Proceedings of the Jangjeon Mathematical Society
21 (2018), No. 4. pp. 617 - 625

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2018.21.4.617

SELF-DUAL CODES OVER THE RING $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$

ANKUR

Abstract. We discuss self-dual codes over the ring $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}, u^2 = 0, v^2 = 0, uv = vu$. We consider definition of trace function and self-dual basis over the field $\mathbb{F}_{2^m}$. We consider the Gray map and self-orthogonal basis to discuss some theoretical properties of self-dual and Type II codes over the ring R. Also we see how Lee weight and trace are related over the ring R for a self-dual basis.

2000 Mathematics Subject Classification. 94B05, 11F72.

Keywords and phrases. Self-dual codes, Gray map, Trace function, Self-orthogonal basis.

1. Introduction

Self-dual codes and Type II codes have been extensively studied from the long period of time by the various researchers. In [3], Bonnecaze and Udaya discussed the cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$. They also discussed the self-dual codes over the ring as the Conway and Sloane discussed the self-dual codes of odd length over the ring of integers modulo 4. In [11], MacWilliams et al. studied self-dual codes over the ring $GF(4)$, they defined the weight enumerators and found the upper bound on the minimum distance and used the generator matrix to discuss the self-dual codes. Dougherty et al. [5] considered the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ and discussed the Type II property of the codes over the ring. They also defined the Lee weight of the elements of the ring as:

$$w_L(0) = 0, w_L(1) = 1 = w_L(1 + u), w_L(u) = 2.$$

Also they defined the generator matrix over the ring and classified all the self-dual codes of lengths upto 8 over the ring $\mathbb{F}_2 + u\mathbb{F}_2$. codes over the ring have been studied by many researchers (we refer to [1, 2, 4, 6, 7, 8, 9, 13, 15] for the detailed description)

San Ling and Patrick Sole [10] considered the ring $\mathbb{F}_4 + u\mathbb{F}_4$ with $u^2 = 0$ and discussed the Type II code by defining a Gray map. They developed the various commutative relations over the rings and constructed a lattice to describe Type II property of the unimodular lattice. Betsumiya et al. [2] considered the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with $u^2 = 0$ and defined a Gray map to discuss Type II property of self-dual codes. They also defined the mass formula for the self-dual codes over the given ring by defining the generator matrix and also gave the classification of self-dual codes over the given ring.

We use the motivation from [2] to extend the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ to $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ with $u^2 = v^2 = 0, uv = vu$ and define a Gray map over the ring R to discuss self-dual and Type II property over the ring R. Also we use the concept of trace orthogonal basis to describe the Type II property and Lee weight of the self-dual codes over the ring R.

2. Preliminaries

We consider the ring $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$, with $u^2 = 0, v^2 = 0$ and $uv = vu$. We define trace of an element $\beta \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$ as:

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = \sum_{i=0}^{m-1} \beta^{q^i}$$

Also we define a trace orthogonal basis $A = \{\beta_1, \beta_2, \ldots, \beta_m\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ as:

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_i\beta_j) = \left\{ \begin{array}{ll} \neq 0 & \text{for } i = j, \\ 0 & i \neq j. \end{array} \right\}$$

We say a trace orthogonal basis self-dual or self-complimentary basis if $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta_i^2) = 1$ for $i = 1, 2, \ldots, m$. Let $A = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a trace orthogonal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$, then A can be visualized as a self-dual basis. We define the Lee weight of a vector $v \in \mathbb{F}_{2^m}$ with respect to the basis A to be the sum of the Lee weights of its components.

We define Euclidean inner product on the ring R by $c \cdot d = \sum_{i=1}^{n} c_i d_i,\ \forall$ $c = (c_1, c_2, \ldots, c_n)$ and $d = (d_1, d_2, \ldots, d_n)$ $c, d \in R$. A code C over R is defined as a sub-module of R^n. We define a dual code of C as $C^\perp = \{d \in R \mid c \cdot d = 0, \forall c \in C\}$. If $C = C^\perp$. Then C is called self-dual. We call a self-dual code to be Type II code with respect to the basis A if the Lee weight of every code word in C is divisible by 4. Definition of Type II code may be independent of the choice of trace orthogonal basis.

