

## QUANTUM CODES FROM CYCLIC CODES OVER

$$\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$$

HU Peng, LI Hui, LIU Xiu-sheng

(*School of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, China*)

**Abstract:** In this paper, we investigate the method of constructing quantum codes from cyclic codes over the ring  $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$  ( $u^2 = u, v^2 = v, uv = vu = 0$ ). By means of the generator polynomials and some decomposition of cyclic codes and their dual over  $R$ , we give a necessary and sufficient condition of the cyclic codes over  $R$  to be construct the quantum codes. Also as an application, we obtain new non binary quantum codes from those classes of cyclic codes.

**Keywords:** cyclic codes; quantum codes; dual codes

**2010 MR Subject Classification:** 94B15; 11T71

**Document code:** A                    **Article ID:** 0255-7797(2021)02-0101-08

### 1 Introduction

Quantum error-correcting codes play an important role in quantum communications and quantum computations. After the pioneering work in [1–4], the theory of quantum codes has developed rapidly in recent years. As we know, the approach of constructing new quantum codes which have good parameters is an interesting research field. However, obtaining the parameters of the new quantum codes, especially the new good quantum codes, is a difficult problem. Recently, a lot of new quantum codes have been constructed by classical linear codes with Hermitian dual containing, which can be found in [5–10].

Cyclic codes over finite rings are an important class of codes from both a theoretical and a practical viewpoint. It has been shown that certain good quantum codes could be found as images of linear codes over some special rings under the Gray map (see[11]). In [12], Kai and Zhu established a construction for quantum codes from cyclic codes of odd length over finite chain ring  $\mathbb{F}_4 + u\mathbb{F}_4$ , where  $u^2 = 0$ . Qian et al. in [13] gave a new method of constructing quantum codes from cyclic codes of odd length over finite ring  $\mathbb{F}_2 + v\mathbb{F}_2$ , where  $v^2 = v$ . Motivated by two papers above, we study quantum codes from cyclic codes over  $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$  where  $u^2 = u, v^2 = v, uv = vu = 0$ , and  $q = p^t$  for some prime  $p$  and positive integer  $t$ .

In this paper, let  $R$  denote the finite ring  $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$  with  $u^2 = u, v^2 = v$ , and  $uv = vu = 0$ . In Section 2, we define the Gray map  $\varphi$  from  $R$  to  $\mathbb{F}_q^3$ . Moreover, we

\* **Received date:** 2018-05-04

**Accepted date:** 2018-11-05

**Foundation item:** Supported by Research Project of Hubei Polytechnic University (17xjz03A).

**Biography:** Hu Peng (1981–), male, born at Huangshi, Hubei, associate professor, major in algebraic coding. E-mail:lh79873304@163.com.

investigate some results about linear codes over  $R$ . In Section 3, we address the relation of Hermitian dual-containing codes between  $R$  and  $\mathbb{F}_q$ . In light of the relation, we get quantum codes with new parameters over  $\mathbb{F}_q$ .

## 2 Linear Codes over $R$

The ring  $R$  is a finite commutative ring with characteristic  $p$  and it contains three maximal ideals which are

$$I_1 = \langle u, v \rangle, I_2 = \langle u - 1, v \rangle, I_3 = \langle u, v - 1 \rangle.$$

Obviously  $\frac{R}{I_1}$ ,  $\frac{R}{I_2}$ , and  $\frac{R}{I_3}$  are isomorphic to  $\mathbb{F}_q$ . i.e.,  $R \cong \mathbb{F}_q^3$ . Therefore  $R$  is a principal ideal ring, i.e.,  $R$  is a Frobenius ring.

Let  $R^n = \{\mathbf{x} = (x_1, \dots, x_n) \mid x_j \in R\}$  be  $R$ -module. A  $R$ -submodule  $C$  of  $R^n$  is called a linear code of length  $n$  over  $R$ . We assume throughout paper that all codes are linear.

