Hulls of Linear Codes Revisited with Applications*

Somphong Jitman and Satanan Thipworawimon†

September 11, 2019

Abstract

Hulls of linear codes have been of interest and extensively studied due to their rich algebraic structures and wide applications. In this paper, alternative characterizations of hulls of linear codes are given as well as their applications. Properties of hulls of linear codes are given in terms of their Gramians of their generator and parity-check matrices. Moreover, it is show that the Gramian of a generator matrix of every linear code over a finite field of odd characteristic is diagonalizable. Subsequently, it is shown that a linear code over a finite field of odd characteristic is complementary dual if and only if it has an orthogonal basis. Based on this characterization, constructions of good entanglement-assisted quantum error-correcting codes are provided.

Keywords: Hulls of linear codes, Gramians, Diagonalizability, Entanglement-assisted quantum error correcting codes
MSC 2010: 94B05, 94B60

1 Introduction

Hulls have been introduced to classify finite projective planes in [1]. Later, it turned out that the hulls of linear codes play a vital role in determining the complexity of some algorithms in coding theory in [18,19,27,28]. Due to their wide applications, hulls

†S. Jitman and S. Thipworawimon are with the Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand. Email: sjitman@gmail.com, thipworawimon_s@su.ac.th.

1

of linear codes have been extensively studied. The number of linear codes of length n over $\mathbb{F}_q$ whose hulls have a common dimension and the average hull dimension of linear codes were studied in [11] and [25]. Recently, hulls of linear codes have been studied and applied in constructions of good entanglement-assisted quantum error correcting codes in [11] and [20].

Some families of linear codes with special hulls such as self-orthogonal codes and linear complementary dual (LCD) codes have been of interest and extensively studied. Precisely, self-orthogonal codes are linear codes with maximal hull and LCD codes are linear codes of minimal hull. These codes are practically useful in communications systems, various applications, and link with other objects as shown in [5–11, 13–16, 21–24, 26] and references therein. Therefore, it is of interest to studied hulls, families of linear codes with special hulls and their applications.

In this paper, we focus on alternative characterizations of hulls of linear codes and their applications. Properties of hulls of linear codes are given in terms of the Gramians of their generator and parity-check matrices. Subsequently, it is shown that the Gramian of generator matrix of every linear code over a finite field of odd characteristic is diagonalizable. This implies that a linear code over a finite field of odd characteristic is LCD if and only if it has an orthogonal basis. Some classes of codes with special hulls such as self-orthogonal, maximal self-orthogonal, complementary dual codes are re-formalized based on these characterizations. Constructions of some good entanglement-assisted quantum error-correcting codes are given based on the above discussion.

The paper is organized as follows. After this introduction, the definition and preliminary results on Euclidean hulls of linear codes are recalled in Section 2. In Section 3, characterizations and properties of Euclidean hulls of linear codes are discussed as well as some remarks on linear codes with special Euclidean hulls. A note on relevant results on Hermitian hulls of linear codes is given in Section 4. Applications of hulls to constructions of entanglement-assisted quantum error-correcting codes are discussed in Section 5.

2 Preliminaries

Let $\mathbb{F}_q$ denote the finite field of order q. For a positive integer n, a *linear code* of length n over $\mathbb{F}_q$ is defined to be a subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$. A linear code C of length n over $\mathbb{F}_q$ is called an $[n, k]_q$ *code* if its $\mathbb{F}_q$-dimension is k. In addition, if the

minimum Hamming distance of C is d, the code C is called an $[n, k, d]_q$ code. For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_q^n$, the Euclidean inner product of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle := \sum_{i=1}^{n} u_i v_i.$$

For a linear code C of length n over $\mathbb{F}_q$, the Euclidean dual $C^\perp$ of C is defined to be the set

$$C^\perp = \{\boldsymbol{v} \in \mathbb{F}_q^n \mid \langle \boldsymbol{c}, \boldsymbol{v} \rangle = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

A linear code C is said to be *Euclidean self-orthogonal* if $C \subseteq C^{\perp_E}$ and it is said to be *Euclidean self-dual* if $C = C^{\perp_E}$. A linear code C is called a *maximal Euclidean self-orthogonal code* if it is Euclidean self-orthogonal and it is not contained in any Euclidean self-orthogonal codes. A linear code C is said to be *Euclidean complementary dual* if $C \cap C^\perp = \{\boldsymbol{0}\}$. The *Euclidean hull* of a linear code C is defined to be $\mathrm{Hull}(C) = C \cap C^{\perp_E}$. It is not difficult to see that a linear code C is Euclidean self-orthogonal if and only if $\mathrm{Hull}(C) = C$ and it is Euclidean complementary dual if and only if $\mathrm{Hull}(C) = \{\boldsymbol{0}\}$.

A $k \times n$ matrix G over $\mathbb{F}_q$ is called a *generator matrix* for an $[n, k]_q$ code C if the rows of G form a basis for C. A *parity-check matrix* for C is defined to a generator matrix of $C^\perp$. For an $m \times n$ matrix A over $\mathbb{F}_q$, by abuse of notation, the *Gram matrix* (or *Gramian*) of A is defined to be AA^T. The Gramian of a generator or parity-check matrix of a linear code plays an important role in the study of self-orthogonal codes, complementary dual codes, and hulls of linear codes.

Proposition 2.1 ([11, Proposition 3.1]). *Let C be a linear $[n, k, d]_q$ code with parity check matrix H and generator matrix G. The ranks of the Gramians HH^T and GG^T are independent of H and G so that*

$$\mathrm{rank}(HH^T) = n - k - \dim(\mathrm{Hull}(C)) = n - k - \dim(\mathrm{Hull}(C^\perp)),$$

and

$$\mathrm{rank}(GG^T) = k - \dim(\mathrm{Hull}(C)) = k - \dim(\mathrm{Hull}(C^\perp)).$$

From this proposition, it is well known that a linear code with generator matrix G is Euclidean self-orthogonal if and only if the Gramian GG^T is zero and it is Euclidean complementary dual if and only if the Gramian GG^T is non-singular. It can be summarized in the next corollary.

