A Study of Cyclic Codes Via a Surjective Mapping

1Mriganka S. Dutta* and 2Helen K. Saikia

1Department of Mathematics, Nalbari College
Nalbari, Pin-781335, India
2Department of Mathematics, Gauhati University
Guwahati, Pin-781014, India

*Corresponding author: dutta.mriganka82@gmail.com

Abstract In this article, cyclic codes of length \( n \) over a formal power series ring and cyclic codes of length \( nl \) over a finite field are studied. We have defined a bijective mapping \( \Phi_l \) on \( R_\infty \), where \( R_\infty \) is the formal power series ring over a finite field \( F \). We have proved that a cyclic shift in \( (F)^n \) corresponds to a \( \Phi_l \)-cyclic shift in \( (R_\infty)^n \) by defining a mapping from \( (R_\infty)^n \) onto \( (F)^n \). We have also derived some related results.

Keywords Cyclic codes; constacyclic shift; formal power series ring; isomorphism.

Mathematics Subject Classification 94B15

1 Introduction

Error-correcting codes are basically used to detect errors when messages are transmitted through a noisy communication channel. Most of the codes are also used to correct errors. In coding theory, we encode the data by adding a certain amount of redundancy to the original message. As a consequence the original message can be recovered if not too many errors have occurred.

Cyclic codes play an important role in coding theory as seen in [1,6]. In the very beginning, the properties of Cyclic codes were studied over the binary field \( \mathbb{F}_2 \), then the study was extended 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 \( \mathbb{F}_q[x]/\langle x^n - 1 \rangle \) [4]. Dougherty, Liu, and Park [5] defined a series of finite chain rings and introduced the concept of \( \gamma \)-adic codes over a formal power series rings. Dougherty and Liu [4] have given the concept of \( \lambda \)-cyclic code of length \( n \) over \( R_\infty \). By defining a module isomorphism between \( R^n \) and \( (Z_4)^{2^n} \), Dinh and Lopez-Permouth proved that a cyclic shift in \( (Z_4)^{2^n} \) corresponds to a constacyclic shift in \( R^n \) by \( u \), where \( R = Z_4[u]/\langle u^{2^n} - 1 \rangle \) [2]. In this article, we have introduced the concept of \( \Phi_{\lambda} \)-cyclic code of length \( n \) over a formal power series ring and derived some related results.
Some Important Definitions and Results

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

**Definition 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 2**[4] Let $x, y$ be vectors in $R^n$. The inner product of $x$ and $y$ is defined by $[x, y] = x_1y_1 + x_2y_2 + \ldots + x_ny_n$.

**Definition 3**[4] For a code $C$ of length $n$ over $R$, the dual code of $C$ is defined by $C^\perp = \{ x \in R^n | [x, c] = 0, \forall c \in C \}$.

**Remark 1** $C^\perp$ is linear whether or not $C$ is linear.

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

**Definition 5**[4] Let $i$ be an arbitrary positive integer and $F$ be a finite field. The ring $R_i$ is defined as $R_i = \{ a_0 + a_1\gamma + \ldots + a_{i-1}\gamma^{i-1} \mid a_i \in F \}$, where $\gamma^{i-1} \neq 0$, but $\gamma^i = 0$ in $R_i$. The operations over $R_i$ are defined as follows:

\[
\sum_{l=0}^{i-1} a_l \gamma^l + \sum_{l=0}^{i-1} b_l \gamma^l = \sum_{l=0}^{i-1} (a_l + b_l) \gamma^l; \quad \left( \sum_{l=0}^{i-1} a_l \gamma^l \right) \cdot \left( \sum_{l=0}^{i-1} b_l \gamma^l \right) = \sum_{s=0}^{i-1} \left( \sum_{l+l'=s} a_l b_{l'} \right) \gamma^s.
\]

