Uluslararası İleri Doğa
Bilimleri ve Mühendislik
Araştırmaları Dergisi
Sayı 7, S. 113-118, 11, 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. 113-118, 11, 2023
Copyright © 2023 IJANSER
Research Article

Inverse Quasi Cyclic Code and Application in Chain Ring

Mustafa ÖZKAN[1*]

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

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

(Received: 03 December 2023, Accepted: 11 December 2023)

(2nd International Conference on Frontiers in Academic Research ICFAR 2023, December 4-5, 2023)

ATIF/REFERENCE: Özkan, M. (2023). Inverse Quasi Cyclic Code and Application in Chain Ring. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(11), 113-118.

Abstract *–* The existence of inverse quasi-cyclic codes in the $\mathrm{F}_2 + u\mathrm{F}_2$ ring is presented. Here, Gray transform and inverse quasi cyclic code definitions are given first. Afterwards, its relationship with automorphism and cyclic codes is mentioned. The proposition including Nechaev permutation, quasi cyclic codes and Gray transformation is explained. From this it is concluded that inverse quasi cyclic codes correspond to Gray images of the cyclic code. Finally, a 4-length repeat code example is included regarding this topic.

Key Words – Chain Rings, Linear Codes, Cyclic Codes, Quasi-Cyclic Codes, Gray Map.

I. INTRODUCTION

Chain in the ring well ideals ranked in rings coding theory with relating to studies in literature place is taking. In this study chain of the ring Workman number is four. One of these finite rings is the 4 element $IF_2[u]\big/_{<u^2>}$ 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.

This ring from studies some Qian and of the team, Bonnecazeye And Udaya's and Zhu and belongs to the team [5], [3] and [8]. Moreover, Ozkan and Oke by written This ring in his studies place [9].

This study is a continuation of the study titled Inverse Quasi-Cyclic Codes and Automorphism Cyclic Codes in [11]. The following basis information is also available in

[11] place is taking . Below is information about this ring.

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

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

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

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

is written. $u^2 = 0$ to be in case $IF_2\left[u\right]\Big/_{<u^2>} = \left\{m_0 + u\,m_1 + <u^2> \mid m_0\,, m_1 \in IF_2 \right\}$ ring $\mathrm{F}_2 + u\mathrm{F}_2$ to the ring isomorphic . $\mathrm{F}_2 + u\mathrm{F}_2$ $= \left\{0,1,u,1+u\right\}$ in below defined $+$ and $\bullet$ operations is a ring .

$+$	0	1	u	$1+u$
0	0	1	u	$1+u$
1	1	0	$1+u$	u
u	u	$1+u$	0	1
$1+u$	$1+u$	u	1	0

$\bullet$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

$R = \mathrm{F}_2 + u\mathrm{F}_2$ ring have three ideal . these ideals $\langle 0\rangle$,$\langle 1\rangle$ and $\langle u\rangle$ is $\langle 0\rangle \subseteq \langle u\rangle \subseteq \langle 1\rangle = R$ is provided.

II. PRELIMINARIES

This chapter given definition, proposition and concepts in 2023, M. Özkan by written automorphism cyclic codes on $\mathrm{F}_2 + u\mathrm{F}_2$ and titled Inverse Quasi-Cyclic Codes and Automorphism Cyclic Codes from his work has been written.

The following definition object on you gives distance. Linear in codes weight concept with distance concept each other equal, it is possible.

2.1 Definition: on F_2 field;

each $c \in \mathrm{F}_2$ for $w_H(c) = \begin{cases} 0 & , \ c = 0 \\ 1 & , \ c = 1 \end{cases}$

form defined to function F_2 Hamming weight on function It is called. In this case every $c = (c_1, c_2, ..., c_n) \in \mathrm{F}_2^n$ for $w_H(c) = \sum_{i=1}^{n} w_H(c_i)$. It is possible.

The following definition 4 elements $R = IF_2 + u\,IF_2$ of the ring elements on you It gives the distance (weight).

