ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.10, 8511–8524
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.10.78

SOME RESULTS ON CYCLIC AND NEGACYCLIC CODES OVER FORMAL POWER SERIES RINGS AND FINITE CHAIN RINGS

MRIGANKA S. DUTTA[1] AND HELEN K. SAIKIA

ABSTRACT. In this article, relationship between cyclic codes of composite length mn over formal power series ring and $u-$constacyclic code of length m over $\frac{R_\infty[x]}{<x^n-1>}$ has been established by constructing an isomorphism. For two odd numbers m and n, relationship between $u-$constacyclic code of length m over $\frac{R_\infty[x]}{<x^n-1>}$ and $u-$constacyclic code of length m over $\frac{R_\infty[x]}{<x^n+1>}$ has been obtained. The ideals of the rings $\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}$ and $\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>}$ have also been determined.

1. INTRODUCTION

Due to the rich algebraic structure, cyclic codes play an important role in coding theory as seen in [1, 7]. Initially, the researchers studied the properties of Cyclic codes over the binary field $\mathbb{F}_2$, then they extended the study to $\mathbb{F}_q$ with $q = p^r$ for some prime p and $r \geq 1$. The structure of cyclic codes was obtained by viewing a cyclic code C of length n over a finite field $\mathbb{F}_q$ as an ideal of the ring $\frac{\mathbb{F}_q[x]}{<x^n-1>}$. Dinh and Lopez-Permouth [2] in the year 2004 published a paper on structure of cyclic and negacyclic codes over finite chain rings. Dougherty, Liu, and Park [5] in 2011 defined a series of finite chain rings and introduced the concept of $\gamma-$adic codes over formal power series rings. In 2011 Dougherty and Liu [4] have given the concept of $\lambda-$cyclic code of length n over formal

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 94B15.
Key words and phrases. Cyclic codes, Constacyclic shift, Formal power series ring, Isomorphism.

power series rings. They established a relation between cyclic codes and negacyclic codes over formal power series rings. They obtained a relation between cyclic codes over formal power series rings and cyclic codes over finite chain rings. Dougherty and Ling [3] in the year 2006 proved that a cyclic shift in $\mathbb{Z}_4^{2^k n}$ corresponds to a $u-$constacyclic shift in $(\frac{\mathbb{Z}_4[u]}{<u^{2^k}-1>})^n$ by constructing a module isomorphism between $(\frac{\mathbb{Z}_4[u]}{<u^{2^k}-1>})^n$ and $\mathbb{Z}_4^{2^k n}$. Dutta and Saikia [6] have introduced the concept of $\Phi_{\lambda l}-$cyclic code of length n over a formal power series ring and derived some related results. Sobhani and Molakarimi [8] in the year 2013 constructed a one-to-one correspondence between cyclic codes of length $2n$ over the ring $R_{k-1,m}$ and cyclic codes of length n over the ring $R_{k,m}$ for odd n and determined the number of ideals of the ring $R_{2,m}$ and $R_{3,m}$. Hence in [8] they have obtained the number of cyclic codes of odd length over $R_{2,m}$ and $R_{3,m}$ as a corollary. In this article, we have constructed an isomorphism between $\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}$ and $\frac{R_\infty[x]}{<x^{mn}-1>}$ and proved that cyclic codes of composite length mn over the formal power series ring R_∞ corresponds to $u-$constacyclic code of length m over $\frac{R_\infty[x]}{<x^n-1>}$. Here, considering both m and n as odd numbers we have proved that $u-$constacyclic codes of length m over $\frac{R_\infty[x]}{<x^n-1>}$ corresponds to $u-$constacyclic code of length m over $\frac{R_\infty[x]}{<x^n+1>}$. Thus corresponding to every cyclic code of odd length mn over R_∞ there exists a negacyclic code of same length over R_∞. Finally, we have also determined the types of ideals of the ring $\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}$ as well as the ring $\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>}$ that will give us cyclic codes over R_∞ and R_i respectively.

2. Finite Chain Ring and Formal Power Series Ring

In this article, we assume that all rings are commutative with identity $1 \neq 0$.