We define a Gray map

$$\psi_m : R^n \to \mathbb{F}_{2^m}^{4n},$$

$$a + ub + vc + uvd \mapsto (a + b + c + d, c + d, b + d, d)$$

where $a, b, c, d \in \mathbb{F}_{2^m}^n$. The map ψ_m is a linear isometry from (R^n, Lee distance) to ($\mathbb{F}_{2^m}^{4n}$, Lee distance).

We define the Lee distance between two code words a and b to be the Lee weight of $a - b$. If m can be factorized as $m = rst$, we choose bases for the tower of finite fields $\mathbb{F}_2 \subset \mathbb{F}_{2^t} \subset \mathbb{F}_{2^r} \subset \mathbb{F}_{2^m}$. Before doing this we consider the more general situation. Consider the tower $\mathbb{F}_q \subset \mathbb{F}_{q^t} \subset \mathbb{F}_{q^{rt}} \subset \mathbb{F}_{q^{rst}}$ and let $A_1 = \{\beta_1, \beta_2, \ldots, \beta_s\}$, $A_2 = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ and $A_3 = \{\gamma_1, \gamma_2, \ldots, \gamma_t\}$ be trace orthogonal basis for $\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}$, $\mathbb{F}_{q^{rt}}/\mathbb{F}_{q^t}$ and $\mathbb{F}_{q^t}/\mathbb{F}_q$, respectively. In general it does not follow that $A = \{\alpha_i\beta_j\gamma_k \mid 1 \leq i \leq r, 1 \leq j \leq s, 1 \leq k \leq t\}$ is a trace orthogonal basis for $\mathbb{F}_{q^{rst}}/\mathbb{F}_q$.

We define a Gray map $\phi : \mathbb{F}_{2^m}^n \to (\mathbb{F}_2)^{mn}$,

$$a_1\beta_1 + a_2\beta_2 + \ldots + a_m\beta_m \mapsto (a_1, a_2, \cdots, a_m),$$

where $a_1, a_2, \ldots, a_m \in \mathbb{F}_2^n$. The Gray map ϕ is an isometry.
Let $(R_u)_m$ denote the commutative ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ with $u^2 = 0$, we define the Gray map

$$\phi_m : (R_u)_m^n \to \mathbb{F}_{2^m}^{2n},$$
$$a + ub \mapsto (b, a + b)$$

where $a, b \in \mathbb{F}_{2^m}^n$. The map ϕ_m is an $\mathbb{F}_{2^m}$-linear isometry. We can now extend the map ϕ to the Gray map $\phi' : (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})^n \to (\mathbb{F}_2 + u\mathbb{F}_2)^{mn}$,

$$a_1\beta_1 + a_2\beta_2 + \ldots + a_m\beta_m \mapsto (a_1, a_2, \ldots, a_m)$$

where $a_1, a_2, \ldots, a_m \in (\mathbb{F}_2 + u\mathbb{F}_2)^n$. The Gray map ϕ' is an $(\mathbb{F}_2 + u\mathbb{F}_2)$-linear isometry from $((\mathbb{F}_{2^m} + u\mathbb{F}_{2^m})^n$, Lee distance) to $((\mathbb{F}_2 + u\mathbb{F}_2)^{mn}$, Lee distance). We can now extend the Gray map ϕ' to the Gray map

$$\phi'' : (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m})^n \to (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^{mn},$$
$$a_1\beta_1 + a_2\beta_2 + \ldots + a_m\beta_m \mapsto (a_1, a_2, \cdots, a_m),$$

where $a_1, a_2, \ldots, a_m \in (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^n$. The Gray map ϕ'' is an $(\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)$-linear isometry from $((\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m})^n$,Lee distance) to $(((\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2))^{mn}$, Lee distance).

