Hermitian LCD codes over finite rings and their applications to maximal entanglement EAQECCs

Heqian Xu[*]
School of Mathematical Sciences
University of Science and Technology of China
Hefei, China
School of Mathematics and Statistics
Hefei Normal University
Hefei, China
heqianxu@mail.ustc.edu.cn

Wei Du
School of Mathematics and Statistics
Hefei Normal University
Hefei, China
duwei@hfnu.edu.cn

Abstract

Let $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$, where $\mathbb{F}_{q^2}$ is the finite field with q^2 elements, q is a power of a prime p, and $u^2 = 0$. In this paper, a class of maximal entanglement entanglement-assisted quantum error-correcting codes (EAQECCs) is obtained by employing Hermitian linear complementary dual (LCD) $(1-u)$-constacyclic codes over R of length n. First, we give a sufficient condition for a linear code C over R to be Hermitian LCD and claim that there does not exist a non-free Hermitian LCD code over R. Also, assume that $\gcd(n, q) = 1$, and γ is a unit in R, we obtain all γ-constacyclic LCD codes. Further, we give a technique to find the Hamming minimum distance of a $(1-u)$-constacyclic code of length n over R. Finally, we derive symplectic LCD codes over $\mathbb{F}_{q^2}$ as Gray images of linear and constacyclic codes over R. By using the explicit symplectic method in [10], we get the desired maximal entanglement EAQECCs.

1 Introduction

Linear complementary dual (LCD) codes are linear codes that meet their duals trivially, and have been widely applied in data storage, communications systems, consumer electronics, and cryptography. In [20], Massey proved that LCD codes provide an optimum linear coding solution for the two-user binary adder channel. Carlet and Guilley [3] investigated an interesting application of binary LCD codes against so-called side channel attacks (SCA) and fault injection attacks (FIA). A necessary and sufficient condition for

[*]First Author is supported by the Excellent Young Talents Fund Program of Higher Education Institutions of Anhui Province (CN)(gxyqZD2016228).

a cyclic code to be an LCD code has been provided by Yang and Massey [26]. In [12], quasi-cyclic codes that are LCD have been characterized and studied using their concatenated structures. Li et al. [17] constructed some LCD cyclic codes over finite fields and analyzed their parameters. With the development of classical error-correcting codes and their applications to quantum error-correcting codes (QECCs), people have extensively studied the Euclidean and Hermitian inner product and investigated the corresponding LCD codes (see, for example, [4, 6, 7, 16]).

In [1], Brun et al. introduced entanglement-assisted quantum error-correcting codes (EAQECCs), which allow the use of classical error-correcting codes without orthogonality. The concept of maximal entanglement EAQECCs was introduced by Lai et al [14]. It was shown that maximal entanglement EAQECCs can achieve the entanglement-assisted quantum capacity of a depolarizing channel. Additionally, there is a close link between EAQECCs and LCD codes. The application of LCD codes in constructing good EAQECCs has aroused the interest of researchers in the past few years, and many classes of maximal entanglement EAQECCs have been constructed (see [11, 19, 22, 23]).

In this paper, we focus on Hermitian LCD codes over finite rings and their applications to maximal entanglement EAQECCs. Let $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$, where $\mathbb{F}_{q^2}$ is the finite field with q^2 elements, q is a power of a prime p, and $u^2 = 0$. We give a sufficient condition for a linear code C over a finite ring R of length n to be Hermitian LCD. We claim that there does not exist a non-free Hermitian LCD code over R. Assume that $\gcd(n, q) = 1$, and γ is a unit in R, all γ-constacyclic Hermitian LCD codes are obtained. We introduce a Gray map, and derive symplectic LCD codes over finite fields as Gray images of linear and constacyclic codes over R. As an application, we present a construction of a class of maximal entanglement EAQECCs by employing a class of Hermitian LCD $(1-u)$-constacyclic codes over R of length n.

The work is organized as follows. Section 2 gives preliminaries and background. In Section 3, we give the characterizations of Hermitian LCD codes and Hermitian LCD constacyclic codes. In Section 4, LCD codes with respect to the symplectic inner over finite fields product by employing codes over R. Based on aforementioned results, a construction of a class of maximal entanglement EAQECCs is obtained in Section 5.

2 Preliminaries

2.1 Codes over ring R

Let $\mathbb{F}_{q^2}$ denote the finite field of order q^2, where $q = p^m$, and p is a prime number. Consider the ring $R = \mathbb{F}_{q^2} + u\mathbb{F}_{q^2}$, where $u^2 = 0$. The ring R is a finite chain ring with a unique maximal ideal $\langle u \rangle$, i.e., R is a local ring. The units of R are the elements $\{a + ub | a \neq 0, a, b \in \mathbb{F}_{q^2}\}$ and the residue field is $\mathbb{F}_{q^2}$.

