat{F}_s,u^{s-2}\hat{F}_{s-1},\cdots,u\hat{F}_2,\hat{F}_1\in(g(x)).$$

Consequently, $C=(g(x))$. □

Theorem 1.4 Let C be a linear code of length n over C, where $x^n-1=F_0\cdots F_s$ and $F_i(0\leqslant i\leqslant s)$ are basic irreducible and pairwise coprime polynomials. Then there exist polynomials $f_0,f_1,\cdots,f_{s-1}$ in $R[x]$ such that $C=(f_0,uf_1,\cdots,u^{s-1}f_{s-1})$, where $f_{s-1}\mid f_{s-2}\mid\cdots\mid f_0\mid(x^n-1)$ and $|C|=q^k$, $k=\sum\limits_{i=0}^{s-1}(s-i)(n-\deg F_{i+1})$.

Proof We can obtain the desired results by taking

$$f_i(x)=\begin{cases}F_0(x)F_{i+2}(x)\cdots F_s(x), & \\ \quad\text{if } 0\leqslant i\leqslant s-2; & \\ F_0(x), \quad \text{if } i=s-1. &\end{cases}$$

In fact, Theorem 1.4 provides an alternative expression form of the structure of cyclic codes over R.

2 The constacyclic codes over R

For some fixed unit λ of R, let v_λ be the automorphism on R^n given by $v_\lambda=(a_0,a_1,\cdots,a_{n-1})=(\lambda a_{n-1},a_0,a_1,\cdots,a_{n-2})$. Recall that a subset C of R^n is a constacyclic code of length n if there exists a unit λ of R such that it is invariant under the automorphism v_λ, that is, $v_\lambda(C)=C$. If $\lambda=1$ the code is said to be cyclic. Constacyclic linear codes of length n over R can be identified as ideals in the quotient ring $R[x]/(x^n-\lambda)$ via the isomorphism φ from R^n to $R[x]/(x^n-\lambda)$ defined by

$$(a_0,a_1,\cdots,a_{n-1})\mapsto a_0+a_1x+\cdots+a_{n-1}x^{n-1}.$$

Theorem 2.1 Let C be a cyclic code of length n over R. Then C is a λ-cyclic code of code length n if and only if $\varphi(C)$ is the ideal of ring $R[x]/(x^n-\lambda)$.

Proof For $\forall c=(c_0,c_1,\cdots,c_{n-1})\in C$, $\varphi(c)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}=c(x)$, the corresponding polynomial of $\tilde{c}=V_\lambda(c)=(\lambda c_{n-1},c_0,c_1,\cdots,c_{n-2})$ is

$$\widetilde{c(x)}=\lambda c_{n-1}+c_0x+c_1x^2+\cdots+c_{n-2}x^{n-1}\equiv c_0x+c_1x^2+\cdots+c_{n-1}x^{x-1}(\text{mod } x^n-\lambda)=x(c_0+c_1x+\cdots+c_{n-1}x^{n-1})\equiv xc(x)(\text{mod } x^n-\lambda).$$

Because $\varphi(C)$ is the ideal of ring $R[x]/(x^n-\lambda)$, it follows that $\forall c(x)\in\varphi(C)$, $xc(x)\in\varphi(C)$, hence $\widetilde{c(x)}\in\varphi(C)$. Namely $\tilde{c}=(\lambda c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$, thus C is a λ-cyclic code. Next we prove the reverse. Suppose C is a λ-cyclic code over R, it follows that for $\forall c=(c_0,c_1,\cdots,c_{n-1})\in C$, $v_\lambda(c)=(\lambda c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$, equivalently for

$$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in\varphi(c),$$

$$\lambda c_{n-1}+c_0x+c_1x^2+\cdots+c_{n-2}x^{n-1}=xc(x)(\text{mod } x^n-\lambda)\in\varphi(C).$$

