8-2022

Properties and classifications of certain LCD codes.

Dalton Seth Gannon
University of Louisville

PROPERTIES AND CLASSIFICATIONS OF CERTAIN LCD CODES

By

Dalton Seth Gannon
B.A., Transylvania University, 2015
M.S., University of Dayton, 2017
M.A., University of Louisville, 2018

A Dissertation
Submitted to the Faculty of the
College of Arts and Sciences of the University of Louisville
in Partial Fulfillment of the Requirements
for the Degree of

Doctor of Philosophy
in
Applied and Industrial Mathematics

Department of Mathematics
University of Louisville
Louisville, Kentucky

August 2022

PROPERTIES AND CLASSIFICATIONS OF CERTAIN LCD CODES

Submitted by

Dalton Seth Gannon

A Dissertation Approved on

May 18th, 2022

by the Following Dissertation Committee:

Dr. Hamid Kulosman,
Dissertation Director

Dr. Csaba Biro

Dr. Ryan Gill

Dr. Jinja Li

Dr. Aly Farag

DEDICATION

To Maverick & The Gannons.

ACKNOWLEDGEMENTS

I would like to thank my advisor Dr. Hamid Kulosman for all of his guidance, patience, and support. The confidence I gained from his abstract algebra course paired with his willingness to research coding theory with me made this dissertation possible. I would like to thank the members of my dissertation committee, Dr. Csaba Biro, Dr. Ryan Gill, Dr. Jinjia Li, and Dr. Aly Farag, for their dedication, time, and valuable suggestions. I would like to give a special thanks to Dr. Thomas Riedel, for his support, advice, and unexpected conversations that were always a bright spot in my day. I would like to thank my colleagues and friends for their support, companionship studying, and for celebrating the good times together. I would like to thank my family, who believed in me even when I was unsure of myself. To these people, I am forever grateful.

ABSTRACT

PROPERTIES AND CLASSIFICATIONS OF CERTAIN LCD CODES

Dalton Seth Gannon

May 18th, 2022

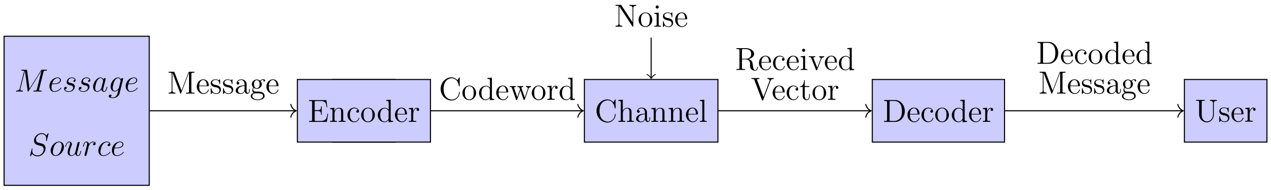
A linear code C is called a linear complementary dual code (LCD code) if $C \cap C^{\perp} = 0$ holds. LCD codes have many applications in cryptography, communication systems, data storage, and quantum coding theory. In this dissertation we show that a necessary and sufficient condition for a cyclic code C over $\mathbb{Z}_4$ of odd length to be an LCD code is that $C = \big(f(x)\big)$ where f is a self-reciprocal polynomial in $\mathbb{Z}_4[X]$ which is also in our paper [10]. We then extend this result and provide a necessary and sufficient condition for a cyclic code C of length N over a finite chain ring $R = \big(R, \mathfrak{m} = (\gamma), \kappa = R/\mathfrak{m}\big)$ with $\nu(\gamma) = 2$ to be an LCD code. In [6] a linear programming bound for LCD codes and the definition for $\mathrm{LD}_2(n,k)$ for binary LCD $[n,k]$-codes are provided. Thus, in a different direction, we find the formula for $\mathrm{LD}_2(n,2)$ which appears in [11]. In 2020, Pang et al. defined binary LCD $[n,k]$ codes with biggest minimal distance, which meets the Griesmer bound [23]. We give a correction to and provide a different proof for [23, Theorem 4.2], provide a different proof for [23, Theorem 4.3], examine properties of LCD ternary codes, and extend some results found in [14] for any q which is a power of an odd prime.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Algebraic coding theory (or coding theory for short) originated in 1948 from the paper, “A Mathematical Theory of Communication” by Claude Shannon. In his paper, Shannon was able to prove that data can be encoded before a transmission so that data sent through a noisy channel can be decoded to a specified degree of accuracy. The theorem proves the existence of such codes; however, Shannon does not provide any error-correcting codes. Thus, coding theory focuses on the design of error-correcting codes for the reliable transmission of information across a noisy channel. Below is a diagram which represents a communication channel described in Shannon’s Theorem:



In general, we say that an (n, M, d) code C over a field $\mathbb{F}_q$ is a code of length n with M codewords whose minimum distance is d. While codes can be non-linear this dissertation only examines linear codes. If a code C is linear we say it is an [n,k,d] code where $k = log_q M$ and d is the minimum weight of the code [16]. A main goal of coding theory is to create ‘good’ codes. A good (n, M, d)-code has small n for fast transmission of messages, large M to enable transmission of a wide variety of messages and large d to correct many errors [15]. Maximizing these parameters is conflicting, which creates what is known as the ‘main coding theory problem’. That is, to optimize one of the parameters n, M, d for given values of the other two. The usual version of the problem is to find the largest code of given length and given minimum distance.

An important subset of linear codes is the hull of a linear code. The hull of a linear code is the intersection of the code itself with it’s respective dual code. These codes have been widely studied due to their applications in coding theory ([18],[24],([25]). The hull of linear codes play an important role in determining algorithms in coding theory such as computing the automorphism group of a linear code. The hull of codes have also been used in the construction of good entaglement-assisted quantum error correcting codes, which can be seen in [12]. There are two special cases of the hull of a code. One is when the hull is only the zero codeword. In that case the code is known as a linear complementary dual (LCD) code, which is the focus of this dissertation. The other case is when the hull is equal to the code itself, and the code is called a self-dual code.

There are two foundational papers for the LCD codes. The first is [21] by James L. Massey in 1992. In this paper Massey defined a necessary and sufficient for a linear code over a field to be an LCD code in terms of the generator matrix. Later, Massey along with Yang in [27] gave a necessary and sufficient condition for a cyclic code over a field to be an LCD code. The following are natural question stemming from their result.

Question 1: What would a necessary and sufficient condition be for cyclic codes over $\mathbb{Z}_4$ to be an LCD?

Question 2: Furthermore, if such condition exists, could it be generalized to other finite chain rings?

In a more recent paper [6], Daugherty et al. investigated the maximum minimum distance such that a binary LCD codes exists for fixed n and k. In the paper they provide a few values for the maximum minimum distance for when $k = 2$ and $n \in \{3, 4, 5, 6, 7\}$. This result prompted the following question:

Question 3: Can the maximum minimum distance for a binary LCD codes be formulated for any n given $k = 2$?

In ([4], [5], [14], [23]) the idea of bounding the maximum minimum distance for LCD $[n, 2]$ is explored. Their results lead to the following questions:

Question 4: Can the Griesmer Bound be applied to biggest minimal distance of LCD $[n, 2]$ binary and ternary codes?

Question 5: Can the bounds and properties established for $\mathrm{LD}_2(n, k)$ and $\mathrm{LD}_3(n, k)$ be expanded to $\mathrm{LD}_q(n, k)$?

The purpose of this dissertation is to answer the fore-mentioned questions and is organized as follows. In Chapter 2 concepts for linear codes over fields are reviewed. In Chapter 3 we expand on the results of Massey and Yang. We use a theorem from the recent paper [18], in which a formula for the number of elements in hull(C) was given in terms of the generators of a cyclic code C of odd length N over $\mathbb{Z}_4$. Using that theorem we give a necessary and sufficient condition for a cyclic code C over $\mathbb{Z}_4$ of odd length to be an LCD code [10], answering **Question 1**. In Chapter 4 we use results from [17] and [22] to generalize our result from Chapter 3 and give a condition for a cyclic code C over a finite chain ring with nilpotency

2 to be an LCD code which answers **Question 2**. In Chapter 5 we expand on the values presented in [6] and give a formula for the maximal minimum distance such that a binary LCD codes exists given $k = 2$ [11] which answers **Question 3**. In 2020, Pang et al. defines binary linear LCD $[n, 2]$ codes with biggest minimal distance, that meet the Griesmer Bound [23]. We give a correction to and provide a different proof for [23, Theorem 4.2], provide a different proof for [23, Theorem 4.3], examine properties of LCD ternary codes, and extend some results found in [14] for any q which is a power of an odd prime, which answers **Question 4** and **Question 5**. Lastly, in Chapter 6 we give our conclusions and recommendations for future work.