Definition 2.1. *[4] Let R be a ring and I be an ideal of R. I is called a principal ideal if it is generated by a singleton set.*

Definition 2.2. *[4] A finite ring is called a chain ring if all its ideals are linearly ordered by inclusion.*

Theorem 2.1. *[4] All the ideals of a finite chain ring are principal.*

Remark 2.1. *Let R be a finite chain ring. As R is finite, it must have finitely many ideals. Again R is a chain ring. Thus all the ideals of R must be linearly ordered* *by inclusion. Hence every finite chain ring R has a unique maximal ideal. Let I be the unique maximal ideal of R. As all the ideals of R are principal, I must have some generator. Let γ be a generator of I.*

Definition 2.3. *[4] Let i be an arbitrary positive integer and $\mathbb{F}$ be a finite field. The ring R_i is a finite chain ring and is defined as*

$$R_i = \{a_0 + a_1\gamma + ... + a_{i-1}\gamma^{i-1} \mid a_i \in \mathbb{F}\},$$

where $\gamma^{i-1} \neq 0$, but $\gamma^i = 0$ in R_i. The operations over R_i are defined as follows:

$$\sum_{l=0}^{i-1} a_l\gamma^l + \sum_{l=0}^{i-1} b_l\gamma^l = \sum_{l=0}^{i-1}(a_l + b_l)\gamma^l;\ (\sum_{l=0}^{i-1} a_l\gamma^l).(\sum_{l=0}^{i-1} b_l\gamma^l) = \sum_{s=0}^{i-1}(\sum_{l+l'=s} a_l b_{l'})\gamma^s.$$

Definition 2.4. *[4] The ring R_∞ is called a formal power series ring which is defined as*

$$R_\infty = \mathbb{F}[[\gamma]] = \{\sum_{l=0}^{\infty} a_l\gamma^l \mid a_l \in \mathbb{F}\}.$$

Addition and multiplication over R_∞ are defined by extending the addition and multiplication of polynomials, namely, term-by-term addition

$$\sum_{l=0}^{\infty} a_l\gamma^l + \sum_{l=0}^{\infty} b_l\gamma^l = \sum_{l=0}^{\infty}(a_l + b_l)\gamma^l,$$

and the Cauchy product

$$(\sum_{l=0}^{\infty} a_l\gamma^l).(\sum_{l=0}^{\infty} b_l\gamma^l) = \sum_{s=0}^{\infty}(\sum_{l+l'=s} a_l b_{l'})\gamma^s.$$

Lemma 2.1. *[4] If a and b are any two elements of R_∞ such that both not zero, then the greatest common divisor $gcd(a,\ b)$ exists.*

Corollary 2.1. *[4] If $a_1,\ a_2, \dots,\ a_n\ \in\ R_\infty$ such that $a_j \neq 0$ for some $0 \leq\ J \leq\ n$, then the greatest common divisor $gcd(a_1,\ a_2, \dots, a_n)$ exists. If a_j is a unit for some j, then, $gcd(a_1,\ a_2, \dots,\ a_n) = 1$.*

Definition 2.5. *[4] Let $i,\ j$ be two integers with $i \leq j$. In [4], the mapping Ψ_i^j is defined by*

$$\Psi_i^j : R_j \longrightarrow R_i,\ \sum_{l=0}^{j-1} a_l\gamma^l \longmapsto \sum_{l=0}^{i-1} a_l\gamma^l.$$

Definition 2.6. *[4] Let i be any positive integer. In [4], the mapping Ψ_i is defined by*

$$\Psi_i : R_\infty \longrightarrow R_i,\ \sum_{l=0}^{\infty} a_l\gamma^l \longmapsto \sum_{l=0}^{i-1} a_l\gamma^l.$$

It can be proved that Ψ_i^j and Ψ_i are homomorphisms. We can extend Ψ_i^j naturally from R_j^n to R_i^n. Similarly Ψ_i can be extended naturally from R_∞^n to R_i^n.

