MacDonald codes over the ring $F_3 + vF_3$

Yasemin Cengellenmis
Mathematics Department
Trakya University, Edirne, TURKEY.
E.mail:ycengellenmis@yahoo.com

Mohammed M. AL-Ashker
Mathematics Department
Islamic University of Gaza P.O.Box 108, Gaza, Palestine
E.mail:mashker@iugaza.edu.ps

Abstract:

In this paper, we construct MacDonald codes of type α over the ring $F_3 + vF_3$, where $v^2 = 1$, $F_3 = \{0, 1, 2\}$ is the field of three elements and investigate some of their properties such as torsion codes and weight distributions..

AMS, Mathematics Classification: Primary 94B05, secondary 51E22.

Key words: MacDonald codes, simplex codes over finite rings.

1. Introduction

The binary MacDonald codes were introduced in [9] and $q-$ary version ($q \geq 2$) MacDonald code over the finite field F_q was studied in [10]. In [5], C.J.Colbourn and M.Gupta obtained two families of MacDonald codes over the ring Z_4 from Z_4-simplex codes of types α and β, S_k^{α} and S_k^{β}. They studied some fundamental properties of the codes. In [1], it was shown that the results of [5] concerning the codes over the ring Z_4 are valid for the ring $F_2 + uF_2$ where $u^2 = 0$ and F_2 is a field of two elements. In [2], the MacDonald codes over the ring $F_2+uF_2+u^2F_2$ were constructed, where $u^3 = 0$ and $F_2 = \{0, 1\}$ by using simplex codes over the ring $F_2+uF_2+u^2F_2$. Their properties were described. In [6], the MacDonald codes over $F_2 + vF_2$ were constructed where $v^2 = v$.

In [3], the simplex codes of type α over the ring $F_3 + vF_3$ where $v^2 = 1$, $F_3 = \{0, 1, 2\}$ were introduced and the minimum Hamming, Lee and Bachoc weights of these codes were obtained.

In this paper, we construct MacDonald codes over the ring $F_3 + vF_3$ by using the simplex codes over the ring F_3+vF_3 of type α, where $v^2 = 1$ and we study torsion codes and weight distributions.

2. Preliminaries

The alphabet $R = F_3 + vF_3 = \{0, 1, 2, v, 2v, a = 1 + v, b = 2 + v, c = 1 + 2v, d = 2 + 2v\}$ is a commutative ring with nine elements where $v^2 = 1$ and $F_3 = \{0, 1, 2\}$. The elements $1, 2, v, 2v$ are units. Addition and multiplication operation over R are given in the following tables,

+	0	1	2	v	2v	a	b	c	d
0	0	1	2	v	2v	a	b	c	d
1	1	2	0	a	c	b	v	d	2v
2	2	0	1	b	d	v	a	2v	c
v	v	a	b	2v	0	c	d	1	2
2v	2v	c	d	0	v	1	2	a	b
a	a	b	v	c	1	d	2v	2	0
b	b	v	a	d	2	2v	c	0	1
c	c	d	2v	1	a	2	0	b	v
d	d	2v	c	2	b	0	1	v	a

·	0	1	2	v	2v	a	b	c	d
0	0	0	0	0	0	0	0	0	0
1	0	1	2	v	2v	a	b	c	d
2	0	2	1	2v	v	d	c	b	a
v	0	v	2v	1	2	a	c	b	d
2v	0	2v	v	2	1	d	b	c	a
a	0	a	d	a	d	d	0	0	a
b	0	b	c	c	b	0	b	c	0
c	0	c	b	b	c	0	c	b	0
d	0	d	a	d	a	a	0	0	d

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

The Hamming weight $wt_H(x)$ of a codeword $x = (x_1, x_2, \ldots, x_n) \in R^n$ is the number of nonzero components. 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 $x = (x_1, x_2, \ldots, x_n) \in R^n$ is defined by, $wt_L(x) = \sum_{i=1}^{n} wt_L(x_i)$ where,

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

In [4], the Bachoc weight for the codeword $x = (x_1, x_2, \ldots, x_n) \in R^n$ is defined by, $wt_B(x) = \sum_{i=1}^{n} wt_B(x_i)$ where,

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

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

For $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in R^n$, $d_H(x, y) = |\{i | x_i \neq y_i\}|$ is called distance between x and $y \in R^n$ 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 $d_H(C) = wt_H(C)$, $d_L(C) = wt_L(C)$, $d_B(C) = wt_B(C)$.