CHAPTER 2

PRELIMINARIES

2.1 Linear Codes

While non-linear codes exist, this dissertation focuses on linear codes. More specifically, codes over certain finite fields and linear codes over certain finite chain rings, which will be discussed later.

An $[n, k, d]$ linear code C over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of dimension k. The vectors in C are called codewords. A binary linear $[n, k]$-code where n is the length of the code and k is the dimension of the code is a vector subspace C of dimension k of the vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$. Similarly, a code over $\mathbb{F}_3$ is called a ternary code. The (Hamming) distance between two vectors $\mathbf{u}$ and $\mathbf{v}$ of $\mathbb{F}_q^n$, denoted as $d(\mathbf{u}, \mathbf{v})$, is the number of places in which they differ. For example if $C = \{000, 110, 011, 101\} \in \mathbb{F}_2^3$ then , $d(110, 011) = 2$ The hamming distance is a metric and must satisfy the following conditions for $\mathbf{u}, \mathbf{v}, \mathbf{w} \in C \subseteq \mathbb{F}_2^n$:

1. $d(\mathbf{u}, \mathbf{v}) \geq 0$.

2. $d(\mathbf{u}, \mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$.

3. $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u}) \ \forall \ \mathbf{u}, \mathbf{v}$.

4. $d(\mathbf{u}, \mathbf{v}) \leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$.

The minimum distance of the code C, denoted $d(C)$, is the smallest of the distances between two distinct codewords. That is

$$d(C) = \min\{d(\mathbf{u}, \mathbf{v}) | \mathbf{u}, \mathbf{v} \in C,\ \mathbf{u} \neq \mathbf{v}\}.$$

The (Hamming) weight denoted $wt(\mathbf{u})$ for a vector $\mathbf{u} \in \mathbb{F}_q^n$ is the number of nonzero coordinates in $\mathbf{u}$. The distance and weights of two codewords are related in the following way: if $\mathbf{u},\ \mathbf{v} \in \mathbb{F}_q^n$ then $d(\mathbf{u}, \mathbf{v}) = wt(\mathbf{u} - \mathbf{v})$ and if C is a linear code, the minimum distance d is the same as the minimum weight of the nonzero codewords of C.

A $k \times n$ matrix whose rows form a basis of a linear code $[n, k]$-code is called a generator matrix of the code two $k \times n$ matrices generate equivalent linear $[n, k]$-codes over $\mathbb{F}_q$ if one matrix can be obtained from the other by a sequence of operations of the following types:

(R1) Permutation of the rows.

(R2) Multiplication of a row by a non-zero scalar.

(R3) Addition of a scalar multiple of one row to another.

(C1) Permutations of the columns.

(C2) Multiplication of any column by a non-zero scalar.

If G is a generator matrix of an $[n, k]$-code, then by performing the operations described above, G can be transformed to the standard form

$$[I_k|A],$$

where I_k is the $k \times k$ identity matrix, and A is a $k \times (n - k)$ matrix.

2.2 Dual Codes

Given a linear $[n, k]$ code C, the dual code of C, denoted by $C^\perp$ is defined to be the set of those vectors of $\mathbb{F}_q^n$ which are orthogonal to every codeword of

C i.e. $C^{\perp} = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v} \cdot \mathbf{u} = 0, \ \forall \ \mathbf{u} \in C\}$. For example, the dual code for $C = \{000, 110, 011, 101\}$ is $C^{\perp} = \{000, 111\}$. A parity-check matrix H for an $[n, k]$-code C is a generator matrix of $C^{\perp}$. Thus H is an $(n-k) \times n$ matrix satisfying $GH^T = 0$ and if H is a parity-check matrix of C, then

$$C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H^T = 0\}.$$

If $G = [I_k|A]$ is the standard form generator matrix of an $[n, k]$-code C, then a parity-check matrix for C is $H = [-A|I_{n-k}]$. Also, a parity-check matrix H is said to be in standard form if $H = [B|I_{n-k}]$.

An important subcode of a linear code C is the hull of a linear code C which is defined to be hull$(C) = C \cap C^{\perp}$. A linear code C is said to be self-orthogonal provided $C \subseteq C^{\perp}$. As mentioned previously, there are two special cases of the hulls of linear codes. One is a self-dual code, which is defined for a linear code C provided $C = C^{\perp}$. The other is a linear code with a complementary dual (a LCD code) which is a linear code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = 0$, i.e. Hull$(C) = 0$.

2.3 Cyclic Codes

A linear code C of length n over $\mathbb{F}_q^n$ is said to be cyclic if $(c_0, c_1, ..., c_{n-1}) \in C$ implies $(c_{n-1}c_0, c_1, ..., c_{n-2}) \in C$. A codeword $(c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n$ can be represented as $c_0 + c_1x + ... + c_{n-1}x^{n-1} \in \frac{\mathbb{F}_q[X]}{(X^n-1)}$ by the following bijection

$$\mathbb{F}_q^n \to \frac{\mathbb{F}_q[X]}{(X^n-1)}$$

$$(c_0, c_1, ..., c_{n-1}) \to c_0 + c_1x + ... + c_{n-1}x^{n-1}$$

. Thus we may observe that:

$$c_0 + c_1x + ... + c_{n-1}x^{n-1} \in C \Rightarrow x(c_0 + c_1x + ... + c_{n-1}x^{n-1}) \in C$$

$$\Rightarrow c_{n-1} + c_0x + c_1x^2 + ... + c_{n-2}x^{n-1} \in C$$

which is equivalent to

$$(c_0, c_1, ..., c_{n-1}) \in C \Rightarrow (c_{n-1,}c_0, c_1, ..., c_{n-2}) \in C$$

For any $g(x) \in \frac{\mathbb{F}_q[X]}{(X^n-1)}$, the set $\langle g(x) \rangle$ is a cyclic code; it is called the code generated by $g(x)$.

Let C be a non-zero cyclic code in $\frac{\mathbb{F}_q[X]}{(X^n-1)}$. Then,

1. There exists a unique monic polynomial $g(x)$ of smallest degree in C,
2. $C = \langle g(x) \rangle$,
3. $g(x)$ is a factor $x^n - 1$.

In a non-zero cyclic code C the monic polynomial of least degree is called the generator polynomial of C. Any cyclic code C with generator polynomial

$$g(x) = g_0 + g_1x + ... + g_rx^r$$

of degree r with $\dim(C) = n - r$ then C has a generator matrix with the following form:

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & ..... & & g_r & 0 & 0.....0 \\ 0 & g_0 & g_1 & g_2 & ..... & & g_r & 0.....0 \\ 0 & 0 & g_0 & g_1 & g_2 & ..... & g_r & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & ..... & g_0 & g_1 & g_2 & ..... & g_r. \end{bmatrix}$$

2.4 Bounds for Linear Codes

Below are bounds on linear codes that will be used throughout this dissertation.

Sphere Packing Bound: (Hamming Bound)

$$B_q(n,d) \leq A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i} \quad \text{where} \quad t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

$A_q(n,d)$ denotes the maximum possible size of a q-ary code of length n and minimum Hamming distance d between elements of a code. $B_q(n,d)$ denotes the maximum possible size of a linear q-ary code of length n and minimum Hamming distance d between elements of a linear code.