3. Polynomial Rings over R_∞ and R_i

The polynomial ring over R_∞ is given by

$$R_\infty[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \ \in\ R_\infty,\ n\ \geq\ 0\}.$$

Since R_∞ is a domain, $R_\infty[x]$ is also a domain [4]. We shall consider a polynomial

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \ \in\ R_\infty[x].$$

We can define the following mapping:

$$\psi_j : R_\infty[x] \to R_j[x],\ f(x) \longmapsto \psi_j(f(x)),$$

where

$$\psi_j(f(x)) = \psi_j(a_0) + \psi_j(a_1)x + \cdots + \psi_j(a_n)x^n \ \in\ R_j[x].$$

Thus by projecting the coefficients of the elements in $R_\infty[x]$ onto the coefficients of the elements in $R_j[x]$, we got the ring of polynomials over R_j from the ring of polynomials over R_∞ [4].

Again we shall consider

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \ \in\ R_j[x].$$

Now we can define a mapping as follows:

$$\psi_i^j : R_j[x] \to R_i[x],\ f(x) \longmapsto \psi_i^j(f(x)),$$

where

$$\psi_i^j(f(x)) = \psi_i^j(a_0) + \psi_i^j(a_1)x + \cdots + \psi_i^j(a_n)x^n \ \in\ R_i[x].$$

Definition 3.1. *[4] If $f(x) \in R_\infty[x]$ such that $deg(f(x)) > 0$ and $gcd(a_1,\ a_2, \ldots,$ $a_n) = 1$, then $f(x)$ is called a primitive element.*

Lemma 3.1. *[4] If $f(x) \in R_\infty[x]$ such that $deg(f(x)) > 0$, then $f(x)$ is a primitive polynomial iff $\psi_i(f(x)) \neq 0 \; \forall \; i < \infty$.*

Theorem 3.1. *[4] If $f(x) \in R_\infty[x]$ such that $deg(f(x)) > 0$, then there exist a unique s and a primitive polynomial $g(x)$, such that $f(x) = \gamma^s g(x)$.*

Definition 3.2. *[4] If $< f(x) > + < g(x) >= R_i[x]$, then the polynomials $f(x),\ g(x) \in R_i[x]$ are called coprime, where $i < \infty$ or equivalently, if there exists $u(x), v(x) \in R_i[x]$ such that $f(x)u(x) + g(x)v(x) = 1$, then the polynomials $f(x), g(x) \in R_i[x]$ are called coprime.*

4. Linear, Cyclic and Negacyclic Codes

Definition 4.1. *[4] Let R be a ring and R^n be the $R-$module. A $R-$submodule C of R^n is called a linear code of length n over R.*

Note that in this study all codes are linear.

Definition 4.2. *[4] Let $x,\ y$ be vectors in R^n. The inner product of x and y is defined by*

$$[x, y] = x_1y_1 + x_2y_2 + ... + x_ny_n.$$

Definition 4.3. *[4] For a code C of leangth n over R, the dual code of C is defined by*

$$C^\perp = \{x\epsilon R^n | [x, c] = 0, \forall c\epsilon C\}.$$

Remark 4.1. *$C^\perp$ is linear whether or not C is linear.*

In our study p is the characteristic of the finite field $\mathbb{F}$. Thus p is prime. We assume that n is relatively prime to p.

Let λ be an arbitrary unit of R_∞ and let

$$\frac{R_\infty[x]}{< x^n - \lambda >} = \{f(x)+ < x^n - \lambda > | f(x) \in R_\infty[x]\}$$

Let

$$f(x)+ < x^n - \lambda >, g(x)+ < x^n - \lambda >\in \frac{R_\infty[x]}{< x^n - \lambda >},$$

such that $0 \leq deg(f(x)), deg(g(x)) < n$, and $f(x)+ < x^n - \lambda >= g(x)+ < x^n - \lambda >$. Then, we have $f(x) - g(x) \in< x^n - \lambda >$. Which implies that $f(x) = g(x)$ as R_∞ is a domain. Hence, for each $f(x)+ < x^n - \lambda >\in \frac{R_\infty[x]}{<x^n-\lambda>}$, there is a unique

$f(x)$ with $deg(f(x)) < n$. We can identify each coset $f(x)+ < x^n - \lambda >$ with its unique representative polynomial $f(x)$, where $deg(f(x)) < n$. That is,

$$\frac{R_\infty[x]}{< x^n - \lambda >} = \{f(x)+ < x^n - \lambda > |\text{where } deg(f(x)) < n \text{ or } f(x) = 0\}.$$