A linear code C over R of length n is an R-submodule of R^n. The Hamming weight of a codeword $c \in C$, denoted by $w_H(c)$, is the number of its nonzero entries. The Hamming distance of two codewords x, y, denoted by $d_H(x, y)$, is the number of entries where they are different. The Hamming minimum distance of a linear code C is defined by $d_H = d_H(C) = \min\{w_H(c) :$ for all nonzero $c \in C\}$, and the minimum distance is bounded by the Singleton bound: $d_H \leq n-k+1$. A code meeting the bound is called MDS. For any $x = a+ub \in R$, where $a, b \in \mathbb{F}_{q^2}$, the conjugate of x is defined as $\bar{x} = \bar{a} - u\bar{b}$, where $\bar{a} = a^q, \bar{b} = b^q$. Let $c = (c_1, c_2, \cdots, c_n), c' = (c'_1, c'_2, \cdots, c'_n) \in C$, the Hermitian inner product of c, c' is defined by $\langle c, c' \rangle_H = \sum_{i=1}^n \bar{c}_i c'_i$. For a linear code C over R, the Hermitian dual of C is defined as $C^{\perp_H} = \{x \in R^n : \langle x, c \rangle_H = 0 \text{ for all } c \in C\}$.

2.2 Notations about symplectic inner product

Next, we introduce some basic results and notations about symplectic inner product.

For $x = (u|v), y = (u'|v') \in \mathbb{F}_{q^2}^{2n}$, where $u, v, u', v' \in \mathbb{F}_{q^2}^n$, the symplectic inner product of x, y is defined by

$$\langle x, y \rangle_S = x\Omega y^T = \langle u, v' \rangle_E - \langle u', v \rangle_E,$$

where $\langle , \rangle_E$ denotes the Euclidean inner product, $\Omega = \begin{pmatrix} \mathbf{0} & I_n \\ -I_n & \mathbf{0} \end{pmatrix}$, I_n is the identity matrix of order n and y^T denotes transposed vector of y. An $[n, k]$ linear code C over $\mathbb{F}_{q^2}$ is a k-dimensional subspace of $\mathbb{F}_{q^2}^n$. For an $\mathbb{F}_{q^2}$-linear code C in $\mathbb{F}_{q^2}^{2n}$, define the symplectic dual code as

$$C^{\perp_S} = \{x \in \mathbb{F}_{q^2}^{2n} : x\Omega c^T = 0 \text{ for all } c \in C\}.$$

It is easy to show that $C^{\perp_S}$ is an $\mathbb{F}_{q^2}$-linear code C in $\mathbb{F}_{q^2}^{2n}$, and dim $C^{\perp_S}$ + dim $C = 2n$.

For a vector $(u|v) \in \mathbb{F}_{q^2}^{2n}$, the symplectic weight is defined by $\mathrm{w}_S(u|v) = |\{i : u_i \neq 0, \text{ or } v_i \neq 0\}|$, where $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_{q^2}^n$. For two vectors $(u|v), (u'|v') \in \mathbb{F}_{q^2}^{2n}$, the symplectic distance is defined by $d_S((u|v), (u'|v')) = \mathrm{w}_S(u-u'|v-v')$. The symplectic minimum distance of a linear code C is defined by

$$d_S = d_S(C) = \min\{wt_S(u|v) : \text{ for all nonzero } (u|v) \in C\}.$$

Then it is straightforward to verify that an $[2n, k]$ linear code C also satisfies the symplectic Singleton bound: $k + 2d_S \leq 2n+2$. A code achieving the bound is called a simplectic MDS code.

3 LCD codes over ring R

3.1 Hermitian LCD codes over R

A linear code C over R is called a Hermitian LCD code if and only if $C \cap C^{\perp_H} = \{\mathbf{0}\}$. The purpose of this section is to study Hermitian LCD codes. Therefore, the following notations are given first.

By $M_{m\times l}(R)$, we mean the set of all $m \times l$ matrices over R. For $A \in M_{m\times l}(R)$, A^T denotes the transpose matrix of A, $\bar{A}$ denotes the conjugate matrix of A and $A^\dagger$ denotes the conjugate transpose of A over R. If the rows of A are linearly independent, then we say that A is a full-row-rank (FRR) matrix. If there is an $l \times m$ matrix B over R such that $AB = I$, then we say that A is right-invertible and B is a right inverse of A. If $m = l$ and the determinant of A is a unit of R, then we say that A is nonsingular.

The following two results about FRR matrices over R appear in [8].

Lemma 1. *$A \in M_{m\times l}(R)$ is FRR if and only if A is right-invertible.*

Lemma 2. *Let $A \in M_{m\times m}(R)$. The following statements are equivalent:*
(1) A is invertible.
(2) A is nonsingular.
(3) A is FRR.

In [5], we know that any nonzero linear code over R is permutation-equivalent to a code C with generator matrix

$$G = \begin{pmatrix} I_{k_1} & A & B_1 + uB_2 \\ \mathbf{0} & uI_{k_2} & uD \end{pmatrix} \tag{1}$$

where A, B_1, B_2, and D are matrices over $\mathbb{F}_{q^2}$. C is a free code if and only if $k_2 = 0$. Define the residue code $\mathrm{Res}(C)$ and the torsion code $\mathrm{Tor}(C)$ as: $\mathrm{Res}(C) = \{x \in \mathbb{F}_{q^2}^n : \exists y \in \mathbb{F}_{q^2}^n, s.t. x + uy \in C\}$, and $\mathrm{Tor}(C) = \{x \in \mathbb{F}_{q^2}^n : ux \in C\}$.

