MATEMATIKA, 2018, Volume 34, Number 2, 325–332

A Study of Cyclic Codes Via a Surjective Mapping

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

[1]Department of Mathematics, Nalbari College
Nalbari, Pin-781335, India

[2]Department of Mathematics, Gauhati University
Guwahati, Pin-781014, India

*Corresponding author: dutta.mriganka82@gmail.com

Article history
Received: 23 May 2015
Received in revised form: 14 June 2018
Accepted: 31 October 2018
Published on line: 1 December 2018

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 Φ_l on R_∞, where R_∞ is the formal power series ring over a finite field $\mathbb{F}$. We have proved that a cyclic shift in $(\mathbb{F})^{ln}$ corresponds to a Φ_l-cyclic shift in $(R_\infty)^n$ by defining a mapping from $(R_\infty)^n$ onto $(\mathbb{F})^{ln}$. 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 $\mathbb{F}_q[x]/< x^n - 1 >$ [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_∞. By defining a module isomorphism between R^n and $(Z_4)^{2^k n}$, Dinh and Lopez-Permouth proved that a cyclic shift in $(Z_4)^{2^k n}$ corresponds to a constacyclic shift in R^n by u, where $R = Z_4[u]/< u^{2^k} - 1 >$ [2]. In this article, we have introduced the concept of $\Phi_{\lambda l}-$cyclic code of length n over a formal power series ring and derived some related results.

2 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*

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

Definition 3 [4] *For a code C of length n over R, the dual code of C is defined by*

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

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 $\mathbb{F}$ be a finite field. The ring R_i is defined as*

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

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

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

Definition 6 [4] *The ring R_∞ is called a formal power series ring which is defined as*

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

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

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

Definition 7 [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 8 [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.

Definition 9 *Let l be any positive integer. We define a mapping Φ_l on R_∞ as follows:*

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

We have the following lemma.

Lemma 1 *Assume the notations given above. Then, we have*
(a) *Φ_l is bijective.*
(b) *The inverse of Φ_l is Φ_l^{l-1}.*
(c) *It preserves addition.*
(d) *It does not preserve multiplication.*

Proof
(a) For $\sum_{i=0}^{\infty} a_i\gamma^i \ \epsilon\ R_\infty$ = Co-domain. There exists $\sum_{i=1}^{l-1} a_i\gamma^{i-1} + a_0\gamma^{l-1} + \sum_{i=l}^{\infty} a_i\gamma^i \ \epsilon\ R_\infty$ = 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

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

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

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

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

$$\Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = a_{l-1} + \gamma\sum_{i=0}^{l-2} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i$$

Thus

$$\Phi_l^2\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \Phi_l\Big(\Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big)\Big) = a_{l-2} + \gamma a_{l-1} + \gamma^2\sum_{i=0}^{l-3} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i.$$

Continuing the process l times we get

$$\Phi_l^l\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \Phi_l\Big(\Phi_l^{l-1}(\sum_{i=0}^{\infty} a_i\gamma^i\Big)\Big) = \sum_{i=0}^{\infty} a_i\gamma^i.$$

Thus Φ_l^{l-1} is the inverse of Φ_l.
(c) Let

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

Now

$$\Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i + \sum_{i=0}^{\infty} b_i\gamma^i\Big) = \Phi_l\Big(\sum_{i=0}^{\infty}(a_i+b_i)\gamma^i\Big) = a_{l-1} + b_{l-1} + \gamma\sum_{i=0}^{l-2}(a_i+b_i)\gamma^i + \sum_{i=l}^{\infty}(a_i+b_i)\gamma^i.$$

Again

$$\Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = a_{l-1} + \gamma\sum_{i=0}^{l-2} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i$$

and

$$\Phi_l\Big(\sum_{i=0}^{\infty} b_i\gamma^i\Big) = b_{l-1} + \gamma\sum_{i=0}^{l-2} b_i\gamma^i + \sum_{i=l}^{\infty} b_i\gamma^i.$$

Therefore

$$\Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) + \Phi_l\Big(\sum_{i=0}^{\infty} b_i\gamma^i\Big) = a_{l-1} + b_{l-1} + \gamma\sum_{i=0}^{l-2}(a_i+b_i)\gamma^i + \sum_{i=l}^{\infty}(a_i+b_i)\gamma^i.$$

Thus

$$\Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i + \sum_{i=0}^{\infty} b_i\gamma^i\Big) = \Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) + \Phi_l\Big(\sum_{i=0}^{\infty} b_i\gamma^i\Big).$$

