Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 7, S. 460-465, 10, 2023
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

IJANSER
https://alls-academy.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 7, pp. 460-465, 10, 2023
Copyright © 2023 IJANSER
Research Article

Inverse Quasi-Cyclic Codes and Automorphism Cyclic Codes

Mustafa ÖZKAN[1*]

[1] *Mathematics and life Science Department / Faculty of Education, Trakya University, Turkiye*

[*] *mustafaozkan@trakya.edu.tr*

(Received: 21 November 2023, Accepted: 27 November 2023)

(4th International Conference on Engineering and Applied Natural Sciences ICEANS 2023, November 20-21, 2023)

ATIF/REFERENCE: Özkan, M. (2023). Inverse Quasi-Cyclic Codes and Automorphism Cyclic Codes. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(10), 460-465.

Abstract – Certain information is included to introduce cyclic codes on the finite ring. These are the structure of the ring, its status as a linear code, weight function and distance concepts. Here the Lee weight function is given for the ring. An automorphism is defined on the ring. With the help of defined function, the composition of automorphism cyclic codes was constructed. A separate isometry is defined to determine the correspondences of the codes on the rings on the objects. Then, the definition of the inverse quasi-cyclic code is given and certain propositions and theorems are presented. It has been shown that the image code of a code under isometry and the inverse quasi-cyclic shift transformation are the same code as automorphism and the image of a cyclic code under isometry is the same code. Moreover, the results and proofs regarding the written permutation, inverse quasi-cyclic code and automorphism cyclic codes are included.

Anahtar Kelimeler –Cyclic Codes, Automorphism Codes, Quasi-Cyclic Codes, Lee Distance, Gray Map.

I. INTRODUCTION

Many codes have been studied on finite rings. One of these finite rings is the 4 element $IF_2[u] / < u^2 >$ ring in the $u^2 = 0$ state. These 4 element rings were used in the codes written in this study. This ring has been featured in many studies before. One of them is the work of Qian and his team in [5], published in 2006. Cyclic and constacyclic codes are included in this ring. Another one is the article in [9] published by Özkan M., Öke F. in 2016. In this article, the hadamard codes on this ring are presented.

Below is information about this ring.

$IF_2 = GF(2)$ to be Galois Field,

$$IF_2[u] / < u^2 > =$$

$$\{ m_0 + u\, m_1 + < u^2 > \mid m_0 , m_1 \in IF_2 \}$$

ring in case $u^2 = 0$ $\quad m_0 + u\, m_1 + < 0 >$

$$= \{ m_0 + u\, m_1 + 0.k \mid m_0 , m_1 \in IF_2 \ , k \in IF_2[u] \}$$

$= \{ m_0 + u\, m_1 \}$ since it will be in the form

$$IF_2[u] / < u^2 > = \{ \{ m_0 + u\, m_1 \} \mid m_0 , m_1 \in IF_2 \}$$

is written. In case of $u^2=0$, $IF_2[u] \Big/ <u^2>$ = $\{ \{m_0+u\,m_1\} \mid m_0, m_1 \in IF_2 \}$ is also a ring. Thus, $R = IF_2 + u\,IF_2 = \{ m_0+u\,m_1 \mid m_0, m_1 \in IF_2 \}$ is a ring where $u^2=0$. There is an isomorphism defined in the form of

$$f : IF_2 + u\,IF_2 \longrightarrow IF_2[u] \Big/ <u^2>$$

$$m_0+u\,m_1 \mapsto f(m_0+u\,m_1) = \{m_0+u\,m_1\}$$

between the R and $IF_2[u] \Big/ <u^2>$ rings.

This situation is indicated by

$$R = IF_2 + u\,IF_2 := IF_2[u] \Big/ <u^2> .$$

Notation: By saying $C \subseteq R^n$, it will be understood that C is a linear code of length n in R.

II. BASIC KNOWLEDGE

2.1 Definition : Let it be IF_q equal $GF(q)$. The Hamming weight of any element $x=(x_1,x_2,...,x_n)$ of the vector space IF_q^n is defined as

$$w_H(x) = \left| \{ i \mid for\, i=1,2,...,n,\ x_i \neq 0,\ x_i \in IF_q \} \right|$$

If C is a linear code of length n over IF_q, then $w_H(C) = \min\{ w_H(x) \mid x \neq 0,\ x \in C \}$ is descriptioned the minimum Hamming weight of C code.