Let  $\mathbf{x}, \mathbf{y} \in R^n$ , the Euclidean inner product of  $\mathbf{x}, \mathbf{y}$  is defined as the following

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + \dots + x_ny_n.$$

We call

$$C^\perp = \{\mathbf{x} \in R^n \mid \mathbf{x} \cdot \mathbf{c} = 0, \forall \mathbf{c} \in C\}$$

as the dual code of  $C$ . Notice that  $C^\perp$  is linear if  $C$  is linear or not.

In [14], it is proved that for any linear code  $C$  over a finite Frobenius ring,  $|C| \cdot |C^\perp| = R^n$ . The following concepts and results can be found in [1].

The Gray map  $\varphi : R^n \rightarrow \mathbb{F}_q^{3n}$  is defined by  $\varphi(\mathbf{x}) = (\beta(x_1), \dots, \beta(x_n))$  for  $\mathbf{x} = (x_1, \dots, x_n)$ , where  $\beta(a + ub + vc) = (a, a + b, a + c)$  for  $a + ub + vc \in R$  with  $a, b, c \in \mathbb{F}_q$ . Using this map, we can define the Lee weight  $W_L$  and Lee distance  $d_L$  as follows.

For any element  $\mathbf{x} = (x_1, \dots, x_n) \in R^n$ , we define  $W_L(\mathbf{x}) = W_H(\varphi(\mathbf{x}))$ , where  $W_H$  denotes the ordinary Hamming weight for codes over  $\mathbb{F}_q$ . The Lee distance  $d_L(\mathbf{x}, \mathbf{y})$  between two codewords  $\mathbf{x}$  and  $\mathbf{y}$  is the Lee weight of  $\mathbf{x} - \mathbf{y}$ .

**Lemma 2.1** [1] The Gray map  $\varphi$  is a distance-preserving map from  $(R^n, \text{Lee distance})$  to  $(\mathbb{F}_q^{3n}, \text{Hamming distance})$  and also  $\mathbb{F}_q$ -linear.

The following theorem is obvious.

**Theorem 2.2** [1] If  $C$  is a linear code of length  $n$  over  $R$ , size  $q^k$  and Lee distance  $d_L$ , then  $\varphi(C)$  is a linear code over  $\mathbb{F}_q$  with parameters  $[3n, k, d_L]$ .

**Theorem 2.3** [1] If  $C$  is a linear code of length  $n$  over  $R$ , then  $\varphi(C^\perp) = \varphi(C)^\perp$ . Moreover, If  $C$  is a self-dual code, so is  $\varphi(C)$ .

Let  $e_1 = 1 - u - v, e_2 = u, e_3 = v$ . It is easy to check that  $e_i e_j = \delta_{ij} e_i$  and  $\sum_{k=1}^3 e_k = 1$ , where  $\delta_{ij}$  stands for Dirichlet function, i.e.,  $\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$  According to [15], we have  $R = e_1 R \oplus e_2 R \oplus e_3 R$ .

Now, we mainly consider some familiar structural properties of linear code  $C$  over  $R$ . The proof of following results can be found in [16], so we omit them here.

Let  $A_i$  ( $i = 1, 2, 3$ ) be codes over  $R$ . We denote

$$A_1 \oplus A_2 \oplus A_3 = \{a_1 + a_2 + a_3 | a_1 \in A_1, a_2 \in A_2, a_3 \in A_3\}.$$

If  $C$  is a linear code of length  $n$  over  $R$ , we define that

$$C_1 = \{\mathbf{a} \in \mathbb{F}_q^n | \text{there are } \mathbf{b}, \mathbf{c} \in \mathbb{F}_q^n \text{ such that } e_1\mathbf{a} + e_2\mathbf{b} + e_3\mathbf{c} \in C\},$$

$$C_2 = \{\mathbf{b} \in \mathbb{F}_q^n | \text{there are } \mathbf{a}, \mathbf{c} \in \mathbb{F}_q^n \text{ such that } e_1\mathbf{a} + e_2\mathbf{b} + e_3\mathbf{c} \in C\},$$

$$C_3 = \{\mathbf{c} \in \mathbb{F}_q^n | \text{there are } \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \text{ such that } e_1\mathbf{a} + e_2\mathbf{b} + e_3\mathbf{c} \in C\}.$$

It is easy to verify that  $C_i$  ( $i = 1, 2, 3$ ) are linear codes of length  $n$  over  $\mathbb{F}_q$ . Furthermore,  $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$ , and  $|C| = |C_1| |C_2| |C_3|$ . Throughout the paper  $C_i$  ( $i = 1, 2, 3$ ) will be reserved symbols referring to these special subcodes.

