Bull. Korean Math. Soc. **53** (2016), No. 6, pp. 1617–1628
http://dx.doi.org/10.4134/BKMS.b150544
pISSN: 1015-8634 / eISSN: 2234-3016

ON QUANTUM CODES FROM CYCLIC CODES OVER A CLASS OF NONCHAIN RINGS

Mustafa Sari and Irfan Siap

Abstract. In this paper, we extend the results given in [3] to a nonchain ring $R_p = \mathbb{F}_p + v\mathbb{F}_p + \cdots + v^{p-1}\mathbb{F}_p$, where $v^p = v$ and p is a prime. We determine the structure of the cyclic codes of arbitrary length over the ring R_p and study the structure of their duals. We classify cyclic codes containing their duals over R_p by giving necessary and sufficient conditions. Further, by taking advantage of the Gray map π defined in [4], we give the parameters of the quantum codes of length pn over $\mathbb{F}_p$ which are obtained from cyclic codes over R_p. Finally, we illustrate the results by giving some examples.

1. Introduction

The advantage of quantum mechanics compared to classical mechanics led researches to consider and study quantum communication and quantum computation. Hence, instead of classical bits used in computers working by the rules of classical mechanic, quantum bits or shortly qubits are proposed to be studied. Due to the superposition state of qubits, theoretically qubits can store more information in transition or storage compared to the classical case. While qubits have some superiorities than classical bits, one of the main problems for qubits is the decoherence that destroys the information in a superposition of qubits. While it seems that the decoherence makes the quantum communication and computation challenging even impossible, however the quantum error correcting codes (QEC) overcome this problem. The first solution to this problem was proposed by Shor by introducing a quantum error correcting code that encoded one qubit to highly entangled state of nine qubits [13]. Later in [6], Calderbank and Shor gave a method for constructing QEC from the classical error correcting codes, where this construction is called CSS construction. In [9], Gottesman defined the stabilizer quantum codes as the subspaces stabilized by a subgroup of the group consisting of all quantum errors. He also showed that stabilizer quantum codes include the QEC obtained by CSS construction. In [14], a generalized construction for QEC which enables to obtain many new

Received July 9, 2015.
2010 *Mathematics Subject Classification.* 81P70, 94B15.
Key words and phrases. quantum codes, cyclic codes, gray map.

codes was given. In [5, 15], the problem of constructing QEC was carried over the finite field with four elements $\mathbb{F}_4$. While the original QEC were over binary fields, QEC have been generalized to nonbinary cases [2, 10]. In [2], the errors on $\mathbb{F}_q$ were defined and the notion of self-orthogonal codes over $\mathbb{F}_4$ and binary quantum codes were generalized to self-orthogonal codes over $\mathbb{F}_q$ and q-ary quantum codes. In [11], the authors gave a new but simple construction for stabilizer codes which is based on syndrome assignment by classical parity-check matrices. To give the exact parameters of a quantum code constructed via CSS construction, it is enough to find a classical linear code containing its dual. Hence, the conditions for linear codes containing their duals have been investigated in [1, 3, 7, 12, 16]. In [1], the BCH codes containing their Euclidean or Hermitian duals were studied and the quantum BCH codes were obtained. In [16], the condition for cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ where $u^3 = 0$ containing their duals are studied and moreover a Gray map from $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ to $\mathbb{F}_2^3$ which preserves the orthogonality is defined and binary QEC are obtained as Gray images of these cyclic codes. In [12], the results given in [16] were considered over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ where $u^2 = u$. By taking the Gray images of some special cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, a class of binary quantum codes were obtained. In [3], the findings in [12] are generalized to the ring $\mathbb{F}_3 + v\mathbb{F}_3$ with $v^2 = 1$ and a construction of a class of ternary quantum codes is presented. Further, in [7], the conditions of cyclic codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$ where $v^3 = v$ containing their duals are established and the a class of binary QEC with its parameters is presented.

This paper is organized as follows: In Section 2, the basic definitions needed in the next sections are given. In Section 3, the Gray map from R_p^n to $\mathbb{F}_p^{pn}$ defined in [4] is stated and its properties are further studied. In Section 4, we investigate the cyclic codes of arbitrary length over R_p and characterize the structure of cyclic codes and their duals over R_p. We also determine the conditions for cyclic codes over R_p containing their duals. Furthermore, we construct a family of quantum error correcting codes over $\mathbb{F}_p$ by making advantage of the Gray map. Finally, in Section 5, we conclude this paper by presenting some examples.