The function d_H defined as $d_H(x,y) = w_H(x-y)$ for each $x, y \in IF_q^n$ is called the Hamming distance. If is a linear code of length n over IF_q, then $w_H(C) = \min\{ w_H(x) \mid x \neq 0,\ x \in C \}$ is called the minimum Hamming distance of C code.

2.2 Definition : If C is a code of length n over the ring $R = IF_2 + u\,IF_2$, Lee weight of the $c=(c_0,c_1,...,c_{n-1}) \in C$ codeword ,

$$w_L(0)=0 ,$$

$$w_L(1)=1 ,$$

$$w_L(u)=2$$

$$w_L(1+u)=1 \quad \text{including} ,$$

It is defined as $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$.

For $d_L(c,d) = w_L(c-d)$ every $c, d \in R^n$. The function defined d_L as is called Lee distance . If C is a linear code of length n on R, The minimum Lee distance is defined as

$$d_L(C) = \min\{ w_L(c) \mid c \in C \setminus \{0\} \}.$$

2.3 Definition: Let D be a linear code of length $2n$ over IF_2 . For transformation

$$\sigma : IF_2^{2n} \longrightarrow IF_2^{2n}$$

$$(d_0,d_1,...,d_{2n-1}) \mapsto \sigma(d_0,d_1,...,d_{2n-1})$$

$$\sigma(d_0,d_1,...,d_{2n-1}) = (d_{2n-1},d_0,d_1,...,d_{2n-2})$$

If $\sigma(D)=D$, the D code is defined a cyclic code of length $2n$.

2.4 Definition :

$$\theta : IF_2 + u\,IF_2 \longrightarrow IF_2 + u\,IF_2$$

$$a \mapsto (1+u).a$$

It is a transformation that leaves the Lee distance constant. Using this transformation

$$\Psi : R^n \longrightarrow R^n$$

$$(s_0, s_1, ..., s_{n-1}) \mapsto \Psi(s_0, s_1, ..., s_{n-1})$$

$\Psi(s_0, s_1, ..., s_{n-1}) = (\theta(s_{n-1}), \theta(s_0), ..., \theta(s_{n-2}))$ be defined .

Let E is a code of length n over the ring $R = IF_2 + u\,IF_2$. For Ψ transformation, if $\Psi(E) = E$, E linear code is defined a automorphism cyclic code of length n.

2.5 Definition: $R = IF_2 + uIF_2$ a ring to be

$$\Phi : R^n \longrightarrow IF_2^{2n}$$

$$(y_0, y_1, ..., y_{n-1}) \mapsto \Phi(y_0, y_1, ..., y_{n-1})$$

$$\Phi(y_0, y_1, ..., y_{n-1}) = (p_0, p_1, ..., p_{n-1}, t_0 + p_0, ..., t_{n-1} + p_{n-1})$$

$$(\, y_i = t_i + u\,p_i \quad , \quad 0 \le i \le n-1 \,)$$

the transformation defined in the form is called the Gray transformation on R^n .

Gray transformation on R as well

$$\Phi : R = IF_2 + uIF_2 \longrightarrow IF_2^2$$

$$t + u\,p \mapsto \Phi(t + u\,p) = (p\ , t + p)$$

It is in the form .

2.6 Proposition : let $R = IF_2 + uIF_2$ a ring, Gray transform on R^n is a $R\_$ module homomorphism and an isometry.

Proof: Let's show that the Gray transform is $R\_$ a module homomorphism .

$$\Phi : R^n \longrightarrow IF_2^{2n}$$

$$(y_0, y_1, ..., y_{n-1}) \mapsto \Phi(y_0, y_1, ..., y_{n-1})$$

$$\Phi(y_0, y_1, ..., y_{n-1}) = (p_0, p_1, ..., p_{n-1}, p_0 + t_0, ..., p_{n-1} + t_{n-1})$$

$\forall\ z, l \in R^n$ let's get

$$\exists\ y_i = t_i + u\,p_i\ ,\ l_i = v_i + u\,s_i \quad (0 \le i \le n-1)$$

$\ni t_i, p_i, v_i, s_i \in IF_2$ and

$y = (y_0, y_1, ..., y_{n-1})$, $l = (l_0, l_1, ..., l_{n-1})$ is possible .

