Received: November 16, 2017
Accepted:January 29, 2018

Quasi-Cyclic Codes over the Field F_p

Mustafa ÖZKAN[1*], Figen ÖKE[2]

[1,2]Trakya University, Faculty of Sciences, Mathematics Department, 22030, Edirne, Turkey

Abstract

In this study, images of cyclic codes in two variable rings with coefficient field F_p are detected. A special ring in two variables is defined under certain conditions. The Gray images of the cyclic codes over this ring are investigated. Relations between the codes over this ring and the codes over a finite chain ring in one variable are obtained via a Gray map. Another Gray map from the finite chain ring to a finite field is defined and then the images of cyclic codes are obtained. It is obtained that the Gray image of a cyclic code over R with length n.

Keywords: Codes Over Rings, Quasi-Cylic Codes, Gray Map, Finite Field, Linear Codes.

F_p Cismi üzerinde Quasi-Cyclic Kodlar

Mustafa ÖZKAN[1*], Figen ÖKE[2]

Özet

Bu çalışmada, katsayıları F_p cisminde iki değişkenli halkalar üzerinde cyclic kodların görüntüleri tespit edilmiştir. Belirli koşullar altında iki değişkenli özel bir halka tanımlanmıştır. Bu halkalar üzerinde cyclic kodların Gray görüntüleri incelenmiştir. Gray dönüşümü yoluyla bu halkalar üzerindeki kodlar ve bir değişkenli sonlu zincir halkası üzerindeki kodlar elde edilmiştir. Sonlu zincir halkasından sonlu bir cisme başka Gray dönüşümü tanımlanmış ve sonra cyclic kodların görüntüleri elde edilmiştir. n uzunluğundaki R üzerinde bir cyclic kodun Gray görüntüsü bulunmuştur.

Anahtar Kelimeler :Halkalar üzerindeki kodlar, Quasi-Cylic kodlar, Gray dönüşümü, Sonlu cisimler, Lineer kodlar.

1. Introduction

Constacyclic codes, cyclic codes, quasi-cyclic codes, negacyclic codes over different rings (Finite chain rings, Frobenious rings, Galois rings i.e.) were studied before. Also the Gray images of these codes and structure of codes over fields were discussed before. Previous years the relations between codes over the polynomial rings in one variable and the codes over fields were studied.

[*] *Corresponding Author*, e- mail: mustafaozkan@trakya.edu.tr, mustafaozkan22@icloud.com

In recent years the relations between the codes over the polynomial rings in more variables and the codes over fields have been studied.

Especially in [7]; $(1+v)$ -constacyclic codes over $\mathrm{F}_2+u\mathrm{F}_2+v\mathrm{F}_2+uv\mathrm{F}_2$ where $u^{\;2}=v^2=0, u.v-v.u=0$ were studied by S. Karadeniz and B. yıldız. In [2]; X. Xiaofang studied $(1+v)$ -constacyclic codes over the ring $\mathrm{F}_2+u\mathrm{F}_2+v\mathrm{F}_2$ where $u^{\;2}=v^2=0, u.v=v.u=0$. Moreover, on the codes over the ring $\mathrm{F}_2+v\mathrm{F}_2+u\mathrm{F}_2+u^2\mathrm{F}_2$ where $u^3=0, v^2=0, u.v=v.u=0$ were studied by M. Özkan and F. Öke in [5].

In this study a special ring in two variables is defined under certain conditions. The Gray images of the cyclic codes over this ring are investigated. Relations between the codes over this ring and the codes over a finite chain ring in one variable are obtained via a Gray map. Another Gray map from the finite chain ring to a finite field is defined and then the images of cyclic codes are obtained.

