Bull. Malays. Math. Sci. Soc. (2021) 44:3377–3390
https://doi.org/10.1007/s40840-021-01114-x

BULLETIN *of the*
MALAYSIAN MATHEMATICAL
SCIENCES SOCIETY
http://www.springer.com/mathematics/journal/40840

Constructions of Symplectic LCD MDS Codes

H. Q. Xu[1,2] · W. Du[2]

Received: 27 February 2020 / Revised: 14 September 2020 / Accepted: 25 March 2021 /
Published online: 9 April 2021

Abstract
Linear complementary dual (LCD) codes are linear codes whose intersections with their duals are trivial. In this paper, characterizations of LCD codes with respect to the symplectic inner product, i.e. symplectic LCD codes, over finite fields are given. Some methods for constructing symplectic LCD codes and symplectic LCD MDS codes are presented. As an application, a class of symplectic LCD MDS codes is constructed by employing Vandermonde matrices, and the corresponding MDS maximal entanglement entanglement-assisted quantum error-correcting codes (EAQECCs) are constructed.

Keywords Linear codes · Complementary dual · Entanglement-assisted quantum codes · MDS codes · Vandermonde matrix

Mathematics Subject Classification 11T71 · 94B05

1 Introduction

In [21], Massey first introduced the concept of LCD codes, which have been widely applied in data storage, communications systems, and cryptography. Carlet and Guilley [4] 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 a cyclic code to be an LCD code has been provided by Yang and Massey in [30]. In [13], quasi-cyclic codes that are LCD have been characterized and studied using their concatenated structures. With the development of classical error-correcting

Communicated by Miin Huey Ang.

✉ H. Q. Xu
heqianxu@mail.ustc.edu.cn ; heqianx@hfnu.edu.cn

[1] School of Mathematical Sciences, University of Science and Technology of China, Hefei 230027, China

[2] School of Mathematics and Statistics, Hefei Normal University, Hefei 230601, China

codes and their applications to LCD codes, more and more works have been done([4–7,9,14,18,25–28]). In [3], Brun et al. introduced EAQECCs, which allow the use of classical error-correcting codes without orthogonality conditions. Additionally, there is a close link between EAQECCs and LCD codes. Recently, the application of LCD codes in constructing good EAQECCs has aroused the interest of researchers. With the development of classical error-correcting codes and the applications to EAQECCs, people have extensively studied the Euclidean, Hermitian and symplectic inner product and investigated the corresponding LCD codes, and many classes of maximal entanglement EAQECCs have been constructed (see [10,12,15–17,19,22,23,29]).

In this work, the paper will mainly focus on LCD MDS codes over finite fields with respect to the symplectic inner product. As an application of symplectic LCD MDS codes, we present a construction of a class of MDS maximal entanglement EAQECCs.

The work is organized as follows. Section 2 gives preliminaries and background. In Sect. 3, we give the characterizations of symplectic LCD codes. Based on aforementioned results, we present some constructions of symplectic LCD MDS codes in Sects. 4 and 5, and a construction of a class of MDS maximal entanglement EAQECCs is obtained in Sect. 6.

2 Preliminaries

Let $\mathbb{F}_q$ denotes the finite field of order q, where q is a prime power. An $[n, k, d]$-linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d, and the minimum distance is bounded by the Singleton bound $d \leq n - k + 1$. A code meeting the bound is called maximum distance separable (MDS). For $u = (u_1, u_2, \cdots, u_n)$, $v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_q^n$, the Euclidean inner product $\langle , \rangle_E$ is defined by $\langle u, v\rangle_E = \sum_{i=1}^n u_i v_i$. For an $\mathbb{F}_q$-linear code C in $\mathbb{F}_q^n$, define the Euclidean dual $C^{\perp_E} = \{x \in \mathbb{F}_q^n : \langle x, c\rangle_E = 0 \text{ for all } c \in C\}$. For any $x \in \mathbb{F}_{q^2}$, the conjugate of x is defined as $\bar{x} = x^q$. For a matrix $A = \left(a_{ij}\right)$ over $\mathbb{F}_{q^2}$, A^T denotes the transposed matrix of A, and $\bar{A} = \left(a_{ij}^q\right)$ denotes the conjugate matrix of A. When we use the vertical bar | in a matrix, such as $[A|B]$, it means that $[A|B]$ is a block matrix, which is the juxtaposition of matrices A and B. For $u, v \in \mathbb{F}_{q^2}^n$, the Hermitian inner product $\langle , \rangle_H$ is defined by $\langle u, v\rangle_H = \sum_{i=1}^n \bar{u}_i v_i$. For an $\mathbb{F}_{q^2}$-linear code C in $\mathbb{F}_{q^2}^n$, define the Hermitian dual $C^{\perp_H} = \{x \in \mathbb{F}_{q^2}^n : \langle x, c\rangle_H = 0 \text{ for all } c \in C\}$.

A linear code C over F_q is called an Euclidean LCD code if $C \cap C^{\perp_{\mathrm{E}}} = \{\mathbf{0}\}$. A linear code C over $\mathbb{F}_{q^2}$ is called a Hermitian LCD code if $C \cap C^{\perp_H} = \{\mathbf{0}\}$.

The following proposition gives a complete characterization of Euclidean and Hermitian LCD codes.

