Journal of Universal Mathematics
Vol.2 No.2 pp.127-136 (2019)
ISSN-2618-5660

QUANTUM CODES FROM CODES OVER THE RING $\mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m}$

MURAT GÜZELTEPE AND MUSTAFA ERÖZ

Abstract. Let i, j, k be elements of real quaternions $\mathbb{H}$. Let α, β, γ be the elements corresponding to $1+i, 1+j, 1+k$, respectively. In this study, quantum codes from classical codes over $\mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m}$ are obtained.

1. Introduction

The relationship between quantum codes and classical codes has been discussed by the authors since the first quantum error correcting codes obtained. It was shown in [1] that quantum codes can be obtained from classical self-orthogonal codes. Thms. 1-3 in [1] have been used by many researchers to establish a bridge between quantum codes and classical codes. Many researchers have utilized different finite fields and finite rings to construct quantum codes. For example, regarding Gray image of linear or cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$, some quantum codes were presented in [2]. A different method to obtain quantum error-correcting codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ was given in [3].

On the other hand, linear and cyclic codes over some special rings were defined by some researchers. In [4], codes over the ring $\mathbb{Z}_{2m} + \alpha\mathbb{Z}_{2m} + \beta\mathbb{Z}_{2m} + \gamma\mathbb{Z}_{2m}$, in [5], Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ were defined.

In this paper, we construct quantum codes via codes over the ring $\mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m}$. Some of these quantum codes are better than previous ones. We prefer the ring $\mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m}$ to the ring $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$, where $u^2 = v^2 = 0, uv = vu$ since, using a norm function, one can easily determine the minimum distance of a code.

In what follows, we consider the following:

Shortly, we take the finite field $\mathbb{F}_{2^m}$ as a field extension of $\mathbb{F}_2$ such that

$$\mathbb{F}_{2^m} = \mathbb{Z}_2[x]/(p(x))$$

where $p(x)$ is an irreducible monic polynomial in $\mathbb{Z}_2[x]$ of degree m. The Gray map ϕ from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2^m$ is defined as $\phi\left(a_0 + a_1x + \cdots + a_{m-1}x^{m-1}\right) = \left(\ a_0, \quad a_1, \quad \ldots, \quad a_{m-1}\ \right)$.

2000 *Mathematics Subject Classification.* 94B05, 94B15, 94B35, 94B60.
Key words and phrases. Block codes, Quantum codes.
This study is supported by TÜBİTAK under the project number 116F318.

For example, let $p(x) = x^3 + x + 1$ then

$$\mathbb{F}_{2^3} = \left\{a_0 + a_1 x + a_2 x^2 : \, a_0, a_1, a_2 \in \mathbb{F}_2\right\}$$

and hence we get $\phi(0) = \begin{pmatrix} 0, & 0, & 0 \end{pmatrix}$, $\phi(1) = \begin{pmatrix} 1, & 0, & 0 \end{pmatrix}$, $\phi(1+x) = \begin{pmatrix} 1, & 1, & 0 \end{pmatrix}$, etc. This Gray map can naturally be extended to $\mathbb{F}_{2^m}^n$ by applying it coordinatewise.

The Hamming weight of a vector $u \in \mathbb{F}_2^m$ is defined as the number of nonzero components and the Hamming weight of a vector $u \in \mathbb{F}_{2^m}$ is naturally defined as the number of nonzero components of $\phi(u)$ and denoted by $wt(\phi(u))$.

Definition 1.1. [6] The Hamilton Quaternion Algebra over the set of the real numbers ($\mathbb{R}$), denoted by $H(\mathbb{R})$, is the associative unital algebra given by the following representation:

i)$H(\mathbb{R})$ is the free $\mathbb{R}$ module over the symbols $1, i, j, k$, that is, $H(\mathbb{R}) = \{a_0 + a_1 i + a_2 j + a_3 k : \, a_0, a_1, a_2, a_3 \in \mathbb{R}\}$;

ii)1 is the multiplicative unit;

iii) $i^2 = j^2 = k^2 = -1$;

iv) $ij = -ji = k, \; ki = -ik = j, \; jk = -kj = i$.

From here onwards, R_{2m} denotes the ring $\mathbb{Z}_{2m} + \alpha\mathbb{Z}_{2m} + \beta\mathbb{Z}_{2m} + \gamma\mathbb{Z}_{2m}$.

