https://doi.org/10.15446/recolma.v56n1.105620

Revista Colombiana de Matemáticas
Volumen 56(2022)1, páginas 77-91

On quantum codes from codes over R_m

Sobre códigos cuánticos a través de códigos sobre R_m

Shahram Mehry

Malayer University, Malayer, Iran

Abstract. Let $R_m = \mathbb{F}_q[y]/\langle y^m - 1\rangle$, where $m \mid q-1$. In this paper, we obtain the structure of linear and cyclic codes over R_m. Also, we introduce a preserving-orthogonality Gray map from R_m to $\mathbb{F}_q^m$. Among the main results, we obtain the exact structure of self-orthogonal cyclic codes over R_m to introduce parameters of quantum codes from cyclic codes over R_m.

Key words and phrases. Self-orthogonal codes, Cyclic codes, Quantum codes.

2020 Mathematics Subject Classification. 94B05, 94B15, 81-04.

Resumen. Sea $R_m = \mathbb{F}_q[y]/\langle y^m - 1\rangle$ donde $m \mid q-1$. En este artículo, obtenemos la estructura de códigos lineales y cíclicos sobre R_m. También introducimos una aplicación de Gray de R_m a $\mathbb{F}_q^m$ que preserva la ortogonalidad. Entre los resultados principales, obtenemos la estructura exacta de los códigos cíclicos auto-ortogonales sobre R_m para introducir parámetros de los códigos cuánticos a través de los códigos cíclicos sobre R_m.

Palabras y frases clave. códigos auto-ortogonales, códigos cíclicos, códigos cuánticos.

1. Introduction

Quantum error correcting codes were introduced by Shor [10]. In a 1998 paper [3], the theory of finding quantum error-correcting codes is transformed into the problem of finding additive codes over the field $\mathbb{F}_4$ which are self-orthogonal with respect to a certain trace inner product. Recently, codes over rings that serve as a source for QEC have also been of interest.

In [7], quantum codes from cyclic codes over $F_2 + vF_2$ are studied. Also, in [1], a construction for quantum codes from cyclic codes over $R = \mathbb{F}_3 + v\mathbb{F}_3$ where $v^2 = 1$ was given. In [4], a method to obtain self-orthogonal codes over $\mathbb{F}_2$ is given and the parameters of quantum codes which are obtained from cyclic codes over $R = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^m\mathbb{F}_2$ are determined. Also the construction of quantum codes over $\mathbb{F}_q$ from cyclic codes over a finite non-chain ring $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, where $q = p^r$, p is a prime, $3 \mid p-1$ and $v^4 = v$ was given in [5]. Recently, Sari and Siap extended the results of [1] over $R_p = \mathbb{F}_p + v\mathbb{F}_p + \cdots + v^{p-1}\mathbb{F}_p$ where $v^p = v$ and p is a prime [9].

In this paper, we introduce some classes of quantum codes over $\mathbb{F}_q$ from linear and cyclic codes over the ring $R_m = \mathbb{F}_q[y]/\langle y^m - 1\rangle$, where $m \mid q-1$. In Section 2, we recall the definition of quantum codes and we provide some basic background. In Section 3, the structure of linear codes over R_m is given. In addition, we introduce a preserving-orthogonality gray map from R_m to $\mathbb{F}_q^m$. Also we obtain the parameters of quantum codes over $\mathbb{F}_q$ from linear codes over R_m. In the last Section, the exact structure of self-orthogonal cyclic codes over R_m is given in Theorem 4.4. Using this exact structure, we obtain an exact relation between cyclic codes over R_m and quantum codes over $\mathbb{F}_q$ these results are presented in Theorem 4.5. At the end of the paper, some examples of self-orthogonal cyclic codes and their relations with quantum codes are given.

2. Quantum codes

In [3], the problem of finding quantum-error-correcting codes is transformed into the problem of finding additive codes over the field $\mathbb{F}_4$. These quaternary codes are linear over $\mathbb{F}_2$. The natural generalization from $\mathbb{F}_2$ to an arbitrary finite ground field $\mathbb{F}_q$ was provided in [2, Definition 1] as follows.

Definition 2.1. Let $E = V(2, q)$ be the 2-dimensional vector space over $\mathbb{F}_q$. An $\mathbb{F}_q$-linear quantum code $[[n, k, d]]_q$ is an $\mathbb{F}_q$-subspace $C \subseteq E^n$, which satisfies the following conditions:

(1) C has $\mathbb{F}_q$-dimension $n - k$.

(2) $C \subseteq C^{\perp}$. Here the dual is taken with respect to an $\mathbb{F}_q$-linear symplectic scalar product on E^n, where each copy of E is a hyperbolic plane.

(3) The elements in $C^{\perp} \setminus C$ have weight $\geq d$.

In above definition, a symplectic form is a non-degenerate bilinear form β such that $\beta(x, y) = -\beta(y, x)$. Also a hyperbolic plane is a 2-dimensional subspace $H \subseteq E^n$, such that the restriction of β to H is non-degenerate.

The following proposition gives a method to construct quantum codes over a finite ground field $\mathbb{F}_q$.

