Malaysian Journal of Mathematical Sciences 14(3): 519–532 (2020)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Decomposition of Self-dual Codes Over a Commutative Non-Chain Ring

Ankur * and Kewat, P. K.

Department of Mathematics & Computing, Indian Institute of Technology (ISM), Dhanbad-826004, India

E-mail: ankuriitm@am.ism.ac.in
** Corresponding author*

Received: 23 February 2019
Accepted: 20 May 2020

ABSTRACT

We discuss the theory of the decomposition of self-dual codes over the ring $R_{u,v} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2, u^2 = 0, v^2 = 0, uv = vu$. We also discuss about the equivalence of these self-dual codes theoretically.

Keywords: Self-dual codes, gray map, decomposition of codes, equivalence of self-dual codes, automorphism group.

1. Introduction

The decomposition theory for self dual linear codes with automorphism of odd prime order over finite fields was first studied by Huffman Huffman (1982) and Yorgov Yorgov (1983). They applied the theory to the study of extremal self-dual even binary codes of lengths 40 and 48. In Huffman (1998), the theory was generalized to codes over $\mathbb{Z}_4$ and applied to study $\mathbb{Z}_4$ codes of length 24. In Huffman (2007, 2009), Huffman discussed the decomposition of self-dual linear codes with automorphism of odd prime order over the ring $R_u = \mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$, and used this decomposition to classify the Lee extremal and Lee optimal self dual codes over R_u of lengths 9 to 20. One can refer Ankur and Shum (2020), Ankur and Kumar (2020), Ankur and Kewat (2019) for more details.

In this paper, our main aim is to discuss the decomposition of self-dual codes theoretically with automorphism of odd order over the ring $R_{u,v} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2, u^2 = 0, v^2 = 0, uv = vu$. We also discuss about the automorphism groups of these codes. At the end we discuss about the equivalence of self-dual codes with automorphism of odd order over $R_{u,v}$. We get similar results as in Huffman (2007, 2009) for self dual codes over $R_{u,v}$.

As pointed out in Yildiz and Karadeniz (2010a), we can not get a generating matrix (in the standard form) for a linear code over $R_{u,v}$ of the form that we had for a linear code over a finite field and a chain ring. Therefore, the decomposition theory for self dual codes over $R_{u,v}$ may not be helpful in classifying all Lee extremal self dual codes over $R_{u,v}$. Though, it can be used to classify Lee extremal self dual codes over $R_{u,v}$ which are permutation equivalent to a certain self dual code with generator matrix in the standard form.

2. Preliminaries

Let $R_{u,v} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, $u^2 = v^2 = 0$ and $uv = vu$. Note that $R_{u,v}$ is not a chain ring, but its ideals can easily be described as

$$\begin{aligned} I_0 = \{0\} \subseteq I_{uv} = uvR_{u,v} = \{0, uv\} \subseteq I_u, I_v, I_{u+v} \subseteq I_{u,v} \subseteq I_1 = R_{u,v}, \\ \text{where } I_u = uR_{u,v} = \{0, u, uv, u + uv\}, \\ I_v = vR_{u,v} = \{0, v, uv, v + uv\}, \\ I_{u+v} = (u + v)R_{u,v} = \{0, u + v, uv, u + v + uv\}, \\ I_{u,v} = \{0, u, v, u + v, uv, u + uv, v + uv, u + v + uv\} =< u, v > . \end{aligned}$$

We note that $R_{u,v}$ has the maximal ideal $I_{u,v}$, hence $R_{u,v}$ is a local ring.

We first define an ordinary inner product $\langle \cdot, \cdot \rangle$ on $R^n_{u,v}$ as defined in Yildiz and Karadeniz (2010a) by

$$\langle x, y \rangle = \sum_{i=0}^{n} x_i y_i,$$

where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are in $R^n_{u,v}$. Dual code $C^\perp$ of C can be defined as

$$C^\perp = \{x \in R^n_{u,v} \ \mid \ \langle x, y \rangle = 0, \forall y \in C\}.$$

We say that C is self orthogonal if $C \subseteq C^\perp$ and self dual if $C = C^\perp$. Note that the length of binary self dual codes is always even, but self dual codes over $R_{u,v}$ can have odd length.

Definition 1. A linear code C over the ring $R_{u,v}$ of length n is an $R_{u,v}$ - submodule of $R^n_{u,v}$.

Definition 2. Let $\phi : (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^n \to \mathbb{F}_2^{4n}$ be the map given by

$$\phi(a + ub + vc + uvd) = (a + b + c + d, c + d, b + d, d).$$

It is easy to see that ϕ is a linear map and takes binary linear code over $R_{u,v}$ length n to a binary linear code of length $4n$.

Definition 3. For an element $a_1 + ub_1 + vc_1 + uvd_1 \in R_{u,v}$, we define the Lee weight-w_L as $w_L(a_1+ub_1+vc_1+uvd_1) = w_H(a_1+b_1+c_1+d_1, c_1+d_1, b_1+d_1, d_1)$, where w_H is the Hamming weight for binary codes.