Let us define a mapping

$$P_\lambda : R_\infty^n \longrightarrow \frac{R_\infty[x]}{< x^n - \lambda >}$$

given by

$$(a_0, a_1, \ldots, a_{n-1}) \longmapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + < x^n - \lambda > .$$

Putting $\lambda = 1$ and $\lambda = -1$ we get P_1 and P_{-1} as follows:

$$P_1 : R_\infty^n \longrightarrow \frac{R_\infty[x]}{< x^n - 1 >}$$

given by

$$(a_0, a_1, \ldots, a_{n-1}) \longmapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + < x^n - 1 >,$$

and

$$P_{-1} : R_\infty^n \longrightarrow \frac{R_\infty[x]}{< x^n + 1 >}$$

given by

$$(a_0, a_1, \ldots, a_{n-1}) \longmapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + < x^n - 1 > .$$

Let C be an arbitrary subset of R_∞^n. We denote the image of C under the map P_λ by $P_\lambda(C)$. We use $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}$ to denote the image of $(a_0, a_1, \ldots, a_{n-1})$ under P_λ, P_1 and P_{-1} respectively ([4]).

Definition 4.4. *[4] Let C be a linear code of length n over R_∞. The code C is called a $\lambda-$cyclic code over R_∞, if*

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C \implies (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

If $\lambda = 1$ then C is called a cyclic code and if $\lambda = -1$, then C is called a negacyclic code, otherwise, it is called a constacyclic code. Thus

$$P_\lambda(C) = \{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + < x^n - \lambda > |(c_0, c_1, \ldots, c_{n-1}) \in C\}.$$

Now the following lemma can be easily proved.

Lemma 4.1. *[4] A linear code C of length n over R_∞ is a $\lambda-$cyclic code iff $P_\lambda(C)$ is an ideal of $\frac{R_\infty[x]}{<x^n - \lambda>}$*

From Lemma 4.1 we get the following corollary:

Corollary 4.1. *[4] Assuming the notations given above*
(i) *A linear code C of length n over R_∞ is a cyclic code iff $P_1(C)$ is an ideal of $\frac{R_\infty[x]}{<x^n-1>}$;*
(ii) *A linear code C of length n over R_∞ is a negacyclic code iff $P_{-1}(C)$ is an ideal of $\frac{R_\infty[x]}{<x^n+1>}$.*

Let us consider the following ring homomorphism:

$$\psi_i : \frac{R_\infty[x]}{< x^n - 1 >} \longrightarrow \frac{R_i[x]}{< x^n - 1 >}$$

given by

$$f(x) \longmapsto \psi_i(f(x)).$$

Since ψ_i is a ring homomorphism, therefore if I is an ideal of $\frac{R_\infty[x]}{<x^n-1>}$, then $\psi_i(I)$ is an ideal of $\frac{R_i[x]}{<x^n-1>}$.

Theorem 4.1. *[4] If C is a cyclic code over R_∞, then, $\psi_i(C)$ is a cyclic code over R_i for all $i < \infty$.*

Now we are going to establish an important result which is the central result of our present work. Let $\mathbb{F}$ be a finite field and p be the characteristic of $\mathbb{F}$. Thus p is a prime. Let $R_\infty = \mathbb{F}[[\gamma]] = \{\sum_{l=0}^{\infty} a_l \gamma^l | a_l \in \mathbb{F}\}$ be the formal power series ring over $\mathbb{F}$, where γ is the indeterminate. Let λ be an arbitrary unit of R_∞. If we consider m and n to be two positive integers relatively prime to p, then we have the following result:

Theorem 4.2. *Assuming the notations given above we have*

$$\frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{< x^m - u >} \cong \frac{R_\infty[x]}{< x^{mn} - \lambda >}.$$

Proof. Let us define a mapping $\Phi : \frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>} \longrightarrow \frac{R_\infty[x]}{<x^{mn}-\lambda>}$ given by

$$\Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j} u^i) x^j) = \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j} (x^m)^i) x^j.$$

