



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

On Quantum Codes Obtained From Cyclic Codes Over Family Of Finite Rings $A_{q,s}$

Madhu Kant Thakur ¹

Abstract

In this paper, we construct the quantum codes from cyclic codes over the family of finite rings $A_{q,s}$, where q is prime power for arbitrary length n . We obtain self-orthogonal codes over $\mathbb{F}_q$ as gray map of linear and cyclic codes over $A_{q,s}$. Finally, we determine the parameters of quantum codes over $A_{q,s}$ in which some of our quantum codes $[[2^s n, 2k - 2^s n, d_L]]_q$ are new in literature.

Keywords. Quantum codes, Finite rings, cyclic codes, Gray map, CSS codes.

1 Introduction

Quantum computers have a extraordinary potential to solve very complex problems very quickly than any classical computer. It uses quantum mechanical phenomena to perform and compute data. Quantum error correction is used in quantum computing to protect quantum information from errors due to decoherence and quantum noise. It plays a important role in quantum computation and quantum information.

Shor [4] and independently, Steane [7] were the first to introduce impressive technique for quantum error correction. Then a construction method, which is known as CSS construction method, was introduced by Calderbank et al. [5] to construct quantum error-correcting codes from classical error correcting codes. They found quantum error-correcting codes by transforming the problem of finding quantum error correction codes into finding additive codes over the field F_4 which are self-orthogonal. It brings great revolution in quantum computing. Many good quantum codes have been constructed since then by using classical cyclic codes over binary and non-binary fields with self orthogonal properties (see references 8-14). The studies of quantum error correction is mostly on binary codes but later these are generalized to non-binary codes in order to relate it with the binary case. For example, Ashikhmin and Knill [12] gave a q -ary quantum codes from the self-orthogonal codes over F_q^2 for any prime power q . On the analogs to Calderbank-Shor-Steane codes (CSS codes) and of $GF(4)$ Rains [13] constructed families of quantum codes over non-binary fields.

Many good quantum codes have been constructed by some authors using linear and cyclic codes over finite rings. Qian et. al. [3] gave construction method of quantum error correcting codes using cyclic codes over $F_2 + uF_2, u^2 = 0$. Kai and Zhu [2] constructed the quantum codes from linear and cyclic codes over $F_4 + uF_4, u^2 = 0$. Qian [6] introduced a new construction method of quantum codes from cyclic codes over $F_2 + vF_2, v^2 = v$. Dertli et. al. [1] obtained quantum codes over A_2 . Asraf and Mohammad [14] gave construction of quantum codes from cyclic codes over $F_q + uF_q + vF_q + uvF_q, u^2 = u, v^2 = v, uv = vu$, where $q = p^m$, p is a odd prime. Abhay Kumar Singh et. al. [15] obtained quantum codes over $F_2 + uF_2 + u^2F_2, u^3 = u$

¹ Dr. M. K. Thakur, Ranchi, India (madhukant05@gmail.com)

In this paper we construct quantum error-correcting code over $\mathbb{F}_q$ from cyclic codes over the family of finite rings $A_{q,s}$ where $s \geq 1$ and $q = p^m$, where p is any prime. We can find many good codes over the family of finite rings $A_{q,s}$.

This paper is organized as follows. In Sec. 2, we discuss the structure and some basic knowledge about the finite ring $A_{q,s}$. In Sec.3 we introduce a generalized form of Gray map ϕ_s over $A_{q,s}$, and we show that if C is orthogonal then $\phi_s(C)$. In Sec. 4 we discuss linear and cyclic codes over the ring $A_{q,s}$. Also we give a necessary and sufficient condition for cyclic code over $A_{q,s}$ that contains its dual. In Sec. 5, we obtain the parameters of quantum error correcting codes over $A_{q,s}$. Sec. 6 contains some examples.

2 Preliminaries

Define the ring,

$$A_{q,s} = \frac{\mathbb{F}_q[v_1, v_2, \dots, v_s]}{\langle v_i^2 = v_i, v_i v_j = v_j v_i, \forall i, j = 1, 2, \dots, s \rangle}$$

for $s \geq 1$ and $q = p^m$ where p is a prime.

The ring $A_{q,s}$ is a finite commutative ring with cardinality q^{2^s} and characteristic q . It is not a local ring and not a finite chain ring. It is a semi-local ring with 2^s maximal ideal and a principal ideal ring.

The ring $A_{q,s}$ can be recursively defined as

$$A_{q,s} = A_{q,s-1} + v_s A_{q,s-1}$$

For any subset $\Delta \subseteq \{1, 2, \dots, s\}$, we define

$$v_\Delta = \prod_{i \in \Delta} v_i$$

with $v_{\Delta=\emptyset} = 1$.

Then any element of $A_{q,s}$ is expressed as

$$\sum_{\Delta \subseteq \{1, 2, \dots, s\}} c_\Delta v_\Delta, \quad c_\Delta \in \mathbb{F}_q$$

A code C of length n over $A_{q,s}$ is a non-empty subset of $A_{q,s}^n$ and a code C is linear over $A_{q,s}$ if it is an $A_{q,s}$ -submodule of $A_{q,s}^n$.

A linear code C over $A_{q,s}$ is a cyclic code if $c = (c_0, c_1, \dots, c_{n-1}) \in C \Rightarrow \sigma(c) = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$.

