# Linear codes with arbitrary dimensional hull and pure LCD code.*

Maouche Youcef

[1] Faculty of Mathematics, University of Science and Technology Houari Boumediene, Bab Ezzouar, Algiers, Algeria.

**Abstract.** In this paper, we introduce a general construction of linear codes with small dimension hull from any non LCD codes. Furthermore, we show that for any linear code $\mathcal{C}$ over $\mathbb{F}_q$ ($q > 3$) with $dim(Hull(\mathcal{C})) = h$ there exist an equivalent codes $\mathcal{C}_j$ with $dim(Hull(\mathcal{C}_j)) = j$ for any integer $0 \leq j \leq h$. We also introduce the notion of pure LCD code; an LCD code and all its equivalent are LCD; and construct an infinite family of pure LCD codes. In addition, we introduce a general construction of linear codes with one dimension hull.

**Keywords.** LCD codes; Pure LCD codes; Hulls; Entanglement-assisted quantum error correcting codes.

2010 *Mathematics Subject Classification.* Primary 94B15, 94B05; Secondary 11T71.

## 1 Introduction

The Euclidean hull of a linear code $\mathcal{C}$ is the intersection of $\mathcal{C}$ and its Euclidean dual $C^{\perp}$. A linear code $\mathcal{C}$ is called $h$-dim hull if $dim(hull(C)) = h$. With this definition, a linear

*ymaouche@usthb.dz.

complementary dual (LCD) code is a 0-dim hull code and an $[n, k]$ self-orthogonal code is $k$-dim hull. LCD codes have been widely applied in data storage, communications and cryptography [3, 4, 5, 6, 7, 10, 17, 18]. Massey [12] gave the algebraic characterization of LCD codes, and showed that asymptotically good LCD codes exist. In [6], the authors show that any linear code over $\mathbb{F}_q\,(q > 3)$ is equivalent to an Euclidean LCD code and any linear code over $\mathbb{F}_{q^2}\,(q > 2)$ is equivalent to a Hermitian LCD code.

Linear code with small hull are also interesting due to its crucial role in checking permutation equivalence of two linear codes and determining the complexity of algorithms for computing the automorphism group of a linear code [14, 11, 7]. In [11], the authors present some necessary and sufficient conditions that a linear codes and cyclic codes have one-dimensional hull and construct cyclic codes with one dimensional hull. In [7], Claude et al. employ character sums in semi-primitive case to construct LCD codes and linear codes with one-dimensional hull from cyclotomic fields and multiplicative subgroups of finite fields. In [5], Hao prove that for a nonnegative integer $h$ satisfying $0 \leq h \leq n-1$, a linear $[2n, n]$ self-dual code is equivalent to a linear $h$-dimension hull code. Recently, there have been a lot of research works on linear codes with small hulls and its application in entanglementassisted quantum error-correcting codes (EAQECCs), the reader is referred to [15, 8, 14].

The main goal of this manuscript is to extend the results in [7, 9] and construct an arbitrary dimensional hull from an existing one. We show that for any $[n, k, d]$ linear code over $\mathbb{F}_q\ (q > 3)$, with $h$ dimensional hull there exist a monomial equivalent codes $\mathcal{C}_j$ to $\mathcal{C}$ with $j$ dimensional hull for any $0 \leq j \leq h$. More precisely, we introduce a general construction of small dimensional hull codes from any linear codes and arbitrary dimensional hulls from any self-orthogonal code. Furthermore, we introduce pure LCD code and show that such codes are very rare or do not exist over finite fields with characteristic 2. In addition, we construct an infinite family of pure LCD code over finite fields with odd characteristics.

This paper is organized as follows. In Section 2, we give some preliminaries on linear codes and necessary and sufficient conditions for such code to be $h$ dimensional hull. In Section 3, we construct linear codes with small dimensional hull from any linear code and arbitrary dimensional hull from self-orthogonal codes. In Section 4, we introduce the notion of pure LCD codes and give a general construction of linear codes with one-dimensional hull.