Griesmer Bound: Let C be an $[n,k,d]$ code over $\mathbb{F}_q$ with $k \geq 1$ then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

CHAPTER 3

CLASSIFICATION OF CYCLIC LCD CODES OVER $\mathbb{Z}_4$

3.1 $\mathbb{Z}_4$ Linear Codes and Motivation

A linear code over $\mathbb{Z}_4$ of length n is a sub-module C of $\mathbb{Z}_4$-module $\mathbb{Z}_4^n$. A nonempty subset of $\mathbb{Z}_4^n$ is a $\mathbb{Z}_4$ cyclic code if and only if its image under the natural bijection

$$\mathbb{Z}_4^n \to \frac{\mathbb{Z}_4[X]}{(X^n - 1)}$$

is an ideal of $\frac{\mathbb{Z}_4[X]}{(X^n-1)}$.

Below is a description of the Gray map which relates codes over $\mathbb{Z}_4$ to codes over $\mathbb{F}_2$.

The Gray map is the map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ defined by:

- $\phi(0) = (0, 0)$
- $\phi(1) = (0, 1)$
- $\phi(2) = (1, 1)$
- $\phi(3) = (1, 0)$

The map ϕ is not an additive group homomorphism from $(\mathbb{Z}_4, +)$ to $(\mathbb{Z}_2^2, +)$ It is beneficial to introduce the following three maps α, β, γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ by the following table:

$x \in \mathbb{Z}_4$	$\alpha(x)$	$\beta(x)$	$\gamma(x)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

α is an additive group homomorphism from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ but β and γ are not. Each element of $x \in \mathbb{Z}_4$ has a binary expansion:

$$x = \alpha + 2\beta$$

ϕ can be extended to $\mathbb{Z}_4^n$ as follows:

$$\phi(x) = (\beta(x), \gamma(x)) \ \forall \ x \in \mathbb{Z}_4^n$$

The extended ϕ is a bijection from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. For any $x \in \mathbb{Z}_4^n$, $\phi(x)$ is called the binary image of x under ϕ. ([26])

The map ϕ can be used to map a linear code of length n over $\mathbb{Z}_4$ to a (non-linear) code of length $2n$ over $\mathbb{F}_2$ (which is just a subset of $\mathbb{F}_2^{2n}$ with good word distance properties). The existence of such codes over $\mathbb{F}_2$ was known, but no one was able to explain why the codes have good distance properties even though they are not linear. Eventually it was discovered that the codes are images under the Gray map of linear codes over $\mathbb{Z}_4$. From that moment on, linear codes over $\mathbb{Z}_4$, and other commutative rings, became very important, especially over finite chain rings (for example, $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ that we are going to examine). Before that, only codes over fields were used. In [27] Massey and Yang provided the following result:

Theorem 3.1. *[27] If $g(x)$ is the generator polynomial of a q-ary (n, k) cyclic code*

C of block length n, then C is an LCD code if and only if $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in $x^n - 1$.

This theorem provides a condition for when cyclic codes over a field are LCD codes. We will classify cyclic LCD codes over $\mathbb{Z}_4$.

Denote $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ the ring of residues modulo n. The group of invertible elements of this ring is denotes by $\mathbb{Z}_n^*$ and the order of an element $k \in \mathbb{Z}_n^*$ is denoted by $\text{ord}_{\mathbb{Z}_n^*}(k)$. For the sake of notational convenience we will later assume that $\text{ord}_{\mathbb{Z}_1^*}(2)$ means $\text{ord}_{\mathbb{Z}_1^*}(2(\text{mod } 1))$, which is equal to 1. We denote by $\varphi(n)$ the Euler function. We will also use the following two functions for n odd: $\gamma_2(n) = \frac{\varphi(n)}{\text{ord}_{\mathbb{Z}_n^*}(2)}$ and $\beta_2(n) = \frac{\varphi(n)}{2\text{ord}_{\mathbb{Z}_n^*}(2)}$.

If R is a commutative ring, the cyclic codes over R of length N are the ideals of the quotient ring $\frac{R[X]}{(X^N-1)}$. We denote the elements of $R[X]$ by $f(X)$, or shortly by f, while the elements of $\frac{R[X]}{(X^N-1)}$ are denoted by $f(x)$ (so that $x = X + (X^N - 1)$) and $f(x) = f(X) + (X^N - 1)$).

Definition 3.2. Let $f(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + X^n$ be a monic polynomial in $\mathbb{Z}_4[X]$ whose constant term a_0 is a unit in $\mathbb{Z}_4$. The reciprocal polynomial f^* of f is defined by

$$f^*(X) = a_0^{-1}X^{\deg(f)}f(\frac{1}{X}).$$

Clearly $(f^*)^* = f$ and $(fg)^* = f^*g^*$ if g is another monic polynomial in $\mathbb{Z}_4[X]$ with unit constant term. A monic polynomial $f \in \mathbb{Z}_4[X]$ with unit constant term is said to be self reciprocal if $f = f^*$. Otherwise the pair (f, f^*) is called a reciprocal pair. For a positive integer N we say that the pair $(N, 2)$ is good if $N \mid (2^k + 1)$ for some natural number k. Otherwise we say the pair $(N, 2)$ is bad. Also, for an odd positive integer N the polynomial $X^N - 1 \in \mathbb{Z}_4[X]$ can be decomposed in $\mathbb{Z}_4[X]$

into a product of monic irreducible factors in the following way:

$$X^N - 1 = \prod_{\substack{n|N \\ (n,2) \text{ good}}} \left(\prod_{i=1}^{\gamma_2(n)} g_{i,n} \right) \prod_{\substack{n|N \\ (n,2) \text{ bad}}} \left(\prod_{i=1}^{\beta_2(n)} f_{i,n} f_{i,n}^* \right),$$

where the polynomials $g_{i,n}$ are self-reciprocal and the pairs $(f_{i,n}, f_{i,n}^*)$ are reciprocal pairs in (3.1).

This decomposition is unique up to the order of factors, and the polynomials that appear on the right hand side are pairwise relatively prime and basic irreducible. Moreover, any monic factor g of $X^N - 1$ factors uniquely (up to the order of factors) into a product of monic irreducible polynomials in $\mathbb{Z}_4[X]$ and those monic irreducible are from the set

$$\text{Fact}(X^N - 1) = \{g_{i,n}, f_{i,n}, f_{i,n}^* |\ i, n\}.$$

Where $\text{Fact}(g)$ denotes the set of monic irreducible factors of g that appear in the decomposition. Thus, $\text{Fact}(g) \subset \text{Fact}(X^N - 1)$.

Theorem 3.3. *[2, Theorem 6] For every cyclic code C over $\mathbb{Z}_4$ of odd length N there are unique monic polynomials $f(X), g(X),$ and $h(X)$ in $\mathbb{Z}_4[X]$ such that $X^N - 1 = f(X)g(X)h(X)$ and $C = (f(x)g(x), 2f(x))$.*

Theorem 3.4. *[18, Theorem 3.2] Let $C = (f(x)g(x), 2f(x))$ be a cyclic code over $\mathbb{Z}_4$ of odd length N, where $f(X), g(X),$ and $h(X)$ are monic divisors of $X^N - 1$ in $\mathbb{Z}_4[X]$ such that $X^N - 1 = f(X)g(X)h(X)$.*

Then,

$$|Hull(C)| = 4^{deg(H(X))} 2^{deg(G(X))},$$

where G and H are monic polynomials from $\mathbb{Z}_4[X]$ defined by

$$H(X) = gcd(h(X), f^*(X)),$$

and

$$G(X) = \frac{X^N - 1}{gcd(h(X), f^*(X)) \cdot lcm(f(X), h^*(X))}.$$

3.2 Results

The next theorem is the necessary and sufficient condition for a cyclic code over $\mathbb{Z}_4$ of odd length to have a complementary dual.