Consequently; it is shown that quasi-cyclic codes over the field F_p can be obtained from the cyclic codes over the ring $\mathrm{F}_p+v\mathrm{F}_p+u\mathrm{F}_p+u^2\mathrm{F}_p$ using the composite of two new Gray maps. It is known that $S=\mathrm{F}_p+u\mathrm{F}_p+u^2\mathrm{F}_p$ where $u^3=0$ is the finite chain ring. $R=\mathrm{F}_p+v\mathrm{F}_p+u\mathrm{F}_p+u^2\mathrm{F}_p$ is a ring with the usual addition and multiplication under the conditions $u^3=0, v^2=0, uv=vu=0$.

It is easily seen that R is isomorphic to the ring $\mathrm{F}_p[u,v]\big/_{<u^3=0,\; v^2=0, uv=vu=0>}$. Let C be a linear $[n,k,d]$_ code. It means that C has the length n, it's dimention is k and it's minimum distance is d. Let R be a ring. Each submodule C of R^n is called a linear code with lenght n over the ring R. A subspace C of $\mathrm{F}_p{}^n$ is called a linear code with lenght n over the field F_p. Each codeword c in such a code C is a $n-$tuple of the form $c=(c_o,c_1,...,c_{n-1})\in R^n$ and can be represented by

$$c=(c_1,c_2,...,c_n)\longleftrightarrow c(x)=\sum_{i=1}^{n}c_i.x^i\in R[x] \tag{1}$$

This notation can be written for the elements of S^n and $\mathrm{F}_p{}^n$ similarly. In here p is odd prime number.

2. Materials and Methods

In this section, a new Gray map will be defined from R to S^2. Then w_R weight function will be given over R as the orginal.

The Gray map from the ring R to S^2 is defined as ;

$$\varphi_1 : R\longrightarrow S^2$$
$$a+bv+cu+du^2 \text{ a } \varphi_1(a+bv+cu+du^2)=\varphi_1(r+qv)=((p-1).q, q+(p-1).r) \tag{2}$$

where $r = a + cu + du^2$ and $q = b + au + (a+c)u^2$.

Then we have

$$\begin{aligned}\varphi_1(a+bv+cu+du^2) = ((p-1).b+(p-1).au+((p-1).a+(p-1).c)u^2,(b+(p-1).a)\\ +(a+(p-1).c)u+(a+c+(p-1).d)u^2)\end{aligned} \quad (3)$$

The map φ_1 can be generalized to R^n as ;

$$\varphi_1(t_0,t_1,...,t_{n-1}) = ((p-1)q_0,(p-1)q_1,...,(p-1)q_{n-1},q_0+(p-1)r_0,q_1+(p-1)r_1,...,q_{n-1}+(p-1)r_{n-1}) \quad (4)$$

where $t_i = r_i + q_i v$ such that $r_i = a_i + c_i u + d_i u^2$, $q_i = b_i + a_i u + (a_i + c_i)u^2$ for all $i = 0,1,...,n-1$.

Note that the Gray map from S to $\mathrm{F}_p^{p^2}$ is defined as ;

$$\begin{aligned}\varphi_2 : S &\longrightarrow \mathrm{F}_p^{p^2}\\ x+yu+zu^2 \text{ a } &\ \varphi_2(x+yu+zu^2)\end{aligned} \quad (5)$$

here $\varphi_2(x+yu+zu^2) = (m_0 \mid m_1 \mid ... \mid m_{p-1})$, $m_i \in \mathrm{F}_p^{p^2}$ for all $i = 0,1,..., p-1$.

$m_0 = (z, y+z, 2y+z,...,(p-1)y+z)$,

$m_1 = (x+z, x+y+z,..., x+(p-1)y+z), \ldots,$

$m_{p-1} = ((p-1)x+z,(p-1)x+y+z,...,(p-1)x+(p-1)y+z)$.

The map φ_2 can be generalized to S^n likewise φ_1 function.

The Hamming weight on F_p is defined as ;

$$w_H(c) = \begin{cases} 0 \ ; c = 0 \\ 1 \ ; c \neq 0 \end{cases} \quad (6)$$

Hence $w_H(c) = \sum_{i=0}^{n-1} w_H(c_i)$ is hold for each $c = (c_0, c_1,..., c_{n-1}) \in \mathrm{F}_p^n$.