In the ring $R_{u,v}$, we have four elements $(1, 1+u, 1+v, 1+u+v+uv)$ of weight 1, six elements $(u, v, u+v, u+uv, v+uv, u+v+uv)$ of Lee weight 2, four elements $(1+uv, 1+u+uv, 1+v+uv, 1+u+v)$ of weight 3, and one element uv of Lee weight 4.

3. Code decomposition

Let $R_u = \mathbb{F}_2 + u\mathbb{F}_2, u^2 = 0$ and $R_{u,v} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2, u^2 = 0, v^2 = 0, uv = vu$. We can write $R_{u,v} = R_u + vR_u$ We extend the code decomposition over R_u from Huffman (2007) to codes over $R_{u,v}$. Suppose $q(X) \in \mathbb{F}_2[X]$, where X is an indeterminate. Let $(q(X))$ be a principal ideal of $R_u[X]$ generated by $q(X)$ and $[q(X)]$ be a principal ideal of $R_{u,v}[X]$ generated by $q(X)$. We have the following.

Lemma 3.1. *If* $q(X) \in \mathbb{F}_2[X]$, *then* $R_{u,v}[X]/[q(X)] = R_u[X]/(q(X)) \oplus v(R_u[X])/(q(X))$.

Proof. Let $e(X) + [q(X)]$ be an element of $R_{u,v}[X]/[q(X)]$.

We can write $e(X) = g(X) + vh(X)$ uniquely with $g(X), h(X) \in R_u[X]$. An element of $[q(X)]$ has the form $q(X)(r(X) + vt(X))$ where $r(X), t(X) \in R_u[X]$.

We have $e(X) + q(X)(r(X) + vt(X)) = g(X) + vh(X) + q(X)(r(X) + vt(X)) = g(X) + q(X)r(X) + v(h(X) + q(X)t(X))$ implying $e(X) + [q(X)] = g(X) + (q(X)) + v(h(X) + (q(X)))$.

Also $R_u \cap vR_u = \{0\}$. Thus the result follows.

The above Lemma can be applied to $q(X) = X^r - 1$, where r is an odd positive integer. Let $\mathfrak{R}_r = R_{u,v}[X]/[X^r - 1]$ and $\mathcal{R}_r = R_u[X]/(X^r - 1)$.

By the above Lemma, $\mathfrak{R}_r = \mathcal{R}_r \oplus v\mathcal{R}_r$. The ring $\mathcal{R}_r$ is semisimple.

Let $X^r - 1 = \prod_{i=0}^{t} m_i(X)$, where $m_i(X)$ is irreducible over $\mathbb{F}_2$ with $m_0(X) = X - 1$.

We define $\mathcal{I}_i$ to be a principal ideal of $\frac{\mathbb{F}_2[X]}{<X^r-1>}$ generated by $(X^r - 1)/m_i(X)$.

Then $\mathcal{R}_r = (\mathcal{I}_0 + u\mathcal{I}_0) \oplus (\mathcal{I}_1 + u\mathcal{I}_1) \oplus \cdots \oplus (\mathcal{I}_t + u\mathcal{I}_t)$.

Therefore, $\mathfrak{R}_r = (\mathcal{I}_0 + u\mathcal{I}_0 + v\mathcal{I}_0 + uv\mathcal{I}_0) \oplus (\mathcal{I}_1 + u\mathcal{I}_1 + v\mathcal{I}_1 + uv\mathcal{I}_1) \oplus \cdots \oplus (\mathcal{I}_t + u\mathcal{I}_t + v\mathcal{I}_t + uv\mathcal{I}_t)$.

Let d_i be the degree of $m_i(X)$, each $\mathcal{I}_i$ is an extension field of order 2^{d_i} over $\mathbb{F}_2$.

Also $\mathcal{I}_i\mathcal{I}_j = \{0\}$ when $i \neq j$, and $\mathcal{I}_0 = \{k(1 + X + \cdots + X^{r-1}) | k \in \mathbb{F}_2\} \simeq \mathbb{F}_2$.

Define $\nu_b : \frac{\mathbb{F}_2[X]}{<X^r-1>} \longrightarrow \frac{\mathbb{F}_2[X]}{<X^r-1>}$ by $\nu_b\left(\sum_{i=0}^{r-1} c_i X^i\right) = \sum_{i=0}^{r-1} c_i X^{bi}$; note that

$\nu_b = \nu_a$ if $b \equiv a \pmod{r}$, for b to be relatively prime to r.

The map ν_b is the identity on $\mathcal{I}_0$, permutes $\mathcal{I}_1, \cdots, \mathcal{I}_t$, and if $\nu_b(\mathcal{I}_i) = \mathcal{I}_j$, ν_b is a field isomorphism of $\mathcal{I}_i$ onto $\mathcal{I}_j$.

The map ν_b can be extended to $\mathcal{R}_r$ by $\nu_b(a(X) + uc(X)) = \nu_b(a(X)) + u\nu_b(c(X))$. It is easy to see that ν_b is a ring automorphism of $\mathcal{R}_r$. The map ν_b can be extended to a ring automorphism of $\mathfrak{R}_r$ by $\nu_b(a(X)+uc(X)+vf(X)+uvg(X)) = \nu_b(a(X)) + u\nu_b(c(X)) + v\nu_b(f(X)) + uv\nu_b(g(X))$.