A subset C of $A_{q,s}^n$ is a linear cyclic code of length n if and only if its polynomial representation is an ideal of $\frac{A_{q,s}[x]}{\langle x^n - 1 \rangle}$.

Let C be a code of length n over $\mathbb{F}_q$ and a codeword $e = (e_0, e_1, \dots, e_{n-1}) \in \mathbb{F}_q^n$. Then the Hamming weight $wt_H(e)$ of a codeword e is the number of nonzero components i.e.

$$wt_H(e) = \sum_{i=0}^{n-1} e_i; \quad \text{where } wt_H(e_i) = 1 \text{ if } e_i = 1 \text{ and } wt_H(e_i) = 0 \text{ if } e_i = 0.$$

The minimum weight of a code C is denoted by $wt_H(C)$ and is the smallest weight among all its nonzero codewords.

Hamming distance $d_H(e, e')$ between two codewords $e, e' \in \mathbb{F}_q^n$ of a code C is defined as

$$d_H(e, e') = wt_H(e - e')$$

The Hamming distance of C is defined by

$$d_H(C) = \min_{e, e' \in C, e \neq e'} d_H(e, e'); \text{ where for any } e' \in C, e \neq e'$$

3 Gray Map ϕ_s , $s \geq 1$ over $A_{q,s}$

Since ring $A_{q,s}$ can be recursively written as $A_{q,s} = A_{q,s-1} + v_s A_{q,s-1}$. So every element of $A_{q,s}$ can be expressed as

for $k = 1$, $a + v_1 b$, where $a, b \in \mathbb{F}_q$, and

for $s \geq 2$, $\alpha + v_s \beta$, where $\alpha, \beta \in A_{q,s-1}$

The gray map ϕ_1 from $A_{q,1}^n$ to $\mathbb{F}_q^{2n}$ is defined in terms of vectors as

$$\phi_1(a' + v_1 b') = (a', a' + 2b')$$

Where $a', b' \in \mathbb{F}_q^n$ and for $s \geq 2$, let $c' = c_1' + v_s c_2' \in A_{q,s}^n$, where $c_1', c_2' \in A_{q,s-1}^n$ we define $\phi_s: A_{q,s}^n \rightarrow \mathbb{F}_q^{2^s n}$ by

$$\phi_s(c') = (\phi_{s-1}(c_1'), \phi_{s-1}(c_1') + 2\phi_{s-1}(c_2'))$$

For any $c' \in A_{q,s}$, the Lee weight is defined as

$$wt_L(c) = wt_H(\phi_s(c))$$

The Lee distance between $x, y \in A_{q,s}$ is defined as

$$d_L(x, y) = wt_L(x - y)$$

The Lee distance of C is defined by

$$d_L(C) = \min_{x, y \in C, x \neq y} d_L(x, y); \text{ where for any } y \in C, x \neq y$$

Taking into consideration the definition of the gray map, it is possible to verify the following theorem.

Theorem 3.1 The gray map ϕ_s is a weight preserving map from $(A_{q,s}^n, \text{Lee weight})$ to $(\mathbb{F}_q^{2^s n}, \text{Hamming weight})$ and an isometry from $(A_{q,s}^n, \text{Lee distance})$ to $(\mathbb{F}_q^{2^s n}, \text{Hamming distance})$.

Theorem 3.2 If C is an (n, k, d_L) linear code over $A_{q,s}$ then $\phi_s(C)$ is a $(2^s n, k, d)$ linear code over $\mathbb{F}_q$, where $d = d_L$.

Proof. Let $\alpha, \beta \in A_{q,s}$, then

$$\alpha = \alpha_1 + v_s \alpha_2$$

And

$$\beta = \beta_1 + v_s \beta_2$$

Where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in A_{q,s-1}$ So, we have

$$\begin{aligned} \phi_s(\alpha + \beta) &= \phi_s((\alpha_1 + \beta_1) + v_s(\alpha_2 + \beta_2)) \\ &= (\phi_{s-1}(\alpha_1 + \beta_1), \phi_{s-1}((\alpha_1 + \beta_1) + (\alpha_2 + \beta_2))) \\ &= (\phi_{s-1}(\alpha_1) + \phi_{s-1}(\beta_1), \phi_{s-1}(\alpha_1 + \alpha_2) + \phi_{s-1}(\beta_1 + \beta_2)) \\ &= (\phi_{s-1}(\alpha_1), \phi_{s-1}(\alpha_1 + \alpha_2)) + (\phi_{s-1}(\beta_1), \phi_{s-1}(\beta_1 + \beta_2)) \\ &= (\phi_{s-1}(\alpha_1), \phi_{s-1}(\alpha_1) + \phi_{s-1}(\alpha_2)) + (\phi_{s-1}(\beta_1), \phi_{s-1}(\beta_1) + \phi_{s-1}(\beta_2)) \\ &= \phi_s(\alpha) + \phi_s(\beta) \end{aligned}$$

And,

$$\begin{aligned} \phi_s(\tau\alpha) &= (\phi_{s-1}(\tau\alpha_1), \phi_{s-1}(\tau\alpha_1) + \phi_{s-1}(\tau\alpha_2)) \\ &= (\tau\phi_{s-1}(\alpha_1), \tau(\phi_{s-1}(\alpha_1) + \phi_{s-1}(\alpha_2))) \\ &= \tau(\phi_{s-1}(\alpha_1), \phi_{s-1}(\alpha_1) + \phi_{s-1}(\alpha_2)) \\ &= \tau\phi_s(\alpha) \end{aligned}$$

Hence, the map ϕ_s is linear. Since, ϕ_s is a bijection therefore we have $|C| = |\phi_s(C)|$. So we have, $d = d_L$.