It is known that the homogeneous weight of each $s \in S$ is defined as ;

$$w_{\hom}(s) = \begin{cases} p^2 - p & ; \ s \in S - S.u^2 \\ p^2 & ; \ s \in S.u^2 - \{0\} \\ 0 & ; \ s = 0 \end{cases} \quad (7)$$

Then $w_{\hom}(s) = \sum_{i=0}^{n-1} w_{\hom}(s_i)$ is satisfied for each element $s = (s_0, s_1,..., s_{n-1}) \in S^n$.

In this paper the weight function w_R for each element r of $R=\mathrm{F}_p+v\mathrm{F}_p+u\mathrm{F}_p+u^2\mathrm{F}_p$ is defined as ;

$$w_R(r)=\begin{cases} 0 & ; \; r=0 \\ 2p^2-2p & ; \; r\in R-S.u \\ 2p^2-p & ; \; r\in S.u-S.u^2 \\ p^2 & ; \; r\in S.u^2-\{0\} \end{cases} \tag{8}$$

Then $w_R(r)=\sum_{i=0}^{n-1} w_R(r_i)$ is satisfied for each element $r=(r_0,r_1,...,r_{n-1})\in R^n$.

The minimum distance of a code is defined as ; $d_H(C)=\min\{d_H(a,b)\}$, where $a,b\in C,\ a\neq b$ if C is a code over F_p, $d_{\hom}(D)=\min\{d_{\hom}(k,t)\}$, where $k,t\in D,\ k\neq t$ if D is a code over S and $d_R(C')=\min\{d_R(x,y)\}$, where $x,y\in C',\ x\neq y$ if C' is a code over R. Each element of R is written as $a+bv+cu+du^2=r+qv$, where $r=a+cu+du^2\in S$, $q=b+au+(a+c)u^2\in S$.

It is clearly seen that the equalities $w_R(r)=w_{\hom}(\varphi_1(r))=w_H(\varphi_2(\varphi_1(r)))$ for each $r\in R^n$ are satisfied. Therefore it means that φ_1 is an isometry from (R^n,d_R) to $(S^{2n},d_{\hom})$ and φ_2 is an isometry from $(S^{2n},d_{\hom})$ to $(\mathrm{F}_p^{2p^2n},d_H)$.

A cyclic shift on R^n is a permutation σ such that

$$\sigma(c_o,c_1,...,c_{n-1})=(c_{n-1},c_0,...,c_{n-2})\,. \tag{9}$$

A linear code C' over R of length n is said to be cyclic code if it is satisfied the equality $\sigma(C')=C'$. (same definition is defined for the ring S and the field F_p)

Let $a\in S^{2n}$ with $a=(a_0,a_1,...,a_{n-1})=(a^{(0)}\,|\,a^{(1)}),a^{(i)}\in S^n$, for all $i=0,1$. Let $\sigma^{\otimes 2}$ be the map from S^{2n} to S^{2n} given by

$$\sigma^{\otimes 2}(a)=(\sigma(a^{(0)})\,|\,\sigma(a^{(1)})) \tag{10}$$

where σ is the usual cyclic shift. A code D of length $2n$ over R_1 is said to be quasicyclic code of index 2 of $\sigma^{\otimes 2}(D)=D$.

A cyclic shift on S^{2n} is a permutation τ such that

$$\tau(d_o,d_1,...,d_{2n-1})=(d_{2n-1},d_0,...,d_{2n-2})\,. \tag{11}$$

A linear code D' over S of length $2n$ is said to be cyclic code if it is satisfied the equality $\tau(D')=D'$.