Proposition 1 [2,4] *If G is a generator matrix for the $[n, k]$-linear code C, then C is an Euclidean (resp. a Hermitian) LCD code if and only if (iff) the $k \times k$ matrix GG^T (resp. $G\bar{G}^T$) is nonsingular.*

3 Characterizations of Symplectic LCD Codes

For $x, y \in \mathbb{F}_q^{2n}$, the symplectic inner product is defined as $\langle x, y\rangle_S = x\Omega y^T$, where $\Omega = \begin{bmatrix} \mathbf{0} & I_n \\ -I_n & \mathbf{0} \end{bmatrix}$, I_n is the identity matrix of order n. For an $\mathbb{F}_q$-linear code in $\mathbb{F}_q^{2n}$, define the symplectic dual code as $C^{\perp_S} = \{x \in \mathbb{F}_q^{2n} : \langle x, c\rangle_S = 0 \text{ for all } c \in C\}$. It is easy to show that $C^{\perp_S}$ is an $\mathbb{F}_q$-linear code in $\mathbb{F}_q^{2n}$, and $\dim(C^{\perp_S}) + \dim(C) = 2n$. For a vector $(u|v) \in \mathbb{F}_q^{2n}$, where $u = (u_1, u_2, \cdots, u_n)$, $v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_q^n$, the symplectic weight is defined by $\mathrm{wt}_S(u|v) = |\{i : (u_i, v_i) \neq (0, 0)\}|$. For two vectors $(u|v), (u'|v') \in \mathbb{F}_q^{2n}$, the symplectic distance is defined by $d_S((u|v), (u'|v')) = \mathrm{wt}_S(u - u'|v - v')$. The minimum symplectic distance of a linear code C is defined by $d_S(C) = \min\{\mathrm{wt}_S(u|v) : \text{ for all nonzero } (u|v) \in C\}$. Then it is straightforward to verify that a $[2n, k]$-linear code C also satisfies the symplectic Singleton bound: $k + 2d_S \leq 2n + 2$. A code achieving the above bound is called a simplectic MDS code.

Definition 1 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 a symplectic LCD MDS code.

The following characterization of symplectic LCD codes is similar to Proposition 1.

Theorem 1 *If G is a generator matrix for the $\mathbb{F}_q$-linear code C in $\mathbb{F}_q^{2n}$ with parameters $[2n, k]$, then C is a symplectic LCD code iff the $k \times k$ matrix $G\Omega G^T$ is nonsingular, where $\Omega = \begin{bmatrix} \mathbf{0} & I_n \\ -I_n & \mathbf{0} \end{bmatrix}$.*

Proof Suppose that $G\Omega G^T$ is singular, then there is a nonzero vector $a \in \mathbb{F}_q^k$, 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 $\exists v \in \mathbb{F}_q^k$, 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, $C \cap C^{\perp_S} = \{\mathbf{0}\}$. □

A generic construction of linear codes over $\mathbb{F}_p$ from subsets of $\mathbb{F}_p^m$ was considered in [8] and restated in [31].

Let $G = [g_1, g_2, \cdots, g_{2n}]$ be an $m \times (2n)$ matrix formed by the column vectors $g_1, g_2, \cdots, g_{2n} \in \mathbb{F}_p^m$, and

$$C = \{(\langle a, g_1\rangle_E, \langle a, g_2\rangle_E, \cdots, \langle a, g_{2n}\rangle_E) : a \in \mathbb{F}_p^m\}.$$

Clearly, C is a $[2n, k]$-linear code generated by the row vectors of the matrix G, where $k = \mathrm{rank}(G)$. In particular, if $k = m$, G is exactly a generator matrix of C.

The following result can be used to determine when C is symplectic LCD.

Theorem 2 *For the linear code* $C = \{(\langle a, g_1\rangle_E, \langle a, g_2\rangle_E, \cdots, \langle a, g_{2n}\rangle_E) : a \in \mathbb{F}_p^m\}$ *and* $G = [g_1, g_2, \cdots, g_{2n}]$*, we have:*

(1) $\dim(C) = \mathrm{rank}(G)$*;*

(2) $\dim(C \cap C^{\perp_S}) = \mathrm{rank}(G) - \mathrm{rank}(G\Omega G^T)$.

Proof (i) It is clear that $\dim(C) = \mathrm{rank}(G)$;

(ii) Let $c = \sum_{i=1}^m x_i c_i$ be any codeword in C, where $x_i \in F_p$ and c_i is the i-th row of the matrix G for $i \in \{1, 2, \cdots, m\}$. Then, $c \in C \cap C^{\perp_S}$ if and only if $\langle c, c_i\rangle_S = 0$ for any $i \in \{1, 2, \cdots, m\}$, that is $G\Omega G^T x = 0$, where $x = (x_1, x_2, \cdots, x_m)^T$. Let σ be the linear transformation from $K = \{x : G\Omega G^T x = 0\}$ to $L = C \cap C^{\perp_S}$ defined by $\sigma(x) = x^T G, \forall x \in K$. Then, $\dim(\ker(\sigma)) = m - \mathrm{rank}(G)$, $\dim(K) = m - \mathrm{rank}(G\Omega G^T)$, where $\ker(\sigma) = \{x : x^T G = 0\}$. Note that σ is surjective, applying the rank-nullity theorem, we have

$$\dim(K) = \dim(L) + \dim(\ker(\sigma)),$$

that is $\dim(L) = \mathrm{rank}(G) - \mathrm{rank}(G\Omega G^T)$. This completes the proof. □

From Theorem 2, we immediately get the condition for C to be symplectic LCD.

Corollary 1 *For the linear code* $C = \{(\langle a, g_1\rangle_E, \langle a, g_2\rangle_E, \cdots, \langle a, g_{2n}\rangle_E) : a \in \mathbb{F}_p^m\}$*, where* $g_1, g_2, \cdots, g_{2n} \in \mathbb{F}_p^m$ *and* $G = [g_1, g_2, \cdots, g_{2n}]$*, C is symplectic LCD iff* $\mathrm{rank}(G) = \mathrm{rank}(G\Omega G^T)$.

