Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$

Claude Carlet[1] Sihem Mesnager[2] Chunming Tang[3] Yanfeng Qi[4] Ruud Pellikaan[5]

This work is dedicated in memory of Solomon W. Golomb
In: IEEE Transactions on Information Theory, vol. 64 (4), pp. 3010–3017, 2018

***Abstract*—Linear codes with complementary duals (abbreviated LCD) are linear codes whose intersection with their dual are trivial. When they are binary, they play an important role in armoring implementations against side-channel attacks and fault injection attacks. Non-binary LCD codes in characteristic 2 can be transformed into binary LCD codes by expansion. In this paper, we introduce a general construction of LCD codes from any linear codes. Further, we show that any linear code over $\mathbb{F}_q (q > 3)$ is equivalent to a Euclidean LCD code and any linear code over $\mathbb{F}_{q^2} (q > 2)$ is equivalent to a Hermitian LCD code. Consequently an $[n, k, d]$-linear Euclidean LCD code over $\mathbb{F}_q$ with $q > 3$ exists if there is an $[n, k, d]$-linear code over $\mathbb{F}_q$ and an $[n, k, d]$-linear Hermitian LCD code over $\mathbb{F}_{q^2}$ with $q > 2$ exists if there is an $[n, k, d]$-linear code over $\mathbb{F}_{q^2}$. Hence, when $q > 3$ (resp. $q > 2$) q-ary Euclidean (resp. q^2-ary Hermitian) LCD codes possess the same asymptotical bound as q-ary linear codes (resp. q^2-ary linear codes). This gives a direct proof that every triple of parameters $[n, k, d]$ which is attainable by linear codes over $\mathbb{F}_q$ with $q > 3$ (resp. over $\mathbb{F}_{q^2}$ with $q > 2$) is attainable by Euclidean LCD codes (resp. by Hermitian LCD codes). In particular there exist families of q-ary Euclidean LCD codes ($q > 3$) and q^2-ary Hermitian LCD codes ($q > 2$) exceeding the asymptotical Gilbert-Varshamov bound. Further, we give a second proof of these results using the theory of Gröbner bases. Finally, we present a new approach of constructing LCD codes by extending linear codes.**

***Index Terms*—Linear codes, complementary dual, LCD codes, Euclidean LCD codes, Hermitian LCD codes, Gröbner bases.**

I. Introduction

A linear complementary dual code (abbreviated LCD) is defined as a linear code $\mathcal{C}$ whose dual code $\mathcal{C}^\perp$ satisfies $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$. LCD codes have been widely applied in data storage, communications systems, consumer electronics, and cryptography. In [24], Massey showed that LCD codes provide an optimum linear coding solution for the two-user binary adder channel. Recently, Carlet and Guilley [4] investigated an interesting application of binary LCD codes against side-channel attacks (SCA) and fault injection attacks (FIA) and presented several constructions of LCD codes. They showed in particular that non-binary LCD codes in characteristic 2 can be transformed into binary LCD codes by expansion. It is then important to keep in mind that, for SCA, the most interesting case is when q is even.

LCD codes are also interesting objects in the general framework of algebraic coding. For asymptotical optimality and bounds of LCD codes, Massey [24] showed that there exist asymptotically good LCD codes. Tzeng and Hartmann [30] proved that the minimum distance of a class of LCD codes is greater than that given by the BCH bound. Sendrier [28] showed that LCD codes meet the asymptotic Gilbert-Varshamov bound using properties of the hull dimension spectrum of linear codes. Dougherty et al. [8] gave a linear programming bound on the largest size of an LCD code of given length and minimum distance. Recently, Galvez et al. [9] studied the maximum minimum distance of LCD codes of fixed length and dimension.

Many works have been devoted to the characterization and constructions of LCD codes. Yang and Massey provided in [32] a necessary and sufficient condition under which a cyclic code has a complementary dual. In [12], quasi-cyclic codes that are LCD have been characterized and studied using their concatenated structures. Criteria for complementary duality of generalized quasi-cyclic codes (GQC) bearing on the component codes are given and some explicit long GQC that are LCD, but not quasi-cyclic, have been exhibited in [11]. In [7], Dinh, Nguyend and Sriboonchitta investigated the algebraic structure of λ-constacyclic codes over finite commutative semi-simple rings. Among others, necessary and sufficient conditions for the existence of LCD, λ-constacyclic codes over such finite semi-simple rings have been provided. In [21], Li et al. constructed several families of (Euclidean) LCD cyclic codes over finite fields and analyzed their parameters. In [22] Li et al. studied two special families of LCD cyclic codes, which are both BCH codes. Mesnager et al. [26] provided a construction of algebraic geometry LCD codes which could be good candidates to be resistant against SCA. Liu and Liu constructed LCD matrix-product codes using quasi-orthogonal

This work was supported by SECODE project and the National Natural Science Foundation of China (Grant No. 11401480, 11531002, 11701129). C. Carlet was partly supported by Bergen Research Foundation. C. Tang also acknowledges support from 14E013, CXTD2014-4 and the Meritocracy Research Funds of China West Normal University. Y. Qi also acknowledges support from Zhejiang provincial Natural Science Foundation of China (LQ17A010008, LQ16A010005).

C. Carlet is with the Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, also with University of Paris XIII, CNRS, LAGA UMR 7539, Sorbonne Paris Cité, 93430 Villetaneuse, France. E-mail: claude.carlet@univ-paris8.fr

S. Mesnager is with the Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, also with University of Paris XIII, CNRS, LAGA UMR 7539, Sorbonne Paris Cité, 93430 Villetaneuse, France, and also with Telecom ParisTech 75013 Paris. E.mail: smesnager@univ-paris8.fr

C. Tang is with School of Mathematics and Information, China West Normal University, Nanchong, Sichuan, 637002, China. E-mail: tangchunmingmath@163.com

Y. Qi is with School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China. E-mail: qiyanfeng07@163.com

R. Pellikaan is with Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands. E-mail: g.r.pellikaan@tue.nl

matrices in [23]. It was also shown by Kandasamy et al. [18] that maximum rank distance codes generated by the trace-orthogonal-generator matrices are LCD codes. However, little is known on Hermitian LCD codes. More precisely, it has been proved in [12] that those codes are asymptotically good. By employing their generator matrices, Boonniyoma and Jitman gave in [2] a sufficient and necessary condition on Hermitian codes for being LCD. Li [20] constructed some cyclic Hermitian LCD codes over finite fields and analyzed their parameters.

In [16], Jin showed that some Reed-Solomon codes are equivalent to LCD codes. In [5], the authors proved that any MDS code is equivalent to an LCD code. Very recently, Jin and Xing [17] showed that an algebraic geometry code over $\mathbb{F}_{2^m}(m \geq 7)$ is equivalent to an LCD code. As a consequence, they proved that there exists a family of LCD codes which is equivalent to algebraic geometry codes exceeding the asymptotical Gilbert-Varshamov bound.

The main goal of this manuscript is to study all possible Euclidean and Hermitian LCD codes. We solve one of the fundamental problems on LCD codes, i.e., for any $[n, k, d]$ linear code over over $\mathbb{F}_q$ with $q > 3$ (resp. over $\mathbb{F}_{q^2}$ with $q > 2$), is there an $[n, k, d]$-linear Euclidean (resp. Hermitian) LCD code obtained from this given linear code? More precisely, we introduce a general construction of LCD codes from any linear codes. Further, we show that any linear code over $\mathbb{F}_q(q > 3)$ is equivalent to a Euclidean LCD code and any linear code over $\mathbb{F}_{q^2}(q > 2)$ is equivalent to a Hermitian LCD code. Consequently an $[n, k, d]$-linear Euclidean LCD code over $\mathbb{F}_q$ with $q > 3$ exists if there is an $[n, k, d]$-linear code over $\mathbb{F}_q$ and an $[n, k, d]$-linear Hermitian LCD code over $\mathbb{F}_{q^2}$ with $q > 2$ exists if there is an $[n, k, d]$-linear code over $\mathbb{F}_{q^2}$. Hence, when $q > 3$, q-ary Euclidean LCD codes are as good as q-ary linear codes and when $q > 2$, q^2-ary Hermitian LCD codes are as good as q^2-ary linear codes. In 2004, Sendrier [28] proved that LCD codes meet the asymptotic Gilbert-Varshamov bound. In 2017, Jin and Xing [17] have shown there exists a family of LCD codes that are equivalent to algebraic geometry codes and exceed the asymptotical Gilbert-Varshamov bound. Our results prove again these results in a much more direct way.