According to the above definitions and [17], we have the following theorem.

**Theorem 2.4.** If  $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$  is a linear code of length  $n$  over  $R$ , then  $C^\perp = e_1C_1^\perp \oplus e_2C_2^\perp \oplus e_3C_3^\perp$ .

The next theorem gives a computation for minimum Lee distance  $d_L$  of a linear code of length  $n$  over  $R$ .

**Theorem 2.5.** If  $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$  is a linear code of length  $n$  over  $R$ , then  $d_L(C) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}$ .

**Proof** By Theorem 2.3, we have,  $d_L(C) = d_H(\varphi(C))$ .

For any codeword  $\mathbf{x}$ , it can be written as  $\mathbf{x} = e_1\mathbf{a} + e_2\mathbf{b} + e_3\mathbf{c}$ , where  $\mathbf{a} \in C_1, \mathbf{b} \in C_2, \mathbf{c} \in C_3$ . Thus,

$$\varphi(\mathbf{x}) = (\mathbf{a}, \mathbf{b}, \mathbf{c}) = (\mathbf{a}, \mathbf{0}, \mathbf{0}) + (\mathbf{0}, \mathbf{b}, \mathbf{0}) + (\mathbf{0}, \mathbf{0}, \mathbf{c}).$$

This means that  $d_L(C) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}$ .

### 3 Quantum Codes from Cyclic Codes over $R$

In this section, we assume that  $q = l^2$ , where  $l$  is a power of the prime  $p$ . Consider the involution  $\bar{\cdot} : a \rightarrow a^l$  defined on  $\mathbb{F}_{l^2}$ . For any  $r = e_1a + e_2b + e_3c \in R$ , we denote the involution on  $R$  by  $\bar{\cdot}$  defined by  $\bar{r} = e_1a^l + e_2b^l + e_3c^l$ .

For a given linear code  $C$  of length  $n$  over  $R$ , denoted by  $C^{\perp_H}$  the Hermitian dual of  $C$  defined with respect to the form  $[\mathbf{x}, \mathbf{y}]_H := \sum_{i=1}^n x_i \bar{y}_i$ , where  $\mathbf{x} = (x_1 \cdots, x_n), \mathbf{y} = (y_1 \cdots, y_n) \in R^n$ . The code  $C$  is said to be Hermitian dual-containing if  $C^{\perp_H} \subset C$ , and Hermitian self-dual if  $C^{\perp_H} = C$ .

We first recall the definition of reciprocal polynomial in  $\mathbb{F}_{l^2}[x]$ . For any polynomial  $f(x) = \sum_{i=0}^k a_i x^i$  of degree  $k$  ( $a_k \neq 0$ ) over  $\mathbb{F}_{l^2}$ , let  $f^*(x)$  denote the reciprocal polynomial of  $f(x)$  given by

$$f^*(x) = x^k f\left(\frac{1}{x}\right) = \sum_{i=0}^k a_{k-i} x^i.$$

Next, we extend the involution map to polynomials in  $\mathbb{F}_{l^2}[x]$ . For  $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  in  $\mathbb{F}_{l^2}[x]$ , we set  $\overline{f(x)} = \overline{a_0} + \overline{a_1}x + \dots + \overline{a_{n-1}}x^{n-1}$ . The conjugate reciprocal polynomial of  $f(x)$  is denoted as  $f^\dagger(x)$  and is equal to  $\overline{f^*(x)}$ .  $f(x)$  is said to be self-conjugate reciprocal if  $f(x) = f^\dagger(x)$ . Otherwise,  $f(x)$  and  $f^\dagger(x)$  form a conjugate reciprocal pair.