2. The ring R_{2^m}

$R_{2^m} = \mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m}$ is a commutative ring. The size of this ring is 2^{4m}, that is, $|R_2^m| = 2^{4m}$. The ring R_{2^m} is a local ring. But it is not a principal ideal ring or finite chain. The ring R_2 has only one maximal ideal which is not principal. The maximal ideal is $\langle\alpha\rangle \oplus \langle\beta\rangle = \{0, 1+i, 1+j, 1+k, i+j, i+k, j+k, 1+i+j+k\}$. The ideals of the ring R_2 can be introduced by

$$\begin{gathered} \langle 0\rangle = \{0\} \subset \langle 1+i+j+k\rangle = \{0, 1+i+j+k\} \subset \langle\alpha\rangle \\ = \{0, 1+i, j+k, 1+i+j+k\}, \langle\beta\rangle, \langle\gamma\rangle \subset \langle\alpha\rangle \oplus \langle\beta\rangle \\ = \langle\alpha\rangle \oplus \langle\gamma\rangle = \langle\beta\rangle \oplus \langle\gamma\rangle \subset \langle 1\rangle = R_2. \end{gathered}$$

Note that $R_2/\langle\alpha\rangle \oplus \langle\beta\rangle$ is isomorphic to $\mathbb{F}_2$ and $\langle\alpha+\beta\rangle = \langle\gamma\rangle$.

The followings were defined in [4]:

- The conjugate of an element $q = a + b\alpha + c\beta + d\gamma$ in R_{2^m} is $\overline{q} = a + b\overline{\alpha} + c\overline{\beta} + d\overline{\gamma}$.
- $\alpha\overline{\alpha} = \beta\overline{\beta} = \gamma\overline{\gamma} = 2$.
- The norm of $q = a + b\alpha + c\beta + d\gamma$ is

$N(q) = q\overline{q} = a^2 + 2b^2 + 2c^2 + 2d^2 + 2ab + 2ac + 2ad + 2bc + 2bd + 2cd$.

The norm of a vector $u = u_t \in R_{2^m}^n$ was given by $\sum N(u_t)$.

It should be noted that if $u \in R_{2^m} - (\langle\alpha\rangle \oplus \langle\beta\rangle)$, $v \in \langle\alpha\rangle \oplus \langle\beta\rangle$ then $N(u) \in \mathbb{F}_{2^m} - \{0\}$, $N(v) = 0$.

3. A Gray map

Let $\psi_{2^m} : \mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m} \to \mathbb{F}_{2^m}^4$ by

$$\psi_{2^m}(a + b\alpha + c\beta + d\gamma) = \begin{pmatrix} b, & c, & d, & a+b+c+d. \end{pmatrix}$$

The map ψ_{2^m} can naturally be extended to $R_{2^m}^n$ by applying it coordinatewise. The Euclidean weight of a vector $u = (u_t) \in \mathbb{F}_{2^m}^n$ is given by $w(u) = \sum (u_t)^2$. For example, for $m = 2$, $p(x) = x^2 + x + 1$, then

$\mathbb{F}_4 + \alpha\mathbb{F}_4 + \beta\mathbb{F}_4 + \gamma\mathbb{F}_4 = \{a + b\alpha + c\beta + d\gamma : a, b, c, d \in F_4\}$,

$$\psi_4\left(1 + x\alpha + x^2\gamma\right) = \begin{pmatrix} x, & 0, & x^2, & 0 \end{pmatrix} = u,$$

$$\sum_{t=0}^{3} (u_t)^2 = x^2 + 0^2 + \left(x^2\right)^2 + 0^2 = x^2 + x^4 = x^2 + x = 1$$

,

$$\psi(1) = (1, 0), \quad wt((1, 0)) = 1.$$

On the other hand the norm of $1 + x\alpha + x^2\gamma = 1 + x(1 + i) + x^2(1 + k) = 1 + x + x^2 + xi + x^2k = xi + x^2k$ is calculated as

$$N(xi + x^2k) = x^2 + x^4 = 1.$$

Note $1 + x + x^2 = 0$ and $x^3 = 1$ in $\mathbb{F}_4$.