Proposition 2.2. *Let C_1 and C_2 be two linear codes such that $C_2 \subseteq C_1$ over $\mathbb{F}_q$, and be with the parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$; respectively. Then there exists a quantum error-correcting code with the parameters $[[n, k_1 - k_2, \min\{d_1, d_2^{\perp}\}]]$, where $d_2^{\perp}$ denotes the minimum hamming distance of the dual code $C_2^{\perp}$ of C_2. Further, if $C_2 = C_1^{\perp}$, then there exists a quantum error-correcting code with the parameters $[[n, 2k_1 - n, d_1]]$.*

Proof. See Lemma 4 in [5]. ☑

We apply this proposition to obtain quantum codes. Note that the above proposition only introduces the parameters $[[n,k,d]]_q$ of the existing quantum codes which can be constructed by linear codes over $\mathbb{F}_q$. In other words, quantum codes as defined in Definition 2.1 are obtained by C_1 and C_2 which is not the purpose of this paper.

3. Quantum codes from linear codes over R

Throughout this paper let $R = R_m = \mathbb{F}_q[y]/\langle y^m - 1\rangle$, where $m \mid q-1$. A linear code C of length n over R is an R-submodule of R^n. In this section, first we obtain the structure of linear codes over R. So we introduce a preserving-orthogonality gray map from R to $\mathbb{F}_q^m$ and we obtain the parameters of quantum codes over $\mathbb{F}_q$ from linear codes over R.

Lemma 3.1. *Let α be a primitive mth root of unity in $\mathbb{F}_q$. If $f_i = y - \alpha^i$ for $i = 1,\dots,m$, then $y^m - 1 = \prod_{i=1}^{m} f_i$ is the unique factorization of $y^m - 1$ into irreducible factors over $\mathbb{F}_q$.*

Proof. Since $q \equiv 1 \mod m$, it follows from Theorem 4.2 in [8]. ☑

Lemma 3.2. *Let $y^m - 1 = \prod_{i=1}^{m} f_i$ be the unique factorization of $y^m - 1$ in above lemma and $\hat{f}_i = \prod_{j\neq i} f_j$, then there are $b_i', b_i \in \mathbb{F}_q[y]$ such that $b_i'\hat{f}_i + b_i f_i = 1$. If $e_i = b_i'\hat{f}_i + \langle y^m - 1\rangle \in R$, then*

(1) $e_1,\dots,e_m$ are mutually orthogonal non-zero idempotents of R.

(2) $e_1 + \cdots + e_r = 1 \in R$.

(3) Let Re_i be the principal ideal of R generated by e_i. Then e_i is the identity of Re_i.

(4) $R = Re_1 \oplus \cdots \oplus Re_m$, where $\oplus$ denotes the direct sum of rings.

(5) For each $i = 1,..,m$ let $R_i = \mathbb{F}_q[y]/\langle f_i\rangle$. Then the map

$$\varphi_i : R_i \to Re_i, g + \langle f_i\rangle \mapsto (g + \langle y^m - 1\rangle)e_i$$

is an isomorphism of rings.

(6) For each $i = 1,..,m$ the map $\psi_i : \mathbb{F}_q \to R_i, a \mapsto a + \langle f_i\rangle$ is an isomorphism of rings.

Proof. See Theorem 4.6 in [8]. ☑

For a positive integer n, let $\psi_i : \mathbb{F}_q^n \to R_i^n$ and $\varphi_i : (R_i)^n \to (Re_i)^n$ be the natural generalizations of ψ_i and φ_i. The following theorem gives the structure of linear codes over R.

Theorem 3.3. (1) $R^n = (Re_1)^n \oplus \cdots \oplus (Re_m)^n$.

(2) C is a linear code over R of length n if and only if

$$C = \varphi_1\psi_1(C_1) \oplus \cdots \oplus \varphi_m\psi_m(C_m),$$

where C_i is a linear code over $\mathbb{F}_q$ of length n. In this case $|C| = \Pi_{i=1}^m |C_i|$.

(3) Let $C^\perp$ be the dual of C with respect to standard inner product in R. Then

$$C^\perp = \varphi_1\psi_1(C_1^\perp) \oplus \cdots \oplus \varphi_m\psi_m(C_m^\perp),$$

where $C_i^\perp$ is the dual of C_i with respect to standard inner product in $\mathbb{F}_q$.

Proof. (1) It follows from Lemma 3.2, part 4.

(2) Let $C \subseteq R^n$ be an R-submodule. By Item 1, $C = \overline{C_1} \oplus \cdots \oplus \overline{C_m}$ where $\overline{C_i}$ is an Re_i-submodule of $(Re_i)^n$. Consider the $\mathbb{F}_q$-linear isomorphisms $\psi_i : (\mathbb{F}_q)^n \to (R_i)^n$ and $\varphi_i : (R_i)^n \to (Re_i)^n$. Since $\overline{C_i}$ is an $\mathbb{F}_q$-submodule, for any i we have that $\overline{C_i} = \varphi_i\psi_i(C_i)$ for some $\mathbb{F}_q$-submodule C_i of $\mathbb{F}_q^n$. Conversely let

$$C = \varphi_1\psi_1(C_1) \oplus \cdots \oplus \varphi_m\psi_m(C_m),$$

where C_i is a linear code over $\mathbb{F}_q$ of length n. Since $\psi_i : \mathbb{F}_q \to R_i$ and $\varphi_i : R_i \to Re_i$ are isomorphisms of rings, $C_i \subseteq \mathbb{F}_q^n$ is an $\mathbb{F}_q$-submodule if and only if $\varphi_i\psi_i(C_i) \subseteq (Re_i)^n$ is an Re_i-submodule. Hence $C \subseteq R^n$ is an R-submodule. Clearly