The following lemma is going to play an important role in constructing quantum codes.

**Lemma 3.1** Let  $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$  be a cyclic codes of length  $n$  over  $R$ .

Then  $C = \langle e_1g_1(x), e_2g_2(x), e_3g_3(x) \rangle$  and  $|C| = q^{3n - \sum_{i=1}^3 \deg g_i(x)}$ , where  $g_i(x)$  is a generator polynomial of cyclic codes  $C_i$  of length  $n$  over  $\mathbb{F}_{l^2}$  for  $i=1,2,3$ .

**Proof** Since  $C_i = \langle g_i(x) \rangle \subset \frac{\mathbb{F}_{l^2}[x]}{\langle x^n - 1 \rangle}$  for  $i = 1, 2, 3$ , and  $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$ ,  $C = \{c(x) | c(x) = e_1f_1(x) + e_2f_2(x) + e_3f_3(x), f_i(x) \in C_i, i = 1, 2, 3\}$ . Thus

$$C \subset \langle e_1g_1(x), e_2g_2(x), e_3g_3(x) \rangle.$$

On the other hand, for any

$$e_1g_1(x)r_1(x) + e_2g_2(x)r_2(x) + e_3g_3(x)r_3(x) \in \langle e_1g_1(x), e_2g_2(x), e_3g_3(x) \rangle \subset \frac{R[x]}{\langle x^n - 1 \rangle},$$

where  $r_1(x), r_2(x)$  and  $r_3(x) \in \frac{R[x]}{\langle x^n - 1 \rangle}$ , there exist  $s_1(x), s_2(x)$  and  $s_3(x) \in \mathbb{F}_{l^2}[x]$  such that  $e_1r_1(x) = e_1s_1(x), e_2r_2(x) = e_2s_2(x)$ , and  $e_3r_3(x) = e_3s_3(x)$ . Hence,

$$e_1g_1(x)r_1(x) + e_2g_2(x)r_2(x) + e_3g_3(x)r_3(x) = e_1g_1(x)s_1(x) + e_2g_2(x)s_2(x) + e_3g_3(x)s_3(x),$$

which implies that  $\langle e_1g_1(x), e_2g_2(x), e_3g_3(x) \rangle \subset C$ . Therefore,  $C = \langle e_1g_1(x), e_2g_2(x), e_3g_3(x) \rangle$ .

Similar to the proof of Theorems 2.4 and 2.5, we can prove the following two theorems.

**Theorem 3.2** Let  $C$  be a linear code of length  $n$  over  $R$ . Then

- (1)  $\varphi(C^{\perp_H}) = \varphi(C)^{\perp_H}$ ;
- (2) if  $C$  is a Hermitian self-dual code, then  $\varphi(C)$  is a Hermitian self-dual code of length  $3n$  over  $\mathbb{F}_{l^2}$ ;
- (3) if  $C$  is a Hermitian dual-containing code, then  $\varphi(C)$  is a Hermitian dual-containing code of length  $3n$  over  $\mathbb{F}_{l^2}$ .

**Theorem 3.3** Let  $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$  be a linear code of length  $n$  over  $R$ . Then

- (1)  $C^{\perp_H} = e_1C_1^{\perp_H} \oplus e_2C_2^{\perp_H} \oplus e_3C_3^{\perp_H}$ . Furthermore,  $C$  is a Hermitian self-dual code if and only if  $C_1, C_2, C_3$  are Hermitian self-dual codes over  $\mathbb{F}_{l^2}$ , and  $C$  is a Hermitian dual-containing code if and only if  $C_1, C_2, C_3$  are Hermitian dual-containing codes over  $\mathbb{F}_{l^2}$ ;
- (2) if  $C = \langle e_1g_1(x), e_2g_2(x), e_3g_3(x) \rangle$  is a cyclic codes of length  $n$  over  $R$ , where

$$C_1 = \langle g_1(x) \rangle, C_2 = \langle g_2(x) \rangle, C_3 = \langle g_3(x) \rangle$$

and

$$x^n - 1 = g_1(x)h_1(x) = g_2(x)h_2(x) = g_3(x)h_3(x)$$

in  $\mathbb{F}_{l^2}[x]$ , then

$$C^{\perp_H} = \langle e_1h_1^\dagger(x), e_2h_2^\dagger(x), e_3h_3^\dagger(x) \rangle = \langle e_1h_1^\dagger(x) + e_2h_2^\dagger(x) + e_3h_3^\dagger(x) \rangle.$$

