Journal of New Results in Engineering and Natural Science, No:8 (2018) 25-30
http://jrens.gop.edu.tr

Received: November 16, 2017
Accepted:December 14, 2017

Certain Rings and Group Codes

Mustafa ÖZKAN[1*], Burcu ÖZTÜRK[2]

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

Abstract

In this study, the structure of certain rings and information about their ideals is given. The operations and the structures of the finite chain rings are discussed. The ideals of these rings are classified. New structures are needed to write new and better codes in coding theory. Substructures of the codes to be written are studied with the structures written here. It is revealed how the structures of the rings can be referenced to the newly writable codes. Moreover it is mentioned about the good codes which can be written in the more basic structure with the group codes which are not very preliminary in the coding theory. The significance of group codes in the coding theory is studied to be indicated and their correlations are established.

Keywords: Group codes, codes over rings, linear codes, rings, Lee distance .

Belirli Halkalar ve Grup Kodlar

Mustafa ÖZKAN[1*], Burcu ÖZTÜRK[2]

Özet

Bu çalışmada, belirli halkaların yapısı ve idealleri hakkında bilgi verilmektedir. Sonlu zincir halkalarının işlemleri ve yapıları ele alınmaktadır. Bu halkaların idealleri sınıflandırılmaktadır. Kodlama teorisinde yeni ve daha iyi kod yazmak için yeni yapılara ihtiyaç duyulmaktadır. Yazılacak kodların alt yapıları burada yazılan yapılarla incelenmektedir. Halkaların yapılarının yeni yazılabilir kodlara nasıl referans olabileceği açıklanmaktadır. Ayrıca kodlama teorisinde öncelikli olmayan grup kodlarıyla daha temel yapıda yazılabilecek iyi kodlara değinilmiştir. Kodlama teorisinde grup kodlarının önemi belirtilmek üzere incelenmiş ve bağlantıları kurulmuştur.

Anahtar Kelimeler : Grup kodlar, halkalar üzerindeki kodlar, lineer kodlar, halkalar,Lee uzaklığı.

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

1. Introduction

In this article, the structure of the finite chain rings with four elements is mentioned. These rings are formed on structure $F_2 + uF_2$ for the states $u^2 = 0, u^2 = 1$ and $u^2 = u$. The operations on these rings and weight functions are given in [5],[6]. From the set feature of these rings the construction of group codes is established with generator matrices.

2. Materials and Methods

Definition 2.1. Let X be a set. A binary operation on X is a function $*: XxX \to X$, (x, y) a $x * y$

Definition 2.2. A non empty set G with a binary operation is called a group if the followings hold:

i) The operation on G is associative, i.e $a*(b*c) = (a*b)*c$ for $\forall a,b,c \in G$

ii) There exist an element $e \in G$ such that $e*a = a*e = a$ for $\forall a \in G$

iii) For every $a \in G$, there exist an element $a^{-1} \in G$ such that $a*a^{-1} = a^{-1}*a = e$

Definition 2.3. A non empty set R with two binary operations, say addition and multiplication defined on it, is called a ring if:

i) R is an abelian group with respect to additive operation

ii) Multiplication on R is associative, i.e. $a.(b.c) = (a.b).c$ for $\forall a,b,c \in G$

iii) The two distributive laws hold, i.e. $a.(b+c) = a.b + a.c$ and $(a+b).c = a.c + b.c$ for $\forall a,b,c \in G$

Definition 2.4. A set F with two operation, say addition and multiplication defined on it, is called a field if:

i) F is a commutative ring with identitiy

ii) Every non-zero element of F is invertible with respect to multiplication

Definition 2.5. A finite field is a field which has a finite number of elements, this number being called the order of the field

Theorem 2.6. There exist a field of order q if and only if q is a prime power

Definition 2.7. A field of order q is often called a Galois field and it is denoted by F_q or $GF(q)$

Example 2.8. $GF(2) = F_2 = \{0,1\}$ with addition and multiplication tables

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

Definition 2.9. A binary block (m,n)-code consists of an encoding function $E: (F_2)^m \to (F_2)^n$ and a decoding function $D: (F_2)^n \to (F_2)^m$. The elements of $\mathrm{Im}\,E$ (image of E) are called code words.

Definition 2.10. An mxn matrix, with $m < n$ over F_2 is called an encoding matrix or generator matrix if the first m columns of it form the identity matrix I_m. Given a generator matrix G, we define an encoding function $E: (F_2)^m \to (F_2)^n$ by $E(x) = xG$.

Definition 2.11. When the code words in a block code form an additive group, the code is called a group code.

In this study, block code and group code notions will be given using the elements of the finite chain rings. So the structures and ideals of these rings are classified. Then weight functions are given depending on them.