## 2 Preliminaries

Throughout this paper, let $\mathbb{F}_q$ be a finite field of order $q = p^m$ where $p$ is prime and $m$ is a positive integer. The multiplicative group of $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^*$. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$ with dimension $k$ and minimum Hamming distance $d$. Let $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$, $\mathbf{y} = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_q^n$, their inner product is defined as usual

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1} \in \mathbb{F}_q.$$

Two vectors $\mathbf{x}$, $\mathbf{y}$ are called orthogonal if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. For a linear code $\mathcal{C}$ over $\mathbb{F}_q$, its dual code $\mathcal{C}^\perp$ is the set of vectors orthogonal to every codeword of $\mathcal{C}$ under the inner product i.e.,

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0, \quad \forall \mathbf{y} \in \mathcal{C}\}.$$

A code $\mathcal{C}$ is called self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and it is called self-dual if $\mathcal{C}^\perp = \mathcal{C}$. The hull of a linear code $\mathcal{C}$ is defined by

$$\text{hull}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp.$$

A linear code $\mathcal{C}$ is called $h$-dim hull if $dim(hull(C)) = h$. With this definition, a linear complementary dual (LCD) code is a 0-dim hull code and $[n, k]$ self-orthogonal code is $k$-dim hull. For any $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$ and permutation $\sigma$ of $\{1, 2, \cdots, n\}$, we define $\mathcal{C}_\mathbf{a}$ and $\sigma(\mathcal{C})$ as the following linear codes

$$\mathcal{C}_\mathbf{a} = \{(a_1 c_1, \cdots, a_n c_n) \ : \ (c_1, \cdots, c_n) \in \mathcal{C}\},$$

and

$$\sigma(\mathcal{C}) = \{(c_{\sigma(1)}, \cdots, c_{\sigma(n)}) \ : \ (c_1, \cdots, c_n) \in \mathcal{C}\}.$$

Two codes $\mathcal{C}$ and $\mathcal{C}'$ over $\mathbb{F}_q$ are called monomial equivalent if $\mathcal{C}' = \sigma(\mathcal{C}_\mathbf{a})$ for some permutation $\sigma$ of $\{1, 2, \cdots, n\}$ and $\mathbf{a} \in (\mathbb{F}_q^*)^n$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two codes over the same field $\mathbb{F}_q$, and let $G_1$ be a generator matrix for $\mathcal{C}_1$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomial equivalent if and only if there is a monomial matrix $M$ (a square matrix with exactly one nonzero entry in each row and column) so that $G_1 M$ is a generator matrix of $\mathcal{C}_2$.

Let $\mathcal{C}$ be an $[n, k]$ linear code. If $\mathcal{C}$ is the direct sum of subspaces $U_i$ for $1 \leq i \leq k$ which are mutually orthogonal, then we shall say that $\mathcal{C}$ is the orthogonal sum of the $U_i$ and use the symbol

$$\mathcal{C} = U_1 \perp \cdots \perp U_k.$$

**Theorem 2.1** *Let $\mathcal{C}$ be an $[n,k]$ linear code over $\mathbb{F}_q$ where $q$ is odd and $Hull(\mathcal{C}) = h$. Then there exist code words $\mathbf{c}_1, \cdots, \mathbf{c}_k \in \mathcal{C}$ such that*

$$\mathcal{C} =< \mathbf{c}_1 > \perp < \mathbf{c}_2 > \perp \cdots \perp < \mathbf{c}_k >$$

*and $\mathcal{C}$ is LCD if and only if $\mathbf{c}_i^2 \neq 0$ for $1 \leq i \leq k$. Furthermore,*

$$Hull(\mathcal{C}) =< \mathbf{c}_{j_1} > \perp < \mathbf{c}_{j_2} > \perp \cdots \perp < \mathbf{c}_{j_l} > \quad \mathbf{c}_{j_r}^2 = 0 \ \forall 1 \leq r \leq l.$$

**Proof.** Following [1], we regard $\mathcal{C}$ with the inner product as a subspace of finite geometry. Therefore, the proof follows from [[1], Theorem 3.7]. ■

**Corollary 2.2** *Let $\mathcal{C}$ be an $[n,k]$ linear code over $\mathbb{F}_q$ with $dim(Hull(\mathcal{C})) = h$ and $q$ is odd. There exists a generator matrix $G$ of $\mathcal{C}$ such that $GG^T$ is a diagonal matrix.*

**Proof.** The proof is immediate from Theorem 2.1 by choosing an orthogonal basis for $\mathcal{C}$. ■

**Theorem 2.3 ([13])** *If $G$ is a generator matrix for the $[n,k]$ linear code $\mathcal{C}$, then $\mathcal{C}$ is an LCD code if and only if, the $k \times k$ matrix $GG^T$ is nonsingular.*

The following proposition was proven in [8]. Theorem 2.1 and Corollary 2.2 give another proof for odd $q$, however, we give a third proof with a direct approach.

