AAECC (2019) 30:161–174
https://doi.org/10.1007/s00200-018-0366-y

ORIGINAL PAPER

Quantum codes from cyclic codes over the ring $\mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$

Yun Gao[1] · Jian Gao[2] · Fang-Wei Fu[1]

Received: 11 February 2018 / Accepted: 16 July 2018 / Published online: 21 July 2018

Abstract
Let $R = \mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$, where q is a power of a prime, $v_i^2 = v_i,\ v_iv_j = v_jv_i = 0$ for $1 \leq i, j \leq r$ and $r \geq 1$. In this paper, the structure of cyclic codes over the ring R is studied and a Gray map ϕ from R^n to $\mathbb{F}_q^{(r+1)n}$ is given. We give a construction of quantum codes from cyclic codes over the ring R. We derive Euclidean dual containing codes over $\mathbb{F}_q$ and Hermitian dual containing codes over $\mathbb{F}_{p^{2m}}$ as Gray images of cyclic codes over R. In particular, we use $r + 1$ codes associated with a cyclic code over R of arbitrary length to determine the parameters of the corresponding quantum code. Furthermore, some new non-binary quantum codes are obtained.

Keywords Quantum codes · Cyclic codes · Dual containing codes · Gray map

1 Introduction

Quantum error-correcting codes were used in quantum communication and quantum computation to protect quantum information from errors due to the decoherence and other quantum noise. Quantum error-correcting codes provided an efficient way to overcome decoherence. After the great discovery in [7,25], the construction of quantum error-correcting codes from classical cyclic codes and their generalizations over the finite field $\mathbb{F}_q$ has developed rapidly.

✉ Jian Gao
dezhougaojian@163.com ; jiangao@mail.nankai.edu.cn

Yun Gao
gaoyun2014@126.com

Fang-Wei Fu
fwfu@nankai.edu.cn

[1] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China

[2] School of Mathematics and Statistics, Shandong University of Technology, Zibo 255091, China

Cyclic codes form an important class of linear codes due to their good algebraic structures in coding theory and decoding theory. There are some papers on quantum codes construction from cyclic codes (see [1–4,10,15–18,21–23]).

The study of coding theory over finite commutative rings was first started in 1970s. Hammons et al. [12] proved that important families of binary non-linear codes were in fact images under a Gray map of linear codes over $\mathbb{Z}_4$. Codes over finite commutative rings have been developed rapidly after the study of Hammons et al., such as [1–3,8,10,11,15,21,24].

As an application, codes over finite commutative rings can be used to construct quantum codes. Qian et al. [23] provided a construction for quantum error-correcting codes starting from cyclic codes over finite chain ring $\mathbb{F}_2+u\mathbb{F}_2$, where $u^2=0$. Later, a construction of quantum codes from cyclic codes of odd length over finite chain ring $\mathbb{F}_4+u\mathbb{F}_4$ was given by Kai and Zhu [15]. In [24], Qian presented a new method of constructing quantum codes from cyclic codes over finite non-chain ring $\mathbb{F}_2+v\mathbb{F}_2$, where $v^2=v$. Motivated by [24], Ashraf and Mohammad [1] gave a construction of quantum codes from cyclic codes over finite non-chain ring $\mathbb{F}_3+v\mathbb{F}_3$, where $v^2=1$. Furthermore, quantum codes from cyclic codes over finite non-chain rings $\mathbb{F}_p+v\mathbb{F}_p$ [2] and $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$ with $u^2=u$, $v^2=v$, $uv=vu$ [3] were also studied by Ashraf and Mohammad. Gao [10] investigated quantum codes from cyclic codes over the 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, $3|(p-1)$ and $v^4=v$. Further, u-constacyclic codes over $\mathbb{F}_p+u\mathbb{F}_p$ with $u^2=1$ and their applications of constructing new non-binary quantum codes were studied by Gao and Wang. Recently, Özen et al. [21] established a construction for quantum codes from cyclic codes over finite non-chain ring $\mathbb{F}_3+u\mathbb{F}_3+v\mathbb{F}_3+uv\mathbb{F}_3$, where $u^2=1$, $v^2=1$ and $uv=vu$. At the same time, Dertli et al. [8] studied the structure of cyclic and quasi-cyclic codes over the finite ring $\mathbb{F}_2+v_1\mathbb{F}_2+\cdots+v_r\mathbb{F}_2$, where $v_i^2=v_i,\ \ v_iv_j=v_jv_i=0$ for $1\le i,j\le r$ and $r\ge 1$.

In this paper, motivated by the previous work [8,21], we study quantum codes construction from cyclic codes over the finite ring $\mathbb{F}_q+v_1\mathbb{F}_q+\cdots+v_r\mathbb{F}_q$, where $v_i^2=v_i,\ \ v_iv_j=v_jv_i=0$ for $1\le i,j\le r$ and $r\ge 1$.

The paper is organized as follows. In Sect. 2, the structure of cyclic codes $\mathbf{C}$ over the ring R is studied and a Gray map ϕ from R^n to $\mathbb{F}_q^{(r+1)n}$ is given. Furthermore, the relationship between $\mathbf{C}$ and $\phi(\mathbf{C})$ is studied. Section 3 gives a method to derive Euclidean dual containing codes over $\mathbb{F}_q$ as Gray images of cyclic codes over R. A necessary and sufficient condition for cyclic codes over R to be Euclidean dual containing is presented. From these linear codes, we obtain some new non-binary quantum codes. A construction of Hermitian dual containing codes over $\mathbb{F}_{p^{2m}}$ as Gray images of cyclic codes over R is introduced in Sect. 4. Some new non-binary quantum codes are obtained.

2 Cyclic codes over the finite ring $\mathbb{F}_q+v_1\mathbb{F}_q+\cdots+v_r\mathbb{F}_q$

In this section, we study the structure of cyclic codes over the ring R and give a Gray map ϕ from R^n to $\mathbb{F}_q^{(r+1)n}$. Furthermore, the relationship between $\mathbf{C}$ and $\phi(\mathbf{C})$ is studied, where $\mathbf{C}$ is a linear code of length n over R. The notations $\mathbf{C}$ and C denote codes over rings and fields, respectively, in the whole paper.

Let $\mathbb{F}_q$ be a finite field of cardinality q, where q is a power of a prime. Let $R = \mathbb{F}_q[v_1, v_2, \dots, v_r]\big/\big\langle v_i^2 - v_i, v_i v_j = v_j v_i = 0\big\rangle = \mathbb{F}_q + v_1\mathbb{F}_q + \cdots + v_r\mathbb{F}_q$, where $1 \leq i, j \leq r$ and $r \geq 1$. It is clear that R is a finite commutative ring with q^{r+1} elements. This ring is a semi-local ring. There are $r+1$ maximal ideals of R. For any element α of R, we have $\alpha = \alpha_0 + \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r$, where $\alpha_i \in \mathbb{F}_q$ for $0 \leq i \leq r$. By the Chinese Remainder Theorem, we have that any element $\alpha \in R$ can be expressed uniquely as

$$\alpha = (1 - v_1 - v_2 - \cdots - v_r)\beta_0 + \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_r v_r,$$

where $\beta_0, \beta_1, \dots, \beta_r \in \mathbb{F}_q$.

