Southeast Asian Journal of Sciences: Vol. 5, No. 2 (2017) pp. 162-173

QUANTUM CODES OVER A CLASS OF FINITE COMMUTATIVE SEMISIMPLE RINGS

Nguyen Trong Bac

Department of Basic Sciences
University of Economics and Business Administration
Thai Nguyen University, Thai Nguyen 250000, Vietnam
e-mail: bacnt2008@gmail.com

Abstract

Direct sum of finite fields $\mathbb{F}_2 \oplus \mathbb{F}_5$ is a commutative semi-simpe ring. In this study, we investigate quantum MDS codes over $\mathbb{F}_2 \oplus \mathbb{F}_5$.

1. Introduction

Constacyclic codes have practical applications as they can be efficiently encoded using simple shift registers. They have rich algebraic structures for efficient error detection and correction, which explains their preferred role in engineering. In fact, constacyclic codes are the most studied of all codes. Many well known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either a class of constacyclic codes or constructed from constacyclic codes.

Classically, the algebraic structures of constacyclic codes are determined by ideals in the polynomial rings over finite fields, Galois rings and finite chain rings. Recently, codes over finite non-chain rings have been also studied. In 2010, Zhu et.al. [32] investigated the structures and properties of cyclic codes

Key words: Constacyclic codes, dual codes, semi-simple rings, quantum codes, MDS codes.

over the ring $\mathbb{F}_2+v\mathbb{F}_2$ where $v^2=v$. The structure of codes over the ring $\frac{\mathbb{Z}_3[v]}{\langle v^3-v\rangle}$ is studied by Bayram and Siap [3]. After that, Gao and Wang [17] introduced a new generalization of [3] by considering the linear codes over $\mathbb{F}_p+v\mathbb{F}_p+v^2\mathbb{F}_p$. In 2014, Bayram and Siap [4] continued to study codes over the ring $\frac{\mathbb{Z}_p[v]}{\langle v^p-v\rangle}$. The algebraic structures of linear, cyclic and constacyclic codes over this ring are determined by means of a Grey map. By using Gray map defined in [4], Sari and Siap [26] obtained the quantum error correcting codes over $\mathbb{F}_p$. Moreover, the algebraic structures of the cyclic codes of arbitrary length over the finite non-chain ring $\mathbb{F}_p+v\mathbb{F}_p+\cdots+v^{p-1}\mathbb{F}_p$ where $v^p=v$ are also introduced in [26]. As noted in Remark 2.5, this ring $\mathbb{F}_p+v\mathbb{F}_p+\cdots+v^{p-1}\mathbb{F}_p$ is in fact a direct sum of p copies of the finite field $\mathbb{F}_p$.

Quantum error correcting codes play an important role in quantum communications and computation. Therefore, the study of quantum codes has developed rapidly in recent decade years. Using CSS, Hermitian constructions and different methods, many classes of quantum codes have been constructed. In recent years, constructing quantum maximal distance separable (MDS) codes has become a hot topic. Some quantum MDS codes with special length over finite fields are introduced. Quantum codes over the non-chain rings are also studied by Qian [28], Ashraf and Mohammad [2], Dertli et.al. [10] and Sari and Siap [26].

In this paper, we study the situation of codes whose alphabets are of the most general form of the rings in [3], [4], [17], [26], [32], i.e., our code-alphabet is a finite commutative semi-simple ring R, which is a direct sum of k finite fields, $R=\mathbb{F}_2\oplus\mathbb{F}_5$. We obtain the structure of all λ-constacyclic codes over R, and we show that each λ-constacyclic code C of length n over R has a (unique) standard representation $C=\oplus_{i=1}^{2}C_i$, where each C_i is a λ_i-constacyclic code of length n over $\mathbb{F}_i$ $(i=1,2)$. The generator polynomials, generator matrices, and sizes of all λ-constacyclic codes are established. We deal with duals of such constacyclic codes, and we show that the dual of $\oplus_{i=1}^{k}C_i$ is $\oplus_{i=1}^{k}C_i^{\perp}$, where $C_i^{\perp}$ are duals of C_i, which are λ_i^{-1}-constacyclic codes of length n over $\mathbb{F}_i$. The structure of linear and constacyclic codes and their duals are used to study quantum error-correcting codes over finite commutative semi-simple rings. We extended the CSS and Hermitian constructions for quantum codes over finite fields to construct quantum MDS codes over semi-simple ring R.

