MacDonald codes over the ring
\[ \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \]

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 \( \alpha \) and \( \beta \) over the ring \( \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \) where \( u^3 = 0 \) and study Gray image properties, torsion code, weight distribution. Finally we obtain linear binary codes by gray map.

AMS, Mathematics Classification: Primary 94B05, Secondary 11H71
Key words: MacDonald codes, linear \( \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \)-codes.
1 Introduction

Recently codes over finite rings have received much attention. In [1] MacDonald codes of type $\alpha$ and $\beta$ over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ were given as a generalization of MacDonald codes over $\mathbb{Z}_4$ [5]. In this paper, we construct MacDonald codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, where $u^3 = 0$ and $\mathbb{F}_2 = \{0, 1\}$ by using simplex codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, besides we describe their properties such as minimum Hamming, Lee and generalized Lee weights.

2 Preliminaries

The ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 = \mathbb{F}_2[u]/(u^3)$ is a commutative chain ring of 8 elements which are $\{0, 1, u, u^2, v, v^2, uv, v^3\}$, where $u^3 = 0$, $v = 1 + u$, $v^2 = 1 + u^2$, $v^3 = 1 + u + u^2$, $uv = u + u^2$.

The ring $R$ is a commutative chain ring with maximal ideal $uR = \{0, u, u^2, uv\}$. Since $u$ is nilpotent with nilpotent index 3, we have

$$R \supset (uR) \supset (u^2R) \supset (u^3R) = 0.$$ 

Moreover $R/uR \cong \mathbb{F}_2$, and $|u^iR| = 2|(u^{i+1}R)| = 2^{3-i}$, $i = 0, 1, 2$.

A linear code $C$ of length $n$ over the ring $R$ is an $R$-submodule of $R^n$. An element of $C$ is called a codeword of $C$. The Hamming weight $wt_H(c)$ of a codeword $c$ is the number of nonzero components. The minimum Hamming weight $wt_H(C)$ of a code $C$ is the smallest weight among all its nonzero codewords. For $x = (x_1, x_2, \cdots, x_n)$, and $y = (y_1, y_2, \cdots, y_n) \in R^n$, $d_H(x, y) = |\{i : x_i \neq y_i\}|$ is called Hamming distance between any distinct vectors $x, y \in R^n$ and 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 minimum distance of $C$ and denoted by $d_H(C) = wt_H(C)$ . The Lee weight of an element $r \in R$ is analogous to the definition of the Lee weight of the elements of the ring $\mathbb{Z}_8$ [7]. The Lee weight $a_r$ of an element $r$ of the ring $R$ is
given by the following equation:

\[ a_r = \begin{cases} 
0 & \text{if } r = 0 \\
1 & \text{if } r = 1, \text{ or } v^2 \\
2 & \text{if } r = u \text{ or } uv \\
3 & \text{if } r = v \text{ or } v^3 \\
4 & \text{if } r = u^2 
\end{cases} \]

Then the Lee weight of an element \( x = (x_1, x_2, ..., x_n) \) of \( R^n \) is

\[ \text{wt}_L(x) = \sum_{i=1}^{n} a_r. \]

**Example 2.1.** Let \( x = (1, 0, 0, u, v, v^2, u^2, uv) \) then \( \text{wt}_L(x) = 13 \).

The Lee distance between \( x \) and \( y \in (R)^n \) is denoted; \( d_L(x, y) = \text{wt}_L(x - y) \). The minimum Lee distance \( d_L \) of a code \( C \) is defined analogously in [7]. Given \( x = (x_1, x_2, \cdots, x_n), y = (y_1, y_2, \cdots, y_n) \in R^n \) their scalar product is, \( xy = x_1y_1 + x_2y_2 + \cdots + x_ny_n \). Two words \( x, y \) are called orthogonal if \( xy = 0 \). For the codes \( C \) over \( R \), its dual \( C^\perp \) is defined as follows, \( C^\perp = \{ x : xy = 0, \forall y \in C \} \). 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. Two codes are equivalent if one can be obtained from the other by permuting the coordinates.

