Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (16): 3227-3232, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.3227.3232

A Class of Constacyclic Codes over Z_{p^m}

Liao Dajian
College of Science, Huaihai Institute of Technology, Lianyungang, China

Abstract: We study μp-1-constacyclic codes over Z_{p^m} of arbitrary length, where μ is a unit in Z_{p^m} and m≥2 a positive integer, p a prime integer. We first derive the structure of μp-1-constacyclic codes over Z_{p^m} of length p^s over Z_{p^m}, these codes are then used to classify allμp-1-constacyclic codes over Z_{p^m} of arbitrary length. The generator polynomials of such constacyclic codes of arbitrary length are determined.

Key words: Finite chain ring, constacyclic codes, generater polynomial, constacyclic shift

INTRODUCTION

Cyclic codes are a very important class of codes, they were studied for over fifty years. Cyclic codes were studied first over the binary field F2, then were extended to Fq with $q = p^r$. By viewing a cyclic code C of length n over a finite field Fq as an ideal of the ring Fq (x)/⟨x^n-1⟩, the structure of cyclic codes was obtained. After the discovery that certain good nonlinear binary codes can be constructed from cyclic codes over Z4 via the Gray map, codes over finite rings have received much more attention. Recently, Shixin Zhu and Xiaoshan Kai study (1+λp)-constacyclic codes over Z_{p^m} of arbitrary length, determine the Hamming and homogeneous distances of these codes. In this study, we investigate μp-1-constacyclic codes over Z_{p^m} of arbitrary length. Using the Chinese remainder theorem, we classify all μp-1 -constacyclic codes over Z_{p^m} of length np^S (n is not divisible by p and s>0 is an integer. The rest of this study is organized as follows. Section 2 gives some notations and results about constacyclic codes and finite commutative chain rings. In section 3, we study the structure of μp-1-constacyclic codes of length p^S over Z_{p^m} and determine the Hamming distances of all such constacyclic codes. In section 4, we classify all μp-1-constacyclic codes over Z_{p^m} of length np^s (n prime to p) by the Chinese remainder theorem.

BASIC CONCEPTS

In this section, we will review some fundamental backgrounds used in this study. Let R be a ring. An ideal I of a ring R is called principal if it is generated by a single element. A finite ring R is called a chain ring if all its ideals are linearly ordered by inclusion. By definition, it can be verified that all the ideals of the finite chain ring R are principal. Let R be a finite commutative chain ring with identity, m is the unique maximal ideal of R and let λ be the generater of the unique maximal ideal m, Then m = ⟨λ⟩ = Rλ, where Rλ = ⟨λ⟩ = {βλ|β∈R}. We have:

$$R = \langle \lambda^0 \rangle \supseteq \langle \lambda^2 \rangle \supseteq \ldots \langle \lambda^{i-1} \rangle \supseteq \quad (1)$$

The chain in 1 cannot be infinite since R is finite. Therefore, there exists i, such that $\lambda^i = 0$. Let e is the minimal number such that $\lambda^e = 0$. The number e is called the nilpotency index of λ. Let F = R/⟨λ⟩ be the residue field of R with characteristic p, where p is is a prime number. Then $|F| = q = p^r$ for some integer r. Let R be a finite commutative ring with identity. A code over R of length N is a nonempty subset of R^N and a code is linearover R of length N if it is an R-submoodule of R^N. For some fixed unit μ of *R*, the μ-constacyclic shift τ_μ on RN is the shift $\tau_\mu (c_0, c_1, ..., c_{N-1}) = (\mu c_{N-1}, c_0, ..., c_{N-2})$ and a linear code C of length N over R is μ-constacyclic if the code is invariant under the μ-constacyclic shift τ_μ. Note that the R-module R^N is isomorphic to the R-module R (x)/⟨x^N-μ⟩. We identify a codeword $(c_0, c_1, \ldots, c_{N-1})$ with its polynomial representation $c(x) = c_0+c_1x + \ldots + c_{N-1}x^{N-1}$. Then xc (x) corresponds to the μ-constacyclic shift of c (x) in the ring R [x]/⟨x^N-μ⟩. Thus μ-constacyclic codes of length N over R can be identified as ideals in the ring R (x)/⟨x^N-μ⟩. The following three lemma are well known, they were proof by Mcdonald (1958).