2. Preliminaries

For a finite ring R, consider the set R^n of n-tuples of elements from R as a module over R. Any subset $C \subseteq R^n$ is called a *code of length* n over R, the code C is *linear* if in addition, C is an R-submodule of R^n. Given an n-tuples $(x_0, x_1, \ldots, x_{n-1}) \in R^n$, the *cyclic shift* τ and *negashift* ν on R^n are defined as usual, i.e.,

$$\tau(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \cdots, x_{n-2}),$$

and

$$\nu(x_0, x_1, \ldots, x_{n-1}) = (-x_{n-1}, x_0, x_1, \cdots, x_{n-2}).$$

A code C is called *cyclic* if $\tau(C) = C$, and C is called *negacyclic* if $\nu(C) = C$.

More generally, if λ is a unit of the ring R, then the λ-*constacyclic* (λ-twisted) *shift* τ_λ on R^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \cdots, x_{n-2}),$$

and a code C is said to be λ-*constacyclic* if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ. In light of this definition, when $\lambda = 1$, λ-constacyclic codes are cyclic codes, and when $\lambda = -1$, λ-constacyclic codes are just negacyclic codes.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. From that, the following fact is well-known and straightforward:

Proposition 2.1. *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n - \lambda \rangle}$.*

Given n-tuples $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, their *inner product* or *dot product* is defined as usual

$$x \cdot y = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1}$$

(evaluated in R). Two n-tuples x, y are called *orthogonal* if $x \cdot y = 0$. For a linear code C over R, its *dual code* $C^\perp$ is the set of n-tuples over R that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{x \mid x \cdot y = 0, \forall y \in C\}.$$

A code C is called *self-orthogonal* if $C \subseteq C^{\perp}$, and it is called *self-dual* if $C = C^{\perp}$. The following result is well-known (cf. [8, 14, 31]).

Proposition 2.2. *Let R be a finite Frobenius ring, and C be a linear code of length n over R. Then $|C| \cdot |C^{\perp}| = |R|^n$.*

The dual of a cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, we have the following implication of the dual of a λ-constacyclic code.

Proposition 2.3. (cf. [11]) *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

Recall that a linear code C over $\mathbb{F}_q$ of length n and the minimum Hamming distance d is denoted by $[n, k, d]_q$, where $|C| = q^k$ and k is called the dimension of the linear code C. The Hamming distance $d_H(x, y)$ between two vectors $x, y \in \mathbb{F}_{p^m}^n$ is defined to be the number of coordinates in which x and y differ.

In this paper, we consider finite commutative semi-simple rings, which are rings that can be expressed as a finite direct sum of finite fields.

$$R = \mathbb{F}_0 \oplus \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_{k-1},$$

where $\mathbb{F}_i$ are finite fields with $|\mathbb{F}_i| = q_i$. The addition $+$ and multiplication $*$ in R are component-wise, i.e., for $(a_0, a_1, \ldots, a_{k-1})$ and $(b_0, b_1, \ldots, b_{k-1})$ in R,

$$(a_0, a_1, \ldots, a_{k-1}) + (b_0, b_1, \ldots, b_{k-1}) = (a_0 + b_0, a_1 + b_1, \ldots, a_{k-1} + b_{k-1}),$$

$$(a_0, a_1, \ldots, a_{k-1}) * (b_0, b_1, \ldots, b_{k-1}) = (a_0 b_0, a_1 b_1, \ldots, a_{k-1} b_{k-1}).$$

Proposition 2.4. *The followings hold true*

(*a*) *R is Frobenius.*

(*b*) *There are $\prod_{i=0}^{k-1}(q_i - 1)$ units of R, they are of the form $\lambda = (\lambda_0, \ldots, \lambda_{k-1})$, where each λ_i is a unit in $\mathbb{F}_i$.*

3. Quantum Codes over R

A quantum computer can certainly solve hard problems much more quickly than the classical computer. Quantum error-correcting codes have a prominent place in quantum communication as well as quantum computation. To protect quantum information from errors due to the decoherence and other quantum

noise, quantum error-correcting codes are used in quantum computing. Many good quantum cyclic error-correcting codes were constructed from Hamming codes, BCH codes and Reed-Solomon codes. Quantum error-correcting codes were first introduced by P. Shor in 1995. Although the theory of quantum error correcting codes is quite different from the theory of classical error correcting codes, Calderbank et. al. transformed the problem of finding quantum error correcting codes from classical error correcting codes over GF(4). In 1998, Calderbank, Shor and Steane introduced a method to construct quantum error-correcting codes from classical error-correcting codes. Recently, the theory of quantum error-correcting codes is studied not only over finite fields but also over some special classes of finite rings. For examples, a new method of constructing quantum error correcting codes from cyclic codes over finite ring $\mathbb{F}_2 + v\mathbb{F}_2, v^2 = v$, for arbitrary length is introduced in [28]. After that, Ashraf and Mohammad [2] studied the quantum codes from cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$, where $v^2 = 1$. Furthermore, good quantum codes obtained from cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ are introduced by Dertli et.al. in a recent paper [10]. In 2015, Sari and Siap [26] obtained the quantum error correcting codes over $\mathbb{F}_p$ from codes over the finite non-chain ring $R_p = \mathbb{F}_p + v\mathbb{F}_p + \cdots + v^{p-1}\mathbb{F}_p$, where $v^p = v$. A crucial construction of quantum error-correcting codes, known as the CSS construction, was given in [7].