Let R^n be the set of n-tuples over R, i.e., $R^n = \{(c_0, c_1, \dots, c_{n-1}) | c_i \in R,\ i = 0, 1, \dots, n-1\}$, where n is a positive integer. A linear code $\mathbf{C}$ of length n over R is defined to be an R-submodule of R^n. For a linear code $\mathbf{C}$ of length n over R, if it is invariant with respect to the cyclic shift operator σ, which maps the element $(c_0, c_1, \dots, c_{n-1})$ of R^n to the element $(c_{n-1}, c_0, \dots, c_{n-2})$, then we call $\mathbf{C}$ a cyclic code. Let $\mathbf{C}$ be a cyclic code of length n over R. It is not difficult to see that $\mathbf{C}$ is an ideal of $\mathcal{R} = R[x]\big/\langle x^n - 1\rangle$.

Let $\mathbf{C}$ be a linear code of length n over R. Let $e_0 = 1 - v_1 - v_2 - \cdots - v_r$, $e_1 = v_1$, …, $e_r = v_r$. It is not difficult to verify that $e_i e_j = 0$ for $i \neq j$, $e_i e_i = e_i$ and $e_0 + e_1 + \cdots + e_r = 1$ in R, where $i = 0, 1, \dots, r$. This implies that e_i is an idempotent in R and $R = e_0 R \oplus e_1 R \oplus \cdots \oplus e_r R = e_0 \mathbb{F}_q \oplus e_1 \mathbb{F}_q \oplus \cdots \oplus e_r \mathbb{F}_q$. Then $\mathbf{C}$ can be uniquely expressed as

$$\mathbf{C} = e_0 C_0 + e_1 C_1 + \cdots + e_r C_r, \tag{1}$$

where $C_0, C_1, \dots, C_r$ are linear codes of length n over $\mathbb{F}_q$.

For any $a = a_0 + a_1 v_1 + \cdots + a_r v_r = e_0 a(0) + e_1 a(1) + \cdots + e_r a(r) \in R$, we identify the element a with the vector $\mathbf{a}$, i.e., $\mathbf{a} = (a(0), a(1), \dots, a(r))$. Let $GL_{r+1}(\mathbb{F}_q)$ be the set of all $(r+1) \times (r+1)$ invertible matrices over $\mathbb{F}_q$. We define a Gray map

$$\begin{aligned} &\phi :\ R \to \mathbb{F}_q^{r+1} \\ &\mathbf{a} = (a(0), a(1), \dots, a(r)) \mapsto (a(0), a(1), \dots, a(r))M, \end{aligned}$$

where $M \in GL_{r+1}(\mathbb{F}_q)$. Clearly, ϕ is an $\mathbb{F}_q$-module isomorphism. For simplicity, we abbreviate the vector $(a(0), a(1), \dots, a(r))M$ as $\mathbf{a}M$ in the rest of this paper. Similarly, the Gray map ϕ can be extended to map from R^n to $\mathbb{F}_q^{(r+1)n}$ as follows

$$\begin{gathered} \phi :\ R^n \to \mathbb{F}_q^{(r+1)n} \\ (\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{n-1}) \mapsto (\mathbf{a}_0 M, \mathbf{a}_1 M, \dots, \mathbf{a}_{n-1} M). \end{gathered}$$

For any element $\mathbf{a} = (a(0), a(1), \dots, a(r)) \in R$, we denote the Hamming weight $wt_H(\mathbf{a}M)$ of $\mathbf{a}M$ as the Gray weight of $\mathbf{a}$, i.e., $wt_G(\mathbf{a}) = wt_H(\mathbf{a}M)$. The Gray weight of any element $(\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{n-1}) \in R^n$ is defined to be the integral $\sum_{i=0}^{n-1} wt_G(\mathbf{a}_i)$. Let $\mathbf{C}$ be a linear code of length n over R, the Gray distance of $c_1, c_2 \in \mathbf{C}$ be defined to be $d_G(c_1, c_2) = wt_G(c_1 - c_2)$. The minimum Gray distance d_G of $\mathbf{C}$ is defined as $d_G(\mathbf{C}) = \min\{wt_G(c) | 0 \neq c \in \mathbf{C}\}$.

According to the above definitions, we have that $\phi(\mathbf{C})$ is a linear code of length $(r+1)n$ over $\mathbb{F}_q$. Furthermore, for any $c = (a_0, a_1, \ldots, a_{n-1}), c_1, c_2 \in \mathbf{C}$, we have

$$\begin{aligned} wt_G(c) &= \sum_{i=0}^{n-1} wt_G(a_i) = \sum_{i=0}^{n-1} wt_H(a_i M) = wt_H(cM), \\ d_G(c_1, c_2) &= wt_G(c_1 - c_2) = wt_H((c_1 - c_2)M) = wt_H(c_1 M - c_2 M) \\ &= d_H(c_1 M, c_2 M). \end{aligned}$$

This implies that the Gray map ϕ is a weight and distance preserving map from R^n (Gray weight or Gray distance) to $\mathbb{F}_q^{(r+1)n}$ (Hamming weight or Hamming distance).

Lemma 1 *Let $\boldsymbol{a} = (a(0), a(1), \ldots, a(r)) \in R$. Then $\boldsymbol{a}$ is a unit if and only if $a(i) \neq 0 \pmod{p}$ for $0 \leq i \leq r$.*

Proof By the Chinese Remainder Theorem, we have that $\mathbf{a}$ is a unit over $R \Longleftrightarrow a(0), a(1), \ldots, a(r)$ are units over $\mathbb{F}_q \Longleftrightarrow a(i) \neq 0 \pmod{p}$ for $0 \leq i \leq r$. The proof is completed. □

According to the decomposition (1) of $\mathbf{C}$ and the notations given above, we give an explicitly expression of C_i as follows. Define

$$C_i = \{c_i \in \mathbb{F}_q^n | \exists\, c_0, \ldots, c_{i-1}, c_{i+1}, \ldots, c_r \in \mathbb{F}_q^n,\ e_0 c_0 + e_1 c_1 + \cdots + e_r c_r \in \mathbf{C}\}$$

for any $0 \leq i \leq r$. Then C_i is a linear code of length n over $\mathbb{F}_q$ such that

$$\mathbf{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_r C_r.$$

Let G be the generator matrix of $\mathbf{C}$, then

$$G = \begin{pmatrix} e_0 G_0 \\ e_1 G_1 \\ \vdots \\ e_r G_r \end{pmatrix}, \tag{2}$$

where $G_0, G_1, \ldots, G_r$ are generator matrices of linear codes $C_1, C_2, \ldots, C_r$, respectively.

According to the above discussion, we have the following results.