Any code over \( R \) is permutation equivalent to a code \( C \) with generator matrix of the form.

\[
G = \begin{pmatrix}
I_{k_0} & A_{01} & A_{02} & A_{03} \\
0 & uI_{k_1} & uA_{12} & uA_{13} \\
0 & 0 & u^2I_{k_2} & u^2A_{23}
\end{pmatrix},
\]

(2.1)

where \( A_{ij} \) are binary matrices for \( i > 0 \). A code with a generator matrix in this form is of type \( \{k_0, k_1, k_2\} \) and has \( 8^{k_0}4^{k_1}2^{k_2} \) vectors [6].

In reference [2], the generalized gray map \( \phi_{GL} \) was defined as follows:

\[
\phi_{GL} : R^n \rightarrow \mathbb{F}_2^{4n}.
\]

\[
\phi_{GL}(x + uy + u^2z) = (z, x + z, y + z, x + y + z), \text{ where } x, y \text{ and } z \in \mathbb{F}_2 \text{ and } (x + uy + u^2z) \in R^n.
\]
**Proposition 2.1.** The generalized gray map $\phi_{GL}$ is distance preserving linear map or isometry from $((R)^n, d_{GL})$ to $((F_2)^4n, d_H)$ [2].

In ref. [2], the generalized Lee weight of the elements $t \in R$ are given by the following equations:

$$wt_{GL}(t) = wt_H(\phi_{GL}(t)) = \begin{cases} 0 & \text{if } t = 0, \\ 2 & \text{if } t \neq u^2, \\ 4 & \text{if } t = u^2. \end{cases}$$

The generalized Lee distance $d_{GL}$ of $C$ is defined analogously in [2].

**Corollary 2.2.** Let $C$ be a linear code over $R$, then

$$d_H \geq \left\lceil \frac{d_{L}}{4} \right\rceil, \text{ and } d_H \geq \left\lceil \frac{d_{GL}}{4} \right\rceil.$$

A linear code over $C$ over $R$ is said to be of type $\alpha(\beta)$ if

$$d_H = \left\lceil \frac{d_{GL}}{4} \right\rceil \text{ if } d_H > \left\lceil \frac{d_{GL}}{4} \right\rceil.$$ See [2].

**Definition 2.1.** [5] For each $1 \leq i \leq n$, let $A_H(i) (A_L(i) \text{ or } A_{GL}(i))$ be the number of codewords of Hamming (Lee) or generalized Lee weight $i$ in $C$.

Then $\{A_H(0), A_H(1), \ldots, A_H(n)\}, (\{A_L(0), A_L(1), \ldots, A_L(n)\})$ or

$(\{A_{GL}(0), A_{GL}(1), \ldots, A_{GL}(n)\})$ is called the Hamming (Lee) or generalized Lee weight distribution of $C$.

The presence of zero divisors in $R$ creates problem in finding linear dependence of vectors in $R^n$. Consequently, defining the dimension of a module as a cardinality of its basis is not meaningful. Recently in [8] Vazirani, Saran and Sundar Rajan have introduced the notion of $p$-dimension for finitely generated modules over $Z_p$. As a consequence we define the 2-dimension for a code $C$ over $R$ in the following.

A vector $v \in R^n$ is a 2-linear combination of the vectors $v_1, v_2, \ldots, v_k$ if $v = l_1v_1 + l_2v_2 + \ldots + l_kv_k$ with $l_i \in F_2$ for $1 \leq i \leq k$. A subset $B = \{v_1, v_2, \ldots, v_k\}$ of $C$ is a 2- basis for the linear code $C$ over
if for each \( i = 1, 2, \cdots, k - 1 \), \( uv_i \) is a 2-linear combination of \( v_{i+1}, \cdots, v_k \), \( uv_k = 0 \). \( C \) is the 2-linear span of \( B \) and \( B \) is 2-linearly independent. The number of elements in the 2-basis for \( C \) is the 2-dimension of \( C \). It follows that the rows of the matrix 

\[
\mathcal{B} = \begin{pmatrix}
I_{k_0} & A_{01} & A_{02} & A_{03} \\
u I_{k_0} & u A_{01} & u A_{02} & u A_{03} \\
u^2 I_{k_0} & u^2 A_{01} & u^2 A_{02} & u^2 A_{03} \\
0 & u I_{k_1} & u A_{12} & u A_{13} \\
0 & u^2 I_{k_1} & u^2 A_{12} & u^2 A_{13} \\
0 & 0 & u^2 I_{k_2} & u^2 A_{23}
\end{pmatrix}
\]

