Two Classes of Repeat–Root Constacyclic Codes of Length $p^s$ Over the Ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + v\mathbb{F}_{p^m} + uv\mathbb{F}_{p^m}$

1Xiaofang Xu and 2Shujie Yun
1School of Mathematics and Physics, Hubei Polytechnic University, Huangshi, 435003, China
2Department 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 of constacyclic codes of length $p^s$ over the ring $\mathbb{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + v\mathbb{F}_{p^m} + uv\mathbb{F}_{p^m}$ are discussed. Let $\lambda = a + bu + cv + du, \ a \neq 0, \ b \neq 0, \ c \neq 0, \ d \neq 0$, then $\lambda$ and $\Lambda$ are units in $\mathbb{R}$. Firstly, by studying ideals of the residue class ring $\frac{\mathbb{R}[x]}{\langle x^s - \lambda \rangle}$, the structure of all $\lambda$-constacyclic codes over $\mathbb{R}$ can be obtained. Then, the ring isomorphism $\Phi$ from the residue class ring $\frac{\mathbb{R}[x]}{\langle x^s - \lambda \rangle}$ to the residue class ring $\frac{\mathbb{R}[x]}{\langle x^s - \Lambda \rangle}$ will be defined. Finally, by using the ring isomorphism $\Phi$, the structure of all $\Lambda$-constacyclic codes over $\mathbb{R}$ 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-Permouh, 2004; Wolfman, 1999; Kanwar and Lopez-Permouh, 1997). The repeat-root constacyclic codes of length $2^p$ over $\mathbb{F}_2 + u\mathbb{F}_2$ have been studied by Dinh (2009). All repeat-root constacyclic codes of length $p^s$ over $\mathbb{F}_p + u\mathbb{F}_p$ have been studied by Dinh (2010). One class of the repeat-root constacyclic codes of length $2^s$ over $\mathbb{F}_2 + u\mathbb{F}_2$ 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 $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ have been studied by Yildiz and Karadeniz (2010, 2011), where the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ is a finite non-chain ring. The cyclic code over the finite non-chain ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ 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 $\mathbb{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + v\mathbb{F}_{p^m} + uv\mathbb{F}_{p^m}$ will be studied. Firstly, by studying the residue class ring $\frac{\mathbb{R}[x]}{\langle x^s - \lambda \rangle}$, the structure of all $\lambda$-constacyclic codes over $\mathbb{R}$ will be obtained. Finally, by using the ring isomorphism $\Phi$ from the residue class ring $\frac{\mathbb{R}[x]}{\langle x^s - \lambda \rangle}$ to the residue class ring $\frac{\mathbb{R}[x]}{\langle x^s - \Lambda \rangle}$, the structure of all $\Lambda$-constacyclic codes over $\mathbb{R}$ will be established.

BASIC CONCEPTS OF REPEAT-ROOT
CONSTACYCLIC CODES

$\mathbb{F}_p$ is a finite field containing $p^m$ elements where $p$ is any prime number and $m$ is an arbitrary positive integer. Let:

$R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + v\mathbb{F}_{p^m} + uv\mathbb{F}_{p^m} = \{a+ub+cv+du | a, b, c, d \in \mathbb{F}_p\}$

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.
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.:

$$P(C) = \sum_{i=0}^{n-1} c_{i,n} \mathbf{e}_i | (c_{i,n}, c_{i,n-1}, \ldots, c_{i,1}) \in C$$

For a unit $\alpha$ of $R$, the $\alpha$-constacyclic ($\alpha$-twisted) shift $\tau_\alpha$ on $R^n$ is the shift:

$$\tau_\alpha(a_0, a_1, \ldots, a_{n-1}) = (\alpha a_{n-1}, a_0, \ldots, a_{n-2})$$

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

$$R[x] \triangleleft_{\alpha - \lambda} R$$

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

$$R[x] \triangleleft_{x - \lambda} R$$

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

$$R[x] \triangleleft_{x^2 - \lambda} R$$

**$\lambda$-CONSTACYCLIC CODE OVER THE RING $R$**

Here, the structure of $\lambda$-constacyclic code over the ring $R$ will be discussed, where $\lambda = 1 + bu$, $1 + cv$, $1 + bu + dnu$, $1 + cu + dnu$, $1 + bu + cv$, $1 + bu + dnu + cv + dnu$, $b, c, d \neq 0$ and $b, c, d \in F_p$.