Theorem 3.3 Let C be a linear code of length n over $A_{q,s}$. If C is an Euclidean self-orthogonal, then $\phi_s(C)$ is also.

Proof. For $s=1$,

Let $a = a_1 + v_1 a_2$, $b = b_1 + v_1 b_2 \in C$, where $a_1, a_2, b_1, b_2 \in \mathbb{F}_q^n$

Now, we have

$$a \cdot b = (a_1 + v_1 a_2) \cdot (b_1 + v_1 b_2)$$

$$= a_1 b_1 + v_1 (a_1 b_2 + a_2 b_1 + a_2 b_2)$$

Since C is self-orthogonal so we have,

$$a_1 b_1 = 0 \quad \text{and} \quad (a_1 b_2 + a_2 b_1 + a_2 b_2) = 0$$

So,

$$\phi_1(a) \cdot \phi_1(b) = (a_1, a_1 + a_2) \cdot (b_1, b_1 + b_2)$$

$= a_1 b_1 + a_1 b_1 + a_1 b_2 + a_2 b_1 + a_2 b_2 = 0$ Hence, $\phi_1(C)$ is self-orthogonal. Thus, the theorem is true for $s = 1$. Suppose theorem is true for $s = m - 1$, so we have for any $x, y \in C$

$$x \cdot y = 0 \Rightarrow \phi_{m-1}(x) \cdot \phi_{m-1}(y) = 0$$

Now, suppose $s = m$, then let $a' = a_1' + v_m a_2'$, $b' = b_1' + v_m b_2' \in C$, where $a_1', a_2', b_1', b_2' \in A_{q,m-1}^n$

$$a' \cdot b' = 0$$

$$\Rightarrow (a_1' + v_m a_2') \cdot (b_1' + v_m b_2') = 0$$

$$\Rightarrow a_1' \cdot b_2' = 0 \quad \text{and} \quad a_1' b_2' + a_2' b_1' + a_2' b_2' = 0$$

$$\Rightarrow \phi_{m-1}(a_1') \cdot \phi_{m-1}(b_1') = 0$$

and

$$\phi_{m-1}(a_1') \cdot \phi_{m-1}(b_2') + \phi_{m-1}(a_2') \cdot \phi_{m-1}(b_1') + \phi_{m-1}(a_2') \cdot \phi_{m-1}(b_2') = 0$$

$$\text{So, } \phi_m(a') \cdot \phi_m(b') = (\phi_{m-1}(a_1'), \phi_{m-1}(a_1') + \phi_{m-1}(a_2')) \cdot (\phi_{m-1}(b_1'), \phi_{m-1}(b_1') + \phi_{m-1}(b_2'))$$

$$= \phi_{m-1}(a_1') \cdot \phi_{m-1}(b_1') + \phi_{m-1}(a_1') \cdot \phi_{m-1}(b_1') + \phi_{m-1}(a_1') \cdot \phi_{m-1}(b_2') + \phi_{m-1}(a_2') \cdot \phi_{m-1}(b_1') + \phi_{m-1}(a_2') \cdot \phi_{m-1}(b_2')$$

$$= 0$$

Therefore, $\phi_m(C)$ is self-orthogonal. Thus, theorem is true $\forall s \in N$.

4 Linear and cyclic codes over $A_{q,s}$

We have for any $\Delta \subseteq \{1, 2, \dots, s\}$, $v_\Delta = \prod_{i \in \Delta} v_i$.

with $v_{\Delta=\emptyset} = 1$.

Let

$$\varepsilon_i = v_{\Delta'} \left(\sum_{\Delta \subseteq \{1, 2, \dots, s\} / \Delta'} (-1)^l v_\Delta \right); \text{ for } i = 1, 2, 3, \dots, 2^s$$

Where l is number of element in Δ and Δ' is some Δ different for each i .

It can be easily observed that

$$\varepsilon_i^2 = \varepsilon_i, \quad \varepsilon_i \varepsilon_j = 0 \quad \text{and} \quad \sum_{i=1}^{2^s} \varepsilon_i = 1, \quad \text{where } i, j = 1, 2, 3, \dots, 2^s \text{ and } i \neq j.$$

We have $A_{q,s} = \bigoplus \varepsilon_i A_{q,s}; \text{ for } i = 1, 2, 3, \dots, 2^s$.