Similar to Proposition 1.2 in [25], we easily get the generator matrix of the Hermitian dual code of C.

Proposition 3. *The Hermitian dual code $C^{\perp_H}$ of the linear code C over R of length n with generator matrix (1) has generator matrix*

$$\begin{pmatrix} (B_1 + uB_2)^\dagger + D^\dagger A^\dagger & D^\dagger & I_{n-k_1-k_2} \\ uA^\dagger & uI_{k_2} & 0 \end{pmatrix}.$$

In terms of the generator matrix, we now give a sufficient condition for a linear code C over R to be Hermitian LCD, which is similar to Theorem 3.5 in [18].

Theorem 4. *Let C be a code over R of length n with generator matrix G in standard form as in (1). If the $k \times k$ matrix $G\bar{G}^T$ is nonsingular, then C is a Hermitian LCD code, where k is the number of rows of G.*

Proof. Let H be a generator matrix of $C^{\perp_H}$. For any $c \in C \cap C^{\perp_H}$, there are $x \in R^k$ and $y \in R^{n-k}$, such that $c = xG = yH$, which implies that $xG\bar{G}^T = yH\bar{G}^T = 0$. Since $G\bar{G}^T$ is invertible, we have $x = 0$, and then $c = 0$. Hence $C \cap C^{\perp_H} = \{\mathbf{0}\}$, i.e., C is Hermitian LCD. □

We have the following corollary when C is a free code over R.

Corollary 5. *Let C be a free code over R with generator matrix G in standard form as in (1). Then C is a Hermitian LCD code if and only if the $k \times k$ matrix $G\bar{G}^T$ is nonsingular, where k is the number of rows of G.*

Proof. The sufficiency follows from Theorem 4, and we will only prove the necessity. Assume that $g_1, \ldots, g_k$ are row vectors of the matrix G. Since C is a free code, then $g_1, \ldots, g_k$ are linearly independent over R. Suppose that $G\bar{G}^T$ is singular, then there is a nonzero vector $x \in R^k$ such that $xG\bar{G}^T = 0$. Note that $c = xG$ is a nonzero vector of C and any codeword $c' \in C$ can be written as $c' = x'G$ for some $x' \in R^k$. So we have

$$c\bar{c'}^T = xG\bar{G}^T(\bar{x'})^T = 0$$

and then $c \in C^{\perp_H}$. It follows that $C \cap C^{\perp_H} \neq \{0\}$, i.e., C is not Hermitian LCD.

□

Next, we prove that there does not exist a non-free Hermitian LCD code over R.

An R-module C of rank k is projective if there is an R-module M such that R^k and $C \oplus M$ are isomorphic. Let A and B be R-modules. If $A \oplus B$ is free, then A and B are projective. For more information, please refer to [13].

Lemma 6 ([13]). *Any projective module over a local ring is free.*

Theorem 7. *Any Hermitian LCD code over R of length n is free.*

Proof. Let C be a Hermitian LCD code over R of length n. Then, $C \oplus C^{\perp_H} = R^n$, so the R-module $C \oplus C^{\perp_H}$ is free. It follows that C is projective. Now C is a finitely generated projective R -module and R is a local ring and by Lemma 6, C is free. □

3.2 Hermitian LCD constacyclic codes over R

Let C be a linear code over R of length n. From now on, we assume that $\gcd(n, q) = 1$, and γ is a unit in R. For any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$, if $(\gamma c_{n-1}, c_0, \ldots, c_{n-2})$ is also a codeword of C, then we say that C is a γ-constacyclic code over R. A linear code C is γ-constacyclic if and only if its polynomial representation is an ideal of the quotient ring $R[x]/ < x^n - \gamma >$.

The projection $\mu : R \to \mathbb{F}_{q^2}$ extends naturally to $R[x] \to \mathbb{F}_{q^2}[x]$ as $\mu(f(x)) = \sum_i \mu(f_i) x^i$ for $f(x) = \sum_i f_i x^i$, and also a projection $R^n \to \mathbb{F}_{q^2}^n$ as

$$\mu(c) = (\mu(c_0), \mu(c_1), \cdots, \mu(c_{n-1})) \text{ for } c = (c_0, c_1, \cdots, c_{n-1}).$$

Thus for any nonempty subset C of $R^n, \mu(C) = \{\mu(c) : c \in C\}$.