Now for

$$a_{0,0} + a_{0,1}x + \cdots + a_{0,m-1}x^{m-1} + a_{1,0}x^m + a_{1,1}x^{m+1} + \cdots + a_{1,m-1}x^{2m-1}$$

$$+\cdots+a_{n-1,0}x^{m(n-1)}+\cdots+a_{n-1,m-1}x^{mn-1}\in\frac{R_\infty[x]}{<x^{mn}-\lambda>},$$

there exists

$$\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}a_{i,j}u^i)x^j\in\frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>}.$$

such that

$$\begin{aligned}
&\Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}a_{i,j}u^i)x^j)=\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}a_{i,j}(x^m)^i)x^j\\
=&\sum_{j=0}^{m-1}(a_{0,j}(x)^0+a_{1,j}x^m+\cdots+a_{n-1,j}x^{m(n-1)})x^j\\
=&a_{0,0}+a_{0,1}x+\cdots+a_{0,m-1}x^{m-1}+a_{1,0}x^m+a_{1,1}x^{m+1}\\
&+\cdots+a_{1,m-1}x^{2m-1}+\cdots+a_{n-1,0}x^{m(n-1)}\\
&+\cdots+a_{n-1,m-1}x^{mn-1}\in\frac{R_\infty[x]}{<x^{mn}-\lambda>}.
\end{aligned}$$

Therefore the mapping Φ is onto.

To prove Φ is one-one, we take

$$\begin{aligned}
&\Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}a_{i,j}u^i)x^j)=\Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}b_{i,j}u^i)x^j)\\
\implies&\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}a_{i,j}(x^m)^i)x^j=\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}b_{i,j}(x^m)^i)x^j\\
\implies&\sum_{j=0}^{m-1}(a_{0,j}(x)^0+a_{1,j}x^m+\cdots+a_{n-1,j}x^{m(n-1)})x^j\\
&=\sum_{j=0}^{m-1}(b_{0,j}(x)^0+b_{1,j}x^m+\cdots+b_{n-1,j}x^{m(n-1)})x^j\\
\implies&a_{0,0}+a_{0,1}x+\cdots+a_{0,m-1}x^{m-1}+a_{1,0}x^m+a_{1,1}x^{m+1}+\dots\\
&+a_{1,m-1}x^{2m-1}+\cdots+a_{n-1,0}x^{m(n-1)}+\cdots+a_{n-1,m-1}x^{mn-1}\\
&=b_{0,0}+b_{0,1}x+\cdots+b_{0,m-1}x^{m-1}+b_{1,0}x^m+b_{1,1}x^{m+1}+\dots\\
&+b_{1,m-1}x^{2m-1}+\cdots+b_{n-1,0}x^{m(n-1)}+\cdots+b_{n-1,m-1}x^{mn-1}
\end{aligned}$$

$$\Longrightarrow a_{0,0} = b_{0,0}, a_{0,1} = b_{0,1}, \ldots, a_{n-1,m-1} = b_{n-1,m-1}$$
$$\Longrightarrow \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}u^i)x^j = \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}u^i)x^j.$$

Thus Φ is one-one and hence it is a bijection.
Now for

$$\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}u^i)x^j, \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}u^i)x^j \in \frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>}$$

$$\Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}u^i)x^j + \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}u^i)x^j) = \Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}(a_{i,j}+b_{i,j})u^i)x^j)$$

$$\Longrightarrow \Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}u^i)x^j + \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}u^i)x^j) = \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1}(a_{i,j}+b_{i,j})(x^m)^i)x^j$$

$$\Longrightarrow \Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}u^i)x^j + \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}u^i)x^j) = \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}(x^m)^i)x^j$$
$$+ \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}(x^m)^i)x^j$$

$$\Longrightarrow \Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}u^i)x^j + \sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}u^i)x^j) = \Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} a_{i,j}u^i)x^j)$$
$$+ \Phi(\sum_{j=0}^{m-1}(\sum_{i=0}^{n-1} b_{i,j}u^i)x^j).$$

Hence Φ preserves addition.