$$\Phi(y + l) = \Phi((y_0, ..., y_{n-1}) + (l_0, ..., l_{n-1}))$$

$$= \Phi(y_0 + l_0, ..., y_{n-1} + l_{n-1})$$

$$= \Phi(t_0 + u\,p_0 + v_0 + u\,s_0, ..., t_{n-1} + u\,p_{n-1} + v_{n-1} + u\,s_{n-1})$$

$$= \Phi((t_0 + v_0) + u(p_0 + s_0), ..., (t_{n-1} + v_{n-1}) + u(p_{n-1} + s_{n-1}))$$

$$= (p_0 + s_0, ..., p_{n-1} + s_{n-1}, p_0 + s_0 + t_0 + v_0, ..., p_{n-1} + s_{n-1} + t_{n-1} + v_{n-1})$$

$$= (p_0, p_1, ..., p_{n-1}, p_0 + t_0, ..., p_{n-1} + t_{n-1}) + (s_0, s_1, ..., s_{n-1}, s_0 + v_0, ..., s_{n-1} + v_{n-1})$$

$= \Phi(y) + \Phi(l)$ is provided .

$\forall\, y \in R^n$ And $\forall\, \alpha \in R$ let's get

$y = (y_0, y_1, ..., y_{n-1})$ it is

$$\Phi(\alpha.y) = \Phi(\alpha.(y_0, ..., y_{n-1}))$$

$$= \Phi(\alpha.y_0,...,\alpha.y_{n-1})$$

$$= \Phi(\alpha(t_0 + u\,p_0),...,\alpha(t_{n-1} + u\,p_{n-1}))$$

$$= \Phi(\alpha.t_0 + u\,\alpha.p_0,...,\alpha.t_{n-1} + u\alpha.\,p_{n-1}))$$

$$= (\alpha.p_0,...,\alpha.p_{n-1},\alpha.(t_0 + p_0),...,\alpha.(t_{n-1} + p_{n-1}))$$

$$= \alpha.(p_0,..., p_{n-1}, t_0 + p_0,..., t_{n-1} + p_{n-1})$$

$$= \alpha.\Phi(y) \quad .$$

$\therefore \Phi \quad R\_$ module is a homomorphism .

Minimum Lee distance d_L of R^n above, minimum Hamming distance d_H of IF_2^{2n} It is easy to see that there is a metric on it . Let us show Φ that is an isometry.So $c_1 = (d_0, d_1,..., d_{n-1}) \in R^n$ for every $c_2 = (e_0, e_1,..., e_{n-1}) \in R^n$

$d_L(c_1, c_2) = d_H(\Phi(c_1), \Phi(c_2))$ Let's show that it is

$$\Phi :\ R = IF_2 + u\,IF_2 \longrightarrow IF_2^2$$

$$t + u\,p \mapsto \Phi(t + u\,p) = (p\,, p + t)$$

transform and $R = IF_2 + u\,IF_2 = \{\ 0,1,u\,,1+u\ \}$

Lee weights of the elements of the ring

Using $w_L\,(0)=0$, $w_L\,(1)=1$, $w_L\,(u)=2$ and $w_L\,(1+u\ )=1$ where

$w_H(\Phi(0)) = w_H(\Phi(0+u.0)) = w_H(0,0)$,

$w_H(\Phi(1)) = w_H(\Phi(1+u.0)) = w_H(0,1)$,

$w_H(\Phi(u)) = w_H(\Phi(0+u.1)) = w_H(1,1)$ and

$w_H(\Phi(1+u\ )) = w_H(\Phi(1+u.1)) = w_H(1,0)$,

is obtained .

