Erzincan Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
2020, 13(ÖZEL SAYI-I), 92-96

Erzincan University
Journal of Science and Technology
2020, 13(SPECIAL ISSUE-I), 92-96

ISSN: 1307-9085, e-ISSN: 2149-4584
DOI: 10.18185/erzifbed.635690

Skew λ-cyclic Codes over Y_2

Abdullah DERTLİ[1*], Yasemin ÇENGELLENMİŞ[2]

[1]Ondokuz Mayıs University, Faculty of Arts and Sciences, Mathematics Department, Samsun, Turkey

[2] Trakya University, Faculty of Sciences, Mathematics Department, Edirne, Turkey

Geliş / Received: 21/10/2019, Kabul / Accepted: 21/02/2020

Abstract
In the present paper, by defining two non-trivial automorphisms and Gray maps over $Y_2=\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4+uv\mathbb{Z}_4$, where $u^2=0, v^2=0, uv=vu$, the algebraic structcure of the skew λ-cyclic codes and their Gray images over the finite ring Y_2 are determined, where $\lambda=1+u+v+uv$.
Keywords: Skew codes, Gray map, Finite rings.

Y_2 Halkası Üzerinde Skew λ-cyclic Kodlar

Öz

Bu çalışmada, $u^2=0, v^2=0, uv=vu, \lambda=1+u+v+uv$, olmak üzere $Y_2=\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4+uv\mathbb{Z}_4$, sonlu halkası üzerinde iki farklı Gray dönüşümü ve otomorfizma tanımlanarak skew λ-cyclic kodların cebirsel yapısı ve bu kodların Gray görüntüleri belirlenmiştir.

Anahtar Kelimeler: Skew kodlar, Gray dönüşümü, Sonlu halkalar.

1. Introduction

Cyclic codes are the most studied class of linear codes with algebraic structure.

Skew polynomial rings form an important family of non-commutative rings. There are many applications in the construction of algebraic codes. As polynomials in skew polynomial ring exhibit many factorizations, there are many more ideals in a skew polynomial ring than in the commutative case. So the researchers on codes have result in the discovery of many new codes with better Hamming distance.

Recently, Delphine Boucher et al. gave skew cyclic and skew λ-cyclic codes defined by using the skew polynomial rings with a non-trivial automorphism, which are generalization of the notion cyclic and constacyclic codes, respectively (Boucher et al., 2007; Boucher et al., 2008).

T. Abualrub, P. Seneviratre studied skew cyclic codes over F_2+vF_2, where $v^2=v$ (Abualrub and Seneviratne, 2012). T. Abualrub, A. Ghrayeb, N. Aydın, I. Siap

*Corresponding Author:abdullah.dertli@gmail.com

introduced skew quasi-cyclic codes. They obtained several new codes with Hamming distance exceeding the distance of the previously best known linear codes with comparable parameters (Abualrub et al., 2010). In (Siap et al., 2011), they studied a special type of linear codes called skew cyclic codes in the most general case. M. Bhaintwal studied skew quasi-cyclic codes over Galois rings (Bhaintwal, 2012). Wu investigated the structures of skew cyclic and skew quasi-cyclic of arbitrary length over Galois rings. They shown that the skew cyclic codes are equivalent to either cyclic and quasi-cyclic codes over Galois rings. Moreover, they gave a necessary and sufficient condition for skew cyclic codes over Galois rings to be free (Wu, 2013).

Dertli et al. studied skew codes over the finite ring to increase the probability of obtaining the large minimum distance (Dertli et al., 2015).

In the present paper, the skew λ-cyclic codes over the finite ring Y_2 are studied by using two different non-trivial automorphism over Y_2, which is motivated by the previous works.

2. Material and Methods

The ring

$$Y_2=\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4+uv\mathbb{Z}_4=\{a+bu+cv+duv\ :\ a,b,c,d\in\mathbb{Z}_4, u^2=0, v^2=0, uv=vu\}$$

is commutative ring with 4^4 elements and characteristic 4. A linear code $\wp$ over Y_2 of length n is a Y_2 submodule of Y_2^n. An element of $\wp$ is called a codeword.