Hence the mapping preserves addition.
(d) Let $\mathbb{F} = \mathbb{F}_2$. Now $1+\gamma+\gamma^2\ \epsilon\ R_\infty$. 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

$$\Phi_l\Big(\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big).\Big(\sum_{i=0}^{\infty} b_i\gamma^i\Big)\Big) \neq \Phi_l\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big).\Phi_l\Big(\sum_{i=0}^{\infty} b_i\gamma^i\Big)$$

which implies that the mapping does not preserve multiplication. Hence it is not an isomorphism. □

Similarly, we can define Φ_{-l} on R_∞ as follows:

$$\Phi_{-l} : R_\infty \longrightarrow R_\infty,\ \sum_{i=0}^{\infty} a_i\gamma^i \longmapsto -a_{l-1} + \gamma\sum_{i=0}^{l-2} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i.$$

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

$$\Phi_{\lambda l} : R_\infty \longrightarrow R_\infty,\ \sum_{i=0}^{\infty} a_i\gamma^i \longmapsto \lambda a_{l-1} + \gamma\sum_{i=0}^{l-2} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i$$

Both Φ_{-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 Φ_{-l} is Φ_{-l}^{2l-1}.*

Proof We know that

$$\Phi_{-l}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = -a_{l-1} + \gamma\sum_{i=0}^{l-2} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i.$$

Thus

$$\Phi_{-l}^2\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \Phi_{-l}\Big(\Phi_{-l}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big)\Big) = -a_{l-2} - \gamma a_{l-1} + \gamma^2\sum_{i=0}^{l-3} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i.$$

Continuing the process $2l$ times we get

$$\Phi_{-l}^{2l}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \Phi_{-l}\Big(\Phi_{-l}^{2l-1}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big)\Big) = \sum_{i=0}^{\infty} a_i\gamma^i.$$

Thus Φ_{-l}^{2l-1} is the inverse of Φ_{-l}. □

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

Proof We know that

$$\Phi_{\lambda l}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \lambda a_{l-1} + \gamma\sum_{i=0}^{l-2} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i.$$

Thus

$$\Phi_{\lambda l}^2\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \Phi_{\lambda l}\Big(\Phi_{\lambda l}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big)\Big) = \lambda a_{l-2} + \lambda a_{l-1}\gamma + \gamma^2\sum_{i=0}^{l-3} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i.$$

Continuing the process sl times we get

$$\Phi_{\lambda l}^{sl}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \Phi_{\lambda l}\Big(\Phi_{\lambda l}^{sl-1}(\sum_{i=0}^{\infty} a_i\gamma^i)\Big) = \lambda^s\Big(\sum_{i=0}^{l-1} a_i\gamma^i\Big) + \sum_{i=l}^{\infty} a_i\gamma^i = \sum_{i=0}^{\infty} a_i\gamma^i.$$

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_∞. The code C is called a $\lambda-$ cyclic code over R_∞ 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, otherwise, it is called a constacyclic code.

Definition 11 *Let C be a linear code of length n over R_∞. Here we have defined C to be a $\phi_{\lambda l}-$cyclic code of length n over R_∞ if*

$$c = \Big(\sum_{j=0}^{\infty} a_{0,j}u^j, \sum_{j=0}^{\infty} a_{1,j}u^j, ..., \sum_{j=0}^{\infty} a_{n-1,j}u^j\Big) \in C.$$

$$\Rightarrow \Big(\phi_{\lambda l}\Big(\sum_{j=0}^{\infty} a_{n-1,j}u^j\Big), \sum_{j=0}^{\infty} a_{0,j}u^j, ..., \sum_{j=0}^{\infty} a_{n-2,j}u^j\Big) \in C.$$

If $\lambda = 1$, then C is called a Φ_l-cyclic code and if $\lambda = -1$, then C is called a $\Phi_{-l}-$cyclic code.

Let $R = Z_4[u]/< u^{2^k} - 1 >$. In [3], the authors have defined an isomorphism $\Psi : R^n \longrightarrow (Z_4)^{2^k n}$ given by

$$\Psi\Big(u\Big(\sum_{j=0}^{2^k-1} a_{n-1,j}u^j\Big), \sum_{j=0}^{2^k-1} a_{0,j}u^j, \sum_{j=0}^{2^k-1} a_{1,j}u^j, ..., \sum_{j=0}^{2^k-1} a_{n-2,j}u^j\Big)$$
$$= (a_{n-1,2^k-1}, a_{0,0}, a_{1,0}, ..., a_{n-2,2^k-1})$$

and proved the following theorem.