Remark 1 (1) In Corollary 1, if G is exactly a generator matrix of C, then $\mathrm{rank}(G) = m = \mathrm{rank}(G\Omega G^T)$, so $G\Omega G^T$ is nonsingular. We get a result similar to Theorem 1 again.

(2) In [6], the concept of σ-LCD codes was introduced first, which includes known Euclidean LCD codes, Hermitian LCD codes, and Galois LCD codes. In addition, we found that a symplectic LCD code is just a σ-LCD code with $\sigma(x|y) = (y|-x)$, where $x, y \in \mathbb{F}_q^n$ and σ is a special mapping from $\mathbb{F}_q^{2n}$ to itself. Hence, the result of the Theorem 1 can also be obtained from Proposition 2.1 in [6].

Example 1 Let C be a linear code generated by the row vectors of the following matrix G.

(1) Let $G = I$, where I denotes the $m \times m$ identity matrix over $\mathbb{F}_2$, and m is even. It is obvious that $\mathrm{rank}(I) = \mathrm{rank}(I\Omega I^T) = \mathrm{rank}(\Omega) = m$. Then C is symplectic LCD from Corollary 1.

(2) Let $G = \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 0 \end{bmatrix}$ be an $m \times m$ matrix over $\mathbb{F}_2$, and m is even. It is easy to check that $\mathrm{rank}(G) = m$ and $\mathrm{rank}(G\Omega G^T) = \mathrm{rank}(G)$. Then C is also symplectic LCD from Corollary 1.

Example 2 Let $G = [I_2|A]$ be a generator matrix for the $\mathbb{F}_2$-linear code C with parameters $[4, 2]$, where $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then we have $G\Omega G^T = A^T - A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is nonsingular, by Theorem 1, C is symplectic LCD.

4 Existence and Constructions of Symplectic LCD Codes

4.1 Symplectic LCD Codes from Smaller Dimensions and Lengths

Symplectic LCD codes can easily be derived from symplectic LCD codes of smaller dimensions and lengths.

Theorem 3 *Let C_i be a q-ary $[2n_i, 2k_i, d_i]$ symplectic LCD code with a generator matrix $G^{(i)} = [G_1^{(i)}|G_2^{(i)}]$, where $i = 1, 2$. Then, $G = \begin{bmatrix} G_1^{(1)} & 0 & G_2^{(1)} & 0 \\ 0 & G_1^{(2)} & 0 & G_2^{(2)} \end{bmatrix}$ generates a q-ary $[2n_1 + 2n_2, 2k_1 + 2k_2, \min\{d_1, d_2\}]$ symplectic LCD code C.*

Proof Since

$$G\Omega G^T = \begin{bmatrix} -G_2^{(1)}\left[G_1^{(1)}\right]^T + G_1^{(1)}\left[G_2^{(1)}\right]^T & \mathbf{0} \\ \mathbf{0} & -G_2^{(2)}\left[G_1^{(2)}\right]^T + G_1^{(2)}\left[G_2^{(2)}\right]^T \end{bmatrix},$$

we only need to prove that $-G_2^{(i)}[G_1^{(i)}]^T + G_1^{(i)}[G_2^{(i)}]^T$ is nonsingular for $i = 1, 2$, and the nonsingularity is guaranteed by the fact that C_i is symplectic LCD. According to Theorem 1, we get the result immediately. □

The theorem above can be generalized to the following result easily.

Theorem 4 *Let C_i be a q-ary $[2n_i, 2k_i, d_i]$ symplectic LCD code for $i = 1, 2, \cdots, n$ and $G^{(i)} = \left[G_1^{(i)}|G_2^{(i)}\right]$ be a generator matrix of C_i. Then,*

$$G = \begin{bmatrix} G_1^{(1)} & 0 & \cdots & 0 & G_1^{(2)} & 0 & \cdots & 0 \\ 0 & G_1^{(2)} & \cdots & 0 & 0 & G_2^{(2)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & G_n^{(n)} & 0 & 0 & \ldots & G_n^{(2)} \end{bmatrix}$$

generates a q-ary $\left[\sum_{i=1}^n n_i, \sum_{i=1}^n k_i, \min\{d_i\}\right]$ symplectic LCD code C.

Remark 2 Unfortunately, although the constructions in this section have certain generality, but the parameters of symplectic LCD codes constructed are usually not good.

4.2 Symplectic LCD MDS Codes from Euclidean LCD MDS Codes

Theorem 5 *Let C be a q-ary linear code with a generator matrix $G = \begin{bmatrix} G_1 & \mathbf{0} \\ \mathbf{0} & G_2 \end{bmatrix}$, where G_i is a generator matrix of a q-ary $[n, k, d_i]$ linear code C_i, $i = 1, 2$. If C_1, C_2 are Euclidean LCD and $G_1^T G_2$ is symmetric, then C is a $[2n, 2k, d_S]$ symplectic LCD code, where $d_S = \min\{d_1, d_2\}$; Further, if C_1, C_2 are both $[n, k, n-k+1]$ MDS codes, then C is a $[2n, 2k, n-k+1]$ symplectic MDS code.*

Proof Since $G\Omega G^T = \begin{bmatrix} \mathbf{0} & G_1 G_2^T \\ -G_2 G_1^T & \mathbf{0} \end{bmatrix}$, we only need to prove $G_1 G_2^T$ is nonsingular. If C_1, C_2 are Euclidean LCD and $G_1^T G_2$ is symmetric, then $G_1 G_1^T$, $G_2 G_2^T$ are nonsingular and $G_1^T G_2 = G_2^T G_1$. For $(G_1 G_2^T)^2 = G_1 G_2^T G_1 G_2^T = G_1 G_1^T G_2 G_2^T$, we have $G_1 G_2^T$ is nonsingular. If C_1, C_2 are both MDS, it is easy to get that the minimum symplectic distance of C is $d_S = n - k + 1$. Obviously, C achieves the symplectic Singleton bound, and becomes symplectic MDS. □

According to the theorem above, we can get the following corollary immediately.

