Journal of Science and Arts Year 20, No. 2(51), pp. 283-290, 2020

ORIGINAL PAPER

MACDONALD CODES OVER THE RING $F_2+uF_2+vF_2$

RABIA DERTLI[1], SENOL EREN[1]

Manuscript received: 07.11.2019; Accepted paper: 20.03.2020;
Published online: 30.06.2020.

Abstract. *In this paper, we construct MacDonald codes of type* α *over the ring* $F_2+uF_2+vF_2$, *where* $u^2=u, v^2=v, uv=vu=0, F_2=\{0,1\}$ *is the field of two elements and investigate their properties such as torsion codes and weight distributions.*

Keywords*: MacDonald codes, weight distributions, rings.*

1. INTRODUCTION

There has been much attention research in codes over finite rings in recent years. By using type α simplex codes we have been constructed MacDonald codes over a ring. MacDonald codes are important in coding theory since they provide the Griesmer bound. In [1], the binary MacDonald codes were introduced and q-ary version ($q \geq 2$) of these over the finite fields were studied in [2].

Motivated by the importance of the MacDonald codes which have been defined over several finite commutative rings [3-7], in this paper, we construct MacDonald codes over the ring $F_2+uF_2+vF_2$ of type α, where $u^2=u$, $v^2=v$, $uv=vu=0, F_2=\{0,1\}$ and we study torsion code weight distributions. We describe their properties such as Hamming, Lee and Bachoc weight distributions.

2. PRELIMINARIES

In [6], A. Dertli and Y. Cengellenmis introduced the finite ring

$$R=F_2+uF_2+vF_2=F_2[u,v]/\left\langle u^2-u, v^2-v, uv-vu\right\rangle$$

The ring R is a commutative ring of 8 elements which are $\{0, 1, u, v, a=1+u, b=1+v, a+b=u+v, ab=1+u+v\}$, where $u^2=u$, $v^2=v$, $uv=vu=0$ and $F_2=\{0,1\}$. The element 1 is unit. Addition and multiplication operation over R are given in Tables 1-2.

A linear code C over R of length n is an R-submodule of R^n. The elements of a linear code are called codewords. There are three well known different weights for codes over R, namely Hamming, Lee and Bachoc weights.

[1] University of Ondokuz Mayıs, Faculty of Arts and Science, Department of Mathematics, Samsun, Turkey.
E-mail: rabia.alim06@gmail.com; seren@omu.edu.tr.

Table 1. Addition operation.

+	0	1	*u*	*v*	*a*	*b*	*a*+*b*	*ab*
0	0	1	*u*	*v*	*a*	*b*	*a*+*b*	*ab*
1	1	0	*a*	*b*	*u*	*v*	*ab*	*a*+*b*
u	*u*	*a*	0	*a*+*b*	1	*ab*	*v*	*b*
v	*v*	*b*	*a*+*b*	0	*ab*	1	*u*	*a*
a	*a*	*u*	1	*ab*	0	*a*+*b*	*b*	*v*
b	*b*	*v*	*ab*	1	*a*+*b*	0	*a*	*u*
a+*b*	*a*+*b*	*ab*	*v*	*u*	*b*	*a*	0	1
ab	*ab*	*a*+*b*	*b*	*a*	*v*	*u*	1	0

Table 2. Multiplication operation.

·	0	1	*u*	*v*	*a*	*b*	*a*+*b*	*ab*
0	0	0	0	0	0	0	0	0
1	0	1	*u*	*v*	*a*	*b*	*a*+*b*	*ab*
u	0	*u*	0	0	0	0	*u*	0
v	0	*v*	0	*v*	*v*	0	*v*	0
a	0	*a*	0	*v*	*ab*	*ab*	*v*	*ab*
b	0	*b*	*u*	0	*ab*	*b*	*u*	*ab*
a+*b*	0	*a*+*b*	*u*	*v*	*v*	*u*	*a*+*b*	0
ab	0	*ab*	0	0	*ab*	*ab*	0	*ab*

The Hamming weight $wt_H(x)$ of a codeword $x=(x_1,\ x_2,\ \dots\ ,x_n)\in R^n$ is the number of non-zero coordinates. The minimum weight $wt_H(C)$ of a code C is the smallest weight among all its nonzero codewords.