In particular, if  $C_1, C_2$ , and  $C_3$  are Hermitian dual-containing code over  $\mathbb{F}_{l^2}$  with parameters  $[n, k_1, d_1], [n, k_2, d_2]$ , and  $[n, k_3, d_3]$ , respectively, then  $\varphi(C)$  is a Hermitian dual-containing code over  $\mathbb{F}_{l^2}$  with parameters  $[3n, k_1 + k_2 + k_3, \min\{d_1, d_2, d_3\}]$ .

It is easy to prove the following lemma.

**Lemma 3.4** Let  $C$  be a cyclic code with a generator polynomial  $g(x)$  over  $\mathbb{F}_{l^2}$ , where  $x^n - 1 = g(x)h(x)$ . Then

$$C^{\perp_H} \subset C \Leftrightarrow h(x)h^\dagger(x) \equiv 0 \pmod{x^n - 1}$$

or equivalently

$$C^{\perp_H} \subset C \Leftrightarrow x^n - 1 \equiv 0 \pmod{g(x)g^\dagger(x)}.$$

Combining Lemma 3.4 with Theorem 3.3, we have the following corollary.

**Corollary 3.5** Let  $C = \langle g(x) \rangle$  be a cyclic codes of length  $n$  over  $R$ , where

$$g(x) = e_1g_1(x) + e_2g_2(x) + e_3g_3(x), C_1 = \langle g_1(x) \rangle, C_2 = \langle g_2(x) \rangle, C_3 = \langle g_3(x) \rangle$$

and

$$x^n - 1 = g_1(x)h_1(x) = g_2(x)h_2(x) = g_3(x)h_3(x)$$

in  $\mathbb{F}_{l^2}[x]$ . Then

$$C^{\perp_H} \subset C \Leftrightarrow x^n - 1 \equiv 0 \pmod{g_i(x)g_i^\dagger(x)}, i = 1, 2, 3.$$

A  $l$ -ary quantum code  $Q$  of length  $n$  and size  $K$  is a  $K$ -dimensional subspace of the  $q^n$ -dimensional Hilbert space  $\mathbb{H} = (C^q)^{\otimes n} = C^q \otimes \cdots \otimes C^q$ . Let  $k = \log_l(K)$ . We use  $[[n, k, d]]_l$  to denote a  $l$ -ary quantum code of length  $n$  with size  $q^k$  and minimum distance  $d$ . If a quantum code has minimum distance  $d$ , then it can detect any  $d - 1$  and correct any  $\lfloor \frac{d-1}{2} \rfloor$  errors. One of the principal problems in quantum coding theory is to construct quantum codes with the best possible minimum distance. Recently, some classes of  $l$ -ary good quantum code have been found by employing the following Hermitian construction (see[3, 6, 8–11]).

**Lemma 3.6** [10] If  $C$  is a Hermitian dual-containing code over  $\mathbb{F}_{l^2}$  with parameters  $[n, k, d]$ , then there exists a  $l$ -ary  $[[n, 2k - n, \geq d]]_l$  quantum code.

Combining Theorem 3.3 with Lemma 3.6, we give the parameters of quantum codes obtained from the cyclic codes over  $R$  containing their Hermitian duals.

**Theorem 3.7** Let  $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$  be a cyclic code of length  $n$  over  $R$ , where

$$C_1 = \langle g_1(x) \rangle, C_2 = \langle g_2(x) \rangle, C_3 = \langle g_3(x) \rangle$$

and

$$x^n - 1 = g_1(x)h_1(x) = g_2(x)h_2(x) = g_3(x)h_3(x)$$

in  $\mathbb{F}_{l^2}[x]$ . If  $x^n - 1 \equiv 0 \pmod{g_i(x)g_i^\dagger(x)}, i = 1, 2, 3$ , then there exists a quantum code with the parameters  $[[3n, 3n - 2s, \geq d_L]]_l$ , where  $s = \sum_{i=1}^3 \deg g_i(x)$  and  $d_L$  is the minimum Lee distance of the code  $C$ .