If $\nu_b(\mathcal{I}_i) = \mathcal{I}_j$, ν_b is a ring isomorphism of $\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i$ onto $\mathcal{I}_j + u\mathcal{I}_j + v\mathcal{I}_j + uv\mathcal{I}_j$. □

Now let C be a linear code of length n over $R_{u,v}$ with an automorphism σ of odd prime order r,
$\sigma = (1, 2, \cdots, r)(r+1, r+2, \cdots, 2r) \cdots ((c-1)r+1, (c-1)r+2, \cdots, cr)$,

σ has c cycles and $f = n - cr$ fixed points.

We use the notation $\Omega_1, \cdots, \Omega_c$ for the r-cycles and $\Omega_{c+1}, \cdots, \Omega_{c+f}$ for $f = n - cr$ fixed points of σ.

For x$\in C$, let x$|_{\Omega_i}$ denote x restricted to Ω_i.

If $1 \leq i \leq c$, y$|_{\Omega_i}$ can be viewed as an element $a_0 + a_1Y + \cdots + a_{r-1}Y^{r-1} \in \mathfrak{R}_r$.

We have y$\sigma|_{\Omega_i} = (a_0 + a_1Y + \cdots + a_{r-1}Y^{r-1})Y$.

Let $C(\sigma)$={y$\in C$ |yσ=y}, $\mathcal{J} = (\mathcal{I}_1 + u\mathcal{I}_1 + v\mathcal{I}_1 + uv\mathcal{I}_1) \oplus \cdots \oplus (\mathcal{I}_t + u\mathcal{I}_t + v\mathcal{I}_t + uv\mathcal{I}_t)$ and $\mu(\sigma)$={y$\in C$ | y$|_{\Omega_k} \in \mathcal{J}$ for $1 \leq k \leq c$ and y$|_{\Omega_k} = 0$ for $c+1 \leq k \leq c+f$}.

Also for $1 \leq i \leq t$,

let $\mu_i(\sigma)$ = {y$\in C$ | y$|_{\Omega_k} \in (\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i)$ for $1 \leq k \leq c$ and y$|_{\Omega_j} = 0$ for $c+1 \leq k \leq c+f$}.

Theorem 3.1. *Let C, $C(\sigma)$ and $\mu(\sigma)$ be as above. Then $C = C(\sigma) \oplus \mu(\sigma)$ and $\mu(\sigma) = \mu_1(\sigma) \oplus \cdots \oplus \mu_t(\sigma)$.*

Proof. Let $v \in C$ and $w = \sum\limits_{i=0}^{r-1} v\sigma^i$. Clearly $w \in C(\sigma)$.

Let $\mathrm{x} = v - (\frac{1}{r})w \in C$, we now claim x lies in $\mu(\sigma)$. If $c+1 \leq i \leq c+f$, then $w|_{\Omega_i} = rv|_{\Omega_i}$, implying that $\mathrm{x}|_{\Omega_i} = 0$ for $c+1 \leq i \leq c+f$.

If $1 \leq i \leq c$ and $v|_{\Omega_i} = \sum\limits_{j=0}^{r-1} v_{ij}Y^j$, then $w|_{\Omega_i} = a_i(1 + Y + \cdots + Y^{r-1})$,

where $a_i = \sum\limits_{j=0}^{r-1} v_{ij}$.

So $\mathrm{x}|_{\Omega_i} = \sum\limits_{j=0}^{r-1}(v_{ij} - (\frac{1}{r})a_i)Y^j$, which when divided by $Y - 1$ has remainder $\sum\limits_{j=0}^{r-1}(v_{ij} - (\frac{1}{r})a_i) = 0$.

Hence $\mathrm{x}|_{\Omega_i} \in \mathcal{J}$ and x$\in \mu(\sigma)$.

So $C = C(\sigma) + \mu(\sigma)$.

Note that if x$\in C(\sigma)$ then for $1 \leq i \leq c$, $\mathrm{x}|_{\Omega_i} \in \mathcal{I}_0 + u\mathcal{I}_0 + v\mathcal{I}_0 + uv\mathcal{I}_0$. Since $\mathcal{I}_0 + u\mathcal{I}_0 + v\mathcal{I}_0 + uv\mathcal{I}_0 \cap \mathcal{J} = \{0\}$, $C(\sigma) \cap \mu(\sigma) = \{0\}$.

Thus $C = C(\sigma) \oplus \mu(\sigma)$.

Let $e_j(Y)$ be the identity of $\mathcal{I}_j + u\mathcal{I}_j + v\mathcal{I}_j + uv\mathcal{I}_j$ and $e(x) = \sum\limits_{j=1}^{t} e_j(Y)$, which is the identity of $\mathcal{J}$.

Let $\mathrm{x} = (\mathrm{x}|_{\Omega_1}, \cdots, \mathrm{x}|_{\Omega_c}, 0, \cdots, 0) \in \mu(\sigma)$ and for $1 \leq j \leq t$, let $\mathrm{x}^j = (\mathrm{x}|_{\Omega_1} e_j(Y), \cdots, \mathrm{x}|_{\Omega_c} e_j(Y), 0, \cdots, 0)$, $x^j \in \mu_j(\sigma)$ because $\mathcal{I}_j$ is an ideal of $\mathcal{R}_r$ and $\mathcal{I}_i\mathcal{I}_j = \{0\}$ when $i \neq j$. So $\mathrm{x} = \sum\limits_{j=1}^{t} \mathrm{x}^{(j)}$ and $\mu(\sigma) = \mu_1(\sigma) + \mu_2(\sigma) + \cdots + \mu_t(\sigma)$.