**Proposition 2.4 ([8])** *Let $\mathcal{C}$ be an $[n,k,d]_q$ linear code with parity check matrix $H$ and generator matrix $G$. Then, $rank(HH^T)$ and $rank(GG)$ are independent of $H$ and $G$ so that*

$$rank(HH^T) = n - k - dim(hull(C^\perp)) = n - k - dim(hull(C)),$$

*and*

$$rank(GG^T) = k - dim(hull(C^\perp)) = k - dim(hull(C)).$$

**Proof.** Since $Hull(C) = Hull(C^\perp)$, the second equalities are obvious. We have

$$\begin{aligned} Hull(C) &= \left\{x \in \mathbb{F}_q^n : x \in C, x \in C^\perp\right\} \\ &= \left\{x \in \mathbb{F}_q^n : x \in C, xG^T = 0\right\} \\ &= \left\{yG : y \in \mathbb{F}_q^k \mid yGG^T = 0\right\}. \end{aligned}$$

Note that $\#Hull(C) = \#Ker(GG^T)$, hence $dim(Hull(C)) = null(GG^T)$. Therefore

$$\begin{aligned} k &= rank(GG^T) + nul(GG^T) \\ &= rank(GG^T) + dim(Hull(C)). \end{aligned}$$

This completes the proof for the second statement. Since $G$ is a parity check matrix of $C^{\perp}$, the first statement can be proven by a similar argument. ■

The next theorem introduces a general construction of LCD code from any linear code over $\mathbb{F}_q$ ($q > 3$).

**Theorem 2.5 ([5])** *Let $q$ be a power of a prime with $q > 3$ and $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$. Then, there exists $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$ with $a_j \neq 0$ for any $1 \leq j \leq n$ such that $\mathcal{C}_{\mathbf{a}}$ is an LCD code.*

Let $M$ be an $k \times k$ matrix over $\mathbb{F}_q$ and $\mathbf{u}$ be a vector in $\mathbb{F}_q^k$. Following [7], we denote by $diag_k[\mathbf{u}]$ the diagonal $k \times k$ matrix whose elements on the diagonal are $u_1, \cdots, u_k$. Let $I = \{i_1, \cdots, i_l\}$ be a subset of $\{1, \cdots, k\}$, we define the submatrix $M_I$ of $M$ obtained by deleting the $i_1, \cdots, i_j$-th rows and columns of $M$. Denote $M_I = 1$ if $I = \{1, 2, \cdots, k\}$ and $M_{\emptyset} = M$. The following lemmas will be used in the sequel.

**Lemma 2.6 ([5])** *Let $M$ be a $k \times k$ matrix over $\mathbb{F}_q$ and $t$ an integer with $0 \leq t \leq k-1$. Suppose that $det(M_I) = 0$ holds for any subset $I$ of $\{1, 2, \cdots, k\}$ with $0 \leq \#I \leq t$. Then, for any $1 \leq j \leq t+1$ and every word $\mathbf{u} \in \mathbb{F}_q^k$ of Hamming weight $j$, denoting its support by $J$, we have:*

$$det(M + diag_k(\mathbf{u})) = \left( \prod_{i \in J} u_i \right) det(M_I).$$

**Lemma 2.7** *Let $M$ be a non-singular $k \times k$ matrix over $\mathbb{F}_q$. For any vector $\mathbf{u} \in \mathbb{F}_q^k / \{0\}$ with Hamming weight $j$ and support $J$, we suppose that $det(M_I) = 0$ holds for any subset $I$ of $J$ with $1 \leq \#I < j$. Then*

$$det(M + diag_k(\mathbf{u})) = det(M) + \left( \prod_{i \in J} u_i \right) det(M_J).$$