$$|C| = \Pi_{i=1}^m |\varphi_i\psi_i(C_i)| = \Pi_{i=1}^m |C_i|.$$

(3) Let

$$a = \varphi_1\psi_1(a_1) + \cdots + \varphi_m\psi_m(a_m) \in \varphi_1\psi_1(C_1^\perp) \oplus \cdots \oplus \varphi_m\psi_m(C_m^\perp)$$

and

$$b = \varphi_1\psi_1(b_1) \oplus \cdots \oplus \varphi_m\psi_m(b_m) \in C = \varphi_1\psi_1(C_1) \oplus \cdots \oplus \varphi_m\psi_m(C_m),$$

where $a_i = (a_{i1}, \ldots, a_{in}) \in C_i^\perp$ and $b_i = (b_{i1}, \ldots, b_{in}) \in C_i$ for $i = 1, \ldots, m$. It is easy to see that $\varphi_i\psi_i(a_i).\varphi_j\psi_j(b_j) = 0$ for $i \neq j$. Therefore

$$\begin{aligned} a.b &= \sum_{i=1}^m \varphi_i\psi_i(a_i).\varphi_i\psi_i(b_i) = \sum_{i=1}^m \varphi_i\psi_i(a_i.b_i) \\ &= \sum_{i=1}^m \varphi_i\psi_i(0) = 0, \end{aligned}$$

where in the last two lines we consider $\psi_i : \mathbb{F}_q \to R_i$ and $\varphi_i : R_i \to Re_i$ and also $a_i.b_i$ denotes the standard inner product over $\mathbb{F}_q$. So $a \in C^\perp$ and hence

$$\varphi_1\psi_1(C_1^\perp) \oplus \cdots \oplus \varphi_m\psi_m(C_m^\perp) \subseteq C^\perp.$$

Since R is a Frobenius ring, $|C||C^\perp| = |R^n| = q^{mn}$. So we have $|C^\perp| = \frac{q^{mn}}{|C|}$. On other hand

$$|\varphi_1\psi_1(C_1^\perp) \oplus \cdots \oplus \varphi_m\psi_m(C_m^\perp)| = \prod_{i=1}^{m} |C_i^\perp| = \prod_{i=1}^{m} \frac{q^n}{|C_i|} = \frac{q^{mn}}{|C|}.$$

Thus

$$|\varphi_1\psi_1(C_1^\perp) \oplus \cdots \oplus \varphi_m\psi_m(C_m^\perp)| = |C^\perp|.$$

Therefore

$$C^\perp = \varphi_1\psi_1(C_1^\perp) \oplus \cdots \oplus \varphi_m\psi_m(C_m^\perp).$$

☑

By Part 4 of Lemma 3.2, for any $\overline{g} = g + \langle y^m - 1\rangle \in R$ there exist $\overline{g_1} = g_1 + \langle y^m - 1\rangle, \ldots, \overline{g_m} = g_m + \langle y^m - 1\rangle \in R$ such that $\overline{g} = \overline{g_1}e_1 + \cdots + \overline{g_m}e_m$. we define a gray map $\phi : R \to \mathbb{F}_q^m$ by $\phi(\overline{g}) = (g_1(\alpha), \ldots, g_m(\alpha^m))$.

Definition 3.4. Let $\overline{g} = \overline{g_1}e_1 + \cdots + \overline{g_m}e_m$ be an element of R. The Lee weight of $\overline{g}$ is defined as follows: $\omega_L(\overline{g}) = \omega_H(g_1(\alpha), \ldots, g_m(\alpha^m))$, where $\omega_H(a)$ denotes the hamming weight of the vector a over $\mathbb{F}_q$. We define the Lee weight of a vector $c = (c_1, \ldots, c_n) \in R^n$ to be the rational sum of Lee weights of its components, i.e. $\omega_L(c) = \sum_{i=1}^{n} \omega_L(c_i)$.

Theorem 3.5. *Let $\phi : R^n \to \mathbb{F}_q^{mn}$ be the natural extension of the gray map ϕ form R to $\mathbb{F}_q^m$. Then*

(1) The gray map ϕ is an $\mathbb{F}_q$-linear isomorphism.

(2) ϕ is a distance-preserving map from R^n (Lee distance) to $\mathbb{F}_q^{mn}$ (hamming distance).

(3) If $C \subseteq R^n$ is a linear code, then $\phi(C^\perp) = \phi(C)^\perp$.

(4) If $C = \varphi_1\psi_1(C_1) \oplus \cdots \oplus \varphi_m\psi_m(C_m)$, then

$$d_L(C) = \min\{d_H(C_i); i = 1, \ldots, m\}$$

where $d_L(C)$ is the Lee distance of C and $d_H(C_i)$ is the hamming distance of C_i.

(5) If $C \subseteq R^n$ is an (n, A, d) linear code, then $\phi(C)$ is an $[mn, \log_q A, d]$ linear code over $\mathbb{F}_q$.