Hence for $\forall 1\leqslant i\leqslant n-1$, $x^ic(x)\in\varphi(C)$, then for $\forall f(x)\in R[x]/(x^n-\lambda)$, it follows that $f(x)c(x)\in\varphi(C)$, so $\varphi(C)\lhd R[x]/(x^n-\lambda)$. □

Theorem 2.2 Let p be prime, $p\nmid n$, $x^n-\lambda=f_1f_2\cdots f_r$, where $f_i\in R[x]$, $1\leqslant i\leqslant r$ are the basic irreducible monic polynomials. Then the ideals of $R_n=R[x]/(x^n-\lambda)$ are the direct sum of some $(\hat{f}_i+(x^n-\lambda))$, $(u\hat{f}_i+(x^n-\lambda))$, $(u^2\hat{f}_i+(x^n-\lambda))$, $\cdots$, $(u^{s-1}\hat{f}_i+(x^n-\lambda))$, where $0\leqslant i\leqslant r$, $\hat{f}_i=(x^n-\lambda)/f_i$.

Proof Since $f_1,f_2,\cdots,f_s$ are pairwise prime polynomials, so

$$(x^n-\lambda)=(f_1f_2\cdots f_s)=(f_1)\cap(f_2)\cap\cdots\cap(f_s),$$

according to the Chinese remainder theorem

$$R_n = R[x]/(x^n - \lambda) =$$
$$R[x]/(f_1) \cap R[x]/(f_2) \cap \cdots \cap R[x]/(f_s).$$

If $I \lhd R_n$, then $I \cong I_1 \oplus I_2 \oplus \cdots \oplus I_s$, where $I_i \lhd R[x]/(f_i)$. Similar to Lemma 2.1[5], $I_i = 0$ or $(u^j + (f_i))$, $0 \leqslant j \leqslant s-1$. Thus I_i corresponded to the ideal $u^j \hat{f}_i + (x^n - \lambda)$ of R_n. □

Theorem 2.3 Let p be prime, $p \nmid n$, C is λ-cyclic code of length n over R, then there exist basic irreducible and pairwise coprime polynomials $F_i (0 \leqslant i \leqslant s)$ such that $x^n - \lambda = F_0 F_1 \cdots F_s$ and $C = (\hat{F}_1, u\hat{F}_2, \cdots, u^{s-1}\hat{F}_s)$ where $\hat{F}_i$ denotes the product of all F_j except F_i, $j \neq i$, $|C^{\perp}| = p^l$,

$$l = \sum_{i=0}^{s-1} (s-i) \deg F_{i+1}.$$

Proof Let $x^n - \lambda = f_1 f_2 \cdots f_r$, where $f_i \in R[x]$, $0 \leqslant i \leqslant r$ are the basic irreducible monic polynomials. According to Theorem 2.2, C is the sum of the following forms

$$(\hat{f}_{l_1+1}), (\hat{f}_{l_1+2}), \cdots, (\hat{f}_{l_1+l_2}); (u\hat{f}_{l_1+l_2+1}), \cdots,$$
$$(u\hat{f}_{l_1+l_2+l_3}); \cdots; (u^{s-1}\hat{f}_{l_1+l_2+\cdots+l_s+1}), \cdots, (u^{s-1}\hat{f}_r),$$

namely

$$C = (f_1 f_2 \cdots f_{l_1} f_{l_1+l_2+1} \cdots f_s,$$
$$u f_1 f_2 \cdots f_{l_1+l_2} f_{l_1+l_2+l_3+1} \cdots f_s,$$
$$u^2 f_1 f_2 \cdots f_{l_1+l_2+l_3} f_{l_1+l_2+l_3+l_4+1} \cdots f_s,$$
$$\cdots, u^{s-1} f_1 f_2 \cdots f_{l_1+l_2+\cdots+l_s}).$$

