# Quantum Codes Over $F_{2}+u F_{2}+v F_{2}$ 

Abdullah Dertli, Yasemin Cengellenmis and Senol Eren<br>Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 94B05; Secondary 94B15.
Keywords and phrases: Cyclic codes, quantum codes, finite rings.
Abstract In this paper, it was constructed quantum codes from cyclic codes over finite ring $S=F_{2}+u F_{2}+v F_{2}, u^{2}=u, v^{2}=v, u v=v u=0$ for arbitrary length $n$. It was given a new Gray map $\Psi$ which is both an isometry and weight preserving map. It was shown that $C$ is self orthogonal codes over $S$, so is $\Psi(C)$. It was given a necessary and sufficient condition for cyclic codes over $S$ that contains its dual and it was determined the parameters of quantum codes which are obtained from cyclic codes over $S$.

## 1 Introduction

Although the theory quantum error correcting codes has striking differences from the theory classical error correcting codes, Calderbank et al. gave a way to construct quantum error correcting codes from classical error correcting codes in [3].

Many good quantum codes have been constructed by using classical cyclic codes over $F_{q}$ with self orthogonal (or dual containing) properties.

Some authors constructed quantum codes by using linear codes over finite rings. For example, in [5], J. Qian et al. gave a new method to obtain self-orthogonal codes over $F_{2}$. They gave a construction for quantum error correcting codes starting from cyclic codes over finite ring, $F_{2}+u F_{2}, u^{2}=0$. X. Kai, S. Zhu gave construction for quantum codes from linear and cyclic codes over $F_{4}+u F_{4}, u^{2}=0$ in [6]. They derived Hermitian self-orthogonal codes over $F_{4}$ as Gray images of linear and cyclic codes over $F_{4}+u F_{4}$. In [7], X. Yin and W. Ma gave an existence condition of quantum codes which are derived from cyclic codes over finite ring $F_{2}+u F_{2}+u^{2} F_{2}$, $u^{3}=0$ with Lee metric. J. Qian gave a new method of constructing quantum error correcting codes from cyclic codes over finite ring $F_{2}+v F_{2}, v^{2}=v$, for arbitrary length $n$ in [4]. A. Dertli et al. gave quantum codes over the finite ring in $[1,2]$.

This paper is organized as follows. In section 2, we give some basic knowledges about the finite ring $S$, cyclic code, dual code. In section 3, we define a new Gray map from $S$ to $F_{2}^{3}$, Lee weights of elements of $S$. We show that if $C$ is self orthogonal so is $\Psi(C)$. In section 4, a necessary and sufficient condition for cyclic code over $S$ that contains its dual is given. The parameters of quantum error correcting codes are obtained from cyclic codes over $S$. In section 5, we give some examples.

## 2 Preliminaries

Let $S$ be the ring $F_{2}+u F_{2}+v F_{2}$ where $u^{2}=u, v^{2}=v, u v=v u=0$ and $F_{2}=\{0,1\}$ a finite commutative ring with 8 elements. $S$ is semi local ring with three maximal ideals and a principal ideal ring. It is not finite chain ring. Let $w=1+u+v$. Addition and multiplication over $S$ are given in the following tables:

| + | 0 | 1 | $u$ | $v$ | $1+u$ | $1+v$ | $u+v$ | $w$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 0 | 0 | 1 | $u$ | $v$ | $1+u$ | $1+v$ | $u+v$ | $w$ |
| 1 | 1 | 0 | $1+u$ | $1+v$ | $u$ | $v$ | $w$ | $u+v$ |
| $u$ | $u$ | $1+u$ | 0 | $u+v$ | 1 | $w$ | $v$ | $1+v$ |
| $v$ | $v$ | $1+v$ | $u+v$ | 0 | $w$ | 1 | $u$ | $1+u$ |
| $1+u$ | $1+u$ | $u$ | 1 | $w$ | 0 | $u+v$ | $1+v$ | $v$ |
| $1+v$ | $1+v$ | $v$ | $w$ | 1 | $u+v$ | 0 | $1+u$ | $u$ |
| $u+v$ | $u+v$ | $w$ | $v$ | $u$ | $1+v$ | $1+u$ | 0 | 1 |
| $w$ | $w$ | $u+v$ | $1+v$ | $1+u$ | $v$ | $u$ | 1 | 0 |