Proposition 2.1. *Let A, A_1, A_2 and A_3 be the bases defined above. A is a trace orthogonal basis, if the trace orthogonal bases A_1, A_2 and A_3 are such that $Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}}(\beta_i^2)$ is a non-zero element of $\mathbb{F}_q$ for every $i = 1, 2, \ldots, s$. In particular, if A_1, A_2 and A_3 are self-dual, then A is self-dual.*

Proof. We need to show that $Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_q}(\alpha_i\beta_j\gamma_k\alpha_{i'}\beta_{j'}\gamma_{k'})$ is non-zero if and only if $i = i'$, $j = j'$ and $k = k'$.
If $Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}}(\beta_i\beta_j)$ is a non-zero element of $\mathbb{F}_q$ for $i = j$, we have

$$\begin{aligned} Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_q}(\alpha_i\beta_j\gamma_k\alpha_{i'}\beta_{j'}\gamma_{k'}) &= Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}(Tr_{\mathbb{F}_{q^r}/\mathbb{F}_{q^t}}(Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}}(\alpha_i\beta_j\alpha_{i'}\beta_{j'}\gamma_k\gamma_{k'}))) \\ &= Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\gamma_k\gamma_{k'}Tr_{\mathbb{F}_{q^r}/\mathbb{F}_{q^t}}(\alpha_i\alpha_{i'})Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}}(\beta_j\beta_{j'})) \\ &= Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\gamma_k\gamma_{k'})Tr_{\mathbb{F}_{q^r}/\mathbb{F}_{q^t}}(\alpha_i\alpha_{i'})Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}}(\beta_j\beta_{j'}) \end{aligned}$$

$$= \left\{ \begin{array}{ll} Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}}(\beta_j^2)Tr_{\mathbb{F}_{q^r}/\mathbb{F}_{q^t}}(\alpha_i\alpha_{i'})Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\gamma_k\gamma_{k'}) & \text{if } j = j', \\ 0 & \text{if } i \neq i'. \end{array} \right\}$$
$$= \left\{ \begin{array}{ll} \neq 0 & \text{if } j = j', i = i' \text{ and } k = k' \\ 0 & \text{otherwise.} \end{array} \right\}$$

If A_1, A_2 and A_3 are self-dual bases, then

$$Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_{q^{rt}}}(\beta_j\beta_{j'}) = \left\{ \begin{array}{ll} 1 & \text{if } j = j', \\ 0 & \text{if } j \neq j'. \end{array} \right\}$$

$$Tr_{\mathbb{F}_{q^{rt}}/\mathbb{F}_{q^t}}(\alpha_i\alpha_{i'}) = \left\{ \begin{array}{ll} 1 & \text{if } i = i', \\ 0 & \text{if } i \neq i'. \end{array} \right\}$$

and

$$Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\gamma_k\gamma_{k'}) = \left\{ \begin{array}{ll} 1 & \text{if } k = k', \\ 0 & \text{if } k \neq k'. \end{array} \right\}$$

Thus we get

$$Tr_{\mathbb{F}_{q^{rst}}/\mathbb{F}_q}(\alpha_i\beta_j\gamma_k\alpha_{i'}\beta_{j'}\gamma_{k'}) = \left\{ \begin{array}{ll} 1 & \text{if } i = i', j = j' \text{ and } k = k' \\ 0 & \text{otherwise,} \end{array} \right\}$$

This shows A is self-dual. □

Now we choose self-dual bases $A_1 = \{\beta_1, \beta_2, \ldots, \beta_s\}$ of $\mathbb{F}_{2^m}$ over $\mathbb{F}_{2^{rt}}$, $A_2 = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ of $\mathbb{F}_{2^{rt}}$ over $\mathbb{F}_{2^t}$ and $A_3 = \{\gamma_1, \gamma_2, \ldots, \gamma_t\}$ of $\mathbb{F}_{2^t}$ over $\mathbb{F}_2$.