The paper is organized as follows. Section II gives preliminaries and background on Euclidean and Hermitian LCD codes. Section III considers the dimension of the hull of a binary or ternary code. In Section IV, we present some results about matrices. In Section V, we firstly provide a construction of Euclidean (resp. Hermitian) LCD codes from any linear codes and prove these main results using linear algebra and the theory of Gröbner bases, respectively. In addition, we also show one can construct LCD codes by extending linear codes.

II. Preliminaries

Throughout this paper, p is a prime and $\mathbb{F}_q$ is the finite field of order q, where $q = p^m$ for some positive integer m. The set of non-zero elements of $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^\times$. For any $x \in \mathbb{F}_{q^2}$, the conjugate of x is defined as $\overline{x} = x^q$. For a matrix A, A^T denotes the transposed matrix of matrix A, $\overline{A}$ denotes the conjugate matrix of A and $\mathrm{Rank}(A)$ denotes the rank of A. When A is a square matrix, $\det A$ denotes the determinant of A. We denote by $\#I$ the cardinality of a finite set I. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q$ with dimension k and minimum (Hamming) distance d. The value $n - k$ is called the *codimension* of $\mathcal{C}$. Given a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$), its Euclidean dual code (resp. Hermitian dual code) is denoted by $\mathcal{C}^\perp$ (resp. $\mathcal{C}^{\perp_H}$). The codes $\mathcal{C}^\perp$ and $\mathcal{C}^{\perp_H}$ are defined by

$$\mathcal{C}^\perp = \{(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_q^n : \sum_{i=0}^{n-1} b_i c_i = 0, \quad \forall (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}\},$$

$$\mathcal{C}^{\perp_H} = \{(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^n : \sum_{i=0}^{n-1} b_i \overline{c}_i = 0, \quad \forall (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}\},$$

respectively.

The minimum distance of an $[n, k, d]$ linear code is bounded by the Singleton bound

$$d \leq n + 1 - k.$$

A code meeting the above bound is called *Maximum Distance Separable* (MDS).

The Euclidean (resp. Hermitian) hull of a linear code $\mathcal{C}$ is defined to be $\mathrm{Hull}_E(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^\perp$ (resp. $\mathrm{Hull}_H(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^{\perp_H}$). Let $h_E(\mathcal{C})$ (resp. $h_H(\mathcal{C})$) be the dimension of $\mathrm{Hull}_E(\mathcal{C})$ (resp. $\mathrm{Hull}_H(\mathcal{C})$). A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is called an *LCD code* (or for short, LCD code) if $h_E(\mathcal{C}) = 0$. A linear code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is called a *Hermitian LCD code* (linear code with Hermitian complementary dual) if $h_H(\mathcal{C}) = 0$. To distinguish between classical LCD codes and Hermitian ones, we shall call *Euclidean LCD codes* in the former case. The following proposition gives a complete characterization of Euclidean and Hermitian LCD codes (see. [2], [4]).

Proposition 2.1: If G is a generator matrix for the $[n, k]$ linear code $\mathcal{C}$, then $\mathcal{C}$ is a Euclidean (resp. a Hermitian) LCD code if and only if, the $k \times k$ matrix GG^T (resp. $G\overline{G}^T$) is nonsingular.

For any prime power q, let α_q^{lin} and α_q^E denote the functions which are defined by

$$\alpha_q^{lin}(\delta) := \sup\{R \in [0, 1] : (\delta, R) \in U_q^{lin}\}, \text{for } 0 \leq \delta \leq 1,$$

and

$$\alpha_q^E(\delta) := \sup\{R \in [0, 1] : (\delta, R) \in U_q^E\}, \text{for } 0 \leq \delta \leq 1.$$

Here U_q^{lin} (resp. U_q^E) is the set of all ordered pairs $(\delta, R) \in [0, 1]^2$ for which there exists a sequence of $[n_i, k_i, d_i]$ linear code (resp. Euclidean LCD code) $\mathcal{C}_i$ over $\mathbb{F}_q$ such that $n_i \to \infty$ as $i \to \infty$ and

$$\delta = \lim_{i\to\infty} \frac{d_i}{n_i}, \quad R = \lim_{i\to\infty} \frac{k_i}{n_i}.$$

α_q^{lin} (resp. α_q^E) is the largest asymptotic information rate that can be achieved for a given asymptotic relative minimum distance δ of q-ary linear codes (resp. Euclidean LCD codes).

We can define $\alpha_{q^2}^H(\delta)$ for Hermitian LCD codes over $\mathbb{F}_{q^2}$ in a similar way. It is trivial to see that $\alpha_q^{lin}(\delta) \geq \alpha_q^E(\delta)$ and $\alpha_{q^2}^{lin}(\delta) \geq \alpha_{q^2}^H(\delta)$.

A classical lower bound for α_q^{lin} is the asymptotical Gilbert-Varshamov (GV) bound [25].

Proposition 2.2: For any prime power q, we have

$$\alpha_q^{lin} \geq R_{GV}(\delta) = 1 - H_q(\delta), \text{ for } 0 < \delta < \frac{q-1}{q},$$

where $H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$ is the q-ary entropy function.

The following TVZ bound, which is better than Gilbert-Varshamov bound, was established in [31] by using algebraic-geometry codes.

Proposition 2.3: Let q be a prime power. Then,

$$\alpha_q^{lin}(\delta) \geq 1 - \delta - \frac{1}{A(q)}, \text{ for } \delta \in [0,1],$$

where $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$ and $N_q(g)$ denotes the maximum number of rational places that a global function field of genus g with full constant field $\mathbb{F}_q$ can have.

It was proved that LCD codes can also attain the asymptotical GV bound in [28], i.e. $\alpha_q^E(\delta) \geq R_{GV}(\delta)$.

Very recently, Jin and Xing [17] proved that $\alpha_q^E(\delta)$ has bound better than the GV bound in some special cases by using algebraic-geometry codes. They proved the following result.

Proposition 2.4: When $q \geq 128$ is a power of 2, then $\alpha_q^E(\delta)$ exceeds the asymptotic Gilbert-Varshamov bound in two intervals of $[0,1]$.

In this paper, we will prove that for any prime power q with $q > 3$ and $\delta \in [0,1]$, $\alpha_q^E(\delta) = \alpha_q^{lin}(\delta)$ holds. Hence, any lower bound of $\alpha_q^{lin}(\delta)$ is also a lower bound of $\alpha_q^E(\delta)$.

For any $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and permutation σ of $\{1, 2, \ldots, n\}$, we define $\mathcal{C}_\mathbf{a}$ and $\sigma(\mathcal{C})$ as the following linear codes

$$\mathcal{C}_\mathbf{a} = \{(a_1c_1, \ldots, a_nc_n) : (c_1, \ldots, c_n) \in \mathcal{C}\},$$

and

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

Two codes $\mathcal{C}$ and $\mathcal{C}'$ in $\mathbb{F}_q^n$ are called *equivalent* if $\mathcal{C}' = \sigma(\mathcal{C}_\mathbf{a})$ for some permutation σ of $\{1, 2, \ldots, n\}$ and $\mathbf{a} \in (\mathbb{F}_q^*)^n$. Any $[n,k]$ linear code over a finite field is equivalent to a code generated by a matrix of the form $[I_k : P]$ where I_k denotes the $k \times k$ identity matrix.