Theorem 3.5. *[10, Theorem 2.1] A cyclic code C over $\mathbb{Z}_4$ of odd length N is an LCD code if and only if $C = (f(x))$, where $f(X)$ is a self-reciprocal monic divisor of $X^N - 1 \in \mathbb{Z}_4[X]$.*

Proof. Let C be a cyclic code over $\mathbb{Z}_4$ of odd length N. Suppose that C is an LCD code. It follows from Theorem 3.3 and Theorem 3.4 that there are unique polynomials $f(X)$,$g(X)$,$h(X)$ in $\mathbb{Z}_4[X]$ such that $C = (f(x)g(x), 2f(x))$ with the following conditions satisfied:

$$f(X)g(X)h(X) = X^N - 1 \tag{3.1}$$

$$f, g, h \text{ are pairwise relatively prime} \tag{3.2}$$

$$\gcd(h(X), f^*(X)) = 1 \tag{3.3}$$

$$\mathrm{lcm}(f(X), h^*(X)) = X^N - 1 \tag{3.4}$$

It follows from (3.3) that

$$\gcd(f(X), h^*(X)) = 1$$

which, together with (3.4) implies the relations

$$\mathrm{Fact}(f) \cap \mathrm{Fact}(h^*) = \emptyset \tag{3.5}$$

$$\mathrm{Fact}(f) \cap \mathrm{Fact}(h^*) = \mathrm{Fact}(X^N - 1) \tag{3.6}$$

The conditions (3.1) and (3.2) can be reformulated as

$$\mathrm{Fact}(f) \cup \mathrm{Fact}(g) \cup \mathrm{Fact}(h) = \mathrm{Fact}(X^N - 1) \tag{3.7}$$

$$\mathrm{Fact}(f), \mathrm{Fact}(g), \mathrm{Fact}(h) \text{ are pairwise disjoint.} \tag{3.8}$$

Now from (3.5), (3.6), (3.7), and (3.8) we can conclude that

$$\mathrm{Fact}(h^*) = \mathrm{Fact}(g) \cup \mathrm{Fact}(h) \tag{3.9}$$

Since Fact(g) and Fact(h) are disjoint, Fact(h) and Fact(h^*) have the same number of elements, we conclude that

$$\mathrm{Fact}(g) = \emptyset, \tag{3.10}$$

or, equivalently, that

$$g = 1. \tag{3.11}$$

Then (3.9) and (3.10) imply that h is self-reciprocal, and, since, due to (3.11), $X^N - 1 = f(X)h(X)$ we have f is also self-reciprocal. Again using (3.11) we have $C = (f(x)g(x), 2f(x)) = (f(x), 2f(x)) = (f(x))$. Conversely, let $C = (f(x))$, where $f(X)$ is a monic self-reciprocal divisor of $X^N - 1$ in $\mathbb{Z}_4$. Then $g(X) = 1$ and $h(X) = \frac{X^N-1}{f(X)}$ are the unique monic divisors of $X^N - 1$ such that $f(X)g(X)h(X) = X^N - 1$ and $C = (f(x)g(x), 2f(x))$. Since $f(X)$ and $h(X)$ are relatively prime and self-reciprocal. By Theorem 3.4 we have $H(X) = 1$ and $G(X) = 1$. Hence $|\mathrm{Hull}(C)| = 1$, i.e., C is an LCD code. □

Corollary 3.6. [10, Corollary 2.3] Let N be an odd positive integer. The number of cyclic LCD codes of length N over $\mathbb{Z}_4$ is 2^{nmsrf}, where

$$\mathrm{nmsrf} = \sum_{\substack{n|N \\ (n,2) \text{ good}}} \frac{\varphi(n)}{\mathrm{ord}_{\mathbb{Z}_n^*}(2)} + \frac{1}{2} \sum_{\substack{n|N \\ (n,2) \text{ bad}}} \frac{\varphi(n)}{\mathrm{ord}_{\mathbb{Z}_n^*}(2)}.$$

where “nmsrf” stands for “number of minimal self-reciprocal factors”.

3.3 Examples

3.3.1 Classification of All Cyclic LCD Codes Over $\mathbb{Z}_4$ of Length 7

The monic irreducible factorization of $X^7 - 1 \in \mathbb{Z}_4[X]$ is given by

$$X^7 - 1 = (X - 1)(X^3 + 2X^2 + X - 1)(X^3 - X^2 + 2X - 1).$$

The divisors of $N = 7$ are 1 and 7, where $(1, 2)$ is a good pair and $(7, 2)$ is a bad pair. Thus the notation of the above factors of $X^7 - 1$ in accordance with [18] is: $g_{1,1} = X - 1$, $f_{1,7} = X^3 + 2X^2 + X - 1$, and $f^*_{1,7} = X^3 - X^2 + 2X - 1$. By Theorem 3.5 we have the following list of all cyclic LCD codes of length 7 over $\mathbb{Z}_4$:

- $C = (1)$
- $C = (g_{1,1}(x))$
- $C = (f_{1,7}(x)f^*_{1,7}(x))$
- $C = (0)$

3.3.2 Classification of All Cyclic LCD Codes Over $\mathbb{Z}_4$ of Length 15

The monic irreducible factorization of $X^{15} - 1 \in \mathbb{Z}_4[X]$ is given by

$$X^{15}-1 = (X-1)(X^2+X+1)(X^4-X^3+2X^2+1)(X^4+2X^2-X+1)(X^4+X^3+X^2+X+1).$$

The divisors of 15 are 1, 3, 5 and 15, where $(1,2)$, $(3,2)$ and $(5,2)$ are good pairs and $(15,2)$ is a bad pair. Thus the notation of the above factors of $X^{15} - 1$ in accordance with [18] is: $g_{1,1} = X-1$, $g_{1,3} = X^2+X+1$, $g_{1,5} = X^4+X^3+X^2+X+1$, $f_{1,15} = X^4 - X^3 + 2X^2 + 1$, and $f^*_{1,15} = X^4 + 2X^2 - X + 1$. By Theorem 3.5 we have the following list of all cyclic LCD codes of length 15 over $\mathbb{Z}_4$:

- $C = (1)$
- $C = (g_{1,1}(x))$
- $C = (g_{1,3}(x))$
- $C = (g_{1,5}(x))$
- $C = (f_{1,15}(x)f^*_{1,15}(x))$
- $C = (g_{1,1}(x))(g_{1,3}(x))$
- $C = (g_{1,1}(x))(g_{1,5}(x))$
- $C = (g_{1,3}(x))(g_{1,5}(x))$
- $C = (g_{1,1}(x))(g_{1,3}(x))(g_{1,5}(x))$
- $C = (g_{1,1}(x))(f_{1,15}(x)f^*_{1,15}(x))$
- $C = (g_{1,3}(x))(f_{1,15}(x)f^*_{1,15}(x))$
- $C = (g_{1,5}(x))(f_{1,15}(x)f^*_{1,15}(x))$
- $C = (g_{1,1}(x))(g_{1,3}(x))(f_{1,15}(x)f^*_{1,15}(x))$
- $C = (g_{1,1}(x))(g_{1,5}(x))(f_{1,15}(x)f^*_{1,15}(x))$
- $C = (g_{1,3}(x))(g_{1,5}(x))(f_{1,15}(x)f^*_{1,15}(x))$
- $C = (0)$

CHAPTER 4

CLASSIFICATION OF CYCLIC LCD CODES OVER $R = \big(R, (\gamma), \kappa\big)$ WITH $\nu(\gamma) = 2$