Theorem 3.1. *If u is a vector in $R_{2^m}^n$ then $N(u) = w(\psi_{2^m}(u))$ implies that $wt(N(u)) = wt(w(\psi_{2^m}(u)))$.*

Proof. Let $u = q = a_0 + a_1\alpha + a_2\beta + a_3\gamma \in R_{2^m}$, where $a_0, a_1, a_2, a_3 \in \mathbb{F}_{2^m}$. Then the norm of $N(u = q) = q\overline{q} = a_0^2 + 2a_1^2 + 2a_2^2 + 2a_3^2 + 2ab + 2ac + 2ad + 2bc + 2bd + 2bc$. On the other hand, $\psi_{2^m}(a_0 + a_1\alpha + a_2\beta + a_3\gamma) = (a_1, a_2, a_3, a_0 + a_1 + a_2 + a_3) = (u_0, u_1, u_2, u_3) = u$. Hence we get

$$\sum_{t=0}^{3} (u_t)^2 = a_1^2 + a_2^2 + a_3^2 + (a_0 + a_1 + a_2 + a_3)^2 = N(u).$$

If u is taken $(q_1, q_2, \ldots, q_n) \in R_{2^m}^n$, it is obtained that $N(u) = w(\psi_{2^m}(u))$ by applying the same method to each component.

□

The proof of the next theorem is clear from the Gray map and Thm. 1.

Theorem 3.2. *The function ψ_{2^m} is linear and bijective.*

4. Linear codes over R_{2^m}

We start to determine the ideals of the ring R_{2^m}. As for the ideal structure we can find the ideals of R_{2^m} to be listed as

$$\begin{gathered} \langle 0\rangle = \{0\} \\ \langle \alpha + \beta + \gamma\rangle = (\alpha + \beta + \gamma)R_{2^m}, \ \ |\langle \alpha + \beta + \gamma\rangle| = 2^m \\ \langle \alpha\rangle = (\alpha)R_{2^m}, \ \ |\langle \alpha\rangle| = 2^{2m} \\ \langle \beta\rangle = (\beta)R_{2^m}, \ \ |\langle \beta\rangle| = 2^{2m} \\ \langle \alpha\rangle + \langle \beta\rangle = (\alpha)R_{2^m} + (\beta)R_{2^m}, \ |\langle \alpha\rangle + \langle \beta\rangle| = 2^{3m}. \end{gathered}$$

Note that

$$R_{2^m}/(\langle \alpha\rangle + \langle \beta\rangle)$$

is isomorphic to the field $\mathbb{F}_{2^m}$ with the characteristic 2 and

$$\langle \alpha\rangle \neq \langle \beta\rangle, \langle \alpha + \beta\rangle = \langle \gamma\rangle.$$

The ideal $\langle\alpha\rangle + \langle\beta\rangle$ is a maximal ideal of R_{2^m} and R_{2^m} has only one maximal ideal. So, R_{2^m} is a local ring. It is well known from algebra that if a ring R is a local ring with maximal ideal M then an element in $R - M$ is a unit in R. Hence, we can determine the units of R_{2^m} as

$$R_{2^m}^* = R_{2^m} - (\langle\alpha\rangle + \langle\beta\rangle)\,,\ |R_{2^m}^*| = \left(2^{3m}\right)(2^m - 1)\,.$$

Definition 4.1. A linear code C of length n over the ring R_{2^m} is an $R_{2^m}-$submodule of $R_{2^m}^n$.

To classify the generators for linear codes over R_{2^m} we must determine linear independence condition of them to establish possible type for linear codes over R_{2^m}. There are six type generators for linear codes over R_{2^m} such that we determine them as $[a], [b], [c], [d], [e], [f]$. Here,

$$\begin{gathered}
[a] \in R_{2^m}^n \backslash (\langle\alpha\rangle + \langle\beta\rangle)^n \\
[b] \in (\langle\alpha\rangle + \langle\beta\rangle)^n, [b] \notin (\langle\alpha\rangle)^n, (\langle\beta\rangle)^n, (\langle\gamma\rangle)^n \\
[c] \in (\langle\alpha\rangle)^n \backslash (\langle\alpha+\beta+\gamma\rangle)^n \\
[d] \in (\langle\beta\rangle)^n \backslash (\langle\alpha+\beta+\gamma\rangle)^n \\
[e] \in (\langle\gamma\rangle)^n \backslash (\langle\alpha+\beta+\gamma\rangle)^n \\
[f] \in (\langle\alpha+\beta+\gamma\rangle)^n.
\end{gathered}$$

Theorem 4.2. *If C is a linear code over R_{2^m} then the size of the code C is $(2)^{4mk_1}(2)^{3mk_2}(2)^{2mk_3}(2)^{2mk_4}(2)^{2mk_5}(2)^{mk_6}$.*

The proof is straightforward from above generators.