Let us consider

$$a_{i,j}u^ix^j, b_{r,s}u^rx^s \in \frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>}.$$

Now we have

$$a_{i,j}u^ix^j.b_{r,s}u^rx^s = a_{i,j}.b_{r,s}u^{i+r}x^{j+s} \in \frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>},$$

$$\Phi(a_{i,j}u^ix^j).\Phi(b_{r,s}u^rx^s) = a_{i,j}.b_{r,s}x^{m(i+r)+j+s} \tag{4.1}$$

$$\Phi(a_{i,j}u^ix^j.b_{r,s}u^rx^s) = \Phi(a_{i,j}.b_{r,s}u^{i+r}x^{j+s}) = a_{i,j}.b_{r,s}x^{m(i+r)+j+s}. \tag{4.2}$$

Hence from (4.1) and (4.2)

$$\Phi(a_{i,j}u^ix^j.b_{r,s}u^rx^s) = \Phi(a_{i,j}u^ix^j).\Phi(b_{r,s}u^rx^s).$$

This implies that Φ preserves multiplication. Thus it is proved that Φ is an isomorphism. Therefore

$$\frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>} \cong \frac{R_\infty[x]}{<x^{mn}-\lambda>}.$$

□

Putting $\lambda = 1$ and $\lambda = -1$, we get the following two corollaries:

Corollary 4.2. *Assuming the notations given above we have*

$$\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>} \cong \frac{R_\infty[x]}{<x^{mn}-1>}.$$

Corollary 4.3. *Assuming the notations given above we have*

$$\frac{\frac{R_\infty[u]}{<u^n+1>}[x]}{<x^m-u>} \cong \frac{R_\infty[x]}{<x^{mn}+1>}.$$

Thus we have established that cyclic codes of composite length mn over the formal power series ring R_∞ corresponds to $u-$constacyclic code of length m over $\frac{R_\infty[u]}{<u^n-1>}$. Similarly negacyclic codes of composite length mn over the formal power series ring R_∞ corresponds to $u-$constacyclic code of length m over $\frac{R_\infty[u]}{<u^n+1>}$.

Theorem 4.3. *Assuming the notations given above we have*

$$\frac{\frac{R_i[u]}{<u^n-\lambda>}[x]}{<x^m-u>} \cong \frac{R_i[x]}{<x^{mn}-\lambda>}.$$

Proof. The proof of this theorem is similar to the proof of the Theorem 4.1. □

Putting $\lambda = 1$ and $\lambda = -1$, we get the following two corollaries:

Corollary 4.4. *Assuming the notations given above we have*

$$\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>} \cong \frac{R_i[x]}{<x^{mn}-1>}.$$

Corollary 4.5. *Assuming the notations given above we have*

$$\frac{\frac{R_i[u]}{<u^n+1>}[x]}{<x^m-u>} \cong \frac{R_i[x]}{<x^{mn}+1>}.$$

Theorem 4.4. *Let m and n are two odd numbers and $gcd(m,p)=1, gcd(n,p)=1$. Then*

$$\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>} \cong \frac{\frac{R_\infty[u]}{<u^n+1>}[x]}{<x^m-u>}.$$

Proof. Since m and n both are odds, mn is also odd. Again $gcd(m,p)=1$ and $gcd(n,p)=1$. Therefore $gcd(mn,p)=1$. We define the map

$$\eta : \frac{R_\infty[x]}{<x^{mn}+1>} \longrightarrow \frac{R_\infty[x]}{<x^{mn}-1>}$$

given by

$$f(x)+<x^{mn}+1> \longmapsto f(-x)+<x^{mn}-1> .$$

Now if

$$f(x)+<x^{mn}+1>=g(x)+<x^{mn}+1>,$$

then we have

$$f(x)-g(x)\in <x^{mn}+1> .$$

Therefore

$$f(x)-g(x)=(x^{mn}+1)q(x) \text{ for some } q(x)$$

and

$$\begin{aligned} f(-x)-g(-x) &= ((-x)^{mn}+1)q(-x) = (-x^{mn}+1)q(-x) \\ &= (x^{mn}-1)(-q(-x)) \in <x^{mn}-1> . \end{aligned}$$

This implies that

$$\begin{aligned} \eta(f(x)+<x^{mn}+1>) &= f(-x)+<x^{mn}-1>= g(-x)+<x^{mn}-1> \\ &= \eta(g(x)+<x^{mn}+1>). \end{aligned}$$

Thus, the correspondence η is a well-defined map. Now

$$\begin{aligned} &\eta((f(x)+<x^{mn}+1>)+(g(x)+<x^{mn}+1>)) \\ =&\eta((f(x)+g(x))+<x^{mn}+1>) = (f(-x)+g(-x))+<x^{mn}-1> \\ =&f(-x)+<x^{mn}-1> +g(-x)+<x^{mn}-1> \\ =&\eta(f(x)+<x^{mn}+1>)+\eta(g(x)+<x^{mn}+1>). \end{aligned}$$

Thus, η preserves addition.

