J COMP SCI APPL MATH
Journal of Computer Science and Applied Mathematics
Vol. 5, no.1, (2023), 17–33
ISSN: 1857-9582 https://doi.org/10.37418/jcsam.5.1.2

BOUNDS AND PROPERTIES OF LCD CODES OVER FIELDS

Seth Gannon and Hamid Kulosman[1]

ABSTRACT. In 2020, Pang et al. defined binary LCD $[n, k]$ codes with biggest minimal distance, which meets the Griesmer bound [1]. We give a correction to and provide a different proof for [1, Theorem 4.2], provide a different proof for [1, Theorem 4.3], examine properties of LCD ternary codes, and extend some results found in [6] for any q which is a power of an odd prime.

1. INTRODUCTION

A linear code C is called a linear complementary dual code (LCD code) if $C \cap C^{\perp} = 0$ holds. LCD codes have many applications in cryptography, communication systems, data storage, and quantum coding theory. In [3] a linear programming bound for LCD codes and the definition for $\mathrm{LD}_2(n, k)$ for binary LCD $[n, k]$-codes are provided. In 2019 we generalized those results to a formula for $\mathrm{LD}_2(n, 2)$ which appears in [2]. In this paper we explore different bounds and properties for the value LD_q where q is a prime power.

The following is Massey's Theorem which will be used often throughout this paper:

[1]*corresponding author*
Key words and phrases. Complementary dual code; LCD code; Minimal distance of a linear code; maximal possible distance; Griesmer Bound.
Submitted: 31.12.2022; *Accepted:* 15.01.2023; *Published:* 13.02.2023.

Theorem 1.1. *([7, Proposition 1]) If G is a generator matrix for the $[n, k]$ linear code C over a field $\mathbb{F}$, then C is an LCD code if and only if the $k \times k$ matrix GG^T is nonsingular.*

2. Binary linear LCD $[n, 2]$ codes with biggest minimal distance, that meet Griesmer Bound

Below is our result from [2] which we provide as a lemma and will use throughout this section.

Lemma 2.1. *[2, Theorem 2.6] For any integer $r \geq 0$ and $s \in \{3, 4, 5, 6, 7, 8\}$ we have:*

$$LD_2(6r + 3, 2) = 4r + 2,$$
$$LD_2(6r + 4, 2) = 4r + 2,$$
$$LD_2(6r + 5, 2) = 4r + 2,$$
$$LD_2(6r + 6, 2) = 4r + 3,$$
$$LD_2(6r + 7, 2) = 4r + 4,$$
$$LD_2(6r + 8, 2) = 4r + 5.$$

In other words:

$$LD_2(6r + s, 2) = 4r + \lfloor \frac{s}{6} \rfloor (1 + s \bmod 6) + 2.$$

Remark 2.1. *Note that the last equality of the above theorem holds for $r = -1$ which yields that: $LD_2(2, 2) = 1$. Also, if you replace r with $r - 1$ you have the following:*

$$LD_2(6r - 3, 2) = 4r - 2,$$
$$LD_2(6r - 2, 2) = 4r - 2,$$
$$LD_2(6r - 1, 2) = 4r - 2,$$
$$LD_2(6r + 0, 2) = 4r - 1,$$
$$LD_2(6r + 1, 2) = 4r + 0,$$
$$LD_2(6r + 2, 2) = 4r + 1.$$

In this section we make a correction of the statement to [1, Theorem 4.2] and give a different proof. We also provide a different proof of [1, Theorem 4.3].

Let C be an $[n,2]$ binary linear code let $\mathbf{u}=(u_1,u_2,\ldots,u_n)$ and $\mathbf{v}=(v_1,v_2,\ldots,v_n)$ be the first and second word in a generator matrix G for C for $i,j\in\{0,1\}$ define

$$S_{i,j}=\{\ell:\left[\begin{smallmatrix}u_\ell\\v_\ell\end{smallmatrix}\right]=\left[\begin{smallmatrix}i\\j\end{smallmatrix}\right],1\le\ell\le n\}.$$

For example $S_{0,0}$ is the number of $\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$ columns in the matrix G.

Lemma 2.2. *[1, Page 4] We have*

$$GG^T=\begin{bmatrix}S_{10}+S_{11} & S_{11}\\ S_{11} & S_{01}+S_{11}\end{bmatrix},$$

where the numbers S_{ij} is the matrix GG^T are taken modulo 2.

Lemma 2.3. *Let $C=\{\mathbf{u},\mathbf{v},\mathbf{u}+\mathbf{v},\mathbf{0}\}$ and Let $C'=\{\mathbf{u}',\mathbf{v}',\mathbf{u}'+\mathbf{v}',\mathbf{0}\}$ be two binary linear $[n,2]$ codes which have the same numbers S_{00}, S_{10}, S_{01}, and S_{11} determined using $\mathbf{u}$, $\mathbf{v}$ in C and $\mathbf{u}'$, $\mathbf{v}'$ in C' are equivalent.*

Proof. Let G (respectively G') be the generator matrix for C (respectively C') whose rows are $\mathbf{u}$, $\mathbf{v}$ (respectively $\mathbf{u}'$, $\mathbf{v}'$). Then G and G' have the same number of columns of the say type, so C and C' are permutation equivalent. For binary codes that is the same as equivalent. □

Lemma 2.4. *Let C be an $[n,2,d]$ binary linear code. Then $d\le\lfloor\frac{2n}{3}\rfloor$.*

Proof. By the Griesmer bound $n>d+\lceil\frac{d}{2}\rceil\ge d+\frac{d}{2}=\frac{3d}{2}$, hence $d\le\frac{2n}{3}$, hence $d\le\lfloor\frac{2n}{3}\rfloor$. □

The following Theorem is a correction of the statement of [1, Theorem 4.2]. It also includes the statement of [1, Theorem 4.3]. The proofs of both of the theorems are different.