Since $I_i \cap \sum\limits_{j \neq i} \mathcal{I}_j = \{0\}$. $\mu(\sigma) = \mu_1(\sigma) \oplus \mu_2(\sigma) \oplus \cdots \oplus \mu_t(\sigma)$. □

Under the correspondence $a(1 + Y + \ldots + Y^{r-1}) \leftrightarrow a$ for $a \in R_{u,v}$, it can be seen that there is an isomorphism between the ring $\mathcal{I}_0 + u\mathcal{I}_0 + v\mathcal{I}_0 + uv\mathcal{I}_0$ to $R_{u,v}$. A codeword $x \in C(\sigma)$ is constant on each r-cycle.

Hence $\mathrm{x}|_{\Omega_k} = \mathrm{x}_k(1+Y+\ldots+Y^{r-1})$,

where x_k is in $R_{u,v}$ for $1 \leq k \leq c$, and $\mathrm{x}|_{\Omega_k} = \mathrm{x}_k \in R_{u,v}$ for $c+1 \leq k \leq c+f$.

The projection of x is defined for $\mathrm{x} \in C(\sigma)$ as $\phi(\mathrm{x})= \mathrm{x}_1 \cdots \mathrm{x}_c \mathrm{x}_{c+1} \cdots \mathrm{x}_{c+f} \in (R_{u,v})^{c+f}$. Thus $\phi(C(\sigma))$ is a code over $R_{u,v}$ of length $(c+f)$. We can visualize each $\mu_i(\sigma)$ as a code of length $c+f$ over $\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i$ where the first c components are in $\mathcal{I}_i+u\mathcal{I}_i+v\mathcal{I}_i+uv\mathcal{I}_i$ and the last f components are zeros. Let $\mu_i(\sigma)^*$ denote $\mu_i(\sigma)$ punctured on the f fixed points. Considering $\mu_i(\sigma)^*$ is a code over $\mathcal{I}_i+u\mathcal{I}_i+v\mathcal{I}_i+uv\mathcal{I}_i$, of length c we define $\mu(\sigma)^* = \mu_1(\sigma)^* \oplus \ldots \oplus \mu_t(\sigma)^*$ as a code over $\mathcal{J}$ of length c. We define a bilinear form $\langle \cdot, \cdot \rangle_{\mathcal{J}}$ on $\mathcal{J}^c$ by

$$\langle x, y \rangle_{\mathcal{J}} = \sum_{i=1}^{c} x_i y_i,$$

where $\mathrm{x} = (x_1, x_2, \ldots x_c)$ and $\mathrm{y} = (y_1, y_2, \ldots y_c)$ are in $\mathcal{J}^c$. The dual code $E^{\perp}$ of a code E over $\mathcal{J}$ of length c is

$$E^{\perp} = \{\mathrm{y} \in \mathcal{J}^c \mid \langle y, z \rangle_{\mathcal{J}} = 0 \text{ for all } \mathrm{z} \in E\}.$$

A code E is self-orthogonal if $E \subseteq E^{\perp}$ and self-dual if $E = E^{\perp}$. Here we give two lemmas that help us in proving the decomposition theorem.

Lemma 3.2. *$C(\sigma)$ is self-orthogonal under $\langle \cdot, \cdot \rangle_{\mathcal{J}}$ if and only if $\phi(C(\sigma))$ is self-orthogonal under $\langle \cdot, \cdot \rangle$.*

Proof. If $p, q \in C(\sigma)$, then $p = (p_{1,0}, p_{1,1}, \ldots, p_{1,r-1}, \ldots, p_{c,0}, p_{c,1}, \ldots, p_{c,r-1}, p_{c+1}, \ldots, p_{c+f})$ and $q = (q_{1,0}, q_{1,1}, \ldots, q_{1,r-1}, \ldots, q_{c,0}, q_{c,1}, \ldots, q_{c,r-1}, q_{c+1}, \ldots, q_{c+f})$, $p_{i,j} = p_i$ and $q_{i,j} = q_i$ for some $p_i, q_i \in R_{u,v}$, for each i with $1 \leq i \leq c$.

We have $\langle p, q \rangle = r \sum\limits_{i=1}^{c} p_i q_i + \sum\limits_{i=c+1}^{c+f} p_i q_i = \sum\limits_{i=1}^{c+f} p_i q_i$ (as r is odd and $R_{u,v}$ has characteristic two).

Thus $\langle p, q \rangle = \langle \phi(p), \phi(q) \rangle$. Hence $C(\sigma)$ is self-orthogonal iff $\phi(C(\sigma))$ is self-orthogonal. □

Let λ be a permutation such that $\nu_{-1}(\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i) = (\mathcal{I}_{\lambda(i)} + u\mathcal{I}_{\lambda(i)} + v\mathcal{I}_{\lambda(i)} + uv\mathcal{I}_{\lambda(i)})$.