Also we can easily observed that $\varepsilon_i A_{q,s} \cong \mathbb{F}_q; \quad \forall i = 1, 2, 3, \dots, 2^s$. So, we have $A_{q,s} = \sum_{i=1}^{2^s} \varepsilon_i \mathbb{F}_q$

Therefore we can express any $a \in A_{q,s}$ uniquely as $a = \sum_{i=1}^{2^s} \varepsilon_i a_i$, where $a_i \in \mathbb{F}_q$, for $i = 1, 2, 3, \dots, 2^s$

Let $B_i, i = 1, 2, 3, \dots, 2^s$ be codes over $\mathbb{F}_q$, We denote

$$\oplus B_i = \{\sum_{i=1}^{2^s} b_i: b_i \in B_i, i = 1, 2, 3, \dots, 2^s\}, \text{ for } i = 1, 2, 3, \dots, 2^s$$

Definition 1 Let $\delta = \sum_{i=1}^{2^s} \varepsilon_i a_i'; a_i' \in \mathbb{F}_q^n$. Let C be a linear code of length n over $A_{q,s}$, we define $C_i = \{\bar{a}_i \in \mathbb{F}_q^n: \exists \bar{a}_j \in \mathbb{F}_q^n, \forall j (\neq i) \in \{1, 2, 3, \dots, 2^s\}, \delta \in C\}, i = 1, 2, 3, \dots, 2^s$.

C_i (for $i = 1, 2, 3, \dots, 2^s$) are linear code of length n over $\mathbb{F}_q$.

Also, we have $C = \oplus \varepsilon_i C_i$; for $i = 1, 2, 3, \dots, 2^s$, with $|C| = |C_1| |C_2| \dots |C_{2^s}|$ and $d_L(C) = \min. \{d_H(C_i), i = 1, 2, 3, \dots, 2^s\}$ If G_i are the generator matrices of q -ary linear codes C_i ($i = 1, 2, 3, \dots, 2^s$) then the generator matrix of C is given by

$$G = [\varepsilon_i G_i]_{i \times 1}; (i = 1, 2, 3, \dots, 2^s)$$

And the generator matrix of $\phi(C)$ is given by

$$\phi(G) = [\phi(\varepsilon_i G_i)]_{i \times 1}; (i = 1, 2, 3, \dots, 2^s)$$

To determine the parameters of related quantum codes, we now provide some results on cyclic codes over R . These findings are particular instances of those found by Yao et al. in [16].

Theorem 4.1 If $C = \oplus \varepsilon_i C_i; (i = 1, 2, 3, \dots, 2^s)$ be a cyclic code of length n over $A_{q,s}$ then $C^\perp = \oplus \varepsilon_i C_i^\perp; (i = 1, 2, 3, \dots, 2^s)$. Moreover, C is self-orthogonal code over $A_{q,s}$ if and only if C_i are self-orthogonal $\forall i = 1, 2, 3, \dots, 2^s$.

Lemma 4.2 If $C = \oplus \varepsilon_i C_i; (i = 1, 2, 3, \dots, 2^s)$ be a linear code of length n over $A_{q,s}$ then C is cyclic code over $A_{q,s}$ if and only if C_i ($i = 1, 2, 3, \dots, 2^s$) are cyclic codes over $\mathbb{F}_q$.

Lemma 4.3 If $C = \oplus \varepsilon_i C_i; (i = 1, 2, 3, \dots, 2^s)$ be a cyclic code of length n over $A_{q,s}$, then

$$C = \langle f_i(x), (i = 1, 2, 3, \dots, 2^s) \rangle$$

Where $f_i(x)$ are generator polynomials of C_i , ($i = 1, 2, 3, \dots, 2^s$) respectively, And, $|C| = q^{2^s n - (\sum_{i=1}^{2^s} \deg(f_i(x)))}$.

Lemma 4.4 If $C = \oplus \varepsilon_i C_i; (i = 1, 2, 3, \dots, 2^s)$ be any cyclic code of length n over $A_{q,s}$ then there exist a unique polynomial $f(x)$ such that $C = \langle f(x) \rangle$ and $f(x) | x^n - 1$ where $f(x) = \sum_{i=1}^{2^s} \varepsilon_i f_i; f_i(x)$ are generator polynomials of C_i , ($i = 1, 2, 3, \dots, 2^s$) respectively.

Lemma 4.5 Let $C = \oplus \varepsilon_i C_i; (i = 1, 2, 3, \dots, 2^s)$ be a cyclic code of length n over $A_{q,s}$, where C_i ($i = 1, 2, 3, \dots, 2^s$) are q -ary codes. Then

$$C^\perp = \langle \varepsilon_i h_i^*; (i = 1, 2, 3, \dots, 2^s) \rangle$$

And

$$|C^\perp| = q^{\sum_{i=1}^{2^s} \deg(f_i(x))}$$

Where for $h_i^*(x)$ are the reciprocal polynomials of $h_i(x) = (x^n - 1) / f_i(x)$, i.e., $h_i^*(x) = x^{\deg(h_i(x))} h_i(x^{-1})$, for $i = 1, 2, 3, \dots, 2^s$.

The necessary and sufficient condition for cyclic codes to be self-orthogonal over F_{p^m} is described by the following lemma:

Lemma 4.6 [17] A q -ary linear cyclic code C with generator polynomial $f(x)$ contains its dual code if and only if $x^n - 1 \equiv 0 \pmod{ff^*}$ where f^* denotes the reciprocal polynomial of f .

5 QUANTUM CODES FROM CYCLIC CODES OVER $A_{q,k}$

For any $x = (x_1, x_2, \dots, x_n)$, $y = (y_1, y_2, \dots, y_n) \in A_{q,s}^n$ the Euclidean inner product of x and y in $A_{q,s}^n$ is defined by

$$\langle x, y \rangle_E = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$$

Then x and y are said to be orthogonal if $\langle x, y \rangle_E = 0$.