III. The dimension of the hull of a code

The method of this paper applies only to finite fields of size $q > 3$, since the dimension of $\mathrm{Hull}_E(\mathcal{C})$ is an invariant of equivalent codes, in case $q = 2$ and $q = 3$, where it can be expressed in terms of the Tutte polynomial of the matroid of $\mathcal{C}$.

Let $M(\mathcal{C})$ be the matroid of the code $\mathcal{C}$ and $t_{M(\mathcal{C})}(X,Y)$ the two variable Tutte polynomial of the matroid.

For a binary code $\mathcal{C}$ we have:

$$|t_{M(\mathcal{C})}(-1,-1)| = 2^{\dim(\mathrm{Hull}_E(\mathcal{C}))}.$$

See [27] for graph codes and [3, Proposition 6.5.4] for arbitrary codes.

For a ternary code $\mathcal{C}$ we have [14]:

$$|t_{M(\mathcal{C})}(j,j^2)| = (\sqrt{3})^{\dim(\mathrm{Hull}_E(\mathcal{C}))},$$

where $j = e^{2\pi i/3}$ is a primitive third root of unity of the complex numbers and $|z|$ is the modulus of the complex number z.

$W_\mathcal{C}(X,Y)$, the weight enumerator of an $\mathbb{F}_q$-linear code $\mathcal{C}$ can be expressed in terms of $t_{M(\mathcal{C})}(X,Y)$ as follows:

$$W_\mathcal{C}(X,Y) = (X-Y)^k Y^{n-k}\ t_\mathcal{C}\left(\frac{X+(q-1)Y}{X-Y}, \frac{X}{Y}\right).$$

See Greene [10]. But the converse is not true.

Example 3.1: The dimension of the hull of a binary code $\mathcal{C}$ cannot be expressed in terms of $W_\mathcal{C}(X,Y)$. Consider the two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of [29, Example 1] with generator matrices $G_1 = (I_3|I_3)$ and $G_2 = (I_3|J_3)$, where J_3 is the 3×3 all ones matrix. Both have the same weight enumerator:

$$W_{\mathcal{C}_1}(X,Y) = W_{\mathcal{C}_2}(X,Y) = X^6 + 3X^4Y^2 + 3X^2Y^4 + Y^6.$$

Furthermore $\mathcal{C}_1$ is self dual, so $\dim(\mathrm{Hull}_E(\mathcal{C}_1)) = 3$. But $\mathrm{Hull}_E(\mathcal{C}_2)$ is generated by the all ones vector, so $\dim(\mathrm{Hull}_E(\mathcal{C}_2)) = 1$.

Remark 3.2: Let $t_\mathcal{C}(X,Y) = t_{M(\mathcal{C})}(X,Y)$. Then $t_\mathcal{C}(X,Y)$ can be expressed in $W_\mathcal{C}(X,Y,T)$, the extended weight enumerator of $\mathcal{C}$ and vice versa. See [15, Theorems 5.9 and 5.10].

$$W_\mathcal{C}(X,Y,T) = (X-Y)^k Y^{n-k}\ t_\mathcal{C}\left(\frac{X+(T-1)Y}{X-Y}, \frac{X}{Y}\right).$$

$$t_\mathcal{C}(X,Y) = Y^n(Y-1)^{-k} W_\mathcal{C}(1, Y^{-1}, (X-1)(Y-1)).$$

So we have in the binary case

$$|W_\mathcal{C}(1,-1,4)| = 2^k |t_\mathcal{C}(-1,-1)| = 2^{k+h}.$$

where k and h are the dimensions of $\mathcal{C}$ and $\mathrm{Hull}_E(\mathcal{C})$, respectively.

Example 3.3: Notice that $W_\mathcal{C}(X,Y,T) - X^n$ is divisible by $T-1$. Define $\bar{W}_\mathcal{C}(X,Y,T) = (W_\mathcal{C}(X,Y,T) - X^n)/(T-1)$. In the previous Example 3.1 we have that

$$\bar{W}_{\mathcal{C}_1}(X,Y,T) = 3X^4Y^2 + 3(T-1)X^2Y^4 + (T-1)^2Y^6$$

So $W_{\mathcal{C}_1}(1,-1,4) = 2^6$. And $\bar{W}_{\mathcal{C}_2}(X,Y,T)$ is equal to

$$3X^4Y^2 + (T-2)X^3Y^3 + 3X^2Y^4 + 3(T-2)XY^5 + (T^2-3T+3)Y^6.$$

So $W_{\mathcal{C}_2}(1,-1,4) = 2^4$.

Remark 3.4: For the ternary case we have

$$t_\mathcal{C}(j,j^2) = j^{2n}(j^2-1)^{-k} W_\mathcal{C}(1,j),$$

since $j^{-2} = j$ and $(j-1)(j^2-1) = 3$. So the dimension of the hull of a ternary code $\mathcal{C}$ can be expressed in terms of $W_\mathcal{C}(X,Y)$. Furthermore

$$W_\mathcal{C}(1,j) = a_0 + a_1 j + a_2 j^2,$$

where $a_0 = \sum_{i=0}^{n/3} A_{3i}$, $a_1 = \sum_{i=0}^{n/3} A_{3i+1}$ and $a_2 = \sum_{i=0}^{n/3} A_{3i+2}$.

IV. Some results on matrices

Let l and j be two integers with $0 \leq j \leq l$ and $l \geq 1$. Let M be an $l \times l$ matrix over $\mathbb{F}_q$. Let $\mathbf{u}$ be a word in $\mathbb{F}_q^l$ of Hamming weight j and $I = \{i_1, \ldots, i_j\}$ its support. Denote by $diag_l[\mathbf{u}]$ the diagonal $l \times l$ matrix whose elements on the diagonal are $u_1, \ldots, u_l$. Define M_I the submatrix of M obtained by deleting the $i_1, \ldots, i_j$-th rows and columns of M. Denote $M_I = 1$ if $I = \{1, 2, \ldots, l\}$ and $M_\emptyset = M$.

Lemma 4.1: Let M be an $l \times l$ matrix over $\mathbb{F}_q$ and t an integer with $0 \leq t \leq l-1$. Suppose that $\det(M_I) = 0$ holds for any subset I of $\{1, 2, \ldots, l\}$ with $0 \leq \#I \leq t$. Then, for any $1 \leq j \leq t+1$ and every word $\mathbf{u}$ of Hamming weight j, denoting its support by J, we have:

$$\det(M + diag_l[\mathbf{u}]) = \Big(\prod_{i \in J} u_i\Big) \det(M_J). \tag{1}$$

Proof: We will prove this statement by induction on t. We first prove that the statement holds if $t = 0$. In this case, $\det(M) = 0$. Then, for any $\mathbf{u}$ of Hamming weight 1, denoting by i_1 the position of its only nonzero coordinate, we have:

$$\begin{aligned}\det(M + diag_l[\mathbf{u}]) =& \det(M) + u_{i_1} \det(M_{\{i_1\}}) \\ =& u_{i_1} \det(M_{\{i_1\}}).\end{aligned}$$