Lemma 2.1: Assume the notations given above. For any α∈R there is a unique integer I, 0<i<e such that $\alpha = \mu\lambda^i$, with μ as a unit, the unit μ is unique module λ^{e-i}.

Lemma 2.2: Let R be a finite commutative chain ring with identity, its maximal ideal ⟨λ⟩, where λ be the generator of the maximal ideal with nilpotency index m. Let V⊆R be a representatives for the equivalence classes of R under congruence modulo λ, Then:

- For all $\alpha \in R$, there are unique $\alpha_0, ..., \alpha_{m-1} \in V$ such that $\alpha = \alpha_0+\alpha_1\lambda+ ... +\alpha_{m-1}\lambda^{m-1}$
- $|V| = |F|$
- $|\langle\lambda^i\rangle| = |F|$ for all $0 \le i < m-1$

From lemma 2.2, we know that any element of Zpm can be written as $a = a_0+a_1p+ ... +a_{m-1}p$ where the a_i's can be viewed as element of Fp. It is well known that a is a unit if and only if $a_0 \neq 0$ in Fp. A polynomial f (x) in R (x) is said to be a basic irreducible polynomial if its reduction modulo p, is irreducible polynomial in Fp (x).

Lemma 2.3: Let R be a finite commutative ring with identity. If x-y is nilpotent in R, then x is a unit if and only if y is a unit.

MP-1-CONSTACYCLIC CODES OF LENGTH P^s OVER Z_{p^m}

In the rest of this study, We denote Z_{p^m} by R and:

$$\Re = R\,[x]/\left\langle x^{p^s} - (\mu p - 1)\right\rangle$$

where, μ is a unit in R. Mp-1-constacyclic codes of length p^S over R are precisely the ideals of $\Re$.

Lemma 3.1: The element x + 1 is nilpotent in $\Re$.

Proof: In $\Re$ we have:

$$(x+1)p^s = x^{p^s} + 1 + \sum_{i=1}^{p^s-1} C_{p^s}^i\, x^i = p\mu + \sum_{i=1}^{p^s-1} C_{p^s}^i\, x^i$$

Since $C_{p^s}^i \equiv 0\,(\text{modP})$ for $1 \le i \le p^S-1$, there exists a polynomial $f(x) \in R\,[x]$ such that:

$$(x+1)^{p^s} = p\mu + pf(x)$$

Hence:

$$(x+1)^{mp^s} = (p\mu + pf(x))^m = (p(\mu + f(x)))^m = 0$$

Thus, x+1 is nilpotent in $\Re$.

Let Φ: $R \rightarrow f_p$, Φ (r) = r (modp) denote the canonical reduction map from R to F_p, the map extends naturally to map from R [x] to F_p [x].

Lemma 3.2: Let $a(x) \in \Re$. Then:

- a (x) Can be written as:

$$a(x) = a_0 + a_1(x+1) + a_2(x+1)^2 + \cdots + a_{p^s-1}(x+1)$$

where, $a_i \in R$, $0 \le i \le p^S-1$

- a (x) is a unit if and only if Φ $(a_0) \neq 0$

Proof: (1) is obvious. (2) Note that a (x) can be expressed as a (x) = a_0+)x+1 q (x) for some $q(x) \in \Re$. Since (x+1) are nilpotent in $\Re$, it follows that (x+1) q (x) is nilpotent in $\Re$. Therefore, by lemma 2.3, a (x) is a unit if and only if Φ $(a_0) \neq 0$.