Lemma 2 *Let $\mathbf{C}$ be a linear code over R with length n, dimension $\sum_{i=0}^{r} k_i$ and minimum Gray distance d_G, i.e., $\mathbf{C}$ is a $[n, \sum_{i=0}^{r} k_i, d_G]_R$ linear code, where k_i is the dimension of C_i for any $0 \leq i \leq r$. Then $\phi(\mathbf{C})$ is a $[(r+1)n, \sum_{i=0}^{r} k_i, d_G]_{\mathbb{F}_q}$ linear code.*

Proof By the definition of the map ϕ, we have $M \in GL_{r+1}(\mathbb{F}_q)$ is a $(r+1) \times (r+1)$ invertible matrix. Since all the rows of the generator matrix G (2) of $\mathbf{C}$ are linear independent, we have that the dimension of $\phi(\mathbf{C})$ is $\sum_{i=0}^{r} k_i$. Since ϕ is a weight and distance preserving map from R^n to $\mathbb{F}_q^{(r+1)n}$, we get $\phi(\mathbf{C})$ is a $[(r+1)n, \sum_{i=0}^{r} k_i, d_G]_{\mathbb{F}_q}$ linear code. □

Lemma 3 *Let $\mathbf{C} = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r$ be a linear code of length n over R. Then $\mathbf{C}$ is a cyclic code over R if and only if $C_0, C_1, \ldots, C_r$ are cyclic codes over $\mathbb{F}_q$.*

Proof Let $(c_{i,0}, c_{i,1}, \ldots, c_{i,n-1}) \in C_i$ and $c_j = \sum_{i=0}^{r} e_i c_{i,j}$ for $0 \leq j \leq n-1$. Then, we have

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathbf{C}.$$

Since $\mathbf{C}$ is a cyclic code over R, we have $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathbf{C}$. It is easy to find that

$$(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) = \sum_{i=0}^{r} e_i(c_{i,n-1}, c_{i,0}, c_{i,1}, \ldots, c_{i,n-2}).$$

By the uniqueness presentation of decomposition of linear codes over R, we get $(c_{i,n-1}, c_{i,0}, c_{i,1}, \ldots, c_{i,n-2}) \in C_i$. This implies that $C_0, C_1, \ldots, C_r$ are cyclic codes over $\mathbb{F}_q$.

Conversely, suppose that C_i is a cyclic code over $\mathbb{F}_q$ for any $0 \leq i \leq r$. Let $(c_0, c_1, \ldots, c_{n-1}) \in \mathbf{C}$, where $c_j = \sum_{i=0}^{r} e_i c_{i,j}$ for $0 \leq j \leq n-1$. Then $(c_{i,0}, c_{i,1}, \ldots, c_{i,n-1}) \in C_i$. It is easy to show that $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) = \sum_{i=0}^{r} e_i(c_{i,n-1}, c_{i,0}, c_{i,1}, \ldots, c_{i,n-2}) \in e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r = \mathbf{C}$, which follows that $\mathbf{C}$ is a cyclic code over R. □

Theorem 1 *Let $\mathbf{C} = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r$ be a cyclic code of length n over R. Then there exists a polynomial $g(x) \in R[x]$, $g(x)|(x^n - 1)$ such that $\mathbf{C} = \langle g(x) \rangle$, where $g(x) = \sum_{i=0}^{r} e_i g_i(x)$ and $g_i(x)$ is the generator polynomial of C_i for $0 \leq i \leq r$.*

Proof Let $\mathcal{C} = \langle \sum_{i=0}^{r} e_i g_i(x) \rangle$ be a cyclic code of length n over R, where $g_i(x)$ is the generator polynomial of C_i for $0 \leq i \leq r$. According to the definition of $\mathbf{C}$, we have $\mathcal{C} \subseteq \mathbf{C}$. On the other hand, since $e_iC_i = e_i\mathcal{C}$, we have $\mathbf{C} \subseteq \mathcal{C}$. Thus we get $\mathbf{C} = \mathcal{C} = \langle \sum_{i=0}^{r} e_i g_i(x) \rangle$.

By the fact that $g_i(x)$ is the generator polynomial of C_i for $0 \leq i \leq r$, we have $g_i(x)|(x^n - 1)$ in $\mathbb{F}_q[x]$. Then, there exists a polynomial $h_i(x) \in \mathbb{F}_q[x]$ such that $x^n - 1 = g_i(x)h_i(x)$ for $0 \leq i \leq r$. Furthermore, it is not difficult to verify that $\left(\sum_{i=0}^{r} e_i g_i(x)\right)\left(\sum_{i=0}^{r} e_i h_i(x)\right) = x^n - 1$. This implies that $g(x) = \sum_{i=0}^{r} e_i g_i(x)|(x^n - 1)$. □

With the notations and results above, we have the following lemma.

Lemma 4 *Let $\mathbf{C} = \langle g(x) \rangle$ be a cyclic code of length n over R, where $g(x) = \sum_{i=0}^{r} e_i g_i(x)$, $g_i(x)$ is the generator polynomial of C_i and* $\deg(g_i(x)) = t_i$ *for $0 \leq i \leq r$. Then, we have $|\mathbf{C}| = |\phi(\mathbf{C})| = q^{(r+1)n-(t_0+\cdots+t_r)}$.*

3 Quantum codes from Euclidean dual containing codes

In this section, we provide a method to derive Euclidean dual containing codes over $\mathbb{F}_q$ as Gray images of cyclic codes over R. From these linear codes, some new non-binary quantum codes are obtained.

For any $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, the Euclidean inner product is defined as

$$x \cdot y = \sum_{i=0}^{n-1} x_i y_i \tag{3}$$

For a linear code $\mathbf{C}$ of length n over R, its Euclidean dual code $\mathbf{C}^{\perp_E}$ is defined as

$$\mathbf{C}^{\perp_E} = \{x \in R^n | x \cdot c = 0 \ \forall \ c \in \mathbf{C}\}.$$

Furthermore, $\mathbf{C}$ is said to be self-orthogonal if $\mathbf{C} \subseteq \mathbf{C}^{\perp_E}$, dual containing if $\mathbf{C}^{\perp_E} \subseteq \mathbf{C}$ and self-dual if $\mathbf{C} = \mathbf{C}^{\perp_E}$.

Theorem 2 *Let $\mathbf{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_r C_r$ be a linear code of length n over R. Then*

$$\mathbf{C}^{\perp_E} = e_0 C_0^{\perp_E} \oplus e_1 C_1^{\perp_E} \oplus \cdots \oplus e_r C_r^{\perp_E} \tag{4}$$

Furthermore, $\mathbf{C}$ is Euclidean self-dual over R if and only if $C_0, C_1, \ldots, C_r$ are Euclidean self-dual over $\mathbb{F}_q$.

Proof By the decomposition (4) of $\mathbf{C}^{\perp_E}$ and the notations given above, we give a explicitly expression of $C_i^{\perp_E}$ as follows. Define

$$\mathfrak{C}_i^{\perp_E} = \{x_i \in \mathbb{F}_q^n | \exists \ x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_r \in \mathbb{F}_q^n, \ e_0 x_0 + e_1 x_1 + \cdots + e_r x_r \in C^{\perp_E}\}$$

for any $0 \le i \le r$. According to the definitions of e_i and $\mathfrak{C}_i^{\perp_E}$, we have $\mathbf{C}^{\perp_E} = e_0 \mathfrak{C}_0^{\perp_E} \oplus e_1 \mathfrak{C}_1^{\perp_E} \oplus \cdots \oplus e_r \mathfrak{C}_r^{\perp_E}$. It is obvious that $\mathfrak{C}_i^{\perp_E} \subseteq C_i^{\perp_E}$ for any $0 \le i \le r$. Let $x_i \in C_i^{\perp_E}$, for any $c_i \in C_i$, there exist $c_0, \ldots, c_{i-1}, c_{i+1}, \ldots, c_r \in \mathbb{F}_q^n$ such that $x_i \cdot (e_0 c_0 + \cdots + e_r c_r) = 0$. With the uniqueness presentation of decomposition of linear codes over R, we have $x_i \in \mathfrak{C}_i^{\perp_E}$, i.e., $C_i^{\perp_E} \subseteq \mathfrak{C}_i^{\perp_E}$. Then we get $\mathbf{C}^{\perp_E} = e_0 C_0^{\perp_E} \oplus e_1 C_1^{\perp_E} \oplus \cdots \oplus e_r C_r^{\perp_E}$.