We defined two Gray maps as follows

$$\Psi_1 : Y_2 \to \mathbb{Z}_4^4$$
$$a+bu+cv+duv \mapsto (a, b-a, c-a, d-a)$$

and

$$\Psi_2 : Y_2 \to \mathbb{Z}_4^8$$
$$a+bu+cv+duv \mapsto (a, 3a, b, 3b, c, 3c, d, 3d)$$

The Gray map Ψ_t can be extended to Y_2^n, naturally, for $t=1,2$.

The Lee weight on $\mathbb{Z}_4$, denoted w_L, is defined as

$$w_L(\eta)=\begin{cases}0, & \eta=0\\ 1, & \eta=1 \text{ or } 3\\ 2, & \eta=2\end{cases}$$

For any $\xi\in Y_2$, the Lee weight of ξ is defined as

$$w_L(\xi)=w_L(\Psi_t(\xi))=\sum_{i=1}^{r} w_L(\eta_i)$$

where $\Psi_t(\xi)=(\eta_1,\eta_2,\dots,\eta_r)$, $\eta_i\in\mathbb{Z}_4, i=1,2,\dots,r, t=1,2.$ The Lee weight of a vector $e=(e_1,\dots,e_n)\in Y_2^n$ is defined to be a sum of the Lee weights of its components, that is $w_L(e)=\sum_{i=1}^{n} w_L(e_i)$. Moreover, for any $e_1,e_2\in Y_2^n$, the Lee distance between e_1 and e_2 is defined as $d_L(e_1,e_2)=w_L(e_1-e_2)$.

Theorem 2.1: *The Gray map Ψ_t is a linear and distance preserving map, for $t=1,2$.*

A code $\wp$ over Y_2 is a λ-cyclic code with the property that if $e=(e_0,e_1,\dots,e_{n-1})\in\wp$ then $\nu(\wp)=(\lambda e_{n-1},e_0,\dots,e_{n-2})\in\wp$ where λ is a unit element of Y_2. A subset $\wp$ of Y_2^n is a λ-cyclic code of length n if and only if it is polynomial representation is an ideal of $Y_2[x]/\langle x^n-\lambda\rangle$. If λ is equal to $1(-1)$, the $\wp$ is called cyclic code (negacyclic code), respectively.

3. Research Findings

3.1. Skew codes over Y_2

Let Y_2 be a finite ring and Ω_i be a non-trivial automorphism over Y_2 and $\lambda=1+u+v+uv$, $i=1,2$.

Definition 3.1.1: *A subset $\wp$ of Y_2^n is called a skew λ-cyclic code of length n if $\wp$ satisfies the following conditions, for $i=1,2$,*

1) *$\wp$ is a submodule of Y_2^n*
2) *If $c=(c_0,c_1,...,c_{n-1})\in\wp$, then $\sigma_{\Omega_i}(c)=(\lambda\Omega_i(c_{n-1}),\Omega_i(c_0),...,\Omega_i(c_{n-2}))\in\wp$, where σ_{Ω_i} is the skew λ-cyclic shift operator.*

By defining two non-trivial automorphisms over Y_2 as follows, we can define the skew λ-cyclic codes over Y_2.

$$\Omega_1:Y_2\to Y_2$$
$$a+bu+cv+duv\mapsto a+cu+bv+duv$$

and

$$\Omega_2:Y_2\to Y_2$$
$$a+bu+cv+duv\mapsto a-bu-cv+duv$$

The order of Ω_i is 2, where $i=1,2$.

The rings

$$Y_2[x,\Omega_i]=\{b_0+b_1x+...+b_{n-1}x^{n-1}\ :\ b_j\in Y_2, n\in N,\ j=0,1,...,n-1\}$$

are called skew polynomial rings with the usual addition of polynomials and the multiplication as follows

$$(ax^s)(bx^l)=a\Omega_i^s(b)x^{s+l}$$

where $i=1,2$. They are non-commutative rings.