**Definition 6**[4] The ring $R_\infty$ 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 $R_\infty$ 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

\[
\left( \sum_{l=0}^{\infty} a_l \gamma^l \right) \cdot \left( \sum_{l=0}^{\infty} b_l \gamma^l \right) = \sum_{s=0}^{\infty} \left( \sum_{l+l'=s} a_l b_{l'} \right) \gamma^s.
\]
Definition 7 [4] Let $i, j$ be two integers with $i \leq j$. In [4], the mapping $\Psi_j^i$ is defined by

$$\Psi_j^i : R_j \rightarrowtail R_i, \sum_{l=0}^{j-1} a_l \gamma^l \mapsto \sum_{l=0}^{i-1} a_l \gamma^l.$$

Definition 8 [4] Let $i$ be any positive integer. In [4], the mapping $\Psi_i$ is defined by

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

It can be proved that $\Psi_j^i$ and $\Psi_i$ are homomorphisms. We can extend $\Psi_j^i$ naturally from $R^n_j$ to $R^n_i$. Similarly $\Psi_i$ can be extended naturally from $R^n_\infty$ to $R^n_i$.

Definition 9 Let $l$ be any positive integer. We define a mapping $\Phi_l$ on $R_\infty$ as follows:

$$\Phi_l : R_\infty \rightarrowtail R_\infty, \sum_{i=0}^{\infty} a_i \gamma^i \mapsto a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=1}^{\infty} a_i \gamma^i.$$

We have the following lemma.

Lemma 1 Assume the notations given above. Then, we have

(a) $\Phi_l$ is bijective.
(b) The inverse of $\Phi_l$ is $\Phi_l^{-1}$.
(c) It preserves addition.
(d) It does not preserve multiplication.

Proof

(a) For $\sum_{i=0}^{\infty} a_i \gamma^i \in R_\infty = \text{Co-domain}$. There exists $\sum_{i=1}^{l-1} a_i \gamma^{i-1} + a_0 \gamma^{l-1} + \sum_{i=l}^{\infty} a_i \gamma^i \in R_\infty = \text{Domain}$, such that $\Phi_l(\sum_{i=1}^{l-1} a_i \gamma^{i-1} + a_0 \gamma^{l-1} + \sum_{i=l}^{\infty} a_i \gamma^i) = \sum_{i=0}^{\infty} a_i \gamma^i$. Thus the mapping is onto.

Let

$$\Phi_l\left(\sum_{i=0}^{\infty} a_i \gamma^i\right) = \Phi_l\left(\sum_{i=0}^{\infty} b_i \gamma^i\right)$$

$$\Rightarrow a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=0}^{\infty} a_i \gamma^i = b_{l-1} + \gamma \sum_{i=0}^{l-2} b_i \gamma^i + \sum_{i=0}^{\infty} b_i \gamma^i$$

$$\Rightarrow a_{l-1} = b_{l-1}, \ a_0 = b_0, \ a_1 = b_1, \ldots$$

Thus

$$\sum_{i=0}^{\infty} a_i \gamma^i = \sum_{i=0}^{\infty} b_i \gamma^i.$$

Therefore the mapping is one-one. Hence the mapping is bijective.

(b) We know that

$$\Phi_l\left(\sum_{i=0}^{\infty} a_i \gamma^i\right) = a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i$$
Thus
\[ \Phi_l^2 \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = \Phi_l \left( \Phi_l \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \right) = a_{l-2} + \gamma a_{l-1} + \gamma^2 \sum_{i=0}^{l-3} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i. \]

Continuing the process \( l \) times we get
\[ \Phi_l^l \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = \Phi_l \left( \Phi_l^{l-1} \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \right) = \sum_{i=0}^{\infty} a_i \gamma^i. \]

Thus \( \Phi_l^{l-1} \) is the inverse of \( \Phi_l \).