The Lee weight for the codeword $x=(x_1,x_2,...,x_n)\in R^n$ is defined by $wt_L(x)=\sum_{i=1}^{n} wt_L(x_i)$ where,

$$wt_L(x_i)=\begin{cases} 0, \text{ if } x_i = 0 \\ 1, \text{ if } x_i = u, v \text{ or } 1+u+v \\ 2, \text{ if } x_i = 1+u, 1+v \text{ or } u+v \\ 3, \text{ if } x_i = 1 \end{cases}$$

The Bachoc weight for the codeword $x=(x_1,x_2,...,x_n)\in R^n$ is defined by $wt_B(x)=\sum_{i=1}^{n} wt_B(x_i)$ where,

$$wt_B(x_i)=\begin{cases} 0, \text{ if } x_i = 0 \\ 1, \text{ if } x_i = 1 \\ 2, \text{ if } x_i = u, v, 1+u, 1+v, u+v \text{ or } 1+u+v \end{cases}$$

The minimum Lee weight $wt_L(C)$ and the minimum Bachoc weight $wt_B(C)$ of code C are defined analogously.

For $x=(x_1,x_2,...,x_n), y=(y_1,y_2,...,y_n)\in R^n$, $d_H(x,y)=\left|\{i\,|\,x_i\neq y_i\}\right|$ is called Hamming distance between $x, y\in R^n$ and it is denoted by $d_H(x,y)=wt_H(x-y)$. The minimum Hamming distance between distinct pairs of codewords of a code C is called the minimum distance of C and denoted by $d_H(C)$ or shortly d_H.

The Lee distance and Bachoc distance between x and $y \in R^n$ is defined by

$$d_L(x,y) = wt_L(x-y) = \sum_{i=1}^{n} wt_L(x_i - y_i)$$

$$d_B(x,y) = wt_B(x-y) = \sum_{i=1}^{n} wt_B(x_i - y_i)$$

respectively.

The minimum Lee and Bachoc distance between distinct pairs of codewords of a code C are called the minimum distance of C and denoted by $d_L(C)$ and $d_B(C)$ or shortly d_L and d_B, respectively. If C is a linear code, then

$$d_H(C) = wt_H(C)$$

$$d_L(C) = wt_L(C)$$

$$d_B(C) = wt_B(C)$$

Given $x = (x_1,...,x_n), y = (y_1,...,y_n) \in R^n$, their scalar product is defined by, $xy = x_1y_1 + ... + x_ny_n$. Two words x, y are called orthogonal if $xy = 0$. For the code C over R, its dual $C^{\perp}$ is defined as follows, $C^{\perp} = \{x \mid xy = 0, \forall y \in C\}$. If $C \subseteq C^{\perp}$, we say that the codes C is self-orthogonal and if $C = C^{\perp}$ we say that the code is self-dual.

If H is a code over R, then H_1 (resp. H_2, H_3) is a binary code. It is obtained that, $H = (1+u+v)H_1 + uH_2 + vH_3$ with

$$H_1 = \{x : \exists y, z \in F_2^n, (1+u+v)x + uy + vz \in H\}$$

$$H_2 = \{y : \exists x, z \in F_2^n, (1+u+v)x + uy + vz \in H\}$$

$$H_3 = \{z : \exists x, y \in F_2^n, (1+u+v)x + uy + vz \in H\}$$

In [8], it was shown that the ring R has three maximal ideals. These are $m_1 = <a> = \{0, a, v, 1+u+v\}, m_2 = <b> = \{0, b\ u, 1+u+v\}$ and $m_3 = <u+v> = \{0, u+v, u, v\}$. Morever $m_1 \cap m_2 \cap m_3 = \{0\}$.