A polynomial $f(x) \in R[x]$ is monic if its leading coefficient is 1, and $f(x)$ is a unit if and only if $\mu(f(x))$ is a unit. Two non-unit polynomials $f(x), g(x) \in R[x]$ are coprime if there are $u(x), v(x) \in R[x]$ such that $f(x)u(x) + g(x)v(x) = 1$. A non-unit $f(x) \in R[x]$ is called basic irreducible if $\mu(f(x))$ is irreducible. Obviously, if $\mu(f(x))$ is irreducible, then so is $f(x)$. It is well known that any $f(x) \in R[x]$ which is not divisible by γ can be written as $f(x) = \epsilon f_1(x)$, where $\epsilon \in R[x]$ is a unit and $f_1(x)$ is monic. Let $f(x) = \sum_i f_i x^i$ be a polynomial in $R[x]$ whose degree is k, where f_0 is a unit in R, the reciprocal polynomial of $f(x)$ is $f^*(x) = x^k f(x^{-1})$. We denote by $f^\dagger(x)$ the conjugation of the reciprocal polynomial of $f(x)$, i.e., $f^\dagger(x) = \overline{f^*(x)}$.

The Hensel lifting plays a key role in the construction of constacyclic codes over R.

Theorem 8 ([21]). *Let $f(x) \in R[x]$ be monic. Assume that there are pairwise coprime monic polynomials $g_1(x), g_2(x), \ldots, g_k(x) \in \mathbb{F}_{q^2}[x]$ such that $\mu(f(x)) = \prod_{i=1}^k g_i(x)$. Then, there are pairwise coprime monic polynomials $f_1(x), f_2(x), \ldots, f_k(x) \in R[x]$ such that $f(x) = \prod_{i=1}^k f_i(x)$ and $\mu(f_i(x)) = g_i(x)$ for $i = 1, 2, \ldots, k$.*

It is easy to prove the following proposition.

Proposition 9. *The dual of any γ-constacyclic code over R of length n is $\bar{\gamma}^{-1}$-constacyclic.*

Lemma 10 ([2])**.** *Let C be a free code over R of length n. If C is both α-constacyclic and β-constacyclic for α, β units in R with $\mu(\alpha) \neq \mu(\beta)$, then either $C = \{\mathbf{0}\}$ or $C = R^n$.*

Lemma 11 ([9])**.** *Suppose that $f_1(x)$ and $f_2(x)$ are monic polynomials over R dividing $x^n - \gamma$. If $C_1 = \langle f_1(x) \rangle$ and $C_2 = \langle f_2(x) \rangle$, then $C_1 \cap C_2 = \langle f(x) \rangle$, where $\mu(f(x)) = lcm(\mu(f_1(x)), \mu(f_2(x)))$.*

Theorem 12. *If $\mu(\gamma\bar{\gamma}) \neq 1$, then any free γ-constacyclic code over R of length n is Hermitian LCD.*

Proof. Let C be a free γ-constacyclic code over R of length n. According to Proposition 9, $C^{\perp_H}$ is a $\bar{\gamma}^{-1}$-constacyclic code. Then, $C \cap C^{\perp_H}$ is both γ-constacyclic and $\bar{\gamma}^{-1}$-constacyclic. When $\mu(\gamma\bar{\gamma}) \neq 1$, by Lemma 10, we have $C \cap C^{\perp_H} = \{\mathbf{0}\}$, since $C \cap C^{\perp_H}$ can not be R^n. Therefore, C is Hermitian LCD. □

Thus, in order to obtain all γ-constacyclic Hermitian LCD codes, we need to consider only the case when $\mu(\gamma\bar{\gamma}) = 1$. The following result gives a necessary and sufficient condition for a γ-constacyclic code over R of length n to be Hermitian LCD, where $\mu(\gamma\bar{\gamma}) = 1$.

Theorem 13. *Let $C = \langle g(x) \rangle$ be a γ-constacyclic code over R of length n and $x^n - \gamma = g(x)h(x)$. If $\gamma\bar{\gamma} = 1$, then C is Hermitian LCD if and only if $g(x) = g(x)^\dagger$.*

Proof. Let $C = \langle g(x) \rangle$, where $x^n - \gamma = g(x)h(x)$. It is not hard to verify that $C^{\perp_H} = \left\langle h(x)^\dagger \right\rangle$. According to Lemma 11, we obtain $C \cap C^{\perp_H} = \langle f(x) \rangle$, where $\mu(f(x)) = \mathrm{lcm}(\mu(g(x)), \mu(h(x)^\dagger))$. If $\gamma\bar{\gamma} = 1$, then $g(x)^* h(x)^* = x^n - \gamma^{-1}$, and then $g(x)^\dagger h(x)^\dagger = x^n - \bar{\gamma}^{-1} = x^n - \gamma = g(x)h(x)$.

If $g(x) = g(x)^\dagger$, then $h(x) = h(x)^\dagger$. Since $x^n - \gamma = g(x)h(x)$, it follows that $\mu(x^n - \gamma) = \mu(g(x))\mu(h(x))$, which implies that $\mathrm{lcm}(\mu(g(x)), \mu(h(x)^\dagger) = \mathrm{lcm}(\mu(g(x)), \mu(h(x))) = \mu(g(x))\mu(h(x))$. So we have, $f(x) = g(x)h(x) = x^n - \gamma$, i.e., $C \cap C^{\perp_H} = \{\mathbf{0}\}$. Therefore, C is Hermitian LCD.