If $C_0, C_1, \ldots, C_r$ are Euclidean self-dual over $\mathbb{F}_q$, then we have $\mathbf{C}$ is Euclidean self-dual over R. On the other hand, if $\mathbf{C}$ is Euclidean self-dual over R, then C_i is self-orthogonal, i.e., $C_i \subseteq C_i^{\perp_E}$. In fact, we have $C_i = C_i^{\perp_E}$. Otherwise, there exists an element $x_i \in C_i^{\perp_E} \backslash C_i$ and $x_j \in C_j$ for $i \neq j$ such that $(e_0 x_0 + e_1 x_1 + \cdots + e_r x_r)^2 \neq 0$. This contradicts the fact that $\mathbf{C}$ is Euclidean self-dual over R. Thus, we have $C_0, C_1, \ldots, C_r$ are Euclidean self-dual over $\mathbb{F}_q$. □

According to Lemma 3 and Theorem 2, we get the following lemma directly.

Lemma 5 *Let* $\mathbf{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_r C_r$ *be a cyclic code of length* n *over* R. *Then its Euclidean dual code* $\mathbf{C}^{\perp_E}$ *is also a cyclic code of length* n *over* R.

For any polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n, the reciprocal of $f(x)$ is defined as $f^*(x) = x^n f(x^{-1})$. Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x) \in \mathbb{F}_q[x]$ and check polynomial $h(x) = (x^n - 1)\big/g(x)$. Let $C^{\perp_E}$ be the Euclidean dual code of C. Then, according to [19, Theorem 4], we have the following result.

Lemma 6 *The Euclidean dual code* $C^{\perp_E}$ *is cyclic and has generator polynomial*

$$g^{\perp_E}(x) = x^{\deg(h(x))} h(x^{-1}) = h^*(x).$$

With the notations above, by Lemma 6, we give the ideal presentation of the Euclidean dual code $\mathbf{C}^{\perp_E}$ of $\mathbf{C}$ in the following theorem.

Theorem 3 *Let* $\mathbf{C} = \langle e_0 g_0(x) + e_1 g_1(x) + \cdots + e_r g_r(x)\rangle$ *be a cyclic code of length* n *over* R. *Then*

$$\mathbf{C}^{\perp_E} = \left\langle e_0 h_0^*(x) + e_1 h_1^*(x) + \cdots + e_r h_r^*(x)\right\rangle$$

and $|\mathbf{C}^{\perp_E}| = q^{\sum_{i=0}^{r} \deg g_i(x)}$, *where* $g_i(x)$ *is the generator polynomial of* C_i *and* $h_i(x) = (x^n - 1)\big/g_i(x)$ *for* $0 \le i \le r$.

Proof Let $C' = \left\langle e_0 h_0^*(x) + e_1 h_1^*(x) + \cdots + e_r h_r^*(x)\right\rangle$. According to the definition of the Euclidean inner product (3) and Lemma 6, it is clear that

$$\begin{aligned}&(e_0 g_0(x) + e_1 g_1(x) + \cdots + e_r g_r(x)) \cdot (e_0 h_0^*(x) + e_1 h_1^*(x) + \cdots + e_r h_r^*(x))^* \\ &= \sum_{i=0}^{r} e_i e_i^* g_i(x) h_i(x) = \sum_{i=0}^{r} e_i e_i^* (x^n - 1) = 0.\end{aligned}$$

Then, we have $C' \subseteq \mathbf{C}^{\perp_E}$. It is not difficult to show that $|C'| = q^{\sum_{i=0}^{r} \deg g_i(x)}$. As, by Lemma 4, $|\mathbf{C}| = q^{(r+1)n - \sum_{i=0}^{r} \deg g_i(x)}$, we have $|C'| = |\mathbf{C}^{\perp_E}|$. This implies that $\mathbf{C}^{\perp_E} = C'$. □

Lemma 7 *Let* $C = \langle g'(x)\rangle$ *be a cyclic code of length* n *over* $\mathbb{F}_q$ *and* $C^{\perp_E} = \langle h'^*(x)\rangle$, *where* $h'(x) = (x^n - 1)\big/g'(x)$ *in* $\mathbb{F}_q[x]$. *Then* $C^{\perp_E} \subseteq C$ *if and only if*

$$x^n - 1 \equiv 0 \pmod{h'(x)h'^*(x)}.$$

Proof If $C^{\perp_E} \subseteq C$, then we have $g'(x)|h'^*(x)$. Thus, there exists a polynomial $k(x) \in \mathbb{F}_q[x]$ such that $h'^*(x) = g'(x)k(x)$. As $h'(x)h'^*(x) = h'(x)g'(x)k(x) = (x^n - 1)k(x)$, we have $x^n - 1 \equiv 0 \pmod{h'(x)h'^*(x)}$.

If $x^n - 1 \equiv 0 \pmod{h'(x)h'^*(x)}$, then there exists a polynomial $k(x) \in \mathbb{F}_q[x]$ such that $h'(x)h'^*(x) = (x^n - 1)k(x) = g'(x)h'(x)k(x)$. This implies that $h'^*(x) \in \langle g'(x)\rangle = C$. Since $h'^*(x)$ is the generator polynomial of $C^{\perp_E}$, we have $C^{\perp_E} \subseteq C$. □

The following theorem gives a necessary and sufficient condition cyclic codes over R to be Euclidean dual containing.

Theorem 4 *Let $\mathbf{C} = \langle e_0 g_0(x), e_1 g_1(x), \ldots, e_r g_r(x)\rangle$ be a cyclic code of length n over R and $\mathbf{C}^{\perp_E} = \left\langle e_0 h_0^*(x), e_1 h_1^*(x), \cdots, e_r h_r^*(x)\right\rangle$. Then $\mathbf{C}^{\perp_E} \subseteq \mathbf{C}$ if and only if $x^n - 1 \equiv 0 \pmod{h_i(x)h_i^*(x)}$ for $0 \leq i \leq r$.*

Proof The proof process is similar to that of [8, Theorem 4.8]. □

It is not difficult to show that Euclidean dual containing cyclic codes given in Theorem 4 exist. From the Ref. [7], we have

$$x^n - 1 = \prod_i p_i(x) \prod_j q_j(x) q_j^*(x),$$

where the $p_i(x)$, $q_j(x)$ and $q_j^*(x)$ are all distinct and $p_i^*(x) = \beta p_i(x)$, β is a unit in R. Then a divisor $g(x)$ of $x^n - 1$ generates a Euclidean dual containing cyclic code if and only if $g(x)$ is divisible by each of $p_i(x)$'s and by at least one from each $q_j(x)$, $q_j^*(x)$ pair.

From the results given above, we have the following corollary directly.