form a 2-basis for a code \( C \) generated by the matrix \( G \) given by equation (2.1). A linear code \( C \) over \( R \) of length \( n \), 2-dimension \( k = \sum_{i=0}^{2}(3-i)k_i \), minimum distance \( d_H \), \( d_L \) and \( d_G \) is called an \([n,k,d_H,d_L,d_G],[n,k,d_H]\) or simply \([n,k]\) code. The higher torsion codes were defined in ref. [3]. In ref. [6] for a code over \( R \), the authors defined the following torsion codes over the field \( F_2 \). For \( 0 \leq i \leq 2 \), \( Tor_i(C) = \{ v : u^iv \in C \} \).

In general we note that, \( Tor_0(C) \subseteq Tor_1(C) \subseteq Tor_2(C) \). If \( i = 0 \), \( Tor_0(C) \) is called the residue code and is denoted by \( Res(C) \). If \( C \) is a free module then \( Tor_0(C) = Tor_2(C) \).

3 Main Results

In this section we will study the Macdonald codes of types \( \alpha \) and \( \beta \) over \( R \) and also we study the properties of their images under the Generalized Gray map.

3.1 R-Macdonald codes of types \( \alpha \) and \( \beta \)

The simplex codes over \( R \) of type \( \alpha \) and \( \beta \) have been constructed in [2]. A type \( \alpha \) simplex code \( S_{k}^{\alpha} \) is a linear code over \( R \) constructed inductively by the following generator matrix. Let \( G_{k}^{\alpha} \) be a \( k \times 2^{3k} \) matrix over \( R \) defined inductively by

\[
G_{k}^{\alpha} = \left[
\begin{array}{c|c|c|c|c|c|c}
00...0 & 11...1 & uu...u & \cdots & v^3v^3...v^3 \\
G_{k-1}^{\alpha} & G_{k-1}^{\alpha} & G_{k-1}^{\alpha} & \cdots & G_{k-1}^{\alpha}
\end{array}\right]; k \geq 2 \tag{3.1}
\]
where

\[ G_1^\alpha = [0, 1, u, v, u^2, uv, v^2, v^3]. \]

A type \( \beta \) simplex code \( S_k^\beta \) is a linear code over \( R \) constructed by omitting some columns from \( G_k^\alpha \).

Let \( G_k^\beta \) be the \( k \times 2^{2(k-1)}(2^k - 1) \) matrix defined inductively by

\[
G_2^\beta = \begin{bmatrix}
111 \ldots 1 \\
0, 1, u, v, u^2, uv, v^2, v^3 \\
\end{bmatrix} 
\begin{bmatrix}
0 & u & u^2 & uv \\
1 & 1 & 1 & 1 \\
\end{bmatrix},
\]

and for \( k > 2 \),

\[
G_k^\beta = \begin{bmatrix}
111 \ldots 1 & 00 \ldots 0 & u, u, \ldots, u & u^2, u^2, \ldots, u^2 & uv, uv, \ldots, uv \\
G_{k-1}^\alpha & G_{k-1}^\beta & G_{k-1}^\alpha & G_{k-1}^\beta & G_{k-1}^\alpha & G_{k-1}^\beta \\
\end{bmatrix},
\]

where \( G_{k-1}^\alpha \) is the generating matrix of \( S_{k-1}^\alpha \) and \( G_k^\beta \) is obtained from \( G_k^\alpha \) by deleting \( 2^{2(k-1)}(3 \cdot 2^k + 1) \) columns.