A generator matrix of C is a matrix whose rows generate C.

Two codes are equivalent if one can be obtained from the other by permuting the coordinates.

In [4], it was shown that the ring R has two maximal ideals. These are $m_1 =< b >=< v-1 >=< v+2 >= \{0, v+2, 1+2v\}$ and $m_2 = < v+1 >= \{0, 1+v, 2+2v\}$. Moreover $m_1 \cap m_2 = \{0\}$. The following map,

$$\phi : R \to R/m_1 \times R/m_2$$

$$a \mapsto (\phi_1(a), \phi_2(a))$$

is an isomorphism where these maps $\phi_i : R \mapsto R/m_i$ are canonical homomorphisms for $i = 1,2$. It is easy to see that R/m_i is isomorphic to F_3, for $i = 1,2$. The map ϕ^{-1} is a ring isomorphism by the generalized Chinese Remainder Theorem and R is isomorphic to $R/m_1 \times R/m_2 \cong F_3 \times F_3$, see [8]. This map can be extended from R^n to F_3^{2n} in the following way:

The Gray map ϕ from R^n to F_3^{2n} is defined as

$$\phi : R^n \to F_3^{2n}$$

$$x + vy \mapsto (x, y)$$

where $x, y \in F_3^n$. The Lee weight of $x + vy$ is the Hamming weight of its Gray image. Note that ϕ is linear.

Let $\mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_k}$ be vectors in R^n. Then $\mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_k}$ are independent if $\sum a_j \mathbf{w_j} = \mathbf{0}$ implies that $a_j \mathbf{w_j} = \mathbf{0}$ for all j. The vectors $\mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_k}$ in R^n are modular independent if $\phi(\mathbf{w_1}), \phi(\mathbf{w_2}), \ldots, \phi(\mathbf{w_k})$ are linearly independent for some i, see [7].

In [7], it was shown that a generating set that is both independent and modular independent is a minimal generating set.

Let $\mathbf{w} = (a_1, \ldots, a_n)$ be a nonzero vector then $< (a_1, \ldots, a_n) >$ is either m_1, m_2 or R. Let $I(\mathbf{w}) = \mid < (a_1, \ldots, a_n) > \mid$. Hence $I(\mathbf{w}) = 3$ or 9.

Theorem 2.1 Let C be a code with minimal generating set $\{\mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_s}\}$, then $\mid C \mid = \prod_{i=1}^{s} I(\mathbf{w_i})$, where $|C|$ mean the number of codewords in C.

Proof The summations $\sum a_i \mathbf{w_i}$ are distinct when each $a_i \mathbf{w_i}$ is not zero and there are 9 choices for a_i if $I(\mathbf{w_i}) = 9$ and there are 3 choices for a_i if $I(\mathbf{w_i}) = 3$.

Corollary 2.2 Let $\{\mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_k}\}$ be a minimal generating set for a linear code C over R where there are k_1 vectors having $0, 1, 2, v, 2v, a, b, c$ and d and k_2 vectors having only 0 , b and c or only 0, a and d among them. Then $\mid C \mid = 9^{k_1} 3^{k_2}$.

In [4], it was shown that any code over R is permutation equivalent to a code generated by the following matrix

$$\begin{pmatrix} I_{k_1} & (1-v)B_1 & (v+1)A_1 & (1+v)A_2 + (1-v)B_2 & (1+v)A_3 + (1-v)B_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)A_4 & 0 \\ 0 & 0 & (1-v)I_{k_3} & 0 & (1-v)B_4 \end{pmatrix}$$

where A_i and B_j are ternary matrices over F_3, by the properties of Chinese Remainder Theorem. Such a code is said to have rank $\{9^{k_1}, 3^{k_2}, 3^{k_3}\}$. If H is a code over R, let H^+ (resp. H^-) be the ternary code such that $(1+v)H^+$ (resp. $(1-v)H^-$) is read H mod $(1-v)$ (resp. H mod $(1+v)$).