Conversely, if C is Hermitian LCD, then $f(x) = x^n - \gamma = g(x)h(x)$. Then, $\mu(f(x)) = \mu(x^n - \gamma) = \mu(g(x))\mu(h(x)) = \mathrm{lcm}(\mu(g(x)), \mu(h(x)^\dagger) = \mu(g(x))\mu(h(x)^\dagger)$. So we have $\mu(h(x)) = \mu(h(x)^\dagger)$ and then $\mu(g(x)) = \mu(g(x)^\dagger)$. Therefore, $g(x) = g(x)^\dagger$. □

Taking $\gamma = 1 - u$ in Propositions 9 and 13, we can obtain the following results.

Corollary 14 ([24])**.** *Let C be a $(1-u)$-constacyclic code over R of length n if and only if $C^{\perp_H}$ is a $(1-u)$-constacyclic code over R of length n.*

Corollary 15. *Let $C = \langle g(x) \rangle$ be a $(1-u)$-constacyclic code over R of length n and $x^n - (1-u) = g(x)h(x)$, then C is Hermitian LCD if and only if $g(x) = g(x)^\dagger$.*

Similar to [15], let $n' \in \{0, 1, \ldots, p-1\}$ such that $nn' \equiv 1(\bmod p)$ and $\beta = 1 + n'u$, where $(n, p) = 1$. We have the following ring isomorphism map $\mu : R[x]/\langle x^n - 1\rangle \to R[x]/\langle x^n - (1-u)\rangle$, where $\mu(c(x)) = c(\beta x)$. The map can extend naturally to $R^n \to R^n$ as $\mu(c) = (c_0, \beta c_1, \cdots, \beta^{n-1}c_{n-1})$, where $c = (c_0, c_1, \cdots, c_{n-1})$. When C is a cyclic code if and only if $\mu(C)$ is a $(1-u)$-constacyclic code. Next, we limit our discussion to $R = \mathbb{F}_{2^{2m}} + u\mathbb{F}_{2^{2m}}$. As a immediate consequence, let $\beta = 1 - u$, we obtained the following method to decompose $x^n - (1-u)$ into monic basic irreducible polynomials in $R[x]$. Let $g_1(x), g_2(x), \ldots, g_r(x)$ be monic basic irreducible polynomials in $R[x]$ such that $x^n - 1 = g_1(x)g_2(x)\cdots g_r(x)$, and let $f_i(x) = (1-u)^{\deg(g_i)}g_i((1-u)x)$ for $1 \leq i \leq r$. Note that $(1-u)^l = 1-u$ if l is odd and $(1-u)^l = 1$ if l is even. Hence the polynomial $x^n-(1-u)$ factors uniquely into basic irreducible polynomials in $R[x]$ as $f_1(x)f_2(x)\cdots f_r(x)$.

Example 16. In $(F_4 + uF_4)[x]$, where $F_4 = \{0, 1, \omega, \omega^2\}$ and $1 + \omega + \omega^2 = 0$. For $x^5 - 1 = g_1(x)g_2(x)g_3(x)$, where $g_1(x) = x - 1, g_2(x) = x^2 + \bar{\omega}x + 1, g_3(x) = x^2 + \omega x + 1$. Then, $x^5 - (1-u) = f_1(x)f_2(x)f_3(x)$, where $f_1(x) = x - (1-u), f_2(x) = x^2 + \bar{\omega}(1-u)x + 1, f_3(x) = x^2 + \omega(1-u)x + 1$.

The following result give a technique to find the Hamming minimum distance of a $(1-u)$-constacyclic code over R of length n.

Theorem 17. *Let C be a $(1-u)$-constacyclic code over R of length n, then $d_H(C) = d_H(Tor(C))$.*

Proof. Let's assume that there is a polynomial $r(x) \in \mathrm{Tor}(C)$, such that $d_H(\mathrm{Tor}(C)) = w_H(r(x))$. Then $ur(x) \in C$, and $w_H(r(x)) = w_H(ur(x))$, and so we have $d_H(\mathrm{Tor}(C)) \geq d_H(C)$. Conversely, suppose $d_H(C) = w_H(c(x))$, where $c(x) \in C$. If all the coefficients of $c(x)$ are zero divisors of R, then we'll get a codeword in C with Hamming weight less than $w_H(c(x))$, which is a contradiction. Therefore, any coefficient of $c(x)$ is either zero or a unit in R. So we must have some $t(x) \in \mathrm{Tor}(C)$ such that $ut(x) = c(x)$. Then, $w_H(c(x)) = w_H(ut(x)) = w_H(t(x))$, and hence $d_H(\mathrm{Tor}(C)) \leq d_H(C)$. Thus, $d_H(C) = d_H(\mathrm{Tor}(C))$. □

4 Symplectic LCD codes from codes over ring R

The goal of this section is to construct q^2-ary LCD codes with respect to the symplectic inner product by employing linear codes over R.

Definition 18. A linear code C is called a symplectic LCD code if $C \cap C^{\perp_S} = \{\mathbf{0}\}$.

A symplectic LCD and also symplectic MDS code will be abbreviated to symplectic LCD MDS.

The following conclusion is a characterization of symplectic LCD codes.