Theorem 4.3. *If C is a linear code over R_{2^m} of length n, size 2^k and minimum Euclidean distance d, then $\psi(C)$ is a $[4n, k, d]-$linear code over $\mathbb{F}_{2^m}$ and $\phi(\psi(C))$ is a binary $[4mn, k, d]-$linear code over $\mathbb{F}_2$.*

Recall that the maps ψ_{2^m} and ϕ are linear and bijective. So, the proof is straightforward.

Before we give a relationship between self-dual codes over R_{2^m} and self-dual codes over $\mathbb{F}_{2^m}$ and $\mathbb{F}_2$, we must give the inner product in $R_{2^m}^n$.

We define a similar inner product in [4] such $\langle u, v\rangle = \phi\left(\sum_{t=1}^{n} u_t\overline{v_t}\right)$, where $u = (u_1, u_2, \ldots, u_n), v = (v_1, v_2, \ldots, v_n) \in R_{2^m}^n$. Recall that the ring R_{2^m} is commutative. So, $\langle u, v\rangle = \langle v, u\rangle$.

Theorem 4.4. *If C is a self-dual code of length n over R_{2^m}, then $\psi_{2^m}(C)$ is a self-dual code of length $4n$ over $\mathbb{F}_{2^m}$ and $\phi(\psi_{2^m}(C))$ is a self-dual code of length $4mn$ over $\mathbb{F}_2$.*

Proof. Let C be a self-dual code over R_{2^m} and let u, v be vectors in C. Let $u = (u_1, u_2, \ldots, u_n), v = (v_1, v_2, \ldots, v_n) \in C$, shortly $u_t = a_t + b_t\alpha + c_t\beta + d_t\gamma, v_t = a_t^{'} + b_t^{'}\alpha + c_t^{'}\beta +_t^{'} \gamma$. It is obvious that

$$\begin{aligned}
&\langle u, v\rangle = 0 \pmod{p(x)} = \sum_t (a_t + b_t\alpha + c_t\beta + d_t\gamma)\left(a_t^{'} + b_t^{'}\alpha + c_t^{'}\beta + d_t^{'}\gamma\right) \\
&= \sum_t (a_t + b_t + c_t + d_t + b_t i + c_t j + d_t k)\left(a_t^{'} + b_t^{'} + c_t^{'} + d_t^{'} + b_t^{'} i + c_t^{'} j + d_t^{'} k\right) \\
&\sum_t \left(\begin{array}{c} (a_t + b_t + c_t + d_t)\left(a_t^{'} + b_t^{'} + c_t^{'} + d_t^{'}\right) + (a_t + b_t + c_t + d_t)\left(b_t^{'} i + c_t^{'} j + d_t^{'} k\right) \\ + (b_t i + c_t j + d_t k)\left(a_t^{'} + b_t^{'} + c_t^{'} + d_t^{'}\right) + (b_t i + c_t j + d_t k)\left(b_t^{'} i + c_t^{'} j + d_t^{'} k\right) \end{array} \right)
\end{aligned}$$

On the other hand, we get

$$\begin{aligned}
&\langle \psi_{2^m}(u), \psi_{2^m}(v)\rangle = \sum_t \left(\psi_{2^m}\left(a_t+b_t\alpha+c_t\beta+d_t\gamma\right)\right)\left(\psi_{2^m}\left(a_t'+b_t'\alpha+c_t'\beta+d_t'\gamma\right)\right)\\
&= \sum_t \left(\begin{array}{cccc} b_t, & c_t, & d_t, & a_t+b_t+c_t+d_t \end{array}\right)\left(\begin{array}{cccc} b_t', & c_t', & d_t', & a_t'+b_t'+c_t'+d_t' \end{array}\right)\\
&= \sum_t b_tb_t'+c_tc_t'+c_tc_t'+(a_t+b_t+c_t+d_t)\left(a_t'+b_t'+c_t'+d_t'\right)\\
&\equiv 0 \pmod{p(x)}
\end{aligned}$$

Thus we get that $\psi_{2^m}(C)$ is a self-orthogonal code over $\mathbb{F}_{2^m}$ and $|\psi_{2^m}(C)| = |C| = 2^{2mn}$ since C is a self-dual code. So, $\psi_{2^m}(C)$ is a self-dual code of length $4n$ over $\mathbb{F}_{2^m}$. Using the same way, it can be seen that $\phi(\psi_{2^m}(C))$ is self-dual.