Theorem 2.1. *Let C be a binary LCD $[n,2]$ code with maximal possible d that meets the Griesmer Bound. Then $n\equiv 2(\text{mod }6)$ or $n\equiv 3(\text{mod }6)$ and in both cases the code C is unique up to equivalence. Conversely, if $n\equiv 2(\text{mod }6)$ or $n\equiv 3(\text{mod }6)$ there exists one and only one (up to equivalence) binary LCD $[n,2]$ code with maximal possible d, that meets Griesmer Bound.*

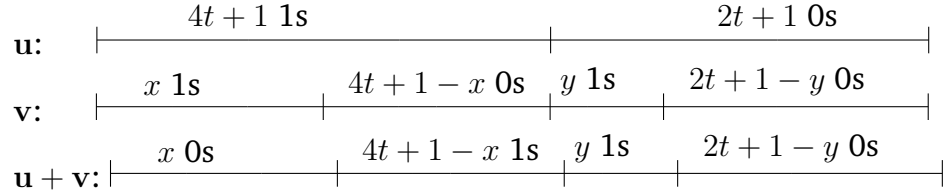
Proof. Let C be an LCD binary $[n,2,d]$ code wit maximal possible d (i.e., such that $d=\text{LD}_2(n,2)$).

i. $n \equiv 0 (\text{mod } 6)$: We can write $n = 6t$ for some $t \geq 1$. By 2.4, $d \leq \lfloor \frac{2n}{3} \rfloor$, we get $d \leq 4t$. For $d = 4t$, $d + \lceil \frac{d}{2} \rceil = 6t$, hence the code would meet Griesmer Bound if $d = 4t$. However, by 2.1, $d = 4t - 1$. Hence no LCD code C with maximal d meets the Griesmer Bound in this case.

ii. $n \equiv 1 (\text{mod } 6)$: We can write $n = 6t + 1$ for some $t \geq 0$. Since by, 2.4, $d \leq \lfloor \frac{2n}{3} \rfloor$, we get $d \leq 4t$. For $d = 4t$, $d + \lceil \frac{d}{2} \rceil = 6t < n$. Hence there is no $[6t + 1, 2]$ code which meets the Griesmer Bound.

iii. $n \equiv 2 (\text{mod } 6)$: We can write $n = 6t + 2$ for some $t \geq 0$. By 2.4, $d \leq \lfloor \frac{2n}{3} \rfloor$, we get $d \leq 4t + 1$. For $d = 4t + 1$, $d + \lceil \frac{d}{2} \rceil = 6t + 2 = n$, hence the code meets the Griesmer Bound when $d = 4t + 1$. By 2.4 in the case $n = 6t + 2$ is equal to $4t + 1$, every LCD $[6t + 2, 2]$ code with maximal possible d meets the Griesmer Bound. It remains to see how many such codes there are up to equivalence.

Let $C = \{\mathbf{u}, \mathbf{v}, \mathbf{u} + \mathbf{v}, \mathbf{0}\}$. We can assume that the non-zero words have the follow form



Then by counting ones in $\mathbf{v}$ and $\mathbf{u} + \mathbf{v}$ we get:

$$x + y \geq 4t + 1$$

$$4t + 1 - x + y \geq 4t + 1.$$

From the second equality

$$y \geq x,$$

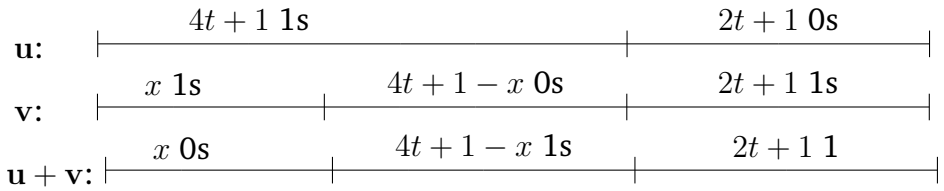
then this and the first inequality imply

$$y \geq 2t + 1.$$

Hence

$$y = 2t + 1.$$

The words $\mathbf{u}$, $\mathbf{v}$, $\mathbf{u} + \mathbf{v}$ now have the following form:



Hence (by considering the ones in $\mathbf{v}$ and $\mathbf{u}+\mathbf{v}$):

$$x + 2t + 1 \geq 4t + 1,$$
$$4t + 1 - x + 2t + 1 \geq 4t + 1.$$

These inequalities imply respectively $x \geq 2t$ and $x \leq 2t+1$. Thus, $x \in \{2t, 2t+1\}$. In the case $x = 2t$, we get from $\mathbf{u}$ and $\mathbf{v}$ the values $S_{10} = 2t+1$, $S_{01} = 2t+1$, and $S_{11} = 2t$. In the case $x = 2t+1$, we get from $\mathbf{u}$ and $\mathbf{u}+\mathbf{v}$, $S_{10} = 2t+1$, $S_{01} = 2t+1$, and $S_{11} = 2t$. Hence, the codes that we obtain in the two cases are equivalent 2.3. These codes are LCD as GG^T (from $\mathbf{u}$, $\mathbf{v}$ in case $x = 2t$) looks like

$$\begin{bmatrix} 4t+1 & 2t \\ 2t & 4t+1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

iv. $n \equiv 3 (\text{mod } 6)$: Reasoning like in the $n \equiv 2 (\text{mod } 6)$ case, we conclude that there is, up to equivalence, exactly one LCD $[n, 2]$ code with maximal d, which meets the Griesmer Bound.

v. $n \equiv 4 (\text{mod } 6)$: Reasoning like in the $n \equiv 1 (\text{mod } 6)$ case, we conclude that there is no $[6t+4, 2]$ code which meets the Griesmer Bound.

vi. $n \equiv 5 (\text{mod } 6)$: We can write $n = 6t+5$ for some $t \geq 0$. In this case the code would meet the Griesmer Bound if $d = 4t+3$, however the maximal d for an LCD $[6t+5, 2]$ codes is $4t+2$. Thus, no LCD code with maximal d meets the Griesmer Bound in this case.

□

3. Ternary linear LCD $[n, 2]$ codes with biggest minimal distance, that meet Griesmer Bound

The quantity $\text{LD}_2(n, k)$ that we defined for binary codes will be denoted by $\text{LD}_3(n, k)$ in the case of ternary codes (i.e. codes over $\mathbb{F}_3$).

Definition 3.1. *$LD_3(n,k) = max\{d \mid$ there exists a ternary $[n,k,d]$ LCD code$\}$.*

Theorem 3.1. *[1, Theorem 5.3 & Theorem 5.4] Let $n \geq 2$. Then $LD_3(n,2) = \lfloor \frac{3n}{4} \rfloor$ for $n \equiv 1,2 (mod\ 4)$ and $LD_3(n,2) = \lfloor \frac{3n}{4} \rfloor - 1$ for $n \equiv 0,3 (mod\ 4)$.*

In the next theorem we will determine for which n ternary LCD $[n,2]$ codes with maximal d meet the Griesmer Bound.

Theorem 3.2. *Let C be a ternary LCD $[n,2,d]$ code with $d = LD_3(n,2)$. Then C meets the Griesmer Bound if and only if $n \equiv 2 (mod\ 4)$.*

Proof. By using the Griesmer Bound we get $n \geq d + \lceil \frac{d}{3} \rceil$, hence $d \leq \frac{3n}{4}$ and $d \leq \lfloor \frac{3n}{4} \rfloor$.

i. $\underline{n \equiv 0 (\text{mod } 4)}$: Set $n = 4t$ for some $t \geq 1$. Then, $d \leq \lfloor \frac{3n}{4} \rfloor = 3t$. We calculate $d + \lceil \frac{d}{3} \rceil$ for $d = 3t$ and get $4t$, which is equal to n, so that the code meets the Griesmer Bound when $d = 3t = \lfloor \frac{3n}{4} \rfloor$. However, $\text{LD}_3(n,2) = \lfloor \frac{3n}{4} \rfloor - 1$, so no ternary $LCD[n,2,d]$ code with $d = \text{LD}_3(n,2)$ can meet the Griesmer Bound in this case.

ii. $\underline{n \equiv 1 (\text{mod } 4)}$: Set $n = 4t+1$ for some $t \geq 1$. Then $\lfloor \frac{3n}{4} \rfloor = 3t$. If we calculate $d + \lceil \frac{d}{3} \rceil$ for $d = 3t$, we get $4t < n$, so the codes with this d do not meet the Griesmer Bound. Since $\text{LD}_3(n,2) = 3t$ we conclude that no ternary LCD $[n,2,d]$ code with $d = \text{LD}_3(n,2)$ can meet the Griesmer Bound in this case too.

iii. $\underline{n \equiv 2 (\text{mod } 4)}$: Set $n = 4t+2$ for some $t \geq 0$. Then $\lfloor \frac{3n}{4} \rfloor = 3t+1$. If we calculate $d + \lceil \frac{d}{3} \rceil$ for $d = 3t+1$, we get $4t+2$ which is equal to n, Since in this case $\text{LD}_3(n,2) = \lfloor \frac{3n}{4} \rfloor = 3t+1$, by Theorem 3.2 we conclude that any ternary LCD $[n,2,d]$ code with $d = \text{LD}_3(n,2)$ meets the Griesmer Bound in this case.

iv. $\underline{n \equiv 3 (\text{mod } 4)}$: By reasoning like in the first case we conclude that no ternary LCD $[n,2,d]$ code with $d = \text{LD}_3(n,2)$ can meet the Griesmer Bound in this case as well.