Theorem 19. *If G is a generator matrix for the $\mathbb{F}_{q^2}$-linear code C in $\mathbb{F}_{q^2}^{2n}$ with parameters $[2n, k]$, then C is a symplectic LCD code if and only if the $k \times k$ matrix $G\Omega G^T$ is nonsingular, where $\Omega = \begin{pmatrix} \mathbf{0} & I_n \\ -I_n & \mathbf{0} \end{pmatrix}$.*

Proof. Suppose that $G\Omega G^T$ is singular, then there is a nonzero vector $a \in \mathbb{F}_{q^2}^k$, such that $a(G\Omega G^T) = \mathbf{0}$. Let $c \in C\backslash\{\mathbf{0}\}$, such that $c = aG$, then $c\Omega G^T = a(G\Omega G^T) = \mathbf{0}$, so that $c \in C^{\perp_S}$, which is a contradiction.

For the converse, suppose that $G\Omega G^T$ is nonsingular. For every $a \in C \cap C^{\perp_S}$, if $a \in C$, then $\exists v \in \mathbb{F}_{q^2}^k$, such that $a = vG$, then $a\Omega[G^T(G\Omega G^T)^{-1}G] = v[(G\Omega G^T)(G\Omega G^T)^{-1}]G = vG = a$. If $a \in C^{\perp_S}$, which implies that $a\Omega G^T = \mathbf{0}$, then $a\Omega[G^T(G\Omega G^T)^{-1}G] = a\Omega G^T(G\Omega G^T)^{-1}G = \mathbf{0}$. Therefore, $C \cap C^{\perp_S} = \{\mathbf{0}\}$. □

Now we are going to discuss how to construct symplectic LCD codes by using linear codes over the ring R. For $x = a + ub \in R$, where $a, b \in \mathbb{F}_{q^2}$, let $\varphi(x) = (b, a + b)$. This Gray map can be naturally extended to R^n as follows: Let $c = (c_0, c_1, \cdots, c_{n-1})$, then $\varphi(c) = (b_0, b_1, \cdots, b_{n-1}, a_0 + b_0, a_1 + b_1, \cdots, a_{n-1} + b_{n-1})$, where $c_i = a_i + ub_i$ with $a_i, b_i \in \mathbb{F}_{q^2}$ for $0 \le i \le n - 1$. Let $\varphi(C) = \{\varphi(c) : \text{ for all } c \in C\}$. After a simple calculation, we will find the following result. We first consider the generator matrix of $\varphi(C)$.

Lemma 20. *If C is a linear code over R of length n with generator matrix G in standard form as in (1), then the generator matrix of $\varphi(C)$ is*

$$\varphi(G) = \begin{pmatrix} I_{k_1} & A & B_1 & I_{k_1} & A & B_1 \\ \mathbf{0} & I_{k_2} & D & \mathbf{0} & I_{k_2} & D \\ \mathbf{0} & \mathbf{0} & B_2 & I_{k_1} & A & B_1 + B_2 \end{pmatrix},$$

and $\varphi(C)$ is a q^2-ary $[2n, 2k_1 + k_2]$ linear code.

Theorem 21. *Let C be a linear code over R of length n. If C is Hermitian LCD, then $\varphi(C)$ is symplectic LCD over $\mathbb{F}_{q^2}$ of length $2n$.*

Proof. For any $c \in C, c' \in C^{\perp_H}$, where $c = \mathbf{a} + u\mathbf{b}, c' = \mathbf{a}' + u\mathbf{b}'$, we have $\langle c, c'\rangle_H = \langle(\mathbf{a} + u\mathbf{b}), (\mathbf{a}' - u\mathbf{b}')\rangle_E = \langle \mathbf{a}, \mathbf{a}'\rangle_E + u(\langle \mathbf{b}, \mathbf{a}'\rangle_E - \langle \mathbf{a}, \mathbf{b}'\rangle_E) = 0$, which implies that $\langle\varphi(c), \varphi(c')\rangle_S = 0$. So we have $\phi(C^{\perp_H}) \subseteq \phi(C)^{\perp_S}$. Since the map φ is bijection, $\varphi(C^{\perp_H}) = \varphi(C)^{\perp_S}$.

If C is Hermitian LCD, then $C \cap C^{\perp_H} = \{\mathbf{0}\}$. We can easily obtain that $\varphi(C \cap C^{\perp_H}) \subseteq \varphi(C) \cap \varphi(C^{\perp_H})$. Again because φ is bijection, we have $\varphi(C) \cap \varphi(C)^{\perp_S} = \varphi(C) \cap \varphi(C^{\perp_H}) = \varphi(C \cap C^{\perp_H}) = \{\mathbf{0}\}$. Thus $\varphi(C)$ is symplectic LCD. □

From the definition of the Gray map, we easily obtain the following result.

Lemma 22. *The Gray map φ is a distance-preserving map from R^n (Hamming distance) to $\mathbb{F}_{q^2}^{2n}$(symplectic distance).*

We have the following corollary when C is a free code over R.

