http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (2): 377-382, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.377.382
© 2014 Asian Network for Scientific Information

Two Classes of Repeat-Root Constacyclic Codes of Length p^S Over the Ring $F_{p^m}+uF_{p^m}+vF_{p^m}+uvF_{p^m}$

[1]Xiaofang Xu and [2]Shujie Yun
[1]School of Mathematics and Physics, Hubei Polytechnic University, Huangshi, 435003, China
[2]Department of Basic, Henan Mechanical and Electrical Engineering College, Xinxiang, 453000, China

Abstract: The study of constacyclic codes over rings plays a more and more important role in the coding theory. And the constacyclic codes over rings have been studied extensively in the past decade. In this study, the structure of two classes constacyclic codes of length p^S over the ring $R=F_{p^m}+uF_{p^m}+vF_{p^m}+uvF_{p^m}$ are discussed. Let λ = 1+bu, 1+cv, 1+bu+duv, 1+cv+duv, 1+bu+cv, 1+bu+cv+duv, Λ = a+bu, a+cv, a+bu+duv, a+cv+duv, a+bu+cv, where $a,b,c,d\in F_{p^m}$, a ≠ 0, b ≠ 0, c ≠ 0, d ≠ 0, then λ and Λ are units in R. Firstly, by studying ideals of the residue class ring $\frac{R[x]}{<x^{p^s}-\lambda>}$, the structure of all λ-constacyclic codes over R can be obtained. Then, the ring isomorphism Φ from the residue class ring $\frac{R[x]}{<x^{p^s}-\lambda>}$ to the residue class ring $\frac{R[x]}{<x^{p^s}-\Lambda>}$ will be defined. Finally, by using the ring isomorphism Φ, the structure of all Λconstacyclic codes over R can be established.

Key words: Repeat-root constacyclic codes, residue class ring, ideal

INTRODUCTION

The study of constacyclic codes over the finite ring is a very important branch of coding theory. Single-root constacyclic codes over finite chain rings have been studied (Dinh and Lopez-Permouth, 2004; Wolfman, 1999; Kanwar and Lopez-Permouth, 1997). The repeat-root constacyclic codes of length 2^S over F_2+uF_2 have been studied by Dinh (2009). All repeat-root constacyclic codes of length p^S over $F_{p^m}+uF_{p^m}$ have been studied by Dinh (2010). One class of the repeat-root constacyclic codes of length 2^S over $F_{2^m}+uF_{2^m}+\cdots+u^{k-1}F_{2^m}$ have been studied by Dinh and Nguyen (2012). But the study of constacyclic codes over the finite non-chain rings is rarely. Linear codes and cyclic codes over the ring $F_2+uF_2+vF_2+uvF_2$ have been studied by Yildiz and Karadeniz (2010, 2011), where the ring $F_2+uF_2+vF_2+uvF_2$ is a finite non-chain ring. The cyclic code over the finite non-chain ring $F_q+uF_q+vF_q+uvF_q$ have been studied by Xu and Liu (2011).

In this study, two classes of repeat-root constacyclic codes of length p^S over the ring $R=F_{p^m}+uF_{p^m}+vF_{p^m}+uvF_{p^m}$ will be studied. Firstly, by studying the residue class ring:

$$\frac{R[x]}{<x^{p^s}-\lambda>}$$

the structure of all λ-constacyclic codes over R will be obtained. Finally, by using the ring isomorphism Φ from the residue class ring:

$$\frac{R[x]}{<x^{p^s}-\lambda>}$$

to the residue class ring:

$$\frac{R[x]}{<x^{p^s}-\Lambda>}$$

the structure of all Λ-constacyclic codes over R will be established.

BASIC CONCEPTS OF REPEAT-ROOT CONSTACYCLIC CODES

F_{p^m} is a finite field containing p^m elements where p is any prime number and m is an arbitrary positive integer.

Let:

$$R = F_{p^m}+uF_{p^m}+vF_{p^m}+uvF_{p^m} = \{a+ub+cv+duv|a, b, c, d\in F_{p^m}\}$$

where, $u^2 = v^2 = 0$ and uv = vu. The ring R is a characteristic p ring. Obviously, the ring R is a local Frobenius ring.