Proof. (1) Since $\phi : R^n \to \mathbb{F}_q^{mn}$ is the natural extension of $\phi : R \to \mathbb{F}_q^m$, it suffices to show that $\phi : R \to \mathbb{F}_q^m$ is an $\mathbb{F}_q$-linear isomorphism. First we show that ϕ is well defined. Let $\overline{g} = \overline{g_1}e_1 + \cdots + \overline{g_m}e_m = 0$. Hence $\overline{g_i}e_i = 0$ for any $i = 1, \dots, m$. But $\overline{g_i}e_i = 0$ if and only if $g_i \in \langle f_i \rangle$. Since $f_i(\alpha^i) = \alpha^i - \alpha^i = 0$, $g_i(\alpha^i) = 0$. Thus $\phi(\overline{g}) = (g_1(\alpha), \dots, g_m(\alpha^m)) = 0$. Now let $\overline{g} = \overline{g_1}e_1 + \cdots + \overline{g_m}e_m$ and $\overline{h} = \overline{h_1}e_1 + \cdots + \overline{h_m}e_m$ be elements of R and $a \in \mathbb{F}_q$. We have that

$$\overline{g} + \overline{h} = \sum_{i=1}^{m} (\overline{g_i} + \overline{h_i})e_i = \sum_{i=1}^{m} \overline{(g_i + h_i)}e_i.$$

Hence

$$\begin{aligned}\phi(\overline{g} + \overline{h}) &= ((g_1 + h_1)(\alpha), \dots, (g_m + h_m)(\alpha^m)) \\ &= (g_1(\alpha), \dots, g_m(\alpha^m)) + (h_1(\alpha), \dots, h_m(\alpha^m)) = \phi(\overline{g}) + \phi(\overline{h}).\end{aligned}$$

Also $a\overline{g} = \overline{ag_1}e_1 + \cdots + \overline{ag_m}e_m$. Thus

$$\phi(a\overline{g}) = (ag_1(\alpha), \dots, ag_m(\alpha^m)) = a(g_1(\alpha), \dots, g_m(\alpha^m)) = a\phi(\overline{g}).$$

Therefore ϕ is an $\mathbb{F}_q$-linear homomorphism. Now let $\phi(\overline{g}) = 0$. We have that $g_i(\alpha^i) = 0$ for $i = 1, \dots, m$. Thus $f_i = (y - \alpha^i) | g_i$ and hence $g_i \in \langle f_i \rangle$. As a result $\overline{g_i}e_i = 0$ for $i = 1, \dots, m$ and consequently

$$\overline{g} = \overline{g_1}e_1 + \cdots + \overline{g_m}e_m = 0.$$

Therefore ϕ is injective. Since $|R| = |\mathbb{F}_q^m|$, ϕ is surjective. This completes the proof.

(2) Let $c_1, c_2 \in R^n$. By Part 1, $\phi(c_1 - c_2) = \phi(c_1) - \phi(c_2)$. Hence

$$\begin{aligned}L(c_1, c_2) &= \omega_L(c_1 - c_2) \\ &= \omega_H(\phi(c_1 - c_2)) \\ &= \omega_H(\phi(c_1) - \phi(c_2)) = d_H(\phi(c_1), \phi(c_2)).\end{aligned}$$

This completes the proof.

(3) Let $c = (c_1, \dots, c_n) \in C$ and $c' = (c'_1, \dots, c'_n) \in C^\perp$ where

$$c_j = \overline{c_{j1}}e_1 + \cdots + \overline{c_{jm}}e_m$$

and

$$c'_j = \overline{c'_{j1}}e_1 + \cdots + \overline{c'_{jm}}e_m$$

for $j = 1, \dots, n$. We have that

$$\begin{aligned}\phi(c) &= (c_{11}(\alpha), c_{12}(\alpha^2), \dots, c_{1m}(\alpha^m), \dots, c_{n1}(\alpha), c_{n2}(\alpha^2), \dots, c_{nm}(\alpha^m)), \\ \phi(c') &= (c'_{11}(\alpha), c'_{12}(\alpha^2), \dots, c'_{1m}(\alpha^m), \dots, c'_{n1}(\alpha), c'_{n2}(\alpha^2), \dots, c'_{nm}(\alpha^m)).\end{aligned}$$

Thus

$$\phi(c').\phi(c) = \sum_{i=1}^{m}(\sum_{j=1}^{n} c'_{ji}(\alpha^i)c_{ji}(\alpha^i)).$$

Now since $c' \in C^{\perp}$, $c'.c = 0$. Therefore

$$\sum_{i=1}^{m} \overline{(\sum_{j=1}^{n} c'_{ji}c_{ji})e_i} = 0$$

and so

$$\overline{(\sum_{j=1}^{n} c'_{ji}c_{ji})e_i} = 0.$$

Thus $(\sum_{j=1}^{n} c'_{ji}c_{ji}) \in \langle f_i \rangle$. Consequently,

$$\sum_{j=1}^{n} c'_{ji}(\alpha^i)c_{ji}(\alpha^i) = (\sum_{j=1}^{n} c'_{ji}c_{ji})(\alpha^i) = 0.$$

Thus $\phi(c').\phi(c) = 0$ which proves that $\phi(c') \in \varphi(C)^{\perp}$. Therefore $\phi(C^{\perp}) \subseteq \phi(C)^{\perp}$. Since R and $\mathbb{F}_q$ are Frobenius rings, we have the following equality:

$$|\phi(C^{\perp})| = |C^{\perp}| = \frac{|R|^n}{|C|} = \frac{|R|^n}{|\phi(C)|} = \frac{|\mathbb{F}_q|^{mn}}{|\phi(C)|} = |\phi(C)^{\perp}|.$$

Therefore $\phi(C^{\perp}) = \phi(C)^{\perp}$.