(c) Let
\[ \sum_{i=0}^{\infty} a_i \gamma^i, \sum_{i=0}^{\infty} b_i \gamma^i \in R_\infty. \]

Now
\[ \Phi_l \left( \sum_{i=0}^{\infty} a_i \gamma^i + \sum_{i=0}^{\infty} b_i \gamma^i \right) = \Phi_l \left( \sum_{i=0}^{\infty} (a_i + b_i) \gamma^i \right) = a_{l-1} + b_{l-1} + \gamma \sum_{i=0}^{l-2} (a_i + b_i) \gamma^i + \sum_{i=l}^{\infty} (a_i + b_i) \gamma^i. \]

Again
\[ \Phi_l \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i \]
and
\[ \Phi_l \left( \sum_{i=0}^{\infty} b_i \gamma^i \right) = b_{l-1} + \gamma \sum_{i=0}^{l-2} b_i \gamma^i + \sum_{i=l}^{\infty} b_i \gamma^i. \]

Therefore
\[ \Phi_l \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) + \Phi_l \left( \sum_{i=0}^{\infty} b_i \gamma^i \right) = a_{l-1} + b_{l-1} + \gamma \sum_{i=0}^{l-2} (a_i + b_i) \gamma^i + \sum_{i=l}^{\infty} (a_i + b_i) \gamma^i. \]

Thus
\[ \Phi_l \left( \sum_{i=0}^{\infty} a_i \gamma^i + \sum_{i=0}^{\infty} b_i \gamma^i \right) = \Phi_l \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) + \Phi_l \left( \sum_{i=0}^{\infty} b_i \gamma^i \right). \]

Hence the mapping preserves addition.

(d) Let \( \mathbb{F} = \mathbb{F}_2 \). Now \( 1 + \gamma + \gamma^2 \in R_\infty \). Then \( \Phi_2(1 + \gamma + \gamma^2) = 1 + \gamma + \gamma^2 \). Thus
\[ \Phi_2(1 + \gamma + \gamma^2).\Phi_2(1 + \gamma + \gamma^2) = 1 + \gamma^2 + \gamma^4 \]
and
\[ \Phi_2((1 + \gamma + \gamma^2).(1 + \gamma + \gamma^2)) = \Phi_2(1 + \gamma^2 + \gamma^4) = \gamma + \gamma^2 + \gamma^4. \]

Hence we have shown that
\[ \Phi_l \left( \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \cdot \left( \sum_{i=0}^{\infty} b_i \gamma^i \right) \right) \neq \Phi_l \left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \cdot \Phi_l \left( \sum_{i=0}^{\infty} b_i \gamma^i \right) \]
which implies that the mapping does not preserve multiplication. Hence it is not an isomorphism.

Similarly, we can define \( \Phi_{-l} \) on \( R_{\infty} \) as follows:

\[
\Phi_{-l} : R_{\infty} \rightarrow R_{\infty}, \quad \sum_{i=0}^{\infty} a_i \gamma^i \mapsto -a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i.
\]

For any scalar \( \lambda \neq 0 \) we can also define \( \Phi_{\lambda l} \) on \( R_{\infty} \) as follows:

\[
\Phi_{\lambda l} : R_{\infty} \rightarrow R_{\infty}, \quad \sum_{i=0}^{\infty} a_i \gamma^i \mapsto \lambda a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i.
\]

Both \( \Phi_{-l} \) and \( \Phi_{\lambda l} \) are bijective, preserves addition, but does not preserve multiplication. Thus they are not isomorphisms.

**Lemma 2** Assume the notations given above. The inverse of \( \Phi_{-l} \) is \( \Phi_{-l}^{2l-1} \).

**Proof** We know that

\[
\Phi_{-l}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = -a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i.
\]

Thus

\[
\Phi_{-l}^{2l}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = \Phi_{-l}\left( \Phi_{-l}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \right) = -a_{l-1} - \gamma a_{l-1} + \gamma^2 \sum_{i=0}^{l-3} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i.
\]

Continuing the process \( 2l \) times we get

\[
\Phi_{-l}^{2l}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = \Phi_{-l}\left( \Phi_{-l}^{2l-1}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \right) = \sum_{i=0}^{\infty} a_i \gamma^i.
\]

Thus \( \Phi_{-l}^{2l-1} \) is the inverse of \( \Phi_{-l} \).