| $\cdot$ | 0 | 1 | $u$ | $v$ | $1+u$ | $1+v$ | $u+v$ | $1+u+v$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $u$ | $v$ | $1+u$ | $1+v$ | $u+v$ | $w$ |
| $u$ | 0 | $u$ | $u$ | 0 | 0 | $u$ | $u$ | 0 |
| $v$ | 0 | $v$ | 0 | $v$ | $v$ | 0 | $v$ | 0 |
| $1+u$ | 0 | $1+u$ | 0 | $v$ | $1+u$ | $w$ | $v$ | $w$ |
| $1+v$ | 0 | $1+v$ | $u$ | 0 | $w$ | $1+v$ | $u$ | $w$ |
| $u+v$ | 0 | $u+v$ | $u$ | $v$ | $v$ | $u$ | $u+v$ | 0 |
| $1+u+v$ | 0 | $w$ | 0 | 0 | $w$ | $w$ | 0 | $w$ |

The ideals are follows:

$$
\begin{aligned}
I_{0} & =\{0\}, I_{1}=S \\
I_{u} & =\{0, u\}, I_{v}=\{0, v\}, I_{1+u+v}=\{0,1+u+v\} \\
I_{u+v} & =\{0, u, v, u+v\}, I_{1+u}=\{0, v, 1+u, 1+u+v\} \\
I_{1+v} & =\{0, u, 1+v, 1+u+v\}
\end{aligned}
$$

A linear code $C$ over $S$ length $n$ is a $S$-submodule of $S^{n}$. An element of $C$ is called a codeword.

For any $x=\left(x_{0}, x_{1}, \ldots, x_{n-1}\right), y=\left(y_{0}, y_{1}, \ldots, y_{n-1}\right)$ the inner product is defined as

$$
x . y=\sum_{i=0}^{n-1} x_{i} y_{i}
$$

If $x . y=0$ then $x$ and $y$ are said to be orthogonal. Let $C$ be linear code of length $n$ over $S$, the dual code of $C$

$$
C^{\perp}=\{x: \forall y \in C, x . y=0\}
$$

which is also a linear code over $S$ of length $n$. A code $C$ is self orthogonal if $C \subseteq C^{\perp}$ and self dual if $C=C^{\perp}$.

A cyclic code $C$ over $S$ is a linear code with the property that if $c=\left(c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C$ then $\sigma(C)=\left(c_{n-1}, c_{0}, \ldots, c_{n-2}\right) \in C$. A subset $C$ of $S^{n}$ is a linear cyclic code of length $n$ iff it is polynomial representation is an ideal of $S[x] /\left\langle x^{n}-1\right\rangle$.

Let $C$ be code over $F_{2}$ of length $n$ and $\dot{c}=\left(\dot{c}_{0}, \dot{c}_{1}, \ldots, \dot{c}_{n-1}\right)$ be a codeword of $C$. The Hamming weight of $\dot{c}$ is defined as $w_{H}(\dot{c})=\sum_{i=0}^{n-1} w_{H}\left(c_{i}\right)$ where $w_{H}\left(\dot{c}_{i}\right)=1$ if $\dot{c}_{i}=1$ and $w_{H}\left(\dot{c}_{i}\right)=0$ if $\dot{c}_{i}=0$. Hamming distance of $C$ is defined as $d_{H}(C)=\min d_{H}(c, \dot{c})$, where for any $c \in C, c \neq \dot{c}$ and $d_{H}(c, c)$ is Hamming distance between two codewords with $d_{H}\left(c, c^{c}\right)=w_{H}(c-c ́ c)$.