2.2 Definition: on $R = \mathrm{F}_2 + u\mathrm{F}_2$ ring;

each $r \in R$ for $w_L(r) = \begin{cases} 0 & , \ r = 0 \\ 1 & , \ r = 1, 1+u \\ 2 & , \ r = u \end{cases}$

form defined to the function, Lee weight function on R is called .

This case every $r = (r_1, r_2, ..., r_n) \in R^n$ for $w_L(r) = \sum_{i=1}^{n} w_L(r_i)$ equality is realised .

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 $d_L(C) = \min\left\{d_L(a,b) \mid a,b \in C, a \neq b\right\}$.

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

F_2^n de Lee weight instead of Hamming weight by writing similar definition is given. F_2^n on One C minimum Hamming distance of the code $d_H(C)$ with is shown.

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:

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

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

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 an automorphism cyclic code of length n.

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

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

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

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

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

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 [11]: let $R = IF_2 + uIF_2$ a ring Φ Gray transform on R^n is a $R_$module homomorphism and an isometry.

2.7 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 .

2.8 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.

2.9 Proposition [11]: if $\Phi:\ R^n \longrightarrow IF_2^{2n}$ and $\Psi:R^n \longrightarrow R^n$ their transformations are as in the 2.4 definition and 2.5 definition. $\Phi \circ\ \Psi=\sigma_{-1}^{\otimes 2}\circ\Phi$ isobtained .

2.10 Theorem [11]: 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.

III. INVERSE QUASI CYCLIC CODES

3.1 Definition: in the set $\{\ 0,1,2,3,...,2n-1\ \}$ $\tau=(0\ \ n).(1\ \ n+1).(2\ \ n+2)...\,(i\ \ n+i)...(n-1\ \ 2n-1)$ permutation let it be given.

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

$$(c_0,c_1,...,c_{2n-1}) \mapsto \pi(c_0,c_1,...,c_{2n-1})$$

$$\pi(c_0,c_1,...,c_{2n-1})=(c_{\tau(0)},c_{\tau(1)},...,c_{\tau(2n-1)})$$

form defined to transformation Nechaev permutation is called .

3.2 Definition and Proposition:

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

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

$$\overline{\mu}(c_0,c_1,...,c_{n-1})=(1+u).\,(c_0,c_1,...,c_{n-1})$$

form written function R^n on special One permutation aspect be defined . $D \subseteq R^n$ a cyclic code let it be. $\overline{\mu}\,(D)$ One automorphism cyclic code indicates.

3.3 Proposition: $\overline{\mu}:R^n \longrightarrow R^n$ transformation in proposition 3.2 like to be about

$\Phi \circ\ \overline{\mu}=\pi\circ\Phi$ it is possible.

Proof:

$$\begin{tikzcd}
IF_2^{2n} \arrow[d, "\pi"] & R^n \arrow[l, "\Phi"'] \arrow[d, "\overline{\mu}"] \\
IF_2^{2n} & R^n \arrow[l, "\Phi"']
\end{tikzcd}$$

Each $c=(c_0,c_1,...,c_i,...,c_{n-1})\in R^n$ let it be.

$$(\ c_i=r_i+uq_i\ ,0\le i\le n-1)$$

$$(\Phi\circ\ \overline{\mu}\ )(c)=\Phi(\overline{\mu}(c))=$$

$$\Phi((1+u).(c_0,c_1,...,c_{n-1}))$$

$$= \Phi((1+u).c_0,(1+u).c_1,...,(1+u).c_{n-1})$$

$$= \Phi((1+u).(r_0+u\,q_0),(1+u).(r_1+u\,q_1),..., (1+u).(r_{n-1}+u\,q_{n-1}))$$

$$= \Phi(r_0+u.(r_0+q_0),r_1+u.(r_1+q_1),...,r_{n-1}+u.(r_{n-1}+q_{n-1}))$$

$$=(r_0+q_0,r_1+q_1,...,r_{n-1}+q_{n-1},q_0,q_1,...,q_{n-1})$$

get is done .Other from the side

$$(\pi\circ\Phi)(c)=\pi(\Phi\ (c))=\pi(\Phi\ (c_0,c_1,...,c_{n-1}))$$

$$=\pi(\Phi\ (r_0+uq_o,r_1+uq_1,...,r_{n-1}+u\,q_{n-1}))$$

$$=\pi(q_0,q_1,...,q_{n-1},r_0+q_0,r_1+q_1,...,r_{n-1}+q_{n-1})$$

$$=(r_0+q_0,r_1+q_1,...,r_{n-1}+q_{n-1},q_0,q_1,...,q_{n-1})$$

it is possible. From here $\forall\ c\in R^n$ for

$(\Phi\circ\bar{\mu})(c)=(\pi\circ\Phi)(c)$ is possible.