We now thus define the intermediate Gray maps as follows:

$$\psi_m^I : \mathbb{F}_{2^m}^n \to \mathbb{F}_{2^{rt}}^{sn},$$

$$a_1\beta_1 + a_2\beta_2 + \ldots + a_s\beta_s \mapsto (a_1, a_2, \ldots, a_s)$$

for $a_1, a_2, \ldots, a_s \in \mathbb{F}_{2^{rt}}^n$.

$$\psi_m^{II} : \mathbb{F}_{2^{rt}}^n \to \mathbb{F}_{2^t}^{rn},$$

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_r\alpha_r \mapsto (a_1, a_2, \ldots, a_r)$$

for $a_1, a_2, \ldots, a_r \in \mathbb{F}_{2^t}^n$ and

$$\psi_m^{III} : \mathbb{F}_{2^t}^n \to \mathbb{F}_2^{tn},$$

$$a_1\gamma_1 + a_2\gamma_2 + \ldots + a_t\gamma_t \mapsto (a_1, a_2, \ldots, a_t)$$

for $a_1, a_2, \ldots, a_t \in \mathbb{F}_2^n$. These maps have the following natural extensions:

$$\psi_m^{I'} : (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m})^n \to (\mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}})^{sn},$$

$$a_1\beta_1 + a_2\beta_2 + \ldots + a_s\beta_s \mapsto (a_1, a_2, \ldots, a_s),$$

where $a_1, a_2, \ldots, a_s \in (\mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}})^n$

$$\psi_m^{II'} : (\mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}})^n \to (\mathbb{F}_{2^t} + u\mathbb{F}_{2^t} + v\mathbb{F}_{2^t} + uv\mathbb{F}_{2^t})^{rn},$$

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_r\alpha_r \mapsto (a_1, a_2, \ldots, a_r),$$

where $a_1, a_2, \ldots, a_r \in (\mathbb{F}_{2^t} + u\mathbb{F}_{2^t} + v\mathbb{F}_{2^t} + uv\mathbb{F}_{2^t})^n$ and

$$\psi_m^{III'} : (\mathbb{F}_{2^t} + u\mathbb{F}_{2^t} + v\mathbb{F}_{2^t} + uv\mathbb{F}_{2^t})^n \to (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^{tn},$$

$$a_1\gamma_1 + a_2\gamma_2 + \ldots + a_t\gamma_t \mapsto (a_1, a_2, \ldots, a_t),$$

where $a_1, a_2, \ldots, a_t \in (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^n$.

By the proposition proved above, self-dual bases A_1, A_2 and A_3 also gives us a self-dual basis $A = \{\alpha_i\beta_j\gamma_k \mid 1 \leq i \leq r, 1 \leq j \leq s, 1 \leq k \leq t\}$ of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ with the corresponding Gray maps $\phi : \mathbb{F}_{2^m}^n \to \mathbb{F}_2^{mn}$ and $\phi'' : (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m})^n \to (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^{mn}$. We get $\phi = \psi_m^{III} \circ \psi_m^{II} \circ \psi_m^I$ and $\phi'' = \psi_m^{III'} \circ \psi_m^{II'} \circ \psi_m^{I'}$ by choosing a suitable ordering of the basis elements $\alpha_i\beta_j\gamma_k$. Also for the Gray map to preserve the self-dual property of a code it is necessary to choose the self-dual basis.

3. Self-dual codes over the ring

In this section we use Gray map to study Type II codes over the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ and discuss some theoretical aspects of codes over the ring.

Proposition 3.1. *Let C be a length n code over the ring R. If C is self-orthogonal, so will be $\psi_m(C)$. A code C is of Type II over the ring R iff $\psi_m(C)$ is a Type II code over $\mathbb{F}_{2^m}$. Also $min\{wt_L(C)\}= min\{wt_L(\psi_m(C))\}$.*

Proof. Let $x = a_1 + ub_1 + vc_1 + uvd_1$ and $y = a_2 + ub_2 + vc_2 + uvd_2$ be two codewords in C, where $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in \mathbb{F}_{2^m}$. Then the Euclidean inner product of x and y is