Let $a \in F_{2}^{3 n}$ with $a=\left(a_{0}, a_{1}, \ldots, a_{3 n-1}\right)=\left(a^{(0)}\left|a^{(1)}\right| a^{(2)}\right), a^{(i)} \in F_{2}^{n}$ for $i=0,1,2$. Let $\varphi$ be a map from $F_{2}^{3 n}$ to $F_{2}^{3 n}$ given by $\varphi(a)=\left(\sigma\left(a^{(0)}\right)\left|\sigma\left(a^{(1)}\right)\right| \sigma\left(a^{(2)}\right)\right)$ where $\sigma$ is a cyclic shift from $F_{2}^{n}$ to $F_{2}^{n}$ given by $\sigma\left(a^{(i)}\right)=\left(\left(a^{(i, n-1)}\right),\left(a^{(i, 0)}\right),\left(a^{(i, 1)}\right), \ldots,\left(a^{(i, n-2)}\right)\right)$ for every $a^{(i)}=\left(a^{(i, 0)}, \ldots, a^{(i, n-1)}\right)$ where $a^{(i, j)} \in F_{2}, 0 \leq j \leq n-1$. A code of length $3 n$ over $F_{2}$ is said to be quasi cyclic code of index 3 if $\varphi(C)=C$.

## 3 Gray Map And Gray Images Of Cyclic Codes Over $S$

Let $x=a+u b+u c$ be an element of $S$ where $a, b, c \in F_{2}$. We define Gray map $\Psi$ from $S$ to $F_{2}^{3}$ by

$$
\begin{aligned}
\Psi & : S \rightarrow F_{2}^{3} \\
\Psi(a+u b+v c) & =(a, a+b, a+c)
\end{aligned}
$$

The Lee weight of elements of $S$ are defined $w_{L}(a+u b+v c)=w_{H}(a, a+b, a+c)$ where $w_{H}$ denotes the ordinary Hamming weight for binary codes. Hence, there is one element whose weight is 0 , there are $u, v, 1+u+v$ elements whose weights are 1 , there are $1+u, 1+v, u+v$ elements whose weights are 2 , there is one element whose weight are 3 .

Let $C$ be a linear code over $S$ of length $n$. For any codeword $c=\left(c_{0}, \ldots, c_{n-1}\right)$ the Lee weight of $c$ is defined as $w_{L}(c)=\sum_{i=0}^{n-1} w_{L}\left(c_{i}\right)$ and the Lee distance of $C$ is defined as $d_{L}(C)=$ $\min d_{L}(c, \dot{c})$, where for any $c \in C, c \neq \dot{c}$ and $d_{L}(c, \dot{c})$ is Lee distance between two codewords with $d_{L}\left(c, c^{c}\right)=w_{L}(c-\bar{c})$. Gray map $\Psi$ can be extended to map from $S^{n}$ to $F_{2}^{3 n}$.

Theorem 3.1. The Gray map $\Psi$ is a weight preserving map from ( $S^{n}$, Lee weight) to ( $F_{2}^{3 n}$, Hamming weight). Moreover it is an isometry from $S^{n}$ to $F_{2}^{3 n}$.

Theorem 3.2. If $C$ is an $\left[n, k, d_{L}\right]$ linear codes over $S$ then $\Psi(C)$ is $a\left[3 n, k, d_{H}\right]$ linear codes over $F_{2}$, where $d_{H}=d_{L}$.

Proof. Let $x_{1}=a_{1}+u b_{1}+v c_{1}, x_{2}=a_{2}+u b_{2}+v c_{2} \in S, \alpha \in F_{2}$ then
$\Psi\left(x_{1}+x_{2}\right)=\Psi\left(a_{1}+a_{2}+u\left(b_{1}+b_{2}\right)+v\left(c_{1}+c_{2}\right)\right)$
$=\left(a_{1}+a_{2}, a_{1}+a_{2}+b_{1}+b_{2}, a_{1}+a_{2}+c_{1}+c_{2}\right)$
$=\left(a_{1}, a_{1}+b_{1}, a_{1}+c_{1}\right)+\left(a_{2}, a_{2}+b_{2}, a_{2}+c_{2}\right)$
$=\Psi\left(x_{1}\right)+\Psi\left(x_{2}\right)$
$\Psi\left(\alpha x_{1}\right)=\Psi\left(\alpha a_{1}+u \alpha b_{1}+v \alpha c_{1}\right)$
$=\left(\alpha a_{1}, \alpha a_{1}+\alpha b_{1}, \alpha a_{1}+\alpha c_{1}\right)$
$=\alpha\left(a_{1}, a_{1}+b_{1}, a_{1}+c_{1}\right)$
$=\alpha \Psi\left(x_{1}\right) \quad$ so $\Psi$ is linear. As $\Psi$ is bijective then $|C|=|\Psi(C)|$. From Theorem 3.1
we have $d_{H}=d_{L}$.
Theorem 3.3. If $C$ is self orthogonal, so is $\Psi(C)$.
Proof. Let $x_{1}=a_{1}+u b_{1}+v c_{1}, x_{2}=a_{2}+u b_{2}+v c_{2}$ where $a_{1}, b_{1}, c_{1}, a_{2}, b_{2}, c_{2} \in F_{2}$.
From $x_{1} \cdot x_{2}=a_{1} a_{2}+u\left(a_{1} b_{2}+b_{1} a_{2}+b_{1} b_{2}\right)+v\left(a_{1} c_{2}+c_{1} a_{2}+c_{1} c_{2}\right)$, if $C$ is self orthogonal,
so we have $a_{1} a_{2}=0, a_{1} b_{2}+b_{1} a_{2}+b_{1} b_{2}=0, a_{1} c_{2}+c_{1} a_{2}+c_{1} c_{2}=0$. From