Let

$$\hat{F}_1 = f_1 f_2 f_3 \cdots f_{l_1} f_{l_1+l_2+1} \cdots f_s,$$
$$\hat{F}_2 = f_1 f_2 f_3 \cdots f_{l_1+l_2} f_{l_1+l_2+l_3+1} \cdots f_s,$$
$$\cdots\cdots$$
$$\hat{F}_s = f_1 f_2 f_3 \cdots f_{l_1+l_2+\cdots+l_s}.$$

Taking

$$F_i(x) = \begin{cases} f_{l_0+l_1+\cdots+l_i+1} \cdots f_{l_0+l_1+\cdots+l_{i+1}}, & \text{if } l_{i+1} \neq 0; \\ 1, & \text{if } l_{i+1} = 0; \end{cases}$$

$l_0 = 0$, $0 \leqslant i \leqslant s$; then it is easy to verify that $x^n - \lambda = F_0 F_1 \cdots F_s$, so

$$C = (\hat{F}_1, u\hat{F}_2, \cdots, u^{s-1}\hat{F}_s) =$$
$$(\hat{F}_1) \oplus (u\hat{F}_2) \cdots \oplus (u^{s-1}\hat{F}_s).$$

Hence

$$|C_1| = |(\hat{F}_1)|\,|(u\hat{F}_2)| \cdots |(u^{s-1}\hat{F}_s)| =$$
$$p^{s(n-\deg \hat{F}_1)} p^{(s-1)(n-\deg \hat{F}_2)} \cdots p^{(n-\deg \hat{F}_s)}.$$ □

Corollary 2.4 Let p be prime, C is a λ-cyclic code of length n over R, $p \nmid n$, then there exist polynomials $g_0, g_1, \cdots, g_k$ such that $g_{s-1} | g_{s-2} | \cdots | g_0 | (x^n - \lambda)$ and $C = (g_0, ug_1, u^2 g_2, \cdots, u^{s-1} g_{s-1})$.

Proof According to Theorem 2.3, $C = (\hat{F}_1, u\hat{F}_2, \cdots, u^{s-1}\hat{F}_s)$, $x^n - \lambda = F_0 F_1 \cdots F_s$, let $g_i = F_0 F_{i+2} \cdots F_s$, $0 \leqslant i \leqslant s-2$; $g_{s-1} = F_0$, then $g_{s-1} | g_{s-2} | \cdots | g_0 | (x^n - \lambda)$, for $\forall i$, $0 \leqslant i \leqslant s-1$,

$$u^i \hat{F}_{i+1} = u^i F_0 F_1 \cdots F_i F_{i+2} \cdots F_s = u^i g_i F_1 F_2 \cdots F_i,$$

so $C \subseteq (g_0, ug_1, u^2 g_2, \cdots, u^{s-1} g_{s-1})$. Because F_1 and F_2 are coprime, then there exist polynomials p, $q \in R[x]$ such that $pF_1 + qF_2 = 1$, hence

$$ug_1 = uF_0 F_3 \cdots F_s =$$
$$u(pF_1 + qF_2) F_0 F_3 \cdots F_s =$$
$$upF_0 F_1 F_3 \cdots F_s + uqF_0 F_2 F_3 \cdots F_s =$$
$$up\hat{F}_2 + uqg_0 = up\hat{F}_2 + uq\hat{F}_1 \in C.$$

Proceeding like this we can conclude that $u^i g_i \in C (1 \leqslant i \leqslant s-1)$. Thus

$$C = (g_0, ug_1, u^2 g_2, \cdots, u^{s-1} g_{s-1}).$$ □

The following corollary can be obtained according to the proof process of Theorem 1.3.

Corollary 2.5 Let p be prime, $p \nmid n$, if $R_n = R[x]/(x^n - \lambda)$ is a principal ideal ring, $C \lhd R_n$, then $C = (g(x)) = (\hat{F}_1 + u\hat{F}_2 + \cdots + u^{s-1}\hat{F}_s)$.

Now we discuss the dual codes of λ-cyclic codes C.