Theorem 3.1. *(CSS Construction) [7] Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ of the parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ such that $C_2 \subseteq C_1$, respectively. Then there exists a quantum error correcting code with the parameters $[[n, k_1 - k_2, \min\{d_1, d_2^{\perp}\}]]_q$ where $d_2^{\perp}$ is the Hamming distance of the dual code $C_2^{\perp}$. Moreover, if $C_2 = C_1^{\perp}$, then there exists a quantum error correcting code having the parameters $[[n; 2k_1 - n; d_1]]_q$.*

By studying classical cyclic codes over finite field $\mathbb{F}_q$ with dual containing properties, many good quantum codes have been constructed. We now extend this construction to give a quantum error correcting code over R.

Theorem 3.2. *Let $C = C_1 \oplus C_2$ be a cyclic code of length n over R. If $C_i^{\perp} \subseteq C_i$, then there exists a quantum error correcting code over R with parameters $([[n, 2k_0 - n, d_0]]_{q_0}, \ldots, [[n, 2k_{k-1} - n, d_{k-1}]]_{q_{k-1}})$.*

Proof. By Theorem 3.1, there exists a quantum error correcting code T_i over $\mathbb{F}_i$ having the parameters $[[n, 2k_i - n, d_i]]_{q_i}$ for each $i = 0, \ldots, k-1$. This implies that $T = \oplus_{i=0}^{k-1} T_i$ is a quantum error correcting code over R with parameters $([[n, 2k_0 - n, d_0]]_{q_0}, \ldots, [[n, 2k_{k-1} - n, d_{k-1}]]_{q_{k-1}})$, as desired. □

We knew that every code C over R can be expressed as $C = \oplus_{i=0}^{k-1} T_i$ for some codes C_i over $\mathbb{F}_i$ $(i = 0, \ldots, k-1)$. Therefore, to construct quantum error correcting code over R, we construct quantum error correcting code over $\mathbb{F}_i$. If $\mathbb{F}_i = \mathbb{F}_q$ for all $i = 0, \ldots, k-1$, then the multiple parameters $([[n, 2k_0 - n, d_0]]_{q_0}, \ldots, [[n, 2k_{k-1} - n, d_{k-1}]]_{q_{k-1}})$ are coincided with the parameters $[[n, 2k - n, d]]_q$.

The quantum Singleton bound for codes was strengthened by Calderbank, Rains, Shor and Sloane [9]. The binary version of the quantum Singleton bound was first proved by Knill and Laflamme [21]. It is known as the Knill and Laflamme formular when d is odd. We introduce quantum Singleton bound here to use it later.

Theorem 5.3. (Quantum Singleton Bound) [20, Theorem 1] *Let $C = [[n, k, d]]_q$ be a quantum error-correction code. Then $k + 2d \leq n + 2$.*

In recent years, constructing quantum maximum distance separable (briefly, MDS) codes have become one of the central topics for quantum codes. The quantum MDS codes can be constructed by the Hermitian construction and the quantum Singleton bound. Therefore, to get q-ary quantum MDS codes, we need to determine linear MDS codes over $\mathbb{F}_{q^2}$ satisfying $C^{\perp_H} \subseteq C$, where $C^{\perp_H}$ is the Hermitian dual code of C. Many new classes of quantum MDS codes are constructed by this idea. For examples, Guardia [19] introduced a class of quantum codes based on cyclic codes. By using negacyclic codes, Kai and Zhu [22] gave two new classes of quantum MDS codes. Motivated the work in [22], from constacyclic codes, Kai et.al. [23] constructed several new quantum MDS codes. In 2014, some classes of dual containing MDS constacyclic codes are given and their parameters are computed by Chen et.al. [5]. These results allowed them to construct new quantum MDS codes.

From Theorem 3.2, we can construct a quantum MDS code by using the CSS Construction.