$$
\Psi\left(x_{1}\right) \cdot \Psi\left(x_{2}\right)=\left(a_{1}, a_{1}+b_{1}, a_{1}+c_{1}\right)\left(a_{2}, a_{2}+b_{2}, a_{2}+c_{2}\right)
$$

$=a_{1} a_{2}+a_{1} b_{2}+b_{1} a_{2}+b_{1} b_{2}+a_{1} a_{2}+a_{1} c_{2}+c_{1} a_{2}+c_{1} c_{2}=0$ Therefore, we have
$\Psi(C)$ is self orthogonal.
Proposition 3.4. Let $\Psi$ be Gray map from $S^{n}$ to $F_{2}^{3 n}$, let $\sigma$ be cyclic shift and let $\varphi$ be a map as in the preliminaries. Then $\Psi \sigma=\varphi \Psi$.

Proposition 3.5. Let $\sigma$ and $\varphi$ be as in the preliminaries. A code $C$ of length $n$ over $S$ is cyclic code if and only if $\Psi(C)$ is quasi cyclic code of index 3 over $F_{2}$ with length $3 n$.

Proof. Similar to proof of in [8].
We denote that $A_{1} \otimes A_{2} \otimes A_{3}=\left\{\left(a_{1}, a_{2}, a_{3}\right): a_{1} \in A_{1}, a_{2} \in A_{2}, a_{3} \in A_{3}\right\}$ and $A_{1} \oplus A_{2} \oplus A_{3}=$ $\left\{a_{1}+a_{2}+a_{3}: a_{1} \in A_{1}, a_{2} \in A_{2}, a_{3} \in A_{3}\right\}$

Let $C$ be a linear code of length $n$ over $S$. Define

$$
\begin{aligned}
& C_{1}=\left\{a \in F_{2}^{n}: \exists b, c \in F_{2}^{n}, a+u b+v c \in C\right\} \\
& C_{2}=\left\{a+b \in F_{2}^{n}: \exists c \in F_{2}^{n}, a+u b+v c \in C\right\} \\
& C_{3}=\left\{a+c \in F_{2}^{n}: \exists b \in F_{2}^{n}, a+u b+v c \in C\right\}
\end{aligned}
$$

Then $C_{1}, C_{2}$ and $C_{3}$ are binary linear codes of length $n$. Moreover, the linear code $C$ of length $n$ over $S$ can be uniquely expressed as $C=(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3}$.