Corollary 2.2. *Let C be a linear code with generator matrix G. Then the following statements hold.*

3

1. C is Euclidean self-orthogonal if and only if $GG^T = [0]$.

2. C is Euclidean complementary dual if and only if GG^T is non-singular

From Proposition 2.1, it is not difficult to see that generator and parity-check matrices of linear codes can be chosen such that their Gramians are of the following special forms (cf. [17, Corollary 3.2]).

Proposition 2.3. *Let C be a linear $[n,k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. Then the following statements hold.*

1. *There exist a parity-check matrix H of C and an invertible $(n-k-\ell) \times (n-k-\ell)$ symmetric matrix A over $\mathbb{F}_q$ such that the Gramian of H is of the form*

$$HH^T = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right].$$

2. *There exist a generator matrix G of C and an invertible $(k-\ell) \times (k-\ell)$ symmetric matrix B over $\mathbb{F}_q$ such that such that the Gramian of G is of the form*

$$GG^T = \left[\begin{array}{c|c} B & 0 \\ \hline 0 & 0 \end{array}\right].$$

Clearly, the Gramians of generator and parity-check matrices of linear codes are always symmetric. Unlike real symmetric matrices, a square symmetric matrix over finite fields does not need to be diagonalizable. From Proposition 2.3, it is therefore interesting to ask whether the Gramian of a generator/parity-check matrix of a linear code is diagonalizable. Equivalently, does a linear code have a generator matrix whose Gramian is a diagonal matrix? In Proposition 3.4, we provide a solution to this problem for the case where q is an odd prime power. A partial solution for the case where q is an even prime power is given in Proposition 3.7.

3   Euclidean Hulls of Linear Codes

In this section, properties of hulls of linear codes are discussed. Alternative characterizations of the hull and the hull dimension of linear codes are given. Conditions for generator and parity-check matrices of linear codes to have diagonalizable Gramians are provided.

3.1 Characterizations of Euclidean Hulls of Linear Codes

The Euclidean hull dimension of linear codes has been determined in terms of the rank of the Gramians of generator and parity-check matrices of linear codes in [11] (see Proposition 2.1).

In the following proposition, alternative characterizations of the Euclidean hull dimension of linear codes are given.

Proposition 3.1. *Let C be a linear $[n, k]_q$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\mathrm{Hull}(C)) = \ell$.

2) $\mathrm{rank}(GG^T) = k - \ell$ *for every generator matrix G of C.*

3) $\mathrm{rank}(G_1 G_2^T) = k - \ell$ *for all generator matrices G_1 and G_2 of C.*

4) $\mathrm{rank}(HH^T) = n - k - \ell$ *for every parity-check matrix H of C.*

5) $\mathrm{rank}(H_1 H_2^T) = n - k - \ell$ *for all parity-check matrices H_1 and H_2 of C.*

Proof. From Proposition 2.1, we have the equivalences 1) $\Leftrightarrow$ 2) and 1) $\Leftrightarrow$ 4). It remains to prove the equivalences 2) $\Leftrightarrow$ 3) and 4) $\Leftrightarrow$ 5). Since the arguments of the proofs are similar, only the detailed proof of 2) $\Leftrightarrow$ 3) is provided.

To prove 2) $\Rightarrow$ 3), let G, G_1 and G_2 be generator matrices of C and assume that $\mathrm{rank}(GG^T) = k - \ell$. Since the rows of G, G_1 and G_2 are base for C, there exist invertible $k \times k$ matrices E_1 and E_2 such that $G_1 = E_1 G$ and $G_2 = E_2 G$. Consequently, we have $G_1 G_2^T = E_1 G (E_2 G)^T = E_1 G (G^T E_2^T) = E_1 (GG^T) E_2^T$. Since E_1 and E_2^T are invertible, we have

$$\mathrm{rank}(G_1 G_2^T) = \mathrm{rank}(E_1 (GG^T) E_2^T) = \mathrm{rank}(GG^T) = k - \ell$$

as desired

The statement 3) $\Rightarrow$ 2) is obvious. $\square$

Based on Proposition 3.1, we have the following characterizations.

Corollary 3.2. *Let C be a linear $[n, k]_q$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\mathrm{Hull}(C)) = \ell$.

2) *There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and generator matrices G_1 and G_2 of C such that*

$$G_1 G_2^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

3) *There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and parity-check matrices H_1 and H_2 of C such that*

$$H_1 H_2^T = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

By convention, the set $\{a_1, a_2, \ldots, a_{k-\ell}\}$ (resp., $\{b_1, b_2, \ldots, b_{n-k-\ell}\}$) will be referred to the empty set if $k - \ell = 0$ (resp., $n - k - \ell = 0$).

Proof. To prove 1) $\Leftrightarrow$ 2), assume that $\dim(\mathrm{Hull}(C)) = \ell$. Let G be a generator matrix of C. By Proposition 3.1, we have that $\mathrm{rank}(GG^T) = k - \ell$. Applying suitable elementary row and column operations, it follows that

$$(PG)(QG)^T = PGG^T Q^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0)$$

for some nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and invertible $k \times k$ matrices P and Q over $\mathbb{F}_q$. Let $G_1 = PG$ and $G_2 = QG$. Then G_1 and G_2 are generator matrices of C such that $G_1 G_2^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0)$.

Conversely, assume that 2) holds. Then $\mathrm{rank}(G_1 G_2^T) = k - \ell$ and hence $\dim(\mathrm{Hull}(C)) = \ell$ by Proposition 3.1.

Since $\mathrm{Hull}(C) = \mathrm{Hull}(C^\perp)$, the equivalence 1) $\Leftrightarrow$ 3) can be obtained similarly. $\square$

3.2   Diagonalizability of Gramians

From Subsection 3.1, it guarantees that for a given linear code C over $\mathbb{F}_q$, there exist generator matrices G_1 and G_2 of C such that $G_1 G_2^T$ is a diagonal matrix. Here, we focus on the diagonalizability the Gramian of a generator matrix of a linear code. The results are given in two cases based on the characteristic of the underlying finite field.