Corollary 23. *Let C be a free linear code over R of length n. Then C is an $[n, k_1, d_H]$ Hermitian LCD code if and only if $\varphi(C)$ is an $[2n, 2k_1, d_S]$ symplectic LCD code, where $d_S = d_H$. Further, if C is MDS, then $\varphi(C)$ is symplectic MDS.*

Proof. The sufficiency follows from Theorem 21, and it just needs to prove the necessity. The generator matrix of C is $G = \begin{pmatrix} I_{k_1} & A & B_1 + uB_2 \end{pmatrix}$, since C is free. According to Lemma 20, the generator matrix of $\varphi(C)$ is

$$\varphi(G) = \begin{pmatrix} I_{k_1} & A & B_1 & I_{k_1} & A & B_1 \\ \mathbf{0} & \mathbf{0} & B_2 & I_{k_1} & A & B_1 + B_2 \end{pmatrix}.$$

According to Theorem 19, if $\varphi(C)$ is a symplectic LCD code, then $\varphi(G)\Omega\varphi(G)^T$ is nonsingular. Since

$$\varphi(G)\Omega\varphi(G)^T = \begin{pmatrix} \mathbf{0} & I_{k_1} + AA^T + B_1{B_1}^T \\ -(I_{k_1} + AA^T + B_1{B_1}^T) & B_2{B_1}^T - B_1{B_2}^T \end{pmatrix},$$

so we have $I_{k_1} + AA^T + B_1{B_1}^T$ is nonsingular. then

$$G\bar{G}^T = I_{k_1} + AA^T + B_1{B_1}^T + u(B_2{B_1}^T - B_1{B_2}^T)$$

is also nonsingular. Hence, C is Hermitian LCD. The parameters of C are easy to obtain according to Lemma 22. □

Example 24. Let $R = \mathbb{F}_2 + u\mathbb{F}_2$, and C be a linear code over R with parameters $[5, 3, 2]$, whose generator matrix is given by $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1+u \\ 0 & 1 & 0 & 1 & 1+u \\ 0 & 0 & 1 & 1 & 1+u \end{pmatrix}$. Note that $G\bar{G}^T = I_3$ is nonsingular, then C is a Hermitian LCD code from Theorem 19. We can easily verify that C satisfies the conditions of Corollary 23, therefore $\varphi(C)$ is a binary symplectic LCD code with parameters $[10, 6, 2]$.

5 Maximal entanglement EAQECCs

An $[[n, k, d; c]]$ EAQECC encodes k logical qubits into n physical qubits using c copies of maximally entangled states, and d is the minimum distance of the code.

The following is the explicit symplectic method of constructing EAQECCs from classical linear codes([10]).

Theorem 25. *Let $C \subseteq \mathbb{F}_{q^2}^{2n}$ be an $(n-k)$-dimensional $\mathbb{F}_{q^2}$-linear space and $H = [H_X|H_Z]$ be a matrix whose row space is C. Let $C' \subseteq \mathbb{F}_{q^2}^{2(n+c)}$ be an $\mathbb{F}_{q^2}$-linear space such that its projection to the coordinates $1, 2, \cdots, n, n+c+1, n+c+2, \cdots, 2n+c$ equals C and $C' \subseteq (C')^{\perp_S}$, where c is the minimum required number of maximally entangled quantum states in $\mathbb{C}^{q^2} \otimes \mathbb{C}^{q^2}$. Then,*

$$2c = rank(H_X H_Z^T - H_Z H_X^T) = dim_{\mathbb{F}_{q^2}} C - dim_{\mathbb{F}_{q^2}} (C \cap C^{\perp_S}).$$

The encoding quantum circuit is constructed from C', and it encodes $k + c$ logical qudits in $\mathbb{C}^{q^2} \otimes \cdots \otimes \mathbb{C}^{q^2}$ into n physical qudits using c maximally entangled pairs. The minimum distance is $d = d_S(C^{\perp_S} \backslash (C \cap C^{\perp_S}))$. In sum, C provides an $[[n, k+c, d; c]]$ EAQECC over the field $\mathbb{F}_{q^2}$.

An EAQECC with $c = n - k$ is called a maximal entanglement EAQECC [14]. It was shown that maximal entanglement EAQECCs can achieve the entanglement-assisted quantum capacity of a depolarizing channel. When $C \cap C^{\perp_S} = \{\mathbf{0}\}$, i.e., C is symplectic LCD, according the theorem above, C provides a maximal entanglement EAQECC. By the Singleton bound for EAQECCs$[[n, k, d; c]]$ [1], we have $2(d - 1) \leq n - (k - c)$ and an EAQECC meeting this bound is called an MDS EAQECC.

Next, based on Hermitian LCD $(1-u)$-constacyclic codes over R introduced in Section 3, the Gray map and the above symplectic construction method, we obtain the following new class of q^2-ary quantum codes.