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

$$R_{1+bu} = R_{1+bu}[x] \triangleleft_{x^p - (1 + bu)x} R_{1+bu}$$

The following lemma will be verified easily.

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

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

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

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

where, $a_{j}, b_{j} \in F_p$. Furthermore, $f(x)$ is invertible if and only if $a_{0} \neq 0$.

**Proof:** Because any element $r$ in $R$ can be represented as $r = r_1 + ur_2 + vr_3 + ur_1$, where, $r_1, r_2, r_3 \in F_p$, then any element $f(x)$ in $R_{1+bu}$ can be uniquely represented as:

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

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

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

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

**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 $v \neq <x-1>$, then there must exist $f_1(x)$ and $f_2(x) \in R[x]$ such that:

$$v = (x-1)f_1(x) + (x^t - (1 + bu))f_2(x)$$

Let $x - 1$, then $v = -bu$ which is a contradiction. Hence, $v \neq <x-1>$. On the other hand, if $x-1 \notin <v>$, then $(x-1)^t = 0$ which is also a contradiction. So $x-1 \notin <v>$. 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 $p^t$ over $R$ are ideals of the ring $R_{1+bu}$ with any one of the following four forms:

**Form 1:** $<p, <1>$

**Form 2:** $I = f(x-1)$, where $0 < k < 2p^t - 1$
Form 3:

\[ l = \langle (x-1)^i + \sum_{j=0}^{3^i} c_{ij} (x-1)^j \rangle \]

where, \( 1 \leq i \leq 2p^i - 1 \)

Form 4:

\[ l = \langle (x-1)^i + \sum_{j=0}^{3^i-1} c_{ij} (x-1)^j, v(x-1)^v \rangle \]

where \( 1 \leq i \leq 2p^i - 1, v \leq 1 \)

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

Case 1: \( I \subseteq \langle v \rangle \). Then, any element of I has the form:

\[ v \sum_{j=0}^{3^i-1} a_{ij} (x-1)^j \]

where, \( a_{ij} \in F_p \). Let \( b(x) \in I \) with the smallest integer \( k \) such that \( a_{00} \neq 0 \). Hence all element \( a(x) \) in I have the form:

\[ a(x) = v(x-1)^i \sum_{j=0}^{3^i-1} a_{ij} (x-1)^{i+k} \]

which implies \( I \subseteq \langle u(x-1)^i \rangle \). On the other hand, if \( b(x) \in I \) then:

\[ b(x) = v(x-1)^i [a_{00} + \sum_{j=0}^{3^i-1} a_{ij} (x-1)^{i+k}] \]

Because \( a_{00} \neq 0 \), then:

\[ a_{00} + \sum_{j=0}^{3^i-1} a_{ij} (x-1)^{i+k} \]

is an invertible element in \( R_{x+u} \). So \( v(x-1)^i \in I \), which implies that the ideal of \( R_{x+u} \) contained in \( \langle v \rangle \) is \( \langle v(x-1)^i \rangle \), \( 0 \leq k \leq 2p^i - 1 \). Hence, I is in Form 2.

Case 2: \( I \subseteq \langle v \rangle \) Any element of I must have the form:

\[ \sum_{j=0}^{3^i-1} a_{ij} (x-1)^j + v \sum_{j=0}^{3^i-1} a_{ij} (x-1)^j \]

and there exists a polynomial:

\[ \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j + v \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j \]

in I such that:

\[ \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j \neq 0 \]

Let:

\[ M = \{ \sum_{j=0}^{3^i-1} a_{0j} (x-1)^j + v \sum_{j=0}^{3^i-1} a_{ij} (x-1)^j \in I \mid \sum_{j=0}^{3^i-1} a_{0j} (x-1)^j \neq 0, a_{0j}, a_{ij} \in F_p \} \]

\[ N = \langle v \sum_{j=0}^{3^i-1} a_{ij} (x-1)^j \rangle \subseteq I \]

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

\[ h(x) = \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j + v \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j \]

in \( H \) with the smallest \( l \) such that \( h_{00} \neq 0 \). Hence:

\[ h(x) = (x-1)^i \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j + v \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j \in M \subseteq I \]

Two sub-cases can be obtained in the following.