Corollary 2 *Let $\tilde{C} = \{(u|v) : u, v \in C\}$, where C is a q-ary linear code C. If C is Euclidean LCD MDS, then $\tilde{C}$ is symplectic LCD MDS.*

If the following MDS conjecture holds, all Euclidean LCD MDS codes have be classified in [5].

MDS conjecture: Let C be an $[n, k]$ MDS code. Then $n \leq q + 1$, except when q is even and $k \in \{3, q - 1\}$, in which case $n \leq q + 2$.

Proposition 2 [5] *Let q be a prime power with $q > 3$ and k, n be integers with $0 \leq k \leq n$. Then there exists a q-ary Euclidean LCD MDS code with parameters $[n, k]$ if one of the following conditions holds.*

(1) $n \leq q + 1$;
(2) $q = 2^m$ *with positive integer* m , $n = q + 2$, *and* $k = 3$ *or* $q - 1$.

When $q = 2$, all 2-ary LCD MDS codes are $[n, k]$ codes with $0 \leq k \leq n \leq 3$ and $[n, k] \neq [2, 1]$. When $q = 3$, all 3-ary LCD MDS codes are $[n, k]$ codes with $0 \leq k \leq n \leq 4$ and $[n, k] \neq [4, 2]$.

According to Corollary 2 and Proposition 2, we can easily get that, there exists a q-ary $[2n, 2k]$ symplectic LCD MDS code if one of the conditions in Proposition 2 holds.

Example 3 (1) As usual take $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega} = \omega^2\}$ with $1 + \omega + \omega^2 = 0$. Let C be an $\mathbb{F}_4$-linear code with parameters $[6, 3, 4]$, whose generator matrix is given by $G = \begin{bmatrix} 1 & 1 & 1 & \omega & 0 & 0 \\ 1 & \omega & \bar{\omega} & 0 & 1 & 0 \\ 1 & \bar{\omega} & \omega & 0 & 0 & \omega \end{bmatrix}$. It's easy to verify that C is Euclidean LCD MDS.

Applying Corollary 2, $\tilde{C} = \{(u|v) : u, v \in C\}$ is a $[12, 6, 4]$ symplectic LCD MDS with a generator matrix $\tilde{G} = \begin{bmatrix} G & \mathbf{0} \\ \mathbf{0} & G \end{bmatrix}$.

(2) Let C be an $\mathbb{F}_5$-linear code with parameters $[5, 2, 4]$, whose generator matrix is given by $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & -1 & 2 \end{bmatrix}$, then C is Euclidean LCD MDS. Applying Corollary 2, $\tilde{C} = \{(u|v) : u, v \in C\}$ is a $[10, 4, 4]$ symplectic LCD MDS code with a generator matrix $\tilde{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & -1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & 2 \end{bmatrix}$.

4.3 Symplectic LCD MDS Codes from Hermitian LCD MDS Codes

The following lemmas are important in the subsequent construction.

Lemma 1 [20] *There must be an element $\gamma \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, such that $\gamma^q = -\gamma + \alpha$, where $\alpha \in \mathbb{F}_q \backslash \{0\}$.*

Lemma 2 [20] *Let C be a q^2-ary linear code in $\mathbb{F}_{q^2}^n$, then, any codeword of C can be written as $u + \gamma v$ with $u, v \in \mathbb{F}_q^n$.*

The map Φ is defined by $\Phi(a + \gamma b) = (a|b)$ for $a, b \in \mathbb{F}_q$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q^2$. Clearly, Φ is a bijection, which extends naturally to a map from $\mathbb{F}_{q^2}^n$ to $\mathbb{F}_q^{2n}$.

The following theorem is easy to be obtained and we omit the proof.

Theorem 6 *Let C be a q^2-ary linear code with parameters $[n, k, d]$ and $\Phi(C) = \{(u|v) : u + \gamma v \in C\}$, where $\gamma \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, then $\Phi(C)$ is a q-ary $[2n, 2k, d_S]$-linear code, where $d_S = d$. Further, if C is MDS, then $\Phi(C)$ is symplectic MDS.*

Theorem 7 *Let C be a q^2-ary $[n, k]$-linear code, and $\Phi(C) = \{(u|v) : u + \gamma v \in C\}$. If C is Hermitian LCD, then $\Phi(C)$ is symplectic LCD.*

Proof For any $c \in C, c' \in C^{\perp_H}$, where $c = u + \gamma v, c' = u' + \gamma v'$, we have $\langle c, c' \rangle_H = \sum_{i=1}^n (u_i + \gamma v_i)^q (u_i' + \gamma v_i') = \sum_{i=1}^n (u_i u_i' + \gamma^{q+1} v_i v_i' + \gamma^q v_i u_i' + \gamma u_i v_i') = \sum_{i=1}^n (u_i u_i' + \gamma^{q+1} v_i v_i' + \alpha v_i u_i') + \gamma \sum_{i=1}^n (u_i v_i' - v_i u_i') = 0$, which implies that $\sum_{i=1}^n (u_i u_i' + \gamma^{q+1} v_i v_i' + \alpha v_i u_i') = 0$ and $\sum_{i=1}^n (u_i v_i' - v_i u_i') = 0$, then $\langle \Phi(c), \Phi(c') \rangle_S = \langle (u|v), (u'|v') \rangle_S = \sum_{i=1}^n (u_i v_i' - v_i u_i') = 0$. So we have $\phi(C^{\perp_H}) \subseteq \phi(C)^{\perp_S}$. Since the map ϕ is bijection, $\phi(C^{\perp_H}) = \phi(C)^{\perp_S}$.