□

Let C be a ternary linear $[n,2]$ code. Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be the first and second word in a generator matrix G for C. For $i, j \in$

$\{0, 1, 2\}$ define the following as in [1, Page 6]

$$S_{i,j} = \{\ell : \left[\begin{smallmatrix} u_\ell \\ v_\ell \end{smallmatrix}\right] = \left[\begin{smallmatrix} i \\ j \end{smallmatrix}\right], 1 \leq \ell \leq n\}.$$

Lemma 3.1. *[1, Page 6] Let C be a ternary linear $[n, 2]$ code with generator matrix G whose rows are $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. Then*

$$GG^T = \left[\begin{smallmatrix} S_{10}+S_{20}+S_{12}+S_{21}+S_{11}+S_{22} & S_{11}+2S_{12}+S_{21}+S_{22} \\ S_{11}+2S_{12}+S_{21}+S_{22} & S_{10}+S_{20}+S_{12}+S_{21}+S_{11}+S_{22} \end{smallmatrix}\right]$$

where the numbers S_{ij} is the matrix GG^T are taken modulo 3.

Proposition 3.1. *When $n = 2$, there is exactly one ternary LCD $[n, 2, d]$ code with the maximal possible d, which meets the Griesmer Bound, namely the code $\mathbb{F}_3^2$.*

Proof. When $n = 2$, $\mathrm{LD}_3(n, 2) = \lfloor \frac{3n}{4} \rfloor = \lfloor \frac{6}{4} \rfloor = 1$ by 3.1. Since for $d = 1$, $d + \lceil \frac{d}{3} \rceil = 2 = n$, every ternary LCD $[2, 2]$ code with maximal d meet the Griesmer Bound. However, there is exactly one such codes since there are 9 linear combinations of two words over $\mathbb{F}_3$, so that the code is equal to $\mathbb{F}_3^2$. □

A statement like the following was not mentioned in [1].

Theorem 3.3. *When $n = 4t + 2$ with $t \geq 1$, there are (up to equivalence) two ternary LCD $[n, 2, d]$ codes with maximal possible d, which meet Griesmer Bound.*

Proof. When $n = 4t + 2$, by 3.1 we have that $\mathrm{LD}_3(n, 2) = \lfloor \frac{3n}{4} \rfloor = \lfloor \frac{12t+6}{4} \rfloor = 3t + 1$. When $d = 3t+1$, $d + \lceil \frac{d}{3} \rceil = 4t+2 = n$, so with this d the codes meet the Griesmer Bound. It remains to see how many such codes there are up to equivalence. Let $\mathbf{u}$ and $\mathbf{v}$ be the first and second rows of a generator matrix of such a code C. We can assume that $\mathbf{u}$ and $\mathbf{v}$ have the following form:

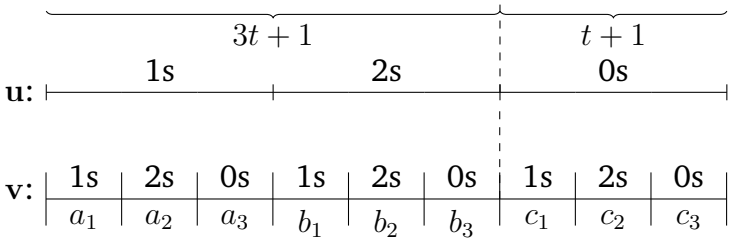


FIGURE 1.

This code is equivalent with the code whose generator matrix has the following words:

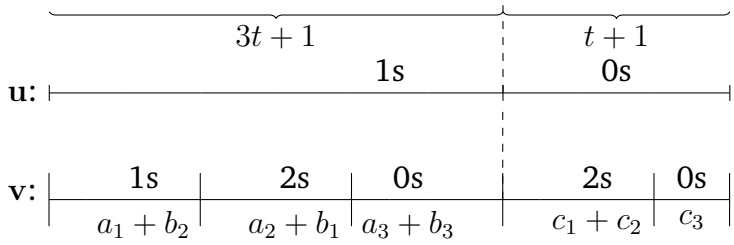


FIGURE 2.

The word $\mathbf{u}+\mathbf{v}$ from 2 has the following form:

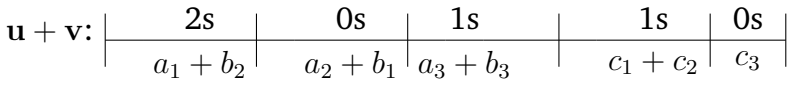


FIGURE 3.

Taking into account the number of ones and twos in the 3 words above, we get:

$$a_1+a_2+a_3+b_1+b_2+b_3=3t+1, \tag{3.1}$$

$$a_1+a_2+b_1+b_2+c_1+c_2\geq 3t+1, \tag{3.2}$$

$$a_1+a_3+b_1+b_3+c_1+c_3\geq 3t+1. \tag{3.3}$$

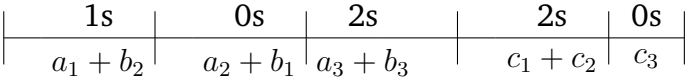
From (3.1) and (3.2) we get

$$c_1+c_2\geq a_3+b_3, \tag{3.4}$$

and from (3.1) and (3.3) we get

$$c_1+c_2\geq a_2+b_1. \tag{3.5}$$

The word $2\mathbf{u}+\mathbf{2v}$ from 2 has the following form:



Counting ones and twos we get

$$a_1+b_2+a_3+b_3+c_1+c_2\geq 3t+1, \tag{3.6}$$

which together with (3.1) implies

$$c_1 + c_2 \geq a_1 + b_2. \tag{3.7}$$

If we consider other linear combinations of $\mathbf{u}$ and $\mathbf{v}$ from 2 and do a similar reasoning, we end up with one of the inequalities (3.4), (3.5), (3.7) or with the inequality (3.1). Note that there are exactly 8 non-zero linear combinations, each of the relations (3.1), (3.4), (3.5), (3.7) would be yielded from exactly two linear combinations. If we add (3.4), (3.5), and (3.7) we get:

$$3(c_1 + c_2) \geq a_1 + b_2 + a_2 + b_1 + a_3 + b_3 = 3t + 1.$$

Hence,

$$c_1 + c_2 \geq t + \frac{1}{3},$$

and so

$$c_1 + c_2 \geq t + 1.$$

However, from the word $\mathbf{u}$ in 2 we can see that

$$c_1 + c_2 \leq t + 1.$$

Hence,

$$\begin{aligned} c_1 + c_2 &= t + 1, \\ c_3 &= 0. \end{aligned} \tag{3.8}$$

Now, (3.4), (3.5), (3.7), and (3.8) imply:

$$a_1 + b_2 \leq t + 1 \tag{3.9}$$

$$a_2 + b_1 \leq t + 1 \tag{3.10}$$

$$a_3 + b_3 \leq t + 1 \tag{3.11}$$

Adding (3.9) and (3.10) we get

$$a_1 + b_2 + a_2 + b_1 \leq 2t + 2, \tag{3.12}$$

which together with (3.1) implies

$$a_3 + b_3 \geq t - 1. \tag{3.13}$$

Similarly, we get

$$a_1 + b_2 \geq t - 1, \tag{3.14}$$

$$a_2 + b_1 \leq t - 1. \tag{3.15}$$

Now from (3.9), (3.10), (3.11), (3.13), (3.14), and (3.15) we conclude

$$a_1 + b_2 \in \{t - 1, t, t + 1\}, \tag{3.16}$$

$$a_2 + b_1 \in \{t - 1, t, t + 1\}, \tag{3.17}$$

$$a_3 + b_3 \in \{t - 1, t, t + 1\}. \tag{3.18}$$

The relations (3.16), (3.17), (3.18), and (3.1) imply that there are six possible cases:

$$a_1 + b_2 = t - 1,\ a_2 + b_1 = a_3 + b_3 = t + 1, \tag{3.19}$$

$$a_2 + b_1 = t - 1,\ a_1 + b_2 = a_3 + b_3 = t + 1, \tag{3.20}$$

$$a_3 + b_3 = t - 1,\ a_1 + b_2 = a_2 + b_1 = t + 1, \tag{3.21}$$

$$a_1 + b_2 = a_2 + b_1 = t,\ a_1 + b_2 = t + 1, \tag{3.22}$$

$$a_1 + b_2 = a_3 + b_3 = t,\ a_2 + b_1 = t + 1, \tag{3.23}$$

(3.24) $$a_2 + b_1 = a_3 + b_3 = t,\ a_1 + b_2 = t + 1.$$

In each of these cases we have codes with maximal possible $d = 3t + 1$ which meet the Griesmer Bound. We need to check which of them are LCD. From 2, we use 3.1 to calculate GG^T. For example, in case (3.19) we get

$$GG^T = \begin{bmatrix} 3t+1 & 3t+1 \\ 3t+1 & 3t+1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

so the code is not a LCD by 1.1. Similarly, the codes (3.20) and (3.22) are not LCD. In the case (3.21) we get

$$GG^T = \begin{bmatrix} 3t+1 & 3t+2 \\ 3t+2 & 3t+2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix},$$

so the code is LCD. Similarly, the codes (3.23) and (3.24) are LCD.

So far we concluded that we have three $[n, 2, d]$ LCD codes with largest possible d (up to equivalence) that meet the Griesmer Bound. They have generator matrices with words $\mathbf{u}$, and $\mathbf{v}$ from 2, with the parameters a_1, a_2, a_3, b_1, b_2, b_3, c_1, and c_2 satisfying (3.8), (3.21), (3.23), and (3.24). We not consider the equivalence of these 3 codes. The code (3.21) has in all of its 8 non-zero words the number of zeros equal to either $t - 1$ or $t + 1$. Since the number of zeros in every non-zero word is not equal to t, we conclude that this code is not equivalent to the codes (3.23) or (3.24). The reason is the fact that the codes (3.23) and (3.24) have some words with t zeros, and the number of zeros cannot be changed by permutation of coordinates and multiplication of certain columns by 2. The code (3.23) and (3.24) are equivalent since the generator matrix with rows $\mathbf{u}$, and $\mathbf{v}$ for the code (3.23) is equal to the generator matrix with rows $\mathbf{u}$, and $2\mathbf{u} + \mathbf{v}$ for the code (3.24). Thus up to equivalence, we have two ternary LCD $[4t + 2, 2]$ codes $(t \geq 1)$ with biggest possible d, which meet the Griesmer Bound. □

4. $\mathrm{LD}_3(n, n - i) = 2$ UNDER CERTAIN ASSUMPTIONS

Theorem 4.1. *For every $i \geq 3$ and $n \geq \frac{3^i+1}{2}$, $LD_3(n, n - i) = 2$.*

