QUANTUM CODES FROM CYCLIC CODES OVER $A_3$

A. Dertli, Y. Cengellenmis

Abstract. In this paper, the quantum codes over $F_2$ are constructed by using the cyclic codes over $A_3 = F_2 + uF_2 + vF_2 + wF_2 + uwF_2 + vwF_2 + uvwF_2$ with $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = wu, vw = vw$. Moreover, the parameters of quantum codes over $F_2$ are determined.

2010 Mathematics Subject Classification: 94B15, 81P68, 94B60.

Keywords: cyclic codes, quantum codes, gray map, rings.

1. Introduction
Quantum error correcting codes are used in quantum computing to protect quantum information from errors. The first error correcting code was discovered by Shor in [14] and independently by Steane in [1]. Although the theory quantum error correcting codes has differences from theory classical error correcting codes, Calderbank et al. gave a way to construct quantum error correcting codes from classical error correcting codes.

Many quantum error correcting codes have been constructed by using classical error correcting codes over many finite rings [2-16].

In [17], the finite ring $A_k = F_2[v_1, ..., v_k]/\langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle, 1 \leq i, j \leq k$ was introduced. In this paper, we give some knowledges about the ring $A_3$, in section 2. A necessary and sufficient condition for cyclic codes over $A_3$ that contains its dual is given in section 3. The parameters of quantum error correcting codes are obtained from cyclic codes over $A_3$. Some examples are given.

2. Preliminaries
In [17], the finite ring $A_k = F_2[v_1, ..., v_k]/\langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle, 1 \leq i, j \leq k$ was introduced firstly. By taking $k = 3$, we get the finite ring
\[ A_3 = F_2 + uF_2 + vF_2 + wF_2 + uwF_2 + vwF_2 + uvwF_2 \]
\[ = \left\{ a_1 + ua_2 + va_3 + wa_4 + uwv_5 + uwv_6 + uvw_7 : a_i \in F_2, 1 \leq i \leq 8 \right\} \]

with \( u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = vu, vw = wv \). This ring has characteristic 2 and cardinality \( 2^3 \). It is not a local ring. The only unit in the ring \( A_3 \) is 1. It is a principal ideal ring. Moreover, it is clear that \( A_3 \) is isomorphic to \( F_2[a,b,c]/\langle a^2 - a, b^2 - b, c^2 - c, ab - ba, ac - ca, bc - cb \rangle \).

We define the Gray map \( \Phi \) from \( A_3 \) to \( F_2^8 \) as follows,
\[ \Phi : A_3 \rightarrow F_2^8 \]
\[ a_1 + ua_2 + va_3 + wa_4 + uwv_5 + uwv_6 + uvw_7 \mapsto \zeta \]
where \( \zeta = (a_8, a_6 + a_7, a_5 + a_7, a_4 + a_5 + a_6 + a_7, a_3 + a_7, a_2 + a_3 + a_6 + a_7, a_1 + a_3 + a_5 + a_7, a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8) \).

This map \( \Phi \) can be extended to \( A_3^n \) in obvious way.

**Theorem 1.** The Gray map \( \Phi \) is a distance preserving map from \( A_3^n \) (Lee distance) to \( F_2^{8n} \) (Hamming distance) and it is also \( F_2 \)-linear.

The Hamming distance \( d_H(x, y) \) between two vectors \( x \) and \( y \) over \( F_2 \) is the Hamming weight of the vector \( x - y \).

The Lee weight \( w_L(x) \) of \( x = (x_0, x_1, \ldots, x_{n-1}) \in A_3^n \) is defined as \( w_L(x) = w_H(\Phi(x)) \). The Lee distance \( d_L(x, y) \) is given by \( d_L(x, y) = w_L(x - y) \) for any \( x, y \in A_3^n \).

A linear code \( C \) of length \( n \) over \( A_3 \) is a \( A_3 \)-submodule of \( A_3^n \).

**Lemma 2.** Let \( C \) be a linear code of length \( n \) over \( A_3 \) with rank \( k \) and minimum Lee distance \( d \), then \( \Phi(C) \) is a \( [8n, k, d] \) linear code over \( F_2 \).

For any \( x = (x_0, \ldots, x_{n-1}) \), \( y = (y_0, \ldots, y_{n-1}) \) the inner product is defined as
\[ xy = \sum_{i=0}^{n-1} x_i y_i \]

If \( xy = 0 \), then \( x \) and \( y \) are said to be orthogonal. Let \( C \) be a linear code of length \( n \) over \( R \), the dual of \( C \)
\[ C^\perp = \{ x : \forall y \in C, xy = 0 \} \]
which is also a linear code over $R$ of length $n$. A code $C$ is self orthogonal, if $C \subset C^\perp$ and self dual, if $C = C^\perp$.