4.1 Preliminaries

As previously mentioned $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{Z}_4$ are special cases of finite chain rings. The ring $A = \frac{\mathbb{F}_2[X]}{(X^2)} = \mathbb{F}_2[u] = \mathbb{F}_2 + u\mathbb{F}_2$, where $u = X + (X^2)$, so that $A = \{a+bu \ : \ a, b \in \mathbb{F}_2\} = \{0, 1, u, 1+u\}$ is known as the ring of dual numbers over $\mathbb{F}_2$ (note: $u^2 = 0$). The ring A is a chain ring with the ideals $A \supseteq \{0, u\} \supseteq \{0\}$. It is one of the four commutative rings with four elements: $\mathbb{F}_2 \times \mathbb{F}_2, \mathbb{F}_4, \mathbb{Z}_4, A = \mathbb{F}_2 + u\mathbb{F}_2$. The units in A are 1 and $1+u$ and the ideals of A are $(0) = \{0\}$, $(1) = (1+u) = A$, and $(1) = \{0, u\}$. A is a local ring $\big($i.e. has unique maximal ideal, namely $(u)\big)$. The maximal ideal $\mathfrak{m} = (u)$ has nilpotency index 2 as $(u)^2 = (u^2) = (0)$. The ring A is of characteristic 2, i.e., $x + x = 0$ for every $x \in A$. A is an extension of the field $\mathbb{F}_2$, as the elements $0, 1$ from A form a subfield $\mathbb{F}_2$ of the ring A and $A/\mathfrak{m} \cong \mathbb{F}_2$ (the residue field of A). The natural map $\pi : A \to A/\mathfrak{m} \cong \mathbb{F}_2$ is given by

$$\pi(0) = 0,\ \pi(1) = 1,\ \pi(u) = 0,\ \pi(1+u) = 1.$$

Let $C \subseteq A^n$ be a linear code over $A = \mathbb{F}_2 + u\mathbb{F}_2$. Then $\overline{C} = \{\overline{\mathbf{w}} = \overline{w_1 w_2} \ldots \overline{w_n} | \mathbf{w} = w_1 w_2 \ldots w_n\}$ will be the projection of C onto a code over $\overline{A}^n = \mathbb{F}_2^n$. The projection is a map $\pi : C \to \mathbb{F}_2^n$. The same notation π is used for the projection $\pi : A = \mathbb{F}_2 + u\mathbb{F}_2 \to \mathbb{F}_2$, as well as for $\pi : A^n \to \mathbb{F}_2^n$.

If R is a finite chain ring and $\mathfrak{m} = (\gamma)$ its maximal ideal, are elements of $\mathfrak{m}$ are nilpotent and $R^* = R \setminus \mathfrak{m}$. The notation $R = (R, \mathfrak{m}, \kappa)$ means that R is a local ring with maximal ideal $\mathfrak{m}$ and residue field $\kappa = \frac{R}{\mathfrak{m}}$. The notation $(R, \mathfrak{m})$ is used when there is no need to specify κ The phrase "finite chain ring $(R, (\gamma), \kappa)$ or $(R, (\gamma))$" means that the maximal ideal of R is generated by γ and $\kappa = \frac{R}{(\gamma)}$. The rings $\mathbb{Z}_4$ and $A = \mathbb{F}_2 + u\mathbb{F}_2$ are examples of finite chain rings $(R, (\gamma))$ with $\nu(\gamma) = 2$. where $\nu(\gamma)$ denotes the index of nilpotency of γ. Similar to the previously mentioned projection the following can be defined for codes over $R = (R, \mathfrak{m}, \kappa)$. Let $C \subseteq R^n$ be a linear code over R. Then $\overline{C} = \{\overline{\mathbf{w}} = \overline{w_1 w_2} \dots \overline{w_n} | \mathbf{w} = w_1 w_2 \dots w_n\}$ will be the projection of C onto a code over $\overline{R}^n = \kappa^n$. The projection is a map $\pi : C \to \kappa^n$. The same notation π is used for the projection $\pi : R \to \kappa$, as well as for $\pi : R^n \to \kappa^n$.
The following theorem describes the unique factorization of a polynomial in $R[X]$ and will be used throughout the rest of this chapter.

Theorem 4.1. *([22, Theorem 4.4]) Suppose $N \geq 1$ is an integer that char$(\kappa) \nmid N$. Then for every ideal I of R_n there exists two unique monic polynomials $f_0(X)$ and $f_1(X)$ from $R[X]$ with $f_1(X)|f_0(X)|X^N - 1$ such that $I = \big(f_0(x), \gamma f_1(x)\big)$.*

We will now define a reciprocal polynomial over R in the same we way we previously defined a reciprocal polynomial over $\mathbb{Z}_4$.

Definition 4.2. Let $f(X) = a_0 + a_1 X + ... + a_{n-1}X^{n-1} + X^n$ be a monic polynomial in R whose constant term a_0 is a unit in R. The reciprocal polynomial f^* of f is defined by

$$f^*(X) = a_0^{-1} X^{\deg(f)} f(\frac{1}{X}).$$

The following is the monic version of Hensel's Lemma which shows how one can get from a factorization in $\kappa[X]$ to a factorization in $R[X]$.

Corollary 4.3. [22, Theorem 2.6] Let $R = \big(R, \mathfrak{m}, \kappa\big)$ be a finite local ring and $f \in$

$R[X]$ be a monic polynomial. Assume there are $g_1, g_2, \dots, g_k \in \kappa[X]$ monic, pairwise relatively prime and such that $\overline{f} = g_1 g_2 \cdots g_k$. Then there are $f_1, f_2, \dots, f_k \in R[X]$ monic, pairwise relatively prime, such that $f = f_1 f_2 \cdots f_k$ and $\overline{f_i} = g_i$ for $i = 1, 2, \dots k$.

4.2 Results

From this point forward we will use the following standing assumptions:

1. $R = (R, \mathfrak{m} = (\gamma), \kappa = \frac{R}{\mathfrak{m}})$ is a finite chain ring with $\nu(\gamma) = 2$.
2. $N \geq 1$ is an integer such that $\operatorname{char}(\kappa) \nmid N$.
3. $R_n = \frac{R[X]}{X^N - 1}$ and $\kappa_n = \frac{\kappa[X]}{X^N - 1}$.

Theorem 4.4. *For every cyclic code C over R of length N there are unique, monic, pairwise coprime polynomials $f(X)$, $g(X)$, and $h(X)$ in $R[X]$ such that $X^N - 1 = f(X)g(X)h(X)$ and $C = \big(f(x)g(x), \gamma f(x)\big)$.*

Proof. By Theorem 4.1, there are unique monic polynomials $f_0(X)$ and $f_1(X)$ in $R[X]$ such that $f_1(X) | f_0(X) | x^N - 1$ and $C = \big(f_0(x), \gamma f_1(x)\big)$. Let $f_0(X) = f_1(X)g_1(X)$ and $h_1(X) = \frac{X^N - 1}{f_0(X)} = \frac{X^N - 1}{f_1(X)g_1(X)}$. Then f_1, g_1 and h_1 are monic, pairwise coprime polynomials (since the assumed condition $\operatorname{char}(\kappa) \nmid N$) such that $X^N - 1 = f_1(X)g_1(X)h_1(X)$ and $C = \big(f_1(x)g_1(x), \gamma f_1(x)$. The polynomials f_1, g_1 and h_1 are unique, otherwise the pair f_0, f_1 from [22, Theorem 4.4], would not be unique. Replacing the notation f_1, g_1 and h_1 by f, g and h we get the statement of the theorem. □

Proposition 4.5. The polynomial $f = X^N - 1 \in R[X]$ has a unique decomposition into distinct monic basic irreducible factors in $R[X]$.

Proof. Since $\text{char}(\kappa) \nmid N$, $\overline{f} = X^N - 1 \in \kappa[X]$ is square free in $\kappa[X]$ hence by [22, Theorem 2.7], $\overline{f} = X^N - 1 \in R[X]$ factors uniquely into monic pairwise coprime basic irreducibles. □

We will denote the set of all monic pairwise coprime basic irreducibles into which $X^N - 1 \in R[X]$ factors in $R[X]$ by $\text{Fact}(X^N - 1)$.

Proposition 4.6. Any monic factor $g(X)$ of $X^N - 1 \in R[X]$ factors uniquely (up to the order of factors) into a product of monic pairwise coprime basic irreducible polynomials from $R[X]$ and those monic irreducibles are from the set $\text{Fact}(X^N - 1)$.

Proof. Since $X^N - 1 \in \kappa[X]$ is square-free, $\bar{g}(X) \in \kappa[X]$ is also square-free. Now the statement follows from [22, Theorem 2.7], and Proposition 4.7. □

Proposition 4.7. [17, Pages 5-6] The polynomial $X^N - 1 \in \mathbb{F}_q[X]$ can be decomposed in $\mathbb{F}_q[X]$ into a product of monic irreducible factors in the following way:

$$X^N - 1 = h_1(X) \dots h_s(X) k_1(X) k_1^*(X) \dots k_t(X) k_t^*(X), \tag{4.1}$$

where the polynomials $h_i(X)$ are self-reciprocal and the pairs $\big(k_j(X), k_j^*(X)\big)$ are reciprocal pairs. This decomposition is unique on the right-hand side of the above equality are pairwise coprime.