In [4], it was obtained that,

$$H = (1+v)H^+ \oplus (1-v)H^-$$

with

$$H^+ = \{s | \exists t \in F_3^n | (1+v)s + (1-v)t \in H\}$$
$$H^- = \{t | \exists s \in F_3^n | (1+v)s + (1-v)t \in H\}$$

The code H^+ is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & 0 & 2A_1 & 2A_2 & 2A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix}$$

where A_i are ternary matrices for $i = 1, 2, 3, 4$ and ternary code H^- is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & 2B_1 & 0 & 2B_2 & 2B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix}$$

where B_i are ternary matrices for $i = 1, 2, 3, 4$ in [4].

In [3], the simplex codes over the ring R of type α were constructed as the following;

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

$$G_k^\alpha = \begin{pmatrix} 0\dots0 & | & 1\dots1 & | & 2\dots2 & | & v\dots v & | & 2v\dots2v & | & a\dots a & | & b\dots b & | & c\dots c & | & d\dots d \\ G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha \end{pmatrix}$$

where

$$G_1^\alpha = \begin{pmatrix} 0 & 1 & 2 & v & 2v & a & b & c & d \end{pmatrix}$$

The columns of G_k^α consist of all distinct k-tuples over R. The code S_k^α generated by G_k^α has length 3^{2k}, see [3].

In [3], it was shown that the minimum weights of S_k^α are $d_H = 6.3^{2(k-1)}$, $d_L = 4.3^{2k-1}$ and $d_B = 2.3^{2k-1}$.

Now, some facts about ternary simplex codes, will be given.

Let $G(S_k)$ (columns consisting of all non zero ternary k-tuples) be a generator matrix for an $[n, k]$ ternary simplex code S_k. Then the extended ternary simplex code $\hat{S}_k$ generated by the matrix

$$G(\hat{S}_k) = (0|G(S_k))$$

Inductively,

$$G(\hat{S}_k) = \begin{pmatrix} 0\dots0 & | & 1\dots1 & | & 2\dots2 \\ G(\hat{S}_{k-1}) & | & G(\hat{S}_{k-1}) & | & G(\hat{S}_{k-1}) \end{pmatrix}$$

with

$$G(\hat{S}_1) = (012)$$

Lemma 2.2 The H^+ (or H^-) ternary codes of S_k^α are equivalent to the 3^k copies of $\hat{S}_k$.

Proof It will be proved by induction, firstly for H^+.Observe that the ternary H^+ code of S_k^α is the set of codewords obtained by replacing a by 1 and d by 2 in all a-linear combination of the rows of the matrix aG_k. For $k = 2$, the result holds.

$$G_2 = \begin{pmatrix} 0\ldots0 & | & 1\ldots1 & | & 2\ldots2 & | & v\ldots v & | & 2v\ldots2v & | & a\ldots a & | & b\ldots b & | & c\ldots c & | & d\ldots d \\ 012v2vabcd & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & 012v2vabcd \end{pmatrix}$$

$$H^+ = \begin{pmatrix} 0\ldots0 & | & 1\ldots1 & | & 2\ldots2 & | & 1\ldots1 & | & 2\ldots2 & | & 2\ldots2 & | & 0\ldots0 & | & 0\ldots0 & | & 1\ldots1 \\ 012122001 & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & 01212001 \end{pmatrix}$$

If aG_{k-1} is permutation equivalent 3^{k-1} copies of a $aG(\hat{S}_{k-1})$, then the matrix aG_k takes the form

$$\begin{pmatrix} 0\ldots0 & | & a\ldots a & | & d\ldots d & | & a\ldots a & | & d\ldots d & | & d\ldots d & | & 0\ldots0 & | & 0\ldots0 & | & a\ldots a \\ aG(\hat{S}_{k-1})\ldots aG(\hat{S}_{k-1}) & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & \ldots & | & aG(\hat{S}_{k-1})\ldots aG(\hat{S}_{k-1}) \end{pmatrix}$$

Regrouping the columns gives the desired result. The proof for the H^- case is similar to the above case.