**Lemma 3** Assume the notations given above. Let \( s \) be the multiplicative order of the scalar \( \lambda \) as an element of the finite field \( R \). Then the inverse of \( \Phi_{\lambda l} \) is \( \Phi_{\lambda l}^{sl-1} \).

**Proof** We know that

\[
\Phi_{\lambda l}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = \lambda a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i.
\]

Thus

\[
\Phi_{\lambda l}^2\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = \Phi_{\lambda l}\left( \Phi_{\lambda l}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \right) = \lambda a_{l-1} \gamma + \gamma^2 \sum_{i=0}^{l-3} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i.
\]

Continuing the process \( sl \) times we get

\[
\Phi_{\lambda l}^{sl}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) = \Phi_{\lambda l}\left( \Phi_{\lambda l}^{sl-1}\left( \sum_{i=0}^{\infty} a_i \gamma^i \right) \right) = \lambda^s \left( \sum_{i=0}^{l-1} a_i \gamma^i \right) + \sum_{i=l}^{\infty} a_i \gamma^i = \sum_{i=0}^{\infty} a_i \gamma^i.
\]

Thus \( \Phi_{\lambda l}^{sl-1} \) is the inverse of \( \Phi_{\lambda l} \).
Definition 10 [4] Let $C$ be a linear code of length $n$ over $R_\infty$. The code $C$ is called a $\lambda-$ cyclic code over $R_\infty$ if
\[ c = (c_0, c_1, ..., c_{n-1}) \in C \Rightarrow (\lambda c_{n-1}, c_0, ..., c_{n-2}) \in C. \]
If $\lambda = 1$, then $C$ is called a cyclic code and if $\lambda = -1$, then $C$ is called a negacyclic code.

Definition 11 Let $C$ be a linear code of length $n$ over $R_\infty$. Here we have defined $C$ to be a $\phi_\lambda-$cyclic code of length $n$ over $R_\infty$ if
\[ c = \left( \sum_{j=0}^{\infty} a_{0,j} u^j, \sum_{j=0}^{\infty} a_{1,j} u^j, ..., \sum_{j=0}^{\infty} a_{n-1,j} u^j \right) \in C. \]
\[ \Rightarrow \left( \phi_\lambda \left( \sum_{j=0}^{\infty} a_{n-1,j} u^j \right), \sum_{j=0}^{\infty} a_{0,j} u^j, ..., \sum_{j=0}^{\infty} a_{n-2,j} u^j \right) \in C. \]
If $\lambda = 1$, then $C$ is called a $\Phi_1-$cyclic code and if $\lambda = -1$, then $C$ is called a $\Phi_{-1}-$cyclic code.

Let $R = Z_4[u]/<u^{2^k}-1>$. In [3], the authors have defined an isomorphism $\Psi : R^n \rightarrow (Z_4)^{2^k n}$ given by
\[ \Psi \left( u \left( \sum_{j=0}^{2^k-1} a_{n-1,j} u^j, \sum_{j=0}^{2^k-1} a_{0,j} u^j, \sum_{j=0}^{2^k-1} a_{1,j} u^j, ..., \sum_{j=0}^{2^k-1} a_{n-2,j} u^j \right) \right) = (a_{n-1,2^k-1}, a_0, a_1, ..., a_{n-2,2^k-1}) \]
and proved the following theorem.

Theorem 1 [3] Cyclic codes over $Z_4$ of length $2^kn$ corresponds to $u-$constacyclic codes over $R = Z_4[u]/<u^{2^k}-1>$ of length $n$ via the map $\Psi$.

Let $R = \frac{Z_2[a][u]}{<a^{2^k}+1>}$. In [7], the authors have defined a natural $Z_2^a-$module isomorphism $\Psi : R^n \rightarrow (Z_2^a)^{2^k n}$ given by
\[ \Psi(a_{0,0}a_{0,1}u + ... + a_{0,2^k-1}u^{2^k-1}, ..., a_{n-1,0}, a_{n-1,1}u + ... + a_{n-1,2^k-1}u^{2^k-1}) = (a_{0,0}, a_{0,1}, ..., a_{n-1,0}, a_{0,1}, ..., a_{n-1,1}, ..., a_{n-1,2^k-1}, a_{n-1,2^k-1}) \]
and proved the following theorem.