2. Preliminaries

A code C of length n over $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is a finite field with q elements. A linear code C of length n over $\mathbb{F}_q$ is defined to be a subspace of $\mathbb{F}_q^n$. A linear code of length n and dimension k over $\mathbb{F}_q$ is denoted by $[n,k]_q$. Let $x = (x_1, x_2, \ldots, x_n)$ be a vector in $\mathbb{F}_q^n$. The Hamming weight $w_H(x)$ of the vector x is defined as the number of nonzero coordinates of the vector x, that is,

$$w_H(x) = |\{i : x_i \neq 0,\ 1 \leq i \leq n\}|.$$

An element of a code C is called a codeword of C. The Hamming weight $w_H(C)$ of a code C is the minimum nonzero weight of all codewords in C, i.e.,

$$w_H(C) = \min\{w_H(c) : 0 \neq c \in C\}.$$

Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two vectors in $\mathbb{F}_q^n$. The Hamming distance $d_H(x, y)$ between the vectors x and y is defined as

$$d_H(x, y) = w_H(x - y).$$

The Hamming distance $d_H(C)$ of a code C is the minimum Hamming distance between all different codewords of C, i.e.,

$$d_H(C) = \min\{d_H(x, y) : x, y \in C,\ x \neq y\}.$$

The notion $|C|$ for a code C is the size of the code C. A code C over $\mathbb{F}_q$ having the length n, the Hamming distance d is denoted by $(n, |C|, d)_q$. A linear code C over $\mathbb{F}_q$ of length n, the dimension k and the Hamming distance d is denoted by $[n, k, d]_q$ where the symbols n, k and d are called the parameters of C. An $[n, k, d]_q$ code is also an $\left(n, q^k, d\right)_q$ code. The operation "$\cdot$" is defined as the usual inner product between x and y in $\mathbb{F}_q^n$, i.e., $x \cdot y = \sum_i x_i y_i$. The dual code $C^\perp$ of a linear code C of length n over $\mathbb{F}_q$ is the set

$$C^\perp = \left\{ x \in \mathbb{F}_q^n : \langle x, c\rangle = \sum_{i=1}^{n} x_i c_i = 0,\ \forall c \in C \right\}.$$

Note that if C is an $[n, k]_q$ code, then the dual code $C^\perp$ is an $[n, n-k]_q$ code.

Linear codes over finite fields have significant role on constructing quantum codes. In what follows we are going to explain this construction by establishing necessary definitions first. Let q be a prime power and let $\mathbb{H}_q(\mathbb{C})$ be a q dimensional Hilbert vector space which represents the states of a quantum mechanical system. Let x range over the elements of a finite field $\mathbb{F}_q$ and let $|x\rangle$ denote the vectors of a distinguished orthonormal basis of $\mathbb{H}_q(\mathbb{C})$[10]. Denote $\mathbb{H}_q^n(\mathbb{C})$ as the n-fold tensor product of $\mathbb{H}_q(\mathbb{C})$, i.e.,

$$\mathbb{H}_q^n(\mathbb{C}) = \underbrace{\mathbb{H}_q(\mathbb{C}) \otimes \cdots \otimes \mathbb{H}_q(\mathbb{C})}_{n\ times}.$$

Then $\mathbb{H}_q^n(\mathbb{C})$ is a q^n dimensional Hilbert space. A quantum code of length n and dimension k over $\mathbb{F}_q$ is defined to be the q^k dimensional subspace of $\mathbb{H}_q^n(\mathbb{C})$ and simply denoted by $[\![n, k]\!]_q$. Recall that a space spanned by all vectors $|\varphi\rangle$ where $\varphi \in \mathbb{F}_q^n$ is a Hilbert space of q^n dimension. Before giving the well-known CSS construction, we state how one can construct a quantum error correcting code from classical linear codes by CSS construction. Let C_1 and C be two linear codes over $\mathbb{F}_q$ such that $C_1 \subseteq C$. For each additive coset D of C_1 in C, define the codeword

$$|\varphi\rangle = \frac{1}{|C_1|} \sum_{x \in D} |x\rangle.$$

Then, the subspace spanned by all codewords $|\varphi\rangle$ is called a quantum error correcting code obtained from two classical linear codes via CSS construction method.

Theorem 2.1 (CSS Construction)**.** *Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ such that $C_2 \subseteq C_1$, respectively. Then, there exists a quantum error correcting code with the parameters $[\![n,k_1-k_2,\min\{d_1,d_2^{\perp}\}]\!]_q$ where $d_2^{\perp}$ is the Hamming distance of the dual code $C_2^{\perp}$. Moreover, if $C_2 = C_1^{\perp}$, then there exists a quantum error correcting code with parameters $[\![n,2k_1-n,d_1]\!]_q$.*

Now, in order to get into our construction and findings which rely on a specific ring, we introduce the ring. Let p be a prime integer and let $R_p = \mathbb{F}_p + v\mathbb{F}_p + \cdots + v^{p-1}\mathbb{F}_p$ where $v^p = v$. The ring R_p is a commutative nonlocal ring with the maximal ideals $\langle v\rangle, \langle v+1\rangle, \ldots, \langle v+p-1\rangle$ and so the ring R_p is a nonchain ring. Denote $j_i = v+i$ for all $0 \leq i \leq p-1$ and define $\nu_i = \frac{v^p - v}{j_i}$ for $0 \leq i \leq p-1$. One can easily see that

$$R_p = \langle \nu_0\rangle \oplus \langle \nu_1\rangle \oplus \cdots \oplus \langle \nu_{p-1}\rangle .$$