Corresponding Author: Xiaofang Xu, School of Mathematics and Physics, Hubei Polytechnic University, Huangshi, 435003, China

A code over the ring R of length n is a nonempty subset of R^n. A linear code over R of length n is an R-submodule of R^n.

Let C be a code of length n over R and P(C) be its polynomial representation, i.e.:

$$P(C) = \{\sum_{i=0}^{n-1} c_i x^i \mid (c_0, c_1, \cdots, c_{n-1}) \in C\}$$

For a unit α of R, the α-constacyclic (α-twisted) shift τ_α on R^n is the shift:

$$\tau_\alpha(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = (\alpha a_{n-1}, a_0, \ldots, a_{n-2})$$

A code C is said to be α-constacyclic if $\tau_\alpha(C) = C$, i.e., C is closed under the α-constacyclic shift τ_α. In the case α = 1, these α-constacyclic codes are called as cyclic codes and in the case α = -1, these α-constacyclic codes are called as negacyclic codes. A code C of length n over R is α-constacyclic if and only if P(C) is an ideal of:

$$\frac{R[x]}{\langle x^n - \alpha \rangle}$$

and a code C of length n over R is cyclic if and only if P(C) is an ideal of:

$$\frac{R[x]}{\langle x^n - 1 \rangle}$$

and a code C of length n over R is negacyclic if and only if P(C) is an ideal of:

$$\frac{R[x]}{\langle x^n + 1 \rangle}$$

λ-CONSTACYCLIC CODE OVER THE RING R

Here, the structure of λ-constacyclic code over the ring R will be discussed, where λ = 1+bu, 1+cv, 1+bu+duv, 1+cv+duv, 1+bu+cv, 1+bu+cv+duv, b, c, d ≠ 0 and b, c, d∈F_{p^m}.

Firstly, the (1+bu)-constacyclic code over the ring R of length p^s will be studied. Obviously, (1+bu)-constacyclic code over the ring R of length p^s are ideals over:

$$R_{1+bu} = \frac{R_{(p,m)}[x]}{\langle x^{p^s} - (1+bu) \rangle}$$

The following lemma will be verified easily.

Lemma 1: The following proposition are true in R_{1+bu}:

- For any nonnegative integer t, then $(x-1)^{p^t} = x^{p^t} - 1$. In particular, $(x-1)^{p^s} = bu$.
- x-1 is nilpotent with the nilpotency index $2p^s$.

Lemma 2: Let f(x) ∈ R_{1+bu}. Then f(x) can be uniquely expressed as:

$$f(x) = \sum_{j=0}^{2p^s-1} a_{0j}(x-1)^j + v\sum_{j=0}^{2p^s-1} a_{1j}(x-1)^j$$

where, $a_{0j}, a_{1j} \in F_{p^m}$. Furthermore, f (x) is invertible if and only if $a_{00} \neq 0$.

Proof: Because any element r in R can be presented as $r = r_1 + ur_2 + vr_3 + uvr_4$, where, $r_1, r_2, r_3, r_4 \in F_{p^m}$ then any element f (x) in R_{1+bu} can be uniquely represented as:

$$f(x) = \sum_{j=0}^{2p^s-1} b_{0j}(x-1)^j + u\sum_{j=0}^{2p^s-1} b_{1j}(x-1)^j + v\sum_{j=0}^{2p^s-1} b_{2j}(x-1)^j + uv\sum_{j=0}^{2p^s-1} b_{3j}(x-1)^j.$$

Since $(x-1)^{p^s} = bu$ in R_{1+bu}, then f (x) can be uniquely expressed as:

$$f(x) = \sum_{j=0}^{2p^s-1} a_{0j}(x-1)^j + v\sum_{j=0}^{2p^s-1} a_{1j}(x-1)^j$$

where, a_{0j}, a_{1j}, ∈ F_p. Because v and x-1 are both nilpotent in R_{1+bu}, so f (x) is invertible if and only if $a_{00} \neq 0$.