3.2.1   Odd Characteristics

For an odd prime power q, the Gramian of a generator/parity-check matrix of a linear code over $\mathbb{F}_q$ will be shown to be diagonalizable.

We begin with the following useful lemma.

Lemma 3.3. *Let C be a linear code of length n over $\mathbb{F}_q$. If q is odd and C is not Euclidean self-orthogonal, then there exists an element $\boldsymbol{v} \in C$ such that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$. In this case, $\boldsymbol{v} \notin \mathrm{Hull}(C)$.*

Proof. Assume that q is an odd prime power and C is not Euclidean self-orthogonal. Then there exist $\boldsymbol{u}$ and $\boldsymbol{w}$ in C such that $\langle \boldsymbol{u}, \boldsymbol{w} \rangle \neq 0$. If $\langle \boldsymbol{u}, \boldsymbol{u} \rangle \neq 0$ or $\langle \boldsymbol{w}, \boldsymbol{w} \rangle \neq 0$, we are done. Assume that $\langle \boldsymbol{u}, \boldsymbol{u} \rangle = 0$ and $\langle \boldsymbol{w}, \boldsymbol{w} \rangle = 0$. Let $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$. Since q is odd, we have $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = \langle \boldsymbol{u}, \boldsymbol{u} \rangle + 2\langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{w}, \boldsymbol{w} \rangle = 2\langle \boldsymbol{u}, \boldsymbol{w} \rangle \neq 0$ as desired. Clearly, the said element is not in $\mathrm{Hull}(C)$. $\qquad\square$

Proposition 3.4. *Let C be a non-zero linear code of length n over $\mathbb{F}_q$. If q is odd, then the Gramian of a generator matrix of C is diagonalizable.*

Proof. Assume that q is an odd prime power. We prove by induction on the dimension of C. If $\dim(C) = 1$, then Gramian of a generator matrix of C is a 1×1 matrix over $\mathbb{F}_q$ which is always diagonalizable.

Assume that $\dim(C) = k$ for some positive integer k and assume that the statement holds true for all linear codes of dimension $k-1$.

If C is Euclidean self-orthogonal, then $GG^T = [0]$ is diagonalizable for all generator matrices G of C by Proposition 3.1. Assume that C is not Euclidean self-orthogonal. Since q is odd, there exist $\boldsymbol{v} \in C$ such that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$ by Lemma 3.3. Let $D = \{ \boldsymbol{c} \in C \mid \langle \boldsymbol{v}, \boldsymbol{c} \rangle = 0 \}$. Since $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$, we have $C = D \oplus \langle \boldsymbol{v} \rangle$ which implies that $\dim(D) = k-1$. By the induction hypothesis, there exists a generator matrix

$$
G = \begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_{k-1} \end{bmatrix}
$$

of D whose Gramian GG^T is diagonal. Since $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{k-1}\} \subseteq D$, $\langle \boldsymbol{v}_i, \boldsymbol{v} \rangle = 0$ for all $1 \leq i \leq k-1$. Hence, $G' = \begin{bmatrix} \boldsymbol{v} \\ G \end{bmatrix}$ is a generator matrix for C such that the Gramian $G'G'^T$ is a diagonal matrix. $\qquad\square$

The following corollary is a direct consequence of Proposition 3.4. Since a parity-check matrix of a linear code is a generator matrix for its dual, the above results can be restated including the parity-check matrix easily.

Corollary 3.5. *Let C be a linear $[n, k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. If q is odd, then the following statements hold.*

7

1. *There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and a generator matrix G of C such that*

$$GG^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

2. *There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and a parity-check matrix H of C such that*

$$HH^T = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

Linear codes with orthogonal or orthonormal basis are good candidates in some applications. However, in general, an orthogonal or orthonormal basis dose not need to be exist. The existence of an orthonormal basis of some Euclidean complementary dual codes has been studied in [8]. Here, characterization for the existence of an orthogonal basis of Euclidean complementary dual codes over finite fields of odd characteristic can be obtained directly from Proposition 3.4.

Corollary 3.6. *Let q be an odd prime power and let C be a linear code over $\mathbb{F}_q$. Then C is Euclidean complementary dual if and only if C has a Euclidean orthogonal basis.*

3.2.2 Even Characteristics

The following results on the diagonalizability of the Gramians of generator and parity-check matrices of linear codes hold true for every prime powers q. However, for an odd prime power q, we already have stronger results described in the previous subsection. In practice, we may assume that q is a two power for the following results.

Proposition 3.7. *Let C be a linear $[n, k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. If $\mathrm{Hull}(C)$ is maximal self-orthogonal in C, then there exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and a generator matrix G of C such that*

$$GG^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

Precisely, the Gramian of a generator matrix of a linear code C whose hull is maximal self-orthogonal in C is diagonalizable.