3. MacDonald codes of type α

In [3], the simplex codes had been obtained. A simplex code S_k^α of type α is a linear $[3^{2k}, 2k, 6.3^{2(k-1)}, 4.3^{2k-1}, 2.3^{2k-1}]$ and inductive generator matrix given by

$$G_k^\alpha = \begin{pmatrix} 0\ldots0 & | & 1\ldots1 & | & 2\ldots2 & | & v\ldots v & | & 2v\ldots2v & | & a\ldots a & | & b\ldots b & | & c\ldots c & | & d\ldots d \\ G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha & | & G_{k-1}^\alpha \end{pmatrix}$$

with

$$G_1^\alpha = \begin{pmatrix} 0 & 1 & 2 & v & 2v & a & b & c & d \end{pmatrix}$$

We define the MacDonald codes via the generator matrices of simplex codes. Let $G_{k,u}^\alpha$ be the matrix obtained from G_k^α by deleting columns corresponding to the columns of G_u^α, for $1 \leq u \leq k-1$ i.e.

$$G_{k,u}^\alpha = \begin{pmatrix} G_k^\alpha & \backslash & \frac{0}{G_u^\alpha} \end{pmatrix}$$

where 0 is a $(k-u)\times 3^{2u}$ zero matrix and $(A\backslash B)$ denotes the matrix obtained from the matrix A by deleting the columns of the matrix B.

The code $M^{\alpha}_{k,u}$ generated by the matrix $G^{\alpha}_{k,u}$ is the punctured code of S^{α}_{k} and is a MacDonald code.

$M^{\alpha}_{k,u}$ is a code of length $n = 3^{2k} - 3^{2u}$ and dimension $2k_1 + k_2$.

Remark We define H^{+} or H^{-} of $M^{\alpha}_{k,u}$ as torsion code for the code $M^{\alpha}_{k,u}$.

Lemma 3.1 The Torsion code of $M^{\alpha}_{k,u}$ is ternary linear $[3^{2k}-3^{2u}, 2k_1+k_2, \sum_{n=1}^{k-u} 6.8.3^{2u-2+(2n-2)}]$ code with weight distribution $A_H(0) = 1, A_H(6.3^{2k-2}) = 3^{k-u} - 1$ and $A_H(\sum_{n=1}^{k-u} 6.8.3^{2u-2+(2n-2)}) = 3^{k-u}(3^{u} - 1)$

Proof First we will prove the H^{+} case by induction on k. Since the H^{+} code of $M^{\alpha}_{k,u}$ is the set of codewords obtained by replacing a by 1 and d by 2 in all a-linear combination of the rows of the matrix $aG^{\alpha}_{k,u}$. For $k = 2$ and $u = 1$ the result holds. Suppose that the result holds for $k-1$ and $1 \leq u \leq k-2$. Then for k and $1 \leq k \leq k-1$ the matrix $aG^{\alpha}_{k,u}$ takes the form

$$aG^{\alpha}_{k,u} = \left(\begin{array}{ccc} aG^{\alpha}_{k} & \backslash & \frac{0}{aG^{\alpha}_{u}} \end{array} \right).$$

Each non zero codeword of $aM^{\alpha}_{k,u}$ has Hamming weight either 6.3^{2k-2} or $\sum_{n=1}^{k-u} 6.8.3^{2u-2+(2n-2)})$, then there will be $3^{k-u} - 1$ codewords of hamming weight 6.3^{2k-2} and the number of codewords with Hamming weight $\sum_{n=1}^{k-u} 6.8.3^{2u-2+(2n-2)})$ is $3^{k-u}(3^{u}-1)$. The prove for the H^{-} case is similar to the above case

Remark Each of the first $k-u$ rows has total number of units 4.3^{2k-2} and total number of non-unit elements 4.3^{2k-2}. Each of the last u rows has total number of units $\sum_{n=1}^{k-u} 4.8.3^{(2u-2)+(2n-2)}$ and total number of non-unit elements $\sum_{n=1}^{k-u} 4.8.3^{(2u-2)+(2n-2)}$.