Using Theorem 3.7, we give some new quantum codes.

**Example 1** In  $\mathbb{F}_4$ ,

$$x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Let  $g_1(x) = g_2(x) = g_3(x) = x^3 + x + 1$ . Then, by Theorem 3.7 and a computer programme, we get a  $[[21, 3, \geq 3]]_2$  quantum code.

**Example 2** In  $\mathbb{F}_9$ ,

$$x^{13} - 1 = (x + 2)(x^3 + 2x + 2)(x^3 + x^2 + 2)(x^3 + x^2 + x + 2)(x^3 + 2x^2 + 2x + 2).$$

Let  $g_1(x) = g_2(x) = g_3(x) = x^3 + x^2 + x + 2$ . Then, by Theorem 3.7 and a computer programme, we get a  $[[39, 15, \geq 3]]_3$  quantum code.

The following result can be found in [12].

**Lemma 3.8** Let  $l$  be an odd prime power. Then

- (1) If  $l \equiv 1 \pmod{4}$ , there exists a Hermitian dual-containing code over  $\mathbb{F}_{l^2}$  with parameters  $[l^2 + 1, l^2 - d + 2, d]$ , where  $2 \leq d \leq l + 1$  is even;
- (2) There exists a Hermitian dual-containing code over  $\mathbb{F}_{l^2}$  with parameters

$$\left[ \frac{l^2 + 1}{2}, \frac{l^2 + 1}{2} - d + 1, d \right],$$

where  $3 \leq d \leq l$  is odd.

By Theorem 3.3, we can immediately get the following lemma:

**Lemma 3.9** Let  $l$  be an odd prime power. Then

- (1) If  $l \equiv 1 \pmod{4}$ , then there exists a Hermitian dual-containing code over  $\mathbb{F}_{l^2}$  with parameters  $[3l^2 + 3, 3l^2 - 3d + 6, d]$ , where  $2 \leq d \leq l + 1$  is even;
- (2) There exists a Hermitian dual-containing code over  $\mathbb{F}_{l^2}$  with parameters

$$\left[ \frac{3(l^2 + 1)}{2}, \frac{3(l^2 + 1)}{2} - 3d + 3, d \right],$$

where  $3 \leq d \leq l$  is odd.

Then by Lemmas 3.6 and 3.9, we have the following theorem.

**Theorem 3.10.** Let  $l$  be an odd prime power. Then

- (1) If  $l \equiv 1 \pmod{4}$ , then there exists a  $l$ -ary  $[[3l^2 + 3, 3l^2 - 6d + 9, \geq d]]_l$  quantum code, where  $2 \leq d \leq l + 1$  is even;
- (2) There exists a  $l$ -ary

$$\left[ \left[ \frac{3(l^2 + 1)}{2}, \frac{3(l^2 + 1)}{2} - 6d + 6, \geq d \right] \right]_l$$

quantum code, where  $3 \leq d \leq l$  is odd.

In Table 1, we list some quantum codes obtained from Theorem 3.10. The table shows that our quantum codes have new parameters compared with the previous quantum codes available (see [18]).

Figure 1: Quantum codes comparison

new quantum codes
$[[15, 3, \geq 3]]_3$
$[[246, 240, \geq 2]]_9$
$[[246, 228, \geq 4]]_9$
$[[246, 216, \geq 6]]_9$
$[[246, 204, \geq 8]]_9$
$[[246, 192, \geq 10]]_9$
$[[123, 111, \geq 3]]_9$
$[[123, 99, \geq 5]]_9$
$[[123, 87, \geq 7]]_9$
$[[123, 75, \geq 9]]_9$

## 4 Conclusion

We have developed a new method of constructing quantum codes from cyclic codes over finite ring  $R$ . Using this method, we have constructed new quantum codes. We believe that cyclic codes over finite ring  $R$  will be a good source for constructing new quantum codes. In a future work, we will use the computer algebra system MAGMA to find more new quantum codes.