(4) Let $c = (c_1, \ldots, c_n) \in R^n$. Then $c = \sum_{i=1}^{m} \varphi_i\psi_i(a_i)$, where

$$a_i = (a_{i1}, \ldots, a_{in}) \in (\mathbb{F}_q)^n,$$

for $i = 1, \ldots, m$. It is easy to see that

$$c_j = (a_{1j} + \langle y^m - 1\rangle)e_1 + \cdots + (a_{mj} + \langle y^m - 1\rangle)e_m$$

for $j = 1, \ldots, n$. So

$$\phi(c) = (a_{11}, \ldots, a_{m1}, \ldots, a_{1n}, \ldots, a_{mn})$$

and hence $\omega_L(c) = \sum_{i=1}^{m} \omega_H(a_i)$. Now let $\omega_L(C) = \omega_L(c)$ for some $c \in C$. We have that $c = \sum_{i=1}^{m} \varphi_i\psi_i(a_i)$ for some $a_i \in C_i$. Let $a_j \neq 0$. Then

$$\omega_L(C) = \omega_L(c) = \sum_{i=1}^{m} \omega_H(a_i) \geq \omega_H(a_j) \geq \min\{\omega_H(C_i); i = 1, \ldots, m\}.$$

On other hand if $a_i \in C_i$, then $c' = \varphi_i\psi_i(a_i) \in C$. But

$$\omega_L(C) \leq \omega_L(c') = \omega_H(a_i).$$

Hence

$$\omega_L(C) \leq \min\{\omega_H(C_i); i = 1, \ldots, m\}.$$

Therefore

$$\omega_L(C) = \min\{\omega_H(C_i); i = 1, \ldots, m\}.$$

Since the maps φ_i, ψ_i and ϕ are linear maps, we have the following equality that completes the proof

$$\begin{aligned} d_L(C) = \omega_L(C) &= \min\{\omega_H(C_i); i = 1, \ldots, m\} \\ &= \min\{d_H(C_i); i = 1, \ldots, m\}. \end{aligned}$$

(5) It is clear by the definition of the gray map ϕ.

☑

The following theorem indicates the existence of some quantum codes.

Theorem 3.6. *Let*

$$C = \varphi_1\psi_1(C_1) \oplus \cdots \oplus \varphi_m\psi_m(C_m)$$

be a linear code over R, where C_i is an $[n, k_i, d_i]$ linear code over $\mathbb{F}_q$. If $C_i^{\perp} \subseteq C_i$, then there exists a quantum error-correcting code with the parameters

$$[[mn, 2(\sum_{i=1}^{m} k_i) - mn, \min\{d_i; i = 1, \ldots, m\}]].$$

Proof. By Theorem 3.3.3,

$$C^{\perp} = \varphi_1\psi_1(C_1^{\perp}) \oplus \cdots \oplus \varphi_m\psi_m(C_m^{\perp}).$$

Then $C^{\perp} \subseteq C$ and so $\phi(C^{\perp}) \subseteq \phi(C)$. But $\phi(C^{\perp}) = \phi(C)^{\perp}$; see Theorem 3.5.3. Hence $\phi(C)^{\perp} \subseteq \phi(C)$. Also by Theorem 3.5, $\phi(C)$ is an

$$[mn, \sum_{i=1}^{m} k_i, \min\{d_i; i = 1, \ldots, m\}]$$

linear code over $\mathbb{F}_q$. Now Proposition 2.2 proves the existence of a quantum error-correcting code with the following parameters

$$[[mn, 2(\sum_{i=1}^{m} k_i) - mn, \min\{d_i; i = 1, \ldots, m\}]].$$

☑

Note that the above theorem only shows the existence of quantum codes with the help of self-orthogonal codes, but obtaining the exact structure of the self-orthogonal code $C = \varphi_1\psi_1(C_1) \oplus \cdots \oplus \varphi_m\psi_m(C_m)$ may not be very efficient. In the next section, as a special case of such codes, we specify the exact structure of self-orthogonal cyclic codes over R_m. Therefore the structure of quantum codes can be obtained with the relation between self-orthogonal codes and quantum codes, mentioned in Proposition 2.2. Moreover, some examples of self-orthogonal cyclic codes are given.

4. Quantum codes from cyclic codes over R

In this section, we obtain the structure of cyclic codes over $R = R_m = \mathbb{F}_q[y]/\langle y^m - 1\rangle$. We determine the parameters of quantum codes over $\mathbb{F}_q$ from cyclic codes over R and some examples are given. Consider the following correspondence.

$$\begin{aligned} \pi : R^n &\to R[x]/\langle x^n - 1\rangle, \\ (a_0, a_1 \dots, a_{n-1}) &\mapsto \qquad a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle. \end{aligned}$$

Clearly π is an R-module isomorphism. We will identify R^n with $R[x]/\langle x^n - 1\rangle$ under π. A nonempty subset C of R^n is a cyclic code if and only if $\pi(C)$ is an ideal of $R[x]/\langle x^n - 1\rangle$. Now consider the decomposition $R = Re_1 \oplus \cdots \oplus Re_m$ in Lemma 3.2. The following theorem gives a decomposition for $R[x]/\langle x^n - 1\rangle$.

Theorem 4.1. *(1) The following map is an isomorphism of rings;*

$$\varphi : \frac{R[x]}{\langle x^n - 1\rangle} \to \frac{Re_1[x]}{\langle e_1x^n - e_1\rangle} \times \cdots \times \frac{Re_m[x]}{\langle e_mx^n - e_m\rangle}$$
$$\overline{h} \mapsto (\overline{he_1}, \dots, \overline{he_m}),$$

where $\overline{h} = h + \langle x^n - 1\rangle$ and $\overline{he_i} = he_i + \langle e_ix^n - e_i\rangle$.