$$x \cdot y = (a_1 + ub_1 + vc_1 + uvd_1) \cdot (a_2 + ub_2 + vc_2 + uvd_2)$$

$= a_1 \cdot a_2 + u(a_1 \cdot b_2 + b_1 \cdot a_2) + v(a_1 \cdot c_2 + c_1 \cdot a_2) + uv(a_1 \cdot d_2 + d_1 \cdot a_2 + b_1 \cdot c_2 + c_1 \cdot b_2)$
since C is self-orthogonal, so $a_1 \cdot a_2 = a_1 \cdot b_2 + b_1 \cdot a_2 = a_1 \cdot c_2 + c_1 \cdot a_2 = a_1 \cdot d_2 + d_1 \cdot a_2 + b_1 \cdot c_2 + c_1 \cdot b_2 = 0$.
Now we have $\psi_m(x) \cdot \psi_m(y) = (a_1 + b_1 + c_1 + d_1, c_1 + d_1, b_1 + d_1, d_1) \cdot (a_2 + b_2 + c_2 + d_2, c_2 + d_2, b_2 + d_2, d_2)$
$= a_1 \cdot a_2 + a_1 \cdot b_2 + b_1 \cdot a_2 + a_1 \cdot c_2 + c_1 \cdot a_2 + a_1 \cdot d_2 + d_1 \cdot a_2 + b_1 \cdot c_2 + c_1 \cdot b_2 = 0$.
Thus $\psi_m(C)$ is self-orthogonal over $\mathbb{F}_{2^m}$.
Since the map ψ_m is an isometry, so image of a Type II code under ψ_m is again a Type II code over $\mathbb{F}_{2^m}$ and hence the minimum of the Lee weight of C is same as minimum of the Lee weight of $\psi_m(C)$. □

Proposition 3.2. *Let $m = rst$, and ψ'_m the Gray map corresponding to a self-dual basis $A = \{\beta_1, \beta_2, \cdots, \beta_s\}$ of $\mathbb{F}_{2^m}$ over $\mathbb{F}_{2^{rt}}$. Let C be a code of length n over $\mathbb{F}_{2^m}$. If C is self-orthogonal, so will be $\psi^I_m(C)$. Image of a Type II code C is again a Type II code under the map ψ^I_m over $\mathbb{F}_{2^m}$. Also $min\ \{wt_L(C)\} = min\ \{wt_L(\psi^I_m(C))\}$.*

Proof. Let $x = \sum_{i=1}^{s} a_i\beta_i$ and $y = \sum_{i=1}^{s} a'_i\beta_i$ be codewords in C, where $a_i, a'_i \in \mathbb{F}^n_{2^{rt}}$. If C is self-orthogonal, then $x \cdot y = \sum_{i,j}(a_i \cdot a'_i)\beta_i\beta_j = 0$.
Taking the trace over $\mathbb{F}_{2^{rt}}$, we get
$0 = Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\sum_{i,j}(a_i \cdot a'_j)\beta_i\beta_j) = \sum_{i,j} Tr_{\mathbb{F}_{2^m}/F_{2^{rt}}}((a_i \cdot a'_j)\beta_i\beta_j)$
$= \sum_{i,j}(a_i \cdot a'_j)Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\beta_i\beta_j)$
Since A is self-dual basis and

$$Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\beta_i\beta_j) = \left\{ \begin{array}{ll} 1 & \text{if } i = j', \\ 0 & \text{if } i \neq j'. \end{array} \right\}$$

Gives us $\sum_{i=j} a_i \cdot a'_j = 0$
This implies that $\psi^I_m(x) \cdot \psi^I_m(y) = 0$. Hence $\psi^I_m(C)$ is self-orthogonal.
Also image of a Type II code is Type II code under ψ^I_m and minimum Lee weight of C coincides with the minimum Lee weight of $\psi^I_m(C)$, because of ψ^I_m being an isometry. □

Proposition 3.3. *Let $m = rst$, and $\psi_m^{I'}$ the Gray map from $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}}$ corresponding to the self-dual basis $A = \{\beta_1, \beta_2, \cdots, \beta_s\}$ of $\mathbb{F}_{2^m}$ over $\mathbb{F}_{2^{rt}}$. Let C be a length n code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$. If C is self-orthogonal, so will be $\psi_m^{I'}(C)$. A code C is of Type II over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ if and only if $\psi_m^{I'}(C)$ is a Type II code over $\mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}}$. The minimum Lee weight of C is equal to the minimum Lee weight of $\psi_m^{I'}(C)$.*