Therefore, every element $r \in R_p$ can be written uniquely as $r = r_0 + r_1 + \cdots + r_{p-1}$, where $r_i \in \langle f_i\rangle$ for $0 \leq i \leq p-1$. The definitions of the codes over the ring R_p are similar to the codes over finite field. A code C over R_p of length n is a nonempty subset of R^n. A linear code C of length n over the ring R_p is an R_p-submodule of R_p^n. The dual code $C^{\perp}$ of a code C over R_p is given by

$$C^{\perp} = \left\{ y \in R_p^n : \langle x,y\rangle = \sum_{i=0}^{n-1} x_i y_i = 0, \, \forall x \in C \right\}.$$

If C is a linear code over R_p, then the dual code $C^{\perp}$ is also linear code over R_p. A code C over R_p of length n and the size M is denoted by (n,M). One can find more details for the structures of the ring R_p and the linear codes over R_p in [8].

In the rest of this paper, we denote $R_p = \mathbb{F}_p + v\mathbb{F}_p + \cdots + v^{p-1}\mathbb{F}_p$ where $v^p = v$ and p is a prime number.

3. A gray map from R_p^n to $\mathbb{F}_p^{pn}$

In [4], the authors defined a Gray map from R_p^n to $\mathbb{F}_p^{pn}$ and studied its properties. In this section, we state and study the properties of the Gray map relevant to our goal. We also reprove that this Gray map preserves the orthogonality with respect to the usual inner product by a method different than the one given in [4].

Definition 3.1. Let the map $\mu : R_p \to \mathbb{F}_p^p$ be defined as

$$r(v) = r_0 + r_1 v + \cdots + r_{p-1}v^{p-1} \to (r(0), r(1), \ldots, r(p-1))$$

for all $r_0 + r_1 v + \cdots + r_{p-1} v^{p-1} \in R_p$ and extend the map μ to $\pi : R_p^n \to \mathbb{F}_p^{pn}$ componentwise as in the usual way, i.e., for all $(c_0, c_1, \ldots, c_{n-1}) \in R^n$

$$\pi\left((c_0, c_1, \ldots, c_{n-1})\right) = \left(\mu\left(c_0\right), \mu\left(c_1\right), \ldots, \mu\left(c_{n-1}\right)\right).$$

We call π the Gray map from R^n to $\mathbb{F}_p^{pn}$.

Note that $\pi\left(r\right) = \left(r\left(0\right), r\left(1\right), \ldots, r\left(p-1\right)\right) = \left(r_0, r_1, \ldots, r_{p-1}\right) A^T$ where

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{p-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & p-1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{pmatrix}_{p \times p}.$$

Proposition 3.2. *For all $1 \leq j \leq p-2$, $\sum_{i=1}^{p-1} i^j \equiv 0\,(\mathrm{modp})$.*

Proof. Let $\mathbb{Z}_p$ be the set of integers modulo p and $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$. Suppose that α is a generator of $\mathbb{Z}_p^*$ and $p-1 = jk$. Since i^j's run through k times the elements of the subgroup $\left\langle \alpha^j \right\rangle$ and the order of α^j is k, we get

$$\sum_{i=1}^{p-1} i^j = k \sum_{x \in \langle \alpha^j \rangle} x = k \left(1 + \alpha^j + \cdots + \alpha^{(k-1)j}\right) = k \frac{\alpha^{kj} - 1}{\alpha^j - 1} \equiv 0\,(\mathrm{mod} p).$$

□

Lemma 3.3. *The matrix A is invertible.*

Proof. Let A_i be the ith column of the matrix A. See that

$$A_i^T A_j = \sum_{k=1}^{p-1} k^{i+j-2}\,(\mathrm{mod} p).$$

Clearly, for i and j providing that $i + j = p + 1$ and for the case $i = j = p$, $A_i^T A_j = p - 1$. Proposition 3.2 implies that $A_i^T A_j = 0$ for the other cases. Then

$$A^T A = (p-1) \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & 1 \\ 0 & 0 & \ddots & 0 & 1 & 0 \\ \vdots & \vdots & \ddots & \iddots & 0 & \vdots \\ \vdots & 0 & \iddots & \ddots & \ddots & \vdots \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}. \tag{3.1}$$

Hence the matrix A has full rank and so is invertible. □

By Lemma 3.3 and the definitions the following theorem follows.

Theorem 3.4. *If C is a linear code over R_p, then so is $\pi\left(C\right)$ over $\mathbb{F}_p$. Moreover, $|C| = |\pi\left(C\right)|$.*

The next theorem plays an important role for the construction of quantum codes from codes over R_p.