(2) C is an ideal of $R[x]/\langle x^n - 1\rangle$ if and only if $\varphi(C) = J_1 \times \cdots \times J_m$, where J_i is an ideal of $Re_i[x]/\langle e_ix^n - e_i\rangle$.

(3) If $J_i = \langle\overline{h_i}\rangle$ for $i = 1, \dots, m$, then $C = \langle\overline{h_1 + \cdots + h_m}\rangle$.

Proof. (1) Let $\overline{h} \in R[x]/\langle x^n - 1\rangle$. Then

$$\begin{aligned} \overline{h} = 0 &\Leftrightarrow h \in \langle x^n - 1\rangle \\ &\Leftrightarrow \exists g \in R[x];\ h = g(x^n - 1) \\ &\Leftrightarrow he_i = g(e_ix^n - e_i)\ for\ i = 1, \dots, m \\ &\Leftrightarrow \overline{he_i} = 0\ for\ i = 1, \dots, m. \end{aligned}$$

Hence φ is well defined and injective. Now let

$$(\overline{h_1}, \ldots, \overline{h_m}) \in \prod_{i=1}^{m} \frac{Re_i[x]}{\langle e_i x^n - e_i \rangle}.$$

Since e_i is the identity of $Re_i[x]$, $h_i = h_i e_i$ for $i = 1, \ldots, m$. Also for $i \neq j$, $h_i e_j = h_i e_i e_j = 0$. Hence $\varphi(\overline{h_1 + \cdots + h_m}) = (\overline{h_1}, \ldots, \overline{h_m})$. Thus φ is surjective. It is easy to see that $\varphi(\overline{h}.\overline{h'}) = \varphi(\overline{h}).\varphi(\overline{h'})$ and $\varphi(\overline{h} + \overline{h'}) = \varphi(\overline{h}) + \varphi(\overline{h'})$ for $\overline{h}, \overline{h'} \in R[x]/\langle x^n - 1\rangle$. Therefore φ is an isomorphism of rings.

(2) It is clear by Item 1.

(3) By the proof of Part 1, we have that

$$\varphi(\overline{h_1 + \cdots + h_m}) = (\overline{h_1}, \ldots, \overline{h_m}).$$

Hence

$$\varphi(C) = J_1 \times \cdots \times J_m = \langle \varphi(\overline{h_1 + \cdots + h_m}) \rangle = \varphi(\langle \overline{h_1 + \cdots + h_m} \rangle).$$

Therefore $C = \langle \overline{h_1 + \cdots + h_m} \rangle$.

☑

Now we want to obtain the structure of cyclic codes over R. First we remind the following lemma that gives the structure of cyclic codes over $\mathbb{F}_q$.

Lemma 4.2. *Let C be a nonzero cyclic code over $\mathbb{F}_q$ of length n. There exists a polynomial $g(x) \in C$ with the following properties:*

(1) $p(x)$ is the unique monic polynomial of minimum degree in C,

(2) $C = \langle p(x) \rangle$, and

(3) $p(x) | (x^n - 1)$.

(4) $|C| = q^{n - \deg p(x)}$.

(5) If $\ell(x) = (x^n - 1)/p(x)$ then $C^{\perp} = \langle \ell^{\star}(x) \rangle$ where $\ell^{\star}(x)$ is the reciprocal polynomial of $\ell(x)$.

(6) C contains its dual code if and only if $(x^n - 1) \equiv 0 \mod p(x)p^{\star}(x)$, where $p^{\star}(x)$ is the reciprocal polynomial of $p(x)$.

Proof. Parts 1, 2, 3 and 4 follow from Theorem 4.2.1 in [6]. Item 5 follows from Theorem 5.6 in [8]. We have Part 6 by Lemma 8 in [5]. ☑

Now let

$$\overline{\psi_i} : \mathbb{F}_q[x]/\langle x^n - 1\rangle \to R_i[x]/\langle 1_{R_i}x^n - 1_{R_i}\rangle$$

and

$$\overline{\varphi_i} : R_i[x]/\langle 1_{R_i}x^n - 1_{R_i}\rangle \to Re_i[x]/\langle e_i x^n - e_i\rangle$$

be the natural extension of isomorphisms ψ_i and φ_i in Lemma 3.2. It easy to see that $\overline{\varphi_i}$ and $\overline{\psi_i}$ are isomorphisms of rings. The following theorem gives the structure of cyclic codes over R.

Theorem 4.3. *(1) C is an ideal of $R[x]/\langle x^n - 1\rangle$ if and only if*

$$\varphi(C) = \overline{\varphi_i}\,\overline{\psi_i}(C_1) \times \cdots \times \overline{\varphi_i}\,\overline{\psi_i}(C_m),$$

where C_i is a cyclic code over $\mathbb{F}_q$ of length n; C_i is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

(2) If $C_i = \langle \overline{p_i(x)}\rangle$ for $i = 1, \ldots, m$, then

$$C = \langle \overline{p_1(x)e_1 + \cdots + p_m(x)e_m}\rangle.$$

In this case $|C| = q^{mn - \sum_{i=1}^{m} \deg(p_i(x))}$.

(3) If $\ell_i(x) = (x^n - 1)/p_i(x)$ for $i = 1, \ldots, m$, then

$$C^{\perp} = \langle \overline{\ell_1^{\star}(x)e_1 + \cdots + \ell_m^{\star}(x)e_m}\rangle$$

where $\ell_i^{\star}(x)$ is the reciprocal polynomial of $\ell_i(x)$.

(4) $R[x]/\langle x^n - 1\rangle$ is a principal ideal ring.