Proof. Let $x = \sum_{i=1}^{s} a_i\beta_i$ and $y = \sum_{i=1}^{s} a'_i\beta_i$ be two codewords in C and write $a_i = a_{i1} + ub_{i1} + vc_{i1} + uvd_{i1}$ and $a'_i = a_{i2} + ub_{i2} + vc_{i2} + uvd_{i2}$ be the elements of $\mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}}$, where $a_{i1}, b_{i1}, c_{i1}, d_{i1}, a_{i2}, b_{i2}, c_{i2}, d_{i2} \in \mathbb{F}_{2^{rt}}$. The inner product of x and y is

$$x \cdot y = \sum_{i,j}(a_{i1} \cdot a_{j2})\beta_i\beta_j + u\sum_{i,j}(a_{i1} \cdot b_{j2} + b_{i1} \cdot a_{j2})\beta_i\beta_j$$
$$+ v\sum_{i,j}(a_{i1} \cdot c_{j2} + c_{i1} \cdot a_{j2})\beta_i\beta_j + uv\sum_{i,j}(a_{i1} \cdot d_{j2} + d_{i1} \cdot a_{j2} + b_{i1} \cdot c_{j2}$$
$$+ c_{i1} \cdot b_{j2})\beta_i\beta_j$$

We define a function $f : \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m} \to \mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}}$ by
$f(a + ub + vc + uvd) := Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(a) + uTr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(b) + vTr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(c) + uvTr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(d)$,
we then have

$$f(x \cdot y) = \sum_{i,j}(a_{i1} \cdot a_{j2})Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\beta_i\beta_j) +$$
$$u\sum_{i,j}(a_{i1} \cdot b_{j2} + b_{i1} \cdot a_{j2})Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\beta_i\beta_j)$$
$$+v\sum_{i,j}(a_{i1} \cdot c_{j2} + c_{i1} \cdot a_{j2})Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\beta_i\beta_j)$$
$$+uv\sum_{i,j}(a_{i1} \cdot d_{j2} + d_{i1} \cdot a_{j2} + b_{i1} \cdot c_{j2} + c_{i1} \cdot b_{j2})Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\beta_i\beta_j).$$

Since

$$Tr_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{rt}}}(\beta_i\beta_j) = \left\{ \begin{array}{ll} 1 & \text{if } i = j', \\ 0 & \text{if } i \neq j'. \end{array} \right\}$$

Therefore

$$f(x \cdot y) = \sum_{i=1}^{s}(a_{i1} \cdot a_{i2}) + u\sum_{i=1}^{s}(a_{i1} \cdot b_{i2} + b_{i1} \cdot a_{i2}) + v\sum_{i=1}^{s}(a_{i1} \cdot c_{i2} + c_{i1} \cdot a_{i2})$$
$$+uv\sum_{i=1}^{s}(a_{i1} \cdot d_{i2} + d_{i1} \cdot a_{i2} + b_{i1} \cdot c_{i2} + c_{i1} \cdot b_{i2})$$
$$= \sum_{i=1}^{s}(a_i \cdot a'_i) = \psi_m^{I'}(x) \cdot \psi_m^{I'}(y).$$

Thus if $x \cdot y = 0$, then $\psi_m^{I'}(x) \cdot \psi_m^{I'}(y) = 0$.
Since the map $\psi_m^{I'}$ is an isometry, hence the last two assertions hold. □

Proposition 3.4. *If C is a self-dual code over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$, then C contains the all uv-vector.*

Proof. A self-orthogonal vector x must have an even number of units, because for a unit a and a non-unit b, $a^2 = 1$ and $b^2 = 0$ in the ring R. Also $uv \cdot a = uv$ and $uv \cdot b = 0$ in R. This implies that x is orthogonal to the all uv-vector, and since C is self-dual, this gives that C contains the all uv-vector. □

Corollary 3.5. *Self-dual codes over the ring R of all lengths n exist.*

Corollary 3.6. *The minimum Lee weight of a self-dual $(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m})$-code C of length n does not exceed $4n$.*