If $u^2=0$ then ring $F_2[u]/<u^2>=\{a_0+a_1u+<u^2>\,|\,a_0,a_1\in F_2\}$ isomorphic to the ring F_2+uF_2. $F_2+uF_2=\{0,1,u,1+u\}$ is a ring with the + and . operations defined below when $u^2=0$

Table1

+	u	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

Table2

.	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

Ring $R_1=F_2+uF_2$ has three ideals. These ideals are $\langle 0\rangle$, $\langle 1\rangle$, $\langle u\rangle$ and $\langle 0\rangle\subseteq\langle u\rangle\subseteq\langle 1\rangle=R_1$ are provided.

If $u^2=1$ then ring $F_2[u]/<u^2-1>=\{a_0+a_1u+<u^2-1>\,|\,a_0,a_1\in F_2\}$ isomorphic to the ring F_2+uF_2. Addition and multiplication operations on the ring $R_2=F_2+uF_2=\{0,1,u,1+u\}$ defined below when $u^2=1$.

Table3

+	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

Table4

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

In this case the ideals of ring $R_2 = \mathrm{F}_2 + u\mathrm{F}_2$ are $\langle 0\rangle = \{0\}$, $\langle 1+u\rangle = \{0, 1+u\}$, $\langle u\rangle = \langle 1\rangle = R_2$

There is a relation $\langle 0\rangle \subseteq \langle 1+u\rangle \subseteq \langle u\rangle \subseteq \langle 1\rangle = R_2$ between the ideals and so R_2 is a local ring.

If $u^2 = u$ then ring $\mathrm{F}_2[u]/ < u^2 - u >= \{a_0 + a_1 u + < u^2 - u > \,|\, a_0, a_1 \in \mathrm{F}_2\}$ isomorphic to the ring $\mathrm{F}_2 + u\mathrm{F}_2$. Addition and multiplication operations on the ring $R_3 = \mathrm{F}_2 + u\mathrm{F}_2 = \{0, 1, u, 1+u\}$ defined below when $u^2 = u$.

Table5

$+$	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

Table6

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

In this case the ideals of ring $R_3 = \mathrm{F}_2 + u\mathrm{F}_2$ are $\langle 0\rangle = \{0\}$, $\langle u\rangle = \{0, u\}$, $<1+u>=\{0, 1+u\}$ and $<1>= R_3$. The relations between the ideals are $<0>\subseteq<1+u>\subseteq<1>= R_3$ and $\langle 0\rangle \subseteq \langle v\rangle \subseteq \langle 1\rangle = R_3$. So R_3 isn't a local ring.

Definition 2.12. On the ring R_1 , the function defined as

$$w_{L_{R_1}}(r) = \begin{cases} 0 & ; \ r = 0 \\ 1 & ; \ r = 1, 1+u \\ 2 & ; \ r = u \end{cases} \tag{1}$$

for each $r \in R_1$ is called the Lee weight function on R_1 . In this case $w_{L_{R_1}}(r) = \sum_{i=1}^{n} w_{L_{R_1}}(r_i)$ equality occurs for each $r = (r_1, r_2, ..., r_n) \in R_1^n$.

Definition 2.13. On the ring R_2 , the function defined as

$$w_{L_{R_2}}(r) = \begin{cases} 0 & ; \ r = 0 \\ 1 & ; \ r = 1, u \\ 2 & ; \ r = 1+u \end{cases} \tag{2}$$

for each $r \in R_2$ is called the Lee weight function on R_2 . In this case $w_{L_{R_2}}(r) = \sum_{i=1}^{n} w_{L_{R_2}}(r_i)$ equality occurs for each $r = (r_1, r_2, ..., r_n) \in R_2^n$.

Definition 2.14. On the ring R_3, the function defined as

$$w_{L_{R_3}}(r)=\begin{cases}0 & ; r=0\\ 1 & ; r=u,1+u\\ 2 & ; r=1\end{cases} \tag{3}$$

for each $r\in R_3$ is called the Lee weight function on R_3. In this case $w_{L_{R_3}}(r)=\sum_{i=1}^{n} w_{L_{R_3}}(r_i)$ equality occurs for each $r=(r_1,r_2,...,r_n)\in R_3^n$.

Definition 2.15. Minimum Lee distance of a code C is defined as $d_{L_{R_1}}(C)=\min\left\{d_{L_{R_1}}(a,b)\,\middle|\, a,b\in C, a\neq b\right\}$ where $d_{L_{R_1}}(a,b)=w_{L_{R_1}}(a-b)$ is the distance between every $a, b\in R_1^n$, $a\neq b$ vectors.

The minimum Lee distance definition on R_2 and R_3 is given similarly.

3. Results and Discussion

In this section, all the standard form generator matrices over the rings R_1, R_2, R_3 are considered and it is determined that the block codes generated by these matrices are the group code.

Teorem 3.1. 16-element block codes with all generator matrices of type $G=\begin{bmatrix}1 & 0 & a\\ 0 & 1 & b\end{bmatrix}$ are group code where $a,b\in R_1$ (or R_2 or R_3)

Proof: Let $\begin{bmatrix}x & y\end{bmatrix}$ be the matrix form of $x,y\in R_1$. Using the generator matrix property of G it is found that $\begin{bmatrix}x & y\end{bmatrix}.G=\begin{bmatrix}x & y & ax+yb\end{bmatrix}$. Since R_1 is a group at the same time it is seen that $ax\in R_1$, $yb\in R_1$ and also $ax+yb\in R_1$. Hence R_1^3 is a group code. Proof is similarly made for R_2 and R_3.