Proof. Let C be a ternary $[n, n-i, d]$ code. Using the sphere packing bound we have

$$3^{n-i}\big(1+2n+\cdots+2^t\tbinom{n}{t}\big) \leq 3^n,$$

where $t = \lfloor \frac{d-1}{2} \rfloor$. Hence

$$1+2n+\cdots+2^t\tbinom{n}{t} \leq 3^i. \tag{4.1}$$

When $n \geq \frac{3^i+1}{2}$, $1+2n \geq 3^i+2$. Hence (4.1) implies that $t=0$, i.e., $\lfloor \frac{d-1}{2} \rfloor = 0$. Hence $d \leq 2$. Now we show that there is a ternary LCD $[n, n-i, 2]$ code for every $i \geq 3$ and $n \geq \frac{3^i+1}{2}$. If $i \equiv 0 (\text{mod } 3)$, let

$$G = \Big[I_{n-i} \,\Big|\, \underbrace{\mathbb{1} \quad \mathbb{1} \quad \dots \quad \mathbb{1}}_{i} \Big], \text{ where } \mathbb{1} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \} n-i.$$

Let $R_1, R_2, \dots R_{n-i}$ be the rows of G. Then $\langle R_j, R_j \rangle = 1$ for every $j \in \{1, 2, \dots, n-i\}$, and $\langle R_j, R_{j'} \rangle = 0$ for any $j, j' \in \{1, 2, \dots, n-i\}$ with $j \neq j'$. Hence $GG^T = I_{n-i}$. If $i \equiv 1 (\text{mod } 3)$, let

$$G = \Big[I_{n-i} \,\Big|\, \underbrace{\mathbb{1} \quad \mathbb{1} \quad \dots \quad \mathbb{1} \quad \mathbf{0}}_{i} \Big], \text{ where } \mathbf{0} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \} n-i.$$

Using the same Reasoning as the previous case we see that $GG^T = I_{n-i}$. Finally if $i \equiv 2 (\text{mod } 3)$, let

$$G = \Big[I_{n-i} \,\Big|\, \underbrace{\mathbb{1} \quad \mathbb{1} \quad \dots \quad \mathbb{1} \quad \mathbf{0} \quad \mathbf{0}}_{i} \Big].$$

Like in the previous two cases $GG^T = I_{n-i}$. Whenever $GG^T = I_{n-i}$, the code C whose generator matrix is G is LCD by 5.1. Note also that the minimum distance will always be ≥ 2 since we always have at least one $\mathbb{1}$ column (since $i \geq 3$) and a linear combination of greater than or equal to 2 rows of G has at least 2 non-zero values coming from the I_{n-i} part. □

5. Nonexistence of certain LCD ternary codes

Lemma 5.1. *There is no $[n, 1, 3j]$ LCD code for $j \geq 1$ and $n \geq 3$.*

Proof. Suppose to the contrary. Let C be an LCD$[n, 1, 3j]$ ternary code. Then $GG^T = [\langle R_1, R_1 \rangle] = [0]$ since each addend in $\langle R_1, R_1 \rangle$ is either 0 or 1 and there

are $3j$ ones, hence $\langle R_1, R_1\rangle = 0$. Here R_1 is the only row of a generator matrix G of C. Now by 1.1 C is not a LCD code, a contradiction. □

Theorem 5.1. *Suppose* $i, k \geq 1$

i. If $n \equiv 0 (mod\ 3)$ *and* $n \geq 12i$*, there is no* $[n, k, n-3i]$ *LCD ternary code.*

ii. If $n \equiv 1 (mod\ 3)$ *and* $n \geq 12i+4$*, there is no* $[n, k, n-3i-1]$ *LCD ternary code.*

iii. If $n \equiv 2 (mod\ 3)$ *and* $n \geq 12i+8$*, there is no* $[n, k, n-3i-2]$ *LCD ternary code.*

Proof.

i. For $k = 1$, there is no $[n, 1, n-3i]$ LCD ternary code by 5.1 since $n \equiv 0 (\text{mod } 3)$. Let $k = 2$. Suppose to the contrary. Let C be an $[n, 2, n-3i]$ LCD ternary code. By the Griesmer Bound, $n \geq n-3i+\lceil \frac{n-3i}{3} \rceil = n-3i+\frac{n}{3}-i$, which implies $n \leq 12i$. Hence $n = 12i$ (since we assumed $n \geq 12i$). Then $n - 3i = 9i$. However, by 3.1, $\text{LD}_3(12i, 2) = \lfloor \frac{3 \cdot 12i}{4} \rfloor - 1 = 9i - 1$. Which is a contradiction.