## References

- [1] Aly S A, Klappenecker A, Sarvepalli P K. On quantum and classical BCH codes[J]. IEEE Trans. Inf. Theory, 2007, 53(3): 1183–1188.
- [2] Calderbank A R, Rains E M, Shor P W, Sloane N J A. Quantum error correction via codes over  $GF(4)$ [J]. IEEE Trans. Inf. Theory, 1998, 44(4): 1369–1387.
- [3] Ketkar A, Klappenecker A, Kumar S, Sarvepalli P K. Nonbinary quantum stabilizer codes over finite fields[J]. IEEE Trans. Inf. Theory, 2006, 52(11): 4735–4914.
- [4] Steane A M. Simple quantum error correcting codes[J]. Phys. Rev. A, 1996, 54(6): 4741–4751.
- [5] Ashikhmin A, Knill E. Nonbinary quantum stabilizer codes[J]. IEEE Trans. Inf. Theory, 2001, 47(7): 3065–3072.
- [6] Chen B, Ling S, Zhang G. Application of constacyclic codes to quantum MDS codes[J]. IEEE Trans. Inf. Theory, 2015, 61(3): 1474–1484.
- [7] Jin L, Xing C. A construction of new quantum MDS codes[J]. IEEE Trans. Inf. Theory, 2014, 60(5): 2921–2925.
- [8] Jin L, Ling S, Luo J, Xing C. Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes[J]. IEEE Trans. Inf. Theory, 2010, 56(9): 4735–4740.
- [9] Kai X, Zhu S. New quantum MDS codes from negacyclic codes[J]. IEEE Trans. Inf. Theory, 2013, 59(2): 1193–1197.
- [10] Kai X, Zhu S, Li P. Constacyclic codes and some new quantum MDS codes[J]. IEEE Trans. Inf. Theory, 2014, 60(4): 2080–2085.

- [11] Qian J, Ma W, Gou W. Quantum codes from cyclic codes over finite ring[J]. Int. J. Quantum Inform., 2009, 7(6): 1277–1283.
- [12] Kai X, Zhu S. Quaternary construction of quantum codes from cyclic codes over  $\mathbb{F}_4 + u\mathbb{F}_4$ [J]. Int. J. Quantum Inform., 2011, 60(2): 689–700.
- [13] Qian J. Quantum codes from cyclic codes over  $F_2 + vF_2$ [J]. J. Inform. Comput. Sci., 2013, 10(6): 1715–1722.
- [14] Wood J. Duality for modules over finite rings and applications to coding theory[J]. Amer. J. Math., 1999, 121(3): 555–575.
- [15] Anderson F W, Fuller K R. Rings and categories of modules[M]. Springer, 1992.
- [16] Liu X S. On complementary-dual constacyclic codes over  $F_q + vF_q$ [J]. J. Math., 2017, 37(4): 916–924.
- [17] Zhan Y T. Research on constacyclic codes over some classes of finite non-chain ring[D]. Anhui: Hefei University, 2013.
- [18] Edel Y. Some good quantum twisted codes[EB/OL]. <http://www.mathi.uni-heidelberg.de/yves/Matritzen/QT BCH/QT BCHIndex.html>.

## 环 $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ 上的循环码和量子码

胡 鹏, 李 慧, 刘修生

(湖北理工学院数理学院, 湖北 黄石 453000)

**摘要:** 本文研究了环  $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$  ( $u^2 = u, v^2 = v, uv = vu = 0$ ) 上的循环码构造量子码的方法. 利用环  $R$  上循环码的分解与生成多项式, 给出了  $R$  上一个循环码可以构造量子码的一个充要条件. 作为这类循环码的应用, 得到了新的非二元量子码.

**关键词:** 循环码; 量子码; 对偶码

MR(2010)主题分类号: 94B15; 11T71

中图分类号: O157.4