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

Example 4 Let C be the $\mathbb{F}_4$-linear code with parameters $[4, 2, 2]$, whose generator matrix is given by $G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \omega & \omega \end{bmatrix}$. We can easily verify that $G\bar{G}^T$ is nonsingular, then C is Hermitian LCD from Proposition 1. According to Theorem 7, $\Phi(C) = \{(u|v) : u + \omega v \in C\}$ is $[8, 4, 2]$ binary symplectic LCD with a generator matrix $\Phi(G) = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$.

Corollary 3 *Let C be a q^2-linear code in $\mathbb{F}_q^n$, and $\Phi(C) = \{(u|v) : u + \gamma v \in C\}$, where $\gamma \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If C is a q^2-ary $[n, k, n-k+1]$ Hermitian LCD MDS code, then $\Phi(C)$ is a q-ary $[2n, 2k, n-k+1]$ symplectic LCD MDS.*

Proposition 3 [5] *Let q be a prime power and k, n be integers with $0 \leq k \leq n$. Then there exists a q^2-ary Hermitian LCD MDS code with parameters $[n, k]$ if one of the following conditions holds.*

(1) $n \leq q+1, k \leq q-2$ *or* $n-k \leq q-2$*;*
(2) q *odd,* $[n, k] \in \{[2k, k], [2k+1, k], [2k+2, k]\}$ *where k is a positive integer with* $k|(q^2-1), k \nmid (q+1)$*, and* $k < q^2-1$*;*
(3) $q = 2^m \geq 8, n = q+2, k = 3$ *or* $k = q-1$.

According to Corollary 3 and Proposition 3, we can easily get that, there exists a q-ary $[2n, 2k]$ symplectic LCD MDS code if one of the conditions in Proposition 3 holds.

5 Special Symplectic LCD MDS Codes from Vandermonde Matrices

Next, some symplectic LCD MDS codes are constructed from Vandermonde matrices, and the elements of Vandermonde matrices are always restricted in finite field $\mathbb{F}_{2^s}$. We give the following definitions first. For more results, please refer to the literature [24].

An $n \times n$ matrix M is an MDS matrix iff every submatrix of M is nonsingular.

An $m \times m$ matrix $A = van(a_0, a_1, \cdots, a_{m-1}) =$

$$\begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{m-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{m-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & a_{m-1} & a_{m-1}^2 & \cdots & a_{m-1}^{m-1} \end{pmatrix}$$

is called a Vandermonde matrix, where the elements are all different, that is $i \neq j$ implies $a_i \neq a_j$).

A $2^n \times 2^n$ matrix H is a Finite Field Hadamard (FFHadamard) matrix in $\mathbb{F}_{2^s}$ if it can be represented as $H = \begin{pmatrix} U & V \\ V & U \end{pmatrix}$, where U and V are also FFHadamard (see [1]).

Let $H = had(a_0, a_1, a_2, a_3) = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix}$, which implies $h_{i,j} = a_{i \oplus j} (\oplus \text{in } a_{i \oplus j}$: bit-wise XOR). Obviously, the matrix is symmetrical and any two rows of H are orthogonal in $\mathbb{F}_{2^s}$.

5.1 $[2^m, 2k]$ Symplectic LCD MDS Codes

Let's consider the required conditions for the construction of $[2^m, 2k]$ symplectic LCD MDS codes, where $2 \leq m \leq s$ and $1 \leq k \leq 2^{m-1}$. We look at the case of $m = 2$ first.

For matrix $A = van(a_0, a_1, a_2, a_3)$ and $B = van(b_0, b_1, b_2, b_3) = van(a_0 + \Delta, a_1 + \Delta, a_2 + \Delta, a_3 + \Delta)$, where Δ is an arbitrary non-zero number in $\mathbb{F}_{2^s}$.

Let $\tilde{A} =$

$$\begin{pmatrix} a_0^3 + s_0a_0 + s_1 & a_1^3 + s_0a_1 + s_1 & a_2^3 + s_0a_2 + s_1 & a_3^3 + s_0a_3 + s_1 \\ a_0^2 + s_0 & a_1^2 + s_0 & a_2^2 + s_0 & a_3^2 + s_0 \\ a_0 & a_1 & a_2 & a_3 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

where $s_0 = \sum_{i=0}^3 a_i^5 / \sum_{i=0}^3 a_i^3$ and $s_1 = \sum_{i=0}^3 a_i^3$.

The following lemma is a slight modification of Corollary 2 in [24].

Lemma 3 *Let $G = B\tilde{A}$, the elements a_i and b_j must all be different and chosen such that: $a_0 + a_1 + a_2 + a_3 = 0$ and $a_i + b_j = a_l + b_{l \bigoplus i \bigoplus j}$, $i, j, l \in \{0, 1, 2, 3\}$. Then G is a FFHadamard MDS matrix and $G^2 = s_1^2 I_4$.*

With the notations and properties above, we will get the following construction.

Construction 1 *Let $G_\Gamma = (g_i)_{i \in \Gamma}$, which is composed of some row vectors of $G = B\tilde{A}$, where g_i is the i-th row of G and $i \in \Gamma = \{t, 2+t : t \in T \subset \{1, 2\}\}$. Let C_Γ be an $\mathbb{F}_{2^s}$-linear code with the generator matrix G_Γ and $|\Gamma| = 2k$. If $s_1^2 \neq 1$, then C_Γ is a symplectic LCD MDS code with parameters* $[4, 2k]$, *where* $k = 1, 2$.