**Proof.** We prove this statement by induction on $j$. For any vector $\mathbf{u}$ of Hamming weight 1, denoting by $i_1$ the position of its only nonzero coordinate, we have

$$det(M + diag_k(\mathbf{u})) = det(M) + u_{i_1} det(M_{\{i_1\}}).$$

Thus, the statement is true for $j = 1$. Assume the statement is true for any vector $\mathbf{u}$ with Hamming weight $j = 1, 2, \cdots, s \leq k-1$. Let $\mathbf{u}$ be any vector with Hamming weight $s+1$ and $support(\mathbf{u}) = \{i_1, i_2, \cdots, i_{s+1}\} = J$. Let $\mathbf{u}'$ be the vectors with $support(\mathbf{u}') = \{i_1, i_2, \cdots, i_s\} = J'$. Then

$$det(M + diag(\mathbf{u})) = det(M + diag_k(\mathbf{u}')) + u_{i_{s+1}} det\left(M_{\{i_{s+1}\}} + diag_{k-1}(\mathbf{u}')\right).$$

Let $M' = M_{\{i_{s+1}\}}$. Observe that for any subset $I$ of $J'$ with $0 \leq \#I \leq \#J' - 1$ we have $det(M'_I) = det(M_{I \cup i_1}) = 0$. Applying Lemma 2.6, we get

$$det(M + diag(\mathbf{u})) = det(M + diag_k(\mathbf{u}')) + \left(\prod_{i \in J} u_i\right) det\left(M_J\right).$$

By induction assumption we have

$$det(M + diag(\mathbf{u}')) = det(M) + \left(\prod_{i \in J'} u_i\right) det\left(M_{J'}\right) = det(M).$$

This implies

$$det(M + diag_k(\boldsymbol{u})) = det(M) + \left(\prod_{i \in J} u_i\right) det(M_J).$$

This completes the proof. ■

# 3 Arbitrary Hull dimension

In this Section, we construct linear codes with small dimensional hull from any linear code and arbitrary dimensional hull from self-orthogonal codes. The following lemmas are used in the sequel.

**Lemma 3.1** *Let $q$ be a prime power with $q > 3$ and $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$ with $dim(hull(\mathcal{C})) = h$ and a generator matrix $G = [I_k : P]$. Let $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$ with $a_j = 1$ for any $1 \leq j \leq n$ except for one entry $a_i \neq 0, 1$ with $0 \leq i \leq k$. Then*

$$h - 1 \leq dim(Hull(\mathcal{C}_{\mathbf{a}})) \leq h + 1.$$

**Proof.** Let $G'$ be a generator matrices of $\mathcal{C}_{\mathbf{a}}$ by multiplying $j$-th column of $G$ by $a_j$ for $j \in \{1, 2, \cdots, n\}$. Let $M = GG^T$ and $\mathbf{u} \in \mathbb{F}_q^n$ be a vector of length $n$ such that $u_j = a_j^2 - 1$ for $1 \leq j \leq n$. Then $\mathbf{u}$ is a one weight and

$$rank(G'G'^T) = rank(M + diag(\mathbf{u})).$$

Since, $\mathbf{u}$ is a one weight vector then adding $diag(\mathbf{u})$ effect only one entry of $M$. Then the span of $M$ will increase or decrees by a vector. Therefore

$$rank(M) - 1 \leq rank(G'G'^T) \leq rank(M) + 1.$$

Applying Proposition 2.4, we get

$$k - dim(Hull(\mathcal{C})) - 1 \leq k - dim(Hull(\mathcal{C}_a)) \leq k - dim(Hull(\mathcal{C})) + 1.$$

This implies

$$h - 1 \leq dim(Hull(\mathcal{C}_a)) \leq h + 1.$$

This complete the proof. ■

**Lemma 3.2** *Let $q$ be a prime power with $q > 3$ and $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$ with $h$-hull. Then there exist $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$ with $a_j \neq 0$ for any $1 \leq j \leq n$ such that $dim(Hull(\mathcal{C}_{\mathbf{a}})) = h - 1$.*

**Proof.** Without loss of generality we may assume that the generator matrix of $\mathcal{C}$ is in standard form. From the proof of Theorem 2.5 [7], there exist $\mathbf{a}' = (a_1, \cdots, a_k, 1, \cdots, 1) \in \mathbb{F}_q^n$ with $a_j \neq 0$ for $0 \leq j \leq k$ and $dim(Hull(\mathcal{C}_{\mathbf{a}'})) = 0$. Let $\mathbf{a}_1 = (a_1, 1, \cdots, 1)$ and $\mathcal{C}_1 = \mathcal{C}_{\mathbf{a}_1}$, then by Lemma 3.1

$$dim(Hull(\mathcal{C}_1)) = h - 1 \quad \text{or} \quad dim(Hull(\mathcal{C}_1)) \geq h.$$