**Theorem 3.** Let $C$ be a linear code of length $n$ over $A_3$. If $C$ is self orthogonal, so is $\Phi (C)$.

**Proof.** It is proved that as in [3].

Let
\[
\lambda_1 = 1 + u + v + uv + w + uw + vw + uvw
\]
\[
\lambda_2 = u + uw + uv + uvw
\]
\[
\lambda_3 = v + uv + vw + uvw
\]
\[
\lambda_4 = w + uw + vw + uvw
\]
\[
\lambda_5 = uw + uvw
\]
\[
\lambda_6 = uw + uvw
\]
\[
\lambda_7 = vw + uvw
\]
\[
\lambda_8 = uvw
\]

It is easy to show that $\lambda_i^2 = \lambda_i, \lambda_i \lambda_j = 0$ and $\sum_{k=1}^{8} \lambda_k = 1$, where $i, j = 1, 2, \ldots, 8$ and $i \neq j$. This show that $A_3 = \sum_{k=1}^{8} \lambda_k F_2$. Therefore, for any $a \in A_3$, $a$ can be expressed uniquely as $a = \sum_{k=1}^{8} \lambda_k a_k$, where $a_k \in F_2$, for $k = 1, 2, \ldots, 8$.

If $B_i$ $(i = 1, 2, \ldots, 8)$ are codes over $F_2$, we denote their direct sum by

$B_1 \oplus B_2 \oplus \ldots \oplus B_8 = \{b_1 + \ldots + b_8 : b_i \in B_i, i = 1, \ldots, 8\}$

**Definition 1.** Let $C$ be a linear code of length $n$ over $A_3$, we define
\[
C_1 = \{a \in F_2^n : \exists b, c, d, e, f, g, h \in F_2^n, \gamma \in C\}
\]
\[
C_2 = \{b \in F_2^n : \exists a, c, d, e, f, g, h \in F_2^n, \gamma \in C\}
\]
\[
C_3 = \{c \in F_2^n : \exists a, b, d, e, f, g, h \in F_2^n, \gamma \in C\}
\]
\[
C_4 = \{d \in F_2^n : \exists a, b, c, e, f, g, h \in F_2^n, \gamma \in C\}
\]
\[
C_5 = \{e \in F_2^n : \exists a, b, c, d, f, g, h \in F_2^n, \gamma \in C\}
\]
\[
C_6 = \{f \in F_2^n : \exists a, b, c, d, e, g, h \in F_2^n, \gamma \in C\}
\]
\[
C_7 = \{g \in F_2^n : \exists a, b, c, d, e, f, h \in F_2^n, \gamma \in C\}
\]
\[
C_8 = \{h \in F_2^n : \exists a, b, c, d, e, f, g \in F_2^n, \gamma \in C\}
\]

where $\gamma = \lambda_1 a + \lambda_2 b + \lambda_3 c + \lambda_4 d + \lambda_5 e + \lambda_6 f + \lambda_7 g + \lambda_8 h$. 33
It is noted that \( C_i \) \((i = 1, ..., 8)\) are linear codes over \( F_2 \). Moreover, \( C = \lambda_1 C_1 \oplus \cdots \oplus \lambda_8 C_8 \) and \(|C| = |C_1| |C_2| \cdots |C_8|\).

**Theorem 4.** Let \( C = \sum_{i=1}^{8} \lambda_i C_i \) be a linear code of length \( n \) over \( A_3 \). Then \( C^\perp = \sum_{i=1}^{8} \lambda_i C_i^\perp \).

**Lemma 5.** If \( G_i \) are generator matrices of binary linear codes \( C_i \) \((i = 1, ..., 8)\), then the generator matrix of \( C \) is

\[
G = \begin{bmatrix}
\lambda_1 G_1 \\
\lambda_2 G_2 \\
\vdots \\
\lambda_8 G_8
\end{bmatrix}
\]

Let \( d_L \) minimum Lee weight of linear code \( C \) over \( A_3 \). Then,

\[
d_L = d_H(\Phi(C)) = \min\{d_H(C_1), d_H(C_2), \ldots, d_H(C_8)\}
\]

where \( d_H(C_i) \) denotes the minimum Hamming weights of codes \( C_1, C_2, \ldots, C_8 \), respectively.