□

Theorem 4.5. *Let $C_1,\ldots,C_6$ are linear codes over $\mathbb{F}_{2^m}$ such that $C_i\cap C_j=\{0\}$, for $i\neq j$. Let C be a linear code over R_{2^m} and let M be the maximal ideal of R_{2^m}. Then C is expressed as*

$$C=(R_{2^m}\backslash M)\,C_1\oplus(\langle\alpha\rangle+\langle\beta\rangle)\,C_2\oplus(\langle\alpha\rangle)\,C_3\oplus(\langle\beta\rangle)\,C_4\oplus(\langle\gamma\rangle)\,C_5\oplus(\langle\alpha+\beta+\gamma\rangle)\,C_6$$

with the size $|C|=2^{4mk_1+3mk_2+2mk_3+2mk_4+2mk_5+mk_6}$ if and only if $C_1,\ldots,C_6$ are linear codes over $\mathbb{F}_{2^m}$, where $k_1,\ldots,k_6$ denote the dimensions of $C_1,\ldots,C_6$, respectively. Moreover, if C is a self-orthogonal code then $\psi_{2^m}(C)$ is a self-orthogonal code.

The proof is straightforward from the definition of the ideals of R_{2^m} and Thm. 5.

The proof of next theorem is clear from Thms. 5,6.

Theorem 4.6. *Let*

$$C=(R_{2^m}\backslash M)\,C_1\oplus(\langle\alpha\rangle+\langle\beta\rangle)\,C_2\oplus(\langle\alpha\rangle)\,C_3\oplus(\langle\beta\rangle)\,C_4\oplus(\langle\gamma\rangle)\,C_5\oplus(\langle\alpha+\beta+\gamma\rangle)\,C_6$$

be a linear code over R_{2^m} under the conditions above theorem and let

$$C_i\subseteq C_{i-j}^{\perp}, i=6,5,4,3,2, j=1,2,3,4,5.$$

If $C_1,\ldots,C_6$ are self-orthogonal codes then C and $\psi_{2^m}(C)$ is a self-orthogonal code over R_{2^m}.

Example 4.7. We give this example to obtain self-dual, self-orthogonal and quantum code parameters using some classical codes over R_{2^m}.

Case 1. $m=1$, $n=1$. In this case, under the conditions of Thm.6 and Thm.7 we can take the classical code $C=\left\langle\left(\begin{array}{c} 0 \end{array}\right)\right\rangle$.

Note we can change 0 with an element in the same ideal with the norm of that element is 0. Let C be a linear code generated by the generator matrix $G=(0)$. Then we can change 0 with α, β or $\alpha+\beta+\gamma$. So, we can take the generator matrix as, for example, $G=(\alpha+\beta+\gamma)$.

- Let $G=(\alpha+\beta+\gamma)$. If we take $C_6=C$, in Thm.7, then we get a self-orthogonal code with parameters $[4,1,4]$, and corresponding quantum code $[[4,2,2]]$.
- Let $G=(\gamma)$. If we take $C_5=C$ then we get a self-dual code with parameters $[4,2,2]$, and corresponding quantum code $[[4,0,2]]$.

Case 2. $m = 1$, $n = 2$. Note we will no more take $G = (0, 0)$ since it gives us a trivial self-orthogonal code.

In this case, under the conditions of Thm.6 and Thm.7 we can take the classical code $C = \langle (\ 1, \quad 1\ ) \rangle$.

- If we take $C_6 = C$ then we get a self-orthogonal code with parameters $[8, 1, 8]$, and corresponding quantum code $[[8, 6, 2]]$.
- If we take $C_5 = C$ then we get a self-orthogonal code with parameters $[8, 2, 4]$, and corresponding quantum code $[[8, 4, 2]]$.
- If we take $C_2 = C$ then we get a self-orthogonal code with parameters $[8, 3, 4]$, and corresponding quantum code $[[8, 2, 2]]$.
- If we take $C_1 = C$ and change one of the component 1 with $1 + \alpha + \beta + \gamma$ then we get a self-dual code with parameters $[8, 4, 4]$, and corresponding quantum code $[[8, 0, 4]]$.