$\therefore\ \Phi\circ\bar{\mu}=\pi\circ\Phi$ it is possible.

IV. CONCLUSION AND APPLICATION

4.1 Conclusion: in R One D Gray images of cyclic code under image $\Phi(D)=\Gamma$ whereas $\pi(\Gamma)$ having order 2 One is the inverse quasi-cyclic code.

Proof: D R de cyclic code And $\Phi(D)=\Gamma$ let it be. From $\Phi(\bar{\mu}(D))=\pi(\Phi(D))=\pi(\Gamma)$ Proposition 3.3 will happen and Propositions 2.8 from $\bar{\mu}(D)$ skew cyclic code is since it is seen. Above theorem using $\Phi(\bar{\mu}(D))$ of having order 2 inverse quasi-cyclic code will happen to the conclusion is reached.

4.2 Example: $R=IF_2+u\,IF_2$ ring on 4_length $C=\{(0,0,0,0),(u,u,u,u)\}$ code let it be given C both cyclic code and both a skew-cyclic is the code . Gray conversion of this code under image

$\Phi(C)=\{(0,0,0,0,0,0,0,0),(1,1,1,1,1,1,1,1)\}$ IF_2 de 8-long is the code .C minimum Lee distance of the code ; $d_L(C)=8$ And $\Phi(C)$ minimum Hamming distance of the code ; $d_H(\Phi(C))=8$ work.

$\bar{\mu}(0,0,0,0)=(0,0,0,0)$ And $\bar{\mu}(u,u,u,u)=(u,u,u,u)$ since $\bar{\mu}(C)=C$ It is possible.

$$\sigma_{-1}^{\otimes 2}(\Phi(u,u,u,u))=\sigma_{-1}^{\otimes 2}(1,1,1,1,1,1,1,1)$$

$$=(1,1,1,1,1,1,1,1)$$

$$=\Phi(u,u,u,u)$$

$$=\Phi(\Psi(u,u,u,u))$$

it is possible. Similar way

$$\sigma_{-1}^{\otimes 2}(\Phi(0,0,0,0))=\sigma_{-1}^{\otimes 2}(0,0,0,0,0,0,0,0)$$

$$=(0,0,0,0,0,0,0,0)$$

$$=\Phi(0,0,0,0)$$

$$=\Phi(\Psi(0,0,0,0))$$

is seen .

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

This C code for Nechaev permutation $\pi(0,0,0,0,0,0,0,0)=(0,0,0,0,0,0,0,0)$ and

$\pi(1,1,1,1,1,1,1,1) = (1,1,1,1,1,1,1,1)$ since $\Phi \; o \; \bar{\mu} = \pi \, o \, \Phi$ is possible.

C cyclic code for It $\pi(\Phi(C))$ is a 2nd order inverse quasi-cyclic code.

$$\begin{tikzcd}
IF_2^8 \arrow[d, "\pi"'] & C \subseteq R^4 \arrow[l, "\Phi"'] \arrow[d, "\bar{\mu}"] \\
IF_2^8 & \bar{\mu}(C) \subseteq R^4 \arrow[l, "\Phi"']
\end{tikzcd}$$

REFERENCES

[1] F.J. MacWilliams , NJA 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 and 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, A First Course in Coding Theory, Cambridge University Press, 2004.

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

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

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

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

[9] M. Özkan and 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 int. conf. ten app. Sci. conf. book, ISBN: 978-625-6830-51-6, 174-180, 2023.

[11] M. Özkan, Inverse Quasi-Cyclic Codes and Automorphism Cyclic Codes. Int. Journal of Adv. Nat. Sci. and Eng. Res., 7(10), 460-465, 2023.