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

Let $R = \frac{Z_{2^a}[u]}{<u^{2^k}+1>}$. In [7], the authors have defined a natural $Z_{2^a}-$ module isomorphism $\Psi : R^n \longrightarrow (Z_{2^a})^{2^k n}$ given by

$$\Psi(a_{0,0}+a_{0,1}u + ... + a_{0,2^k-1}u^{2^k-1}, ..., a_{n-1,0} + a_{n-1,1}u + ... + a_{n-1,2^k-1}u^{2^k-1})$$
$$= (a_{0,0}, a_{1,0}, ..., a_{n-1,0}, a_{0,1}, a_{1,1}, ..., a_{n-1,1}, ..., a_{0,2^k-1}, a_{n-1,2^k-1})$$

and proved the following theorem.

Theorem 2 [7] *Negayclic codes over Z_{2^a} of length $2^k n$ corresponds to $u-$ constacyclic codes over $R = Z_{2^a}[u]/< u^{2^k} + 1 >$ of length n via the map Ψ.*

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 $\eta : (R_\infty)^n \longrightarrow (\mathbb{F})^{ln}$ given by

$$\eta\Big(\sum_{j=0}^{\infty} a_{0,j}u^j, \sum_{j=0}^{\infty} a_{1,j}u^j, ..., \sum_{j=0}^{\infty} a_{n-1,j}u^j\Big)$$
$$= (a_{0,0}, a_{1,0}, ..., a_{n-1,0}, a_{0,1}, a_{1,1}, ..., a_{n-1,1}, ..., a_{0,l-1}, a_{1,l-1}, ..., a_{n-1,l-1}).$$

Theorem 1 *$\lambda-$ cyclic codes over $\mathbb{F}$ of length nl corresponds to $\Phi_{\lambda l}-$ cyclic codes over R_∞ of length n via the map η.*

Proof We have already defined the mapping

$$\eta : (R_\infty)^n \longrightarrow (\mathbb{F})^{ln}$$

given by

$$\eta\Big(\sum_{j=0}^{\infty} a_{0,j}u^j, \sum_{j=0}^{\infty} a_{1,j}u^j, ..., \sum_{j=0}^{\infty} a_{n-1,j}u^j\Big)$$
$$= (a_{0,0}, a_{1,0}, ..., a_{n-1,0}, a_{0,1}, a_{1,1}, ..., a_{n-1,1}, ..., a_{0,l-1}, a_{1,l-1}, ..., a_{n-1,l-1}).$$

As we have already defined $\Phi_{\lambda l} : R_\infty \longrightarrow R_\infty$ by

$$\Phi_{\lambda l}\Big(\sum_{i=0}^{\infty} a_i\gamma^i\Big) = \lambda a_{l-1} + \gamma\sum_{i=0}^{l-2} a_i\gamma^i + \sum_{i=l}^{\infty} a_i\gamma^i.$$

Thus we have

$$\eta\Big(\phi_{\lambda l}\Big(\sum_{j=0}^{\infty} a_{n-1,j}u^j\Big), \sum_{j=0}^{\infty} a_{0,j}u^j, ..., \sum_{j=0}^{\infty} a_{n-2,j}u^j\Big)$$
$$= (\lambda a_{n-1,l-1}, a_{0,0}, a_{1,0}, ..., a_{n-2,l-1}).$$

Thus the result is proved. □

Corollary 1 *Cyclic codes over $\mathbb{F}$ of length nl corresponds to Φ_l- cyclic codes over R_∞ of length n via the map η.*

Proof Putting $\lambda = 1$ in Theorem 1, we get the above result. □

Corollary 2 *Negayclic codes over $\mathbb{F}$ of length nl corresponds to $\Phi_{-l}-$ cyclic codes over R_∞ of length n via the map η.*

Proof Putting $\lambda = -1$ in Theorem 1, we get the above result. □

4 Conclusion

The map Φ_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 η.

Acknowledgments

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

References

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

[2] Dinh, H. Lopez-Permouth, S. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory*. 2004. 50: 1728–1744.

[3] Dougherty, S. T. and Ling, S. Cyclic codes over Z_4 of even length. *Designs, Codes, Cryptog*. 2006. 34: 127–153.

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

[5] Dougherty, S. T., Liu, H. and Park, Y. H. Lifted codes over finite chain rings. *Mathematical Journal of Okayama University*. 2011. 53: 39–53.

[6] Noton, G. and Salagean, A. On the structure of linear and cyclic codes over a finite chain ring. *Applicable Algebra Engineering Communication and Computing*. 2000. 10: 489–506.

[7] Zhu, S. X. and Kai, X. Dual and self-dual negacyclic codes of even length over Z_{2^a}. *Discrete Mathematics*. 2008. 13: 7–10.