Lemma 3.2 Let $t \in M^{\alpha}_{k,u}, t \neq 0$. If at least one component of t elements is a unit then there are four type of codewords;

I. $w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_a(t) = w_b(t) = w_c(t) = w_d(t) = 3^{2k-2}, w_0(t) = 3^{2k-2} - 3^{2u}$

II. $w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_b(t) = w_c(t) = 3^{2k-2}$ $, w_a(t) = w_d(t) = w_0(t) = 3^{2k-2} - 3^{2u-1}$

III.$w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_a(t) = w_d(t) = 3^{2k-2}$ $, w_c(t) = w_b(t) = w_0(t) = 3^{2k-2} - 3^{2u-1}$

VI. $w_0(t) = w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_a(t) = w_b(t) = w_c(t) =$

$w_d(t) = 3^{2k-2} - 3^{2u-2}$
otherwise
I. $w_a(t) = w_d(t) = 3^{2k-1}, w_0(t) = 3^{2k-1} - 3^{2u}$
II.$w_c(t) = w_b(t) = 3^{2k-1}, w_0(t) = 3^{2k-1} - 3^{2u}$
III. $w_a(t) = w_d(t) = w_0(t) = 3^{2k-1} - 3^{2u-1}$
VI. $w_c(t) = w_b(t) = w_0(t) = 3^{2k-1} - 3^{2u-1}$

Proof By induction on k.

Theorem 3.3 The Hamming and Lee weight distributions of $M^{\alpha}_{k,u}$ are

$$A_H(0) = 1$$
$$A_H(8.3^{2k-2}) = 4$$
$$A_H(6.3^{2k-2} + 2(3^{2k-2} - 3^{2k-1})) = 4(3^{2k-2} - 3)$$
$$A_H(8(3^{2k-2} - 3^{2u-2})) = 3(3^{2k-2} + 3)$$
$$A_H(2.3^{2k-1}) = 4$$
$$A_H(2(3^{2k-1} - 3^{2u-1})) = 2(3^{2k-2} - 3)$$

$$A_L(0) = 1$$
$$A_L(4.3^{2k-2} + 4.2.3^{2k-2}) = 3^{2(k-u)} - 1$$
$$A_L(4(3^{2k-2} - 3^{2u-2}) + 4.2(3^{2k-2} - 3^{2u-2})) = 3^{2k-2u}(3^{2u} - 1)$$

Proof By Lemma 3.2, each non-zero codeword of $M^{\alpha}_{k,u}$ has Hamming weight either $8.3^{2k-2}, 6.3^{2k-2}+2(3^{2k-2}-3^{2k-1}), 8(3^{2k-2}-3^{2u-2}), (2.3^{2k-1})$ or $2(3^{2k-1}-3^{2u-1})$ and Lee weight either $(4.3^{2k-2}+4.2.3^{2k-2})$ or $4(3^{2k-2}-3^{2u-2})+4.2(3^{2k-2}-3^{2u-2})$. The method for counting the weight are similar to one used for S^{α}_{k} in [3]

References

[1] M.M. Al Ashker, Fayik R.EL-Naowq, MacDonald codes over the ring F_2+uF_2, *Journal of the Islamic University of Gaza*, (Series of Natural Studies and Engineering) Vol. no. 2,2005, pp 47-57.

[2] M.M. Al Ashker, MacDonald codes over the ring $F_2+uF_2+u^2F_2$, *The Islamic University Journal*, Series of Natural Studies and Engineering, Vol. 18, No. 2, 2010, pp 1-9.

[3] Y.Cengellenmis, Simplex codes of type α over $F_3 + vF_3$, *Journal Informatics and Mathematical Sciences, submitted.*

[4] R.Chapman, S.T.Dougherty,P.Gaborit and P.Sole, 2-modular lattices from ternary codes, *Journal de Theorie des Nombres de Bordeaux* tome 14, no 1,(2002), pp 73-85.

[5] Charles J. Colbourn, Manish Gupta, On Quaternary MacDonald codes, *Proceeding of the International Conference on Information Technology computers and Com.*, 2003, pp 212-215.

[6] Abdullah Dertli,Y.Cengellenmis, MacDonald codes over the ring $F_2 + vF_2$, *Intrnational Journal of algebra*, Vol. 5, 2011, no. 20, pp 985-991.

[7] S.T.Dougherty,Hongwei Liu, Indepence of vectors in codes over rings,*Des. Codes and Cryp.*, (51), (2009), pp 55-68.

[8] D.MacDonald, Finite rings with identity, Marcel Dekker, New York,(1974).

[9] J.MacDonald, Design methods for maximum minimum distance error-correcting codes,*IBM Journal of Res and Dev.*, 4, 1960, pp 43-57.

[10] A.Patel, Maximal q-ary linear codes with large minimum distance, *IEEE Trans. Inf. Theory*, 21, 1975, pp 106-110.