Thus, the statement holds if $t = 0$. In the following, suppose the statement holds for $t = 0, 1, 2, \ldots, s$. We will prove that the statement holds for $t = s+1$. We only need to check the property for a word $\mathbf{u}$ of Hamming weight $s+2$. Let the support of $\mathbf{u}$ be $J = \{i_1, \ldots, i_{s+2}\}$. Note that if $\mathbf{u}'$ is the word obtained from $\mathbf{u}$ by changing $u_{i_{s+2}}$ into 0 and $\mathbf{u}''$ is the word by deleting the i_{s+2} component of $\mathbf{u}$, we have:

$$\det(M + diag_l[\mathbf{u}']) = 0$$

and

$$\begin{aligned}\det(M + diag_l[\mathbf{u}]) =& \det(M + diag_l[\mathbf{u}']) \\ &+ u_{i_{s+2}} \det(M_{\{i_{s+2}\}} + diag_{l-1}[\mathbf{u}'']) \\ =& u_{i_{s+2}} \det(M_{\{i_{s+2}\}} + diag_{l-1}[\mathbf{u}'']) \\ =& u_{i_1} u_{i_2} \cdots u_{i_{s+2}} \det(M_{\{i_1, i_2, \ldots, i_{s+2}\}}).\end{aligned}$$

Thus, the Equation (1) holds for $j = s+2$. When $1 \leq j \leq s+1$, the Equation (1) holds from the inductive assumption. This completes the proof. ∎

For any matrix M, $\mathrm{Row}(M)$ (resp. $\mathrm{Col}(M)$) denotes the vector space spanned by the rows (resp. columns) of M. Then, $\dim(\mathrm{Row}(M)) = \dim(\mathrm{Col}(M))$ and denote it by $\mathrm{Rank}(M)$, which is called the rank of M. For $\mathbf{v}^i \in \mathbb{F}^k$ ($i \in \{1, 2, \ldots, n\}$), $\mathrm{Span}\{\mathbf{v}^1, \ldots, \mathbf{v}^n\}$ denotes the vector space spanned by $\mathbf{v}^1, \ldots, \mathbf{v}^n$.

Lemma 4.2: Given a matrix G with k rows and n columns, one has $\mathrm{Rank}(GG^T) \leq \mathrm{Rank}(G)$.

Proof: Let $\mathbf{g}^1, \ldots, \mathbf{g}^n$ be the columns vectors of G. Then $GG^T = \sum_{i=1}^n \mathbf{g}^i (\mathbf{g}^i)^T$. By $\mathrm{Col}(\mathbf{g}^i(\mathbf{g}^i)^T) = \mathrm{Span}\{\mathbf{g}^i\}$, $\mathrm{Col}(GG^T) \subseteq \mathrm{Span}\{\mathbf{g}^i : i \in \{1, \ldots, n\}\}$. The result follows from linear algebra. ∎

V. Construction of LCD codes from any linear code

A. Construction of LCD codes which are equivalent to the original one

Let $\mathcal{C}$ be an $[n, k, d]$-linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k : P]$. For any $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, we define $\mathcal{C}_\mathbf{a}$ as the following linear code

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

Theorem 5.1: Let q be a power of a prime and let $\mathcal{C}$ be an $[n, k, d]$-linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k : P]$. Let $M = GG^T$. Let $t \leq k-1$ be a non-negative integer such that $\det(M_I) = 0$ for any subset of $\{1, 2, \ldots, k\}$ with $0 \leq \#I \leq t$ and suppose there exists $J \subseteq \{1, \ldots, k\}$ of size $t+1$ such that $\det(M_J) \neq 0$. Let $\mathbf{a}$ be any word of length n such that $a_j \in \mathbb{F}_q \setminus \{1, -1\}$ for $j \in J$ and $a_j \in \{1, -1\}$ for $j \in \{1, \ldots, n\} \setminus J$, then $\mathcal{C}_\mathbf{a}$ is a Euclidean LCD $[n, k]$-linear code. Furthermore, if $a_j \neq 0$, then $\mathcal{C}_\mathbf{a}$ is a Euclidean LCD $[n, k, d]$-linear code.

Proof: Let G' be the generator matrix of $\mathcal{C}_\mathbf{a}$ obtained from G by multiplying its j-th column by a_j for $j \in \{1, 2, \ldots, n\}$ and let $\mathbf{u}$ be the word of length n and support J such that $u_j = a_j^2 - 1$ for $1 \leq j \leq k$. Then, $G'G'^T = M + diag_k[\mathbf{u}]$. From Lemma 4.1,

$$\begin{aligned}\det(G'G'^T) =& \det(M + diag_k[\mathbf{u}]) \\ =& \Big(\prod_{j \in J} u_j\Big) \det(M_J) \neq 0.\end{aligned}$$

By Proposition 2.1, $\mathcal{C}_\mathbf{a}$ is a Euclidean LCD code. ∎

Proposition 5.2: Let q be a power of a prime and let $\mathcal{C}$ be an $[n, k, d]$-linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k : P]$. Let $M = GG^T$. Let $t \leq k-1$ be a non-negative integer such that $\det(M_I) = 0$ for any subset I of $\{1, 2, \ldots, k\}$ with $0 \leq \#I \leq t$ and suppose there exists $J \subseteq \{1, \ldots, k\}$ of size $t+1$ such that $\det(M_J) \neq 0$. Then, $t \geq h_E(\mathcal{C}) - 1$.

Proof: Let $J \subseteq \{1, \ldots, k\}$ be any size $t+1$ such that $\det(M_J) \neq 0$. Let $\mathcal{C}_1 := \mathrm{Span}\{\mathbf{b}_j : j \in \{1, 2, \ldots, n\} \setminus J\}$, where $\mathbf{b}_j$ is the j-row of G and G_1 is obtained from G by deleting the j-row of G for $j \in J$. Then, G_1 is a generator matrix of $\mathcal{C}_1$ and $\det(G_1 G_1^T) = \det(M_J) \neq 0$. Thus, $\mathcal{C}_1$ is an LCD code.

Suppose that $1 \leq t+1 < h_E(\mathcal{C})$. Then, $\dim(\mathcal{C}_1) + \dim(\mathrm{Hull}_E(\mathcal{C})) = k - (t+1) + h_E(\mathcal{C}) \geq k+1 > \dim(\mathcal{C})$. From $\mathcal{C}_1 \subseteq \mathcal{C}$ and $\mathrm{Hull}_E(\mathcal{C}) \subseteq \mathcal{C}$, $\mathcal{C}_1 \cap \mathrm{Hull}_E(\mathcal{C}) \neq \{\mathbf{0}\}$. Choose any $\mathbf{c} \in \mathcal{C}_1 \cap \mathrm{Hull}_E(\mathcal{C})$. It's easy to observe that $\mathbf{c} \in \mathcal{C}_1 \cap \mathcal{C}_1^\perp$, which contradicts with $\mathcal{C}$ being LCD. ∎

Corollary 5.3: 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 $\mathbf{a} \in (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_j \neq 0$ for any $1 \leq j \leq n$ such that $\mathcal{C}_\mathbf{a}$ is a Euclidean LCD code.

Proof: If $\mathcal{C}$ is a Euclidean LCD code, the result holds by choosing $\mathbf{a} = (1, 1, \ldots, 1)$.

If $\mathcal{C}$ is not a Euclidean LCD code, then $\det(GG^T) = 0$. Let $M = GG^T$. Then there exists a non-negative integer t and a subset J of $\{1, 2, \ldots, k\}$ with $\#J = t+1$ such that

$\det(M_I) = 0$ for any subset of $\{1, 2, \ldots, k\}$ with $0 \leq \#I \leq t$ and $\det(M_J) \neq 0$. Since $q > 3$, $\mathbb{F}_q^* \setminus \{1, -1\} \neq \emptyset$. Thus, one can choose $\mathbf{a} \in \mathbb{F}_q^n$ with $a_j \in \mathbb{F}_q^* \setminus \{-1, 1\}$ for $j \in J$ and $a_j = 1$ for $j \in \{1, \ldots, n\} \setminus J$. From Theorem 5.1, $\mathcal{C}_{\mathbf{a}}$ is a Euclidean LCD code. ∎

Corollary 5.4: Let q be a power of a prime with $q > 3$. Then, an $[n, k, d]$-linear Euclidean LCD code over $\mathbb{F}_q$ exists if there is an $[n, k, d]$-linear code over $\mathbb{F}_q$.