The following map:

$$\varphi : R \to R/m_1 \times R/m_2 \times R/m_3$$

$$a \mapsto (\varphi_1(a), \varphi_2(a), \varphi_3(a))$$

is an isomorphism where these maps $\varphi_i : R \to R/m_i$ are canonical homomorphisms for $i = 1,2,3$. It is easy to see that R/m_i is isomorphic to F_2, for $i = 1,2,3$. The map φ^{-1} is a ring isomorphism by the generalized Chinese Remainder Theorem and R is isomorphic to $R/m_1 \times R/m_2 \times R/m_3 \cong F_2^3$. This map can be extended from R^n to F_2^{3n} in the following way. The Gray map φ from R^n to F_2^{3n} is defined as:

$$\varphi : R^n \to F_2^{3n}$$

$$x + uy + vz \mapsto (x, x+y, x+z)$$

is an isomorphism where $x, y, z \in F_2^n$, [8]. From the definition of the Gray map and the Lee weights, we have the following Lemma.

Lemma 1. If a code C is a self-dual, so is $\varphi(C)$. The minimum Lee weight of C is equal to the minimum Hamming weight of $\varphi(C)$. Thus a code $C = [n, 8^{k_1}4^{k_2}2^{k_3}, d_L]$ over R of length n, $8^{k_1}4^{k_2}2^{k_3}$ codewords with minimum Lee distance of d_L gives rise to binary code $\varphi(C) = [3n, 3k_1 + 2k_2 + k_3, d_H = d_L]$.

Definition1. For each $1 \le i \le n$, let $A_H(i)(A_L(i))$ be the number of codewords of Hamming (Lee) weight i in C. Then $\{A_H(0), A_H(1), ..., A_H(n)\}$ $(\{A_L(0), ..., A_L(n)\})$ is called the Hamming (Lee) weight distribution of C, [1].

3. MACDONALD CODES OF TYPE α

In this section we will study the MacDonald codes of types α over R and also we study the properties of their images under the Gray map.

A type α simplex code S_k^α is a linear code over R constructed inductively by the following generator matrix.

Let G_k^α be $k \times 2^{3k}$ matrix over R defined inductively by

$$G_k^\alpha = \begin{bmatrix} 0...0 & 1...1 & u...u & ... & (ab)...(ab) \\ G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & ... & G_{k-1}^\alpha \end{bmatrix}; \ k \ge 2 \tag{3.1}$$

where $G_1^\alpha = [0\,1\,u\,v\,a\;b\,(a+b)\,(ab)]$.

We will now construct the MacDonald codes by using the generator matrices of simplex codes. For $1 \le t \le k-1$, let $G_{k,t}^\alpha$ be the matrix obtained from G_k^α by deleting columns corresponding to the columns of G_t^α, i.e.

$$G_{k,t}^{\alpha} = \left[G_k^{\alpha} \setminus \frac{0}{G_t^{\alpha}} \right] \tag{3.2}$$

where $[A \setminus B]$ denotes the matrix obtained from the matrix A by deleting the matrix B and 0 in (3.2) is a $(k-t)\times 2^{3t}$ zero matrix. The code $M_{k,t}^{\alpha}$ was generated by the matrix $G_{k,t}^{\alpha}$ is the punctured code of S_k^{α} and is called a MacDonald code. (i.e The MacDonald codes are obtained by deleting some columns of the generator matrices G_k^{α} of the simplex code S_k^{α}).

3.1. PROPERTIES

The code $M_{k,t}^{\alpha}$ is a code of length $n = 2^{3k} - 2^{3t}$ and dimension $3k$.

Lemma 2. The torsion code of $M_{k,t}^{\alpha}$ is binary linear $[2^{3k} - 2^{3t}, k, 2^{3k-1} - 2^{3t-1}]$ code with weight distribution $A_H(0) = 1, A_H(2^{3k-1} - 2^{3t-1}) = [2^{k-2} + 2^{k+t-3}]$ and $A_H(2^{3k-1}) = [2^{k-t} - 1]$.