Proposition 4.8. Let $\kappa = \mathbb{F}_q$. Taking into account Proposition 4.7, the polynomial $X^N - 1 \in R[X]$ can be decomposed in $R[X]$ into a product of monic, basic irreducible factors in the following way:

$$X^N - 1 = g_1(X) \dots g_s(X) f_1(X) f_1^*(X) \dots f_t(X) f_t^*(X), \tag{4.2}$$

where the polynomials $g_i(X)$ are self-reciprocal, the pairs $\big(f_j(X), f_j^*(X)\big)$ are reciprocal pairs, and $\bar{g_i} = h_i$, $\bar{f_i} = k_i$, $\bar{f_i^*} = k_i^*$. The decomposition of $X^N - 1$ into monic basic irreducible is unique up to the order of the factors and the polynomials that appear on the right-hand side the above equality are pairwise coprime.

Proof. The decomposition (4.2) can be obtained by the Hensel lifting, given by Corollary 4.3, of the decomposition (4.1). The uniqueness follows from Proposition 4.5. The uniqueness, together with Proposition 4.9, implies that the polynomials g_j are self-reciprocal and that the pairs $\big(f_j(X), f_j^*(X)\big)$ are reciprocal pairs. The pairwise coprimeness in (4.2) follows from the pairwise coprimeness in (4.1).

□

Proposition 4.9. Let $f \in R[X]$ be a monic polynomial with an invertible constant term. Then $\overline{f^*} = \overline{f}^*$

Proof. Let $f = a_0 + a_1X \cdots + a_{n-1}X^{n-1} + X^N$. Then
$\overline{f^*} = \overline{a_0^{-1}(1 + a_{n-1}X + \cdots + a_1X^{n-1} + X^n)} = \overline{a_0^{-1}(1 + \overline{a_{n-1}}X + \cdots + \overline{a_1}X^{n-1} + \overline{a_0}X))}$.
On the other side, $\overline{f}^* = (\overline{a_0} + \overline{a_1}X + \cdots + \overline{a_{n-1}}X^{n-1} + X^n)^* = \overline{a_0}^{-1}(1 + \overline{a_{n-1}}X + \cdots + \overline{a_1}X^{n-1} + \overline{a_0}X) = \overline{a_0^{-1}}(1 + \overline{a_{n-1}}X + \cdots + \overline{a_1}X^{n-1} + \overline{a_0}X)$. □

We will denote by $\mathrm{Fact}(g)$ the set of monic basic irreducible factors of g that appears in the decomposition from Proposition 4.6. Note that here g is a monic factor of $X^N - 1 \in R[X]$.

Lemma 4.10. Let $p(X)$ and $q(X)$ be two polynomials in $R[X]$ monic divisors of $X^N - 1$. Suppose that $p(X)q(X) = 0$ and let $q'(X) = \frac{X^N-1}{q(X)}$. Then $q'(X)|p(X)$.

Proof. The condition $p(X)q(X) = 0$ implies $p(X)q(X) \in (X^N - 1)$, hence $p(X)q(X) = t(X)(X^N - 1)$ for some $t(X)$. Hence $p(X)q(X) = t(X)q(X)q'(X)$, which implies $q(X)\big(p(X) - t(X)q'(X)\big) = 0$. Since $q(X)$ is monic, it is a regular element of $R[X]$, so that $p(X) - t(X)q'(X) = 0$. Hence $q'(X)|p(X)$. □

Lemma 4.11. [18, Lemma 3.1] Let $\mathbf{u} = (u_0, u_1, \ldots, u_{N-1})$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{N-1})$ be vectors in R^N with corresponding polynomials $u(X)$ and $v(X)$. Then $\mathbf{u}$ is orthogonal to $\mathbf{v}$ and all its shifts if and only if $u(x)v^*(x) = 0$ in R_N.

Lemma 4.12. Let $a(X)$, $b(X)$ be monic divisors of $X^N - 1$ in $R[X]$. Then

$$X^N - 1 = \mathrm{lcm}\big(a(X), b(X)\big) \cdot \mathrm{gcd}\big(\frac{X^N-1}{a(X)}, \frac{X^N-1}{b(X)}\big).$$

Proof. The statement follows from the relation

$\mathrm{Fact}(a) \cup \mathrm{Fact}(b) \cup \big(\mathrm{Fact}(X^N-1) \setminus \mathrm{Fact}(a)\big) \cap \big(\mathrm{Fact}(X^N-1) \setminus \mathrm{Fact}(b)\big)$

$= \mathrm{Fact}(X^N-1)$. □

Corollary 4.13. Let $f(X)$, $g(X)$ and $h(X)$ be monic divisors of $X^N - 1$ in $R[X]$ such that $f(X)g(X)h(X) = X^N - 1$. Then:

$$X^N - 1 = \mathrm{lcm}\big(f(X)g(X), h^*(X)g^*(X)\big) \cdot \mathrm{gcd}\big(h(X), f^*(X)\big)$$

and

$$\frac{\mathrm{lcm}\big(f(X)g(X), h^*(X)g^*(X)\big)}{\mathrm{lcm}\big(f(X), h^*(X)\big)} = \frac{X^N - 1}{\mathrm{gcd}\big(h(X), f^*(X)\big) \cdot \mathrm{lcm}\big(f(X), h^*(X)\big)}.$$

Proof. The first relation follows from Lemma 4.11 since $f(X)g(X)h(X) = X^N - 1$ and $f^*(X)g^*(X)h^*(X) = X^N - 1$, The second relation follows from the first relation. □

The following theorem extends [18, Theorem 3.2] from cyclic codes over $\mathbb{Z}_4$ to cyclic codes over R.

Theorem 4.14. *Let $C = \big(f(x)g(x), \gamma f(x)\big)$ be a cyclic code over R of length N, where $f(xX)$, $g(X)$ are monic divisors of X^N-1 in $R[X]$ such that $f(X)g(X)h(X) = X^N - 1$. Then*

$$Hull(C) = \big(lcm\big(f(X)g(X), h^*(X)g^*(X)\big)\ ,\ \gamma\ lcm\big(f(X), h^*(X)\big)\big)$$

Furthermore,

$$|Hull(C)| = 4^{deg(H(X))}2^{deg(G(X))},$$

where

$$H(X) = gcd\big(h(X), f^*(X)\big)$$

and

$$G(X) = \frac{X^N - 1}{gcd\big(h(X), f^*(X)\big)\, lcm\big(f(X), h^*(X)\big)}.$$

Proof. By [22, Theorem 4.9], we have

$$C^\perp = \big(h^*(x)g^*(x), \gamma h^*(x)\big).$$

Let C' be a cyclic code of length N over R give by

$$C' = \big(F(x)G(x), \gamma F(x)\big),$$

where

$$F(X) = \mathrm{lcm}\big(f(X), h^*(X)$$

and by Lemma 4.12 and Corollary 4.13 we have that

$$G(X) = \frac{\big(\mathrm{lcm}\big(f(X)g(X), h^*(X)g^*(X)\big)}{\mathrm{lcm}\big(f(X), h^*(X)\big)} = \frac{X^N - 1}{\mathrm{gcd}\big(h(X), f^*(X)\big) \cdot \mathrm{lcm}\big(f(X), h^*(X)\big)},$$

and

$$H(X) = \frac{X^N - 1}{\big(\mathrm{lcm}\big(f(X)g(X), h^*(X)g^*(X)\big)} = \mathrm{gcd}\big(h(X), f^*(X)\big)$$

.