Lemma 2.6 Let C be a nonzero linear code of length n over R, $|C| = p^l$, $|C^{\perp}| = p^h$, then $|C|\,|C^{\perp}| = p^{sn}$, where $h + l = ns$.

Lemma 2.7 Let C be λ-cyclic code of length n over R and $C = (\hat{F}_1, u\hat{F}_2, \cdots, u^{s-1}\hat{F}_s)$, where $x^n - \lambda = F_0 F_1 F_2 \cdots F_s$ and F_0, F_1, F_2, $\cdots$, F_s are coprime. Then $C^{\perp} = (\hat{F}_0^*, u\hat{F}_s^*, u^2\hat{F}_{s-1}^*, \cdots, u^{s-1}\hat{F}_2^*)$, $|C^{\perp}| = p^h$, where $h = \sum_{i=0}^{s-1} i \deg F_{i+1}$ and $F^* = x^{\deg(F)} F(1/x)$ is the reciprocal polynomial of F.

Proof Let $C_1 = (\hat{F}_0^*, u\hat{F}_s^*, u^2\hat{F}_{s-1}^*, \cdots, u^{s-1}\hat{F}_2^*)$, for $\forall\, 0 \leqslant i, j \leqslant s-1$, whether $i+1 \neq s-j+1$ or $i+1 \neq s-j+1$ not, we can obtain that $(x^n - \lambda) | (u^i \hat{F}_{i+1})(u^j \hat{F}_{s-j+1}^*)$. Thus $(u^i \hat{F}_{i+1}) \cdot$

$(u^j\hat{F}^*_{s-j+1})\equiv 0(\bmod\ x^n-\lambda)$, so $C_1\subseteq C^{\perp}$. Also $|C_1|=p^{s\deg F_0^*}\ p^{(s-1)\deg F_s^*}\cdots p^{\deg F_2^*}=p^h$, where $h=\sum_{i=0}^{s-1} i\deg\ F_{i+1}, F_{s+1}=F_0$. On the other hand, suppose $|C^{\perp}|=p^{h_1}$, $|C_1|=p^l$, according to Theorem 2. 3, $l=\sum_{i=0}^{s-1}(s-i)\deg F_{i+1}$, according to Lemma 2. 6, $h_1+l=ns$. Hence $h_1=\sum_{k=0}^{s-1} i\deg F_{i+1}=h$, namely $C_1=C^{\perp}$. □

3 The minimal generating set of constacyclic codes over R

Dougherty defined the rank of a code C of length n over R_4 in Ref. [3], defined the rank of C, denoted by rank(C), by the minimum number of generators of C, and defined the free rank of C, denoted by frank(C), by the maximum of the ranks of R-free submodules of C. A code of rank r over R, with free frank k_1 and $k_2=r-k_1$, will have $4^{k_1}2^{k_2}$ elements and we shall often denote the code as being of type $\{k_1, k_2\}$. According to the description above we can define the rank of cyclic codes over ring R naturally.

Definition 3. 1 The cyclic codes over ring R are free R-submodules, denoted the rank of (C) by rank(C), by the number of the elements of its basis, or equivalently by the minimum number of generators of C.

Lemma 3. 2[10] Let $C=(g(x))$ be a cyclic code over R, where $g(x)|x^n-1$ and $\deg g(x)=r$. Then C is a free R-submodule with rank(C) $=n-r$, and its minimal generating set is

$$\beta=\{g(x), xg(x), \cdots, x^{n-r-1}g(x)\}.$$

Theorem 3. 3[10] Let $C=(u^lh(x))$ be a cyclic code over R. In $R[x]$, $h(x)|x^n-1$ and $\deg h(x)=r$, $u^l\neq 0$. Then C is a free R-submodule with rank(C)$=n-r$, and its minimal generating set is