Corollary 5.5: Let q be a power of a prime with $q > 3$. Then, $\alpha_q^E(\delta) = \alpha_q^{lin}(\delta)$ for any $\delta \in [0, 1]$. In particular,

$$\alpha_q^E(\delta) \geq 1 - \delta - \frac{1}{A(q)}, \text{ for } \delta \in [0, 1],$$

where $A(q)$ is defined as in Proposition 2.3.

Theorem 5.6: Let q be a power of a prime, let $\mathcal{C}$ be an $[n, k, d]$-linear code over $\mathbb{F}_{q^2}$ with generator matrix $G = [I_k : P]$ and $M = GG^T$. Suppose $t \leq k-1$ is a non-negative integer such that $\det(M_I) = 0$ for any subset I of $\{1, 2, \ldots, k\}$ with $0 \leq \#I \leq t$ and there exists $J \subseteq \{1, \ldots, k\}$ of size $t + 1$ such that $\det(M_J) \neq 0$. Let $\mathbf{a}$ be any word of length n such that $a_j \in \mathbb{F}_{q^2} \setminus (\mathbb{F}_{q^2}^*)^{q-1}$ for $j \in J$ and $a_j \in (\mathbb{F}_{q^2}^*)^{q-1}$ for $j \in \{1, \ldots, n\} \setminus J$, then $\mathcal{C}_{\mathbf{a}}$ is an $[n, k]$-linear code with Hermitian complementary dual. Furthermore, if $a_j \neq 0$, then $\mathcal{C}_{\mathbf{a}}$ is an $[n, k, d]$-linear code with Hermitian complementary dual.

Proof: Let G' be the generator matrix of $\mathcal{C}_{\mathbf{a}}$ obtained from G by multiplying its j-th column by a_j for $j \in \{1, 2, \ldots, n\}$ and let $\mathbf{u}$ be the word of length n and support J such that $u_j = a_j^{q+1} - 1$ for $1 \leq j \leq k$. Then, $G'\overline{G'}^T = M + diag_k[\mathbf{u}]$. From Lemma 4.1,

$$\begin{aligned}\det(G'\overline{G'}^T) &= \det(M + diag_k[\mathbf{u}]) \\ &= \Big(\prod_{j \in J} u_j\Big) \det(M_J) \neq 0.\end{aligned}$$

By Proposition 2.1, $\mathcal{C}_{\mathbf{a}}$ is a Hermitian LCD code. ∎

Proposition 5.7: Let q be a power of a prime and let $\mathcal{C}$ be an $[n, k, d]$-linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k : P]$. Let $M = G\overline{G}^T$. Let $t \leq k - 1$ be a non-negative integer such that $\det(M_I) = 0$ for any subset of $\{1, 2, \ldots, k\}$ with $0 \leq \#I \leq t$ and suppose there exists $J \subseteq \{1, \ldots, k\}$ of size $t + 1$ such that $\det(M_J) \neq 0$. Then, $t \geq h_H(\mathcal{C}) - 1$.

Proof: Let $J \subseteq \{1, \ldots, k\}$ be any size $t + 1$ such that $\det(M_J) \neq 0$. Let $\mathcal{C}_1 := \text{Span}\{\mathbf{b}_j : j \in \{1, 2, \ldots, n\} \setminus J\}$, where $\mathbf{b}_j$ is the j-row of G and G_1 is obtained from G by deleting the j-row of G for $j \in J$. Then, G_1 is a generator matrix of $\mathcal{C}_1$ and $\det(G_1\overline{G}_1^T) = \det(M_J) \neq 0$. Thus, $\mathcal{C}_1$ is a Hermitian LCD code.
Suppose that $1 \leq t + 1 < h_H(\mathcal{C})$. Then, $\dim(\mathcal{C}_1) + \dim(\text{Hull}_H(\mathcal{C})) = k-(t+1)+h_H(\mathcal{C}) \geq k+1 > \dim(\mathcal{C})$. From $\mathcal{C}_1 \subseteq \mathcal{C}$ and $\text{Hull}_H(\mathcal{C}) \subseteq \mathcal{C}$, $\mathcal{C}_1 \cap \text{Hull}_H(\mathcal{C}) \neq \{\mathbf{0}\}$. Choose any $\mathbf{c} \in \mathcal{C}_1 \cap \text{Hull}_H(\mathcal{C})$. It's easy to observe that $\mathbf{c} \in \mathcal{C}_1 \cap \mathcal{C}_1^{\perp_H}$, which contradicts with $\mathcal{C}$ being Hermitian LCD. ∎

Corollary 5.8: Let q be a power of a prime with $q > 2$ and $\mathcal{C}$ be an $[n, k, d]$-linear code over $\mathbb{F}_{q^2}$. Then, there exists $\mathbf{a} \in (a_1, \ldots, a_n) \in \mathbb{F}_{q^2}^n$ with $a_j \neq 0$ for any $1 \leq j \leq n$ such that $\mathcal{C}_{\mathbf{a}}$ is a Hermitian LCD code.

Proof: If $\mathcal{C}$ is a Hermitian LCD code, the result holds by choosing $\mathbf{a} = (1, 1, \ldots, 1)$.
If $\mathcal{C}$ is not a Hermitian LCD code, then $\det(G\overline{G}^T) = 0$. Let $M = G\overline{G}^T$. Then there exists a non-negative integer t and a subset J of $\{1, 2, \ldots, k\}$ with $\#J = t + 1$ such that $\det(M_I) = 0$ for any subset of $\{1, 2, \ldots, k\}$ with $0 \leq \#I \leq t$ and $\det(M_J) \neq 0$. Since $q > 2$, $\mathbb{F}_{q^2} \setminus \mathbb{F}_{q^2}^{q-1} \neq \emptyset$. Thus, one can choose $\mathbf{a} \in \mathbb{F}_{q^2}^n$ with $a_j \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q^2}^{q-1}$ for $j \in J$ and $a_j = 1$ for $j \in \{1, \ldots, n\} \setminus J$. From Theorem 5.6, $\mathcal{C}_{\mathbf{a}}$ is a Hermitian LCD code. ∎

Corollary 5.9: Let q be a power of a prime with $q > 2$. Then, an $[n, k, d]$-linear Hermitian LCD code over $\mathbb{F}_{q^2}$ exists if there is an $[n, k, d]$-linear code over $\mathbb{F}_{q^2}$.

Corollary 5.10: Let q be a power of a prime with $q > 2$. Then, $\alpha_{q^2}^H(\delta) = \alpha_{q^2}^{lin}(\delta)$ for any $\delta \in [0, 1]$. In particular,

$$\alpha_{q^2}^H(\delta) \geq 1 - \delta - \frac{1}{A(q^2)}, \text{ for } \delta \in [0, 1],$$

where $A(q^2)$ is defined as in Proposition 2.3.

B. A second proof using Gröbner bases

In this section we will give another proof of the Corollaries 5.3 and 5.8 using the theory of Gröbner bases.

The multivariate notation is used for polynomials, that means that X is an abbreviation of $(X_1, \ldots, X_n)$ and the polynomial $f(X)$ of $f(X_1, \ldots, X_n)$. We need a refinement of the well-known property that if $f(X)$ is a nonzero polynomial of $\mathbb{F}_q[X_1, \ldots, X_n]$ such that the degree of $f(X)$ with respect to X_j is at most $q-1$ for all j, then there exists $\mathbf{a} \in \mathbb{F}_q^n$ such that $f(\mathbf{a}) \neq 0$. See [19, V, §4, Theorem 5].