Let $a \in \mathrm{F}_p^{2p^2n}$ with $a = (a_0, a_1, ..., a_{2p^2n-1}) = (a^{(0)} \left| a^{(1)} \right| a^{(2)} \left| ... \right| a^{(p^2-1)}), a^{(i)} \in \mathrm{F}_p^{2n}$,

for all $i = 0,1,..., p^2 - 1$. Let $\sigma^{\otimes p^2}$ be the map from $\mathrm{F}_p^{2p^2n}$ to $\mathrm{F}_p^{2p^2n}$ given by

$$\sigma^{\otimes p^2}(a) = (\sigma(a^{(0)}) \left| \sigma(a^{(1)}) \right| \sigma(a^{(2)}) \left| ... \right| \sigma(a^{(p^2-1)})) \tag{12}$$

where σ is the usual cyclic shift. A code C of lenght $2p^2n$ over F_p is said to be quasicyclic code of index p^2 if $\sigma^{\otimes p^2}(C) = C$.

3. Results and Discussion

In this section firstly it will be shown that the φ_1 Gray image of a cyclic code over R is a quasi-cyclic code of index 2 with even lenght. Secondly it will be shown that the φ_2 Gray image of a cyclic code over S is a quasi-cyclic code of index p^2 with even length.

Proposition 3.1 $\sigma^{\otimes 2}\varphi_1 = \varphi_1\sigma$ is satisfied.

Proof: Let $c = (c_0, c_1, ..., c_{n-1}) \in R^n$ where $c_i = r_i + q_i v$ for $0 \le i \le n-1$.
If $\varphi_1(c) = \varphi_1(c_0, c_1, ..., c_{n-1}) = \varphi_1(r_0 + q_0 v, r_1 + q_1 v, ..., r_{n-1} + q_{n-1} v)$
$= ((p-1)q_0, (p-1)q_1, ..., (p-1)q_{n-1}, q_0 + (p-1)r_0, q_1 + (p-1)r_1, ..., q_{n-1} + (p-1)r_{n-1})$ then
$\sigma^{\otimes 2}(\varphi_1(c)) = ((p-1)q_{n-1}, (p-1)q_0, ..., (p-1)q_{n-2}, q_{n-1} + (p-1)r_{n-1}, q_0 + (p-1)r_0, ..., q_{n-2} + (p-1)r_{n-2})$
On the other hand,
$\sigma(c) = \sigma(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$ .Then
$\varphi_1(\sigma(c)) = \varphi_1(\sigma(c_0, c_1, ..., c_{n-1})) = \varphi_1(c_{n-1}, c_0, ..., c_{n-2})\ \Phi_1(r_{n-1} + vq_{n-1}, r_0 + vq_0, ..., r_{n-2} + vq_{n-2})$
$((p-1)q_{n-1}, (p-1)q_0, ..., (p-1)q_{n-2}, q_{n-1} + (p-1)r_{n-1}, q_0 + (p-1)r_0, ..., q_{n-2} + (p-1)r_{n-2})$.

Theorem 3.2 : A code C with length n over R is a cyclic code if and only if $\varphi_1(C)$ is a quasi-cyclic code of index 2 with length $2n$ over S .
Proof: Suppose that C is a cyclic code. Then $\sigma(C) = C$. By applying φ_1, we have $\varphi_1(\sigma(C)) = \varphi_1(C)$. By using the Proposition 3.1, we have $\sigma^{\otimes 2}(\varphi_1(C)) = \varphi_1(\sigma(C)) = \varphi_1(C)$. So $\varphi_1(C)$ is a quasi-cyclic code of index 2 . Conversely, if $\varphi_1(C)$ is a quasi-cyclic code of index 2 ,

then $\sigma^{\otimes 2}(\varphi_1(C))=\varphi_1(C)$. By using the Proposition 3.1 , we have $\sigma^{\otimes 2}(\varphi_1(C))=\varphi_1(\sigma(C))=\varphi_1(C)$. Since φ_1 is injective then $\sigma(C)=C$.

Proposition 3.3 : $\sigma^{\otimes p^2}\,\varphi_2=\varphi_2\,\tau$ is satisfied.

Proof : The proof is obtained similarly to the proof of Proposition 3.1.