Lemma 3.3: As a element in $\Re$:

$$p = \mu^{-1}\sum_{i=1}^{p^s} b_i\,(x+1)^i$$

Proof: In lemma 3.2, we know that:

$$(x+1)^{p^s} = x^{p^s} + 1 + \sum_{i=1}^{p^s-1} C_{p^s}^i x^i = p\mu + \sum_{i=1}^{p^s-1} C_{p^s}^i\, x^i$$

Write:

$$g(x) = \sum_{i=1}^{p^s-1} C_{p^s}^i\, x^i$$

according to lemma 3.2, g (x) can be written as:

$$g(x)a_0 + a_1(x+1) + a_2(x+1) + ... + a_{p^s-1}(x+1)$$

Obviously a_0 = g(-1), while:

$$(x+1)^{p^s-1} = x^{p^s} + 1 + \sum_{i=1}^{p^s-1} C_{p^s}^i\, x^i$$

hence:

$$(x+1)^{p^S-1} = x + 1 + g(x)$$

let x = -1, we get g (-1) = 0, then:

$$g(x) = a_1(x+1) + a_2(x+1) + \cdots + a_{p^s-1}(x+1)^{p^s-1}$$

and from:

$$(x+1)^{p^s} = p\mu + \sum_{i=1}^{p^s-1} C_{p^s}^i\, x^i$$

we get:

$$p\mu = (x+1)^{p^s} - g(x) = \sum_{i=1}^{p^s} b_i (x+1)^i$$

here:

$$b_{p^s-1} = 1, b_i = -a_i, 1 \le i \le p^s - 1$$

so:

$$p = \mu^{-1} \sum_{i=1}^{p^s} b_i (x+1)^i$$

Lemma 3.4: In $\Re$ we have:

$$(x+1)^{p^s} = p\rho(x)$$

where ρ (x) is a unit in $\Re$.

Proof: Write:

$$g(x) = \sum_{i=1}^{p^s-1} C_{p^s}^i x^i$$

According to the proof of lemma 3.1 and lemma 3.3, g (x) can be written as:

$$g(x) = p\sum_{i=1}^{p^s-1} c_i (x+1)^i$$

so:

$$(x+1)^{p^s} = x^{p^s} + 1 + \sum_{i=1}^{p^s-1} C_{p^s}^i x^i = p(\mu + \sum_{i=1}^{p^s-1} c_i (x+1)^i)$$

by lemma 3.1:

$$\rho(x)\mu + \sum_{i=1}^{p^s-1} c_i (x+1)^i$$

is a unit in $\Re$ since μ is a unit in R and the nilpotent index of x +1 is mp^s.

Theorem 3.1: The ring $\Re$ is a chain ring with maximal ideal $\langle x+1 \rangle$ and residue field Fp and the ideals of $\Re$ are $\langle (x+1)^i \rangle$, $0 \le i \le mp^s$.

Proof: Let a (x) be any element in $\Re$, then according to lemma 3.2, a (x) can be expressed as a (x) = a_0+ (x+1) q (x), where q (x)$\in\Re$[x]. If Φ (a_0) = 0, then a (x) = rp+(x+1) g (x) for some r$\in\Re$, by lemma 3.3:

$$p = \mu^{-1} \sum_{i=1}^{p^s} b_i (x+1)^i$$

hence a (x) = (x + 1) h (x) for some h (x) $\in \Re$. This means a (x) $\in \langle x+1 \rangle$. If Φ (a_0)$\neq$0, then a (x) is a unit in $\langle x+1 \rangle$. Therefore, for any element a (x) of $\Re$, either a (x) is a unit or a (x) $\in\langle x+1 \rangle$. According to proposition 2.1 in (Mcdonald, 1958), $\Re$ is a chain ring whose ideals are $\langle (x+1)^i \rangle$ $0 \le i \le mp^s$.

μp-1-CONSTACYCLIC CODES OF LENGTH np^s OVER Z_{p^m}

In this section, we study μp-1-constacyclic codes of length N over Z_{p^m} where N = np^s and gcd (n, p) = 1, s$\ge$0 is an integer and p is a prime number. We donate:

$$R^N = Z_{p^m}[x] / \langle x^N - (\mu p - 1) \rangle$$

so μp-1-constacyclic codes of length N over Z_{p^m} are precisely the ideals of R^N. We introduce the quotient ring:

$$Z_{p^m}[u] / \langle u^{p^s} - (\mu p - 1) \rangle$$

which can be obtained from $\Re$ by substituting the variable u for x. For convenience, we still denote it by $\Re$ and abbreviate Fp as F. There exists a natural R-module isomorphism φ: $\Re^n \rightarrow R^N$ defined by:

$$\varphi(c_{0,0} + c_{0,1}u + \cdots + c_{0,p^s-1}u^{p^s-1} + \cdots + c_{n-1,0} + c_{n-1,1}u + \cdots + c_{n-1,p^s-1}u^{p^s-1}) = c_{0,0}, c_{1,0}, \cdots c_{n-1,0}, c_{0,1}, c_{1,1}, \cdots, c_{n-1,1}, \cdots, c_{0,p^s-1}, \cdots, c_{n-1,p^s-1})$$