Theorem 3.4. *Let $C = C_1 \oplus C_2$ be a cyclic code of length n over R. If $C_i^{\perp} \subseteq C_i$, then there exists a quantum MDS code over R with parameters $([[n, n - d_0 + 1, d_0]]_{q_0}, [[n, n - d_1 + 1, d_1]]_{q_1}, \ldots, [[n, n - d_{k-1} + 1, d_{k-1}]]_{q_{k-1}})$.*

Proof. By Theorem 3.2, there exists a quantum error correcting code over R with parameters $([[n, 2k_0 - n, d_0]]_{q_0}, \ldots,$
$[[n, 2k_{k-1} - n, d_{k-1}]]_{q_{k-1}})$. This follows that there exists a quantum MDS code over R with parameters $([[n, n - d_0 + 1, d_0]]_{q_0}, [[n, n - d_1 + 1, d_1]]_{q_1}, \ldots, [[n, n - d_{k-1} + 1, d_{k-1}]]_{q_{k-1}})$. □

The Hermitian inner product is defined as $x \circ_{\mathbb{F}_{q^2}} y = x_0\bar{y}_0 + x_1\bar{y}_1 + \cdots + x_{n-1}\bar{y}_{n-1}$, where $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_{q^2}^n$ and $\bar{y}_i = y_i^q$. The Hermitian dual code of C is defined as $C^{\perp_H} = \{x \in \mathbb{F}_{q^2}^n | \sum_{i=0}^{n-1} x_i\bar{y}_i = 0, \forall y \in C\}$. If $C \subseteq C^{\perp_H}$, then C is called a *Hermitian self-orthogonal* code. The code C satisfying $C^{\perp_H} \subseteq C$ is called a *Hermitian dual-containing code*. Hermitian dual-containing codes are also known as weakly Hermitian self-dual codes. If $C^{\perp_H} = C$, then C is called a *Hermitian self-dual code*. It is easy to see that $\{0\}$ is a Hermitian self-orthogonal code and $\mathbb{F}_{q^2}^n$ is a Hermitian dual-containing code, which are refered to as the trivial Hermitian self-orthogonal and trivial Hermitian dual-containing codes, respectively.

For a nonempty subset V of $\mathbb{F}_{q^2}^n$, we define V^q to be the set

$$V^q = \{(v_0^q, v_1^q, \ldots, v_{n-1}^q) : (v_0, v_1, \ldots, v_{n-1}) \in V\}.$$

Clearly, if V is a subspace of $\mathbb{F}_{q^2}^n$, then V^q is also a subspace of $\mathbb{F}_{q^2}$. Moreover, if $(v_0, v_1, \ldots, v_{n-1}), (w_0, w_1, \ldots, w_{n-1}) \in V$ are such that $(v_0^q, v_1^q, \ldots, v_{n-1}^q) = (w_0^q, w_1^q, \ldots, w_{n-1}^q)$, then for all $0 \leq j \leq n-1$, $v_j^q = w_j^q$, hence, $v_j = v_j^{q^2} = w_j^{q^2} = w_j$. It means, $(v_0^q, v_1^q, \ldots, v_{n-1}^q) = (w_0^q, w_1^q, \ldots, w_{n-1}^q) \in V^q$ if and only if $(v_0, v_1, \ldots, v_{n-1}) = (w_0, w_1, \ldots, w_{n-1}) \in V$, and therefore, $|V| = |V^q|$.

If C is a q^2-ary linear code, then C^q is also a q^2-ary linear code, and by definition, $C^{\perp_H} = (C^{\perp})^q$. Since $|C^{\perp}| = |(C^{\perp})^q|$, it follows that $|C^{\perp_H}| = |C^{\perp}|$, i.e., $|C|.|C^{\perp_H}| = q^{2n}$. Furthermore, it is easy to check that $(C^{\perp_H})^{\perp_H} = C$.

Since the Hermitian inner product over $\mathbb{F}_q$ is only defined when q is a square, hereafter, we only consider finite fields whose cardinalities are even powers of primes. From now on, our finite commutative semi-simple rings are of the form $\mathcal{R} = \mathbb{F}_0 \oplus \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_{k-1}$, where $\mathbb{F}_i = \mathbb{F}_{q_i^2}$ for all $i = 0, \ldots, k-1$.

Recall that $x_i \circ_{\mathbb{F}_i} y_i$ denotes the Hermitian inner product over $\mathbb{F}_i$ for all $i = 0, \ldots, k-1$. Then the Hermitian inner product over $\mathcal{R}$ is defined as $x \circ_{\mathcal{R}} y = (x_0, \ldots, x_{k-1}) * (\bar{y}_0, \ldots, \bar{y}_{k-1}) = (x_0 \circ_{\mathbb{F}_0} \bar{y}_0, x_1 \circ_{\mathbb{F}_1} \bar{y}_1, \ldots, x_{k-1} \circ_{\mathbb{F}_{k-1}} \bar{y}_{k-1})$ where $x_i = (x_{i,0}, x_{i,1}, \ldots, x_{i,n-1}), y_i = (y_{i,0}, y_{i,1}, \ldots, y_{i,n-1})$ for all $i = \{0, \ldots, k-1\}$. The Hermitian dual code of C is defined as $C^{\perp_H} = \{x \in \mathcal{R}^n | x \circ_{\mathcal{R}} \bar{y} = (x_0 \circ_{\mathbb{F}_0} \bar{y}_0, x_1 \circ_{\mathbb{F}_1} \bar{y}_1, \ldots, x_{k-1} \circ_{\mathbb{F}_{k-1}} \bar{y}_{k-1}) = 0_{\mathcal{R}}, \forall y \in C\}$. We get the following result for the case of Hermitian dual codes.