Corollary 1 *Let $\mathbf{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_r C_r$ be a cyclic code of length n over R. Then $\mathbf{C}$ is Euclidean dual containing, i.e., $\mathbf{C}^{\perp_E} \subseteq \mathbf{C}$ if and only if $C_i^{\perp_E} \subseteq C_i$ for $0 \leq i \leq r$.*

Let $\mathbf{C}$ be a Euclidean dual containing code of length n over R. With the discussion above, the relationship between $\mathbf{C}$ and $\phi(\mathbf{C})$ is given as follows.

Theorem 5 *Let $\mathbf{C}$ be a Euclidean dual containing code of length n over R and $M \in GL_{r+1}(\mathbb{F}_q)$ such that $MM^T = \lambda I_{r+1}$, where M^T is the transpose of M, $\lambda \in \mathbb{F}_q^*$, I_{r+1} is a $(r+1) \times (r+1)$ identity matrix. Then $\phi(\mathbf{C})$ is a dual containing code of length $(r+1)n$ over $\mathbb{F}_q$. Furthermore, if $\mathbf{C}$ is Euclidean self-dual over R, then $\phi(\mathbf{C})$ is also Euclidean self-dual over $\mathbb{F}_q$.*

Proof For any $c = (c_0, c_1, \ldots, c_{n-1})$, $d = (d_0, d_1, \ldots, d_{n-1}) \in \phi(\mathbf{C})$, there exist $x = (x_0, x_1, \ldots, x_{n-1})$, $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbf{C}$ and $M \in GL_{r+1}(\mathbb{F}_q)$ such that $c = (x_0 M, x_1 M, \ldots, x_{n-1} M)$ and $d = (y_0 M, y_1 M, \ldots, y_{n-1} M)$. Then, we have

$$c \cdot d = cd^T = \sum_{j=0}^{n-1} x_j M M^T y_j^T = \sum_{j=0}^{n-1} x_j \lambda I_{r+1} y_j^T = \lambda \sum_{j=0}^{n-1} x_j y_j^T.$$

Due to $\mathbf{C}$ is self-orthogonal over R, it follows that $x \cdot y = \sum_{j=0}^{n-1} x_j y_j^T = 0$. This implies that $c \cdot d = 0$, i.e., $\phi(\mathbf{C})$ is a self-orthogonal code of length $(r+1)n$ over $\mathbb{F}_q$.

Let $\mathbf{C}$ be a Euclidean self-dual code of length n over R satisfying the above properties. Since ϕ is an $\mathbb{F}_q$-module isomorphism, we have $|\mathbf{C}| = |\phi(\mathbf{C})| = (q^{r+1})^{n/2} = q^{(r+1)n/2}$. Then, we have $\phi(\mathbf{C})$ is Euclidean self-dual over $\mathbb{F}_q$. □

A q-ary quantum code Q of length n and size K is a K-dimensional subspace of the q^n-dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$. Let $k = \log_q(K)$. We use $[[n, k, d]]_q$ to denote a quantum code over $\mathbb{F}_q$ with length n, dimension k and minimum Hamming distance d.

According to [13,14], we have the quantum singleton bound as follows.

Lemma 8 (Quantum Singleton Bound) *Let C be an $[[n, k, d]]_q$ quantum code. Then $k \leq n - 2d + 2$.*

A quantum code $[[n, k, d]]_q$ achieving this quantum singleton bound, i.e., $n = k + 2d - 2$, is called a quantum MDS code. The following lemmas are useful for our results.

Lemma 9 [13, Lemma 20] (CSS Construction) *Let C_1 and C_2 denote two classical linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ such that $C_2^{\perp} \leq C_1$. Then there exists an $[[n, k_1 + k_2 - n, d]]_q$ stabilizer code with minimum distance $d =$* $\min\{wt(c)|c \in (C_1\backslash C_2^{\perp}) \cup (C_2\backslash C_1^{\perp})\}$ *that is pure to $min\{d_1, d_2\}$.*

Lemma 10 [13, Corollary 21] *If C is a classical linear $[n, k, d]_q$ code containing its dual, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code that is pure to d.*

According to Corollary 1, Theorem 5 and Lemmas 8 and 9, with the notations above, we have the existence of non-binary quantum error-correcting codes as follows.

Theorem 6 *Let $\mathbf{C} = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r$ be an $[n, k, d_G]_R$ cyclic code. If $C_i^{\perp_E} \subseteq C_i$ for $0 \leq i \leq r$, then $\mathbf{C}^{\perp_E} \subseteq \mathbf{C}$ and there exists a quantum error-correcting code with parameters $[[(r + 1)n, 2k - (r + 1)n, \geq d_G]]_q$, where $k = \sum_{i=0}^{r} k_i$ and k_i is the dimension of C_i.*

Next, we give two examples to construct quantum MDS codes over finite fields $\mathbb{F}_7$ and $\mathbb{F}_{11}$.

Example 1 Let $R = \mathbb{F}_7 + v_1\mathbb{F}_7$ and $n = 3$. Then $x^3 - 1 = (x + 3)(x + 5)(x + 6)$ over $\mathbb{F}_7$. Let $g(x) = (1 - v_1)g_0(x) + v_1g_1(x)$ with $g_0 = x + 5$ and $g_1 = x + 3$. By [6] and Lemma 6, we have that $C_0 = \langle x + 5\rangle$ and $C_0^{\perp_E} = \langle 4x^2 + 2x + 1\rangle = \langle (x + 5)(4x + 3)\rangle$. Then we have $C_0^{\perp_E} \subseteq C_0$. With a similar method, we have $C_1^{\perp_E} = \langle 2x^2 + 4x + 1\rangle = \langle (x + 3)(2x + 5)\rangle \subseteq C_1 = \langle x + 3\rangle$. Let $\mathbf{C} = \langle g(x)\rangle$, according to Theorem 3 and Corollary 1, we have $\mathbf{C}^{\perp_E} \subseteq \mathbf{C}$.

Let $M = \begin{pmatrix} 6 & 2 \\ 2 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_7)$. Then we have $MM^T = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$. With the computational algebra systems Magma [6], we have that $\phi(\mathbf{C})$ is an $[6, 4, 3]$ linear code over $\mathbb{F}_7$. By Lemma 7 and Theorem 6, we obtain a quantum MDS code with parameters $[[6, 2, 3]]_7$.

Example 2 Let $R = \mathbb{F}_{11} + v_1\mathbb{F}_{11}$ and $n = 5$. Then $x^5 - 1 = (x + 2)(x + 6)(x + 7)(x + 8)(x + 10)$ over $\mathbb{F}_{11}$. Let $g(x) = (1 - v_1)g_0(x) + v_1g_1(x)$ with $g_0 = x + 6$ and $g_1 = x + 2$. Let $C = \langle g(x)\rangle$, $C_0 = \langle x + 6\rangle$ and $C_1 = \langle x + 2\rangle$. It is not difficult to verify that $C_0^{\perp_E} \subseteq C_0$ and $C_1^{\perp_E} \subseteq C_1$. By Theorem 3 and Corollary 1, we have $\mathbf{C}^{\perp_E} \subseteq \mathbf{C}$.