Theorem 3.5. *The Gray map π is a map preserving the orthogonality from R_p^n to $\mathbb{F}_p^{pn}$.*

Proof. It is enough to show for only $n=1$ by linearity. Let $r = r_0 + r_1 v + \cdots + r_{p-1}v^{p-1}$ and $s = s_0 + s_1 v + \cdots + s_{p-1}v^{p-1}$ be two elements in R_p such that $r \perp s$. Then, $r \perp s$ implies that

$$r_0 s_{p-1} + r_1 s_{p-2} + \cdots + r_{p-2}s_1 + r_{p-1}s_0 + r_{p-1}s_{p-1} = 0. \tag{3.2}$$

We observe that $A_i A_j^T$ gives the number of $r_{i-1}s_{j-1}$'s and $r_{j-1}s_{i-1}$'s appearing in $\langle \pi(r), \pi(s) \rangle$. By considering Equation 3.2 and it is sufficient to prove that

$$\begin{aligned} & \langle \pi(r), \pi(s) \rangle \\ = \; & (p-1)\left(r_0 s_{p-1} + r_1 s_{p-2} + \cdots + r_{p-2}s_1 + r_{p-1}s_0 + r_{p-1}s_{p-1}\right)(\text{mod} p). \end{aligned}$$

Let $t_{i,j}$ denote the number of $r_{i-1}s_{j-1}$'s appearing in $\langle \pi(r), \pi(s) \rangle$, i.e., $A_i^T A_j = (t_{i,j})$. By (3.1), we have

$$t_{i,j} = \begin{cases} p-1, & i+j = p+1 \\ p-1, & i=j=p \\ 0, & \text{otherwise} \end{cases}$$

which completes the proof. □

By Theorem 3.4 and Theorem 3.5 we obtain the following corollary as a consequence.

Corollary 3.6. *If C is a linear code containing its dual over R_p, then so is $\pi(C)$ over $\mathbb{F}_p$.*

Proof. Let C be a code over R_p such that $C^\perp \subseteq C$. Clearly, $\pi\left(C^\perp\right) \subseteq \pi(C)$. Theorem 3.5 implies that $\pi\left(C^\perp\right) \subseteq \pi(C)^\perp$. Comparing the cardinalities of $\pi\left(C^\perp\right)$ and $\pi(C)^\perp$, one can get that $\pi\left(C^\perp\right) = \pi(C)^\perp$ and so $\pi(C)^\perp \subseteq \pi(C)$. □

We define the Lee weight $w_L(r)$ of an element $r \in R$ to be $w_L(r) = w_H(\pi(r))$. The Lee weight is extended to R^n componentwise, i.e., the Lee weight of a vector $r = (r_0, r_1, \ldots, r_{n-1})$ in R^n is

$$w_L(r) = \sum_{i=0}^{n-1} w_L(r_i).$$

The Lee distance $d_L(r,s)$ between two vectors $r = (r_0, r_1, \ldots, r_{n-1})$ and $s = (s_0, s_1, \ldots, s_{n-1})$ in R^n is defined to be as

$$d_L(r,s) = w_L(r-s).$$

Then, the followings are immediate.

Theorem 3.7. *The Gray map π is a distance-preserving map from (R^n, d_L) and $\left(\mathbb{F}_p^{pn}, d_H\right)$.*

Corollary 3.8. *If C is an $(n, |C|, d_L)$ linear code over R_p, then $\pi(C)$ is a $(pn, |C|, d_L)$ linear code over $\mathbb{F}_p$ where $|C|$ is the cardinality of the code C.*

4. Quantum codes from cyclic codes over R_p

A code C of length n over the ring R_p (resp. $\mathbb{F}_q$) is called cyclic if $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also a codeword in C for all codewords $(c_0, c_1, \ldots, c_{n-1})$ in C. It is well-known that a cyclic code of length n over R_p (resp. $\mathbb{F}_q$) corresponds to an ideal in the quotient ring $R_p[x]/(x^n-1)$(resp. $\mathbb{F}_q[x]/(x^n-1)$). Since every ideal is principal in $\mathbb{F}_q[x]/(x^n-1)$, for all cyclic codes C of length n over $\mathbb{F}_q$, $C = \langle g(x)\rangle$ for some monic polynomial $g(x)$ in $\mathbb{F}_q[x]/(x^n-1)$, where $g(x)$ is called the generator polynomial of the cyclic code C. To determine the cyclic codes over R_p of length n, we need to investigate the ideal structure of the quotient ring $R_p[x]/(x^n-1)$.

Note that every element r of the ring R_p can be expressed uniquely as $r = \nu_0\lambda_0 + \nu_1\lambda_1 + \cdots + \nu_{p-1}\lambda_{p-1}$ for some $\lambda_0, \lambda_1, \ldots, \lambda_{p-1} \in \mathbb{F}_p$. This leads to the following lemma:

Lemma 4.1. *A linear code C over R_p of length n has the form $\nu_0C_0 \oplus \nu_1C_1 \oplus \cdots \oplus \nu_{p-1}C_{p-1}$, where $C_0, C_1, \ldots, C_{p-1}$ are linear codes of length n over $\mathbb{F}_p$. Moreover, a cyclic code C over R_p of length n has the form $\nu_0C_0 \oplus \nu_1C_1 \oplus \cdots \oplus \nu_{p-1}C_{p-1}$, where $C_0, C_1, \ldots, C_{p-1}$ are cyclic codes of length n over $\mathbb{F}_p$.*

Also, we have the following:

Corollary 4.2. *Let $C = \nu_0C_0 \oplus \nu_1C_1 \oplus \cdots \oplus \nu_{p-1}C_{p-1}$ be a linear code over R_p for some linear codes $C_0, C_1, \ldots, C_{p-1}$ over $\mathbb{F}_p$. Then, C is a cyclic code of length n over R_p if and only if $C_0, C_1, \ldots, C_{p-1}$ are cyclic codes of length n over $\mathbb{F}_p$.*

Corollary 4.3. *If $C = \nu_0C_0 \oplus \nu_1C_1 \oplus \cdots \oplus \nu_{p-1}C_{p-1}$ is a cyclic code over R_p of length n, then $C = \langle \nu_0g_0(x), \nu_1g_1(x), \ldots, \nu_{p-1}g_{p-1}(x)\rangle$ and $|C| = p^{pn-\sum_{i=0}^{p-1}\deg g_i(x)}$ where $g_i(x)$'s are the generator polynomials of C_i for $i = 0, 1, \ldots, p-1$, respectively.*

The following lemma is necessary for the proof of Proposition 4.5.

Lemma 4.4. *The followings hold*:

(1) *For all $i, j \in \{0, 1, \ldots, p-1\}$ such that $i \neq j$, $\nu_i\nu_j = 0$.*
(2) *For all $i \in \{0, 1, \ldots, p-1\}$, $\nu_i^2 = \lambda\nu_i$ for some nonzero $\lambda \in \mathbb{F}_p$.*
(3) $\sum_{i=0}^{p-1} \nu_i = -1$.

Proof. (1) It is clear from the definition of ν_i.

(2) Since $\nu_i^2 \in \langle\nu_i\rangle = \{\lambda\nu_i : \lambda \in F_p\}$, it is enough to show that $\nu_i^2 \neq 0$ for all $0 \leq i \leq p-1$. For the case $p = 2$ and $i = 0$, $\nu_0 = v + 1$ and so $\nu_0^2 =$

$(v+1)^2 = f_0 \neq 0$. For the case odd prime p and $i=0$, $\nu_0 = \frac{v^p - v}{v} = v^{p-1} - 1$ and so $\nu_0^2 = \left(v^{p-1}-1\right)^2 = -2\left(v^{p-1}-1\right) = -2\nu_0 \neq 0$. For the case $i \neq 0$ and all primes p, $\nu_i = \frac{v^p - v}{v+i} = v.\prod\limits_{\substack{j=1 \\ j\neq i}}^{p-1} v+j$. Since the constant term of $\prod\limits_{\substack{j=0 \\ j\neq i}}^{p-1} v+j$ is equal to $\prod\limits_{\substack{j=0 \\ j\neq i}}^{p-1} j\,(\mathrm{mod} p)$. Since $(j,p)=1$ for all $1 \leq j \leq p-1$, $\prod\limits_{\substack{j=0 \\ j\neq i}}^{p-1} j\,(\mathrm{mod} p) \neq 0$. Hence, $\nu_i^2 \neq 0$ and so $\nu_i^2 = \lambda f_i$ for some nonzero element λ in $\mathbb{F}_p$.

(3) Note that $\nu_0 = v^{p-1} - 1$ and $\nu_i = \sum\limits_{j=0}^{p-2} (-1)^j i^j v^{p-(j+1)}$ for $1 \leq i \leq p-1$. Then,

$$\sum_{i=0}^{p-1} \nu_i = \nu_0 + \sum_{i=1}^{p-1}\sum_{j=0}^{p-2} (-1)^j i^j v^{p-(j+1)} = -1 + \sum_{i=1}^{p-1}\sum_{j=1}^{p-2} (-1)^j i^j v^{p-(j+1)}.$$

Since the coefficient of $v^{p-(j+1)}$ for $1 \leq j \leq p-2$ is equal to $(-1)^j \sum\limits_{i=1}^{p-1} i^j$, it remains to show that $\sum\limits_{i=1}^{p-1} i^j \equiv 0\,(\mathrm{mod} p)$ for the proof. By Proposition 3.2, we are done. □

We are now ready to give the exact characterization of the cyclic codes over R_p.

Proposition 4.5. *Let C be a cyclic code over R_p of length n and suppose that $C = \nu_0 C_0 \oplus \nu_1 C_1 \oplus \cdots \oplus \nu_{p-1} C_{p-1}$ for some cyclic codes $C_0, C_1, \ldots, C_{p-1}$ of length n over $\mathbb{F}_p$. Then, C is principal, i.e., $C = \langle g(x) \rangle$ where $g(x) = \nu_0 g_0(x) + \nu_1 g_1(x) + \cdots + \nu_{p-1} g_{p-1}(x)$ and $C_i = \langle g_i(x) \rangle$ for $i = 1, 2, \ldots, p-1$. Furthermore, if $g_0(x) = g_1(x) = \cdots = g_{p-1}(x)$, then $C = \langle g_0(x) \rangle$.*

Proof. Since

$$\begin{aligned} C &= \nu_0 C_0 \oplus \nu_1 C_1 \oplus \cdots \oplus \nu_{p-1} C_{p-1}, \\ C &= \langle \nu_0 g_0(x), \nu_1 g_1(x), \ldots, \nu_{p-1} g_{p-1}(x) \rangle . \end{aligned}$$