Lemma 3: R_{1+bu} is a local ring with the maximal ideal <v, x-1> but it is not a chain ring.

Proof: By lemma 2, the ideal <v, x-1> is the set of all non-invertible elements of R_{1+bu}. Then R_{1+bu} is a local ring with maximal ideal <v, x-1>. If v∈< x-1> Then there must exist f_1 (x) and f_2 (x) ∈ R [x] such that:

$$v = (x-1)f_1(x) + (x^{p^s} - (1+bu))f_2(x)$$

Let x = 1, then v = -bu which is a contradiction. Hence, v∉<x-1>. On the other hand, if x-1∈<v>, then $(x-1)^2 = 0$ which is also a contradiction. So x-1∉<v>. Therefore, the maximal ideal <v, x-1> is not principal in R_{1+bu}. So, R_{1+bu} is not a chain ring.

Theorem 4: (1+bu)-constacyclic codes of length p^s over R are ideals of the ring R_{1+bu} with any one of the following four forms:

Form 1: <0>, <1>
Form 2: I = <v $(x-1)^k$ >, where $0 \le k \le 2p^s-1$

Form 3:

$$I = < (x-1)^l + v\sum_{j=0}^{l-1} c_{1j}(x-1)^j >$$

where, $1 \le l \le 2p^s-1$

Form 4:

$$I = < (x-1)^l + v\sum_{j=0}^{w-1} c_{1j}(x-1)^j, v(x-1)^w >$$

where $1 \le l \le 2p^s-1$, $w \le l$

Proof: Ideals of Form 1 are the trivial ideals. Next, any nontrivial ideal I over the ring R_{1+bu} will be considered.

Case 1: $I \subseteq <v>$. Then, any element of I has the form:

$$v\sum_{j=0}^{2p^s-1} a_{0j}(x-1)^j$$

where, $a_{0j} \in F_{p^m}$. Let b (x) $\in$ I with the smallest integer k such that $a_{0k} \neq 0$. Hence all element a (x) in I have the form:

$$a(x) = v(x-1)^k \sum_{j=k}^{2p^s-1} a_{0j}(x-1)^{j-k}$$

which implies $I \subseteq < u(x-1)^k >$. On the other hand, if b (x) $\in$I then:

$$b(x) = v(x-1)^k [a_{0k} + \sum_{j=k+1}^{2p^s-1} a_{0j}(x-1)^{j-k}]$$

Because $a_{0k} \neq 0$, then:

$$a_{0k} + \sum_{j=k+1}^{2p^s-1} a_{0j}(x-1)^{j-k}$$

is an invertible element in R_{1+bu}. So v $(x-1)^k \in I$, which implies that the ideal of R_{1+bu} contained in <v> is $< v(x-1)^k >, 0 \le k \le 2p^s-1$. Hence, I is in Form 2.

Case 2: $I \subseteq <v>$ Any element of I must have the form:

$$\sum_{j=0}^{2p^s-1} a_{0j}(x-1)^j + v\sum_{j=0}^{2p^s-1} a_{1j}(x-1)^j$$

and there exists a polynomial:

$$\sum_{j=0}^{2p^s-1} b_{0j}(x-1)^j + v\sum_{j=0}^{2p^s-1} b_{1j}(x-1)^j$$

in I such that:

$$\sum_{j=0}^{2p^s-1} b_{0j}(x-1)^j \neq 0$$

Let:

$$M = \{\sum_{j=0}^{2p^s-1} a_{0j}(x-1)^j + v\sum_{j=0}^{2p^s-1} a_{1j}(x-1)^j \in I \,\Big|\, \sum_{j=0}^{2p^s-1} a_{0j}(x-1)^j \neq 0, a_{0j}, a_{1j} \in F_{p^m}\}$$

$$N = \{v\sum_{j=0}^{2p^s-1} a_{1j}(x-1)^j \in I \,\Big|\, a_{1j} \in F_{p^m}\}$$

Setting δ = min {deg (m (x))|m (x)$\in$M} and H = {h (x)$\in$M|deg (h (x)) = δ}. Then, there exist an element:

$$h_1(x) = \sum_{j=0}^{2p^s-1} h_{0j}(x-1)^j + v\sum_{j=0}^{2p^s-1} h_{1j}(x-1)^j$$

in H with the smallest l such that $h_{0l} \neq 0$. Hence:

$$h_l(x) = (x-1)^l [h_{0l} + \sum_{j=l+1}^{2p^s-1} h_{0j}(x-1)^{j-l}] + v\sum_{j=0}^{2p^s-1} h_{1j}(x-1)^j \in M \subset I$$

Two sub-cases can be obtained in the following.