Proposition 5.11: Let $f(X)$ be a nonzero polynomial of $\mathbb{F}_q[X_1, \ldots, X_n]$ such that the degree of $f(X)$ with respect to X_j is at most $q-2$ for all j. Then there exists $\mathbf{a} \in (\mathbb{F}_q \setminus \{0\})^n$ such that $f(\mathbf{a}) \neq 0$.

Proof: For the theory of Gröbner bases and the concepts of a footprint and delta set we refer to [1], [6], [13].
Let $f(X)$ be a nonzero polynomial of $\mathbb{F}_q[X_1, \ldots, X_n]$ such that the degree of $f(X)$ with respect to X_j is at most $q - 2$ for all j.
Consider the ideal $I_{q,n}$ in $\mathbb{F}_q[X_1, \ldots, X_n]$ generated by the $X_j^{q-1} - 1$, $j = 1, \ldots, n$. Then $(\mathbb{F}_q \setminus \{0\})^n$ is the zero set of $I_{q,n}$, and $I_{q,n}$ is the vanishing ideal of $(\mathbb{F}_q \setminus \{0\})^n$. The footprint or delta set of the $X_j^{q-1} - 1$, $j = 1, \ldots, n$ is equal to $(\{0, 1, \ldots, q-2\})^n$ and contains the delta set of the ideal of $I_{q,n}$. The delta set of $I_{q,n}$ is finite and has size $(q-1)^n$, the size of the zero set of $I_{q,n}$ and it is equal to the size of delta set of the $X_j^{q-1} - 1$, $j = 1, \ldots, n$. Hence the delta set of $I_{q,n}$ is equal to $(\{0, 1, \ldots, q-2\})^n$ and $\{X_j^{q-1} - 1 | j = 1, \ldots, n\}$ is a Gröbner basis of $I_{q,n}$ with respect to the total degree lex order.
Now $f(X)$ is a nonzero element of $\mathbb{F}_q[X_1, \ldots, X_n]$. The exponent of the leading monomial of $f(X)$ is in the delta set of $I_{q,n}$, since the degree of $f(X)$ with respect to X_j is at most $q - 2$ for all j. Therefore $f(X) \notin I_{q,n}$.
Suppose that $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in (\mathbb{F}_q \setminus \{0\})^n$. Then $f(X)$ is in the vanishing ideal of $(\mathbb{F}_q \setminus \{0\})^n$, which is $I_{q,n}$. So

$f(X) \in I_{q,n}$. This is a contradiction.
Therefore there exists $\mathbf{a} \in (\mathbb{F}_q \setminus \{0\})^n$ such that $f(\mathbf{a}) \neq 0$. ■

Proof: Now we give another proof of Corollary 5.3. Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear code with $q \geq 4$.
Without loss of generality we may assume that $\mathcal{C}$ has a generator matrix of the form $G = [I_k : B]$. Let $\mathbf{a} = (a_1, \ldots, a_k)$ be an k-tuple of nonzero elements of $\mathbb{F}_q$. Let $D(\mathbf{a})$ be the diagonal matrix with $\mathbf{a}$ on its diagonal. Let $[D(\mathbf{a}) : B]$ be the generator matrix of the code $\mathcal{C}_{\mathbf{a}}$. Then $\mathcal{C}_{\mathbf{a}}$ is monomial equivalent with $\mathcal{C}$. Let $X = (X_1, \ldots, X_k)$. Now define

$$f(X) = \det([D(\mathbf{a}) : B]\,[D(\mathbf{a}) : B]^T).$$

Then

$$f(X) = \det(D(X_1^2, \ldots, X_k^2) + BB^T).$$

Hence $f(X)$ is a polynomial in the variables $X_1, \ldots, X_k$ and the degree of $f(X)$ with respect to X_i is 2 for all i, which is at most $q-2$, since $q \geq 4$. The leading term of $f(X)$ with respect to the total degree lex order is $X_1^2 \cdots X_k^2$. So $f(X)$ is a nonzero polynomial. Therefore $f(\mathbf{a}) \neq 0$ for some $\mathbf{a} \in (\mathbb{F}_q \setminus \{0\})^k$ by Proposition 5.11.
Hence $\mathcal{C}_{\mathbf{a}}$ is an LCD code for this choice of $\mathbf{a}$ by Proposition 2.1. ■

Proof: Now we give another proof of Corollary 5.8 similar to the previous proof. Let C be an $\mathbb{F}_{q^2}$-linear code with $q > 2$.
Without loss of generality we may assume that C has a generator matrix of the form $G = [I_k : B]$. Let $\mathbf{a} = (a_1, \ldots, a_k)$ be an k-tuple of nonzero elements of $\mathbb{F}_{q^2}$. Let $D(\mathbf{a})$ be the diagonal matrix with $\mathbf{a}$ on its diagonal. Let $[D(\mathbf{a}) : B]$ be the generator matrix of the code $C_{\mathbf{a}}$. Then $C_{\mathbf{a}}$ is monomial equivalent with C. Let $X = (X_1, \ldots, X_k)$. Now define

$$g(X) = \det([D(\mathbf{a}) : B]\,\left[D(X^q) : \bar{B}\right]^T).$$

Then

$$g(X) = \det(D(X_1^{q+1}, \ldots, X_k^{q+1}) + B\bar{B}^T).$$

Hence $g(X)$ is a polynomial in the variables $X_1, \ldots, X_k$ and the degree of $g(X)$ with respect to X_i is $q+1$ for all i, which is at most q^2-2, since $q > 2$. The leading term of $f(X)$ with respect to the total degree lex order is $X_1^{q+1} \cdots X_k^{q+1}$. So $f(X)$ is a nonzero polynomial. Therefore $f(\mathbf{a}) \neq 0$ for some $\mathbf{a} \in (\mathbb{F}_{q^2} \setminus \{0\})^k$ by Proposition 5.11 applied to the field $\mathbb{F}_{q^2}$.
Hence $C_{\mathbf{a}}$ is a Hermitian LCD code for this choice of $\mathbf{a}$ by Proposition 2.1. ■

C. Construction of LCD codes by extending linear codes

Lemma 5.12: Let $\mathcal{C}$ be an $[n,k]$-linear over $\mathbb{F}_q$ with $h := h_E(\mathcal{C}) > 0$. Let $\{\mathbf{c}^i\}_{i=1}^k$ be a basis of $\mathcal{C}$ such that $\{\mathbf{c}^i\}_{i=1}^h$ is a basis of $\mathrm{Hull}_E(\mathcal{C})$. Then $\mathrm{Span}\{\mathbf{c}^i : i = h+1, h+2, \ldots, k\}$ is a Euclidean LCD code.