Theorem 2 [7] Negacyclic codes over $Z_2^a$ of length $2^kn$ corresponds to $u-$constacyclic codes over $R = Z_2^a[u]/<u^{2^k}+1>$ of length $n$ via the map $\Psi$.

3 The Main Results

Our main objective is to prove the following theorem which is the central result in our present work. The next two results entirely depends on this. Before going to prove the result we define a mapping $\eta : (R_\infty)^n \rightarrow (F)^{kn}$ given by
\[ \eta \left( \sum_{j=0}^{\infty} a_{0,j} u^j, \sum_{j=0}^{\infty} a_{1,j} u^j, ..., \sum_{j=0}^{\infty} a_{n-1,j} u^j \right) = (a_{0,0}, a_{1,0}, ..., a_{n-1,0}, a_{0,1}, ..., a_{n-1,1}, ..., a_{0,l-1}, a_{1,l-1}, ..., a_{n-1,l-1}). \]
Theorem 1 \(\lambda\)-cyclic codes over \(\mathbb{F}\) of length \(nl\) corresponds to \(\Phi_{\lambda l}\)-cyclic codes over \(R_{\infty}\) of length \(n\) via the map \(\eta\).

Proof We have already defined the mapping
\[
\eta : (R_{\infty})^n \longrightarrow (\mathbb{F})^l^n
\]
given by
\[
\eta\left(\sum_{j=0}^{\infty} a_{0,j} u^j, \sum_{j=0}^{\infty} a_{1,j} u^j, \ldots, \sum_{j=0}^{\infty} a_{n-1,j} u^j\right) = (a_{0,0}, a_{1,0}, \ldots, a_{n-1,0}, a_{0,1}, a_{1,1}, \ldots, a_{n-1,1}, \ldots, a_{0,l-1}, a_{1,l-1}, \ldots, a_{n-1,l-1}).
\]
As we have already defined \(\Phi_{\lambda l} : R_{\infty} \longrightarrow R_{\infty}\) by
\[
\Phi_{\lambda l}\left(\sum_{i=0}^{\infty} a_i \gamma^i\right) = \lambda a_{l-1} + \gamma \sum_{i=0}^{l-2} a_i \gamma^i + \sum_{i=l}^{\infty} a_i \gamma^i.
\]
Thus we have
\[
\eta\left(\sum_{j=0}^{\infty} a_{n-1,j} u^j, \sum_{j=0}^{\infty} a_{0,j} u^j, \ldots, \sum_{j=0}^{\infty} a_{n-2,j} u^j\right) = (\lambda a_{n-1,l-1}, a_{0,0}, a_{1,0}, \ldots, a_{n-2,l-1}).
\]
Thus the result is proved. \(\square\)

Corollary 1 Cyclic codes over \(\mathbb{F}\) of length \(nl\) corresponds to \(\Phi_{l}\)-cyclic codes over \(R_{\infty}\) of length \(n\) via the map \(\eta\).

Proof Putting \(\lambda = 1\) in Theorem 1, we get the above result. \(\square\)

Corollary 2 Negacyclic codes over \(\mathbb{F}\) of length \(nl\) corresponds to \(\Phi_{-l}\)-cyclic codes over \(R_{\infty}\) of length \(n\) via the map \(\eta\).

Proof Putting \(\lambda = -1\) in Theorem 1, we get the above result. \(\square\)

4 Conclusion

The map \(\Phi_{l}\) is not an isomorphism. We can investigate the properties of this map and study cyclic codes over formal power series rings and cyclic codes over finite fields simultaneously. We can replace the finite field by any arbitrary ring and study cyclic codes over that arbitrary ring via the map \(\eta\).

Acknowledgments

The authors would like to thank the referees for their valuable comments and suggestions.
References