Thereafter, we give only special codes for some cases to understand the construction.

Example 4.8. Let $m = 2$, $n = 2$. Let $F_4 = \{0, 1, w, w^2\}$, where $w^2 + w + 1 = 0, w^3 = 1$. In this case, under the conditions of Thm.6 and Thm.7 we can take the classical a code C with a generator matrix

$$G = \begin{pmatrix} 1 & w & w^2 & 0 \\ 0 & w & 1 & w^2 \end{pmatrix}.$$

Using this generator matrix G we can easily write a generator matric for a self-dual code $C^{'}$ over R_4 such that

$$C^{'} = \left\langle \begin{pmatrix} 1 & w(1+\alpha+\beta+\gamma) & w^2(1+\alpha) & w(\alpha+\beta) \\ \alpha+\beta & w(1+\alpha+\beta+\gamma) & 1+\alpha & w^2 \end{pmatrix} \right\rangle.$$

Here, we changed the component w with $w(1 + \alpha + \beta + \gamma)$, changed w^2 with $w^2(1 + \alpha)$, changed 0 with $w(\alpha + \beta)$ since the norm of w is equal to the norm of $w(1 + \alpha + \beta + \gamma)$ and apply the same argument the other components.

Theorem 4.9. *If C is a binary self-dual code with parameters $[n, \frac{n}{2}, d]$ then there exists a binary self-dual code with parameters $[4mn, 2mn, \geq 2d]$. Hence there exists a quantum code with parameters $[[4mn, 0, \geq 2d]]$.*

Proof. Let us assume that C be a binary self-dual code with generator matrix G. Using above method and taking $C_1 = C$, we get a self-dual code over the ring R_{2^m} with parameters $[4mn, 2mn, \geq 2d]$. Using the function ψ and ϕ, the intended is obtained.

□

Example 4.10. Let C be the well known binary code $[2, 1, 2]$ with the generator matrix $G = (1, 1)$. If we take the generator matrix $G^{'} = (1,\ 1 + \alpha + \beta + \gamma)$ for a code $C^{'}$, then we get a quantum code with parameters $[[8, 0, 4]]$.

Example 4.11. Let C be the binary self-dual code with parameters $[6, 3, 2]$. The generator matrix G of C is

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

It is clear that the minimum weight of this code is 2. Using the generator matrix G, we now construct a self-dual code. Take $k_1 = k = 3$ and $C_1 = C$ in Thm.6. The first row of G is $(1, 0, 0, 1, 0, 0)$. So, we can use two elements from the set $R_2 - M$ and can use four elements from the set $\langle\alpha\rangle \oplus \langle\beta\rangle$ since there are two reversible elements in the first row of G. The same manner holds for the other rows. Hence we get a generator matrix of a code $C^{'}$ over R_2 such as

$$G^{'} = \begin{pmatrix} 1 & 0 & 0 & 1+\alpha+\beta+\gamma & \beta & \alpha+\beta \\ 0 & 1 & 0 & \beta & 1+\beta+\gamma & \beta+\gamma \\ 0 & 0 & 1 & \alpha+\beta & \beta+\gamma & 1+\alpha+\gamma \end{pmatrix}.$$

This code with parameters $[6, 3, 8]$ is a self-dual code over R_2. The image under the function ψ, that is $\psi(C^{'})$, is also a binary self-dual code with parameters $[24, 12, 8]$. This binary self-dual code $[24, 12, 8]$ is an extremal self-dual code since $8 = 4\left\lfloor\frac{24}{24}\right\rfloor + 4$.

Notice that we obtain a binary self-dual code whose minimum distance is 8 via a binary self-dual code whose minimum distance is 2.

How can we determine the generator matrix $G^{'}$ of the code $C^{'}$ over $\mathbb{F}_{2^m}$ using the generator matrix G of the code C over R_{2^m}? Note here that $C^{'} = \psi(C)$.