**Proposition 1.** Let \( C = \sum_{i=1}^{8} \lambda_i C_i \) be a linear code of length \( n \) over \( A_3 \), where \( C_i \) are codes over \( F_2 \) of length \( n \) for \( i = 1, \ldots, 8 \). Then \( C \) is a cyclic code over \( A_3 \) iff \( C_i, i = 1, \ldots, 8 \) are all cyclic codes over \( F_2 \).

**Proof.** Let \((a_0^i, a_1^i, \ldots, a_{n-1}^i) \in C_i \), where \( i = 1, \ldots, 8 \). Assume that \( m_i = \lambda_1 a_1^i + \lambda_2 a_2^i + \cdots + \lambda_8 a_8^i \) for \( i = 0, 1, \ldots, n-1 \). Then \((m_0, m_1, \ldots, m_{n-1}) \in C \). Since \( C \) is a cyclic code, it follows that \((m_{n-1}, m_0, \ldots, m_{n-2}) \in C \). Note that \((m_{n-1}, m_0, \ldots, m_{n-2}) = \lambda_1 (a_{n-1}^1, a_0^1, \ldots, a_{n-2}^1) + \cdots + \lambda_8 (a_{n-1}^8, a_0^8, \ldots, a_{n-2}^8) \). Hence \((a_{n-1}^i, a_0^i, \ldots, a_{n-2}^i) \in C \) for \( i = 1, \ldots, 8 \). Therefore, \( C_1, C_2, \ldots, C_8 \) are cyclic codes over \( F_2 \).

Conversely, suppose that \( C_1, C_2, \ldots, C_8 \) are cyclic codes over \( F_2 \). Let \((m_0, m_1, \ldots, m_{n-1}) \in C \), where \( m_i = \lambda_1 a_1^i + \lambda_2 a_2^i + \cdots + \lambda_8 a_8^i \) for \( i = 0, 1, \ldots, n-1 \). Then \((a_0^i, a_1^i, \ldots, a_{n-1}^i) \in C_i \) for \( i = 1, \ldots, 8 \). Note that \((m_{n-1}, m_0, \ldots, m_{n-2}) = \lambda_1 (a_{n-1}^1, a_0^1, \ldots, a_{n-2}^1) + \cdots + \lambda_8 (a_{n-1}^8, a_0^8, \ldots, a_{n-2}^8) \in C = \lambda_1 C_1 \oplus \cdots \oplus \lambda_8 C_8 \). So, \( C \) is a cyclic code over \( A_3 \).

**Proposition 2.** Suppose that \( C = \sum_{i=1}^{8} \lambda_i C_i \) is a cyclic code of length \( n \) over \( A_3 \). Then

\[
C = \langle \lambda_1 f_1, \lambda_2 f_2, \ldots, \lambda_8 f_8 \rangle
\]

34
where \( f_1, f_2, \ldots, f_8 \) are generator polynomials of \( C_1, C_2, \ldots, C_8 \) respectively.

**Lemma 6.** For any cyclic code \( C = \sum_{i=1}^{8} \lambda_i C_i \) of length \( n \) over \( A_3 \), there exist a unique polynomial \( f(x) \) such that \( C = \langle f(x) \rangle \) and \( f(x) \mid x^n - 1 \) where \( f_i(x) \) are the generator polynomials of \( C_i, i = 1, 2, \ldots, 8 \) and \( f(x) = \lambda_1 f_1(x) + \lambda_2 f_2(x) + \ldots + \lambda_8 f_8(x) \).

**Lemma 7.** Let \( C = \sum_{i=1}^{8} \lambda_i C_i \) be a cyclic code of length \( n \) over \( A_3 \), where \( C_1, C_2, \ldots, C_8 \) are binary codes. Then

\[
C^\perp = \langle \lambda_1 h_1^* + \lambda_2 h_2^* + \ldots + \lambda_8 h_8^* \rangle
\]

where for \( h_i^*(x) \) are the reciprocal polynomials of \( h_i(x) = (x^n - 1)/f_i(x) \), that is, \( h_i^*(x) = x^{\deg h_i(x)} h_i(x^{-1}) \) for \( i = 1, 2, \ldots, 8 \).

**Lemma 8.** A cyclic code \( C \) with generator polynomial \( f(x) \) contains its dual code iff

\[
x^n - 1 \equiv 0 \pmod{ff^*}
\]

where \( f^*(x) \) is the reciprocal polynomial of \( f(x) \), [7].