Since ν_{-1} is the identity on $\mathcal{I}_0$, permutes $\mathcal{I}_1, \mathcal{I}_2, \cdots, \mathcal{I}_t$. So, such a permutation exists.

Lemma 3.3. *$\mu(\sigma) \subseteq \mu(\sigma)^{\perp}$ under $\langle \cdot, \cdot \rangle$ if and only if $\mu_{\lambda(i)}(\sigma)^* \subseteq (\nu_{-1}(\mu_i(\sigma)^*))^{\perp}$ under $\langle \cdot, \cdot \rangle_{\mathcal{J}}$ for $1 \leq i \leq c$.*

Proof. First suppose $\mu(\sigma) \subseteq \mu(\sigma)^{\perp}$.

Choose a $\in \mu_{\lambda(i)}(\sigma)$ and b $\in \mu_i(\sigma)$ with associated vectors $a^* \in \mu_{\lambda(i)}(\sigma)^*$ and $b^* \in \mu_i(\sigma)^*$.

Then $\langle a\sigma^j, b \rangle = 0$ for all j with $0 \leq j \leq r-1$.

Following in a similar fashion as in Lemma 2.2 of Huffman (2007) and in Lemma 9.5 of Pless et al. (1998), we get $\langle a^*, \nu_{-1}(b)^* \rangle_{\mathcal{J}} = \sum\limits_{j=0}^{r} \langle a\sigma^j, b \rangle X^{-j}$.

Therefore, $\langle a^*, \nu_{-1}(b)^* \rangle_{\mathcal{J}} = 0$. Hence $\mu_{\lambda(i)}(\sigma)^* \subseteq (\nu_{-1}(\mu_i(\sigma)^*))^{\perp}$.

Conversely, suppose $\mu_{\lambda(i)}(\sigma)^* \subseteq (\nu_{-1}(\mu_i(\sigma)^*))^{\perp}$ for all i, with $1 \leq i \leq t$.

If $a^* \in \mu_{\lambda(i)}(\sigma)^*$ and $b^* \in \mu_i(\sigma)^*$, then $\langle a^*, \nu_{-1}(b)^* \rangle_{\mathcal{J}} = 0$.

Now consider $a^* \in \mu_{\lambda(i)}(\sigma)^*$ and $b^* \in \mu_j(\sigma)^*$ with $i \neq j$.

Since $\nu_{-1}(b)^*$ has entries in $\mathcal{I}_{\lambda(j)}$, $\langle a^*, \nu_{-1}(b)^* \rangle_{\mathcal{J}}$ is a sum of products xy with $x \in \mathcal{I}_{\lambda(i)}$, $y \in \mathcal{I}_{\lambda(j)}$.

Note that $xy \in \mathcal{I}_{\lambda(i)}\mathcal{I}_{\lambda(j)} \subseteq \mathcal{I}_{\lambda(i)} \cap \mathcal{I}_{\lambda(j)} = \{0\}$.

This implies that $\langle a^*, \nu_{-1}(b)^* \rangle_{\mathcal{J}} = 0$, for all $a^*, b^* \in \mu(\sigma)^*$.

Thus $\langle a, b \rangle = 0$ for all $a, b \in \mu(\sigma)$. Hence $\mu(\sigma) \subseteq \mu(\sigma)^{\perp}$.

□

We now prove the decomposition theorem.

Theorem 3.2. *Let C be a code over $R_{u,v}$ of length n with automorphism σ. Then the following hold.*

1. *If C is self-dual, then $\phi(C(\sigma))$ is self-dual under $\langle\cdot,\cdot\rangle$, and for $1 \leq i \leq t$, $\mu_{\lambda(i)}(\sigma)^* = (\nu_{-1}(\mu_i(\sigma)^*))^{\perp}$ under $\langle\cdot,\cdot\rangle_{\mathcal{J}}$.*

2. *Conversely, if $\phi(C(\sigma))$ is self dual under $\langle\cdot,\cdot\rangle$, and for $1 \leq i \leq t, \mu_{\lambda_i}(\sigma)^* = (\nu_{-1}(\mu_i(\sigma)^*))^{\perp}$ under $\langle\cdot,\cdot\rangle_{\mathcal{J}}$, then C is self dual.*

Proof. If C is self-dual, then by Lemma 3.3, $\phi(C(\sigma))$ is self-orthogonal.

As $\phi(C(\sigma))$ is self-orthogonal, from Lemma 2.7 of Yildiz and Karadeniz (2010b), we have

$$\begin{aligned} &\mid C \mid\mid C^{\perp} \mid=\mid R \mid^n, \\ &|\phi(C(\sigma))| \leq 4^{c+f}. \end{aligned} \tag{1}$$

As we can write $|(\nu_{-1}\mu_i(\sigma)^*)^{\perp}| = |\nu_{-1}((\mu_i(\sigma)^*))^{\perp}| = |(\mu_i(\sigma)^*)^{\perp}| = |\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i)|^c/|\mu_(\sigma)^*|$ as ν_{-1} is an isomorphism of $\mathfrak{R}_r$. Since C is self-dual, by Lemma 3.4, $\mu_{\lambda(i)}(\sigma)^* \subseteq (\nu_{-1}(\mu_i(\sigma)^*))^{\perp}$, and therefore,

$$|\mu_{\lambda(i)}(\sigma)^*| \leq \frac{|\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i)|^c}{|\mu_i(\sigma)^*|}. \tag{2}$$