Theorem 3.4 : A code C with length $2n$ over S is a cyclic code if and only if $\varphi_2(C)$ is a quasicyclic code of index p^2, with length $2p^2n$ over F_p.

Proof: If C is a cyclic code , $\tau(C)=C$. Then have $\varphi_2(\tau(C))=\varphi_2(C)$, we have $\sigma^{\otimes p^2}(\varphi_2(C))=\varphi_2(\tau(C))=\varphi_2(C)$ from Proposition 3.3. So $\varphi_2(C)$ is quasicyclic code of index p^2. Conversely, if $\varphi_2(C)$ is quasicyclic code of index p^2, then $\sigma^{\otimes p^2}(\varphi_2(C))=\varphi_2(C)$. By using the Proposition 3.3 , we have $\sigma^{\otimes p^2}(\varphi_2(C))=\varphi_2(\tau(C))=\varphi_2(C)$. Since φ_2 is injective then $\tau(C)=C$.

Using the above theories the main conclusion is given below:

Corollary 3.5 : A code C with odd length n over R is a cyclic code if and only if $\varphi_2(\varphi_1(C))$ is a quasicyclic code of index p^2 and with length $2p^2n$ over F_p.

In this study a special ring in two variables is defined under certain conditions. The Gray images of the cyclic codes over this ring are investigated. Relations between the codes over this ring and the codes over a finite chain ring in one variable are obtained via a Gray map. Another Gray map from the finite chain ring to a finite field is defined and then the images of cyclic codes are obtained.

4. Conclusions

In this study a special ring in two variables is defined under certain conditions. The Gray images of the cyclic codes over this ring are investigated. Relations between the codes over this ring and the codes over a finite chain ring in one variable are obtained via a Gray map. Another Gray map

from the finite chain ring to a finite field is defined and then the images of cyclic codes are obtained.

Acknowledgements

The authors are grateful to the anonymous referee for a careful checking of the details and ISMSIT2017.

5. References

[1] Özkan M, Öke F(2016), Some Special Codes Over $\mathrm{F}_3+v\mathrm{F}_3+u\mathrm{F}_3+u^2\mathrm{F}_3$, Mathematical Sciences and Applications E-Notes .Vol. 4 No 1,pp 40-44.

[2] Xioafang X (2013), $(1+v)$-constacyclic codes over $IF_2+uIF_2+vIF_2$,Computer Engineering and Applications,49, 12, 77-79.

[3] Udomkavanich P, Jitman S (2009) , On the Gray Image of $(1-u^m)$-Cyclic Codes $\mathrm{F}_{p^k}+u\mathrm{F}_{p^k}+...+u^m\mathrm{F}_{p^k}$, Int.J.Contemp. Math. Sciences,Vol.4, No.26, 1265-1272.

[4] Roman S (1992), Coding and Information Theory, Graduate Texts in Mathematics, Springer Verlag.

[5] Özkan M, Öke F (2017), Gray images of $(1+v)-$constacyclic codes over a particular ring, Palestine Journal of Mathematics. Vol. 6(S.I.2), 241-245.

[6] Karadeniz S,Yıldız B (2011), On $(1+v)$-constacyclic codes over $\mathrm{F}_2+u\mathrm{F}_2+v\mathrm{F}_2+uv\mathrm{F}_2$,Journal of the Franklin Institute , 348, 2625-2632.

[7] Özkan M, Öke F (2017) ,Repeat codes, Even codes, Odd codes and Their equivalence, General Letters in Mathematics, Vol. 2, No :1, pp : 110-118.

[8] Özkan M, Öke F (2017) ,Codes defined via especial matrices over the ring and Hadamard codes, Mathematical Sciences and Applications E-Notes, Volume 5, No :1, pp : 93-98.

[9] Özkan M, Öke F(2016) ,A relation between Hadamard codes and some special codes over F2+uF2, App.Mathematics and Inf. Sci. Vol.10, No: 2, pp : 701-704.