Proof. Let $\mathcal{B} = \{r_1, r_2, \ldots, r_\ell\}$ be a basis of $\mathrm{Hull}(C)$. Assume that $\mathrm{Hull}(C)$ is maximal self-orthogonal in C. If there exists a codeword $x \in C \backslash \mathrm{Hull}(C)$ such that $\langle x, x \rangle = 0$, then $\langle x, c \rangle = 0$ for all $c \in \mathrm{Hull}(C)$. This implies that $\mathrm{Hull}(C) + \langle x \rangle$ is self-orthogonal in C which is containing $\mathrm{Hull}(C)$, a contradiction. Hence, $\langle x, x \rangle \neq 0$ for

8

all $\boldsymbol{x} \in C \backslash \mathrm{Hull}(C)$. Extending $\mathcal{B}$ to a basis $\mathcal{B} \cup \{\boldsymbol{t}_{\ell+1}, \boldsymbol{t}_{\ell+2}, \ldots, \boldsymbol{t}_k\}$ of C. Using the Gram-Schmidt process, $\langle \boldsymbol{t}_{\ell+1}, \boldsymbol{t}_{\ell+2}, \ldots, \boldsymbol{t}_k \rangle$ contains an orthogonal basis, denoted by $\{\boldsymbol{r}_{\ell+1}, \boldsymbol{r}_{\ell+2}, \ldots, \boldsymbol{r}_k\}$. Hence $\mathcal{B}' = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_\ell, \boldsymbol{r}_{\ell+1}, \boldsymbol{r}_{\ell+2}, \ldots, \boldsymbol{r}_k\}$ is a basis for C such that $\langle \boldsymbol{r}_i, \boldsymbol{r}_i \rangle \neq 0$ for all $\ell + 1 \leq i \leq k$ and $\langle \boldsymbol{r}_i, \boldsymbol{r}_j \rangle = 0$ for all $1 \leq i \leq k$ and $1 \leq j \leq k$ such that $i \neq j$ or $1 \leq i = j \leq \ell$.

For $1 \leq i \leq k - \ell$, let $a_i = \langle \boldsymbol{r}_{\ell+i}, \boldsymbol{r}_{\ell+i} \rangle \neq 0$. Let $G_1 = \begin{bmatrix} \boldsymbol{r}_{\ell+1} \\ \vdots \\ \boldsymbol{r}_k \end{bmatrix}$, $G_2 = \begin{bmatrix} \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_\ell \end{bmatrix}$

and $G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}$. Then $G_1 G_1^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell})$, $G_1 G_2^T = [0]$, $G_2 G_1^T = [0]$ and $G_2 G_2^T = [0]$. Hence,

$$
GG^T = \left[\begin{array}{c|c} G_1 G_1^T & G_1 G_2^T \\ \hline G_2 G_1^T & G_2 G_2^T \end{array} \right] = \left[\begin{array}{c|c} \begin{matrix} a_1 & & \\ & \ddots & \\ & & a_{k-\ell} \end{matrix} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array} \right] = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0)
$$

as desired. □

Similarly to the previous proposition, we can replace a generator matrix G by a parity-check matrix H of C and derive the following result.

Corollary 3.8. *Let C be a linear $[n, k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. If $\mathrm{Hull}(C)$ is maximal self-orthogonal in $C^{\perp}$, then there exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and a parity-check matrix H of C such that*

$$
HH^T = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).
$$

In the case where C is maximal self-orthogonal, then $\mathrm{Hull}(C) = C$ is maximal self-orthogonal in $C^{\perp}$. Hence, we have the following corollary.

Corollary 3.9. *Let C be a linear $[n, k]_q$ code. If C is maximal self-orthogonal, then there exist nonzero elements $b_1, b_2, \ldots, b_{n-2k}$ in $\mathbb{F}_q$ and a parity-check matrix H of C whose Gramian is*

$$
HH^T = \mathrm{diag}(b_1, b_2, \ldots, b_{n-2k}, 0, \ldots, 0).
$$

Lemma 3.10. *Let C be a linear $[n, k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. Then the following statements hold.*

1) *If $k - \ell \leq 1$, then $\mathrm{Hull}(C)$ is maximal self-orthogonal in C.*

2) *If $n - k - \ell \leq 1$, then* $\mathrm{Hull}(C)$ *is maximal self-orthogonal in* $C^{\perp}$.

Proof. To prove 1), assume that $k - \ell \leq 1$. If $k - \ell = 0$, then we have $k = \ell$ which means $\mathrm{Hull}(C) = C$. Hence, $\mathrm{Hull}(C)$ is a self-orthogonal in C, i.e., C is maximal self-orthogonal in C. Assume that $k - \ell = 1$. Then there exists $\boldsymbol{v} \in C \backslash \mathrm{Hull}(C)$. Suppose that $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0$. Then $C = \langle \boldsymbol{v} \rangle + \mathrm{Hull}(C)$. Since $\langle \boldsymbol{v}, \boldsymbol{c} \rangle = 0$ for all $\boldsymbol{c} \in C$, we have $\boldsymbol{v} \in \mathrm{Hull}(C)$ which is a contradiction. Hence, $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \neq 0$. Therefore, $\mathrm{Hull}(C)$ is maximal self-orthogonal in C.

By replacing C with $C^{\perp}$ in 1), the result of 2) follows similarly. $\qquad\square$

Corollary 3.11. *Let C be a linear $[n, k]_q$ code such that $\dim(\mathrm{Hull}(C)) = \ell$. If q is even, then the following statements hold.*

1) *$k - \ell \leq 1$ if and only if $\mathrm{Hull}(C)$ is maximal self-orthogonal in C.*

2) *$n - k - \ell \leq 1$ if and only if $\mathrm{Hull}(C)$ is maximal self-orthogonal in $C^{\perp}$.*

Proof. Assume that q is even. The sufficient part follows from Lemma 3.10. For necessity, assume that $k - \ell > 1$. Then there exist two linearly independent elements $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ in $C \setminus \mathrm{Hull}(C)$. Then $\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle \neq 0$ and $\langle \boldsymbol{v}_2, \boldsymbol{v}_2 \rangle \neq 0$. Since q is even, every element in $\mathbb{F}_q$ is square. Let a be an element in $\mathbb{F}_q$ such that $a^2 = \frac{\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle}{\langle \boldsymbol{v}_2, \boldsymbol{v}_2 \rangle}$. Then $\langle \boldsymbol{v}_1 + a\boldsymbol{v}_2, \boldsymbol{v}_1 + a\boldsymbol{v}_2 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle + 2a\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle + a^2\langle \boldsymbol{v}_2, \boldsymbol{v}_2 \rangle = 2\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle = 0$ and $\boldsymbol{v}_1 + a\boldsymbol{v}_2 \in C \setminus \mathrm{Hull}(C)$. Hence, $\mathrm{Hull}(C) + \langle \boldsymbol{v}_1 + a\boldsymbol{v}_2 \rangle$ is Euclidean self-orthogonal and $\mathrm{Hull}(C) \subsetneq \mathrm{Hull}(C) + \langle \boldsymbol{v}_1 + a\boldsymbol{v}_2 \rangle \subseteq C$. Therefore, $\mathrm{Hull}(C)$ is not maximal self-orthogonal in C.