The dual code $C^{\perp_E}$ of C is defined by

$$C^\perp = \{x \in A_{q,s}^n \mid \langle x, y \rangle_E = 0 \quad \forall y \in C\}$$

Which is again a linear code of length n over $A_{q,s}^n$.

If $C \subseteq C^{\perp_E}$ then code C is called self-orthogonal and if $C = C^{\perp_E}$ then C is self dual.

One important lemma for quantum error-correcting codes, or CSS construction, is as follows:

Lemma 5.1 [9] Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ respectively and $C_2^{\perp_E} \subseteq C_1$. Then an $[[n, k_1 + k_2 - n, d]]_q$ quantum code can be constructed, where $d = \min.\{wt(v): v \in ((C_1 \setminus C_2^{\perp_E}) \cup (C_2 \setminus C_1^{\perp_E}))\} \geq \min.\{d_1, d_2\}$. In particular, if $C_1^{\perp_E} \subseteq C_1$, then there exist an $[[n, 2k_1 - n, d_1]]_q$ quantum code, where $d_1 = \min.\{wt(v): v \in C_1 \setminus C_1^{\perp_E}\}$.

For cyclic codes over $A_{q,s}$ that contain its dual, we now provide a necessary and sufficient condition.

Theorem 5.2 Let $C = \langle f(x) \rangle$ be a cyclic code of arbitrary length n over $A_{q,s}$ where $f(x) = \sum_{i=1}^{2^s} \varepsilon_i f_i(x)$. Then, $C^{\perp_E} \subseteq C$ if and only if $x^n - 1 \equiv 0 \pmod{f_i f_i^*}$ for $i = 1, 2, 3, \dots, 2^s$ where f_i^* denotes the reciprocal polynomial of f_i , respectively for $i = 1, 2, \dots, 2^s$.

Corollary 5.3 If $C = \bigoplus \varepsilon_i C_i$; ($i = 1, 2, 3, \dots, 2^s$) be any cyclic code of length n over $A_{q,s}$. Then $C^{\perp_E} \subseteq C$ if and only if $C_i^{\perp_E} \subseteq C_i$, for $i = 1, 2, 3, \dots, 2^s$.

Now by using Lemma 5.1 and Theorem 5.2, one can construct quantum codes as follows:

Theorem 5.4 Let $C = \bigoplus \varepsilon_i C_i$; ($i = 1, 2, 3, \dots, 2^s$) be a cyclic code of length n over $A_{q,s}$. If $C_i^{\perp_E} \subseteq C_i$, ($i = 1, 2, 3, \dots, 2^s$), then $C^{\perp_E} \subseteq C$ and there exists a quantum code with parameters $[[2^s n, 2k - 2^s n, d_L]]_q$ where d_L is the minimum Lee weight of the code C and k is the dimension of the code $\phi(C)$.

6 Examples

Now we provide the following examples which demonstrate the usefulness of our result:

Example 6.1 Let $A_{8,1} = \frac{\mathbb{F}_8[v_1]}{\langle v_1^2 - v_1 \rangle}$ and let $n = 7$.

$x^7 - 1 = (x + 1)(x + w)(x + w^2)(x + w^3)(x + w^4)(x + w^5)(x + w^6)$ in $\mathbb{F}_8[x]$. Let $f_1(x) = f_2(x) = x^3 + w^4 x^2 + x + w^2$.

Then, $C_i = \langle f_i(x) \rangle, i = 1, 2$ are the cyclic codes over $\mathbb{F}_8$ having the parameters $[7, 4, 4]$.

Thus,

$$C = \langle \varepsilon_i f_i(x) \rangle, i = 1, 2$$

is a cyclic code of length 7 over $A_{8,1}$. Since $f_i f_i^*$ divide $x^7 - 1$ for $i = 1, 2$, so we have $C^{\perp_E} \subseteq C$. Also, $\phi_1(C)$ is $[14, 8, 4]$ linear code. Hence we obtain a quantum code with parameters $[[14, 2, 4]]$. This is a new quantum error correcting code in literature.

Example 6.2 Let $A_{2,5} = \frac{\mathbb{F}_2[v_1, v_2, \dots, v_5]}{\langle v_i^2 = v_i, v_i v_j = v_j v_i, \forall i, j = 1, 2, \dots, 5 \rangle}$ and let $n = 4$.

$x^4 - 1 = (x + 1)^4$ in $\mathbb{F}_2[x]$. Let $f_1(x) = f_3(x) = f_5(x) = f_7(x) = f_9(x) = f_{11}(x) = f_{13}(x) = f_{15}(x) = f_{17}(x) = f_{19}(x) = f_{21}(x) = f_{23}(x) = f_{25}(x) = f_{27}(x) = f_{29}(x) = f_{31}(x) = f_2(x) = f_4(x) = f_6(x) = f_8(x) = f_{10}(x) = f_{12}(x) = f_{14}(x) = f_{16}(x) = f_{18}(x) = f_{20}(x) = f_{22}(x) = f_{24}(x) = f_{26}(x) = f_{28}(x) = f_{30}(x) = f_{32}(x) = (x + 1)$.