Proof: Since the torsion code of $M_{k,t}^{\alpha}$ is the set of codewords obtained by replacing u by 1 in all u-linear combination of the rows of the matrix $u\,.G_{k,t}^{\alpha}$ (where $G_{k,t}^{\alpha}$ is defined in (3.2)).
We prove by induction with respect to k and t. For $k = 2$ and $t = 1$ the result holds. Suppose the result holds for $k-1$ and $1 \le t \le k-2$. Then for k and $1 \le t \le k-1$ the matrix $u.G_{k,t}^{\alpha}$ takes the form, $u.G_{k,t}^{\alpha} = \left[u.G_k^{\alpha} \setminus \frac{0}{u.G_t^{\alpha}} \right]$. Each non-zero codeword of $u.M_{k,t}^{\alpha}$ has Hamming weight either $2^{3k-1} - 2^{3t-1}$ or 2^{3k-1} and the dimension of the torsion code of $M_{k,t}^{\alpha}$ is k, then there will be $2^{k-2} + 2^{k+t-3}$ codewords of Hamming weight $2^{3k-1} - 2^{3t-1}$ and the number of codewords with Hamming weight 2^{3k-1} is $2^{k-t} - 1$.

Remark 1. Each of the first $k-t$ rows of (3.2) has total number of units 2^{4k-t-4} and total number of non-zero divisors 3.2^{4k-t-3} and the last t rows has total number of units $2^{3k+t-4} - 2^{4t-4}$ and total number of non-zero divisors $3.(2^{3k+t-3} - 2^{4t-3})$.

Remark 2. Let $j \in R$ and let c be a codeword in the code C. We denote $w_j(c) = \left|\{k \,:\, c_k = j\}\right|$.

Lemma 3. Let $c \in M_{k,t}^{\alpha}$, $c \ne 0$. If at least one component of t elements is a unit then there are eight type of codewords.

I. $w_0(t) = w_1(t) = w_u(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-3} - 2^{3t-3}$

II. $w_1(t) = w_u(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-3}$, $w_0(t) = 2^{3k-3} - 2^{3t}$

III. $w_1(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-3}$, $w_0(t) = w_u(t) = 2^{3k-3} - 2^{3t-1}$

$IV.\ \ w_1(t)=w_u(t)=w_a(t)=w_b(t)=w_{a+b}(t)=w_{ab}(t)=2^{3k-3},\ w_0(t)=w_v(t)=2^{3k-3}-2^{3t-1}$

$V.\ \ w_1(t)=w_u(t)=w_v(t)=w_a(t)=w_b(t)=w_{a+b}(t)=2^{3k-3},\ w_0(t)=w_{ab}(t)=2^{3k-3}-2^{3t-1}$

$VI.\ \ w_1(t)=w_u(t)=w_b(t)=w_{a+b}(t)=2^{3k-3},\ w_0(t)=w_a(t)=w_v(t)=w_{ab}(t)=2^{3k-3}-2^{3t-2}$

$VII.\ \ w_1(t)=w_v(t)=w_a(t)=w_{a+b}(t)=2^{3k-3},\ w_0(t)=w_u(t)=w_b(t)=w_{ab}(t)=2^{3k-3}-2^{3t-2}$

$VIII.\ w_1(t)=w_a(t)=w_b(t)=w_{ab}(t)=2^{3k-3},\ w_0(t)=w_u(t)=w_v(t)=w_{a+b}(t)=2^{3k-3}-2^{3t-2}$

Otherwise:

$I.\ \ w_0(t)=w_u(t)=w_v(t)=w_{ab}(t)=2^{3k-1}-2^{3t-1}$

$II.\ \ w_0(t)=w_u(t)=w_v(t)=w_a(t)=w_b(t)=w_{a+b}(t)=w_{ab}(t)=2^{3k-2}-2^{3t-2}$