### 3. Quantum Codes from Cyclic Codes over \( A_3 \)

**Lemma 9.** Let \( C_1 \) and \( C_2 \) be linear codes over \( F_q \) with parameters \( [n, k_1, d_1]_q \) and \( [n, k_2, d_2]_q \), respectively and \( C_2^\perp \subseteq C_1 \). Furthermore, let

\[
d = \min\{w_i(v) : v \in (C_1 \setminus C_2^\perp) \cup (C_2 \setminus C_1^\perp)\} \geq \min\{d_1, d_2\}
\]

Then, there exist a quantum error correcting code \( C \) with parameters \( [n, k_1 + k_2 - n, d]_q \).

In particular, if \( C_1^\perp \subseteq C_1 \), then there exist a quantum error correcting code \( C \) with parameter \( [n, 2k_1 - n, d] \), where \( d_1 = \min\{w_i(v) : v \in C_1 \setminus C_1^\perp\} \), [11].

**Theorem 10.** Let \( C \) be a cyclic code of arbitrary length \( n \) over \( A_3 \), where \( f(x) = \lambda_1 f_1(x) + \lambda_2 f_2(x) + \ldots + \lambda_8 f_8(x) \), then \( C^\perp \subseteq C \) iff \( x^n - 1 \equiv 0 \pmod{f_i(x)f_i^*(x)} \), where \( f_i^*(x) \) are the reciprocal polynomials of \( f_i(x) \) respectively, for \( i = 1, 2, \ldots, 8 \).

**Proof.** Let \( x^n - 1 \equiv 0 \pmod{f_i(x)f_i^*(x)} \) for \( i = 1, 2, \ldots, 8 \). By using Lemma 8 \( C_i^\perp \subseteq C_i \) for \( i = 1, 2, \ldots, 8 \). By using this, we get

\[
\lambda_i C_i^\perp \subseteq \lambda_i C_i
\]

35
for \( i = 1, 2, \ldots, 8 \). Hence, \( \sum_{j=1}^{8} \lambda_j C_j^\perp \subseteq \sum_{j=1}^{8} \lambda_j C_j \). So, we have \( \left\langle \sum_{j=1}^{8} \lambda_j h_j^*(x) \right\rangle \subseteq \left\langle \sum_{j=1}^{8} \lambda_j f_j(x) \right\rangle \). This implies that \( C^\perp \subseteq C \).

Conversely, if \( C^\perp \subseteq C \), then \( \sum_{j=1}^{8} \lambda_j C_j^\perp \subseteq \sum_{j=1}^{8} \lambda_j C_j \). Since \( C_i \) are the binary codes such that \( \lambda_i C_i \) is equal to \( C \) mod \( \lambda_i \), \( i = 1, \ldots, 8 \), we have \( C_i^\perp \subseteq C_i \), \( i = 1, \ldots, 8 \). So, \( x^n - 1 \equiv 0 \pmod{f_i(x)f_i^*(x)} \), \( i = 1, \ldots, 8 \).

**Theorem 11.** Let \( C = \sum_{i=1}^{8} \lambda_i C_i \) be a cyclic code of length \( n \) over \( A_3 \). If \( C_i^\perp \subseteq C_i \) where \( i = 1, 2, \ldots, 8 \), then \( C^\perp \subseteq C \) and there exists a quantum error-correcting code with parameters \( [[8n, 2k - 8n, d_L]] \), where \( d_L \) is the minimum Lee weight of the code \( C \) and \( k \) is the dimension of the code \( \Phi(C) \).

### 4. Examples

**Example 1.** Let \( n = 7 \)

\[ x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) \in F_2[x] \]

Let \( f_i(x) = x^3 + x + 1 \), \( i = 1, 2, \ldots, 8 \). Thus \( C_i \) are \([7, 4, 3]\) linear codes of length 7. So, \( \Phi(C) \) is \([56, 32, 3]\) linear code. Clearly, \( C^\perp \subseteq C \). Hence we obtain a quantum code with parameters \( [[56, 8, 3]] \).
5. Conclusion

In this paper, we have given the structure of cyclic codes over $A_3 = F_2 + uF_2 + vF_2 + wF_2 + uvF_2 + uwF_2 + vwF_2 + uvwF_2$ with $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = vu, vw = vw$ to obtain quantum codes from cyclic codes over this ring. We have established a method to obtain self-orthogonal codes over $F_2$ as the Gray images of cyclic codes over the ring $A_3$. Finally, we have constructed some examples of quantum codes to illustrate the main result in which some of them are new in literature.

References


Abdullah Dertli
Department of Mathematics, Faculty of Art and Science,
University of Ondokuz Mayis,
Samsun, Turkey
email: abdullah.dertli@gmail.com
Yasemin Cengellenmis
Department of Mathematics, Faculty of Science,
University of Trakya,
Edirne, Turkey
email: ycengellenmis@gmail.com