Sub-case 2.1: $N \subseteq <h_1(x)>$. For f (x) $\in$ M, by the division algorithm, f (x) can be written as:

$$f(x) = q(x)h_1(x) + r(x)$$

where, q (x), r (x) $\in$ R_{1+bu} and r (x) = 0 or deg (r (x))<deg (h_1 (x)). Suppose r (x) $\notin$ N Then r (x)$\neq$0. Hence r (x) = f (x)-q (x)h_1 (x)$\in$M which contradicts the assumption of h_1 (x). Then r (x)$\in$N So, I = <h_1 (x)>. Therefore:

$$vh_1(x) = v(x-1)^l [h_{0l} + \sum_{j=l+1}^{2p^s-1} h_{1j}(x-1)^{j-l}] \in I$$

and:

$$h_{0l} + \sum_{j=l+1}^{2p^s-1} h_{0j}(x-1)^{j-t}$$

is an invertible element in R_{1+bu}, then v $(x-1)^l \in$ I hence:

$$\tilde{h}_l(x) = (x-1)^l [h_{0l} + \sum_{j=l+1}^{2p^s-1} h_{0j}(x-1)^{j-l}] + v\sum_{j=0}^{l-1} h_{1j}(x-1)^j \in I$$

Let:

$$c(x)=\tilde{h}_l(x)[h_{0l}+\sum_{j=l+1}^{2p^s-1}h_{0j}(x-1)^{j-l}]^{-1}\in I$$

and c (x) can be expressed as:

$$c(x)=(x-1)^l+v\sum_{j=0}^{l-1}c_{lj}(x-1)^j$$

where, $c_{lj}\in F_{p^m}$ Therefore:

$$I=<(x-1)^l+v\sum_{j=0}^{l-1}c_{lj}(x-1)^j>$$

where, $1\le l\le 2p^s$ Hence I is in Form 3.

Sub-case 2.2: $N\subseteq<h_l(x)>=<c(x)>$. For any $n(x)\in N$, then there exist the smallest integer w such that $n(x)=v(x-1)^w n_1(x)$, where $n_1(x)\in R_{1+bu}$.

Obviously, $v(x-1)^w$ but $v(x-1)^w\notin<h_l(x)>=<c(x)>$. So:

$$I=<(x-1)^l+v\sum_{j=0}^{l-1}c_{lj}(x-1)^j, v(x-1)^w>$$

Suppose w>1, Then:

$$v(x-1)^w=v(x-1)^{w-1}[(x-1)^l+v\sum_{j=0}^{l-1}c_{lj}(x-1)^j]\in<c(x)>$$

which is a contradiction. Thus:

$$I=<(x-1)^l+v\sum_{j=0}^{w-1}c_{lj}(x-1)^j, v(x-1)^w>$$

where $1\le l\le 2p^s-1$, $w\le l$. So, I is in Form 4.

Similar to the discussion in theorem 4, the following theorems will be obtained easily.