Again

$$\begin{aligned}&\eta((f(x)+<x^{mn}+1>).(g(x)+<x^{mn}+1>))\\=&\eta((f(x).g(x))+<x^{mn}+1>)=(f(-x).g(-x))+<x^{mn}-1>\\=&(f(-x)+<x^{mn}-1>).(g(-x)+<x^{mn}-1>)\\=&\eta(f(x)+<x^{mn}+1>).\eta(g(x)+<x^{mn}+1>).\end{aligned}$$

Thus η preserves multiplication.

For $f(-x)+<x^{mn}-1>\in \frac{R_\infty[x]}{<x^{mn}-1>}$ there exists $f(x)+<x^{mn}+1>\in \frac{R_\infty[x]}{<x^{mn}+1>}$ such that

$$\eta(f(x)+<x^{mn}+1>)=f(-x)+<x^{mn}-1>.$$

Hence η is onto.

Let

$$\begin{aligned}&\eta(f(x)+<x^{mn}+1>)=\eta(g(x)+<x^{mn}+1>)\\\Longrightarrow\ &f(-x)+<x^{mn}-1>=g(-x)+<x^{mn}-1>\\\Longrightarrow\ &f(x)+<-x^{mn}-1>=g(x)+<-x^{mn}-1>\\&\text{(Replacing } x \text{ by } -x \text{ and since } mn \text{ is odd)}\\\Longrightarrow\ &f(x)+<x^{mn}+1>=g(x)+<x^{mn}+1>.\end{aligned}$$

Hence η is bijective. Thus it is an isomorphism. Therefore

$$\frac{R_\infty[x]}{<x^{mn}+1>}\cong\frac{R_\infty[x]}{<x^{mn}-1>}.$$

Because

$$\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}\cong\frac{R_\infty[x]}{<x^{mn}-1>} and \frac{\frac{R_\infty[u]}{<u^n+1>}[x]}{<x^m-u>}\cong\frac{R_\infty[x]}{<x^{mn}+1>}.$$

Therefore

$$\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}\cong\frac{\frac{R_\infty[u]}{<u^n+1>}[x]}{<x^m-u>}.$$

□

Theorem 4.5. *A linear code C of length mn over R_∞ is a $\lambda-$cyclic code if and only if $\Phi^{-1}(P_\lambda(C))$ is an ideal of $\frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>}$.*

Proof. From Lemma 4.1 we know that, a linear code C of length mn over R_∞ is a $\lambda-$cyclic code, if, and only if, $P_\lambda(C)$ is an ideal of $\frac{R_\infty[x]}{<x^{mn}-\lambda>}$. Again Φ is an isomorphism between $\frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>}$ and $\frac{R_\infty[x]}{<x^{mn}-\lambda>}$. Thus Φ^{-1} is an isomorphism.

So $\Phi^{-1}(P_\lambda(C))$ is an ideal of $\frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>}$, if, and only if, $(P_\lambda(C))$ is an ideal of $\frac{R_\infty[x]}{<x^{mn}-\lambda>}$. Thus A linear code C of length mn over R_∞ is a $\lambda-$cyclic code if and only if $\Phi^{-1}(P_\lambda(C))$ is an ideal of $\frac{\frac{R_\infty[u]}{<u^n-\lambda>}[x]}{<x^m-u>}$. □

Corollary 4.6. *Assuming the notations given above we have*

(i) *A linear code C of length mn over R_∞ is a cyclic code if and only if $\Phi^{-1}(P_1(C))$ is an ideal of $\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}$.*

(ii) *A linear code C of length mn over R_∞ is a negacyclic code if and only if $\Phi^{-1}(P_{-1}(C))$ is an ideal of $\frac{\frac{R_\infty[u]}{<u^n+1>}[x]}{<x^m-u>}$.*

Theorem 4.6. *If C is a cyclic code of length mn over R_∞ then, $\Phi^{-1}(\psi_i(P_1(C)))$ is an ideal of $\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>}$.*