$$\beta=\{u^lh(x), xu^lh(x), \cdots, x^{n-r-1}u^lh(x)\}.$$

Theorem 3. 4 Let $C=(g_0, ug_1, \cdots, u^{s-1}g_{s-1})$ be any constacyclic code over R, where $g_{s-1}|g_{s-2}|\cdots|g_0|(x^n-1)$, $\deg\ g_i=r_i$ and $r_{s-1}<r_{s-2}<\cdots<r_0$. Then C is a free R-submodule with its rank(C)$=n-r_{s-1}$, and its minimal generating set is

$$\beta=\left\{\begin{matrix} g_0 & xg_0 & \cdots & x^{n-r_0-1}g_0 \\ ug_1 & xug_1 & \cdots & x^{r_0-r_1-1}ug_1 \\ \cdots & \cdots & \cdots & \cdots \\ u^{s-2}g_{s-2} & xu^{s-2}g_{s-2} & \cdots & x^{r_{s-3}-r_{s-2}-1}u^{s-2}g_{s-2} \\ u^{s-1}g_{s-1} & xu^{s-1}g_{s-1} & \cdots & x^{r_{s-2}-r_{s-1}-1}u^{s-1}g_{s-1} \end{matrix}\right\}$$

Proof Let $C=(g_0, ug_1, \cdots, u^{s-1}g_{s-1})$ be any cyclic code over R, where $g_{s-1}|g_{s-2}|\cdots|g_0|(x^n-1)$, $\deg\ g_i=r_i$ and $r_{s-1}<r_{s-2}<\cdots<r_0$. If any of the generators in C above is equal to 0, then we eliminate it from the generators. So we may assume all the generators are nonzero. First, we show that β spans C, by Lemma 3. 3, it suffices to show that β spans

$$\boldsymbol{B}=\left\{\begin{matrix} x^{r_0-r_1}ug_1 & \cdots & x^{n-r_1-1}ug_1 \\ x^{r_1-r_2}u^2g_2 & \cdots & x^{n-r_2-1}u^2g_2 \\ \cdots & \cdots & \cdots \\ x^{r_{s-3}-r_{s-2}}u^{s-2}g_{s-2} & \cdots & x^{n-r_{s-2}-1}u^{s-2}g_{s-2} \\ x^{r_{s-2}-r_{s-1}}u^{s-1}g_{s-1} & \cdots & x^{n-r_{s-1}-1}u^{s-1}g_{s-1} \end{matrix}\right\}$$

By similarity, we only need to show that β spans $x^{r_0-r_1}uf_1$. Since $x^{r_0-r_1}\ ug_1$, $ug_0\in(ug_1)$. By Lemma 3. 3, it follows that

$$x^{r_0-r_1}ug_1-ug_0=\alpha_0ug_1+\alpha_1xug_1+\cdots+ \alpha_{r_0-r_1-1}x^{r_0-r_1-1}ug_1+\alpha_{r_0-r_1}x^{r_0-r_1}ug_1+\cdots+ \alpha_{n-r_1-1}x^{n-r_1-1}ug_1. \quad (1)$$

Since we may assume that g_0, g_1 are monic, then the largest power on the left-hand side of Eq. (1) is less than r_0. Therefore $\alpha_{r_0-r_1}u=\cdots=\alpha_{n-r_1-1}u=0$. Hence,

$$x^{r_0-r_1}ug_1=ug_0+\alpha_0ug_1+\alpha_1xug_1+ \cdots+\alpha_{r_0-r_1-1}x^{r_0-r_1-1}ug_1.$$

Hence, β spans $\boldsymbol{B}$. Now, we show that none of the elements in β is a linear combination of the others. Suppose that xu^ig_i for $i=0, 1, \cdots, s-1$ is a linear combination of some elements in $\beta-xu^if_i$ for $i=0, 1, \cdots, s-1$ (Note that the proof works if we choose any other element). The largest power in xu^ig_i is equal to r_i+1. It is easy to see that no linear combination of elements in $\beta-xu^ig_i$ will give a polynomial of degree equal to r_i+1. So, β is a minimal generating set for C, with its rank$=n-r_{s-1}$.

(下转第 593 页)