Theorem 5: (1+bu+duv), (1+bu+cv+duv), (1+bu+cv+duv)- constacyclic codes of length p^s over R are:

Form 1: <0>, <1>
Form 2: $I=<v(x-1)^k>$, where $0\le k\le 2p^s-1$
Form 3:

$$I=<(x-1)^l+v\sum_{j=0}^{l-1}c_{lj}(x-1)^j>$$

where $1\le l\le 2p^s-1$

Form 4:

$$I=<(x-1)^l+v\sum_{j=0}^{l-1}c_{lj}(x-1)^j, v(x-1)^w>$$

where, $1\le l\le 2p^s-1$, $w\le l$

Theorem 6: (1+cv) (1+cv+duv)-constacyclic codes of length p^s over R are:

Form 1: <0>, <1>
Form 2: $I=<u(x-1)^k>$, where $0\le k\le 2p^s-1$
Form 3:

$$I=<(x-1)^l+u\sum_{j=0}^{l-1}c_{lj}(x-1)^j>$$

where $0\le l\le 2p^s-1$

Form 4:

$$I=<(x-1)^l+u\sum_{j=0}^{l-1}c_{lj}(x-1)^j, u(x-1)^w>$$

where $0\le l\le 2p^s-1$, $w\le l$.

Λ-CONSTACYCLIC CODE OVER THE RING R

In this section, Λ-constacyclic code over the ring R of length p^s will be discussed, where Λ = a+bu, a+cv, a+bu+duv, a+cv+duv, a+bu+cv, a+bu+cv+duv and:

$$a,b,c,d\in F_{p^m}, a\ne 0, b\ne 0, c\ne 0, d\ne 0$$

The (a+bu)-constacyclic code over the ring R of length p^s will be firstly discussed. Obviously, (a+bu)-constacyclic code over the ring R of length p^s are ideals over the residue class ring:

$$R_{a+bu}=\frac{R[x]}{<x^{p^s}-(a+bu)>}$$

Since s and m are two positive integers, by means of the division algorithm, there exists nonnegative integer a_q and a_r such that $s=a_q m+a_r$ where $0\le a_r\le m-1$. Let:

$$\alpha_0=a^{-p^{(a_q+1)m-s}}=a^{-p^{m-a_r}}$$

then:

$$\alpha_0^{p^s}=a^{-p^{(a_q+1)m}}=a^{-1}$$

Property 7: Define map Φ: $R_{a+bu}\to R_{1+a^{-1}bu}$ by $\Phi(f(x))=f(\alpha_0 x)$. Then Φ is a ring isomorphism.

Proof: For any f (x), g (x) ∈ R [x] then:

$$f(x) \equiv g(x)(\bmod x^{p^s} - (1 + a^{-1}bu))$$

if and only if there exist h (x) ∈ R [x] such that:

$$f(x) - g(x) = h(x)(x^{p^s} - (1 + a^{-1}bu))$$

if and only if:

$$f(\alpha_0 x) - g(\alpha_0 x) = h(\alpha_0 x)(\alpha_0 x)^{p^s} - (1 + a^{-1}bu)) = a^{-1}h(\alpha_0 x)(x^{p^s} - (a + bu))$$

which is equivalent to:

$$f(\alpha_0 x) \equiv g(\alpha_0 x)(\bmod x^{p^s} - (a + bu))$$

From the above, for any $f(x), g(x) \in R_{1+a^{-1}bu}$, then Φ (f (x)) = Φ (g (x)) if and only if f (x) = g (x). So Φ is well defined and one to one. Obviously, Φ is a onto mapping. It is easy to be proved that Φ is a ring homomorphism. Thus Φ is a ring isomorphism.

By property 7, the following corollary is easy to be get.

Corollary 8: Let:

$$A \subseteq R_{1+a^{-1}bu}, B \subseteq R_{a+bu}$$

and Φ (A) = B. Then A is the ideal of the residue class ring $R_{1+a^{-1}bu}$ if and only if B is the ideal of the residue class ring R_{a+bu}. Namely, A is the $1+a^{-1}bu$-constacyclic codes of length p^s over R if and only if B is the a+bu-constacyclic codes of length p^s over R.

By the ring isomorphism Φ, the corollary 8 and the theorem 4, the structure of the (a+bu)-constacyclic codes of length p^s over R can be obtained easily.