The second statement follows immediately from 1). $\qquad\square$

Corollary 3.12. *Let C be a non-zero linear code of length n over $\mathbb{F}_q$. If q is even and $\dim(C) - \dim(\mathrm{Hull}(C)) \leq 1$, then the Gramian of a generator matrix of C is diagonalizable.*

The diagonalizabilty studied above will be useful in the applications in Section 5.

4 Hermitian Hulls of Linear Codes

For a prime power q, the *Hermitian inner product* of $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_{q^2}^n$ is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_H := \sum_{i=1}^{n} u_i v_i^q.$$

10

The *Hermitian dual* $C^{\perp_H}$ of C is defined to be the set

$$C^{\perp_H} = \{\boldsymbol{v} \in \mathbb{F}_{q^2}^n \mid \langle \boldsymbol{c}, \boldsymbol{v} \rangle_H = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

The *Hermitian hull* of a code C is $C \cap C^{\perp_H}$ and denote by $\text{Hull}_H(C) = C \cap C^{\perp_H}$. A code C is said to be *Hermitian self-orthogonal* if $C \subseteq C^{\perp_H}$ and it is said to be *Hermitian complementary dual* if $\text{Hull}_H(C) = \{\boldsymbol{0}\}$. Clearly, C is Hermitian self-orthogonal if $\text{Hull}_H(C) = C$. For an $m \times n$ matrix $A = [a_{ij}]$, denote by $A^\dagger = [a_{ji}^q]$ the conjugate transpose of A. For each $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_{q^2}^n$, denote by $\overline{\boldsymbol{v}} = (v_1^q, v_2^q, \ldots, v_n^q)$ the conjugate vector of $\boldsymbol{v}$.

In this section, a discussion on Hermitian hulls of linear codes is given. We note that most of the results in this section can be obtained using the arguments analogous to those in Section 3. Therefore, the proofs for those results will be omitted. Some proofs are provided if they are required and different from those in Section 3. For convenience, the theorem numbers are given in the form $3.N'$ if it corresponds to $3.N$ in Section 3.

The Hermitian hull dimension of linear codes has been characterized in [11]. Here, we provide an alternative characterizations of the Hermitian hull dimension of linear codes.

Proposition 4.1. *Let C be a linear $[n, k]_{q^2}$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\text{Hull}_H(C)) = \ell$.

2) $\text{rank}(GG^\dagger) = k - \ell$ *for every generator matrix G of C.*

3) $\text{rank}(G_1 G_2^\dagger) = k - \ell$ *for all generator matrices G_1 and G_2 of C.*

4) $\text{rank}(HH^\dagger) = n - k - \ell$ *for every parity-check matrix H of C.*

5) $\text{rank}(H_1 H_2^\dagger) = n - k - \ell$ *for all parity-check matrices H_1 and H_2 of C.*

From Proposition 4.1, the following characterizations can be obtained directly.

Corollary 4.2. *Let C be a linear $[n, k]_{q^2}$ code and let ℓ be a non-negative integer. Then the following statements are equivalent.*

1) $\dim(\text{Hull}_H(C)) = \ell$.

2) *There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_{q^2}$ and generator matrices G_1 and G_2 of C such that*

$$G_1 G_2^\dagger = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

3) *There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_{q^2}$ and parity-check matrices H_1 and H_2 of C such that*

$$H_1 H_2^\dagger = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

For an odd prime power q, we show that $GG^\dagger$ is always diagonalizable for every generator matrix G of a linear code over $\mathbb{F}_{q^2}$. We begin with the following useful lemma.

Lemma 4.3. *Let C be a linear code of length n over $\mathbb{F}_{q^2}$. If q is odd and C is not Hermitian self-orthogonal, then there exists an element $v \in C$ such that $\langle v, v \rangle_H \neq 0$.*

Proof. Assume that q is an odd prime power and C is not Hermitian self-orthogonal. Then there exist u and w in C such that $\langle u, w \rangle_H \neq 0$. If $\langle u, u \rangle_H \neq 0$ or $\langle w, w \rangle_H \neq 0$, we are done. Assume that $\langle u, u \rangle_H = 0$ and $\langle w, w \rangle_H = 0$. Let $v = u + \langle u, w \rangle_H w$. Since q is odd, we have

$$\begin{aligned}
\langle v, v \rangle_H &= \langle u, u \rangle_H + \langle u, w \rangle_H^q \langle u, w \rangle_H + \langle u, w \rangle_H \langle w, u \rangle_H + \langle u, w \rangle_H^{q+1} \langle w, w \rangle_H \\
&= \langle u, w \rangle_H^q \langle u, w \rangle_H + \langle u, w \rangle_H \langle u, w \rangle_H^q \\
&= 2 \langle u, w \rangle_H^q \langle u, w \rangle_H \\
&\neq 0
\end{aligned}$$

as desired. $\qquad\square$

Applying Lemma 4.3 instead of Lemma 3.3, the next proposition can be obtained using the arguments similar to those for the proof of Proposition 3.4.

Proposition 4.4. *Let C be a non-zero linear code of length n over $\mathbb{F}_{q^2}$. If q is odd, then $GG^\dagger$ is diagonalizable for every generator generator matrix G of C.*

The following corollary is a direct consequence of Proposition 4.4

Corollary 4.5. *Let C be a linear $[n, k]_{q^2}$ code such that $\mathrm{dim}(\mathrm{Hull}(C)) = \ell$. If q is odd, then the following statements hold.*

1. There exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_q$ and a generator matrix G of C such that

$$GG^T = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

2. There exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_q$ and a parity-check matrix H of C such that

$$HH^T = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

Corollary 4.6. *Let q be an odd prime power and let C be a linear code over $\mathbb{F}_{q^2}$. Then C is Hermitian complementary dual if and only if C has a Hermitian orthogonal basis.*

The following results hold true for every prime powers q. However, for an odd prime power q, we already have stronger results in discussion above. In practice, we may assume that q is even.