Proof Let $G = \begin{pmatrix} U & V \\ V & U \end{pmatrix}$, where U and V are also FFHadamard. Let $g_i = (u_i|v_i)$ and $g_{2+i} = (v_i|u_i)$ for $1 \le i \le 2$, where u_i and v_i are row vectors of U and V respectively. The (i, j) element of $G\Omega G^T$ is $g_i \Omega g_j^T$, which is denoted as $s_{i,j}$,

If $1 \le i, j \le 2$, then $s_{i,j} = g_i \Omega g_j^T = (u_i|v_i)\Omega(u_j|v_j)^T = u_i v_j^T - v_i u_j^T = 0$. Similarly, $s_{2+i,2+j} = v_i u_j^T - u_i v_j^T = 0$.

If $1 \le i \le 2$ and $j = 2 + i$, then $s_{i,j} = g_i \Omega g_{2+i}^T = (u_i|v_i)\Omega(v_i|u_i)^T = u_i u_i^T - v_i v_i^T$. From Lemma 3, $s_{i,j} = s_1^2 - 1 \neq 0$. Similarly, $s_{j,i} = 1 - s_1^2 \neq 0$.

In summary,

$$G_\Gamma \Omega G_\Gamma^T = (s_1^2 - 1) \begin{pmatrix} \mathbf{0} & I_k \\ -I_k & \mathbf{0} \end{pmatrix}$$

is nonsingular, where $|\Gamma| = 2k$. Applying Theorem 1, C_Γ is a symplectic LCD code with parameters $[4, 2k]$.

For G_Γ is the parity check matrix of $C_\Gamma^{\perp_E}$ and G is an MDS matrix, we have every $2k$ columns of G_Γ are linearly independent. Obviously, some $2k + 1$ columns of G_Γ are linearly dependent. Therefore, $C_\Gamma^{\perp_E}$ has minimum distance $2k + 1$, which means that $C_\Gamma^{\perp_E}$ is MDS, then C_Γ is also an MDS code with parameters $[4, 2k, d_H]$, where $k = 1, 2$, $d_H = 5 - 2k$. Obviously, we have $d_S \ge \lceil d_H/2 \rceil = 3 - k$. On the other hand, C_Γ also satisfies the symplectic Singleton bound, then $d_S \le 3 - k$. Therefore, $d_S = 3 - k$, that is, C_Γ is symplectic MDS. □

Now, let's extend the case to $[2^m, 2k]$, where $m \ge 3$.

Definition 2 [24] The matrix $A = van(a_0, a_1, \cdots, a_{2^m-1})$ is called a Special Vandermonde (SV) matrix if

$$a_i + a_{i \oplus 2^k} = R_k, \text{ for all } k \in \{0, 1, \cdots, m-1\},$$

where R_k's are different non-zero constants such that for $\mu_i \in \{0, 1\}$,

$$\sum_{i=0}^{m-1} \mu_i R_i = 0 \Rightarrow \mu_i = 0, \text{ for all } i \in \{0, 1, \cdots, m-1\}.$$

It's easy to observe that all a_i's are constructed from $a_0, R_0, R_1, \cdots, R_{m-1}$.

For an SV matrix $A = van(a_0, a_1, \cdots, a_{2^m-1})$ and $B = van(b_0, b_1, \cdots, b_{2^m-1}) = van(a_0 + \Delta, a_1 + \Delta, \cdots, a_{2^m-1} + \Delta)$, where $a_i + b_j = a_l + b_{l \oplus i \oplus j}$ and a_i, b_j are all different. Let $G = B\tilde{A}$, where the j-th column of $\tilde{A}$ is $\tilde{A}_{col(j)} =$

$$\begin{pmatrix} a_j^{2^{m-1}+2^{m-2}+\ldots+1} + s_0 a_j^{2^{m-2}+2^{m-3}+\ldots+1} + \cdots + s_{m-2}a_j + s_{m-1} \\ \vdots \\ a_j^{2^{m-1}+2^{m-2}} + s_0 a_j^{2^{m-2}} + s_1 \\ \vdots \\ a_j^{2^{m-1}} + s_0 a_j \\ a_j^{2^{m-1}} + s_0 \\ \vdots \\ a_j \\ 1 \end{pmatrix},$$

and $s_0 = \sum a_i^{2^{m+1}-2^{m-1}-1} / \sum a_i^{2^m-1}$, $s_1 = \sum a_i^{2^{m+1}-2^{m-2}-1} / \sum a_i^{2^m-1}, \cdots$, $s_{m-1} = \sum a_i^{2^{m+1}-1-1} / \sum a_i^{2^m-1}$. Then G is a FFHadamard MDS matrix and $G^2 = (\sum a_i^{2^m-1})^2 I_{2^m}$ (see [24]).

For the FFHadamard MDS matrix defined above, we get the following construction. The proofs are similar to construction 1 and we omit it here.

Construction 2 *Let $G_\Gamma = (g_i)_{i \in \Gamma}$, which is composed of some row vectors of $G = B\tilde{A}$, where g_i is the i-th row of G and $\Gamma = \{t, 2^{m-1} + t : t \in T \subset \{1, 2, \cdots, 2^{m-1}\}\}$. Let C_Γ be an $\mathbb{F}_{2^s}$-linear code with the generator matrix G_Γ and $|\Gamma| = 2k$. If $(\sum a_i^{2^m-1})^2 \neq 1$, then C_Γ is a symplectic LCD MDS code with parameters $[2^m, 2k]$, where $k = 1, 2, \cdots, 2^{m-1}$.*

According to the construction of C_Γ and the proof, it is not difficult to obtain the following result, which will be useful in Sect. 6.