Proof. (1) Since $\overline{\varphi_i}$ and $\overline{\psi_i}$ are isomorphisms of rings, it follows from Theorem 4.1.2.

(2) It is easy to see that

$$\overline{\varphi_i}\,\overline{\psi_i}(\overline{p_i(x)}) = \overline{p_i(x)e_i}.$$

Hence

$$\overline{\varphi_i}\,\overline{\psi_i}(C_i) = \overline{\varphi_i}\,\overline{\psi_i}(\langle \overline{p_i(x)}\rangle) = \langle \overline{\varphi_i}\,\overline{\psi_i}(\overline{p_i(x)})\rangle = \langle \overline{p_i(x)e_i}\rangle.$$

Now by Theorem 4.1.3,

$$C = \langle \overline{p_1(x)e_1 + \cdots + p_m(x)e_m}\rangle.$$

By Lemma 4.2.4, $|C_i| = q^{n - \deg p_i(x)}$. Hence

$$|C| = \prod_{i=1}^{m} |C_i| = q^{mn - \sum_{i=1}^{m} \deg(p_i(x))}.$$

(3) Consider the isomorphisms

$$\pi : R^n \to \frac{R[x]}{\langle x^n - 1\rangle}$$

and

$$\pi_i : (Re_i)^n \to \frac{Re_i[x]}{\langle e_i x^n - e_i\rangle}.$$

Let $C = \pi(C')$ and $C_i = \pi_i(C'_i)$, where $C' \subseteq R^n$ and $C'_i \subseteq (Re_i)^n$. By these correspondences, C and C' have the same dual as linear codes. Also C_i and C'_i have the same dual. Denote the dual of these linear codes by $C^\perp$, $C'^\perp$, $C_i^\perp$ and $C_i'^\perp$. It is easy to see that

$$C'^\perp = \varphi_1\psi_1(C_1'^\perp) \oplus \cdots \oplus \varphi_m\psi_m(C_m'^\perp)$$

if and only if

$$\varphi(C^\perp) = \overline{\varphi_1}\,\overline{\psi_1}(C_1^\perp) \times \cdots \times \overline{\varphi_m}\,\overline{\psi_m}(C_m^\perp).$$

But by Lemma 4.2.5, $C_i^\perp = \langle\overline{\ell_i^\star(x)}\rangle$. Hence by Item 2,

$$C^\perp = \langle\overline{\ell_1^\star(x)e_1 + \cdots + \ell_m^\star(x)e_m}\rangle.$$

(4) By Lemma 3.2, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is a principal ideal ring. So by Part 2, $R[x]/\langle x^n - 1\rangle$ is a principal ideal ring.

☑

Theorem 4.4. *Let*

$$C = \langle\overline{p_1(x)e_1 + \cdots + p_m(x)e_m}\rangle$$

be a cyclic code of length n over R. Then $C^\perp \subseteq C$ if and only if for any $i = 1, \ldots, m$ we have that

$$(x^n - 1) \equiv 0 \mod p_i(x)p_i^\star(x).$$

Proof. By above theorem $\varphi(C) = \overline{\varphi_1}\,\overline{\psi_1}(C_1) \times \cdots \times \overline{\varphi_m}\,\overline{\psi_m}(C_m)$, where $C_i = \langle\overline{p_i(x)}\rangle$. Clearly

$$\begin{aligned}\varphi(C^\perp) &= \overline{\varphi_1}\,\overline{\psi_1}(C_1^\perp) \times \cdots \times \overline{\varphi_m}\,\overline{\psi_m}(C_m^\perp) \subseteq \varphi(C)\\ &= \overline{\varphi_1}\,\overline{\psi_1}(C_1) \times \cdots \times \overline{\varphi_m}\,\overline{\psi_m}(C_m)\end{aligned}$$

if and only if

$$\overline{\varphi_i}\,\overline{\psi_i}(C_i^\perp) \subseteq \overline{\varphi_i}\,\overline{\psi_i}(C_i),$$

for $i = 1, \ldots, m$. Hence $C^\perp \subseteq C$ if and only if $C_i^\perp \subseteq C_i$ for $i = 1, \ldots, m$. But by Lemma 4.2.6, $C_i^\perp \subseteq C_i$ if and only if $(x^n - 1) \equiv 0 \mod p_i(x)p_i^\star(x)$. This completes the proof. ☑

Theorem 4.5. *Let $C = \langle \overline{p_1(x)e_1 + \cdots + p_m(x)e_m} \rangle$ be a cyclic code of length n over R with $d_L(C) = d$. If $(x^n - 1) \equiv 0 \mod p_i(x)p_i^\star(x)$ for $i = 1, \ldots, m$, then there exists a quantum error-correcting code over $\mathbb{F}_q$ with the following parameters*

$$[[mn, mn - 2\sum_{i=1}^{m} \deg(p_i(x)), d]].$$

Proof. By Theorem 4.4, $C^\perp \subseteq C$. Also $|C| = q^{mn - \sum_{i=1}^{m} \deg(p_i(x))}$ by Theorem 4.3.2. Apply the gray map ϕ on C. Then $\phi(C)$ is an

$$[mn, mn - \sum_{i=1}^{m} \deg(p_i(x)), d]$$

linear code over $\mathbb{F}_q$. Now by Proposition 2.2, we have the result. ☑

Example 4.6. Let $R = \mathbb{F}_7[y]/\langle y^3 - 1 \rangle$ and $n = 7$. Then $x^7 - 1 = (x-1)^7$ over $\mathbb{F}_7$. Consider the polynomials $p_1(x) = x - 1$, $p_2(x) = (x-1)^2$ and $p_3(x) = (x-1)^3$. Let

$$C = \langle \overline{p_1(x)e_1 + p_2(x)e_2 + p_3(x)e_3} \rangle.$$

By Theorem 3.5.4 and Theorem 4.32, it is easy to see that C is a $(7, 7^{15}, 2)$ cyclic code over R. By Theorem 4.4, $C^\perp \subseteq C$. Now by Theorem 4.5 there exists a quantum error-correcting code with parameters $[[21, 9, 2]]$ over $\mathbb{F}_7$.