Proposition 4.7. *Let C be a linear $[n, k]_{q^2}$ code such that $\dim(\mathrm{Hull}_H(C)) = \ell$. If $\mathrm{Hull}_H(C)$ is maximal self-orthogonal in C, then there exist nonzero elements $a_1, a_2, \ldots, a_{k-\ell}$ in $\mathbb{F}_{q^2}$ and a generator matrix G of C such that*

$$GG^\dagger = \mathrm{diag}(a_1, a_2, \ldots, a_{k-\ell}, 0, \ldots, 0).$$

We can replace a generator matrix G by a parity-check matrix H of C and derive the result as follows.

Corollary 4.8. *Let C be a linear $[n, k]_{q^2}$ code such that $\dim(\mathrm{Hull}_H(C)) = \ell$. If $\mathrm{Hull}_H(C)$ is maximal self-orthogonal in $C^{\perp_H}$, then there exist nonzero elements $b_1, b_2, \ldots, b_{n-k-\ell}$ in $\mathbb{F}_{q^2}$ and a parity-check matrix H of C such that*

$$HH^\dagger = \mathrm{diag}(b_1, b_2, \ldots, b_{n-k-\ell}, 0, \ldots, 0).$$

Corollary 4.9. *Let C be a linear $[n, k]_{q^2}$ code. If C is maximal Hermitian self-orthogonal, then there exist nonzero elements $b_1, b_2, \ldots, b_{n-2k}$ in $\mathbb{F}_{q^2}$ and a parity-check matrix H of C such that*

$$HH^\dagger = \mathrm{diag}(b_1, b_2, \ldots, b_{n-2k}, 0, \ldots, 0).$$

Corollary 4.10. *Let C be a linear $[n, k]_{q^2}$ code such that $\dim(\mathrm{Hull}_H(C)) = \ell$. If q is even, then the following statements hold.*

1) $k - \ell \leq 1$ *if and only if* $\mathrm{Hull}_H(C)$ *is maximal self-orthogonal in C.*

13

2) $n - k - \ell \leq 1$ if and only if $\mathrm{Hull}_H(C)$ is maximal self-orthogonal in $C^{\perp_H}$.

Corollary 4.11. *Let C be a non-zero linear code of length n over $\mathbb{F}_{q^2}$. If q is even and $\dim(C) - \dim(\mathrm{Hull}_H(C)) \leq 1$, then $GG^\dagger$ is diagonalizable for every generator matrix G of C.*

5 Applications

In this section, hulls and the diagonalizability of the Gramians discussed in Sections 3 and 4 are applied to constructions of Entanglement-Assisted Quantum Error Correcting Codes (EAQECCs). EAQECCs were introduced in [12] which can be constructed from classical linear codes. In this case, the performance of the resulting quantum codes can be determined by the performance of the underlying classical codes. Precisely, an $[[n, k, d; c]]_q$ EAQECC encodes k logical qudits into n physical qudits using c copies of maximally entangled states and its performance is measured by its rate $\frac{k}{n}$ and net rate $(\frac{k-c}{n})$. As shown in [4], the net rate of an EAQECC is positive it is possible to obtain catalytic codes. The readers may refer to [3], [11] and the references therein for more details on EAQECCs.

The following results from [11] are useful for constructions of EAQECCs from classical linear codes and their hulls.

Proposition 5.1 ([11, Corollary 3.1]). *Let C be a classical $[n, k, d]_q$ linear code and $C^\perp$ its Euclidean dual with parameters $[n, n - k, d^\perp]_q$. Then there exist $[[n, k - \dim(Hull(C)), d; n-k-\dim(\mathrm{Hull}(C))]]_q$ and $[[n, n-k-\dim(\mathrm{Hull}(C)), d^\perp; k-\dim(\mathrm{Hull}(C))]]_q$ EAQECCs.*

Proposition 5.2 ([11, Corollary 3.2]). *Let C be a classical $[n, k, d]_{q^2}$ code and let $C^{\perp_H}$ be its Hermitian dual with parameters $[n, n-k, d^{\perp_H}]_{q^2}$. Then there exists $[[n, k - \dim(\mathrm{Hull}_H(C)), d; n - k - \dim(\mathrm{Hull}_H(C))]]_q$ and $[[n, n - k - \dim(\mathrm{Hull}_H(C)), d^\perp; k - \dim(\mathrm{Hull}_H(C))]]_q$ EAQECCs.*

Based on the diagonalizability of Gramians studied in Sections 3 and 4, EAQECCs can be constructed from all linear codes over finite fields of odd characteristic as follows.

Proposition 5.3. *Let $q \geq 5$ be an odd prime power and let C be a classical $[n, k, d]_q$ linear code such that $\dim(\mathrm{Hull}(C)) = \ell$. Then there exists an $[[n + r, k - \ell, d'; n - k - \ell + r]]_q$ EAQECC with $d \leq d' \leq d + r$ for each $0 \leq r \leq k - \ell$.*

14

Proof. If $r = 0$ or $k = \ell$, then the result follows directly from Proposition 5.1. Next, assume that $1 \le r \le k - \ell$. Since q is odd, there exists a generator matrix G for C such that the Gramian GG^T is diagonalizable by Proposition 3.4. Precisely, there exist linearly independent elements $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k-\ell}$ in C such that $\boldsymbol{x}_i \boldsymbol{x}_i^T \ne 0$ for all $1 \le i \le n - k$ and $\boldsymbol{x}_i \boldsymbol{x}_j^T = 0$ for all $1 \le i < j \le k - \ell$.