Let

$$G = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}_{k\times n}, \qquad \begin{array}{llllll} u_1 = & (u_{11}, & u_{12}, & \ldots, & u_{1n}) \\ u_2 = & (u_{21}, & u_{22}, & \ldots, & u_{2n}) \\ & & \vdots & & \\ u_k = & (u_{k1}, & u_{k2}, & \ldots, & u_{kn}) \end{array},$$

where $u_{ij} \in R_{2^m}$. To obtain the generator matrix $G^{'}$, we first write the following matrix A;

$$A = \begin{pmatrix} u_1 \\ (1+\alpha)\,u_1 \\ (1+\beta)\,u_1 \\ (1+\gamma)\,u_1 \\ u_2 \\ (1+\alpha)\,u_2 \\ \vdots \\ u_k \\ (1+\alpha)\,u_k \\ (1+\beta)\,u_k \\ (1+\gamma)\,u_k \end{pmatrix}_{4k\times n}.$$

Then the generator matrix $G^{'}$ is

$$G^{'} = \begin{pmatrix} \psi(u_1) \\ \psi((1+\alpha)\,u_1) \\ \vdots \\ \psi((1+\gamma)\,u_k) \end{pmatrix}_{4k\times 4n},$$

where $\psi(u_1) = (\psi(u_{11}), \psi(u_{12}), \ldots, \psi(u_{1k}))$ and so on.

Let us assume that the matrix $G^{''}$ is the standard form matrix of $G^{'}$ such that

$$G^{''} = \psi(A) = \begin{pmatrix} \begin{pmatrix} u_1^{'} \end{pmatrix} \\ \begin{pmatrix} u_2^{'} \end{pmatrix} \\ \vdots \\ \begin{pmatrix} u_{4k}^{'} \end{pmatrix} \end{pmatrix}_{4k \times 4n},$$

Let $1, w, ..., w^{m-1}$ be the elements of the finite field $\mathbb{F}_{2^m}$. We can define a matrix B as

$$B = \begin{pmatrix} u_1^{'} \\ w\begin{pmatrix} u_1^{'} \end{pmatrix} \\ w^2\begin{pmatrix} u_1^{'} \end{pmatrix} \\ \vdots \\ w^{m-1}\begin{pmatrix} u_1^{'} \end{pmatrix} \\ \begin{pmatrix} u_2^{'} \end{pmatrix} \\ w\begin{pmatrix} u_2^{'} \end{pmatrix} \\ \vdots \\ w^{m-1}\begin{pmatrix} u_{4k}^{'} \end{pmatrix} \end{pmatrix}_{4km \times 4n}.$$

Hence, $\phi(B)$ gives us the generator matrix of a linear binary code. The dimension of the matrix $\phi(B)$ is $4km \times 4nm$.

Example 4.12. Let $m = 2$, $n = 2$. Let $F_4 = \{0, 1, w, w^2\}$, where $w^2 + w + 1 = 0, w^3 = 1$. Let the generator matrix G of a code $C^{'}$ over R_4 be

$$\begin{aligned} G &= \begin{pmatrix} 1 & \alpha+\lambda & 1+\alpha+\beta & w(\alpha+\beta) \\ \alpha+\lambda & 1+\alpha+\beta+\gamma & w(\alpha+\beta) & 1+\alpha+\beta \end{pmatrix} \\ &= \begin{pmatrix} 1 & i+k & 1+i+j & w(i+j) \\ i+k & i+j+k & w(i+j) & 1+i+j \end{pmatrix}. \end{aligned}$$

Then the matrix A is

$$A = \begin{pmatrix} 1 & i+k & 1+i+j & w(i+j) \\ i & 1+j & 1+i+k & w(1+k) \\ j & i+k & 1+j+k & w(1+k) \\ k & 1+j & i+j+k & w(i+j) \\ i+k & i+j+k & w(i+j) & 1+i+j \\ 1+j & 1+j+k & w(1+k) & 1+i+k \\ i+k & 1+i+k & w(1+k) & 1+j+k \\ 1+j & 1+i+j & w(i+j) & i+j+k \end{pmatrix}.$$

Hence the generator matrix $G^{'}$ is

$$G^{'} = \psi(A) = \begin{pmatrix} 0&0&0&1&1&0&1&0&1&1&0&1&w&w&0&0 \\ 1&0&0&0&0&1&0&1&1&0&1&1&0&0&w&w \\ 0&1&0&0&1&0&1&0&0&1&1&1&0&0&w&w \\ 0&0&1&0&0&1&0&1&1&1&1&0&w&w&0&0 \\ 1&0&1&0&1&1&1&0&w&w&0&0&1&1&0&1 \\ 0&1&0&1&0&1&1&1&0&0&w&w&1&0&1&1 \\ 1&0&1&0&1&0&1&1&0&0&w&w&0&1&1&1 \\ 0&1&0&1&1&1&0&1&w&w&0&0&1&1&1&0 \end{pmatrix}.$$