Then, $C_i = \langle f_i(x) \rangle, i = 1, 2, \dots, 32$ are the cyclic codes over $\mathbb{F}_2$ having the parameters $[4, 3, 2]$.

Thus,

$$C = \langle \varepsilon_i f_i(x) \rangle, i = 1, 2, \dots, 32$$

is a cyclic code of length 4 over $A_{2,5}$. Since $f_i f_i^*$ divide $x^4 - 1$ for $i = 1, 2, \dots, 32$, so we have $C^{\perp_E} \subseteq C$. Also, $\phi_5(C)$ is $[128, 96, 2]$ linear code. Hence we obtain a quantum code with parameters $[[128, 64, 2]]$. This is a new quantum error correcting code in literature.

Example 6.3 Let $A_{4,2} = \frac{\mathbb{F}_4[v_1, v_2]}{\langle v_i^2 = v_i, v_i v_j = v_j v_i, \forall i, j = 1, 2 \rangle}$ and let $n = 27$.

$$x^{27} - 1 = (x + 1)(x + w)(x + w^2)(x^3 + w)(x^3 + w^2)(x^9 + w)(x^9 + w^2) \text{ in } \mathbb{F}_4[x].$$

Let $f_1(x) = f_3(x) = f_2(x) = x + w$ and

$$f_4(x) = x^3 + w$$

Then, $C_i = \langle f_i(x) \rangle, i = 1, 2, 3, 4$ are the cyclic codes over $\mathbb{F}_4$ having the parameters $[27, 24, 2]$.

Thus,

$$C = \langle \varepsilon_i f_i(x) \rangle, i = 1, 2, 3, 4$$

is a cyclic code of length 27 over $A_{4,2}$. Since $f_i f_i^*$ divide $x^{27} - 1$ for $i = 1, 2, 3, 4$, so we have $C^\perp \subseteq C$. Also, $\phi_2(C)$ is $[108, 102, 2]$ linear code. Hence we obtain a quantum code with parameters $[[108, 96, 2]]$. This is a new quantum error correcting code.

Example 6.4 Let $A_{3,4} = \frac{\mathbb{F}_3[v_1, v_2, v_3, v_4]}{\langle v_i^2 = v_i, v_i v_j = v_j v_i, \forall i, j = 1, 2, 3, 4 \rangle}$ and let $n = 9$.

$$x^9 - 1 = (2 + x)^9 \text{ in } \mathbb{F}_3[x]. \text{ Let } f_1(x) = f_3(x) = f_5(x) = f_7(x) = f_9(x) = f_{11}(x) = f_{13}(x) = f_{15}(x) = f_2(x) = f_4(x) = f_6(x) = f_8(x) = f_{10}(x) = f_{12}(x) = f_{14}(x) = f_{16}(x) = (2 + x).$$

Then, $C_i = \langle f_i(x) \rangle, i = 1, 2, \dots, 16$ are the cyclic codes over $\mathbb{F}_3$ having the parameters $[9, 8, 2]$.

Thus,

$$C = \langle \varepsilon_i f_i(x) \rangle, i = 1, 2, \dots, 16$$

is a cyclic code of length 9 over $A_{3,4}$. Since $f_i f_i^*$ divide $x^9 - 1$ for $i = 1, 2, \dots, 16$, so we have $C^\perp \subseteq C$. Also, $\phi_4(C)$ is $[144, 128, 2]$ linear code. Hence we obtain a quantum code with parameters $[[144, 112, 2]]$. This is a new quantum error correcting code in literature.

Example 6.5 Let $A_{9,3} = \frac{\mathbb{F}_9[v_1, v_2, v_3]}{\langle v_i^2 = v_i, v_i v_j = v_j v_i, \forall i, j = 1, 2, 3 \rangle}$ and let $n = 8$.

$$x^8 - 1 = (1 + x)(2 + x)(x + w)(x + w^2)(x + w^3)(x + w^3)(x + w^6)(x + w^7) \text{ in } \mathbb{F}_9[x] \text{ where } \alpha^2 + 1 = 0$$

$$\text{Let } f_1(x) = f_3(x) = f_5(x) = f_7(x) = f_2(x) = f_4(x) = f_6(x) = f_8(x) = (x^3 + w^5 * x^2 + w^3 * x + w^2).$$

Then, $C_i = \langle f_i(x) \rangle, i = 1, 2, \dots, 8$ are the cyclic codes over $\mathbb{F}_9$ having the parameters $[8, 5, 4]$.

Thus,

$$C = \langle \varepsilon_i f_i(x) \rangle, i = 1, 2, \dots, 8$$

is a cyclic code of length 8 over $A_{9,3}$. Since $f_i f_i^*$ divide $x^8 - 1$ for $i = 1, 2, \dots, 8$, so we have $C^\perp \subseteq C$. Also, $\phi_3(C)$ is $[64, 40, 4]$ linear code. Hence we obtain a quantum code with parameters $[[64, 16, 4]]$.