If $dim(Hull(\mathcal{C}_1)) = h - 1$, then the proof is completed. If $dim(Hull(\mathcal{C}_1)) \geq h$, let $\mathbf{a}_2 = (a_1, a_2, 1, \cdots, 1)$ and $\mathcal{C}_2 = \mathcal{C}_{1_{(1,a_2,1\cdots)}} = \mathcal{C}_{\mathbf{a}_2}$. Applying Lemma 3.1 again

$$dim(Hull(\mathcal{C}_2)) = h - 1 \quad \text{or} \quad dim(Hull(C_2)) \geq h$$

and using the same argument again. If $dim(Hull(C_{\mathbf{a}_i})) \geq h$ for all $1 \leq i \leq k$, where $\mathbf{a}_1 = (a_1, 1, \cdots, 1)$, $\mathbf{a}_2 = (a_1, a_2, 1, \cdots, 1)$, $\cdots$, $\mathbf{a}_k = (a_0, a_1, \cdots, a_k, 1, \cdots, 1) = a'$ this will contradict the existence of $a'$ with $dim(Hull(\mathcal{C}_{a'})) = 0$. Therefore, there exist $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$ with $a_j \neq 0$ for $1 \leq j \leq n$ and $dim(Hull(C_a)) = h - 1$. ■

**Theorem 3.3** *Let $q$ be a power of a prime with $q > 3$ and $\mathcal{C}$ be $[n, k, d]$-linear code over $\mathbb{F}_q$ with $dim(Hull(\mathcal{C})) = h$. Then, there exists $\mathcal{C}_j$ codes with the same parameters as $\mathcal{C}$ and*

$$dim(Hull(\mathcal{C}_j)) = h$$

*for any $0 \leq j \leq h$.*

**Proof.** We prove this theorem by induction on $j$. Obviously, the statement holds for $j = h$. Assume, by induction, that the statement holds for all $h, h-1, \cdots, j$. Let $\mathcal{C}_j$ be an $[n, k, d]$ linear code with $dim(Hull(\mathcal{C}_j)) = j$. By Lemma 3.2 there exist a monomial equivalent code $\mathcal{C}_{j-1}$ with $dim(Hull(C_{j-1})) = dim(Hull(C_j)) - 1 = j - 1$. This completes the proof. ■

**Corollary 3.4** *Let $q$ be a power of a prime with $q > 3$ and $\mathcal{C}$ be an $[n, k, d]$ self-orthogonal (self-dual) code over $\mathbb{F}_q$. Then, there exist linear codes with the same parameters as $\mathcal{C}$ with arbitrary Hull.*

**Theorem 3.5 ([2, 16])** *There exist long $q$-ary self-dual codes which meet the Gilbert-Varshamov bound for odd $q$.*

Combine Theorem 3.5 and Corollary 3.4 we get the following results.

**Theorem 3.6** *[9] Let $h$ be a fixed positive integer. There exist long $h$-hull codes which meet the Gilbert-Varshamov bound.*

Now we give a construction of maximal-entanglement EAQECCs from any linear code over $\mathbb{F}_q$ with $q > 3$. Our result significantly improve the results in [7, 9].

**Proposition 3.7 ([4])** *Let $\mathcal{C}$ be a classical $[n, k, d]$ linear code over $\mathbb{F}_q$. Then there exist $[[n, k - dim(Hull(C)), d; n - k - dim(Hull(C))]]$ EAQECCs over $\mathbb{F}_q$. Further, if $\mathcal{C}$ is MDS then the EAQECCs is also MDS.*

**Corollary 3.8** *Let $\mathcal{C}$ be an $[n,k,d]$ linear code over $\mathbb{F}_q$ with $q>3$ and $dim(Hull(\mathcal{C}))=h$. Then there exist $[[n,k-l,d;n-k-l]]_q$ EAQECCs for any $1\leq l\leq h$.*