The polynomials $F(X)$, $G(X)$ and $H(X)$ are monic pairwise coprime and $X^N - 1 = F(X)G(X)H(X)$. since

$$\big(F(x)G(x), \gamma F(x)\big) \subseteq \big(f(x)g(x), \gamma f(x)\big)$$

and

$$\big(F(x)G(x), \gamma F(x)\big) \subseteq \big(h^*(x)g^*(x), \gamma h^*(x)\big)$$

we have

$$C' \subseteq \mathrm{Hull}(C).$$

Now the opposite inclusion is shown. Since Hull(C) is a cyclic code of length N over R, we have

$$C' = \big(A(x)B(x), \gamma A(x)\big),$$

where $A(X)$, $B(X)$ and $C(X)$ are pairwise coprime polynomials in $R[X]$ such that $A(X)B(X)C(X) = X^N - 1$. Since Hull(C) $\subseteq C^{\perp}$ is orthogonal to C, by Lemma 4.11, we have

$$A(X)B(X) \cdot \gamma f^*(X) = 0$$

and

$$\gamma A(X) \cdot f^*(X)g^*(X) = 0$$

which implies by Lemma 4.10 that

$$h^*(X)g^*(X)|A(X)B(X)$$

and

$$h^*(X)|A(X).$$

Similarly, Hull(C) $\subseteq C$ is orthogonal to $C^{\perp}$ which implies by Lemma 4.11 that

$$A(X)B(X) \cdot \gamma h(X) = 0$$

and

$$\gamma A(X) \cdot h(X)g(X) = 0$$

It follows By Lemma 4.10 that

$$f(X)g(X)|A(X)B(X)$$

and

$$f(X)|A(X)$$

Consequently,

$$\mathrm{lcm}\big(f(X)g(X),h^*(X)g^*(X)\big)\ (|A(X)B(X))$$

and

$$\mathrm{lcm}\big(h^*(X),f(X)\big)|A(X)$$

which implies that

$$F(X)H(X)|A(X)B(X)$$

and

$$F(X)|A(X).$$

Hence $\mathrm{Hull}(C)\subseteq C'$. Therefore $\mathrm{Hull}(C)=C'$

Assuming that

$$f_0(X)=\mathrm{lcm}\big(f(X)g(X),h(X)^*g(X)^*\big)$$

and

$$f_1(X)=\mathrm{lcm}\big(f(X)g^*(X)\big)$$

it follows from [22, Theorem 4.5], that $|\mathrm{Hull}(C)|=4^{\deg(H(X))}2^{\deg(G(X))}$ as

$$H(X)=\frac{X^N-1}{f_0(X)}$$

such that

$$\deg(H(X))=N-\deg(f_0(X)),$$

and

$$G(X)=\frac{f_0(X)}{f_1(X)}$$

so that

$$\deg(G(X))=\deg(f_0(X))-\deg(f_1(X))$$

□

The following is the condition for a cyclic code over R to be an LCD code and extends the result of [27] and our results in [10].

Theorem 4.15. *A cyclic code C over R of length N is an LCD code if and only if $C = \big(f(x)\big)$, where $f(X)$ is a self-reciprocal monic divisor of $X^N - 1$ in $R[X]$.*

We now provided two proofs for the above theorem.

Proof. (First Proof) Let C be a cyclic code over R of length N. Suppose that C is an LCD code. It follows from Theorem 4.1 and Theorem 4.14 that there are unique polynomials $f(X)$, $g(X)$, $h(X)$ in $R[X]$ such that $C = \big(f(x)g(x), \gamma f(x)\big)$ with the following conditions satisfied:

$$f(X)g(X)h(X) = X^N - 1 \tag{4.3}$$

$$f, g, h \ \text{ are pairwise coprime} \tag{4.4}$$

$$\gcd(h(X), f^*(X)) = 1 \tag{4.5}$$

$$\operatorname{lcm}(f(X), h^*(X)) = X^N - 1 \tag{4.6}$$

The relations (4.5), respectively (4.6), are true because $H(X) = 1$, respectively, $G(X) = 1$, in the formula for $|\text{Hull}(C)|$ in Theorem 5.14. It follows from (4.5) that:

$$\gcd(f(X), h^*(X)) = 1$$

which, together with (4.6) implies then following relations:

$$\text{Fact}(f) \cap \text{Fact}(h^*) = \emptyset \tag{4.7}$$

$$\mathrm{Fact}(f) \cup \mathrm{Fact}(h^*) = \mathrm{Fact}(X^N - 1). \tag{4.8}$$

The conditions (4.3) and (4.4) can be reformulated as

$$\mathrm{Fact}(f) \cup \mathrm{Fact}(g) \cup \mathrm{Fact}(h) = \mathrm{Fact}(X^N - 1) \tag{4.9}$$

$$\mathrm{Fact}(f),\ \mathrm{Fact}(g),\ \mathrm{Fact}(h) \text{ are pairwise disjoint.} \tag{4.10}$$

Now from (4.7), (4.8), (4.9), and (4.10) we can conclude that

$$\mathrm{Fact}(h^*) = \mathrm{Fact}(g) \cup \mathrm{Fact}(h) \tag{4.11}$$

Since Fact(g) and Fact(h) are disjoint, Fact(h) and Fact(h^*) have the same number of elements, we conclude that

$$\mathrm{Fact}(g) = \emptyset, \tag{4.12}$$

or, equivalently, that

$$g = 1. \tag{4.13}$$

Then (4.11) and (4.12) imply that h is self-reciprocal, and, since due to (4.13) $X^N - 1 = f(X)h(X)$ we have f is also self-reciprocal.

Also again using (4.13), we have $C = (f(x)g(x), \gamma f(x)) = (f(x), \gamma f(x)) = (f(x))$ Conversely, let $C = (f(x))$, where $f(X)$ is a monic self-reciprocal divisor of $X^N - 1$ in $R[X]$. Then $g(X) = 1$ and $h(X) = \frac{X^N-1}{f(X)}$ are the unique monic divisors of $X^N - 1$ such that $f(X)g(X)h(X) = X^N - 1$ and $C = (f(x)g(x), \gamma f(x))$. Since

$f(X)$ and $h(X)$ are relatively prime and self-reciprocal, then in Theorem 4.13 we have $H(X) = 1$ and $G(X) = 1$. Hence, by Theorem 4.13, $|\text{Hull}(C)| = 1$, i.e., C is an LCD code. □

For the second proof we will need the following definitions:

Definition 4.16. C is a free code if it is a free R-module. In other words, if C has a basis.

Definition 4.17. Let C be a linear code over R. Define a linear code $(C : \gamma) = \{\mathbf{w} \in R^n : \gamma\mathbf{w} \in C\}$.

Definition 4.18. Let

$$k_0(C) = \dim_\kappa \overline{C},$$

$$k_1(C) = \dim_\kappa \overline{(C : \gamma)} - \dim_\kappa \overline{C}.$$

We say C is of type $\big(k_0(C), k_1(C)\big)$ and $k(C) = k_0(C) + k_1(C)$.

Proof. (Second Proof) Suppose that C is an LCD cyclic code of length N over R. Then by [7, Proposition 4.1]. C is free. Let $C = \big(f(x)g(x), \gamma f(x)\big)$ for some monic divisors f, g, and h of $X^N - 1$ in $R[X]$ such that $f(X)g(X)h(X) = X^N - 1$. Assuming that $f_0 = fg$ and $f_1 = f$, we have by [22, Theorem 4.5], that $k_0(C) = n - \deg(f_0) = \deg(h)$ and $k_1(C) = n - \deg(f_0) - \deg(f_1) = \deg(g)$. By [22, Proposition 3.13], C is free if and only if $k_1(C) = 0$, i.e., if and only if $g = 1$. Hence $C = \big(f(x), \gamma f(x)\big) = \big(f(x)\big)$. It remains to show that f is self-reciprocal. Note that by Theorem 4.14 that when $g = 1$, then

$$\text{Hull}(C) = \big(\text{lcm}(f, h^*)\big)$$

and we need to see when is $\big(\text{lcm}(f, h^*)\big) = X^N - 1$, i.e., $\text{Hull}(C) = \big(0\big)$. Taking into account Proposition 4.8 and the fact that f and h are pairwise coprime monic divisors of $X^N - 1$ such that $f(X)h(X) = X^N - 1$. Let Γ_f (respectively Γ_h) be the set of the elements from $\{g_1(X)\dots g_s(X)\}$ that participate in the factorization of f (respectively h). Let Φ_f (respectively Φ_h) be the set of all $f_j(X), f_j^*(X)$ which both participate in the factorization of f (respectively h). Finally, let Δ_f be the set of all $f_j(X)$ which participate in the factorization of f, but where $f_j^*(X)$ participate in the factorization of h and those $f_j^*(X)$ form Δ_h. Then

$$f = \Pi\ \Gamma_f \cdot \Pi\Phi_f \cdot \Pi\Delta_f$$

$$h = \Pi\ \Gamma_h \cdot \Pi\Phi_h \cdot \Pi\Delta_h$$

so that

$$\mathrm{lcm}\big(f, h^*\big) = \Pi\ \Gamma_f \cdot \Pi\ \Gamma_h \cdot \Pi\Delta_f$$