Theorem 3.6. Let $C$ be a linear code of length $n$ over $S$. Then $\Psi(C)=C_{1} \otimes C_{2} \otimes C_{3}$ and $|C|=\left|C_{1}\right|\left|C_{2}\right|\left|C_{3}\right|$.
Proof. For any $\left(a_{0}, a_{1}, \ldots, a_{n-1}, b_{0}, b_{1}, \ldots, b_{n-1}, c_{0}, c_{1}, \ldots, c_{n-1}\right) \in \Psi(C)$. Let $r_{i}=a_{i}+u\left(a_{i}+b_{i}\right)+$ $v\left(a_{i}+c_{i}\right), i=0,1, \ldots, n-1$. Since $\Psi$ is a bijection $r=\left(r_{0}, r_{1}, \ldots, r_{n-1}\right) \in C$. By definitions of $C_{1}, C_{2}$ and $C_{3}$ we have $\left(a_{0}, a_{1}, \ldots, a_{n-1}\right) \in C_{1},\left(b_{0}, b_{1}, \ldots, b_{n-1}\right) \in C_{2},\left(c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C_{3}$. So, $\left(a_{0}, a_{1}, \ldots, a_{n-1}, b_{0}, b_{1}, \ldots, b_{n-1}, c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C_{1} \otimes C_{2} \otimes C_{3}$. That is $\Psi(C) \subseteq C_{1} \otimes C_{2} \otimes C_{3}$.

On the other hand, for any $\left(a_{0}, a_{1}, \ldots, a_{n-1}, b_{0}, b_{1}, \ldots, b_{n-1}, c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C_{1} \otimes C_{2} \otimes C_{3}$ where $\left(a_{0}, a_{1}, \ldots, a_{n-1}\right) \in C_{1},\left(b_{0}, b_{1}, \ldots, b_{n-1}\right) \in C_{2},\left(c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C_{3}$. There are $x=$ $\left(a_{0}, a_{1}, \ldots, a_{n-1}\right), y=\left(b_{0}, b_{1}, \ldots, b_{n-1}\right), z=\left(c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C$ such that $x_{i}=a_{i}+(u+v) p_{i}$, $y_{i}=b_{i}+(1+u) q_{i}, z_{i}=c_{i}+(1+v) s_{i}$ where $p_{i}, q_{i}, s_{i} \in F_{2}$ and $0 \leq i \leq n-1$. Since $C$ is linear we have $r=(1+u+v) x+(u) y+(v) z=a+u(a+b)+v(a+c) \in C$. It follows then $\Psi(r)=\left(a_{0}, a_{1}, \ldots, a_{n-1}, b_{0}, b_{1}, \ldots, b_{n-1}, c_{0}, c_{1}, \ldots, c_{n-1}\right)$, which gives $C_{1} \otimes C_{2} \otimes C_{3} \subseteq \Psi(C)$. Therefore, $\Psi(C)=C_{1} \otimes C_{2} \otimes C_{3}$. The second result is easy to verify.

Corollary 3.7. If $\Psi(C)=C_{1} \otimes C_{2} \otimes C_{3}$, then $C=(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3}$.
It is easy to see that,

$$
\begin{aligned}
|C| & =\left|C_{1}\right|\left|C_{2}\right|\left|C_{3}\right|=2^{n-\operatorname{deg}\left(f_{1}\right)} 2^{n-\operatorname{deg}\left(f_{2}\right)} 2^{n-\operatorname{deg}\left(f_{3}\right)} \\
& =2^{3 n-\left(\operatorname{deg}\left(f_{1}\right)+\operatorname{deg}\left(f_{2}\right)+\operatorname{deg}\left(f_{3}\right)\right)}
\end{aligned}
$$

where $f_{1}, f_{2}$ and $f_{3}$ are the generator polynomials of $C_{1}, C_{2}$ and $C_{3}$, respectively.
Corollary 3.8. If $G_{1}, G_{2}, G_{3}$ and $G_{4}$ are generator matrices of binary linear codes $C_{1}, C_{2}$ and $C_{3}$ respectively, then the generator matrix of $C$ is

$$
G=\left[\begin{array}{c}
(1+u+v) G_{1} \\
(u) G_{2} \\
(v) G_{3}
\end{array}\right]
$$

We have

$$
\Psi(G)=\left[\begin{array}{c}
\Psi\left((1+u+v) G_{1}\right) \\
\Psi\left((u) G_{2}\right) \\
\Psi\left((v) G_{3}\right)
\end{array}\right]=\left[\begin{array}{ccc}
G_{1} & 0 & 0 \\
0 & G_{2} & 0 \\
0 & 0 & G_{3}
\end{array}\right]
$$

Let $d_{L}$ minimum Lee weight of linear code $C$ over $S$. Then,

$$
d_{L}=d_{H}(\Psi(C))=\min \left\{d_{H}\left(C_{1}\right), d_{H}\left(C_{2}\right), d_{H}\left(C_{3}\right)\right\}
$$

where $d_{H}\left(C_{i}\right)$ denotes the minimum Hamming weights of binary codes $C_{1}, C_{2}$ and $C_{3}$, respectively.