**Example 3.9** *Let $\mathcal{C}$ be $[7,3,2]$ self-orthogonal linear code over $\mathbb{F}_5$ with the following generator matrix*

$$G=\begin{pmatrix}1&0&0&0&0&2&0\\0&1&0&2&2&0&4\\0&0&1&1&3&0&3\end{pmatrix}$$

*Let $a_0=(2,2,2,1,1,1,1)$, $a_1=(2,2,1,1,1,1,1)$ $a_2=(2,1,1,1,1,1,1)$ $a_3=(1,1,1,1,1,1,1)$. Then $\mathcal{C}_{a_i}$ are linear codes with the same parameters as $\mathcal{C}$ and*

$$dim(Hull(\mathcal{C}_{a_i}))=i,$$

*for $0\leq i\leq 3$.*

# 4 One Dimensional Hull and Pure LCD code

In Section 3 we showed that for any $h$-hull linear code and any integer $j$ with $0<j\leq h$, there exist an equivalent code $\mathcal{C}_j$ with $dim(Hull(\mathcal{C}_j))=j$. A natural question rise; is this operation invertible? For any LCD code $\mathcal{C}$ with parameters $[n,k,d]$, does a monomial equivalent code $\mathcal{C}_1$ to $\mathcal{C}$ with $dim(Hull(\mathcal{C}))=1$ exist?. It turns out that, there exist linear codes where all their monomial equivalent codes are LCD. We introduce the following definition.

**Definition 4.1** *A linear code $\mathcal{C}$ is called* ***Pure LCD*** *code if and only if all its monomial equivalent codes are LCD. i.e*

$$dim(Hull(\mathcal{C}_a))=0,\quad \text{for all } \mathbf{a}\in(\mathbb{F}_q^*)^n.$$

**Remark 4.2** *Note that the hull of a linear code over a finite field $\mathbb{F}_q$ with $q=2$ or $q=3$ is an invariant of equivalent codes. Therefore, a linear code $\mathcal{C}$ over $\mathbb{F}_q$ ($q\in\{2,3\}$) is pure LCD if and only if $\mathcal{C}$ is LCD.*

The following example shows that pure LCD code over $\mathbb{F}_q$ ($q>3$) does exist.

**Example 4.3** *Let $\mathcal{C}$ be the code over $\mathbb{F}_5$ with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 & 4 & 0 \\ 0 & 0 & 1 & 0 & 0 & 3 \end{pmatrix}.$$

*Using Magma we can check that all monomial equivalent codes to $\mathcal{C}$ are LCD codes. Hence, $\mathcal{C}$ is pure LCD code.*

**Theorem 4.4** *Let $q$ be a prime power with $q > 3$ and $\mathcal{C}$ be $[n, k, d]$ LCD code over $\mathbb{F}_q$ with generator matrix $G = [I_k : P]$. Let $M = GG^T$. Assume that there exist $1 \leq i \leq k$ with $-det(M)/det(M_{\{i\}}) + 1$ is a nonzero square, then $\mathcal{C}$ is not pure LCD code. Furthermore, let $\mathbf{a} = (a_1, \cdots, a_n)$ with $a_i^2 = -det(M)/det(M_i) + 1$ and $a_j = 1$ for all $1 \leq j \leq n$ and $j \neq i$, then $\mathcal{C}_\mathbf{a}$ is one dimensional hull.*

**Proof.** Let $G'$ be a generator matrix of $\mathcal{C}_a$ obtained from $G$ by multiplying its $i$-th column by $a_i$. Then

$$det(G'G'^T) = det(M) + (a_i^2 - 1)det(M_{\{i\}}) = 0.$$

Therefore, $\mathcal{C}_a$ is not LCD by Theorem 2.3. Furthermore

$$rank(G'G'^T) = rank(M + diag(0, \cdots, 0, a_i^2 - 1, 0, \cdots, 0)).$$

By Lemma 3.1, $rank(G'G'^T) = k$ or $= k - 1$. Since $det(G'G'^T) = 0$ then $rank(G'G'^T) = k - 1$ and $\mathcal{C}_a$ is one dimensional hull by Proposition 2.4. ■

**Remark 4.5** *Using a computer we check that most codes that are not pure LCD codes meet the requirement of Theorem 4.4. Therefore, combining Theorem 3.3 and Theorem 4.4 is very efficient for constructing one-dimensional Hull codes from any linear codes.*