In polynomial representation, a skew λ-cyclic code of length n over Y_2 is defined as a left ideal of the quotient ring $A_{\Omega_i,n}=Y_2[x,\Omega_i]/\langle x^n-\lambda\rangle$, if the order of Ω_i divides n, that is n is even. If the order of Ω_i does not divides n, a skew λ-cyclic code of length n over Y_2 is defined as a left $Y_2[x,\Omega_i]$-submodule of $A_{\Omega_i,n}$, since the set

$$A_{\Omega_i,n}=Y_2[x,\Omega_i]/\langle x^n-\lambda\rangle=\{f_i(x)+\langle x^n-\lambda\rangle\ :\ f_i(x)\in Y_2[x,\Omega_i]\}$$

is a left $Y_2[x,\Omega_i]$-module, for $i=1,2$.

In both case, the following is hold.

Theorem 3.1.2: *Let $\wp$ be a skew λ-cyclic code over Y_2 and let $g(x)$ be a polynomial in $\wp$ of minimal degree. If the leading coefficient of $g(x)$ is a unit in Y_2, then $\wp=\langle g(x)\rangle$, where $g(x)$ is a right divisor of $x^n-\lambda$.*

Proof: It is proved as in the proof of Lemma 3 and Theorem 1 in (Gao et al., 2017).

Proposition 3.1.3: *Let* Ω_1, ν *and* Ψ_1 *be as above. Then* $\Psi_1\sigma_{\Omega_1} = \rho\Psi_1\nu$, *where* ρ *is a permutation defined by*

$$\rho(x,y,k,p) = (x,k,y,p)$$

for $x,y,k,p \in \mathbb{Z}_4^n$.

Proof: Let $e_i = a_i + b_i u + c_i v + d_i uv$ be the elements of Y_2 for $i = 0,1,\ldots,n-1$. Then

$$\sigma_{\Omega_1}(e_0,\ldots,e_{n-1}) = (\lambda\Omega_1(e_{n-1}),\Omega_1(e_0),\ldots,\Omega_1(e_{n-2})) = \begin{pmatrix} a_{n-1} + (a_{n-1}+c_{n-1})u + (a_{n-1}+b_{n-1})v + \\ (a_{n-1}+b_{n-1}+c_{n-1}+d_{n-1})uv, a_0 + c_0 u + b_0 v + d_0 uv \\ ,\ldots, a_{n-2} + c_{n-2}u + b_{n-2}v + d_{n-2}uv \end{pmatrix}.$$

By applying Ψ_1, we have

$$\Psi_1(\sigma_{\Omega_1}(e_0,\ldots,e_{n-1})) = \begin{pmatrix} a_{n-1},\ldots a_{n-2}, c_{n-1},\ldots, c_{n-2} - a_{n-2}, b_{n-1},\ldots, \\ b_{n-2}, -a_{n-2}, b_{n-1} + c_{n-1} + d_{n-1},\ldots, d_{n-2} - a_{n-2} \end{pmatrix}.$$

On the other hand

$$\Psi_1\nu(e_0,\ldots,e_{n-1}) = \begin{pmatrix} a_{n-1},\ldots a_{n-2}, b_{n-1},\ldots, b_{n-2} - a_{n-2}, c_{n-1},\ldots, \\ c_{n-2}, -a_{n-2}, b_{n-1} + c_{n-1} + d_{n-1},\ldots, d_{n-2} - a_{n-2} \end{pmatrix}.$$

If we apply ρ, we have

$$\rho\Psi_1\nu(e_0,\ldots,e_{n-1}) = \begin{pmatrix} a_{n-1},\ldots a_{n-2}, c_{n-1},\ldots, c_{n-2} - a_{n-2}, b_{n-1},\ldots, \\ b_{n-2}, -a_{n-2}, b_{n-1} + c_{n-1} + d_{n-1},\ldots, d_{n-2} - a_{n-2} \end{pmatrix}.$$

We have the expected result.