Table 1 New quantum codes $[[n, k, d]]_q$

n	r	$\langle g_0(x), \ldots, g_r(x)\rangle$	$\phi(\mathbf{C})$	$[[n, k, d]]_q$	$[[n', k', d']]_q$
12	2	$\langle 12, 12, 12\rangle$	$[36, 33, 2]_3$	$[[36, 30, 2]]_3$	$[[36, 28, 2]]_3$ (Ref. [21])
24	2	$\langle 12, 12, 12\rangle$	$[72, 69, 2]_3$	$[[72, 66, 2]]_3$	$[[72, 64, 2]]_3$ (Ref. [21])
20	2	$\langle 12, 12, 13\rangle$	$[60, 57, 2]_5$	$[[60, 54, 2]]_5$	$[[60, 48, 2]]_5$ (Ref. [3])
32	2	$\langle 12, 12, 12\rangle$	$[96, 93, 2]_5$	$[[96, 90, 2]]_5$	$[[96, 80, 2]]_5$ (Ref. [3])
40	2	$\langle 12, 12, 13\rangle$	$[120, 117, 2]_5$	$[[120, 114, 2]]_5$	$[[120, 112, 2]]_5$ (Ref. [3])
28	3	$\langle 12, 12, 12, 12\rangle$	$[112, 108, 2]_5$	$[[112, 104, 2]]_5$	$[[112, 64, 2]]_5$ (Ref. [3])
3	1	$\langle 15, 13\rangle$	$[6, 4, 3]_7$	$[[6, 2, 3]]_7$	MDS
56	2	$\langle 11, 16, 11\rangle$	$[168, 165, 2]_7$	$[[168, 162, 2]]_7$	$[[98, 94, 2]]_7$ (Ref. [11])
126	1	$\langle 16, 11\rangle$	$[252, 250, 2]_7$	$[[252, 248, 2]]_7$	$[[238, 234, 2]]_7$ (Ref. [11])
5	1	$\langle 16, 12\rangle$	$[10, 8, 3]_{11}$	$[[10, 6, 3]]_{11}$	MDS
11	2	$\langle 1(10), 191, 1(10)\rangle$	$[33, 29, 3]_{11}$	$[[33, 25, 3]]_{11}$	$[[24, 16, 3]]_{11}$ (Ref. [9])

Let $M = \begin{pmatrix} 10 & 2 \\ 2 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_{11})$. Then we have $MM^T = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$. Using Magma [6], we have that $\phi(\mathbf{C})$ is an [10, 8, 3] linear code over $\mathbb{F}_{11}$. By Lemma 7 and Theorem 6, we obtain a quantum MDS code with parameters $[[10, 6, 3]]_{11}$.

At the last of this section, with the methods given in Examples 1 and 2, we list some new non-binary quantum codes for $r \geq 1$ and $q \leq 11$ in Table 1. For simplicity, we list the coefficients of the polynomials in descending order in Table 1. For example, the polynomial $x^6 + x^5 + x^4 + 2x + 3$ is represented by 1110023.

4 Quantum codes from Hermitian dual containing codes

In this section, we introduce a construction of Hermitian dual containing codes over $\mathbb{F}_{p^{2m}}$ as Gray images of cyclic codes over R. Moreover, we construct some new non-binary quantum codes according to these linear codes.

Let $q = p^{2m}$, where p is a prime and m is a positive integer. In this section, we consider the ring $R = \mathbb{F}_{p^{2m}}[v_1, v_2, \ldots, v_r]/\langle v_i^2 - v_i, v_i v_j = v_j v_i\rangle = \mathbb{F}_{p^{2m}} + v_1\mathbb{F}_{p^{2m}} + \cdots + v_r\mathbb{F}_{p^{2m}}$. For any vectors $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}^n_{p^{2m}}$, their Hermitian inner product is defined as

$$\langle x, y\rangle_H = \sum_{i=0}^{n-1} x_i y_i^{p^m}.$$

Furthermore, x and y are called orthogonal with respect to the Hermitian inner product if $\langle x, y\rangle_H = 0$.

Let $\mathbf{C}$ be a linear code over R. the Hermitian dual code of $\mathbf{C}$ is defined as

$$\mathbf{C}^{\perp_H} = \{x \in R^n | \langle x, c\rangle_H = 0 \; \forall \; c \in \mathbf{C}\}.$$

$\mathbf{C}$ is called dual containing if $\mathbf{C}^{\perp_H} \subseteq \mathbf{C}$ and self-dual if $\mathbf{C} = \mathbf{C}^{\perp_H}$. For any $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbf{C}$, we denote $c^{p^m} = (c_0^{p^m}, c_1^{p^m}, \ldots, c_{n-1}^{p^m})$. Similarly, for any invertible matrix $M = (m_{ij})_{0 \leq i,j \leq r} \in GL_{r+1}(\mathbb{F}_{p^{2m}})$, denote $M^{p^m} = (m_{ij}^{p^m})_{0 \leq i,j \leq r}$.

A q^2-cyclotomic coset modulo n containing a is defined by $C_a = \{aq^{2k} (\text{mod } n) : k \geq 0\}$, where a is not necessarily the least number in C_a. The set of q^2-cyclotomic cosets modulo n is denoted by $C^{q^2,n}$. Let C be a cyclic code over $\mathbb{F}_{q^2}$. Then C is an ideal of $\mathbb{F}_{q^2}[x] / \langle x^n - 1 \rangle$ and $C = \langle g(x) \rangle$, where $g(x) | (x^n - 1)$. The defining set of C is defined as

$$Z = \{i : g(\alpha^i) = 0, 0 \leq i < n\},$$

where α is a primitive nth root of unity in some extension of $\mathbb{F}_{q^2}$.

According to [4,20], we have a necessary and sufficient condition for the existence of dual containing cyclic codes over $\mathbb{F}_{q^2}$ in the following lemma.

Lemma 11 [20, Lemma 4.1] *Assume that* $\gcd(q, n) = 1$. *A cyclic code of length n over $\mathbb{F}_{q^2}$ with defining set Z contains its Hermitian dual code if and only if $Z \cap Z^{-q} = \phi$, where $Z^{-q} = \{-qz (\text{mod } n) : z \in Z\}$.*

With the notations and properties above, we consider Hermitian dual containing cyclic codes over the ring R.

Theorem 7 *Let $\mathbf{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_r C_r$ be a cyclic code of length n over R. Then*

(i) the Hermitian dual code of $\mathbf{C}$ is

$$\mathbf{C}^{\perp_H} = e_0 C_0^{\perp_H} \oplus e_1 C_1^{\perp_H} \oplus \cdots \oplus e_r C_r^{\perp_H}.$$

Furthermore, $C_0^{\perp_H}, C_1^{\perp_H}, \ldots, C_r^{\perp_H}$ are cyclic codes of length n over $\mathbb{F}_{p^{2m}}$ and $\mathbf{C}^{\perp_H}$ is a cyclic code of length n over R.

(ii) $\mathbf{C}$ is Hermitian self-dual over R if and only if $C_0, C_1, \ldots, C_r$ are Hermitian self-dual over $\mathbb{F}_{p^{2m}}$.