Define $g(x) = \nu_0 g_0(x) + \nu_1 g_1(x) + \cdots + \nu_{p-1} g_{p-1}(x)$. Clearly, $\langle g(x) \rangle \subseteq C$. Conversely, by Lemma 4.4 for each $i \in \{0, 1, \ldots, p-1\}$, $\nu_i^2 = \lambda \nu_i$ and $\nu_i \nu_j = 0$ when $i \neq j$. Then, for each $i \in \{0, 1, \ldots, p-1\}$

$$\nu_i g(x) = \nu_i^2 g_i(x) = \lambda \nu_i g_i(x) \in C$$

and so $\nu_i g_i(x) \in C$. This implies that $C \subseteq \langle g(x) \rangle$. Hence, $C = \langle g(x) \rangle$. The last assertion directly follows from the fact $\nu_0 + \nu_1 + \cdots + \nu_{p-1} = -1$. □

Similar to the case for the cyclic codes over finite field, the dual code of a cyclic code over R_p is also a cyclic code over R_p. We now investigate the structure of the dual code of a cyclic code over R_p.

Proposition 4.6. *Let $C = \langle \nu_0 g_0(x) + \nu_1 g_1(x) + \cdots + \nu_{p-1} g_{p-1}(x) \rangle$ be a cyclic code over R_p of length n. Then*

$$C^{\perp} = \left\langle \nu_0 h_0^r(x) + \nu_0 h_0^r(x) + \cdots + \nu_{p-1} h_{p-1}^r(x) \right\rangle,$$

where $h_i(x)\, g_i(x) = x^n - 1$ for $i = 0, 1, \ldots, p-1$ and $\left|C^{\perp}\right| = p^{\sum\limits_{i=0}^{p-1} \deg g_i(x)}$.

Proof. Let $C_i = \langle g_i(x) \rangle$, $i = 0, 1, \ldots, p-1$. Recall that for each $i \in \{0, 1, \ldots, p-1\}$, $C_i^{\perp} = \langle h_i^r(x) \rangle$ where $x^n - 1 = g_i(x)\, h_i(x)$. Define the ideal $A = \left\langle \nu_0 h_0^r(x), \nu_1 h_1^r(x), \ldots, \nu_{p-1} h_{p-1}^r(x) \right\rangle$. Since $\nu_i g_i(x)\, \nu_j h_j(x) = 0$ for all $0 \leq i, j \leq p-1$, we get $A \subseteq C^{\perp}$. By comparing the cardinalities of A and $C^{\perp}$, we conclude that $A = C^{\perp}$. By Proposition 4.5,

$$C^{\perp} = \left\langle \nu_0 h_0^r(x) + \nu_1 h_1^r(x) + \cdots + \nu_{p-1} h_{p-1}^r(x) \right\rangle. \qquad \square$$

Next, we state the well-known fact for cyclic codes over finite fields.

Lemma 4.7. *Let C be a cyclic code with generator polynomial $g(x)$ over finite field where $g(x)\, h(x) = x^n - 1$. Then,*

$$C^{\perp} \subseteq C \;\Leftrightarrow\; h(x)\, h^r(x) \equiv 0 \,(\mathrm{mod} x^n - 1)$$

or equivalently

$$C^{\perp} \subseteq C \;\Leftrightarrow x^n - 1 \equiv 0 \,(\mathrm{mod} g(x)\, g^r(x)).$$

Now, we are ready to explore cyclic codes over R_p of length n containing their duals.

Lemma 4.8. *Let $C = \langle g(x) \rangle$ be a cyclic code over R_p of length n, where $g(x) = \nu_0 g_0(x) + \nu_1 g_1(x) + \cdots + \nu_{p-1} g_{p-1}(x)$ for some polynomials $g_1(x), g_2(x), \ldots, g_3(x)$ over $\mathbb{F}_p$. Then,*

$$C^{\perp} \subseteq C \;\Leftrightarrow\; x^n - 1 \equiv 0 \,(\mathrm{mod} g_i(x)\, g_i^r(x)), i = 0, 1, \ldots, p-1.$$

Proof. Since $C = \langle g(x) \rangle$ and $g(x) = \nu_0 g_0(x) + \nu_1 g_1(x) + \cdots + \nu_{p-1} g_{p-1}(x)$, $C = \nu_0 C_0 \oplus \nu_1 C_1 \oplus \cdots \oplus \nu_{p-1} C_{p-1}$ where $C_i = \langle g_i(x) \rangle$ for $0 \leq i \leq p-1$. Suppose that C contains its dual. Then, for each $0 \leq i \leq p-1$

$$\begin{aligned} &C^{\perp}\,(\mathrm{mod}\,(\nu_0, \nu_1, \ldots, \nu_{i-1}, \nu_{i+1}, \ldots, \nu_{p-1})) \\ &\subseteq C\,(\mathrm{mod}\,(\nu_0, \nu_1, \ldots, \nu_{i-1}, \nu_{i+1}, \ldots, \nu_{p-1})). \end{aligned}$$