$\therefore \forall c \in R = IF_2 + u\,IF_2,\ w_L(c) = w_H(\Phi(c))$ ... (1)

for

$\forall\ c_1 = (d_0, d_1,..., d_{n-1}),\ c_2 = (e_0, e_1,..., e_{n-1}) \in R^n$,

$$d_L(c_1, c_2) \ = \ w_L(c_1 - c_2)$$

$$= \ w_L((d_0, d_1,..., d_{n-1}) - (e_0, e_1,..., e_{n-1}))$$

$$= \ w_L(d_0 - e_0, d_1 - e_1,..., d_{n-1} - e_{n-1})$$

$$= \sum_{i=0}^{n-1}\ w_L\,(d_i - e_i\,)$$

$(d_i\,, e_i \in R\ , d_i - e_i \in R)$

$$= \sum_{i=0}^{n-1}\ w_H\,(\Phi(d_i - e_i\,))\,\text{(from (2))}$$

$$= \sum_{i=0}^{n-1}\ w_H\,(\Phi(d_i) - \Phi(e_i\,))$$

$(\Phi \quad R_$module homomorphism)

$$= \ w_H\,(\Phi(c_1) - \Phi(c_2))$$

$$= \ d_H(\Phi(c_1), \Phi(c_2)) \quad \text{is obtained..}$$

$\therefore\ \Phi$ The transformation is an isometry.

$\therefore\ \Phi \quad R_$module homomorphism is an isometry.

2.7 Proposition [10]:

$$\overline{\mu} : R^n \longrightarrow R^n$$

$$(d_0, d_1,..., d_{n-1}) \mapsto \overline{\mu}(d_0, d_1,..., d_{n-1})$$

$$= (1+u).\,(d_0, d_1,..., d_{n-1})$$

a permutation defined in the form be given.

$D \subseteq R^n$ code is cyclic code if ony if $\overline{\mu}\ (D)$ code automorphism cyclic code.

III. INVERSE QUASI CYCLIC CODES AND AUTOMORPHISM CYCLIC CODES

3.1 Definition: Let D be a linear code of length $2n$ over $IF_2 = GF(2)$.

$$\sigma_{-1}^{\otimes 2} \ : \ IF_2^{2n} \longrightarrow IF_2^{2n}$$

$$(a_0, a_1, ..., a_{2n-1}) \mapsto \sigma_{-1}^{\otimes 2} \ (a_0, a_1, ..., a_{2n-1})$$

$$\sigma_{-1}^{\otimes 2} \ (a_0, a_1, ..., a_{2n-1}) = (b_1, b_2, ..., b_{2n})$$

$$b_i = \begin{cases} a_{2n-1} & ; \quad i = 1 \\ a_{i+n-2} & ; \quad i = 2,3,...,n \\ a_{n-1} & ; \quad i = n+1 \\ a_{i-n-2} & ; \quad i = n+2,...,2n \end{cases}$$

Let's define a transformation in the form . If $\sigma_{-1}^{\otimes 2}(D) = D$, so the code is called an D inverse quasi-cyclic code of order 2 .

3.2 Proposition : if $\Phi : R^n \longrightarrow IF_2^{2n}$ and $\Psi : R^n \longrightarrow R^n$ their transformations are as in the 4th and 5th definitions. $\Phi \circ \Psi = \sigma_{-1}^{\otimes 2} \circ \Phi$ is obtained .

Proof:

$$\begin{tikzcd} IF_2^{2n} \arrow[d, "\sigma_{-1}^{\otimes 2}"'] & R^n \arrow[l, "\Phi"'] \arrow[d, "\Psi"] \\ IF_2^{2n} & R^n \arrow[l, "\Phi"] \end{tikzcd}$$

every $(a_0, a_1, ..., a_{n-1}) \in R^n$ and

$a_i = t_i + u\, p_i \quad \ni t_i\, ,\, p_i \in IF_2$ including

$i = 0,1,...,n-1$

$$(\Phi \circ \Psi)\ (a_0, a_1, ..., a_{n-1}) = \Phi(\Psi(a_0, a_1, ..., a_{n-1}))$$

$$= \Phi(\theta(a_{n-1}), \theta(a_0), ..., \theta(a_{n-2}))$$

$$= \Phi((1+u).a_{n-1}, (1+u).a_0, ..., (1+u).a_{n-2}))$$

$$= \Phi((1+u).(t_{n-1} + u\, p_{n-1}), (1+u).(t_0 + u\, p_0), ..., (1+u).(t_{n-2} + u\, p_{n-2}))$$

$$= (t_{n-1} + p_{n-1}, t_0 + p_0, ..., t_{n-2} + p_{n-2}, t_{n-1}, p_0, ..., p_{n-2})$$