Proof. Let $A = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a self-dual basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Since the map ψ preserves weight, $wt_L^A(\beta_i uv) = wt_L^A(\beta_i) + wt_L^A(\beta_i) + wt_L^A(\beta_i) + wt_L^A(\beta_i)$, for $i = 1, 2, \ldots, m$. Hence element $\beta_i(uv, uv, \ldots, uv) \in C$ has Lee weight $4n$. □

Let $m = rst(m > r > t \geq 1)$. We define the automorphism μ_r on $\mathbb{F}_{2^{rt}}^{4sn}$ as follows:
A vector $x = (x_1, x_2, \ldots, x_{4sn}) \in \mathbb{F}_{2^{rt}}^{4sn}$, can be written as $x = (X_1, X_2, \ldots, X_{4s})$ where $X_i = (x_{(i-1)n+1}, x_{(i-1)n+2}, \ldots, x_{in})$ for $i = 1, 2, \ldots, s$. Let $\mu_r(x) := (X_1, X_{s+1}, X_{2s+1}, X_{3s+1}, X_2, \ldots, X_s, X_{2s}, X_{3s}, X_{4s})$.

Proposition 3.7. *There is a commutative diagram:*

$$\begin{array}{ccc}
(\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m})^n & \xrightarrow{\psi_m^{I'}} & (\mathbb{F}_{2^{rt}} + u\mathbb{F}_{2^{rt}} + v\mathbb{F}_{2^{rt}} + uv\mathbb{F}_{2^{rt}})^{sn} \\
\Big\downarrow{\scriptstyle \psi_m} & & \Big\downarrow{\scriptstyle \mu_r \circ \psi_r} \\
F_{2^m}^{4n} & \xrightarrow{\psi_m^I} & F_{2^{rt}}^{sn}
\end{array}$$

Proof. Let $\{\beta_1, \beta_2, \ldots, \beta_s\}$ be a self-dual basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_{2^{rt}}$. If $x = \sum_{i=1}^{s} a_i\beta_i + \sum_{i=1}^{s} b_i\beta_i u + \sum_{i=1}^{s} c_i\beta_i v + \sum_{i=1}^{s} d_i\beta_i uv \in (\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m})^n$, where $a_i, b_i, c_i, d_i \in \mathbb{F}_{2^{rt}}^n$, we have

$$\psi_m^I \circ \psi_m(x) = (a_1 + b_1 + c_1 + d_1, c_1 + d_1, b_1 + d_1, d_1, \ldots, a_s + b_s + c_s + d_s, c_s + d_s, b_s + d_s, d_s) \in \mathbb{F}_{2^{rt}}^{4sn}.$$

and

$$\psi_r \circ \psi_m^{I'}(x) = (a_1 + b_1 + c_1 + d_1, \ldots, a_s + b_s + c_s + d_s, c_1 + d_1, \ldots, c_s + d_s, b_1 + d_1, \ldots, b_s + d_s, d_1, d_2, \ldots, d_s).$$

Therefore

$$\mu_r \circ \psi_r \circ \psi_m^{I'} = (a_1 + b_1 + c_1 + d_1, c_1 + d_1, b_1 + d_1, d_1, \ldots, a_s + b_s + c_s + d_s, c_s + d_s, b_s + d_s, d_s).$$

Thus

$$\mu_r \circ \psi_r \circ \psi_m^{I'} = \psi_m^I \circ \psi_m(x).$$

□

Lemma 3.8. *Let $A = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a self-dual basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Then $wt_L^A(\beta_j \sum_{i=1}^{m} x_i\beta_i) \equiv x_j$ (mod 2)*

Proof. Any $y \in \mathbb{F}_{2^m}$ can be represented as,

$$y = Tr(\beta_1 y)\beta_1 + Tr(\beta_2 y)\beta_2 + \ldots + Tr(\beta_m y)\beta_m. \quad (1)$$