Proposition 3.5.

(i) *For any code $C = C_1 \oplus C_2$ of length n over $\mathcal{R}$, its Hermitian dual code is*

$C^{\perp_H} = \oplus_{i=0}^{1} C_i^{\perp_H}$.

(ii) *C is Hermitian self-dual if and only if C_i are Hermitian self-dual for all $i = 0, 1$.*

(iii) *C is Hermitian self-orthogonal if and only if C_i are Hermitian self-orthogonal for all $i = 0, 1$.*

(iv) *C is Hermitian dual-containing if and only if C_i are Hermitian dual-containing for all $i = 0, 1$.*

(v) *C is Hermitian LCD if and only if C_i are Hermitian LCD for all $i = 0, 1$.*

(vi) *For any linear code C of length n over $\mathcal{R}$, $|C|.|C^{\perp_H}| = |\mathcal{R}^n|$.*

Proof. (i): Let $(x_0, x_1, \ldots, x_{k-1})$ be arbitrary in $\oplus_{i=0}^{k-1} C_i^{\perp_H}$. That means, for $0 \leq i \leq k-1$, $x_i \in C_i^{\perp_H}$, and hence, for any $c = (c_0, c_1, \ldots, c_{k-1}) \in C$,

$$(x_0, x_1, \ldots, x_{k-1}) * (\bar{c}_0, \bar{c}_1, \ldots, \bar{c}_{k-1}) = (x_0 \circ_{\mathbb{F}_0} \bar{c}_0, x_1 \circ_{\mathbb{F}_1} \bar{c}_1, \ldots, x_{k-1} \circ_{\mathbb{F}_{k-1}} \bar{c}_{k-1}) = 0_{\mathcal{R}},$$

implying $(x_0, x_1, \ldots, x_{k-1}) \in C^{\perp_H}$. This shows that $\oplus_{i=0}^{k-1} C_i^{\perp_H} \subseteq C^{\perp_H}$. On the other hand, for all $x = (x_0, \ldots, x_{k-1}) \in C^{\perp_H}$, we have $(x_0, \ldots, x_{k-1}) * (\bar{y}_0, \ldots, \bar{y}_{k-1}) = (x_0 \circ_{\mathbb{F}_0} \bar{y}_0, \ldots, x_{k-1} \circ_{\mathbb{F}_{k-1}} \bar{y}_{k-1}) = 0_{\mathcal{R}}$, for all $y = (y_0, y_1, \ldots, y_{k-1}) \in C$. Note that $x_i = (x_{i,0}, \ldots, x_{i,n-1}), \bar{y}_i = (\bar{y}_{i,0}, \ldots, \bar{y}_{i,n-1}) \in C_i$, for all $i = 0, \ldots, k-1$. Since $x_i \circ_{\mathbb{F}_i} \bar{y}_i = 0_{\mathbb{F}_i}$, for any $\bar{y}_i \in C_i$, we have $x_i \in C_i^{\perp_H}$ for all $i = 0, \ldots, k-1$. This means that $x \in \oplus_{i=0}^{k-1} C_i^{\perp_H}$. It follows that $C^{\perp_H} \subseteq \oplus_{i=0}^{k-1} C_i^{\perp_H}$. Hence $C^{\perp_H} = \oplus_{i=0}^{k-1} C_i^{\perp_H}$.
(ii), (iii), (iv) and (v) are straightforward to see from (i).
(vi): From (i), we have $|C^{\perp_H}| = \prod_{i=0}^{k-1} |C_i^{\perp_H}| = \prod_{i=0}^{k-1} \frac{|q_i^{2n}|}{|C_i|} = \frac{\left(\prod_{i=0}^{k-1} q_i^2\right)^n}{\prod_{i=0}^{k-1} |C_i|} = \frac{|\mathcal{R}^n|}{|C|}$. Therefore, $|C|.|C^{\perp_H}| = |\mathcal{R}^n|$. □