The standard form matrix $G^{''}$ of $G^{'}$ is

$$G^{''} = \begin{pmatrix} 1&0&0&0&0&0&0&0&w^2&w&w^2&w^2&1&0&w^2&w \\ 0&1&0&0&0&0&0&0&w&w^2&w^2&w^2&0&1&w&w^2 \\ 0&0&1&0&0&0&0&0&w^2&w^2&w^2&w&w^2&w&1&0 \\ 0&0&0&1&0&0&0&0&w^2&w^2&w&w^2&w&w^2&0&1 \\ 0&0&0&0&1&0&0&0&1&0&w^2&w&w&w^2&w&w \\ 0&0&0&0&0&1&0&0&0&1&w&w^2&w^2&w&w&w \\ 0&0&0&0&0&0&1&0&w^2&w&1&0&w&w&w&w^2 \\ 0&0&0&0&0&0&0&1&w&w^2&0&1&w&w&w^2&w \end{pmatrix}.$$

The code $C^{''}$ with the generator matrix $G^{''}$ is a [16,8,6] self dual code over $GF(4)$. Consequently, we obtain the matrix $\phi(B)$ as

$$\phi(B) = \begin{pmatrix} 1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,1,1,1,1,1,0,0,0,1,1,0,1 \\ 0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1,0,1,0,0,1,0,0,1,0,1,1 \\ 0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,0,0,1,0,0,1,1,1,1 \\ 0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,1,0,1,0,0,0,0,1,1,1,1,0 \\ 0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,0,1,1,1,0,1,1,0,0,0 \\ 0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1,1,1,0,1,1,0,1,0,0 \\ 0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,1,1,1,1,0,1,1,1,0,1,1,1,0,0,1,0 \\ 0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1,0,1,1,1,0,1,1,1,0,0,0,0,1 \\ 0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,1,1,0,1,0,1,1,1,0,1,0,1 \\ 0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1,0,1,1,1,1,1,0,1,1,1,1,1 \\ 0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,0,1,0,0,1,1,1,1,0,1,0,1,0,1,0 \\ 0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1,1,1,1,0,1,0,1,1,1,1,1,1,1,1 \\ 0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,1,0,1,1,0,0,0,0,1,0,1,0,1,1,1 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,1,0,1,0,0,1,1,1,1,1,1,1,0 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,1,1,0,0,1,0,0,1,0,1,1,1,0,1 \\ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,0,0,0,0,1,1,1,1,1,1,0,1,1 \end{pmatrix}$$

Using this classical code with generator matrix $\phi(B)$, we obtain $[[32,0,6]]$ quantum code over $\mathbb{F}_2$.

5. Conclusion

In this paper, we obtain new classes of quantum codes from classical codes over the ring R_{2^m}. To obtain these quantum codes, we define a Gray map from R_{2^m} to $\mathbb{F}_{2^m}^4$. Also, we study on the algebraic structure of the ring R_{2^m}. We characterize cyclic, self-dual and self-orthogonal codes over this ring.

References

[1] Calderbank A. R., Rains, E. M., Shor, P. W., Sloane, N. J. A., "Quantum error correction via codes over $GF(4)$", IEEE Trans. Inform. Theory, vol. 44, pp. 1369- 1387, 1998.

[2] Kai X., Zhu S., "Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4+u\mathbb{F}_4$", Int. Journal of Quantum Inf., vol. 9, no. 2, pp. 689-700, 2011.

[3] Qian J., "Quantum Codes from Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$", Journal of Information and Computational Science, vol. 10, no. 6, pp. 1715-1722, 2013.

[4] YoungJu Choie, Steven T. Dougherty, "Codes over Σ_{2m} and Jacobi forms over Quaternions", AAECC, vol. 15, pp. 129-147, 2004.

[5] Yildiz B., Karadeniz S., "Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", Des. Codes Cryptogr., vol. 58, pp. 221234, 2011. (DOI: 10.1007/s10623-010-9399-3)

[6] Davidoff, G., Sarnak, P., Valette, A., *Elementary number theory, group theory, and Ramanujan graphs*, Cambridge University Press, 2003.

Department of Mathematics, Sakarya University, 54187, Sakarya, Türkiye
Email address: mguzeltepe@sakarya.edu.tr

Email address: meroz@sakarya.edu.tr