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

\[ f(x) = q(x) h(x) + r(x) \]

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

\[vh(x) = v(x-1)^i \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j \in I \]

and:

\[ h_{00} + \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j \]

is an invertible element in \( R_{x+u} \). Then \( v(x-1)^x \notin I \) hence:

\[ \tilde{h}(x) = (x-1)^i \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j + v \sum_{j=0}^{3^i-1} b_{0j} (x-1)^j \]

Let:
\[ c(x) = h_0(x)[h_a + \sum_{i=0}^{2p-1} h_i (x-1)^i] \in \mathbb{R} \]

and \( c(x) \) can be expressed as:
\[ c(x) = (x-1)^l + v \sum_{i=0}^{2p-1} c_i (x-1)^i \]

where, \( c_i \in F_p^* \). Therefore:
\[ I = \langle (x-1)^l + v \sum_{i=0}^{2p-1} c_i (x-1)^i \rangle \]

where, \( 1 \leq 2p^l \). Hence \( I \) is in Form 3.

**Sub-case 2.2:** \( \langle h_i(x) \rangle = \langle c(x) \rangle \). For any \( n(x) \in \mathbb{N} \), there exist a smallest integer \( n \) such that \( n(x) = v(x-1)^n \), \( n_i(x) \), where \( n_i \in R_{x_i \cdot \nu} \).

Observe, \( v(x-1)^{n_i} \) but \( v(x-1)^{n_i} \not\in \langle h_i(x) \rangle \). So:
\[ I = \langle (x-1)^l + v \sum_{i=0}^{2p-1} c_i (x-1)^i, v(x-1)^r \rangle \]

Suppose \( w \geq 1 \), then:
\[ v(x-1)^r - v(x-1)^{r+1} + v \sum_{i=0}^{2p-1} c_i (x-1)^i \in \langle c(x) \rangle \]

which is a contradiction. Thus:
\[ I = \langle (x-1)^l + v \sum_{i=0}^{2p-1} c_i (x-1)^i, v(x-1)^r \rangle \]

where \( 1 \leq 2p^l \), \( w \leq 1 \). So, \( I \) is in Form 4.

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

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

**Form 1:** \( \langle 0 \rangle, \langle 1 \rangle \)

**Form 2:** \( I = \langle v(x-1)^l \rangle \), where \( 0 \leq k \leq 2p^l-1 \)

**Form 3:**
\[ I = \langle (x-1)^l + v \sum_{i=0}^{2p-1} c_i (x-1)^i \rangle \]

where \( 1 \leq 2p^l \)

**Form 4:**
\[ I = \langle (x-1)^l + v \sum_{i=0}^{2p-1} c_i (x-1)^i, v(x-1)^r \rangle \]

where, \( 1 \leq 2p^l-1, w \leq 1 \)

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

**Form 1:** \( \langle 0 \rangle, \langle 1 \rangle \)

**Form 2:** \( I = \langle u(x-1)^l \rangle \), where \( 0 \leq k \leq 2p^l-1 \)

**Form 3:**
\[ I = \langle (x-1)^l + u \sum_{i=0}^{2p-1} c_i (x-1)^i \rangle \]

where \( 0 \leq 2p^l-1 \)

**Form 4:**
\[ I = \langle (x-1)^l + u \sum_{i=0}^{2p-1} c_i (x-1)^i, u(x-1)^r \rangle \]

where \( 0 \leq 2p^l-1, w \leq 1 \)

**Λ-CONSTACYCLIC CODE OVER THE RING \( R \)**

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

\[ a, b, c, d \in F_p, a \neq 0, b \neq 0, c \neq 0, d \neq 0 \]

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

\[ R_{x^m} = \frac{R[\langle x \rangle]}{\langle x^m \rangle} \]