For a monic polynomial $f(x) \in \mathbb{F}_{q^2}[x]$ of degree k with $f(0) \neq 0$, the *reciprocal polynomial* of $f(x)$ denoted by $f(x)^\star$ is $f(0)^{-1} x^k f(x^{-1})$. Observe that the automorphism α of $\mathbb{F}_{q^2}$ given by $\alpha(a) = \bar{a} = a^q$ can be extended to an automorphism φ of $\mathbb{F}_{q^2}[x]$ in an obvious way $\varphi(f(x)) = \varphi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \bar{a}_i x^i$. We put $\overline{f(x)} = \sum_{i=0}^{n} \bar{a}_i x^i$. Recall from [5] that a monic polynomial $f(x)$ in $\mathbb{F}_{q^2}[x]$ with $f(0) \neq 0$ is called *conjugate-self-reciprocal* if $f(x) = \overline{f(x)}^\star$. [5] gave necessary and sufficient conditions for the existence of a nontrivial Hermitian dual-containing λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ as follows.

Theorem 3.6. [5, Theorem 2.9] *Let $\lambda \in \mathbb{F}_{q^2}^{\star}$ satisfy $\lambda = \bar{\lambda}^{-1}$. Nontrivial Hermitian dual-containing λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ exist if and only if there exists at least one conjugate-reciprocal polynomial pair among the monic irreducible factors of $x^n - \lambda$ over $\mathbb{F}_{q^2}$.*

Using Proposition 3.5 and Theorem 3.6, we obtain necessary and sufficient conditions for the existence of a nontrivial Hermitian dual-containing λ-constacyclic code of length n over $\mathcal{R}$:

Theorem 3.7. *Let $C = C_1 \oplus C_2$ be a λ-constacyclic code of length n over $\mathcal{R}$. Then C is a Hermitian dual containing code if and only if for each $0 \leq i \leq k-1, C_i$ is a Hermitian dual containing code, if and only if there exists at least one conjugate-reciprocal polynomial pair among the monic irreducible factors of $x^n - \lambda_i$ over $\mathbb{F}_i$.*

Many classes of quantum codes have been constructed by different methods. The following so-called Hermitian construction is one of the important methods given in [1].

Proposition 3.8. (Hermitian construction) [1] *If C is a q^2-ary $[n, k, d]$ linear code such that $C^{\perp_H} \subseteq C$, then there exists a q-ary quantum code with parameters $[[n, 2k - n, \geq d]]_q$.*

The Hermitian construction can be extended to quantum codes over $\mathcal{R}$ as follows.

Theorem 3.9. *Let $C = C_1 \oplus C_2$ be a λ-constacyclic code of length n over $\mathcal{R}$. If for each $0 \leq i \leq k-1$, C_i is a q_i^2-ary $[n, k, d]_{q_i}$ linear code such that $C_i^{\perp_H} \subseteq C_i$, then there exists a quantum code over $\mathcal{R}$ with parameters $([[n, 2k_0 - n, \geq d_0]]_{q_0}, [[n, 2k_1 - n, \geq d_1]]_{q_1}, \ldots, [[n, 2k_{k-1} - n, \geq d_{k-1}]]_{q_{k-1}})$.*

Proof. There exists a quantum code T_i over $\mathbb{F}_i$ having the parameters $[[n, 2k_i - n, \geq d_i]]_{q_i}$ for each $i = 0, \ldots, k-1$ by Proposition 3.8. Put $T = \oplus_{i=0}^{k-1} T_i$. Then T is a quantum code over $\mathcal{R}$ with parameters $([[n, 2k_0 - n, \geq d_0]]_{q_0}, [[n, 2k_1 - n, \geq d_1]]_{q_1}, \ldots, [[n, 2k_{k-1} - n, \geq d_{k-1}]]_{q_{k-1}})$. □

A quantum code satisfying $k + 2d = n + 2$, i.e. meeting the Quantum Singleton Bound (cf. Theorem 3.3), namely, $C = [n, n - 2d + 2, d]$, is called a *quantum MDS code*. Using the Hermitian construction, we can construct a quantum MDS code over $\mathcal{R}$ from quantum MDS codes over finite fields, as follows.

Theorem 3.10. *Let $C = C_1 \oplus C_2$ be a λ-constacyclic code of length n over*

$\mathcal{R}$. If for each $0 \leq i \leq k-1$, C_i is a q_i^2-ary $[n, k_i, d_i]_{q_i}$ linear code such that $C_i^{\perp_H} \subseteq C_i$, then there exists a quantum MDS code over $\mathcal{R}$ with parameters $([[n, n-2d_0+2, \geq d_0]]_{q_0}, [[n, n-2d_1+2, \geq d_1]]_{q_1}, \ldots, [[n, n-2d_{k-1}+2, \geq d_{k-1}]]_{q_{k-1}})$.