Proof (i) With a similar proof process of Theorem 2, we define $\mathcal{C}_i^{\perp_H} = \{x_i \in \mathbb{F}_{p^{2m}}^n | \exists\, x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_r \in \mathbb{F}_{p^{2m}}^n,\ e_0 x_0 + e_1 x_1 + \cdots + e_r x_r \in \mathbf{C}^{\perp_H}\}$ for any $0 \leq i \leq r$. Then we have $\mathbf{C}^{\perp_H} = e_0 \mathcal{C}_0^{\perp_H} \oplus e_1 \mathcal{C}_1^{\perp_H} \oplus \cdots \oplus e_r \mathcal{C}_r^{\perp_H}$. It is not difficult to show that $C_i^{\perp_H} = \mathcal{C}_i^{\perp_H}$. Then we have

$$\mathbf{C}^{\perp_H} = e_0 C_0^{\perp_H} \oplus e_1 C_1^{\perp_H} \oplus \cdots \oplus e_r C_r^{\perp_H}.$$

Since $\mathbf{C} = e_0 C_0 \oplus e_1 C_1 \oplus \cdots \oplus e_r C_r$ is a cyclic code of length n over R, by Lemma 3, we have that C_i is cyclic code of length n over $\mathbb{F}_{p^{2m}}$ for $0 \leq i \leq r$. Then $C_i^{\perp_H}$ is a cyclic code of length n over $\mathbb{F}_{p^{2m}}$. This implies that $\mathbf{C}^{\perp_H}$ is a cyclic code of length n over R.

(ii) If $C_0, C_1, \ldots, C_r$ are Hermitian self-dual over $\mathbb{F}_{p^{2m}}$, then we have $\mathbf{C}$ is Hermitian self-dual over R. Conversely, if $\mathbf{C}$ is Hermitian self-dual over R, then C_i is self-orthogonal, i.e., $C_i \subseteq C_i^{\perp_H}$. In fact, we have $C_i = C_i^{\perp_H}$. Otherwise, there exists an element $x_i \in C_i^{\perp_H} \backslash C_i$ and $x_j \in C_j$ for $i \neq j$ such that

$$\langle (e_0x_0 + e_1x_1 + \cdots + e_rx_r), (e_0x_0 + e_1x_1 + \cdots + e_rx_r) \rangle_H \neq 0.$$

This leads to a contradiction. Then we have $C_0, C_1, \ldots, C_r$ are Hermitian self-dual over $\mathbb{F}_{p^{2m}}$. □

Theorem 8 *Let $\mathbf{C} = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r$ be a cyclic code of length n over R. Let Z_i be the defining set of C_i and $Z_i^{-p^m} = \{-p^m z_i (\text{mod } n) : z_i \in Z_i\}$ be the defining set of $C_i^{\perp_H}$ for $0 \leq i \leq r$. Then $\mathbf{C}^{\perp_H} \subseteq \mathbf{C}$ if and only if $Z_i \cap Z_i^{-p^m} = \phi$.*

Proof According to Lemma 10, if $Z_i \cap Z_i^{-p^m} = \phi$ for $0 \leq i \leq r$, then we have $C_i^{\perp_H} \subseteq C_i$. It is obvious that $e_iC_i^{\perp_H} \subseteq e_iC_i$. Then we have $e_0C_0^{\perp_H} \oplus e_1C_1^{\perp_H} \oplus \cdots \oplus e_rC_r^{\perp_H} \subseteq e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r$. This implies that $\mathbf{C}^{\perp_H} \subseteq \mathbf{C}$.

On the other hand, if $\mathbf{C}^{\perp_H} \subseteq \mathbf{C}$, then we have $e_0C_0^{\perp_H} \oplus e_1C_1^{\perp_H} \oplus \cdots \oplus e_rC_r^{\perp_H} \subseteq e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r$. By taking mod e_0, mod $e_1, \ldots$, mod e_r, respectively, we have $C_i^{\perp_H} \subseteq C_i$ for $0 \leq i \leq r$. Then $Z_i \cap Z_i^{-p^m} = \phi$. □

Let $\mathbf{C}$ be a Hermitian dual containing code of length n over R. The following theorem gives the relationship between $\mathbf{C}$ and $\phi(\mathbf{C})$.

Theorem 9 *Let $\mathbf{C}$ be a Hermitian dual containing code of length n over R and $M \in GL_{r+1}(\mathbb{F}_{p^{2m}})$ such that $M(M^p)^T = \lambda I_{r+1}$, where $\lambda \in \mathbb{F}_{p^{2m}}^*$, I_{r+1} is a $(r+1) \times (r+1)$ identity matrix. Then $\phi(\mathbf{C})$ is a Hermitian dual containing code of length $(r+1)n$ over $\mathbb{F}_{p^{2m}}$. Furthermore, if $\mathbf{C}$ is Hermitian self-dual over R, then $\phi(\mathbf{C})$ is also Hermitian self-dual over $\mathbb{F}_{p^{2m}}$.*

Proof The proof process is similar to that of Theorem 5. □

By [5,13], we can construct quantum codes via the Hermitian construction given in the following lemma.

Lemma 12 (Hermitian Construction) *If there exists a classical linear $[n, k, d]_{q^2}$ code C such that $C^{\perp_H} \subseteq C$, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code.*

With the results given above, we obtain a method to construct quantum codes over $\mathbb{F}_p$ immediately.

Theorem 10 *Let $\mathbf{C} = e_0C_0 \oplus e_1C_1 \oplus \cdots \oplus e_rC_r$ be a $[n, k, d_G]_R$ cyclic code. If $C_i^{\perp_H} \subseteq C_i$ for $0 \leq i \leq r$, then $\mathbf{C}^{\perp_H} \subseteq \mathbf{C}$ and there exists a quantum error-correcting code with parameters$[[(r+1)n, 2k - (r+1)n, d_G]]_{p^m}$, where $k = \sum_{i=0}^{r} k_i$ and k_i is the dimension of C_i.*

With the notations and results above, we give some new quantum codes over $\mathbb{F}_{13}$ and $\mathbb{F}_{17}$.

Table 2 New quantum codes $[[n,k,d]]_{p^m}$

n	r	$\langle g_0(x),\ldots,g_r(x)\rangle$	$\phi(\mathbf{C})$	$[[n,k,d]]_{p^m}$
5	1	$\langle 1w^{30}1, 1w^{54}1\rangle$	$[10,6,4]_{13^2}$	$[[10,2,4]]_{13}$
5	2	$\langle 1w^{30}1, 1w^{30}1, 1w^{54}1\rangle$	$[15,9,5]_{13^2}$	$[[15,3,5]]_{13}$
6	1	$\langle 16(12), 17(12)\rangle$	$[12,8,3]_{13^2}$	$[[12,4,3]]_{13}$
8	2	$\langle 1w^{26}w^{63}, 1w^{110}w^{63}, 1w^{131}w^{105}\rangle$	$[24,18,4]_{13^2}$	$[[24,12,4]]_{13}$
12	2	$\langle 1(11), 19, 15\rangle$	$[36,33,2]_{13^2}$	$[[36,30,2]]_{13}$
12	2	$\langle 178, 12(11), 1(11)(11)\rangle$	$[36,30,4]_{13^2}$	$[[36,24,4]]_{13}$
12	1	$\langle 1972(10), 147(11)(10)\rangle$	$[24,16,5]_{13^2}$	$[[24,8,5]]_{13}$
12	1	$\langle 135(12)(11)5, 1(10)51(11)8\rangle$	$[24,14,6]_{13^2}$	$[[24,4,6]]_{13}$
8	2	$\langle 18, 18, 18\rangle$	$[24,21,2]_{17^2}$	$[[24,18,2]]_{17}$
12	2	$\langle 1\eta^{168}, 14, 1\eta^{264}\rangle$	$[36,33,2]_{17^2}$	$[[36,30,2]]_{17}$
16	2	$\langle 15(10), 1(11)(11), 1(14)7\rangle$	$[48,42,3]_{17^2}$	$[[48,36,3]]_{17}$
16	2	$\langle 1(12)(11)2, 167(13), 1368\rangle$	$[48,39,4]_{17^2}$	$[[48,30,4]]_{17}$
16	2	$\langle 1(16)8(12)8, 182(10)9, 171(15)(15)\rangle$	$[48,36,5]_{17^2}$	$[[48,24,5]]_{17}$
16	1	$\langle 1(11)(13)6(16)(11), 13(16)(12)1(14)\rangle$	$[32,22,6]_{17^2}$	$[[32,12,6]]_{17}$
16	2	$\langle 1(13)1(15)(11)95, 1(12)93767, 159(14)7(11)7\rangle$	$[48,30,7]_{17^2}$	$[[48,12,7]]_{17}$
16	1	$\langle 12(11)4(16)78(13), 1(15)(11)(13)(16)(10)84\rangle$	$[32,18,8]_{17^2}$	$[[32,4,8]]_{17}$