Proposition 3.2. Let $G=\begin{bmatrix}1 & 0 & a\\ 0 & 1 & b\end{bmatrix}$ is a generated matrix for (2,3)-group codes on R_1, R_2 and R_3. If a and b are different from zero, minimum Lee weight is two and if at least one of a and b is zero, the Lee weight is one for the rings R_1 and R_2. Minimum Lee weight on R_3 is one for all conditions.

Example 3.3. When the generator matrices $G_1=\begin{bmatrix}1 & 0 & 1+u\\ 0 & 1 & u\end{bmatrix}$ and $G_2=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 1+u\end{bmatrix}$ are used for the block codes over the rings R_1^2, R_2^2 and R_3^2 , we have the followings.

The codes generated by matrix G_1 are;

$C_1=\{(0,0,0),(0,1,u),(0,u,0),(0,1+u,u),(1,0,1+u),(1,1,1),(1,u,1+u),$
$(1,1+u,1),(u,0,u),(u,1,0)(u,u,u),(u,1+u,0),(1+u,0,1),$
$(1+u,1,1+u),(1+u,u,1),(1+u,1+u,1+u)\}\subseteq R_1^3$

$C_2=\{(0,0,0),(0,1,u),(0,u,1),(0,1+u,1+u),(1,0,1+u),(1,1,1),(1,u,u),$
$(1,1+u,0),(u,0,1+u),(u,1,1),(u,u,u),(u,1+u,0),(1+u,0,0),$
$(1+u,1,u),(1+u,u,1),(1+u,1+u,1+u)\}\subseteq R_2^3$

$C_3=\{(0,0,0),(0,1,u),(0,u,u),(0,1+u,0),(1,0,1+u),(1,1,1),(1,u,1),(1,1+u,1+u),$
$(u,0,0),(u,1,u),(u,u,u),(u,1+u,0),(1+u,0,1+u),$
$(1+u,1,1),(1+u,u,1),(1+u,1+u,1+u)\}\subseteq R_3^3$

Then the codes C_1, C_2 and C_3 are (2,3)-group code. Minimum Lee weight of the codes C_1 and C_2 is two and minimum Lee weight of the code C_3 is one. At the same time C_1 and C_2 are (3,16,2)-code and C_3 is (3,16,1)-code.

The codes generated by matrix G_2 are;

$D_1 = \{(0,0,0), (0,1, 1+u),(0, u, u), (0, 1+u,1),(1,0,0),(1,1,1+u),(1,u,u),$
$(1,1+u,1),(u,0,0),(u,1,1+u),(u,u,u),(u,1+u,1),(1+u,0,0),$
$(1+u,1, 1+u),(1+u,u,u),(1+u,1+u,1)\} \subseteq R_1^3$

$D_2 =\{(0,0,0),(0,1, 1+u),(0, u, 1+u),(0, 1+u,0),(1,0,0),(1,1, 1+u),(1, u, 1+u),$
$(1,1+u,0),(u,0,0),(u,1, 1+u),(u, u, 1+u),(u, 1+u,0),(1+u,0,0),$
$(1+u,1, 1+u), (1+u,u, 1+u),(1+u,1+u,0)\} \subseteq R_2^3$

$D_3 =\{(0,0,0),(0,1, 1+u),(0, u,0),(0, 1+u,1+u),(1,0,0),(1,1, 1+u),(1, u,0),$
$(1, 1+u,1+u),(u,0,0),(u,1, 1+u),(u, u,0), (u, 1+u,1+u),$
$(1+u,0,0), (1+u,1, 1+u),(1+u,u,0), (1+u, 1+u, 1+u)\} \subseteq R_3^3$

All of the codes D_1, D_2 and D_3 are (2,3)-group code and also (3,16,1)-code.

4. Conclusions

It is shown that the block codes considered here are group codes and these codes are classified according to their parameters. It is also determined how the weights of codes are written according to the elements of the generator matrices in the standard form.

4. References

[1] Özkan M, Öke F (2016). Some Special Codes Over $F_3+vF_3+uF_3+u^2F_3$. *Mathematical Sciences and Applications E-Notes*, Vol. 4 No 1, pp 40-44.

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

[3] 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.

[4] 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.

[5] 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.

[6] Özkan M, Öke F (2016). A relation between Hadamard codes and some special codes over F_2+uF_2. *App.Mathematics and Inf. Sci.* Vol.10, No: 2, pp : 701-704.

[7] Huffman W.C, Pless V (2003). *Fundamentals of Error Correcting Codes*, Cambridge.

[8] Vermani L.R (1996). *Elements of Algebraic Coding Theory*, Chapman Hall, India,