Theorem 9: (a+bu)-constacyclic codes of length p^s over R are:

Form 1: <0>, <1>
Form 2: I = <v $(\alpha_0 x-1)^k$>, where $0 \le k \le 2p^s-1$
Form 3:

$$I = \langle (\alpha_0 x - 1)^l + v\sum_{j=0}^{l-1} c_{lj} (\alpha_0 x - 1)^j \rangle$$

where $1 \le l \le 2p^s-1$

Form 4:

$$I = \langle (\alpha_0 x - 1)^l + v\sum_{j=0}^{w-1} c_{lj} (\alpha_0 x - 1)^j, v(\alpha_0 x - 1)^w \rangle$$

where $1 \le l \le 2p^s-1$, $w \le l$

Similar to the above discussion and combining the theorem 5 and the theorem 6, the structure of (a+bu+cv), (a+bu+cv+duv), (a+cv), (a+cv+duv)-constacyclic codes of length p^s over R will be given.

Theorem 10: (a+bu+duv), (a+bu+cv), (a+bu+cv+duv)-constacyclic codes of length p^s over R are:

Form 1: <0>, <1>
Form 2: I = <v $(\alpha_0 x-1)^k$> where $0 \le k \le 2p^s-1$
Form 3:

$$I = \langle (\alpha_0 x - 1)^l + v\sum_{j=0}^{l-1} c_{lj} (\alpha_0 x - 1)^j \rangle$$

where $1 \le l \le 2p^s-1$

Form 4:

$$I = \langle (\alpha_0 x - 1)^l + v\sum_{j=0}^{l-1} c_{lj} (\alpha_0 x - 1)^j, v(\alpha_0 x - 1)^w \rangle$$

where $1 \le l \le 2p^s-1$, $w \le l$

Theorem 11: (a+cv), (a+cv+duv)-constacyclic codes of length p^s over R are:

Form 1: <0>, <1>
Form 2: I = <u $(\alpha_0 x-1)^k$>, where $0 \le k \le 2p^s-1$
Form 3:

$$I = \langle (\alpha_0 x - 1)^l + u\sum_{j=0}^{l-1} c_{lj} (\alpha_0 x - 1)^j \rangle$$

where $1 \le l \le 2p^s-1$

Form 4:

$$I = \langle (\alpha_0 x - 1)^l + u\sum_{j=0}^{l-1} c_{lj} (\alpha_0 x - 1)^j, u(\alpha_0 x - 1)^w \rangle$$

where $1 \le l \le 2p^s-1$, $w \le l$

CONCLUSION

In this study, two classes of constacyclic codes over the ring $F_{p^m} + uF_{p^m} + vF_{p^m} + uvF_{p^m}$ of length p^s have been studied by using ideals over the residue ring. Another direction of research about this topic are the structure of cyclic and negacyclic codes of length p^s over this ring.

ACKNOWLEDGMENT

This study is supported by Science and Technology Research Project of the 2013 Hubei Provincial Department of Education under Grant No. B2013069.

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.

Dinh, H.Q., 2009. Constacyclic codes of length 2^s over Galois exlension rings of $BBF_2 + uBBF_2$. IEEE Trans. Inform. Theor., 55: 1730-1740.

Dinh, H.Q., 2010. Constacyclic codes of length p^s over $F_p^m+uF_p^m$. J. Algebra, 324: 940-950.

Dinh, H.Q. and H.D.T. Nguyen, 2012. On some classes of constacyclic codes over polynomial residue rings. Adv. Math. Commun., 6: 175-191.

Kanwar, P. and S.R. Lopez-Permouth, 1997. Cyclic codes over the integers modulop^m. Finite Fields Their Appl., 3: 334-352.

Wolfman, J., 1999. Negacyclic and cyclic codes over Z_4. IEEE Trans. Inform. Theory, 45: 2527-2532.

Xu, X. and X. Liu, 2011. On the structure of cyclic codes over $F_q+uF_q+vF_q+uvF_q$. Wuhan Univ. J. Nat. Sci., 16: 457-460.

Yildiz, B. and S. Karadeniz, 2010. Linear codes over $F_2+uF_2+vF_2+uvF_2$. Designs Codes Cryptogr., 54: 61-81.

Yildiz, B. and S. Karadeniz, 2011. Cyclic codes over $F_2+uF_2+vF_2+uvF_2$. Designs Codes Cryptogr., 58: 221-234.