## 4 Quantum Codes From Cyclic Codes Over $S$

Theorem 4.1. (CSS Construction) Let $C$ and $C$ be two binary codes with parameters $\left[n, k_{1}, d_{1}\right.$ ] and $\left[n, k_{2}, d_{2}\right]$, respectively. If $C^{\perp} \subseteq \mathcal{C}$, then an $\left[\left[n, k_{1}+k_{2}-n, \min \left\{d_{1}, d_{2}\right\}\right]\right]$ quantum code can be constructed. Especially, if $C^{\perp} \subseteq C$, then there exists an $\left[\left[n, 2 k_{1}-n, d_{1}\right]\right]$ quantum code.

Proposition 4.2. Let $C=(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3}$ be a linear code over $S$. Then $C$ is a cyclic code over $S$ iff $C_{1}, C_{2}$ and $C_{3}$ are binary cyclic codes.
Proof. Let $\left(a_{0}, a_{1}, \ldots, a_{n-1}\right) \in C_{1},\left(b_{0}, b_{1}, \ldots, b_{n-1}\right) \in C_{2}$ and $\left(c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C_{3}$. Assume that $m_{i}=(1+u+v) a_{i}+(u) b_{i}+(v) c_{i}$ for $i=0,1, \ldots, n-1$. Then $\left(m_{0}, m_{1}, \ldots, m_{n-1}\right) \in C$. Since $C$ is a cyclic code, it follows that $\left(m_{n-1}, m_{0}, \ldots, m_{n-2}\right) \in C$. Note that $\left(m_{n-1}, m_{0}, \ldots, m_{n-2}\right)=$ $(1+u+v)\left(a_{n-1}, a_{0}, \ldots, a_{n-2}\right)+(u)\left(b_{n-1}, b_{0}, \ldots, b_{n-2}\right)+(v)\left(c_{n-1}, c_{0}, \ldots, c_{n-2}\right)$.Hence $\left(a_{n-1}, a_{0},\right.$. ..,$\left.a_{n-2}\right) \in C_{1},\left(b_{n-1}, b_{0}, \ldots, b_{n-2}\right) \in C_{2}$ and $\left(c_{n-1}, c_{0}, \ldots, c_{n-2}\right) \in C_{3}$. Therefore, $C_{1}, C_{2}$ and $C_{3}$ cyclic codes over $F_{2}$.

Conversely, suppose that $C_{1}, C_{2}$ and $C_{3}$ cyclic codes over $F_{2}$. Let $\left(m_{0}, m_{1}, \ldots, m_{n-1}\right) \in C$ where $m_{i}=(1+u+v) a_{i}+(u) b_{i}+(v) c_{i}$ for $i=0,1, \ldots, n-1$. Then $\left(a_{0}, a_{1}, \ldots, a_{n-1}\right) \in C_{1}$, $\left(b_{0}, b_{1}, \ldots, b_{n-1}\right) \in C_{2}$ and $\left(c_{0}, c_{1}, \ldots, c_{n-1}\right) \in C_{3}$. Note that $\left(m_{n-1}, m_{0}, \ldots, m_{n-2}\right)=(1+u+$ v) $\left(a_{n-1}, a_{0}, \ldots, a_{n-2}\right)+(u)\left(b_{n-1}, b_{0}, \ldots, b_{n-2}\right)+(v)\left(c_{n-1}, c_{0}, \ldots, c_{n-2}\right) \in C=(1+u+v) C_{1} \oplus$ $(u) C_{2} \oplus(v) C_{3}$. So, $C$ is cyclic code over $S$.

Proposition 4.3. Suppose $C=(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3}$ is a cyclic code of length $n$ over S. Then

$$
C=<(1+u+v) f_{1},(u) f_{2},(v) f_{3}>
$$

and $|C|=2^{3 n-\left(\operatorname{deg} f_{1}+\operatorname{deg} f_{2}+\operatorname{deg} f_{3}\right)}$ where $f_{1}, f_{2}$ and $f_{3}$ generator polynomials of $C_{1}, C_{2}$ and $C_{3}$ respectively.