Theorem 3.1.4: *The Gray image of a skew* λ*-cyclic code over* Y_2 *of length* n *is permutation equivalent to a* λ*-cyclic code over* $\mathbb{Z}_4$ *of length* $4n$.

Proof: Let $\wp$ be a skew λ-cyclic code over Y_2 of length n. That is $\sigma_{\Omega_1}(\wp) = \wp$. If we apply Ψ_1, we have $\Psi_1(\sigma_{\Omega_1}(\wp)) = \Psi_1(\wp)$. From Proposition 3.1.3, we get $\Psi_1(\sigma_{\Omega_1}(\wp)) = \Psi_1(\wp) = \rho\Psi_1\nu(\wp)$. So $\Psi_1(\wp)$ is permutation equivalent to a λ-cyclic code over $\mathbb{Z}_4$ of length $4n$.

Proposition 3.1.5: *Let* Ω_2, ν *and* Ψ_2 *be as above. Then* $\Psi_2\sigma_{\Omega_2} = \psi\Psi_2\nu$, *where* ψ *is a permutation defined by*

$$\psi(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = (x_1,x_2,x_4,x_3,x_6,x_5,x_7,x_8)$$

for $x_i \in \mathbb{Z}_4^n, i = 1,2,\ldots,8$.

Proof: It is proved as in the proof of the Proposition 3.1.3.

Theorem 3.1.6: *The Gray image of a skew* λ*-cyclic code over* Y_2 *of length* n *is permutation equivalent to a* λ*-cyclic code over* $\mathbb{Z}_4$ *of length* $8n$.

Proof: It is proved as in the proof of the Theorem 3.1.4.

Example 3.1.7: *Let* $n = 3$. *We have*

$$x^3 - \lambda = \left(x^2 + (1-u-v+uv)x + (1-u-v)\right)\left(x - (1-u-v+uv)\right)$$

in $Y_2[x,\Omega_i]$, *for* $i = 1,2$.

Let $g(x) = x - (1-u-v+uv)$. *Then* $g(x)$ *generates a skew* λ*-cyclic code of length 3 with the minimum distance* $d = 2$. *This code is permutation equivalent to a* λ*-cyclic code of length 12 (24) over* $\mathbb{Z}_4$.

4. Conclusion

The skew λ-cyclic codes over the finite ring Y_2 are studied because of to increase the probability of obtaining the large minimum distance. A new two Gray maps and two non-trivial automorphisms over Y_2 are defined and the Gray images of skew λ-cyclic codes are determined. So, we can obtain many new codes with better Hamming distance.

5. References

Abualrub T., Seneviratne P. 2012. "On θ-cyclic codes over F_2+vF_2", *Australasian Journal of Com.*, 54, 115-126.

Abualrub T., Ghrayeb A., Aydın N., Siap I. 2010. "On the construction of skew quasi-cyclic codes", *IEEE Transsactions on Information Theory*, 56, 2081-2090.

Bhaintwal M. 2012., "Skew quasi-cyclic codes over Galois rings", *Designs, codes and Cryptography*, 62, 85-101.

Boucher D., Willi G., Ulmer F. 2007. "Skew cyclic codes", *Applicable Algebra in Engineering, Communication and Computing*, 17, 379-389.

Boucher D., Sole P., Ulmer F. 2008. "Skew constacyclic codes over Galois rings", *Advances in mathematics of communications*, 3, 273-292.

Dertli A., Cengellenmis Y., Eren S. 2015. On "Skew Cyclic and Quasi-cyclic Codes over $F_2+vF_2+uF_2$", *Palestine Journal of Mathematics*, 4, 540-546.

Gao J., Fanghui M., Fu F. 2017. "Skew constacyclic codes over the ring F_q+vF_q", *Applied Mathematics and Computing*, 6, 286-295.

Siap I, Abualrub T., Aydın N., Seneviratne P. 2011. "Skew cyclic codes of arbitrary length", *Int. Journal of Information and Coding Theory*, 2, 10-20.

Wu M. 2013. "Skew cyclic and quasi-cyclic codes of arbitrary length over Galois rings", *International Journal of Algebra*, 7, 803–807.