Proof. We can see that C_i are linear MDS codes having parameters $[[n, n-d_i+1, d_i]]_{q_i}$over $\mathbb{F}_{q_i^2}$ satisfying $C_i^{\perp_H} \subseteq C_i$ for each $i = 0, \ldots, k-1$. By Hermitian construction (cf. Proposition 3.8), there exists a quantum MDS code T_i over $\mathbb{F}_{q_i}$ having the parameters $[[n, 2(n-d_i+1)-n = n-2d_i+2, \geq d_i]]_{q_i}$ for each $i = 0, \ldots, k-1$. Hence $T = \oplus_{i=0}^{k-1} T_i$ is a quantum MDS code over $\mathcal{R}$ with parameters $([[n, n-2d_0+2, \geq d_0]]_{q_0}, [[n, n-2d_1+2, \geq d_1]]_{q_1}, \ldots, [[n, n-2d_{k-1}+2, \geq d_{k-1}]]_{q_{k-1}})$. □

Example 3.11.

(i) [5, Example 3.8] Let $q = 9$ and $n = 16$. Suppose that $\mathbb{F}_{81}^{\star} = \langle \theta \rangle$. Put $\lambda = \theta^{16}$. We have 4 quantum MDS codes with parameters $[[16, 8, 5]]_9$, $[[16, 10, 4]]_9$, $[[16, 12, 3]]_9$, $[[16, 14, 2]]_9$.

(ii) [23, Example 3.3] Let $q^2 = 81$ and $n = 40$. We have 5 quantum MDS codes with parameters $[[40, 32, 5]]_9$, $[[40, 30, 6]]_9$,

$[[40, 28, 7]]_9$, $[[40, 26, 8]]_9$, and $[[40, 24, 9]]_9$.

Example 3.12. Suppose that $\mathbb{F}_{81}^{\star} = \langle \theta \rangle$. Put $\lambda = \theta^{16}$ and let C_1, C_2 be quantum MDS codes with the parameters $[[16, 8, 5]]_9, [[16, 10, 4]]_9$ respectively. We consider the ring $\mathcal{R} = \mathbb{F}_{81} + v\mathbb{F}_{81}$. By Theorem 5.10, we can see that $C_i \oplus C_j$ for all $i, j = 1, \ldots, 4$ are quantum MDS codes over $\mathcal{R} = \mathbb{F}_{81} + v\mathbb{F}_{81}$.

Example 3.13 We now consider the semi-simple ring: $R = \mathbb{F}_2 + v\mathbb{F}_2$ and $n = 7$. We can see that $C = C_1 \oplus C_2 = \langle g(x) \rangle = \langle (g_0(x), g_1(x)) \rangle$ is a cyclic code over R, where $g_0(x) = x - 1, g_1(x) = x - 1$. Over $\mathbb{F}_2$, $x^7 - 1$ can be written as $(x-1)^2$. From this, we can compute $|C| = 2^{2.2-\deg(g_0(x))-\deg(g_1(x)))} = 2^{28-1-1} = 2^{26}$. This implies that the dimension of cyclic code C is $k = 26$. The reciprocal of $g_0^*(x) = g_1^*(x) = 1 - x$. We have $C_i = \langle g_i(x) \rangle$ contains its dual because $x^n - 1 \equiv 0 \pmod{g_i(x) g_i^*(x)}$ for all $i = 0, 1$. Hence, $C^{\perp} \subseteq C$. It is easy to verify that Hamming distance of cyclic code C is 2. Therefore, by applying Theorem 3.1 (CSS construction), we can obtain a quantum code with parameters $[[2n, 2k-2n, d]] = [[14, 38, 2]]$ over $\mathbb{F}_2$.

We end this section by an important remark.

Remark 3.14. Quantum codes over the ring $\mathcal{R} = \mathbb{F}_q + v\mathbb{F}_q$ where $v^2 = v$

using CSS construction can be extended to [4]. However, quantum MDS codes using Hermitian construction over the ring $\mathcal{R} = \mathbb{F}_q + v\mathbb{F}_q$ where q is a square and $v^q = v$ have not been studied in the past. In our paper, we solved a special case. The general case can be investigated in another paper.

References

[1] A. Ashikhmin and E. Knill, *Nonbinary quantum stablizer codes*, IEEE Trans. Inf. Theory **47** (2001), 3065-3072.

[2] M. Ashraf and G. Mohammad, *Quantum codes from cyclic codes over* $\mathbb{F}_3 + v\mathbb{F}_3$*,* Int.J. Quantum Inform **6** (2014), 1450042 (8 pages).

[3] A. Bayram and I. Siap, *Structure of codes over the ring* $\frac{\mathbb{Z}_3[v]}{\langle v^3 - v \rangle}$, Applicable Algebra in Engineering, Communication and Computing **24** (2013), 369-386.