We have:

$$\varphi(u(\sum_{j=1}^{p^s-1} c_{n-1,j}u^j), \sum_{j=1}^{p^s-1} c_{0,j}u^j, \ldots, \sum_{j=1}^{p^s-1} c_{n-2,j}u^j) = (\mu p - 1)c_{n-1,p^s-1}, c_{0,0}, c_{1,0}, \cdots, c_{n-2,p^s-1})$$

this gives that a u-constacyclic shift in $\Re^n$ corresponds to a μp-1-constacyclic shift in R^N. Thus, (μp-1)-constacyclic codes of length N over Z_{p^m} correspond to u-constacyclic codes over $\Re$ of length n via the map φ. In the following, we focus on the structure of μp-1-constacyclic codes of length N over Z_{p^m}. We know uconstacyclic codes over $\Re$ of length n can be identified as ideals in the ring $\Re$ [x]/$\langle x^n$-u$\rangle$, so we study the ideals of the ring $\Re$ [x]/$\langle x^n$-u$\rangle$ in detail. Define a map $\Re \rightarrow$ F, $\bar{r}$ = r (mod (u+1)). The map can be extended from $\Re$ [x] to F [x]. Let f (x) = a_0+a_1x+a_2x^2+ ... a_nx^n $\in \Re$ [x], we have the following maps: $\Re[x] \rightarrow F[x], f(x) \rightarrow \overline{f(x)}$. A polynomial f (x) in $\Re$ [x] is said to be a basic irreducible polynomial if $\overline{f(x)}$ is irreducible in F (x). Two polynomial f_1 (x), f_2 (x) $\in \Re$ [x] are said to be coprime if there exist u_1 (x), u_2 (x) $\in \Re$ [x] such that u_1 (x), f_1 (x)+u_1 (f), f_2 (x) = 1. The following result is well known cf (Norton and Salagean, 2000).

Lemma 4.1: Let f_1 (x), f_2 (x)$\in\Re$[x]. Then f_1 (x) and u_1 (x), f_2 (x) are coprime in $\Re$ [x] if and only if $\overline{f_1(x)}$ and $\overline{f_2(x)}$ are coprime in F (x).

The following lemma is well known as Hensel's Lemma (Mcdonald, 1958).

Lemma 4.2: (hensel's Lemma) Let R be a finite commutative chain ring with maximal ideal ⟨λ⟩ and residue field F_q, ($q = p^r$) the nilpotency index of λ is e, f be a polynomial over R, assume f = g_a, g_2, ..., g_r where, g_1, g_2, ..., g_r are pairwise coprime polynomials over F, and f is the reduction modulo λ of f (x). Then there exists pairwise coprime polynomials f_1, f_2, ..., f_r over R such that f = f_1, f_2, ..., f_r and $\overline{f_1} = g_i$ for I = 1, 2, ..., r.

Lemma 4.3: Let f (x) is a monic basic irreducible polynomial over R, then R [x]/⟨f (x)⟩ is a finite chain ring with residue field F_p, and whose ideals are ⟨φ (λ^i)⟩, 0≤i≤m, where k = deg (f (x)), the map φ denote the canonical map R [x] → R [x]/⟨f (x)⟩. Proof of this lemma can be found in (Dinh and Lopez-Permouth, 2004).

A finite family $(a_i)_{i=1}^k$ of ideals of a commutative R, such that the canonical homomorphism of R to $\oplus_{i=1}^k (R/a_i)$ is an isomorphism is called a direct decomposition of R. The next Lemma is well-known.