**Lemma 4.6** *Let $q = 2^t$ with $t > 1$ and $\mathcal{C}$ be $[n, k]$ linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k : P]$. Let $M = GG^T$. Assume that there exist $\mathbf{u} \in \mathbb{F}_q^n$ with $u_i \in \mathbb{F}_q/\{1\}$ and*

$$det(M + diag(\mathbf{u})) = 0.$$

*Then $\mathcal{C}$ is not pure LCD code.*

**Proof.** Let $\mathbf{a} = (a_1, \cdots, a_n)$ where $a_i^2 - 1 = u_i$ for all $1 \leq i \leq n$. Then $M + diag(\mathbf{u})$ is a generator matrix of $\mathcal{C}_{\mathbf{a}}$. The rest of the proof follows from Proposition 2.4 and the fact that all non-zero element of $\mathbb{F}_q$ are square. ■

In [9], the author present a week condition on the existence of pure LCD code over $\mathbb{F}_{2^t}$. In the next theorem we give another conditions and one conjecture.

**Theorem 4.7** *Let $q = 2^t$ with $t > 1$ and let $\mathcal{C}$ be $[n, k, d]$ linear code over $\mathbb{F}_q$. Assume one of the following conditions holds*

- *$det(M_j) \neq 0$ and $det(M_j) \neq det(M)$ for some integer $1 \leq j \leq k$.*
- *There exist a subsets $J \subseteq \{1, \cdots, n\}$ with $det(M_J) \neq 0$ and $det(M_I) = 0$ for any subset $I$ of $J$ with $1 \leq I < \#J$.*

*Then, $\mathcal{C}$ is not pure LCD code and there exists $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$ with $a_j \neq 0$ for any $1 \leq j \leq n$ such that $\mathcal{C}_a$ is one dimensional hull.*

**Proof.** If $\mathcal{C}$ is not an LCD code, the result holds from Theorem 3.3. We assume that $\mathcal{C}$ is LCD code and let $G = [I_k : P]$ be its generator matrix. Let $M = GG^T$, then $det(M) \neq 0$.

**Case 1:** If $det(M_j) \neq 0$ and $det(M_j) \neq det(M)$ for some integer $1 \leq j \leq k$. The results holds from Theorem 4.4 and the fact that all element of $\mathbb{F}_q$ are squares.

**Case 2:** Note that, there exist a subsets $J \subseteq \{1, \cdots, n\}$ with $det(M_J) \neq 0$ and $det(M_I) = 0$ for any subset $I$ of $J$ with $1 \leq I < \#J$. Let $\mathbf{u} = (u_1, \cdots, u_n)$ with $u_i = 0$ for $i \notin J$. Using Lemma 2.6 we get

$$\begin{aligned} det(M + diag(\mathbf{u})) &= det(M) + \left(\prod_{i \in J} u_i\right) det(M_J) \\ &= det(M) + u_{j_1} u_{j_2} \left(\prod_{i \in J \setminus \{j_1, j_2\}} u_i\right) det(M_J). \end{aligned}$$

By choosing $u_j \in \mathbb{F}_q \setminus \{0, 1\}$ for $j \in J \setminus \{j_1, j_2\}$ and

$$u_{j_1} = \begin{cases} u_{j_2}^{-1} & \text{if } \left(\prod_{i \in J/\{j_1, j_2\}} u_i\right) \frac{det(M_J)}{det(M)} = 1, \\ \left(\prod_{i \in J/\{j_1, j_2\}} u_i\right)^2 \left(\frac{det(M_J)}{det(M)}\right)^2 & \text{otherwise.} \end{cases}$$

Because $u_i \neq 1$ for all $1 \leq i \leq n$ and $det(M + diag(\mathbf{u})) = 0$, the result holds from Lemma 4.6 and Theorem 3.3.

■

**Remark 4.8** *Theorem 4.7, give very powerful restriction on the existence of pure LCD code over $\mathbb{F}_{2^t}$. In fact, linear $[n, k]$ codes with generator matrix $GG^T = I_k$ are the only codes we found that escape this two condition and its not difficult to prove such codes are not pure LCD code. Therefore we introduce the following conjecture.*

**Conjecture 4.1** *Let $q = 2^t$ with $t > 1$ and $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. Then $\mathcal{C}$ is not pure LCD code.*

In the following theorem we shows that there exist infinitely many pure LCD codes.