This implies that $\nu_i C_i^{\perp} \subseteq \nu_i C_i$ and so $C_i^{\perp} \subseteq C_i$ for all $0 \leq i \leq p-1$. By Lemma 4.7, one direction is complete. Conversely, if $x^n - 1 \equiv 0 \,(\mathrm{mod} g_i(x)\, g_i^r(x))$ for $i = 0, 1, \ldots, p-1$, then $C_i^{\perp} \subseteq C_i$ and so $\langle \nu_i h_i^r \rangle \subseteq \langle \nu_i g_i \rangle$ for $i = 0, 1, \ldots, p-1$. This implies that

$$\left\langle \nu_0 h_0^r, \nu_1 h_1^r, \ldots, \nu_{p-1} h_{p-1}^r \right\rangle \subseteq \langle \nu_0 g_0, \nu_1 g_1, \ldots, \nu_{p-1} g_{p-1} \rangle.$$

Hence, $C^{\perp} \subseteq C$. $\square$

By Lemma 4.8, we have the following theorem.

Theorem 4.9. *Let $C = \nu_0 C_0 \oplus \nu_1 C_1 \oplus \cdots \oplus \nu_{p-1} C_{p-1}$ be a cyclic code over R_p. Then,*

$$C^{\perp} \subseteq C \;\Leftrightarrow\; C_i^{\perp} \subseteq C_i,\; i = 0, 1, \ldots, p-1.$$

Combining Theorem 4.9, Corollary 3.6 and Theorem 2.1, we give the parameters of quantum codes obtained from the cyclic codes over R_p containing their duals.

Theorem 4.10. *Let $C = \nu_0 C_0 \oplus \nu_1 C_1 \oplus \cdots \oplus \nu_{p-1} C_{p-1}$ be a cyclic code over R_p of length n, where for each $i \in \{0, 1, \ldots, p-1\}$, $C_i = \langle g_i(x) \rangle$, where $g(x) | x^n - 1$ over $\mathbb{F}_p$. If $C_i^{\perp} \subseteq C_i$ for $i = 0, 1, \ldots, p-1$, then there exists a quantum code with the parameters $[\![pn, pn - 2t, d_L]\!]_p$ where $t = \sum_{i=0}^{p-1} \deg g_i(x)$ and d_L is the minimum Lee distance of the code C.*

Now, we give some examples to illustrate what we discuss in this paper. Note that since the characteristics of $\mathbb{F}_p$ and the ring R_p are the same, $x^n - 1$ has the same factorization over $\mathbb{F}_p$ and the ring R_p.

Example 4.11. Over $\mathbb{F}_2$, $x^7 - 1 = (x+1)\left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right)$. Let $g_0(x) = g_1(x) = \left(x^3 + x + 1\right)$. Then, by Proposition 4.6, $C = \left\langle x^3 + x + 1 \right\rangle$. Since $\left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right) \big| x^7 - 1$, $C^{\perp} \subseteq C$ and so Corollary 3.6 implies that $\pi(C)^{\perp} \subseteq \pi(C)$. By a computer programme, $\pi(C)$ is a $[14, 8, 3]_2$ linear code. Hence, by Theorem 4.9, we get a $[\![14, 2, 3]\!]_2$ quantum code.

Example 4.12. Over $\mathbb{F}_3$, $x^3 - 1 = (x+2)^3$. Let $g_0(x) = g_1(x) = g_2(x) = x + 2$. Then, by Proposition 4.6, $C = \langle x + 2 \rangle$. Since $(x+2)(2x+1) = -(x+2)^2 \Big| x^3 - 1$, $C^{\perp} \subseteq C$ and so Corollary 3.6 implies that $\pi(C)^{\perp} \subseteq \pi(C)$. By a computer programme, $\pi(C)$ is a $[9, 6, 2]_3$ linear code. Hence, by Theorem 4.9, we get a $[\![9, 3, 2]\!]_3$ quantum code.

Example 4.13. Over $\mathbb{F}_3$, $x^6 - 1 = \left(x^2 - 1\right)^3 = (x+1)^3 (x+2)^3$. Some of quantum codes over $\mathbb{F}_3$ of length 18 obtained by Theorem 4.9 are presented in Table 1.

Example 4.14. Over $\mathbb{F}_5$, $x^5 - 1 = (x+4)^5$. Let $g_0(x) = \cdots = g_4(x) = x + 4$. Then, by Proposition 4.6, $C = \langle x + 4 \rangle$. Since $(x+4)(4x+1) = -(x+4)^2 \Big| x^5 - 1$, $C^{\perp} \subseteq C$ and so Corollary 3.6 implies that $\pi(C)^{\perp} \subseteq \pi(C)$. By a computer programme, $\pi(C)$ is a $[25, 20, 2]_5$ linear code. Hence, by Theorem 4.9, we get a $[\![25, 15, 2]\!]_5$ quantum code. Let $g_1(x) = \cdots = g_5(x) = (x+4)^2$. Then, by Proposition 4.6, $C = \left\langle (x+4)^2 \right\rangle$. Since $g_0(x)\, g_0^r(x) = (x+4)^4 \Big| x^5 - 1$, $C^{\perp} \subseteq C$ and so Corollary 3.6 implies that $\pi(C)^{\perp} \subseteq \pi(C)$. By a computer programme, $\pi(C)$ is a $[25, 15, 3]_5$ linear code. Hence, by Theorem 4.9, we get a $[\![25, 5, 3]\!]_5$ quantum code.