Theorem 26. *There exists a maximal entanglement EAQECC over $\mathbb{F}_{q^2}$ with parameters $[[n, n-k, d_\tau^\perp; k]]$ or $[[n, k, d_\tau; n-k]]$, where $d_\tau^\perp = d_H(Tor(C^{\perp_H})$ and $d_\tau = d_H(Tor(C)$.*

Proof. Let C be a Hermitian LCD $(1 - u)$-constacyclic code of length n over R, applying Theorems 21 and 25, we get a symplectic LCD cyclic code $\varphi(C)$ of length $2n$ over $\mathbb{F}_{q^2}$ which provides a class of q^2-ary $[[n, n - k, d; k]]$ quantum codes which is maximal entanglement. The Hamming minimum distance of the quantum code is $d = d_S(\varphi(C)^{\perp_S})$, since $\varphi(C)$ is symplectic LCD. From Lemma 22 and Theorem 17, $d = d_H(\mathrm{Tor}(C^{\perp_H})$, which is denoted as $d_\tau^\perp$. The remaining is similar. □

From the theorem above, we can see that a class of maximal entanglement EAQECCs can be obtained if we found a class of Hermitian LCD constacyclic codes C. Further, if C is MDS, then the quantum code is MDS EAQECC. This is different from the previous case of Hermitian or Euclidean inner products. We believe that more maximal entanglement EAQECCs can be obtained from this method.

References

[1] T. A. Brun, I. Devetak, M. H. Hsieh. Correcting quantum errors with entanglement. Science, 314: 436-439, 2006.

[2] S. Bhowmick, A. Fotue-Tabue, E. Martinez-Moro, R. Bandi, S. Bagchi. Do non-free LCD codes over finite commutative Frobenius rings exist? arXiv: 1901.10836v1, 2019.

[3] C. Carlet and S. Guilley. Complementary dual codes for counter-measures to side-channel attacks. In: Coding Theory and Applications, 97-105, 2015.

[4] C. Carlet, S. Mesnager, C. Tang, Y. Qi. Euclidean and Hermitian LCD MDS codes. Des. Codes Cryptogr. 1-14, 2014.

[5] S. T. Dougherty, P. Gaborit, M. Harad, et al. Type II codes over $F_2 + uF_2$. IEEE Trans. Inform. Theory, 45(1): 32-45, 1999.

[6] S. T. Dougherty, J. L. Kim, B. Ozkaya, L. Sok, P. Sole. The combinatorics of LCD codes: linear programming bound and orthogonal matrices. International Journal of Information and Coding Theory, 4(2/3): 116, 2015.

[7] M. Esmaeili, S. Yari. On complementary-dual quasi-cyclic codes. Finite Fields Appl. 15:375-386, 2009.

[8] Y. Fan, S. Ling, H. Liu. Matrix product codes over finite commutative Frobenius rings. Des. Codes Cryptogr. 71, 2014. 201-227

[9] A. Fotue-Tabue, E. Martnez-Moro, T. Blackford. On polycyclic codes over a finite chain ring. Adv. Math. Commun. arXiv:1811.07975, 2018.

[10] C. Galindo, F. Hernando, R. Matsumoto, D. Ruano. Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quantum Inf. Process. 18(4): 116, 2019.

[11] K. Guenda, S. Jitman, T.A. Gulliver. Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. 86: 121-136, 2018.

[12] C. Guneri, B. Ozkaya, and P. Sole. Quasi-cyclic complementary dual codes. Finite Fields Appl., 42: 67-80, 2016.

[13] I. Kaplansky. Projective modules. Ann. of Math., 68: 372-377, 1958.

[14] C.-Y. Lai, T. A. Brun, M. M. Wilde. Duality in entanglement-assisted quantum error correction. IEEE Trans. Inf. Theory 59(6): 4020-4024, 2013.

[15] S. Ling, J. Blackford. $Z_{p^{k+1}}$-linear code. IEEE Trans. Inf. Theory. 48(9): 2592-2606, 2002.

[16] S. Li, C. Ding, H. Liu. Parameters of two classes of LCD BCH codes. arxiv: 1608.02670, 2016.

[17] C. Li, C. Ding, S. Li. LCD cyclic codes over finite fields. IEEE Trans. Inf. Theory, 63(7): 4344-4356, 2017.

[18] X. Liu, H. Liu. LCD codes over finite chain rings. Finite Fields Appl., 34: 1-19, 2015.

[19] L. Lu, R. Li, L. Guo, Fu Q. Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. Quantum Inf. Process. 14: 165-182, 2015.

[20] J. L. Massey. Linear codes with complementary duals. Discrete Math., 106/107: 337-342, 1992.

[21] B.R. McDonald. Finite Rings with Identity. Marcel Dekker, New York, 1974.

[22] J. Qian, L Zhang. Entanglement-assisted quantum codes from arbitrary binary linear codes. Des. Codes Cryptogr. 77: 193-202, 2015.

[23] J. Qian, L Zhang. On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. 87: 1565-1572, 2018.

[24] Y. Tang, T. Yao, Z. Sun, S. Zhu, X. Kai. Nonbinary quantum codes from constacyclic codes over polynomial residue rings. Quantum Inf. Process. 19(3): 83-96, 2020.

[25] Z.X. Wan. Quaternary Codes. World Scientific, Singapore, 1997.

[26] X. Yang, J. L. Massey. The necessary and sufficient condition for a cyclic code to have a complementary dual. Discret. Math. 126: 391-393, 1994.