First part will be done if we verify equality in equations (1) and (2) for all $1 \leq i \leq t$. Now

$$4^{cr+f} = |C| = C(\sigma)\prod_{i=1}^{t}|\mu_i(\sigma)^*|. \tag{3}$$

By using (2), $\prod\limits_{i=1}^{t}|\mu_i(\sigma)^*| = \prod\limits_{i=1}^{t}|\mu_{\lambda(i)}(\sigma)^*| \leq \prod\limits_{i=1}^{t}\frac{|\mathcal{I}_i+u\mathcal{I}_i+v\mathcal{I}_i+uv\mathcal{I}_i)|^c}{|\mu_i(\sigma)^*|}$. Note that $\prod\limits_{i=1}^{t}|\mu_i(\sigma)^*|^2 \leq \prod_{i=1}^{t}|\mathcal{I}_i+u\mathcal{I}_i+v\mathcal{I}_i+uv\mathcal{I}_i)|^c$. Thus $\prod\limits_{i=1}^{t}|\mu_i(\sigma)^*| \leq \prod_{i=1}^{t}|\mathcal{I}_i+u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i)|^{c/2}$.

Note that, $\prod_{i=1}^{t}|\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i)| = 16^{(r-1)}$.

Therefore

$$\prod_{i=1}^{t}|\mu_i(\sigma)^*| \leq (\prod_{i=1}^{t}|\mathcal{I}_i + u\mathcal{I}_i + v\mathcal{I}_i + uv\mathcal{I}_i)|^{c/2}) = 4^{(r-1)c}. \tag{4}$$

We have strict inequality in equation (4) iff we have strict inequality in equation (2) for some i. From equations (1), (3) and (4) we get $4^{cr+f} \leq 4^{c+f}4^{(r-1)c}$.

But $4^{c+f}4^{(r-1)c} = 4^{cr+f}$ and so no strict inequality in either (1) or (2) can exist. This completes the proof of first part.

For part 2 arguments of the proof of part 1 can be reversed to prove that $|C| = 4^{cr+f} = 4^n$.

By Lemma 3.3 and 3.4, $C(\sigma) \subseteq C(\sigma)^{\perp}$ and $\mu(\sigma) \subseteq \mu(\sigma)^{\perp}$. It is sufficient to show that $C(\sigma) \subseteq \mu(\sigma)^{\perp}$.

Let $r \in C(\sigma)$ and $s \in \mu(\sigma)$, we need to show that $\langle r, s\rangle = 0$.

Note that $\langle r, s\rangle = \langle r', s'\rangle$ where $r^{\star}$ and $s^{\star}$ are r and s punctured on the f fixed points as r and s are zero on these points. If we let r^* to be r' viewed as an element of $\mathcal{I}_0 + u\mathcal{I}_0 + v\mathcal{I}_0 + uv\mathcal{I}_0$ and s^* to be s' viewed as an element of $\mathcal{J}$, also

$$\sum_{i=1}^{c} r_i^* \nu_{-1}(s_i^*) = \sum_{h=0}^{r-1} < r'\sigma^h, s' > Y^{-h}. \tag{5}$$

However, $r_i^* \in \mathcal{I}_0 + u\mathcal{I}_0 + v\mathcal{I}_0 + uv\mathcal{I}_0$ and $\nu_{-1}(s_i^*) \in \mathcal{J}$. because $(\mathcal{I}_0 + u\mathcal{I}_0 + v\mathcal{I}_0 + uv\mathcal{I}_0)\mathcal{J} = \{0\}$, the left hand side of (5) is zero and therefore $\langle r'\sigma^h, s'\rangle = 0$ for all h; in particular $\langle r', s'\rangle = 0$, proving the second part. □

We adopt methods developed in Bannai et al. (2003), Huffman (2007, 2009) to discuss the equivalence of linear codes over $R_{u,v}$ of length n. It turns out that we get similar results for the equivalence of linear codes over $R_{u,v}$ as obtained in Huffman (2007, 2009) for linear codes over R_u. Suppose C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ of length n. Let $\mathcal{M}_n$ be the set of $n \times n$ invertible monomial matrices over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and S_n be the symmetric group on $\{1, 2, \cdots, n\}$ viewed either in cycle form or as matrices in $\mathcal{M}_n$. Define $\nu \in S_{4n}$ as $\nu = (1, 2)(3, 4)\cdots(4n-1, 4n)$. Let $C_H(\nu)$ denote the centralizer in H of ν, where H is a subgroup of S_{4n}.

Let M_{4n} be the set of all $4n \times 4n$ invertible monomials over the field $\mathbb{F}_2$. We denote the centralizer of ν in M_{4n} by $C_{M_{4n}}(\nu)$. We define a map $\phi\nu\phi^{-1} : \mathbb{F}_2^{4n} \to \mathbb{F}_2^{4n}$ as $(\phi\nu\phi^{-1})(x) = (\phi\nu)(\phi^{-1}(x)) = \phi((\phi^{-1}(x))\nu)$, for $\nu \in \mathcal{M}_n$ (where ϕ is defined in Definition 2). One can see that there exists a one-to-one correspondence between the centralizers of ν and $\phi\mathcal{M}_n\phi^{-1}$ We now discuss the results for the automorphism of C.