We will now construct the Macdonald codes by using the generator matrices of simplex codes. For \( 1 \leq t \leq k - 1 \), Let \( G_{k,t}^\alpha \) (\( G_{k,t}^\beta \)) be the matrix obtained from \( G_k^\alpha \) (\( G_k^\beta \)) by deleting columns corresponding to the columns of \( G_t^\alpha \) (\( G_t^\beta \)) by deleting columns corresponding to the columns of \( G_t^\alpha \) (\( G_t^\beta \)). i.e.,

\[
G_{k,t}^\alpha = \begin{bmatrix}
G_k^\alpha \setminus G_t^\alpha \\
\end{bmatrix} \quad (3.2)
\]

and

\[
G_{k,t}^\beta = \begin{bmatrix}
G_k^\beta \setminus G_t^\beta \\
\end{bmatrix} \quad (3.3),
\]

where

\[
\begin{bmatrix}
A \\
\end{bmatrix} \setminus \begin{bmatrix}
B \\
\end{bmatrix}
\]

denotes the matrix obtained from the matrix \( A \) by deleting the matrix \( B \) and \( 0 \) in (3.2)(respectively) (3.3)) is a \( (k - t) \times e \) (respectively \( (k - t) \times 2^{2(t-1)}(2^t - 1) \)) zero matrix. The code \( \mathcal{M}_{k,t}^\alpha(\mathcal{M}_{k,t}^\beta) \) was generated by the matrix \( G_{k,t}^\alpha \) (\( G_{k,t}^\beta \)) is the punctured code of \( S_k^\alpha \) (\( S_k^\beta \)) and is called a MacDonald code. i.e. (The MacDonald codes are obtained by deleting some columns of the generator matrices \( G_k^\alpha \) (\( G_k^\beta \)) of the simplex codes \( S_k^\alpha \) (\( S_k^\beta \))).

6
3.2 Properties

The code $\mathcal{M}^\alpha_{k,t}$ is an $R-$code of length $n = 2^{3k} - 2^{3t}$ and is a 2-dimensional $3k$ and $\mathcal{M}^\beta_{k,t}$ is an $R-$code of length $n = 2^{2(k-1)}(2^k - 1) - 2^{2(t-1)}(2^t - 1) = 3^{3k-2} - 2^{2k-2} - 3^{3t-2} + 2^{2t-1}$ and is a 2-dimensional $3k$.

Lemma 3.1. The torsion code $\text{Tor}_2(\mathcal{C})$ of $\mathcal{M}^\alpha_{k,t}$ is a binary linear code $[2^{3k} - 2^{3t}, k, 2^{3k-1} - 2^{3t-1}]$ two weight code with weight distributions

1) $A_H(0) = 1$.

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

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

Proof. Since the torsion code of $\mathcal{M}^\alpha_{k,t}$ is the set of codewords obtained by replacing $u^2$ by 1 in all linear combinations of the rows of the matrix $u^2G_{k,t}^\alpha$ (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 $1 \leq t \leq k - 2$. Then for $k$ and $1 \leq t \leq k - 1$ the matrix $u^2G_{k,t}^\alpha$ takes the form

$$u^2G_{k,t}^\alpha = \left[ u^2G_k^\alpha \setminus 0 \right].$$

Each nonzero codeword of $u^2\mathcal{M}^\alpha_{k,t}$ has Hamming weight either $2^{3k-1} - 2^{3t-1}$ or $2^{3k-1}$ and the dimension of the torsion code of $\mathcal{M}^\alpha_{k,t}$ is $k$, then there will be $2^k - 2^{k-t}$ codewords of Hamming weight $2^{3k-1} - 2^{3t-1}$ and the number of codewords with Hamming weight $2^{3k-1}$ is $(2^{k-t} - 1)$. The result now follows.

Lemma 3.2. The torsion code of $\mathcal{M}^\beta_{k,t}$ is a binary linear code $[2^{2(k-1)}(2^k - 1) - 2^{2(t-1)}(2^t - 1), k, 2^{3k-3} - 2^{3t-3}]$ with weight distributions

1) $A_H(0) = 1$.

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

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

Proof. Same as the proof in lemma 3.1.
Remark 3.1. Each of the first $k-t$ rows of (3.2) has total number of units $2^{3k-1}$ and total number of nonzero divisors $3 \cdot 2^{3k-3}$ and the last $t$ rows has total number of units $2^{3k-1} - 2^{3t-1}$ and total number of nonzero divisors $3 \cdot (2^{4k-3} - 2^{3t-3})$.