$III.\ \ w_u(t)=w_v(t)=w_{ab}(t)=2^{3k-1},\ \ w_0(t)=2^{3k-1}-2^{3t}$

$IV.\ \ w_u(t)=w_a(t)=w_{a+b}(t)=w_{ab}(t)=2^{3k-2},\ \ w_0(t)=w_v(t)=2^{3k-2}-2^{3t-1}$

$V.\ \ w_v(t)=w_{a+b}(t)=2^{3k-2},\ \ w_0(t)=w_u(t)=2^{3k-2}-2^{3t-1}$

$VI.\ \ w_u(t)=w_v(t)=w_a(t)=w_b(t)=2^{3k-2},\ \ w_0(t)=w_{ab}(t)=2^{3k-2}-2^{3t-1}$

$VII.\ \ w_u(t)=w_v(t)=w_a(t)=w_b(t)=w_{a+b}(t)=w_{ab}(t)=2^{3k-2},\ w_0(t)=2^{3k-2}-2^{2t+1}$

$VIII.\ w_a(t)=w_b(t)=w_{ab}(t)=2^{3k-2},\ w_0(t)=w_u(t)=w_v(t)=2^{3k-2}-2^{3t-1}$

Theorem 1. The Hamming, Lee and Bachoc weight distributions of $M_{k,t}^{\alpha}$ are:

(1) $A_H(0)=1$

$A_H(7.2^{3k-3})=(2^{k-t}-1).(2^{k-t}-1).(2^{k-t}-1)$

$A_H(2^{3k-1}-2^{3t-1})=3.(2^{k+t-3}+1)$

$A_H(2^{3k-1})=3.(2^{k-t}-1)$

$A_H(3.2^{3k-2})=3.(2^{k-t}-1).(2^{k-t}-1)$

$A_H(3.(2^{3k-2}-2^{3t-2}))=3.(2^{k+t-1}-2^{k-2}+1)$

$$A_H(7.(2^{3k-3}-2^{3t-3}))=2^{3.(k-t)}.(2^t-1).(2^t-1).(2^t-1)$$

$$A_H(7.2^{3k-3}-2^{3t-1})=3.[2^{3k-2t}.(2^t-1)-2^k(2^{2k-2}-3.2^{k-1}+4)-5.2^{k+t-3}-1]$$

$$A_H(3.2^{3k-2}-2^{3t-1})=3.2^k$$

$$A_H(7.2^{3k-3}-3.2^{3t-2})=3.[(2^{k-1}-1).(2^{k-1}-1).(2^{k-1}-1).2+2^{k-2}+1]$$

(2) $A_L(0)=1$

$$A_L(3.2^{3k-1})=(2^{k-t}-1).(2^{k-t}-1).(2^{k-t}-1)$$

$$A_L(2^{3k-1}-2^{3t-1})=3.(2^{k+t-3}+1)$$

$$A_L(2^{3k-1})=3.(2^{k-t}-1)$$

$$A_L(2^{3k}-2^{3t})=3.(2^{k+t-1}-2^{k-2}+1)$$

$$A_L(2^{3k}-2^{3t-1}))=3.2^k$$

$$A_L(2^{3k})=3.(2^{k-t}-1).(2^{k-t}-1)$$

$$A_L(3.(2^{3k-1}-2^{3t-1}))=2^{3.(k-t)}.(2^t-1).(2^t-1).(2^t-1)$$

$$A_L(3.2^{3k-1}-2^{3t})=3.[(2^{k-1}-1).(2^{k-1}-1).(2^{k-1}-1).2+2^{k-2}+1]$$

$$A_L(3.2^{3k-1}-2^{3t-1})=3.[2^{3k-2t}.(2^t-1)-2^k(2^{2k-2}-3.2^{k-1}+4)-5.2^{k+t-3}-1]$$