Table 1. Some of the quantum codes over $\mathbb{F}_3$ obtained via Theorem 4.9 in Example 4.13.

$g_0(x)$	$g_1(x)$	$g_2(x)$	$\pi(C)$	Quantum Code
$x+2$	$x+2$	$x+2$	$[18,15,2]_3$	$[\![18,12,2]\!]_3$
$x+1$	$x+1$	$x+1$	$[18,15,2]_3$	$[\![18,12,2]\!]_3$
x^2+2	x^2+2	x^2+2	$[18,12,2]_3$	$[\![18,6,2]\!]_3$
$x+2$	$x+2$	$x+1$	$[18,15,2]_3$	$[\![18,12,2]\!]_3$

5. Conclusion

In this study we extend the findings obtained in [3] to a more general class of nonchain rings $R_p = \mathbb{F}_p + v\mathbb{F}_p + \cdots + v^{p-1}\mathbb{F}_p$, where $v^p = v$ and p is a prime. Firstly, we state the Gray map defined in [4] and its properties and reprove that this Gray map preserves the orthogonality from R_p^n to $\mathbb{F}_p^{pn}$. We give the exact structure of cyclic codes and their duals over R_p of arbitrary length and obtain a necessary and sufficient condition for the existence of a cyclic code over R_p containing its dual. Taking the Gray images of cyclic codes over R_p with the condition that they contain their duals, we construct a family of quantum codes over $\mathbb{F}_p$. Finally, we illustrate the results arising in this paper and give some examples of quantum error correcting codes derived in Section 4.

Acknowledgment. This research is partially supported by the grant of Yildiz Technical University Research Support Unit, Project No: 2013-01-03-KAP02. This work is partially presented in the 6th International Conference On Modeling, Simulation And Applied Optimization, ICMSAO'15.

References

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, *Primitive quantum BCH codes over finite fields*, Proc. IEEE Int. Symp. Inf. Theory, Seattle, WA, pp. 1105–1108, 2006.

[2] A. Ashikhmin and E. Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inform. Theory **47** (2000), 3065–3072.

[3] M. Ashraf and G. Mohammad, *Quantum codes from cyclic codes over* $\mathbb{F}_3 + v\mathbb{F}_3$, Int. J. Quantum Inf. **12** (2014), no. 6, 1450042, 8 pp.

[4] A. Bayram and I. Siap, *Cyclic and constacyclic codes over a non-chain ring*, J. Algebra Comb. Discrete Struct. Appl. **1** (2014), no. 1, 1–12.

[5] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, *Quantum error correction via codes over* $GF(4)$, IEEE Trans. Inform. Theory **44** (1998), no. 4, 1369–1387.

[6] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A **54** (1996), no. 2, 1098–1105.

[7] A. Dertli, Y. Cengellenmis, and S. Eren, *On quantum codes obtained from cyclic codes over* $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$, http://arxiv.org/abs/1407.1232v1.

[8] S. J. Devitt, W. J. Munro, and K. Nemoto, *Quantum Error Correction for Beginners*, http://arxiv.org/pdf/0905.2794v4.pdf.

[9] D. Gottesman, *Stabilizer codes and quantum error correction*, Caltech Ph. D. Thesis, eprint:quant-ph/9705052.

[10] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory **52** (2006), no. 11, 4892–4914.

[11] C. Y. Lai and C. C. Lu, *A construction of quantum stabilizer codes based on syndrome assignment by classical parity-check matrices*, IEEE Trans. Inform. Theory **57** (2011), no. 10, 7163–7179.

[12] J. Qian, *Quantum codes from cyclic codes over* $\mathbb{F}_2 + v\mathbb{F}_2$, J. Inform. Comput. Sci. **10** (2013), no. 6, 1715–1722.

[13] P. W. Shor, *Scheme for reducing decoherence in quantum memory*, Phys. Rev. A **52** (1995), 2493–2496.

[14] A. M. Steane, *Enlargement of Calderbank-Shor-Steane quantum codes*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2492–2495.

[15] V. D. Tonchev, *The existence of optimal quaternary* $[28, 20, 6]$ *and quantum* $[[28, 12, 6]]$ *codes*, J. Algebra Comb. Discrete Appl. **1** (2014), no. 1, 13–17.

[16] Y. Xunru and M. Wenping, *Gray map and quantum codes over the ring* $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$, in Proc. IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, Changsha, China(IEEE Computer Society Press), pp. 897–899, 2011.

Mustafa Sari
Department of Mathematics
Faculty of Art and Sciences
Yildiz Technical University
34210, Istanbul-Turkey
E-mail address: `msari@yildiz.edu.tr`

Irfan Siap
Department of Mathematics
Faculty of Art and Sciences
Yildiz Technical University
34210, Istanbul-Turkey
E-mail address: `irfan.siap@gmail.com`