Proof. From Theorem 4.1 we know that if C is a cyclic code over $R\infty$, then, $\psi_i(C)$ is a cyclic code over R_i for all $i < \infty$. Thus if C is a cyclic code of length mn over R_∞ then $\psi_i(P_1(C))$ is an ideal of $\frac{R_i[x]}{<x^{mn}-1>}$. As Φ is an isomorphism between $\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>}$ and $\frac{R_i[x]}{<x^{mn}-1>}$, Φ^{-1} is an isomorphism between $\frac{R_i[x]}{<x^{mn}-1>}$ and $\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>}$. Hence $\psi_i(P_1(C))$ is an ideal of $\frac{R_i[x]}{<x^{mn}-1>}$ if and only if $\Phi^{-1}(\psi_i(P_1(C)))$ is an ideal of $\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>}$. Thus if C is a cyclic code of length mn over R_∞ then, $\Phi^{-1}(\psi_i(P_1(C)))$ is an ideal of $\frac{\frac{R_i[u]}{<u^n-1>}[x]}{<x^m-u>}$. □

5. Conclusion

In [4] Dougherty and Liu proved that corresponding to every cyclic code of odd length n over R_∞ there exists a negacyclic code of same length over R_∞. Here we have considered both m and n as odd numbers and proved that $u-$constacyclic codes of length m over $\frac{R_\infty[x]}{<x^n-1>}$ corresponds to $u-$constacyclic code of length m over $\frac{R_\infty[x]}{<x^n+1>}$. Neither a counter example have been found to disprove that $u-$constacyclic codes of length m over $\frac{R_\infty[x]}{<x^n-1>}$ corresponds to $u-$constacyclic code of length m over $\frac{R_\infty[x]}{<x^n+1>}$, nor any isomorphism has been constructed between $\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}$ and $\frac{\frac{R_\infty[u]}{<u^n+1>}[x]}{<x^m-u>}$ to prove that $u-$constacyclic codes of length m over $\frac{R_\infty[x]}{<x^n-1>}$ corresponds to $u-$constacyclic codes of length m over $\frac{R_\infty[x]}{<x^n+1>}$, when at least one of m or n is even. Hence still the problem whether

$\frac{\frac{R_\infty[u]}{<u^n-1>}[x]}{<x^m-u>}$ is isomorphic to $\frac{\frac{R_\infty[u]}{<u^n+1>}[x]}{<x^m-u>}$ or not is unsolved, when at least one of m or n is even.

REFERENCES

[1] T. BLACKFORD: *Cyclic codes over Z_4 of oddly even length*, Discrete Applied Mathematics, **128** (2003), 27–46.

[2] H. DINH, S. LOPEZ-PERMOUTH: *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory, **50** (2004), 1728–1744.

[3] S. T. DOUGHERTY, S. LING: *Cyclic codes over Z_4 of even length*, Designs, Codes, Cryptogr., **34** (2006), 127–153.

[4] S. T. DOUGHERTY, H. LIU: *Cyclic codes over formal power series rings*, Acta Mathematica Scientia, **31B** (1) (2011), 331–343.

[5] S. T. DOUGHERTY, H. LIU, Y. H. PARK: *Lifted codes over finite chain rings*, Mathematical Journal of Okayama University, **53** (2011), 39–53.

[6] M. S. DUTTA, H. K. SAIKIA: *A Study of Cyclic Codes Via a Surjective Mapping*, Matematika, **34** (2) (2018), 325–332.

[7] G. NOTON, A. SALAGEAN: *On the structure of linear and cyclic codes over a finite chain ring*, Applicable Algebra Engineering Communication and Computing, **10** (2000), 489–506.

[8] R. SOBHANI, M. MOLAKARIMI: *Some Results on Cyclic Codes over the Ring $R_{2,m}$*, Turkish Journal of Mathematics, **37** (2013), 1061–1074.

DEPARTMENT OF MATHEMATICS
NALBARI COLLEGE
NALBARI, PIN-781335, INDIA
Email address: dutta.mriganka82@gmail.com

DEPARTMENT OF MATHEMATICS
GAUHATI UNIVERSITY
GUWAHATI, PIN-781014, INDIA
Email address: hsaikia@yahoo.com