Proof: Let $\mathcal{C}_1 = \mathrm{Span}\{\mathbf{c}^i : i = h+1, h+2, \ldots, k\}$ and $\mathbf{c} \in \mathcal{C}_1 \cap \mathcal{C}_1^{\perp}$. Then, for any $\mathbf{c}' = (c_1', \ldots, c_n') \in \mathcal{C}_1$ and $\mathbf{c}'' = (c_1'', \ldots, c_n'') \in \mathrm{Hull}_E(\mathcal{C})$, $\sum_{i=1}^n c_i c_i' = 0$ and $\sum_{i=1}^n c_i c_i'' = 0$. Thus, $\mathbf{c} \in \mathcal{C}^{\perp}$. Hence, $\mathbf{c} = 0$ from $\mathcal{C}_1 \cap \mathcal{C}^{\perp} = \{\mathbf{0}\}$. It completes the proof of this lemma. ■

Let $\mathcal{C}$ be a linear code and t be a positive integer. $L = (l_1, \ldots, l_t)$ denotes a linear transform from $\mathcal{C}$ to $\mathbb{F}_q^t$ defined by

$$\mathbf{c} \longmapsto (l_1(\mathbf{c}), \ldots, l_t(\mathbf{c})), \text{ for } \mathbf{c} \in \mathcal{C},$$

where l_i is any linear form over $\mathcal{C}$ for $i \in \{1, 2, \ldots, t\}$. Define

$$\mathcal{C}_L := \{(\mathbf{c}, l_1(\mathbf{c}), \ldots, l_t(\mathbf{c})) : \mathbf{c} \in \mathcal{C}\}. \tag{2}$$

Let $\mathrm{Ker}(L) := \{\mathbf{c} \in \mathcal{C} : L(\mathbf{c}) = 0\}$, $\mathrm{Im}(L) := \{L(\mathbf{c}) : \mathbf{c} \in \mathcal{C}\}$ and $\mathrm{Rank}(L) := \dim(\mathrm{Im}(L))$.
In the following statement, we give a sufficient condition such that the code $\mathcal{C}_L$ does not give rise to a Euclidean LCD code.

Theorem 5.13: Let $\mathcal{C}$ be an $[n,k]$-linear over $\mathbb{F}_q$ with $h := h_E(\mathcal{C}) > 0$ and L be a linear transform from $\mathcal{C}$ to $\mathbb{F}_q^t$ such that $\mathcal{C} = \mathrm{Ker}(L) \oplus \mathrm{Hull}(\mathcal{C})$. If $\mathrm{Rank}(L) < h$, then $\mathcal{C}_L$ (defined by Equation (2)) is not a Euclidean LCD code.

Proof: From $\mathcal{C} = \mathrm{Ker}(L) \oplus \mathrm{Hull}(\mathcal{C})$, there is a basis $\{\mathbf{c}^i\}_{i=1}^k$ of $\mathcal{C}$ such that $\{\mathbf{c}^i\}_{i=1}^h$ is a basis of $\mathrm{Hull}_E(\mathcal{C})$ and $\{\mathbf{c}^i\}_{i=h+1}^k$ is a basis of $\mathrm{Ker}(L)$. Let G be the generator of $\mathcal{C}$ with the i-th row being $\mathbf{c}^i$ and $M = GG^T$. Let G_1 be the generator of $\mathcal{C}_1 := \mathrm{Span}\{\mathbf{c}^i : i = h+1, h+2, \ldots, k\}$ with the i-th row being $\mathbf{c}^{h+i}$ and $M_{k-h,k-h} = G_1 G_1^T$. Then, M has the form

$$M = \begin{bmatrix} 0_{h,h} & 0_{h,k-h} \\ 0_{k-h,h} & M_{k-h,k-h} \end{bmatrix},$$

where $0_{*,*}$ is the matrix with all entries being 0.

Let G_2 be the matrix with the i-th row being $(l_1(\mathbf{c}^i), \ldots, l_t(\mathbf{c}^i))$ for $i \in \{1, \ldots, h\}$ and $M_2 = G_2 G_2^T$. Then G_2 is a generator matrix of $\mathcal{C}_L$. Then,

$$M = \begin{bmatrix} 0_{h,h} + M_2 & 0_{h,k-h} \\ 0_{k-h,h} & M_{k-h,k-h} \end{bmatrix} = \begin{bmatrix} M_2 & 0_{h,k-h} \\ 0_{k-h,h} & M_{k-h,k-h} \end{bmatrix}.$$

Since $t < h$, $\det(M_2) = 0$ from Lemma 4.2. Hence, $\det(M) = \det(M_2)\det(M_{k-h,k-h}) = 0$ and $\mathcal{C}_L$ is not a Euclidean LCD code. ■

Theorem 5.14: Let $\mathcal{C}$ be an $[n,k]$-linear over $\mathbb{F}_q$ with $h := h_E(\mathcal{C}) > 0$ and L be a linear transform from $\mathcal{C}$ to $\mathbb{F}_q^h$ such that $\mathcal{C} = \mathrm{Ker}(L) \oplus \mathrm{Hull}(\mathcal{C})$. If the linear transform L is surjective, then $\mathcal{C}_L$ (defined by Equation (2)) is a Euclidean LCD code.

Corollary 5.15: If there is an $[n,k,d]$-linear code $\mathcal{C}$ over $\mathbb{F}_q$ with $h := h_E(\mathcal{C}) > 0$, then there is a linear Euclidean LCD code with parameters $[n+h, k, \geq d]$.

VI. Concluding Remarks

LCD codes have applications in information protection. This paper is devoted to determine all possible Euclidean and Hermitian LCD codes. More precisely, we introduce a general construction of LCD codes from any linear code. Further, we show that any linear code over $\mathbb{F}_q (q > 3)$ is equivalent to a Euclidean LCD code and any linear code over $\mathbb{F}_{q^2} (q > 2)$ is equivalent to a Hermitian LCD code. Consequently an $[n,k,d]$-linear Euclidean LCD code over $\mathbb{F}_q$ with $q > 3$ exists if there is an $[n,k,d]$-linear code over $\mathbb{F}_q$ and an $[n,k,d]$-linear Hermitian LCD code over $\mathbb{F}_{q^2}$ with $q > 2$ exists if there is an $[n,k,d]$-linear code over $\mathbb{F}_{q^2}$. Hence, when $q > 3$, q-ary Euclidean LCD codes are as good as q-ary linear codes.

When $q > 2$, q^2-ary Hermitian LCD codes are as good as q^2-ary linear codes. We also give a second proof of these results using the theory of Gröbner bases. Our results show in a direct way that there exist families of LCD codes exceeding the asymptotical Gilbert-Varshamov bound. We finally, present a new construction of LCD codes by extending linear codes. An interesting extension to this work would be to complete the classification of Euclidean LCD and Hermitian LCD codes by studying the case of Euclidean LCD codes over $\mathbb{F}_2$ or $\mathbb{F}_3$ and Hermitian LCD codes over $\mathbb{F}_4$.

Acknowledgement. The authors are grateful to the Assoc. Edit. Prof. Moshe Schwartz and the anonymous reviewers for their valuable comments which have highly improved the manuscript.