**Theorem 4.9** *Let $q$ be an odd prime power. Let $\mathcal{C}$ be an $[n, k]_q$ linear code with the generator matrix $G = [I_k : I_k]$. If $-1$ is not a square in $\mathbb{F}_q$ then $\mathcal{C}$ is pure LCD code.*

**Proof.** Let $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{F}_q$ with $a_j \neq 0$ for any $1 \leq j \leq n$. Let $G'$ be the generator matrix of $\mathcal{C}_\mathbf{a}$ obtained from $G$ by multiplying its $j$-th column by $a_j$ for $j \in \{1, 2, \cdots, n\}$. Then

$$G'G'^T = \begin{pmatrix} a_1^2 + a_{k+1}^2 & & & 0 \\ & a_2^2 + a_{k+2}^2 & & \\ & & \ddots & \\ 0 & & & a_k^2 + a_{2k}^2 \end{pmatrix}.$$

Since, $-1$ is not a square in $\mathbb{F}_q$ then $a_i^2 + a_{i+k}^2 = 0$ if and only if $a_i = 0$ and $a_{i+k} = 0$. Hence $rank(G'G'^T) = k$. Therefore, by Proposition 2.4

$$dim(Hull(\mathcal{C}_a)) = 0.$$

This completes the proof. ■

# Concluding remarks

In this paper, we presented a general construction of linear code with a small dimensional hull from any linear codes. We showed that for any linear code with $h$-hull dimension, there exists an equivalent code with $h$-hull for any $0 \leq j \leq c$. In particular, for any $[n, k, d]$ self-orthogonal code there exists a code with the same parameters and with an arbitrary dimensional hull. We also introduce the notion of pure LCD code. Furthermore, we give sufficient conditions for the existence of one dimensional $[n, k, d]$ code from another code with the same parameters.

Finally, we present a family of pure LCD codes over finite fields with odd characteristics and very week conditions for the existence of pure LCD code over finite fields with even characteristics and rise a conjecture for this case. An interesting extension to this work would be to give a necessary and sufficient condition for the existence of pure LCD code over finite fields with odd characteristics.

# References


[1] Artin, E.: Geometric Algebra (Interscience Tracts in Pure and Applied Mathematics No. 3), Interscience, New York, 1957.

[2] Bassa A., Stichtenoth H., Self-dual codes better than the GilbertVarshamov bound, Des., Codes and Cryptogr. 87, 173-182, (2019).

[3] Boonniyom, K., Jitman, S.: Complementary dual subfield linear codes over finite fields. [Online]. Available: https://arxiv.org/abs/1605.06827 (2016).

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

[5] 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. Inf. Theory 64(4), 3010-3017 (2018).

[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 Transactions on Information Theory, 64(4), 3010-3017 (2018).

[7] Carlet, C., Li, C., Mesnager, S.: Linear codes with small hulls in semi-primitive case. Des. Codes Cryptogr, (87), 3063-3075 (2019).

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

[9] Chen, H. On the Hull-Variation Problem of Equivalent Linear Codes. IEEE Trans. Inf. Theory 69(5), 2911-2922 (2023).

[10] Jin L.: Construction of MDS codes with complementary duals. IEEE Trans. Inf. Theory 63(5), 2843–2847 (2017).

[11] Li, C., Zeng, P.: Constructions of linear codes with one-dimensional hull, IEEE Trans. Inf. Theory, 65(3), 1668-1676 (2019).

[12] Massey, J. L.: Linear codes with complementary duals. Discrete Mathematics, 106, 337-342 (1992).

[13] Massey J.L.: Linear codes with complementary duals. Discret. Math. 106(107), 337-342 (1992).

[14] Sendrier N.: On the dimension of the hull. SIAM J. Discret. Math. 10(2), 282–293 (1997).

[15] Sok, L.: MDS linear codes with one-dimensional hull. Cryptography and Communications, 14(5), 949-971 (2022).

[16] Stichtenoth H., Transative and self-dual codes attaining the TsafasmanVladut-Zink bound, IEEE Trans. Inf. Theory, 52(5), 2218-2224, (2006).

[17] Yan H., Liu H., Li C., Yang S.: Parameters of LCD BCH codes with two lengths. Adv. Math. Commun. 12(3), 579–594 (2018). 39.

[18] Yang X., Massey J.L.: The condition for a cyclic code to have a complementary dual. Discret. Math. 126(1-3), 391-393 (1994).