Lemma 4.4: ([21]Proposition 2.4) Let R be a commutative ring, $(a_i)_{i=1}^k$ a direct decompositionof R and m an R- module. With the notation we have:

- There exists a family $(a_i)_{i=1}^k$ of idempotents of R such that e_i e_j = 0 for I≠, j:

$$\sum_{i=1}^{k} e_i = 1$$

  and a_i = R (1-e_i) for I = 1, 2, ..., k
- The submodule m_i = e_i m is a complement in m of the submodule a_i m = (1-e_i) m and so the R/a_i modules m_i and m/a_i m are isomorphic via the map π_i: m_i→m/ a_i m, x→x+a_i m
- Every submodule N of m is a internal direct sum of submodules N_i = e_i N ∈ m_i which, are isomorphic via π_i with the submodules N_i'= (a_i m+e_i N)/a_i m of m/a_i m (i = 1, 2, ..., k), Each N_i' is isomorphic to N/a_i N.

  Conversely, if for every i = 1, 2, ..., k, N_i', is a submodule of m/a_i m, then there is a unique submodule N of m, such that N is isomorphic with $\oplus_{i=1}^k N_i$

Theorem 4.1: The canonical homomorphism:

$$\psi : \Re[x]/\langle x^n - u\rangle \rightarrow \oplus_{i=1}^k \Re[x]/\langle f_i(x)\rangle$$

is isomorphism, where f_1, f_2, ..., f_r are pairwise coprime monic basic irreducible polynomial over $\Re$ such that xn-u = $f_1 f_2$ ... f_r.

Proof: We know that $\Re$ is a chain ring with maximal ideal ⟨u+1⟩, so $\overline{x^n - u} = \overline{x^n + 1 - (1+u)} = \overline{x^n + 1} = x^n + 1$, where, $\overline{f(x)}$ is the reduction modulo u + 1 of f (x) which is a polynomial over $\Re$. Assume x^n+1 = $g_1 g_2$ ... g_r in Z_p, where, $g_1 g_2$ ... g_k are monic irreducible polynomials over Z_p. Since gcd (n, p) = 1, then g_1, g_2, ... g_k are pairwise coprime. By lemma 4.2, we know that there are pairwise coprime monic irreducible polynomial f_1, f_2, ... f_k over $\Re$ such that x^n-u = $f_1 f_2$, ... f_k and $\overline{f_1} = g_i$ for I = 1, 2, ..., k, then ⟨f_1⟩, ⟨f_2⟩, ..., ⟨f_k⟩ are pairwise coprime ideals of the ring $\Re$ [x] and ⟨x^n-u⟩ = ⟨f_1⟩, ⟨f_2⟩, ..., ⟨f_k⟩, by Chinese Remainder Theorem, the canonical homomorphism:

$$\psi : \Re[x]/\langle x^n - u\rangle \rightarrow \oplus_{i=1}^k \Re[x]/\langle f_i(x)\rangle$$

is isomorphism.

Let C be a u-constacyclic codes over $\Re$ of length n, c = (c_1, c_2, ..., c_n) ∈ $\Re^n$ is a codeword with:

$$c(x) = \Sigma_{i=1}^{n-1} c_i x^i$$

the corresponding polynomial C (x) = {c (x)|c∈C} is an ideal of $\Re$ [x]/⟨x^n-u⟩, denote C (x)/(C (x)⟨f_i(x)⟩) by C_i, 1≤i≤k, obviously, C_i is the ideal of $\Re$ [x]/⟨f_i⟩. By theorem 4.1, it is easy to verify that $C \cong \oplus_{i=1}^k C_i$ and we have the following enumeration result.

Corollary 4.1: The number of distinct μp-1-constacyclic codes of length N = np^s over Z_{p^m} is $(mp^s+1)^k$, where k is the number of distinct monic basic divisors of x^n-u in $\Re$ [x].

In the following we describe μp = 1-constacyclic codes of length N = np^S over Z_{p^m} in terms of its generator polynomials. We have the following lemma.