Example 6.6 Let $A_{5,4} = \frac{\mathbb{F}_5[v_1, v_2, v_3, v_4]}{\langle v_i^2 = v_i, v_i v_j = v_j v_i, \forall i, j = 1, 2, 3, 4 \rangle}$ and let $n = 11$.

$$x^{11} - 1 = (4 + x)(4 + x + x^2 + 4x^3 + 2x^4 + x^5)(4 + 3x + x^2 + 4x^3 + 4x^4 + x^5) \text{ in } \mathbb{F}_5[x]. \text{ Let } f_1(x) = f_3(x) = f_5(x) = f_7(x) = f_9(x) = f_{11}(x) = f_{13}(x) = f_{15}(x) = (4 + 3x + x^2 + 4x^3 + 4x^4 + x^5) \text{ and } f_2(x) = f_4(x) = f_6(x) = f_8(x) = f_{10}(x) = f_{12}(x) = f_{14}(x) = f_{16}(x) = (4 + x + x^2 + 4x^3 + 2x^4 + x^5).$$

Then, $C_i = \langle f_i(x) \rangle, i = 1, 2, \dots, 16$ are the cyclic codes over $\mathbb{F}_5$ having the parameters $[11, 9, 5]$.

Thus,

$$C = \langle \varepsilon_i f_i(x) \rangle, i = 1, 2, \dots, 16$$

is a cyclic code of length 4 over $A_{5,4}$. Since $f_i f_i^*$ divide $x^{11} - 1$ for $i = 1, 2, \dots, 16$, so we have $C^\perp \subseteq C$. Also, $\phi_4(C)$ is $[176, 144, 5]$ linear code. Hence we obtain a quantum code with parameters $[[176, 106, 5]]$. This is a new quantum error correcting code in literature.

Example 6.7 Let $A_{25,1} = \frac{\mathbb{F}_{25}[v_1]}{\langle v_1^2 = v_1 \rangle}$ and let $n = 15$.

$$x^{18} - 1 = (x + 1)(x + 4)(x + w^4)(x + w^8)(x + w^{16})(x + w^{20})(x^3 + w^4)(x^3 + w^8)(x^3 + w^{16})(x^3 + w^{20}) \text{ in } \mathbb{F}_{25}[x]. \text{ Let } f_1(x) = (x + w^{16}) \text{ and } f_2(x) = (x^3 + w^4).$$

Then, $C_i = \langle f_i(x) \rangle, i = 1, 2$ are the cyclic codes over $\mathbb{F}_{25}$ having the parameters $[15, 12, 2]$.

Thus,

$$C = \langle \varepsilon_i f_i(x) \rangle, i = 1, 2$$

is a cyclic code of length 18 over $A_{25,1}$. Since $f_i f_i^*$ divide $x^{18} - 1$ for $i = 1, 2$, so we have $C^\perp \subseteq C$. Also, $\phi_1(C)$ is $[36, 32, 2]$ linear code. Hence we obtain a quantum code with parameters $[[36, 28, 2]]$. This is a new quantum error correcting code in literature.

Table 1: The Quantum Codes Over $A_{25,1}$

n	f_1	f_2	$\phi_2(C)$	$[[n, k, d]]$
6	$14cmx + 1$	$14cmx + w^4$	$[12, 10, 2]$	$[[12, 8, 2]]$
10	$14cm \quad x^5 + 4x^4 + 3 * x^3 + 2x^2 + x + 4$	$14cm \quad x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1$	$[20, 10, 4]$	$[[20, 0, 4]]$
13	$14cm \quad x^5 + 3x^3 + 2x^2 + 4$	$14cmx^4 + x^3 + 4x^2 + x + 1$	$[26, 17, 4]$	$[[26, 8, 4]]$
25	$14cmx + 4$	$14cmx + 4$	$[50, 48, 2]$	$[[50, 46, 2]]$
36	$14cmx^4 + 4$	$14cmx^4 + 4$	$[72, 64, 2]$	$[[72, 56, 2]]$
40	$14cm \quad x^4 + x^3 + x^2 + w^7x + w^{21}$	$14cm \quad x^4 + w^8x^3 + w^{10}x^2 + w^5x + 3$	$[80, 72, 4]$	$[[80, 64, 4]]$
62	$14cm \quad x^{12} + 4x^{10} + 4x^7 + x^6 + x^5 + x^3 + 3x^2 + 4x + 1$	$14cm \quad x^{12} + 4x^{10} + 4x^7 + x^6 + x^5 + 4x^4 + x^3 + 3x^2 + 4x + 1$	$[124, 100, 9]$	$[[124, 76, 9]]$
70	$14cm \quad x^{15} + w^{13}x^{14} + w^{20}x^{13} + w^{19}x^{12} + w^{11}x^{11} + w^9x^{10} + w^{15}x^9 + w^5x^8 + wx^7 + w^3x^6 + w^3x^6 + w^{21}x^5 + w^7x^4 + w^{23}x^3 + w^4x^2 + w^{17}x + 1$	$14cm \quad x^{15} + w^{13}x^{14} + w^{20}x^{13} + w^{19}x^{12} + w^{11}x^{11} + w^9x^{10} + w^{15}x^9 + w^5x^8 + wx^7 + w^3x^6 + w^{21}x^5 + w^7x^4 + w^{23}x^3 + w^4x^2 + w^{17}x + 1$	$[140, 110, 14]$	$[[140, 80, 14]]$