Theorem 3.3. The Hamming, Lee and Generalized Lee weight distributions of $M^\alpha_{k,t}$ are

1) $A_H(0) = 1$, $A_H(2^{3k-1} - 2^{3t-1}) = 2^{k-1}(2^t - 1)$, $A_H(2^{3k-1}) = (2^{k-t+1} - 1)$, $A_H(3 \cdot 2^{3k-2}) = 2^{k-t}(2^{k-1} - 1)$, $A_H(3 \cdot (2^{3k-2} - 2^{3t-2})) = 2^{2k-t}(2^t - 1)$, $A_H(7 \cdot 2^{3k-3}) = 2^{2k-t}(2^{k-1} - 1)$, $A_H(7 \cdot (2^{3k-3} - 2^{3t-3})) = 2^{3k-t}(2^t - 1)$, $A_H(7 \cdot 2^{3k-3} - 2^{3t-1}) = 2^{2k-t} - (2^t - 1)(2^{k-t} - 1)$.

2) $A_L(0) = 1$, $A_L(2^{3k+1}) = 2^{3(k-t)} - 1$, $A_L(2^{3k+1} - 2^{3t+1}) = 2^{3k-3t}(2^{3t} - 1)$.

3) $A_{GL}(0) = 1$, $A_{GL}(2^{3k+1}) = 2^{3(k-t)} - 1$, $A_{GL}(2^{3k+1} - 2^{3t+1}) = 2^{3(k-t)}(2^{3k} - 1)$.

Proof. Each non zero codeword of $M_{k,t}$ has Hamming weight either $2^{3k-1} - 2^{3t-1}$, $2^{3k-1}$, $3 \cdot 2^{3k-2}$, $3(2^{3k-2} - 2^{3t-2})$, $3 \cdot 2^{2k-2} - 2^{2t-1}$, $7 \cdot 2^{3k-3} - 2^{3t-3}$, $7(2^{3k-3} - 2^{3t-3})$, or $7 \cdot 2^{3k-3} - 2^{3t-1}$, Lee weight either $2^{3k+1}$, $2^{3k+1} - 2^{3t+1}$ and Generalized lee weights $2^{3k+1}$ or $2^{3k+1} - 3^{3t+1}$. The counting of the weight followed by the weight distribution of the torsion code of $M_{k,t}$, (see lemma 3.1) and the argument is similar to that used in [2].

Theorem 3.4. The image of $M^\alpha_{k,t}$ under the generalized Gray map is a linear $[2^{3k+1} - 2^{3t+1}, 2^{3k}, 2^{3k+1} - 2^{3t+1}]$ binary two weight code with possible weight $2^{3k+1} - 2^{3t+1}$ and $2^{3k+1}$.

Proof. The binary image of the generalized Gray map is linear by proposition 2.1. We prove by induction with respect to $k$. For $k = 2$ the result holds. The matrix (3.2) can be written as $G_{k,t}^\alpha = [G_{k,k-1}^\alpha | G_{k,t-1}^\alpha]$. Suppose the result is true for $k - 1$, then the possible Generalized weight of $M^\alpha_{k-1,t}$ are $2^{3(k-1)+1} - 2^{3(t-1)+1}$ and $2^{3(k-1)+1}$ and the possible Generalized Lee weight of $M^\alpha_{k-1,t}$ are $2^{3k+1} - 2^{3(k-1)+1}$ and $2^{3k+1}$. Then the possible Lee weight of $M^\alpha_{k,t}$ are $2^{3k-2} - 2^{3t+1} + 2^{3k+1} - 2^{3k-2} = 2^{3k+1} - 2^{3t+1}$ and $2^{3k+1}$. Since by proposition 2.1 the minimum Hamming weight of the binary image of the generalized Gray map of $M^\alpha_{k,t}$ is equal the minimum Lee weight of $M^\alpha_{k,t}$ then the result follows.
Theorem 3.5. The image of $M_{k,t}^2$ under the generalized Gray map is a linear $[2^{3k+1} - 2^{3t+1} - 2^{2k+1} + 2^{2t+1}, 2^{3k}]$ binary code.

Proof. Similar to the proof in theorem 3.4.

3.3 Conclusion

In this paper we have studied $R$- MacDonald codes and some of their properties. One can also extend these ideas to a more general rings like $\sum_{n=0}^{s} u^n F_2$ and to $\sum_{n=0}^{s} u^n F_p$, where $p$ is a prime integer and $u^{s+1} = 0$.

References