[4] A. Bayram and I. Siap, *Cyclic and constacyclic codes over a nonchain ring*, Journal of Algebra, Combinatorics, Discrete Structures and Applications **1** (2014), 1-12.

[5] B. Chen, S. Ling and G. Zhang *Application of Constacyclic codes to Quantum MDS Codes* IEEE Trans. Inform. Theory, **61** (2014), 1474-1478.

[6] T. Blackford, *Negacyclic duadic codes*, Finite Fields and Their Applications **14** (2008) 930-943.

[7] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A, **54** (1996), 1098-1106.

[8] A.R. Calderbank and N.J. A. Sloane, *Modular and p-adic codes*, Des. Codes Cryptogr **6** (1995), 21-35.

[9] A.R. Calderbank, E. M. Rains, P. W. Shor and N.J. A. Sloane, *Quantum Error Correction Via Codes Over GF(4)* , IEEE Trans. Inform. Theory **44** (1998), 1369-1387.

[10] A. Dertli, Y. Cengellenmis and S. Eren, *On quantum codes obtained from cyclic codes over* A_2*,* Int.J. Quantum Inform **13** (2015), 1550031 (9 pages).

[11] H.Q. Dinh, *Constacyclic codes of length* p^s *over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra **324** (2010), 940-950.

[12] H.Q. Dinh, *Repeated-root constacyclic codes of length* $2p^s$*,* Finite Fields and Their Applications **18** (2012) 133-143.

[13] H.Q. Dinh, *Structure of repeated-root constacyclic codes of length* $3p^s$ *and their duals*, Discrete Mathematics **313** (2013), 983-991.

[14] H.Q. Dinh and S.R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), 1728-1744.

[15] M. Esmaeili and S. Yari, *On complementary-dual quasi-cyclic codes*, Finite Fields and Their Applications **15** (2009), 375-386.

[16] J.Gao, *Some results on linear codes over* $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, J. Appl. Math. Comput. **47** (2014), 473-485.

[17] J. Gao and Y. Wang, *Some results on linear codes over* $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p + v^3\mathbb{F}_p$, Journal of Applied Mathematics and Computing **47** (2015), 473-478.

[18] K. Guenda and T. A. Gulliver, *Self-dual Repeated Root Cyclic and Negacyclic Codes over Finite Fields*, IEEE International Symposium on Information Theory Proceedings, (2012), 2904-2908.

[19] G. G. L. Guardia, *Constructions of new families of nonbinary quantum codes,* Phys. Rev. A, **80** (2009), 042331-1-042331-11.

[20] M. Grassl, T. Beth, and M. Ṙotteler *On optimal quantum codes,* Int. J. Quantum Inform, **2** (2004), 757-766.

[21] E. Knill and R. Laflamme, *Theory of quantum error-correcting codes,* Phys. Rev. A, **55** (1997), 900-911.

[22] X. Kai and S. Zhu *New quantum MDS codes from negacyclic codes,* IEEE Trans. Inform. Theory, **59** (2013), 1193-1197.

[23] X. Kai, S. Zhu, and P. Li *Constacyclic codes and some new quantum MDS codes,* IEEE Trans. Inform. Theory, **60** (2014), 2080-2086.

[24] J.L. Massey, *Linear codes with complementary duals*, Discrete Math **106/107** (1992), 337-342.

[25] Y. Jia, S. Ling, and C. Xing, *On Self-Dual Cyclic Codes Over Finite Fields*, IEEE Trans. Inform. Theory **57** (2011), 2243-2251.

[26] M. Sari and I. Siap, *Quantum Codes from Cyclic Codes over A Class of Nonchain Rings,* Proc. 2015 6th Int. Conf. Modeling, Simulation, and Applied Optimization (ICMSAO) (Istanbul, Turkey, 2015), pp. 1-2.

[27] N. Sendrier, *Linear codes with complementary duals meet the Gilbert-Varshamov bound*, Discrete Math. **285** (2004), 345-347.

[28] J. Qian, *Quantum Codes from Cyclic Codes over* $\mathbb{F}_2 + v\mathbb{F}_2$, Journal of Information and Computational Science **6** (2013), 1715-1722.

[29] Y. Yang and W. Cai, *On self-dual constacyclic codes over finite fields*, Des. Codes Cryptogr. **74** (2015) 355-364.

[30] X. Yang and J.L. Massey, *The condition for a cyclic code to have a complementary dual*, Discrete Math. **126** (1994), 391-393.

[31] J.A. Wood, *Duality for modules over finite rings and applications to coding theory*, American J. of Math. **121** (1999), 555-575.

[32] S. Zhu, Y. Wang and M. Shi, *Some results on cyclic codes over* $\mathbb{F}_2 + v\mathbb{F}_2$, IEEE Trans. Inform. Theory **56** (2010), 1680-1684.