Table 2: The Quantum Codes Over $A_{4,3}$

n	$f_1 = f_3 = f_5 = f_7$	$f_2 = f_4 = f_6 = f_8$	$\phi_2(C)$	$[[n, k, d]]$
4	$14cmx^2 + 1$	$14cmx^2 + 1$	$[32, 16, 2]$	$[[32, 0, 2]]$
6	$14cmx^2 + w^2 * x + w$	$14cmx^2 + x + 1$	$[48, 32, 2]$	$[[48, 16, 2]]$
7	$14cmx + 1$	$14cmx^3 + x^2 + 1$	$[56, 40, 2]$	$[[56, 24, 2]]$
10	$14cmx + 1$	$14cmx^2 + w^2 * x + 1$	$[80, 68, 2]$	$[[80, 56, 2]]$
19	$14cm \quad x^9 + wx^8 + wx^6 + wx^5 + w^2x^4 + w^2x^3 + w^2x + 1$	$14cm \quad x^9 + wx^8 + wx^6 + wx^5 + w^2x^4 + w^2x^3 + w^2x + 1$	$[152, 80, 8]$	$[[152, 8, 8]]$
35	$14cm \quad x^{12} + w^2x^{11} + w^2x^8 + x^6 + wx^5 + x^4 + w^2x^3 + x + 1$	$14cm \quad x^{12} + w^2x^{11} + w^2x^8 + x^6 + wx^5 + x^4 + w^2x^3 + x + 1$	$[280, 184, 4]$	$[[280, 88, 4]]$
78	$14cmx + 1$	$14cmx^6 + x^5 + wx^3 + wx + 1$	$[624, 596, 2]$	$[[624, 568, 2]]$
91	$14cm \quad x + 1$	$14cmx + 1$	$[728, 720, 2]$	$[[728, 712, 2]]$

8 Conclusion

In this paper, we have constructed the quantum codes from cyclic codes over the family of finite rings $A_{q,s}$, where q is prime power. We have given some examples to illustrate the construction of

quantum codes over $A_{q,s}$ in which some of our quantum codes $\left[[2^s n, 2k - 2^s n, d_L]\right]_q$ are new in literature. We believe that cyclic codes over the family of finite rings $A_{q,s}$ will be a good source for constructing many good quantum codes.

References

- [1] Dertli, Abdullah, Yasemin Cengellenmis, and Senol Eren. "On quantum codes obtained from cyclic codes over A_2 ." International journal of quantum information 13.03 (2015): 1550031.
- [2] Kai, Xiaoshan, and Shixin Zhu. "QUATERNARY CONSTRUCTION OF QUANTUM CODES FROM CYCLIC CODES OVER $F_4 + uF_4$." International Journal of Quantum Information 9.02 (2011): 689-700.
- [3] Qian, Jianfa, Wenping Ma, and Wangmei Guo. "Quantum codes from cyclic codes over finite ring." International Journal of Quantum Information 7.06 (2009): 1277-1283.
- [4] Shor, Peter W. "Scheme for reducing decoherence in quantum computer memory." Physical review A 52.4 (1995): R2493.
- [5] Calderbank, A. Robert, et al. "Quantum error correction via codes over GF (4)." IEEE Transactions on Information Theory 44.4 (1998): 1369-1387.
- [6] Qian, Jianfa. "Quantum Codes from Cyclic Codes over $F_2 + vF_2$." JOURNAL OF INFORMATION & COMPUTATIONAL SCIENCE 10.6 (2013): 1715-1722.
- [7] Steane, Andrew M. "Simple quantum error-correcting codes." Physical Review A 54.6 (1996): 4741.
- [8] Aly, Salah A., Andreas Klappenecker, and Pradeep Kiran Sarvepalli. "On quantum and classical BCH codes." IEEE Transactions on Information Theory 53.3 (2007): 1183-1188.
- [9] Grassl, Markus, Thomas Beth, and Martin Roetteler. "On optimal quantum codes." International Journal of Quantum Information 2.01 (2004): 55-64.
- [10] Beth, T., and Markus Grassl. "The quantum Hamming and hexacodes." Fortschritte der Physik Progress of Physics 46.4-5 (1998): 459-491.
- [11] Li, Ruihu, and Xueliang Li. "Quantum codes constructed from binary cyclic codes." International Journal of Quantum Information 2.02 (2004): 265-272.
- [12] Ashikhmin, Alexei, and Emanuel Knill. "Nonbinary quantum stabilizer codes." IEEE Transactions on Information Theory 47.7 (2001): 3065-3072.
- [13] Rains, Eric M. "Nonbinary quantum codes." IEEE Transactions on Information Theory 45.6 (1999): 1827-1832.
- [14] Ashraf, Mohammad, and Ghulam Mohammad. "Quantum codes from cyclic codes over $F_q + uF_q + vF_q + uvF_q$." Quantum Information Processing 15.10 (2016): 4089-4098.
- [15] Singh, Abhay Kumar, et al. "On quantum codes obtained from cyclic codes over $F_2 + uF_2 + u^2F_2$." Asian-European Journal of Mathematics 11.01 (2018): 1850009.
- [16] Yao, T., Shi, M., Sole, P. "Skew cyclic codes over $F_q + uF_q + vF_q + uvF_q$." J. Algebra Comb. Discrete Appl. 2.3 (2015): 163-168.
- [17] Calderbank, A.R., Rains, E.M., Shor, P.M., Sloane, N.J.A. "Quantum error-correction via codes over GF(4)" IEEE Trans. Inf. Theory 44 (1998): 1369-1387.