Since $q \ge 5$, we have that $\{a^2 \mid a \in \mathbb{F}_q^*\}$ contains at least 2 elements. Hence, for each $i \in \{1, 2, \ldots, k - \ell\}$, there exists $\alpha_i \in \mathbb{F}_q^*$ such that $\alpha_i^2 \ne -\boldsymbol{x}_i \boldsymbol{x}_i^T$. Let H be a parity check matrix for C and let C' be the code with parity check matrix

$$H' = \begin{pmatrix} \begin{array}{c|c} 0 & H \\ \hline \alpha_1 & \boldsymbol{x}_1 \\ & \vdots \\ \ddots & \vdots \\ \alpha_r & \boldsymbol{x}_r \end{array} \end{pmatrix}.$$

Then

$$H'(H')^T = \begin{pmatrix} HH^T & 0 & \ldots & 0 \\ 0 & \alpha_1^2 + \boldsymbol{x}_1 \boldsymbol{x}_1^T & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \alpha_r^2 + \boldsymbol{x}_r \boldsymbol{x}_r^T \end{pmatrix}.$$

Since $\alpha_i^2 \ne -\boldsymbol{x}_i \boldsymbol{x}_i^T$ for all $1 \le i \le r$ and $\mathrm{rank}(HH^T) = n - k - \ell$, we have that $\mathrm{rank}(H'(H')^T) = n - k - \ell + r \ge 0$ since $\ell \le \min\{k, n - k\}$ and $r \ge 0$. Equivalently, $\dim(\mathrm{Hull}(C')) = \ell$. Since every $d - 1$ columns of H are linearly independent and $\alpha_i \ne 0$ for all $i \in \{1, 2, \ldots, r\}$, every $d - 1$ columns of H' are linearly independent. It follows that C' is an $[n + r, k, d']_q$ code where $d \le d' \le d + r$. Then by Proposition 5.1, there exists an $[[n + r, k - \ell, d'; n - k - \ell + r]]_q$ EAQECC. $\qquad\square$

In the same fashion, the Hermitian hulls of linear codes can be applied in constructions of EAQECCs in the following proposition.

Proposition 5.4. *Let $q \ge 3$ be an odd prime power and let C be a classical $[n, k, d]_{q^2}$ linear code such that $\dim(\mathrm{Hull}_H(C)) = \ell$. Then there exists an $[[n + r, k - \ell, d'; n - k - \ell + r]]_q$ EAQECC with $d \le d' \le d + r$ for each $0 \le r \le k - \ell$.*

Proof. If $r = 0$ or $k = \ell$, then the result follows directly from Proposition 5.2. Next, assume that $1 \le r \le k - \ell$. Since q is odd, there exists a generator matrix G for C such that $GG^\dagger$ is diagonalizable by Proposition 4.4. Precisely, there exist linearly independent elements $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{k-\ell}$ in C such that $\boldsymbol{x}_i \boldsymbol{x}_i^\dagger \ne 0$ for all $1 \le i \le n - k$ and $\boldsymbol{x}_i \boldsymbol{x}_j^\dagger = 0$ for all $1 \le i < j \le k - \ell$.

For each $i \in \{1, 2, \ldots, r\}$, there exist $\alpha_i \in \mathbb{F}_{q^2}^*$ such that $\alpha_i{}^{q+1} \neq -\boldsymbol{x}_i \boldsymbol{x}_i^\dagger$ since $q \geq 3$. Let H be a generator matrix for $C^{\perp_H}$ and let C' be the code with parity check matrix

$$
H' = \left(\begin{array}{ccc|c}
0 & & & H \\
\alpha_1 & & & \boldsymbol{x}_1 \\
& \ddots & & \vdots \\
& & \alpha_r & \boldsymbol{x}_r
\end{array} \right).
$$

Then

$$
H'(H')^\dagger = \left(\begin{array}{cccc}
HH^\dagger & 0 & \cdots & 0 \\
0 & \alpha_1^{q+1} + \boldsymbol{x}_1 \boldsymbol{x}_1^\dagger & & 0 \\
\vdots & & \ddots & \\
0 & 0 & & \alpha_r^{q+1} + \boldsymbol{x}_r \boldsymbol{x}_r^\dagger
\end{array} \right).
$$

Since $\alpha_i^{q+1} \neq -\boldsymbol{x}_i \boldsymbol{x}_i^\dagger$ for all $1 \leq i \leq r$ and $\mathrm{rank}(HH^\dagger) = n - k - \ell$, we have that $\mathrm{rank}(H'(H')^\dagger) = n - k - \ell + r \geq 0$ since $\ell \leq \min\{k, n - k\}$ and $r \geq 0$. Equivalently, $\dim(\mathrm{Hull}_H(C')) = \ell$. It is easily seen that very $d - 1$ columns of H' are linearly independent. Hence, C' is an $[n + r, k, d']_{q^2}$ code where $d \leq d' \leq d + r$. By Proposition 5.2, there exists an $[[n + r, k - \ell, d'; n - k - \ell + r]]_q$ EAQECC. $\qquad \square$

Observe that linear $[n, k]_q$ and $[n, k]_{q^2}$ codes with $\frac{n}{2} < k \leq n$ have hull dimension $\ell \leq \min\{k, n - k\} \leq n - k$ which implies that $k - \ell \geq 2k - n$. From the constructions in Propositions 5.3 and 5.4, we have an EAQECC Q with parameters $[[n + r, k - \ell, d'; n - k - \ell + r]]_q$ for all $0 \leq r \leq k - \ell$. Hence, the net rate of Q is

$$
\frac{(k - \ell) - (n - k - \ell + r)}{n + r} = \frac{2k - n - r}{n + r} > 0
$$

for all classical linear codes with $k > \frac{n}{2}$ and $0 \leq r < 2k - n$ since $2k - n \leq k - \ell$. In addition, if the dimension of the input linear code is

$$
k \geq \frac{3n + r}{4}, \tag{1}
$$

its hull dimension is $\ell \leq \min\{k, n - k\} \leq n - k \leq n - \frac{3n+r}{4} = \frac{n-r}{4}$ which implies that $k - \ell \geq k - \frac{n-r}{4} \geq \frac{3n+r}{4} - \frac{n-r}{4} = \frac{n+r}{2}$, and hence, the rate of Q is

$$
\frac{k - \ell}{n + r} \geq \frac{1}{2}.
$$

To obtain EAQECCs with good minimum distances, the input linear code using Propositions 5.3 and 5.4 can be chosen from the best-known linear codes in the database of [2]. Moreover, the required number of maximally entangled states $c := n - k - \ell + r$ can be adjusted by the parameter r.