Proposition 4 *If C_Γ is a $[2^m, 2k, 2^{m-1} - k + 1]$ symplectic LCD MDS code, then $C_\Gamma^{\perp_S}$ is also a $[2^m, 2^m - 2k, k + 1]$ symplectic LCD MDS code, where $k = 1, 2, \cdots, 2^{m-1}$.*

5.2 Numerical Example

Example 5 For SV matrices $A = van(a_0, a_1, a_2, a_3) = van(41_x, 40_x, f7_x, f6_x)$, the parameter $\Delta = 32_x$, and the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. Based on the method introduced in Sect. 5.1, we can get $B = van(b_0, b_1, b_2, b_3) = van(a_0 + \Delta, a_1 + \Delta, a_2 + \Delta, a_3 + \Delta)$ and

$$\tilde{A} = \begin{pmatrix} e4_x & b1_x & 7c_x & f1_x \\ 15_x & 14_x & 7b_x & 7a_x \\ 41_x & 40_x & f7_x & f6_x \\ 01_x & 01_x & 01_x & 01_x \end{pmatrix}.$$

Let $G = B\tilde{A}$, then we have

$$G = \begin{pmatrix} 21_x & a6_x & 82_x & dd_x \\ a6_x & 21_x & dd_x & 82_x \\ 82_x & dd_x & 21_x & a6_x \\ dd_x & 82_x & a6_x & 21_x \end{pmatrix},$$

where $s_1^2 = (\sum_{i=0}^{3} b_i^3)^2 = 83_x \neq 01_x$. According to Construction 1, G and

$$G_1 = \begin{pmatrix} 21_x & a6_x & 82_x & dd_x \\ 82_x & dd_x & 21_x & a6_x \end{pmatrix} \text{ or } \begin{pmatrix} a6_x & 21_x & dd_x & 82_x \\ dd_x & 82_x & a6_x & 21_x \end{pmatrix}$$

generate symplectic LCD MDS codes with parameters [4, 4, 1] and [4, 2, 2] respectively.

Example 6 Let $a_0 = 04_x, R_0 = 01_x, R_1 = 02_x, R_2 = 09_x$, then $A = van(04_x, 05_x, 06_x, 07_x, 0d_x, 0c_x, 0f_x, 0e_x)$ is an SV matrix, the parameter $\Delta = 73_x$ and the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. we can get $B = van(77_x, 76_x, 75_x, 74_x, 7e_x, 7f_x, 7c_x, 7d_x)$ and

$$\tilde{A} = \begin{pmatrix} e5_x & 76_x & 4d_x & 3d_x & c2_x & a8_x & d9_x & 90_x \\ 4e_x & 77_x & b3_x & 9e_x & 49_x & fd_x & c7_x & 67_x \\ a0_x & 8d_x & 90_x & af_x & 20_x & c8_x & 05_x & ff_x \\ 28_x & 29_x & 38_x & 39_x & e4_x & e5_x & f4_x & f5_x \\ 40_x & 55_x & 78_x & 6b_x & ba_x & e7_x & 24_x & 7f_x \\ 10_x & 11_x & 14_x & 15_x & 51_x & 50_x & 55_x & 54_x \\ 04_x & 05_x & 06_x & 07_x & 0d_x & 0c_x & 0f_x & 0e_x \\ 01_x & 01_x & 01_x & 01_x & 01_x & 01_x & 01_x & 01_x \end{pmatrix}.$$

Let $G = B\tilde{A}$, then we have

$$G = \begin{pmatrix} ec_x & 66_x & dc_x & f0_x & 14_x & bd_x & e0_x & 2f_x \\ 66_x & ec_x & f0_x & dc_x & bd_x & 14_x & 2f_x & e0_x \\ dc_x & f0_x & ec_x & 66_x & e0_x & 2f_x & 14_x & bd_x \\ f0_x & dc_x & 66_x & ec_x & 2f_x & e0_x & bd_x & 14_x \\ 14_x & bd_x & e0_x & 2f_x & ec_x & 66_x & dc_x & f0_x \\ bd_x & 14_x & 2f_x & e0_x & 66_x & ec_x & f0_x & dc_x \\ e0_x & 2f_x & 14_x & bd_x & dc_x & f0_x & ec_x & 66_x \\ 2f_x & e0_x & bd_x & 14_x & f0_x & dc_x & 66_x & ec_x \end{pmatrix},$$

where $(\sum_{i=0}^{7} b_i^7)^2 = de_x \neq 01_x$. According to Construction 2, G_Γ generates symplectic LCD MDS codes with parameters $[8, 2k, 5-k]$, where $k = 1, 2, 3, 4$.

6 MDS 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. By the Singleton bound for EAQECCs [3], we have $2(d-1) \leq n-k+c$, and an EAQECC meeting this bound is called an MDS EAQECC. An EAQECC with $c = n-k$ is called a maximal entanglement EAQECC [17]. It was shown that maximal entanglement EAQECCs can achieve the entanglement-assisted quantum capacity of a depolarizing channel.

The following is the explicit symplectic method of constructing EAQECCs from classical linear codes [11].

Theorem 8 *Let $C \subseteq \mathbb{F}_q^{2n}$ be an $(n-k)$-dimensional $\mathbb{F}_q$-linear space and $H = [H_X|H_Z]$ be a matrix whose row space is C. Let $C' \subseteq \mathbb{F}_q^{2(n+c)}$ be an $\mathbb{F}_q$-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 $\mathbb{C}^q \otimes \mathbb{C}^q$. Then,*

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

The encoding quantum circuit is constructed from C', and it encodes $k+c$ logical qudits in $\mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$ 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 $\mathbb{F}_q$.

Combining Proposition 4 and Theorem 8, we can obtain the following MDS maximal entanglement EAQECCs with length $2 \leq m \leq s$.