Example 3 Let $R=\mathbb{F}_{13^2}+v_1\mathbb{F}_{13^2}+v_2\mathbb{F}_{13^2}$ and $n=5$. Then $C_0^{169,5}=\{0\}$, $C_1^{169,5}=\{1,4\}$ and $C_2^{169,5}=\{2,3\}$. Let $Z_0=Z_1=\{1,4\}$ and $Z_2=\{2,3\}$ be the defining sets of C_0, C_1 and C_2, respectively. It is easy to show that $Z_0^{-13}=Z_1^{-13}=\{2,3\}$ and $Z_2^{-13}=\{1,4\}$. Then, we have $Z_i\cap Z_i^{-13}=\phi$ for $0\le i\le 2$, i.e., $C_i^{\perp_H}\subseteq C_i$. According to Theorem 8, we have $\mathbf{C}=e_0C_0\oplus e_1C_1\oplus e_2C_2$ is a Hermitian dual containing code over R, i.e., $\mathbf{C}^{\perp_H}\subseteq\mathbf{C}$.

Let $g_0(x)=g_1(x)=(x-\rho^1)(x-\rho^4)=x^2+w^{30}x+1$ and $g_2(x)=(x-\rho^2)(x-\rho^3)=x^2+w^{54}x+1$, where w is a primitive element of $\mathbb{F}_{13^2}=\mathbb{F}_{13}[x]/\langle x^2+12x+2\rangle$ with $\mathrm{ord}(w)=13^2-1=168$ and ρ is a primitive 5th root of unity over the splitting field of x^5-1 over $\mathbb{F}_{13^2}$. Then, $C_0=\langle g_0(x)\rangle$, $C_1=\langle g_1(x)\rangle$ and $C_2=\langle g_2(x)\rangle$.

Let $M=\begin{pmatrix}11&2&1\\12&11&2\\2&1&2\end{pmatrix}\in GL_2(\mathbb{F}_{13^2})$. Then we have $M(M^{13})^T=\begin{pmatrix}9&0&0\\0&9&0\\0&0&9\end{pmatrix}$. With the computational algebra systems Magma [6], we have that $\phi(\mathbf{C})$ is a $[15,9,5]$ linear code over $\mathbb{F}_{13^2}$. By Theorems 9 and 10, we obtain a quantum code with parameters $[[15,3,5]]_{13}$.

At the last of this example, we give some new quantum codes over $\mathbb{F}_{13}$ and $\mathbb{F}_{17}$ from cyclic codes over the ring R in Table 2, where η is a primitive element of $\mathbb{F}_{17^2}=\mathbb{F}_{17}[x]/\langle x^2+16x+3\rangle$ with $\mathrm{ord}(\eta)=17^2-1=288$.

Acknowledgements Part of this work was done when Gao was visiting the Chern Institute of Mathematics, Nankai University. Gao would like to thank its kind invitation. This research is supported by the 973 Program of China (Grant No. 2013CB834204), the National Natural Science Foundation of China (Nos. 61571243, 11701336, 11626144, 11671235), and the Fundamental Research Funds for the Central Universities of China.

References

1. Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$. Int. J. Quantum Inf. **12**, 1450042 (2014)
2. Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. Int. J. Inf. Coding Theory **3**, 137–144 (2015)
3. Ashraf, M., Mohammad, G.: Quantum codes from cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. Quantum Inf. Process. **15**, 4089–4098 (2016)
4. Aly, S.A., Klappenecker, A., Sarvepalli, P.K.: On quantum and classical BCH codes. IEEE Trans. Inf. Theory **53**(3), 1183–1188 (2007)
5. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001)
6. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)
7. 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**, 1369–1387 (1998)
8. Dertli, A., Cengellenmis, Y., Eren, S.: Some results on the linear codes over the finite ring $\mathbb{F}_2 + v_1\mathbb{F}_2 + \cdots + v_r\mathbb{F}_2$. Int. J. Quantum Inf. **14**, 12 (2016)
9. Gao, J., Wang, Y.: Quantum codes derived from negacyclic codes. Int. J. Theor. Phys. **57**, 682–686 (2018)
10. Gao, J.: 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 Inf. **13**(8), 8 (2015)
11. Gao, J., Wang, Y.: u-Constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and their applications of constructing new non-binary quantum codes. Quantum Inf. Process. **17**, 4 (2018). https://doi.org/10.1007/s11128-017-1775-8
12. Hammons Jr., A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inf. Theory **40**, 301–319 (1994)
13. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**(11), 4892–4914 (2006)
14. Knill, E., Laflamme, R.: Theory of quantum error-correcting codes. Phys. Rev. A **55**(2), 900–911 (1997)
15. Kai, X., Zhu, S.: Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Int. J. Quantum Inf. **9**, 689–700 (2011)
16. La Guardia, G.G.: Quantum codes derived from cyclic codes. Int. J. Theor. Phys. **56**(8), 2479–2484 (2017)
17. La Guardia, G.G.: New quantum MDS codes. IEEE Trans. Inf. Theory **57**(8), 5551–5554 (2011)
18. La Guardia, G.G.: On the construction of nonbinary quantum BCH codes. IEEE Trans. Inf. Theory **60**(3), 1528–1535 (2014)
19. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
20. Mi, J., Cao, X., Xu, S., Luo, G.: Quantum codes from Hermitian dual-containing cyclic codes. Int. J. Comput. Math. **2**(3), 14 (2016)
21. Özen, M., Özzaim, N.T., Ince, H.: Quantum codes from cyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$. Int. Conf. Quantum Sci. Appl. J. Phys. Conf. Ser. **766**, 012020-1–012020-6 (2016)
22. Qian, J., Zhang, L.: Improved constructions for nonbinary quantum BCH codes. Int. J. Theor. Phys. **56**(4), 1355–1363 (2017)
23. Qian, J., Ma, W., Gou, W.: Quantum codes from cyclic codes over finite ring. Int. J. Quantum Inf. **7**, 1277–1283 (2009)
24. Qian, J.: Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. J. Inf. Comput. Sci. **10**(6), 1715–1722 (2013)
25. Shor, P.W.: Scheme for reducing decoherence in quantum memory. Phys. Rev. A **52**, 2493–2496 (1995)