Remark 5.1. We have the following observations and suggestions for the constructions of EAQECCs in Propositions 5.3 and 5.4.

1. By choosing best-known linear codes in [2] satisfy the condition $k \geq \frac{3n+r}{4}$ in (1), all the EAQECCs obtained in Propositions 5.3 and 5.4 are good in the sense that they have good rate and positive net rate. Moreover, some of them have good minimum distances.

2. Under the assumption $\ell \leq k - \frac{n+r}{2}$, EAQECCs constructed in Propositions 5.3 and 5.4 have good rate

$$\frac{k-\ell}{n+r} \geq \frac{1}{2}$$

and positive net rate

$$\frac{(k-\ell)-(n-k-\ell+r)}{n+r} = \frac{2k-n-r}{n+r} > 0$$

for all $0 \leq r < 2k - n$. It is easily seen that the condition $\ell \leq k - \frac{n+r}{2}$ is slightly lighter than (1) and it is equivalent to finding classical linear codes with large dimension and small Euclidean/Hermitian hull dimension. Therefore, linear complementary dual codes studied in [5–8, 11, 21] would be good candidates in constructions of EAQECCs.

References

[1] Assmus, E. F., Key, J. D.: Affine and projective planes, Discrete Math. **83**, 161–187 (1990).

[2] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language, J. Symbolic Comput. **24**, 235–265 (1997).

[3] Brun, T., Devetak, I., Hsieh, H. M.: Correcting quantum errors with entanglement, Science **314**, 436–439 (2006).

[4] Brun T., Devetak I., Hsieh M. H.: Catalytic quantum error correction, IEEE Trans. Inform. Theory **60**, 3073–3089 (2014).

[5] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks, Adv. Math. Commun. **10**, 131–150 (2016).

[6] Carlet, C., Mesnager, S., Tang, C., Qi, Y., Pellikaan, R.: Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, IEEE Trans. Inform. Theory **64**, 3010–3017 (2018).

[7] Carlet, C., Mesnager, S., Tang, C., Qi, Y.: Euclidean and Hermitian LCD MDS codes, Des. Codes Cryptogr. **86**, 2605–2618 (2018).

[8] Carlet, C., Mesnager, S., Tang, C., Qi, Y.: New characterization and parametrization of LCD codes, IEEE Trans. Inform. Theory **65**, 39–49 (2019).

[9] Ezerman, M. F., Jitman, S., Kiah, H. M., Ling, S.: Pure asymmetric quantum MDS codes from CSS construction: A complete characterization, Int. J. of Quantum Information **11**, 1350027 (2013).

[10] Fish, W., Key, J. D., Mwambene, E., Rodrigues, B.: Hamming graphs and special LCD codes, J. Appl. Math. Comput. (2019). https://doi.org/ 10.1007/s12190-019-01259-w.

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

[12] Hsich, M. H., Devetak, I., Brun, T.: General entanglement-assisted quantum error-correcting codes, Phys. Rev. A **76**, 062313 (2007).

[13] Jin, L.: Construction of MDS codes with complementary duals, IEEE Trans. Inform. Theory **63**, 2843–2847 (2017).

[14] Jin, L., Ling, S., Luo, J., Xing, C.: Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes, IEEE Trans. Inform. Theory **56**, 4735–4740 (2010).

[15] Jin, L., Xing, C.: Euclidean and Hermitian self-orthogonal algebraic geometry and their application to quantum codes, IEEE Trans. Inform. Theory **58**, 5484–5489 (2012).

[16] Lidl, R., Niederreiter, H.: Finite fields, Cambridge University Press, (1997).

[17] Liu, H., Pan, X.: Galois hulls of linear codes over finite fields, (2018) https://arxiv.org/pdf/1809.08053

[18] Leon, J. S.: Computing automorphism groups of error-correcting codes, IEEE Trans. Inform. Theory **28**, 496–511 (1982).

[19] Leon, J. S.: Permutation group algorithms based on partition, I: theory and algorithms, J. Symbolic Comput. **12**, 533–583 (1991).

[20] Luo, G., Cao, X., Chen, X.: MDS codes with hulls of arbitrary dimensions and their quantum error correction, IEEE Trans. Inform. Theory **65**, 2944–2952 (2019).

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

[22] Pang, B., Zhu, S., Li, J: On LCD repeated-root cyclic codes over finite fields, J. Appl. Math. Comput. **56**, 625–635 (2018).

[23] Pless, V.: A classification of self-orthogonal codes over GF(2), Discrete Math. **3**, 209–246 (1972).

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

[25] Sendrier, N.: On the dimension of the hull, SIAM J. Appl. Math. **10**, 282–293 (1997).

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

[27] Sendrier, N.: Finding the permutation between equivalent codes: the support splitting algorithm, IEEE Trans. Inform. Theory **46**, 1193–1203 (2000).

[28] Sendrier, N., Skersys, G.: On the computation of the automorphism group of a linear code, in: Proceedings of IEEE ISIT'2001, Washington, DC, 2001, p. 13.

[29] Wilde, M. M., Brun, T. A.: Optimal entanglement formulas for entanglement-assisted quantum coding, Phys. Rev. A **77**, 064302 (2008).