Lemma 4.5: Let f_1, f_2, ..., f_r are pairwise coprime monic basic irreducible polynomial over $\Re$ such that x^n-u = $f_1 f_2$ ..., f_r and g_1, g_2, ..., g_r are pairwise coprime monic basic irreducible polynomial over $\Re$ such that $x^n+1 = g_1 g_2 \ldots g_r$. There are $\xi_1^i, \xi_2^i, \cdots, \xi_{h_i}^i$ in $\Re$ [x] /$\langle f_i(x)\rangle$such that:

$$f_i(x) = \Pi_{h=1}^{h_i}(x - \xi_h^i)$$

and there are:

$$\eta_1^i, \mu_2^i, \ldots, \eta_{h_i}^i$$

in $\Re$ [x]/$\langle f_i(x)\rangle$ such that:

$$g_i(x) = \Pi_{h=1}^{h_i}(x - \eta^i{}_h)$$

then:

- $g_i(\xi_h^j)$ is a unit in $\Re$ [x]/$\langle f_j(x)\rangle$ h = 1, 2, ..., h_j, if i≠j
- $g_i(\xi_h^j) \in \langle u+1\rangle$ but $g_i(\xi_h^j)$ is not in $\langle (u+1)^2\rangle$, h = 1, 2, ..., h_i
- If r (x)∈$\Re$ [x] and $g_i(\xi_h^j)$ = 0 for any h, 0≤h≤h_i, then r (x)∈$\langle f_i(x)\rangle$

Proof: (1) For I = 1, 2, ..., k, since $\xi_1^i, \xi_2^i, \cdots, \xi_h^i$ are the roots of f_i (x) = 0 in $\Re$ [x]/$\langle f_i(x)\rangle$, such that:

$$f_i(x) = \Pi_{h=1}^{h_i}(x - \xi_h^i)$$

it follows that:

$$\overline{g_i(x)} = \overline{f_i(x)} = \overline{\Pi_{h=1}^{h_i}(x - \xi^i{}_h)} = \Pi_{h=1}^{h_i}(x - \overline{\eta^i{}_h})$$

then:

$$\overline{g_i(\xi^j{}_1)} = \overline{f_i(\xi^j{}_1)} = \Pi_{h=1}^{h_i}(\overline{\xi^j{}_1 - \eta^i{}_h})$$

if i≠j, then:

$$\overline{\xi^j{}_1 - \eta^i{}_h} \neq 0$$

and $\xi^j{}_1 - \eta^i{}_{h_i}$ is noninvertible for any l = 1, 2, ..., h_j, h = 1, 2, ..., h_i. Hence, $g_i(\xi_h^j)$ is a unit for h = 1, 2, ..., h_j if I≠j, (2) Since $x^n - u = f_1 f_2 \cdots f_k, \xi^i{}_1, \xi^i{}_2, \cdots, \xi^i{}_{h_i}$ are the roots of f_i (x) = 0 in $\Re$ [x]/$\langle f_i(x)\rangle$, then $(\xi_h^i)^n = u, h = 1, 2, \cdots, h_i$. For i = 1, 2, ..., k. We know that x_n+1 = $g_1 g_2 \ldots g_k$, then $g_1(\xi^i{}_h) g_2(\xi^i{}_h) \cdots g_k(\xi^i{}_h) = (\xi^i{}_h)^n + 1 = u + 1$, we have $g_j(\xi_h^i)$ is a unit in $\Re$ [x]/$\langle f_i(x)\rangle$, if i≠j hence:

$$g_i(\xi_h^i) = (\Pi_{j\neq i} g_j(\xi_h^i))^{-1}(u+1) = a(u)(u+1)$$

where, $a(u) = (\Pi_{j\neq i} g_j(\xi_h^i))^{-1}$ is a unit in $\Re$ [x]/$\langle f_i(x)\rangle$. Therefore, $g_i(\xi_h^i)$ is not in $\langle (u+1)^2\rangle$, h = 1, 2, ..., h_i. (3) For 0≤i≤k, since f_i (x) is a monic polynomial in $\Re$ [x], then there are s (x), v (x) ∈ $\Re$ [x] such that deg (v(x))<deg(f_i(x)) and r (x) = s (x) f_i (x)+v (x), then $v(\xi_h^i) = 0$. If v (x) ≠ 0, there is an integer l1 0≤l≤mp^s-1, such that:

$$v(x) = \Sigma_{i=1}^{ep^s-1} v_i(x)(u+1)^i$$

where, v_i (x) ∈ $\Re$ (x) and $\overline{v_1(x)} \neq 0$ then:

$$v(\xi^i{}_h) = v_1(\eta^i{}_h)(u+1)^l + r(u+1)^{l+1}$$

$\overline{f_i}(\overline{\xi_h^i}) = 0$ for some r ∈ $\Re$(x)/$\langle f_i(x)\rangle$since $v(\xi_h^i) = 0$ then $\overline{v}(\overline{\xi_h^i}) = 0$ since $\overline{f_i}(\overline{\xi_h^i}) = 0$ and f_i (x) ∈ $\Re$ [x] is a basic irreducible polynomial and $\deg(\overline{v_1}(x)) < \deg(\overline{f_1}(x))$, contradiction, so v (x) hence r (x) ∈ $\langle f_i(x)\rangle$.

Theorem 4.2: Let C be μp-1-constacyclic codes of length np^s (n prime to p) over Z_{p^m}. Then there are integers 0≤j_i≤mp^s, I = 1, 2 ... k such that:

$$C = \left\langle \prod_{i=1}^k g_i^{ji}(x) \right\rangle$$

where g_i (x)'s are monic irreducible divisors of x^n+1 over $\Re$ [x].

Proof: By Lemma 4.4, $C \cong \oplus_{i=1}^k C_i$ where, Ci = C (x)/ (C (x) $\langle f_i(x)\rangle$)define a map $\psi: C(x) \to C(\xi_h^i), \psi(c(x)) = c(\xi_h^i)$. Where:

$$C(\xi_h^i) = \{c(\xi_h^i) \mid c(x) \in C(x)\}$$

By (iii) of Lemma 4.5, $\ker(\psi) = C(x)\langle f_i(x)\rangle$, then $C(x)/(C(x)\langle f_i(x)\rangle) \cong C(\xi_h^i), C_i \cong C(\xi_h^i)$ can be viewed as a ideal of $\Re$ [x] /$\langle f_i\rangle$, by Lemma 4.3, we can assume C_i isomorphic to the ideal $\langle (u+1)^{ji}\rangle$ of $\Re$[x]/$\langle f_i\rangle$, i = 1, 2, ... , k, let $g(x) = \Pi_{i=1}^k g_i^{ji}(x)$ then by Lemma 4.5:

$$\left\langle g(\xi_h^i)\right\rangle = \left\langle \Pi_{i=1}^k g_i^{k}(\xi^i{}_h)\right\rangle = \left\langle (u+1)^{ji}\right\rangle$$

I = 1, 2, ..., k. Thus, by (3) of Lemma 4.4, we can take g (x) as the generator polynomial of C.

Corollary 4.3: Let:

$$C = \left\langle \Pi_{i=1}^k g_i^{ji}(x)\right\rangle$$

be a μp-1-constacyclic codes of length np^s (n prime to p) over Z_{p_m}, where g_i (x)'s are monic irreducible divisors of x^n+1over $\Re$ [x], then |C| = p^h, where:

$$h = \Sigma_{i=1}^{k} (mp^s - j_i)\deg(g_i(x))$$

Proof: Since $C \cong \oplus_{i=1}^{k} C_i$ then the size of C is:

$$\Pi_{i=1}^{k} |C_i|$$

By the proof of theorem 4.2, C_i isomorphic to the ideal $\langle (u+1)^{ji} \rangle$ of $\Re[x]/\langle f_i \rangle$, I = 1, 2, ..., k, then by lemma 4.3 $|C_i| = p(mp^s - j_i)\deg(g_i(x))$. Calculating the product, we get the result.

REFERENCES

Dinh, H.Q. and S.R. Lopez-Permouth, 2004. Cyclic and negacyclic codes over finite chain rings. IEEE Trans. Inform. Theor., 50: 1728-1744.

Mcdonald, B.R., 1958. Finite Rings with Identity. Marcel Dekker, Van Nostrand, USA.

Norton, G.H. and A. Salagean, 2000. On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Eng. Commun. Comput., 10: 489-506.