REFERENCES

[1] W. W. Adams and P. Loustaunau.: An introduction to Gröbner bases. American Mathematical Society, 1994.
[2] K. Boonniyoma and S. Jitman.: Complementary dual subfield linear codes over finite fields, arXiv:1605.06827 [cs.IT], 2016.
[3] T. Brylawski and J. Oxley.: The Tutte polynomial and its applications. In: Matroid applications. Cambridge Univ. Press, 1992.
[4] C. Carlet and S. Guilley.: Complementary dual codes for counter-measures to side-channel attacks, In: E. R. Pinto et al. (eds.), Coding Theory and Applications, CIM Series in Mathematical Sciences, vol. 3, pp. 97-105, Springer Verlag, 2014 and Journal Adv. in Math. of Comm. 10(1), pp. 131-150, 2016.
[5] C. Carlet, S. Mesnager, C. Tang and Y. Qi.: Euclidean and Hermitian LCD MDS Codes, arXiv preprint arXiv:1702.08033, 2017.
[6] D. A. Cox, J. Little, and D. O'Shea.: Ideals, varieties, and algorithms. Springer, 2015.
[7] H-Q. Dinh, B-T Nguyen, S. Sriboonchitta.: Constacyclic codes over finite commutative semi-simple rings, Journal Finite Fields and Their Applications, Vol. 45, pp. 1-18, 2017.
[8] S.T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok and P. Solé.: The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices. International Journal of Information and Coding Theory, vol. 4(2-3), pp. 116-128, 2017.
[9] L. Galvez, J-L Kim, N. Lee, Y-G. Roe, B-S Won.: Some Bounds on Binary LCD Codes, arXiv preprint arXiv:1701.04165, 2017.
[10] C. Greene.: Weight enumeration and the geometry of linear codes, Studies in Applied Mathematics, vol. 55, pp. 119-128, 1976.
[11] C. Güneri, F. Özbudak, B. Özkaya, E. Sacikara, Z. Sepasdar and P. Solé.: Structure and performance of generalized quasi-cyclic codes, Finite Fields and Their Applications, vol. 47, pp. 183-202, 2017.
[12] C. Güneri, B. Özkaya, Solé.: Quasi-cyclic complementary dual codes. Journal Finite Fields and Their Applications, vol. 42, pp. 67-80, 2016.
[13] T. Høholdt.: On (or in) the Blahut footprint. In: Codes, curves, and signals. Kluwer Acad. Publ., 1998.
[14] F. Jaeger.: Tutte polynomials and bicycle dimension of ternary matroids, Proc. Amer. Math. Soc., vol. 107(1), pp. 17-25, 1989.
[15] R. P. M. J. Jurrius and R. Pellikaan.: Codes, arrangements and matroids, pp. 219-325. In: Ser. Coding Theory Cryptol. World. Scientific Publishing, 2013.
[16] L. Jin.: Construction of MDS codes with complementary duals, IEEE Transactions on Information Theory, vol. 63(5), pp. 2843-2847, 2017.
[17] L. Jin and C.P. Xing.: Algebraic Geometry Codes with Complementary Duals Exceed the Asymptotic Gilbert-Varshamov bound, arXiv preprint arXiv:1703.01441, 2017.
[18] W.V. Kandasamy, F. Smarandache, R. Sujatha, R. R. Duray.: Erasure Techniques in MRD codes. Infinite Study, 2012.
[19] S. Lang.: Algebra. Addison-Wesley Publishing Co., 1965.
[20] C. Li.: Hermitian LCD codes from cyclic codes, Designs, Codes and Cryptography, pp. 1-18, 2017.
[21] C. Li, C. Ding and S. Li.: LCD Cyclic codes over finite fields. IEEE Trans. Inf. Theory, vol. 63, no. 7, pp. 4344 - 4356, 2017.
[22] S. Li, C. Li, C. Ding, and H. Liu.: Two Families of LCD BCH Codes. IEEE Trans. Inf. Theory, vol 63, no. 9, pp. 5699 - 5717, 2017.
[23] X. Liu X and H. Liu.: Matrix-Product Complementary dual Codes, arXiv preprint arXiv:1604.03774, 2016.
[24] J. L. Massey.: Linear codes with complementary duals, Discrete Math., vol. 106-107, pp. 337-342, 1992.
[25] F.J. MacWilliams and N. J. A. Sloane.: The theory of error-correcting codes. Elsevier, 1977.
[26] S. Mesnager, C. Tang and Y. Qi.: Complementary dual algebraic geometry codes, arXiv preprint arXiv:1609.05649, 2016. IEEE Transactions on Information Theory. To appear.
[27] P. Rosenstiehl and R. C. Read.: On the principal edge tripartition of a graph, Ann. Discrete Math., vol. 3, pp. 195-226, 1978.
[28] N. Sendrier.: Linear codes with complementary duals meet the Gilbert-Varshamov bound. Discrete mathematics, vol. 285 (1), pp. 345-347, 2004.
[29] J. Simonis.: The effective length of subcodes, Appl. Algebra Engrg. Comm. Comput., vol. 5(6), pp. 371-377, 1994.
[30] K. Tzeng and C. Hartmann.: On the minimum distance of certain reversible cyclic codes, IEEE Transactions on Information Theory, vol. 16(5), pp. 644-646, 1970.
[31] M.A.Tsfasman, S.G.Vlăduţ, and T. Zink.: Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachr., vol. 109, pp. 21-28, 1982.
[32] X. Yang and J. L. Massey.: The condition for a cyclic code to have a complementary dual, Journal Discrete Math., vol. 126, pp. 391-393, 1994.

Claude Carlet received the Ph.D. degree from the University of Paris 6, Paris, France, in 1990 and the Habilitation to Direct theses from the University of Amiens, France, in 1994. He was Associate Professor with the Department of Computer Science at the University of Amiens, France, from 1990 to 1994, Professor with the Department of Computer Science at the University of Caen, France, from 1994 to 2000 and with the Department of mathematics, University of Paris 8, Saint-Denis, France since then, where he is now Professor Emeritus. He is also related to the University of Bergen, Norway. His research interests include Boolean functions, cryptology and coding theory. Prof. Carlet was Associate Editor for Coding Theory of IEEE Transactions on Information Theory from March 2002 until February 2005. He is the Editor in Chief of the journal "Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences" (CCDS) published by SPRINGER. He is in the editorial boards of the journals "Designs, Codes and Cryptography" (SPRINGER), "Advances in Mathematics of Communications" (AIMS),"International Journal of Computer Mathematics" (Taylor & Francis) and "International Journal of Information and Coding Theory" (Inderscience publishers).

PLACE PHOTO HERE

Sihem Mesnager received the Ph.D. degree in Mathematics from the University of Pierre et Marie Curie (Paris VI), Paris, France, in 2002 and the Habilitation to Direct Theses (HDR) in Mathematics from the University of Paris VIII, France, in 2012. Currently, she is an associate Professor in Mathematics at the University of Paris VIII (France) in the laboratory LAGA (Laboratory of Analysis, Geometry and Applications), University of Paris XIII and CNRS. She is also Professor adjoint to Telecom ParisTech (France), research group MIC2 in mathematics of the department INFERES, Telecom ParisTech (ex. National high school of telecommunications). Her research interests include discrete mathematics, symmetric cryptography coding theory, commutative algebra and computational algebraic geometry. She is Editor in Chief of the International Journal of Information and Coding Theory (IJOCT) published by Inderscience and Editor in Chief of the international journal Advances in Mathematics of Communications (AMC) published by AIMS. She is an Associate Editor for the international journal IEEE Transactions on information Theory (IEEE-IT) and also serves the editorial board of the international journal Cryptography and Communications Discrete Structures, Boolean Functions and Sequences (CCDS) published by SPRINGER and the international journal RAIRO ITA (Theoretical Informatics and Applications). She was a program co-chair for three International Workshops and served on the board of program comitties of fifteen international conferences and workshops. Since 2016, she is president of the french Chapter of IEEE in information theory and the facilitator at AMIES (Agency for Interaction in Mathematics with Business and Society) in France for coding theory and cryptography.

PLACE PHOTO HERE

Chunming Tang was born in Sichuan, China, in 1982. He received the B. S. degree from Sichuan Normal University, Sichuan, China, in 2004, the M. S. degree and Ph. D. degree from Peking University, Beijing, China, in 2012. He is an associate professor with School of Mathematics and Information, China West Normal University, Nanchong, Sichuan, China. His research fields are cryptography, coding theory, and information security.

PLACE PHOTO HERE

Yanfeng Qi was born in Shandong, China, in 1984. He received the B. S. degree from Shandong Normal University, Shandong, China, in 2006, the M. S. degree and Ph. D. degree from Peking University, Beijing, China, in 2012. From 2012 to 2014, he was a postdoctor in Asino Corporation Inc. and Peking University. He is a researcher with School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, China. His research fields are cryptography, coding theory, and information security.

PLACE PHOTO HERE

Ruud Pellikan has tenure at the Technical University of Eindhoven where his research has shifted from a devotion to coding theory, particularly algebraic geometry codes and their decoding, to code-based cryptography. He previously served as an associate editor of the IEEE Transactions of Information Theory and has organized several conferences. He is co-author of the book Codes, Cryptology and Curves with Computer Algebra that appeared in the fall of 2017 by Cambridge University Press.