Proposition 4.4. Suppose $C$ is a cyclic code of length $n$ over $S$, then there is a unique polynomial $f(x)$ such that $C=\langle f(x)\rangle$ and $f(x) \mid x^{n}-1$ where $f(x)=(1+u+v) f_{1}(x)+(u) f_{2}(x)+$ (v) $f_{3}(x)$.

Proposition 4.5. If $C=(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3}$ is a cyclic code of length $n$ over $S$. Then

$$
C^{\perp}=\left\langle(1+u+v) h_{1}^{*}+(u) h_{2}^{*}+(v) h_{3}^{*}\right\rangle
$$

and $\left|C^{\perp}\right|=2^{\operatorname{deg} f_{1}+\operatorname{deg} f_{2}+\operatorname{deg} f_{3}}$ where for $i=1,2,3, h_{i}^{*}$ are the reciprocal polynomials of $h_{i}$ i.e., $h_{i}(x)=\left(x^{n}-1\right) / f_{i}(x), h_{i}^{*}(x)=x^{\operatorname{deg} h_{i}} h_{i}\left(x^{-1}\right)$ for $i=1,2,3$.

Lemma 4.6. A binary linear cyclic code $C$ with generator polynomial $f(x)$ contains its dual code iff

$$
x^{n}-1 \equiv 0\left(\bmod f f^{*}\right)
$$

where $f^{*}$ is the reciprocal polynomial of $f$.
Theorem 4.7. Let $C=\left\langle(1+u+v) f_{1},(u) f_{2},(v) f_{3}\right\rangle$ be a cyclic code of length $n$ over $S$. Then $C^{\perp} \subseteq C$ iff $x^{n}-1 \equiv 0\left(\bmod f_{i} f_{i}^{*}\right)$ for $i=1,2,3$.

Proof. Let $x^{n}-1 \equiv 0\left(\bmod f_{i} f_{i}^{*}\right)$ for $i=1,2,3$. Then $C_{1}^{\perp} \subseteq C_{1}, C_{2}^{\perp} \subseteq C_{2}, C_{3}^{\perp} \subseteq C_{3}$. By using $(1+u+v) C_{1}^{\perp} \subseteq(1+u+v) C_{1},(u) C_{2}^{\perp} \subseteq(u) C_{2},(v) C_{3}^{\perp} \subseteq(v) C_{3}$. We have $(1+u+v) C_{1}^{\perp} \oplus$ $(u) C_{2}^{\perp} \oplus(v) C_{3}^{\perp} \subseteq(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3} . \mathrm{So},<(1+u+v) h_{1}^{*}+(u) h_{2}^{*}+(v) h_{3}^{*}>\subseteq$ $<(1+u+v) f_{1},(u) f_{2},(v) f_{3}>$. That is $C^{\perp} \subseteq C$.

Conversely, if $C^{\perp} \subseteq C$, then $(1+u+v) C_{1}^{\perp} \oplus(u) C_{2}^{\perp} \oplus(v) C_{3}^{\perp} \subseteq(1+u+v) C_{1} \oplus(u) C_{2} \oplus$ $(v) C_{3}$. By thinking $\bmod (1+u+v), \bmod (u)$ and $\bmod (v)$ respectively we have $C_{i}^{\perp} \subseteq C_{i}$ for $i=1,2,3$. Therefore, $x^{n}-1 \equiv 0\left(\bmod f_{i} f_{i}^{*}\right)$ for $i=1,2,3$.

Corollary 4.8. $C=(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3}$ is a cyclic code of length $n$ over $S$. Then $C^{\perp} \subseteq C$ iff $C_{i}^{\perp} \subseteq C_{i}$ for $i=1,2,3$.