Now suppose $k \geq 3$. Suppose to the contrary. Let C be an $[n, k, n-3i]$ LCD ternary code. Since $n \geq 12i$, $n - 3i \geq 9i$. Hence by the Griesmer Bound, $n \geq n - 3i + \lceil \frac{n-3i}{3} \rceil + \lceil \frac{9i}{9} \rceil$, which implies $3i \geq \frac{n}{3} - i + i$ and so $n \leq 9i$, a contradiction.

ii. For $k = 1$, there is no $[n, 1, n-3i-1]$ LCD ternary code by 5.1 since $n \equiv 0 (\text{mod } 3)$. Let $k = 2$. Suppose to the contrary. Let C be an $[n, 2, n-3i-1]$ LCD ternary code. By the Griesmer Bound we have $n \geq n - 3i - 1 + \lceil \frac{n-3i-1}{3} \rceil$. If we write $n = 3m + 1$ we get from here $3i + 1 \geq m - i$, hence $4i + 1 \geq m = \frac{n-1}{3}$, hence $n \leq 12i + 4$. Hence $n = 12i + 4$ (since we assumed $n \geq 12i + 4$). However, by 3.1, $\text{LD}_3(12i + 4, 2) = 9i + 2$ and $n - 3i - 1 = 9i + 3$. We have a contradiction. Suppose $k \geq 3$. Suppose to the contrary. Let C be an $[n, k, n-3i-1]$ LCD ternary code. Since $n \geq 12i + 4$, $n - 3i - 1 \geq 9i + 3$. Hence by the Griesmer Bound, $n \geq n - 3i - 1 + \lceil \frac{n-3i-1}{3} \rceil + \lceil \frac{9i+3}{9} \rceil$, which implies $3i \geq \frac{n}{3} - 1$ and so $n \leq 9i + 3$, a contradiction.

iii. For $k = 1$, there is no $[n, 1, n-3i-2]$ LCD ternary code by 5.1 since $n \equiv 0 (\text{mod } 3)$. Let $k = 2$. Suppose to the contrary. Let C be an $[n, 2, n-3i-2]$ LCD ternary code. By the Griesmer Bound we have $n \geq n - 3i - 2 +$

$\lceil \frac{n-3i-2}{3} \rceil$. If we write $n = 3m + 2$ we get from here $3i + 2 \geq m - i$, hence $4i + 2 \geq m = \frac{n-2}{3}$, hence $n \leq 12i + 8$. Hence $n = 12i + 8$ (since we assumed $n \geq 12i + 8$). However, by 3.1, $\text{LD}_3(12i + 8, 2) = 9i + 2$ and $n - 3i - 1 = 9i + 3$. We have a contradiction. Now suppose $k \geq 3$. Suppose to the contrary. Let C be an $[n, k, n - 3i - 2]$ LCD ternary code. Since $n \geq 12i + 8$, $n - 3i - 2 \geq 9i + 6$. Hence by the Griesmer Bound, $n \geq n - 3i - 2 + \lceil \frac{n-3i-2}{3} \rceil + \lceil \frac{9i+6}{9} \rceil$, which implies $3i \geq \frac{n}{3} - 2$ and so $n \leq 9i + 6$, a contradiction.

□

6. The relation $\text{LD}_q(n, k) \leq \text{LD}_q(n, k - 1)$

For binary codes the relation $\text{LD}_2(n, k) \leq \text{LD}_2(n, k - 1)$ for any $2 \leq k \leq n$ was proved in [4, Theorem 8]. For ternary codes a proof was given in [6]. For other q a proof was given in the same paper by Harada and Saito. Their proof relies on the proof for $q = 3$ and a theorem from [5] . For codes over $\mathbb{F}_q$ a proof was also attempted in [1], but it is not correct since [1, Lemma 7.1] is not proven correctly. We now give a simple proof over $\mathbb{F}_q$ (q a power of an odd prime) using the following theorem of Serre:

Theorem 6.1. *[4, Proposition 24] Let q be a power of an odd prime. If M is a $k \times k$ regular matrix over $\mathbb{F}_q$ with $k \geq 2$, then there exists a $k \times k$ regular matrix Q such that*

$$QMQ^T = \textit{diag}[1, 1, \ldots, 1, \delta],$$

where $\delta = 1$ if $\det(M)$ is a square in $\mathbb{F}_q$, and δ is any non-square in $\mathbb{F}_q$ if $\det(M)$ is a non-square in $\mathbb{F}_q$

Theorem 6.2. *[4, Theorem 25] Let q be a power of an odd prime and C an $[n, k, d]$ code F_q. Then C is LCD if and only if there is a generator matrix G of C such that $GG^T = \textit{diag}[1, 1, \ldots, 1, \delta]$, where $\delta \in \mathbb{F}_q \setminus \{0\}$.*

Theorem 6.3. *We have*

$$\textit{LD}_q(n, k) \leq \textit{LD}_q(n, k - 1)$$

for any $n \geq 2$, $k \geq 2$ and q a power of an odd prime.

Proof. Let $n \geq 2$, $k \geq 2$ and q a power of an odd prime. Let C be an LCD $[n,k]$ code over $\mathbb{F}_q$ with $d = \mathrm{LD}_q(n,k)$. Then by 6.2 there is a generator matrix G for C such that

$$GG^T = \mathrm{diag}[1,1,\ldots,1,\delta],$$

$\delta \in \mathbb{F}_q \setminus \{0\}$. Let G_1 be the matrix whose rows are the first $k-1$ rows of G and let C_1 be the code with generator matrix G_1. Then C_1 is an $[n,k-1]$ code, which is LCD by as $G_1G_1^T = I_{k-1}$. Since $d(C_1) \geq d(C)$, we in particular have $\mathrm{LD}_q(n,k) \leq \mathrm{LD}_q(n,k-1)$. □

Corollary 6.1. *Suppose $2 \leq k \leq n$. Then*

$$LD_q(n,k) \leq LD_q(n,k-1)$$

for any q.