Theorem 3.3. *Let C_1 and C_2 be linear codes over $R_{u,v}$ of length n. Then two codes C_1 and C_2 are equivalent if and only if there is an element $\rho \in C_{S_{4n}}(\nu)$ such that $\phi(C_1)\rho = \phi(C_2)$.*

The automorphism group of a code C over the ring $R_{u,v}$ is defined by

$$\text{Aut(C)} = \{\nu' \in \mathcal{M}_n \mid C\nu' = C\}.$$

Theorem 3.4. *Let C be a linear code over $R_{u,v}$. Then Aut(C) $\simeq C_{Aut(\phi(C))}(\nu)$.*

Proof.

$$\begin{aligned} Aut(C) &\cong \phi(Aut(C))\phi^{-1} \\ &= \{\phi\nu'\phi^{-1} \mid \nu' \in \mathcal{M}_n, C\nu' = C\} \\ &= \{\rho \in C_{M_{4n}}(\nu) \mid \phi(C)\rho = \phi(C)\} \\ &= C_{Aut(\phi(C))}(\nu). \end{aligned}$$

□

We now discuss about the equivalence of self-dual codes over the ring $R_{u,v}$, for which we discuss the series of maps that will be used.

1. Since $\sigma = (1, 2, \cdots, r)(r+1, r+2, \cdots, 2r)\cdots((c-1)r+1, (c-1)r+2, \cdots, cr)$, let $\sigma_j = ((j-1)r+1, (j-1)r+2, \cdots, (j-1)r+r)$ for $1 \le j \le c$. Thus $\sigma = \sigma_1\sigma_2\cdots\sigma_c$. Let $\mathcal{W} = \{\sigma_1^{a_1}\sigma_2^{a_2}\cdots\sigma_c^{a_c} \mid 0 \le a_i < r, \text{for } 1 \le i \le c\}$. An action of an element of $\mathcal{W}$ to $\mathcal{C}$ cycles each of the r-cycles separately and acts on $a\mid_{\Omega_j}$ for $1 \le j \le c$ by multiplying by a power of X.

2. Define $S'_c = \{\phi' \in S_n \mid \phi \in S_c\}$ with $((a-1)r+b)\phi' = (a\phi-1)r+b$ for $1 \le a \le c$, $1 \le b \le r$, and $y\phi' = y$ for $cr+1 \le y \le cr+f$. Elements of S'_c permute the c r-cycles with the natural order in each r-cycle. So an element of S'_c permutes the r-cycle components of codewords in either $\phi(C(\sigma))$ or $\mu_i(\sigma)^*$.

3. Define $S^*_f = \{\phi^* \in S_n \mid \phi \in S_f\}$ where $y\phi^* = y$ for $1 \le y \le cr$ and $(cr+a)\phi^* = a\phi$ for $1 \le a \le f$. An element of S^*_f fixes the elements of $C(\sigma)$ and will act trivially on $\mu_i(\sigma)^*$.

4. Let $D = \{diag(j_1, j_2, \cdots, j_n) \mid j_i \in R_{u,v}$ for $1 \leq i \leq n$ with $j_{(d-1)r+1} = j_{(d-1)r+2} = \cdots = j_{(d-1)r+r}$ when $1 \leq d \leq c\}$. When elements of D applied on the code $\mathcal{C}$ scales each coordinate on each r-cycle with a constant scalar.

5. For any integer j, let $j_r \equiv j$ (mod r) where $0 \leq j_r \leq r$. For $1 \leq k < r$,define s_k to be the permutation in S_n given by $((a-1)r+1+g)s_k = (a-1)r+1+(gk)_r$ for $1 \leq a \leq c$, $0 \leq g < r$, and $js_k = j$ for $cr+1 \leq j \leq cr+f$. After applying s_k to $\mathcal{C}$ it replace Y by Y^k in each r-cycle, which is nothing but applying ν_k to each r-cycle. Let $G = \{s_k \mid 1 \leq k < r\}$.

6. Define the normalizer $\mathcal{N}$ of σ in $\mathcal{M}_n$ by $\mathcal{N} = \{N \in \mathcal{M}_n \mid N^{-1} < \sigma > N =< \sigma >\}$, where $< \sigma >$ is the cyclic group generated by σ.

Theorem 3.5. *Let C and C^1 be codes over $R_{u,v}$ both having σ in their automorphism groups. Suppose that σ is a Sylow r-subgroup of Aut(C). Then C and C^1 are equivalent if and only if $C^1 = CM$ for some $M \in \mathcal{N}$. Furthermore, $\mathcal{N} = \mathcal{W}S_c'S_f^*DG$.*

Proof. Assume $C^1 = CM$ for some $M \in \mathcal{N}$, then C and C^1 are equivalent. Conversely assume $CR = C^1$ for some $R \in \mathcal{M}_n$. Then R Aut(C^1) $R^{-1} =$ Aut(C), and therefore $< \sigma >$ and $R < \sigma > R^{-1}$ are both Sylow r-subgroups of Aut(C). By Sylow's theorem, there exists $U \in$ Aut(C) such that $UR < \sigma > R^{-1}U^{-1} =< \sigma >$. Hence $M = UR \in \mathcal{N}$ and $CM = CUR = CR = C^1$, this proves the converse part.