Theorem 9 *There exists an MDS maximal entanglement EAQECC over $\mathbb{F}_{2^s}$ with parameters $[[2^{m-1}, 2^{m-1}-k, k+1; k]]$ or $[[2^{m-1}, k, 2^{m-1}-k+1; 2^{m-1}-k]]$.*

From the theorem above, we can see that a class of MDS maximal entanglement EAQECCs can be obtained if we found a class of symplectic LCD MDS codes, and this is different from the previous case of Hermitian or Euclidean inner products (such as [12,19,22,23]). We believe that more MDS maximal entanglement EAQECCs can be obtained from this symplectic method.

7 Concluding Remarks

In this paper, we give characterizations of symplectic LCD codes. Further, we present some methods for constructing symplectic LCD MDS codes from Euclidean LCD codes and Hermitian LCD codes. Especially, some symplectic LCD MDS codes are constructed from Special Vandermonde matrices over finite field $\mathbb{F}_{2^s}$, and all the $[2^m, 2k]$ and $[2^m, 2^m - 2k]$ symplectic LCD MDS codes have been constructed, where $2 \leq m \leq s, k = 1, 2, \cdots, 2^{m-1}$. As an application, a class of MDS maximal entanglement EAQECCs with parameters $[[2^{m-1}, 2^{m-1} - k, k + 1; k]]$ or $[[2^{m-1}, k, 2^{m-1} - k + 1; 2^{m-1} - k]]$ is constructed.

Acknowledgements This work was supported by the National Natural Science Foundation of China under Grant(61572168) and the Excellent Young Talents Fund Program of Higher Education Institutions of Anhui Province (CN)(gxyqZD2016228).

References

1. Barreto P., Rijmen V.: The Anubis Block Cipher. Submission to the NESSIE Project (2000). Available at http://cryptonessie.org
2. Boonniyoma, K., Jitman, S.: Complementary dual subfield linear codes over finite fields. Available at arXiv:1605.06827, (2016)
3. Brun, T.A., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**, 436–439 (2006)
4. Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**(1), 131–150 (2017)
5. Carlet, C., Mesnager, S., Tang, C., Qi, Y.: Euclidean and Hermitian LCD MDS codes. Des. Codes Cryptogr. **86**(11), 2605–2618 (2017)
6. Carlet, C., Mesnager, S., Tang, C., Qi, Y.: On σ-LCD codes. IEEE Trans. Inf. Theory **65**(3), 1694–1704 (2018)
7. Dougherty, S.T., Kim, J.L., Ozkaya, B., Sok, L., Sole, P.: The combinatorics of LCD codes: linear programming bound and orthogonal matrices. Int. J. Inform. Cod. Theory **4**, 116 (2015)
8. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015)
9. Esmaeili, M., Yari, S.: On complementary-dual quasi-cyclic codes. Finite Fields Appl. **15**, 375–386 (2009)
10. Guo, L., Fu, Q., Li, R., Lu, L.: Maximal entanglement entanglement-assisted quantum codes of distance three. Int. J. Quantum Inf. **13**, 1550002 (2015)
11. Galindo, C., Hernando, F., Matsumoto, R., Ruano, D.: Entanglement-assisted quantum error-correcting codes over arbitrary finite fields. Quant. Inf. Process. **18**(4), 116 (2019)
12. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
13. Guneri, C., Ozkaya, B., Sole, P.: Quasi-cyclic complementary dual codes. Finite Fields Appl. **42**, 67–80 (2016)
14. Jin, L.: Construction of MDS codes with complementary duals. IEEE Trans. Inf. Theory **63**(5), 2843–2847 (2017)
15. Kai, X.S., Zhu, S.X.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inf. Theory **59**(2), 1193–1197 (2013)

16. Kai, X.S., Zhu, S.X., Li, P.: Constacyclic codes and some new quantum MDS codes. IEEE Trans. Inf. Theory **60**(4), 2080–2086 (2014)
17. Lai, C.-Y., Brun, T.A., Wilde, M.M.: Duality in entanglement-assisted quantum error correction. IEEE Trans. Inf. Theory **59**(6), 4020–4024 (2013)
18. Li, C., Ding, C., Li, S.: LCD cyclic codes over finite fields. IEEE Trans. Inf. Theory **63**(7), 4344–4356 (2017)
19. Lu, L., Li, R., Guo, L., Fu, Q.: Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. Quant. Inf. Process. **14**, 165–182 (2015)
20. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Pub. Co., Amsterdam (1977)
21. Massey, J.L.: Linear codes with complementary duals. Discrete Math. **106**(107), 337–342 (1992)
22. Qian, J., Zhang, L.: Entanglement-assisted quantum codes from arbitrary binary linear codes. Des. Codes Cryptogr. **77**, 193–202 (2015)
23. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **87**, 1565–1572 (2018)
24. Sajadieh, M., Dakhilalian, M., Mala, H., et al.: On construction of involutory MDS matrices from Vandermonde Matrices in $GF(2^q)$. Des. Codes Cryptogr. **64**(3), 287–308 (2012)
25. Sendrier, N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discret Math. **285**, 345–347 (2004)
26. Shi, M., Zhang, Y.: Quasi-twisted codes with constacyclic constituent codes. Finite Fields Appl. **39**, 159–178 (2016)
27. Shi, M., Yang, S., Zhu, S.: Good p-ary quasicyclic codes from cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. J. Syst. Sci. Compl. **25**(2), 375–384 (2012)
28. Shi, M., Qian, L., Sok, L., Sol, P.: On constacyclic codes over $Z_4[u]/{<}u^2 - 1{>}$ and their Gray images. Finite Fields Appl. **45**, 86–95 (2017)
29. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)
30. Yang, X., Massey, J.L.: The necessary and sufficient condition for a cyclic code to have a complementary dual. Discret Math. **126**, 391–393 (1994)
31. Zhou, Z., Tang, C., Li, X., Ding, C.: Binary LCD codes and self-orthogonal codes from a generic construction. IEEE Trans. Inf. Theory **65**(1), 16–27 (2019)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.