Example 4.7. Let $R = \mathbb{F}_{11}[y]/\langle y^5 - 1 \rangle$ and $n = 11$. Then $x^{11} - 1 = (x-1)^{11}$ over $\mathbb{F}_{11}$. Consider the polynomials $p_1(x) = p_2(x) = (x-1)^4$ and $p_3(x) = p_4(x) = p_5(x) = (x-1)^5$. Let $C = \langle \overline{\sum_{i=1}^{5} p_i(x)e_i} \rangle$. Then C is a $(11, 11^{32}, 5)$ cyclic code over R where $C^\perp \subseteq C$. So there exists a quantum error-correcting code with parameters $[[55, 9, 5]]$ over $\mathbb{F}_{11}$.

Example 4.8. Let $R_m = \mathbb{F}_{13}[y]/\langle y^m - 1 \rangle$ where $m \in \{2, 3, 4, 6\}$. Then

$$x^8 - 1 = (x+1)(x+5)(x+8)(x+12)(x^2+5)(x^2+8)$$

over $\mathbb{F}_{13}$. We obtain some quantum error-correcting codes from cyclic codes over R_m.

(1) Let $m = 2$, $p_1(x) = (x+8)(x^2+8)$ and $p_2(x) = (x+5)(x^2+5)$. Then

$$C = \langle \overline{\sum_{i=1}^{2} p_i(x)e_i} \rangle$$

is a $(8, 13^{10}, 3)$ cyclic code over R where $C^\perp \subseteq C$. Thus we have a quantum error-correcting code with parameters $[[16, 4, 3]]$ over $\mathbb{F}_{13}$.

(2) Let $m = 3$, $p_1(x) = x + 8$, $p_2(x) = x^2 + 8$ and $p_3(x) = x^2 + 5$. Then

$$C = \overline{\langle \sum_{i=1}^{3} p_i(x)e_i \rangle}$$

is a $(8, 13^{19}, 2)$ cyclic code over R where $C^{\perp} \subseteq C$, which proves the existing of a quantum error-correcting code with parameters $[[24, 14, 2]]$ over $\mathbb{F}_{13}$.

(3) Let $m = 4$,

$$p_1(x) = p_2(x) = (x + 8)(x^2 + 8)$$

and

$$p_3(x) = p_4(x) = (x + 5)(x^2 + 5).$$

Then $C = \overline{\langle \sum_{i=1}^{4} p_i(x)e_i \rangle}$ is a $(32, 13^{20}, 3)$ cyclic code over R where $C^{\perp} \subseteq C$. Therefore there exists a quantum error-correcting code with parameters $[[32, 8, 3]]$ over $\mathbb{F}_{13}$.

(4) Let $m = 6$,

$$\begin{aligned} p_1(x) &= (x + 8), \\ p_2(x) &= (x + 5), \\ p_3(x) = p_4(x) &= (x^2 + 8), \\ p_5(x) = p_6(x) &= (x^2 + 5). \end{aligned}$$

Then

$$C = \overline{\langle \sum_{i=1}^{6} p_i(x)e_i \rangle}$$

is a $(48, 13^{38}, 2)$ cyclic code over R where $C^{\perp} \subseteq C$. Hence there exists a quantum error-correcting code with parameters $[[48, 28, 2]]$ over $\mathbb{F}_{13}$.

References

[1] M. Ashraf and G. Mohammad, *Quantum codes from cyclic codes over* $f_3 + vf_3$, Int. J. Quantum Inform. **12** (2014), no. 6, 1450042.

[2] J. Bierbrauer and Y. Edel, *Quantum twisted codes*, J. Combin. Des. **8** (2000), 174–188.

[3] 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. **IT-44** (1998), 1369–1387.

[4] A. Dertli, Y. Cengellenmis, and S. Eren, *Quantum codes over the ring* $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^m\mathbb{F}_2$, Int. J. Algebra. **9** (2015), no. 3, 115 – 121.

[5] J. Gao, *Quantum codes from cyclic codes over* $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, Int. J. Quantum Inform. **13** (2015), no. 8, 1550063.

[6] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[7] J. Qian, *Quantum codes from cyclic codes over* f_2+vf_2, J. Inform. Comput. Sci. **10** (2013), no. 6, 1715–1722.

[8] K. Samei and S. Mahmoudi, *Cyclic r-additive codes*, Discrete Math. **340** (2017), 1657–1668.

[9] M. Sari and I. Siap, *Quantum codes from cyclic codes over a class of nonchain rings*, Bull. Korean Math. Soc., http://dx.doi.org/10.4134/BKMS.b150544 pISSN: 1015-8634 / eISSN: 2234-3016, 2017.

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

(Recibido en mayo de 2021. Aceptado en mayo de 2022)

Mathematical Sciences and Statistics
Malayer University, Malayer, Iran
e-mail: shmehry@malayeru.ac.ir