Next to prove $\mathcal{N} = \mathcal{W}S_c'S_f^*DG$. First we prove $\mathcal{W}S_c'S_f^*DG \subseteq \mathcal{N}$. If $B \in \mathcal{W}S_c'S_f^*D$, $B^{-1}\sigma B = \sigma$. Also $s_k^{-1}\sigma s_k = \sigma^k$. Thus $B \in \mathcal{N}$. Hence $\mathcal{W}S_c'S_f^*DG \subseteq \mathcal{N}$. Now we prove $\mathcal{N} \subseteq \mathcal{W}S_c'S_f^*DG$. Let $M \in \mathcal{N}$, then $M^{-1}\sigma M = \sigma^k$ for some $1 \leq k < r$ implying that $M^{-1}\sigma M = s_k^{-1}\sigma s_k$. Let $R = Ms_k^{-1}$. Then $R^{-1}\sigma R = \sigma$. Since $R = PV$ for P to be a permutation matrix and V a diagonal matrix, $V^{-1}P^{-1}\sigma PV = \sigma$ gives $P^{-1}\sigma P = V\sigma V^{-1}$. However, $P^{-1}\sigma P$ is a permutation matrix and $V\sigma V^{-1}$ is a monomial matrix with the cycle structure same as σ. Hence we have $P^{-1}\sigma P = \sigma$ implies that P permutes the r-cycles of σ among themselves and permutes the fixed points of σ among themselves and $V\sigma V^{-1} = \sigma$ implies $V \in D$. Hence there exist $E \in S_f^*$ and $F \in S_c'$ such that $W = PE^{-1}F^{-1}$ fixes each fixed point as well as each r-cycle of σ. However E, F, and P commute with σ, therefore W commutes with σ. Thus $W \in \mathcal{W}$. But $M = Tg_b = PVg_b = WFEVg_b \in \mathcal{W}S_c'S_f^*DG$. □

Theorem 3.6. *Let C_1 and C_2 be codes over $R_{u,v}$ with σ in their automorphism groups. Suppose that $C_1 = C_1(\sigma) \oplus \mu_1(\sigma) \oplus \cdots \oplus \mu_t(\sigma)$ and $C_2 = C_2(\sigma) \oplus \mu'_1(\sigma) \oplus \cdots \oplus \mu'_t(\sigma)$ are the decompositions of C_1 and C_2. Let $M \in \mathcal{W}S'_c S^*_f DG$ where $C_2 = C_1M$. Then $C_2(\sigma) = C_1(\sigma)M$ and $\mu'_{\lambda(i)}(\sigma) = \mu_i(\sigma)M$ for some permutation λ of $1, 2, \cdots, t$.*

Proof. The theorem is clear from the points (1) to (5). □

4. Conclusion

We consider a Gray map to discuss the theory of the decomposition of self-dual codes over the ring $R_{u,v}$, but as we discussed finding a generator matrix in the standard form over the ring $R_{u,v}$ is not possible, as we found over the field or over the ring $\mathbb{F}_2 + u\mathbb{F}_2$. So the decomposition theory for the self-dual codes over the ring $R_{u,v}$ cannot be used to construct Lee extremal self-dual codes, but one can construct permutation equivalent matrix in the standard form to find Lee extremal self-dual codes.

References

Ankur and Kewat, P. K. (2019). Type I and Type II codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Asian-European Journal of Mathematics*, 12(02):1950025. https://doi.org/10.1142/S1793557119500256.

Ankur and Kumar, R. (2020). Type I and type II codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$. *ARS Combinatoria (Accepted).*

Ankur and Shum, K. P. (2020). Theta series and weight enumerator over an imaginary quadratic field. *Asian-European Journal of Mathematics*, page 2150098. https://doi.org/10.1142/S1793557121500984.

Bannai, E., Harada, M., Ibukiyama, T., Munemasa, A., and Oura, M. (2003). Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to hermitian modular forms. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 73(1):13–42. https://doi.org/10.1007/BF02941267.

Huffman, W. (1982). Automorphisms of codes with applications to extremal doubly even codes of length 48. *IEEE Transactions on Information Theory*, 28(3):511–521.

Huffman, W. C. (1998). Decompositions and extremal type II codes over $\mathbb{Z}_4$. *IEEE Transactions on Information Theory*, 44(2):800–809.

Huffman, W. C. (2007). On the decomposition of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ with an automorphism of odd prime order. *Finite Fields and their Applications*, 13(3):681–712.

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

Pless, V., Brualdi, R. A., and Huffman, W. C. (1998). *Handbook of coding theory*. New York: Elsevier Science Inc.

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

Yildiz, B. and Karadeniz, S. (2010b). 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):1888–1894.

Yorgov, V. (1983). Binary self-dual codes with automorphisms of odd order. *Problems Inform. Transmission*, 19(4):260–270.