Since \( s \) and \( m \) are two positive integers, by means of the division algorithm, there exists nonnegative integer \( a \), and \( a_i \) such that \( s = a_i \cdot m + a \), where \( 0 \leq a_i \leq m-1 \). Let:

\[ α_0 = a_i^{v+1}, α_0^{-1} = a_i^{-v} \]

then:
\[ α_0^q = a_i^{v+1} = a_i \]

**Property 7:** Define map \( Φ: R_{x^m} \rightarrow R_{x^m}^{-1}bu \) by \( Φ(f(x)) = f(α,x) \). Then \( Φ \) is a ring isomorphism.
Proof: For any \( f(x), \ g(x) \in R[x] \) then:
\[
f(x) = g(x)(\mod x^d - 1 + a \cdot bu)
\]
if and only if there exist \( h(x) \in R[x] \) such that:
\[
f(x) - g(x) = h(x)(x^d - 1 + a \cdot bu)
\]
if and only if:
\[
f(a_0 x) - g(a_0 x) = h(a_0 x)(a_0 x)^d - (1 + a \cdot bu) = a^{-1}h(a_0 x)(x^d - (a + bu))
\]
which is equivalent to:
\[
f(a_0 x) = g(a_0 x)(\mod x^d - (a + bu))
\]

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

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

Corollary 8: Let:
\[
A \subseteq R_{a \cdot bu}, \ B \subseteq R_{a \cdot bu}
\]
and \( \Phi(A) = B \). Then \( A \) is the ideal of the residue class ring \( R_{a \cdot bu} \) if and only if \( B \) is the ideal of the residue class ring \( R_{a \cdot bu} \). Namely, \( A \) is the \( l + a \cdot bu \)-constacyclic codes of length \( p' \) over \( R \) if and only if \( B \) is the \( a + bu \)-constacyclic codes of length \( p' \) over \( R \).

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

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

Form 1: \( <0>, <1> \)
Form 2: \( I = \langle (a_0 x - 1)^i \rangle \), where \( 0 \leq k \leq 2p' - 1 \)
Form 3:
\[
I = \langle (a_0 x - 1)^i + \sum_{j=0}^{i-1} c_j (a_0 x - 1)^j \rangle
\]
where \( 1 \leq l \leq 2p' - 1 \)
Form 4:
\[
I = \langle (a_0 x - 1)^i + \sum_{j=0}^{w - 1} c_j (a_0 x - 1)^j, v(a_0 x - 1)^w \rangle
\]
where \( 1 \leq l \leq 2p' - 1, w \leq l \)

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 \( p' \) over \( R \) will be given.

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

Form 1: \( <0>, <1> \)
Form 2: \( I = \langle (a_0 x - 1)^i \rangle \), where \( 0 \leq k \leq 2p' - 1 \)
Form 3:
\[
I = \langle (a_0 x - 1)^i + \sum_{j=0}^{i-1} c_j (a_0 x - 1)^j \rangle
\]
where \( 1 \leq l \leq 2p' - 1 \)
Form 4:
\[
I = \langle (a_0 x - 1)^i + \sum_{j=0}^{w - 1} c_j (a_0 x - 1)^j, v(a_0 x - 1)^w \rangle
\]
where \( 1 \leq l \leq 2p' - 1, w \leq l \)

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

Form 1: \( <0>, <1> \)
Form 2: \( I = \langle (a_0 x - 1)^i \rangle \), where \( 0 \leq k \leq 2p' - 1 \)
Form 3:
\[
I = \langle (a_0 x - 1)^i + \sum_{j=0}^{i-1} c_j (a_0 x - 1)^j \rangle
\]
where \( 1 \leq l \leq 2p' - 1 \)
Form 4:
\[
I = \langle (a_0 x - 1)^i + \sum_{j=0}^{w - 1} c_j (a_0 x - 1)^j, v(a_0 x - 1)^w \rangle
\]
where \( 1 \leq l \leq 2p' - 1, w \leq l \)

CONCLUSION

In this study, two classes of constacyclic codes over the ring \( F_p + uF_p + vF_p + uvF_p \) of length \( p' \) 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 \( p' \) 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