Since $Tr(\beta) = Tr(\beta^2)$ for every $\beta \in \mathbb{F}_{2^m}$, it follows that $Tr(\beta_i) = 1$ for $i = 1, 2, \ldots, m$. Put $y = 1$ in equation (1) we get $\sum_{i=1}^{m} \beta_i = 1$. Since the trace function is linear and from (1) we have

$$\begin{aligned} wt_L^A(y) &\equiv Tr(\beta_1 y) + Tr(\beta_2 y) + \ldots + Tr(\beta_m y)(\text{mod } 2) \\ &\equiv Tr((\beta_1 + \beta_2 + \ldots + \beta_m)y)(\text{mod } 2) \\ &\equiv Tr(y)(\text{mod } 2) \end{aligned}$$

Since $Tr(\beta_j(\sum_i x_i\beta_i)) = x_j$ and $wt_L^A(y) \equiv Tr(y)$.

This gives us $wt_L^A(\beta_j \sum_{i=1}^{m} x_i\beta_i) \equiv x_j$ (mod 2). □

4. Conclusion

We have discussed about the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ and defined the trace function over the field $\mathbb{F}_{2^m}$ and discuss the concept of trace orthogonal basis and self-dual basis by using the Gray map to visualize some properties of the self-dual codes over the ring R. Also we discuss self-duality and Type II property of codes over the ring R and commutative property of the Gray maps over the different rings. Since the form of the generator matrix over the ring R in the standard form can not be found, so computing the mass formula in general will not be an easy problem to solve. We also discussed the relation of Lee weight and trace function over the ring R for a self-dual basis A.

References

[1] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa, and M. Oura, *Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to Hermitian modular forms*. Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, 73, Springer, (2003), 13-42.

[2] K. Betsumiya, S. Ling, and F. R. Nemenzo, *Type II codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$*. Discrete Mathematics, 275(1) (2004), 43-65.

[3] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$*. IEEE Transactions on Information Theory, 45(4) (1999), 1250-1255.

[4] J. H. Conway, V. Pless, and N. J. A. Sloane, *The binary self-dual codes of length up to 32 : a revised enumeration*. Journal of Combinatorial Theory, Series A, 60(2) (1992), 183-195.

[5] S. T. Dougherty, P. Gaborit, M. Harada, and P. Sole, *Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$*. IEEE Transactions on Information Theory, 45(1) (1999), 32-45.

[6] J. Fields, V. Pless, and J. S. Leon, *All self-dual* $\mathbb{Z}_4$ *codes of length* 15 *or less are known*. IEEE International Symposium on Information Theory, (1997), 202.

[7] P. Gaborit, *Mass formulas for self-dual codes over* $\mathbb{Z}_4$ *and* $\mathbb{F}_q + u\mathbb{F}_q$ *rings*. IEEE Transactions on Information Theory, 42(4) (1996), 122-128.

[8] W. C. Huffman, *Self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$ *with an automorphism of odd order*. Finite Fields and Their Applications, 15(3) (2009), 277-293.

[9] P. K. Kewat, B. Ghosh, and S. Pattanayak, *Cyclic codes over the ring* $\mathbb{Z}_p[u, v]/ < u^2, v^2, uv - vu >$. Finite Fields and Their Applications, 34 (2015), 161-175.

[10] S. Ling and P. Sole, *Type II codes over* $\mathbb{F}_4 + u\mathbb{F}_4$. European Journal of Combinatorics, 22(7) (2001), 983-997.

[11] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, Elsevier. 1977.

[12] C. L. Mallows and N. Sloane, *An upper bound for self-dual codes*. Information and Control, 22(2) (1973), 188-200.

[13] A. K. Singh and P. K. Kewat, *On cyclic codes over the ring* $\mathbb{Z}_p[u]/ < u^k >$. Designs, Codes and Cryptography, 74(1) (2015), 1-13.

[14] B. Yildiz and S. Karadeniz, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Designs, Codes and Cryptography, 54(1) (2010), 61-81.

[15] B. Yildiz and S. Karadeniz, *self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Journal of the Franklin Institute, 347(10) (2010), 1888-1894.

Department of Applied Mathematics, Indian Institute Of Technology(ISM), Dhanbad 826 004, India

E-mail address: ankuriitm@am.ism.ac.in