is found . On the other hand

$$(\sigma_{-1}^{\otimes 2} \circ \Phi)\ (a_0, a_1, ..., a_{n-1}) =$$

$$\sigma_{-1}^{\otimes 2}\ (\Phi(a_0, a_1, ..., a_{n-1}))$$

$$= \sigma_{-1}^{\otimes 2}\ (\Phi(t_0 + u\, p_0, t_1 + u\, p_1, ..., t_{n-1} + u\, p_{n-1}))$$

$$= \sigma_{-1}^{\otimes 2}\ (p_0, p_1, ..., p_{n-1}, t_0 + p_0, t_1 + p_1, ..., t_{n-1} + p_{n-1})$$

$$= (d_1, d_2, ..., d_{2n})$$

$$d_i = \begin{cases} r_{n-1} + q_{n-1} & ; \quad i = 1 \\ r_{i-2} + q_{i-2} & ; \quad i = 2,3,...,n \\ q_{n-1} & ; \quad i = n+1 \\ q_{i-n-2} & ; \quad i = n+2,...,2n \end{cases}$$

is obtained.

$$\therefore\ \Phi \circ \Psi = \sigma_{-1}^{\otimes 2} \circ \Phi \quad \text{is possible .}$$

3.3 Theorem : If C automorphism cyclic code on R, C code of image of the code under Gray transformation is a 2nd order inverse quasi-cyclic code.

proof : Let C be automorphism cyclic code.

$$\Psi : R^n \longrightarrow R^n$$

$$(c_0, c_1, ..., c_{n-1}) \mapsto \Psi(c_0, c_1, ..., c_{n-1})$$

$$\Psi(c_0, c_1, ..., c_{n-1}) = (\theta(c_{n-1}), \theta(c_0), ..., \theta(c_{n-2}))$$

using the transformation for every $c \in C$, $\Psi(c) = c'$ is possible . ($c' \in C$)

$\Rightarrow \quad \Phi(\Psi(c)) = \Phi(c')$ It is possible . … (2)

Since it is known from 3.2 proposition that

$\forall\ c \in C$ for $\Phi\ (\Psi(c)) = \sigma_{-1}^{\otimes 2}(\Phi(c))$

using (2) $\Phi(\Psi(c)) = \sigma_{-1}^{\otimes 2}(\Phi(c)) = \Phi(c')$.

Therefore, $c, c' \in C$ it is $\Phi(C)$ an inverse quasi-cyclic code of order 2 .

REFERENCES

[1] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error Correcting Codes,North-Holland Publishing Company, 1977.

[2] J.Wolfmann, Negacyclic and cyclic codes over $\mathbf{Z}_4$, IEEE Trans. Inf. Theory, Vol. 45, 2527-2532, 1999.

[3] A. Bonnecaze, P. Udaya, Cyclic codes and self dual codes $\mathrm{F}_2 + u\mathrm{F}_2$, IEEE Trans. Inf. Theory , Vol. 45, 1250-1255,1999.

[4] S. Ling, C. Xing, Coding Theory A First Course , Cambridge University Pres, 2004.

[5] J. Qian, L. Zhang and S. Zhu, $(1+u)\_$ cyclic and cyclic codes over the ring $\mathrm{F}_2 + u\mathrm{F}_2$, Applied Mathematics Letters, Vol.19, 820-823, 2006.

[6] D. Boucher, W. Geiselmann, and F. Ulmer, Skew-Cyclic Codes, Applicable Algebra in Engineering, Communication and Computing, Vol. 18, 379-389,2007.

[7] M.C.V. Amarra and F.R Nemenzo., On $(1-u)\_$ cyclic codes over $IF_{p^k} + uIF_{p^k}$,Applied Mathematics Letters,21,1129-1133,2008.

[8] S. Zhu, Y. Wang, M. Shi, Some Result On Cyclic Codes over $\mathrm{F}_2 + v\mathrm{F}_2$, IEEE Trans. Inf. Theory , Vol.56, 4, 1680-1684, 2010.

[9] M. Özkan, F. Öke, A relation between Hadamard codes and some special codes over $\mathrm{F}_2 + u\mathrm{F}_2$, App. Mathematics and Inf. Sci.,Vol.10, 2, 701-704, 2016.

[10] M. Özkan, automorphism cyclic codes on $\mathrm{F}_2 + u\mathrm{F}_2$, Areast 2 nd international conference on applied sciences conference book, ISBN: 978-625-6830-51-6, 174-180,2023.