Example 4.9. Let $n=7, S=F_{2}+u F_{2}+v F_{2}$
$x^{7}-1=(x+1)\left(x^{3}+x+1\right)\left(x^{3}+x^{2}+1\right)=f_{1} f_{2} f_{3}$ in $F_{2}[x]$. Hence,

$$
\begin{aligned}
f_{1}^{*} & =x+1=f_{1} \\
f_{2}^{*} & =x^{3}+x^{2}+1=f_{3} \\
f_{3}^{*} & =x^{3}+x+1=f_{2}
\end{aligned}
$$

Let $C=\left\langle(1+u+v) f_{3},(u) f_{2},(v) f_{3}\right\rangle$. Obviously $x^{n}-1$ is divisibly by $f_{i} f_{i}^{*}$ for $i=2,3$. Thus we have $C^{\perp} \subseteq C$.

Using Theorem 4.1 and Theorem 4.7 we can construct quantum codes.
Theorem 4.10. Let $C=C=(1+u+v) C_{1} \oplus(u) C_{2} \oplus(v) C_{3}$ be a cyclic code of arbitrary length $n$ over $S$ with type $8^{k_{1}} 4^{k_{2}} 2^{k_{3}}$. If $C_{i}^{\perp} \subseteq C_{i}$ where $i=1,2,3$ then $C^{\perp} \subseteq C$ and there exists a quantum error-correcting code with parameters $\left[\left[3 n, 3 k_{1}+2 k_{2}+k_{3}-3 n, d_{L}\right]\right]$ where $d_{L}$ is the minimum Lee weights of $C$.

## 5 Examples

| $n$ | $C_{1}$ | $C_{2}$ | $C_{3}$ | $\Psi(C)$ | $[[N, K, D]]$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 7 | $[7,4,3]$ | $[7,4,3]$ | $[7,4,3]$ | $[21,12,3]$ | $[[21,3,3]]$ |
| 8 | $[8,6,2]$ | $[8,4,2]$ | $[8,6,2]$ | $[24,16,2]$ | $[[24,8,2]]$ |
| 15 | $[15,11,3]$ | $[15,8,4]$ | $[15,11,3]$ | $[45,30,3]$ | $[[45,15,3]]$ |
| 30 | $[30,18,5]$ | $[30,21,4]$ | $[30,17,6]$ | $[90,56,4]$ | $[[90,22,4]]$ |

## References

[1] A. Dertli, Y. Cengellenmis, S. Eren, On quantum codes obtained from cyclic codes over $A_{2}$, Int. J. Quantum Inform. 13, (2015).
[2] A. Dertli, Y. Cengellenmis, S. Eren, Quantum codes over the ring $F_{2}+u F_{2}+u^{2} F_{2}+\ldots+$ $u^{m} F_{2}$, Int. Journal of Alg., 3, (2015).
[3] A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error correction via codes over GF (4), IEEE Trans. Inf. Theory, 44, (1998).
[4] J. Qian, Quantum codes from cyclic codes over $F_{2}+v F_{2}$, Journal of Inform.\& computational Science 6, 1715-1722 (2013).
[5] J. Qian, W. Ma, W. Gou, Quantum codes from cyclic codes over finite ring 7, 1277-1283 (2009).
[6] X. Kai, S. Zhu, Quaternary construction bof quantum codes from cyclic codes over $F_{4}+u F_{4}$, Int. J. Quantum Inform., 9, 689-700 (2011).
[7] X. Yin, W. Ma, Gray Map And Quantum Codes Over The Ring $F_{2}+u F_{2}+u^{2} F_{2}$, International Joint Conferences of IEEE TrustCom-11, (2011).
[8] Y. Cengellenmis, A. Dertli, S. T. Dougherty, Codes over an infinite family of rings with a Gray map, 72, 559-580 (2014).

## Author information

Abdullah Dertli, Department of Mathematics, Ondokuz Mayıs University, Faculty of Arts and Sciences, Samsun, TURKEY.
E-mail: abdullah.dertli@gmail.com
Yasemin Cengellenmis, Department of Mathematics, Trakya University, Faculty of Arts and Sciences, Edirne, TURKEY.
E-mail: ycengellenmis@gmail.com
Senol Eren, Department of Mathematics, Ondokuz Mayıs University, Faculty of Arts and Sciences, Samsun, TURKEY.
E-mail: seren@omu.edu.tr
Received: March 9, 2015.
Accepted: May 7, 2015.