Proof. For $q = 2$ see [4, Theorem 8]. For q a power of an odd prime, see 6.3. Now assume $q \geq 4$. Let C be an LCD $[n,k]$ code over $\mathbb{F}_q$ with $d = \mathrm{LD}_q(n,k)$. Let D be any $[n,k-1]$ sub-code of C. By [5], D is equivalent to some LCD $[n,k-1]$ code E. Hence they have the same minimum distance. Since $d(D) \geq d(C)$, we have $d(E) \geq d(C)$. Hence $\mathrm{LD}_q(n,k) \leq \mathrm{LD}_q(n,k-1)$. □

7. An LCD $[n,k+1]$ code containing the given LCD $[n,k]$ code as a subcode

The next theorem was proved for $q = 3$ in [6, Proposition 5(i) and Remark 6]. We give a constructive proof for any q which is a power of an odd prime using [4, Proposition 24].

Theorem 7.1. *Suppose that $1 \leq k \leq n-1$ and that q is a power of an odd prime. For any LCD $[n,k]$ code over $\mathbb{F}_q$ there is an LCD $[n,k+1]$ code containing C as a subcode.*

Before we give a proof of the above theorem, we will give the next corollary of [4, Theorem 25].

Corollary 7.1. *Let q be a power of an odd prime. If C is an LCD $[n,k]$ code over $\mathbb{F}_q$ with $k \geq 1$ and $n-k \geq 1$, then there is a word $\boldsymbol{x} \in C^\perp$ such that $\langle \boldsymbol{x}, \boldsymbol{x} \rangle = 1$.*

Proof. By 1.1, $C^{\perp}$ is an LCD $[n, n-k]$ code. By 6.2 it has a generator matrix G such that $GG^T = \text{diag}[1, 1, \ldots, 1, \delta]$, $\delta \in \mathbb{F}_q \setminus \{0\}$ Hence there is a word in $C^{\perp}$ (a row of the generator matrix) such that $\langle \mathbf{x}, \mathbf{x} \rangle = 1$. □

Proof. Let G be a generator matrix of C. By 1.1, $C^{\perp}$ is an LCD $[n, n-k]$ code. Hence by the 7.1, there is a word $\mathbf{x} \in C^{\perp}$ such that $\langle \mathbf{x}, \mathbf{x} \rangle = 1$. Consider the matrix G' obtained by putting the word $\mathbf{x}$ in the first row of G' and the rows G in the rows below (in the order they are in G). Then

$$G'(G')^T = \begin{bmatrix} 1 & 0 & . & . & . & 0 \\ 0 & & & & & \\ . & & & & & \\ . & & & GG^T & & \\ . & & & & & \\ 0 & & & & & \end{bmatrix}$$

Hence, $G'(G')^T$ is regular (as GG^T is regular), so the code C' whose generator matrix is G' is a LCD code by 1.1 and C is a subcode of C'. □

Remark 7.1. *The difference between this proof and the proof in [6] is in the way the word* $\boldsymbol{x}$ *is produced. In [6, Lemma 3(i)] a theorem about self-orthogonality of ternary codes was used, so the constructive proof given in [6, Remark 6] works for only ternary codes. The above proof uses Serre's Theorem and our constructive proof works for any* $\mathbb{F}_q$, q *a power of an odd prime.*

REFERENCES

[1] B. Pang, S. Zhu, X. Kai: *Some new bounds on LCD codes over finite fields*, Cryptogr. Commun., **12**(4) (2020), 743–755.

[2] S. GANNON, H. KULOSMAN: *The formula for the largest minimal distance of binary LCD* $[n, 2]$ *codes*, arXiv preprint arXiv:1909.00253 (2019)

[3] S.T. DOUGHERTY, J-L. KIM, JON-LARK, B. OZKAYA, L. SOK, LIN, P. SOLÉ: *The combinatorics of LCD codes: linear programming bound and orthogonal matrices*, Int. J. Inf. Commun. Technol., **4**(2-3) (2017), 116–128.

[4] C. CARLET, S. MESNAGER, C. TANG, Y. QI. CHUNMING: *New characterization and parametrization of LCD codes*, IEEE Trans. Inf. Theory., **65**(1) (2018), 39–49.

[5] C. CARLET, S. MESNAGER, C. TANG, Y. QI. CHUNMING, Y.R. PELLIKANN: *Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$*, IEEE Trans. Inf. Theory., **64**(4) (2018), 3010–3017.

[6] M. HARADA, K. SAITO: *Remark on subcodes of linear complementary dual codes*, Inf. Process. Lett., **159** (2020), 105963.

[7] J.L. MASSEY: *Linear codes with complementary duals*, Discrete Math., **106** (1992), 337–342.

DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE
SEWANEE: THE UNIVERSITY OF THE SOUTH
723 UNIVERSITY AVENUE, SEWANEE, TN 37375
USA
Email address: dsgannon@sewanee.edu

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF LOUISVILLE
2301 SOUTH 3RD ST, LOUISVILLE, KY 40292
USA
Email address: hamid.kulosman@louisville.edu