(3) $A_B(0)=1$

$$A_B(13.2^{3k-3})=(2^{k-t}-1).(2^{k-t}-1).(2^{k-t}-1)$$

$$A_B(2^{3k}-2^{3t})=3.(2^{k+t-3}+1)$$

$$A_B(2^{3k})=3.(2^{k-t}-1)$$

$$A_B(3.2^{3k-1})=3.(2^{k-t}-1).(2^{k-t}-1)$$

$$A_B(3.(2^{3k-1}-2^{3t-1}))=3.(2^{k+t-1}-2^{k-2}+1)$$

$$A_B(13.(2^{3k-3}-2^{3t-3}))=2^{3.(k-t)}.(2^t-1).(2^t-1).(2^t-1)$$

$$A_B(13.2^{3k-3}-2^{3t})=3.[2^{3k-2t}.(2^t-1)-2^k(2^{2k-2}-3.2^{k-1}+4)-5.2^{k+t-3}-1]$$

$$A_B(3.2^{3k-1}-2^{3t})=3.2^k$$

$$A_B(13.2^{3k-3}-3.2^{3t-1})=3.[(2^{k-1}-1).(2^{k-1}-1).(2^{k-1}-1).2+2^{k-2}+1]$$

Proof: By Lemma 3, each non-zero codeword of $M_{k,t}^{\alpha}$ has Hamming weight either

$$7.2^{3k-3}, 2^{3k-1}-2^{3t-1}, 2^{3k-1}, 3.2^{3k-2}, 3.(2^{3k-2}-2^{3t-2}), 7.(2^{3k-3}-2^{3t-3}), 7.2^{3k-3}-2^{3t-1}, 3.2^{3k-2}-2^{3t-1}$$

or

$$7.2^{3k-3}-3.2^{3t-2}$$

and Lee weight either

$$3.2^{3k-1}, 2^{3k-1}-2^{3t-1}, 2^{3k-1}, 2^{3k}-2^{3t}, 2^{3k}-2^{3t-1}, 2^{3k}, 3.(2^{3k-1}-2^{3t-1}), 3.2^{3k-1}-2^{3t} \text{ or } 3.2^{3k-1}-2^{3t-1}$$

and Bachoc weight either

$$13.2^{3k-3}, 2^{3k}-2^{3t}, 2^{3k}, 3.2^{3k-1}, 3.(2^{3k-1}-2^{3t-1}), 13.(2^{3k-3}-2^{3t-3}), 13.2^{3k-3}-2^{3t}, 3.2^{3k-1}-2^{3t}$$

or

$$13.2^{3k-3}-3.2^{3t-1}.$$

CONCLUSION

In this paper, it was studied the MacDonald codes and some of their properties over the finite ring R. The results can be extended to more general rings like $F_p + uF_p + vF_p$, where p is a prime number, $u^2 = u, v^2 = v, uv = vu = 0$ and $F_p + v_1F_p + \cdots + v_kF_p$, where p is a prime number, $v_i^2 = v_i, v_iv_j = v_jv_i = 0, i \neq j, i = 1, \ldots, k, j = 1, \ldots, k$. MacDonald codes of type β can be studied, as well.

REFERENCES

[1] MacDonald, J., *IBM Journal of Res and Dev.*, **4**, 43, 1960.
[2] Patel, A., *IEEE Trans. Inf. Theory*, **21**, 106, 1975.
[3] Al-Ashker, M.M., *Journal of the Islamic University of Gaza*, **2**, 47, 2005.
[4] Al-Ashker, M.M., *The Islamic University Journal, Series of Natural Studies and Engineering*, **18**, 1, 2010.
[5] Colbourn, C.J., Gupta, M., On Quaternary MacDonald codes, *Proceeding of the International Conference on Information Technology Coding and Computing*, 212-215, 2003.
[6] Dertli, A., Cengellenmis, Y., *International Journal of Algebra*, **5**, 985, 2011.
[7] Cengellenmis, Y., Al-Ashker, M.M., *IUG Journal for Natural and Engineering Studies*, **20**, 1, 2012.
[8] Dertli, A., Cengellenmis, Y., Eren, S., *Palestine Journal of Mathematics*, **4**, 547, 2015.