Since $\mathrm{lcm}\big(f, h^*\big) = X^N - 1$, we have $\Delta_h = \emptyset$, hence $\Delta_f = \emptyset$, hence f is self-reciprocal. The converse can be proved in the same way as the first proof. □

We again denote by $\varphi(n)$ the Euler function and define the following two functions:

$$\gamma(n, q) = \frac{\varphi(n)}{\mathrm{ord}_{\mathbb{Z}_n^*}(q),}$$

and

$$\beta(n, q) = \frac{\varphi(n)}{2\mathrm{ord}_{\mathbb{Z}_n^*}(q)}$$

where $q = p^r$, p prime, and $p \nmid n$. In order to give the number of cyclic LCD codes of length N over R we again define good and bad pairs and give a decomposition of $X^N - 1$ over R.

Definition 4.19. Let n and r be positive integers. We say that the pair (n, r) is good if $n|(r^k + 1)$ for some integer $k \geq 1$. Otherwise we say that the pair (n, r) is bad.

Proposition 4.20. ([6, Page 5]) The polynomial $X^n - 1 \in \mathbb{F}_q[X]$ can be decomposed in $\mathbb{F}_q[X]$ into a product of monic irreducible factors in the following way:

$$X^N - 1 = \prod_{\substack{n|N \\ (n,q)\text{ good}}} \left(\prod_{i=1}^{\gamma(n,q)} h_{i,n} \right) \prod_{\substack{n|N \\ (n,q)\text{ bad}}} \left(\prod_{i=1}^{\beta(n,q)} k_{i,n} k_{i,n}^* \right), \tag{4.14}$$

where the polynomials $h_{i,n}$ are self-reciprocal and the pairs $(k_{i,n}, k_{i,n}^*)$ are reciprocal pairs. This decomposition is unique up to the order of factors, and the polynomials that appear on the right-hand side of the above equality are pairwise coprime.

Proposition 4.21. Let $k = F_q$. Taking into account Proposition 4.20, the polynomial $X^N - 1 \in R[X]$ can be decomposed in $R[X]$ into a product of monic, basic irreducible factors in the following way:

$$X^N - 1 = \prod_{\substack{n|N \\ (n,q)\text{ good}}} \left(\prod_{i=1}^{\gamma(n,q)} g_{i,n} \right) \prod_{\substack{n|N \\ (n,q)\text{ bad}}} \left(\prod_{i=1}^{\beta(n,q)} f_{i,n} f_{i,n}^* \right), \tag{4.15}$$

where the polynomials g_{in} are self-reciprocal and the pairs $(f_{i,n}, f_{i,n}^*)$ are reciprocal pairs, and $\overline{g_{i,n}} = h_{i,n}$, $\overline{f_{i,n}} = f_{i,n}$, $\overline{f_{i,n}^*} = k_{i,n}^*$. The decomposition of $X^N - 1$ into monic basic irreducible is unique up to the order of factors, and the polynomials that appear on the right-hand side of the above equality are pairwise coprime.

Proof. This proposition follows from Proposition 4.20 in the same way in which Proposition 4.8 follows from Proposition 4.7. □

Theorem 4.22. *The number of cyclic LCD codes of length N over R is 2^{nmsrf},* *where* $\kappa = \mathbb{F}_q$ *and*

$$\mathrm{nmsrf} = \sum_{\substack{n|N \\ (n,q)\ good}} \frac{\varphi(n)}{\mathrm{ord}_{\mathbb{Z}_n^*}(q)} + \frac{1}{2} \sum_{\substack{n|N \\ (n,q)\ bad}} \frac{\varphi(n)}{\mathrm{ord}_{\mathbb{Z}_n^*}(q)}.$$

Proof. Let $\Gamma = \{g_{i,n} : \ i, n\}$ The number of $g_{i,n}$'s is

$$|\Gamma| = \sum_{\substack{n|N \\ (n,q)\ \text{good}}} \gamma(n,q)$$

Let Φ be the set consisting of exactly one element from each pair $\{f_{i,n}, f_{i,n}^*\}$

$$|\Phi| = \sum_{\substack{n|N \\ (n,q)\ \text{bad}}} \beta(n,q)$$

The total number of elements in $\Gamma \cup \Phi$ is

$$\mathrm{nmsrf} = \sum_{\substack{n|N \\ (n,q)\ \text{good}}} \gamma(n,q) \ + \sum_{\substack{n|N \\ (n,q)\ \text{bad}}} \beta(n,q)$$

which is equal to

$$\mathrm{nmsrf} = \sum_{\substack{n|N \\ (n,q)\ \text{good}}} \frac{\varphi(n)}{\mathrm{ord}_{\mathbb{Z}_n^*}(q)} + \frac{1}{2} \sum_{\substack{n|N \\ (n,q)\ \text{bad}}} \frac{\varphi(n)}{\mathrm{ord}_{\mathbb{Z}_n^*}(q)}.$$

Every self-reciprocal monic divisors of $X^N - 1$ is uniquely determined by a subset of $\Gamma \cup \Phi$. Namely if $A \subseteq \Gamma \cup \Phi$, then $A = B \cup C$, where $B \subseteq \Gamma$ and $C \subseteq \Phi$, and the monic divisor corresponding to A can be written as

$$\Pi\{g \in B\} \cdot \Pi\{ff^* \ : \ f \in C\}.$$

Hence the number of self-reciprocal monic divisors of $X^N - 1$ is 2^{nmsrf}. By Theorem 4.15, the number of cyclic LCD codes of length n is 2^{nmsrf}.

□

CHAPTER 5

PROPERTIES OF $\mathrm{LD}_q(n,k)$

5.1 A formula for $\mathrm{LD}_2(n,2)$

It was defined in [21], where a necessary and sufficient condition for a linear code over a field to be an LCD code was given in terms of the generator matrix. LCD codes have been of considerable interest in the last few years since they have several newly discovered applications, including those in quantum coding theory. An important recent paper about LCD codes is [6] which can serve as a foundational paper for a systematic investigation of LCD codes. In that paper the authors introduce the value $\mathrm{LD}_2(n,k)$ for binary LCD $[n,k]$ codes and give the values of $\mathrm{LD}_2(n,2)$ for $n = 3,4,5,6,$ and 7. In this section we find a general formula for $\mathrm{LD}_2(n,2)$.

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

Theorem 5.1. *([21, 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.*

We will now give the definition of the quantity $\mathrm{LD}_2(n,k)$. It was introduced in the paper [6], and used in [11]. In those papers it was denoted by $\mathrm{LCD}[n,k]$

Definition 5.2. The number $\mathrm{LD}_2(n,k)$ is defined in the following way: $\mathrm{LD}_2(n,k) = \max\{d \mid \text{there exists a binary } [n,k,d] \text{ LCD code}\}$.

The following values for $\mathrm{LD}_2(n,2)$ were give in [6]

$$\mathrm{LD}_2(3,2) = 2$$

$$\mathrm{LD}_2(4,2) = 2$$

$$\mathrm{LD}_2(5,2) = 2$$

$$\mathrm{LD}_2(6,2) = 3$$

$$\mathrm{LD}_2(7,2) = 4$$

Whenever we give a generator matrix for an $[n,2]$ code in standard form $G = [I_2|A]$, we will denote the word in the first row of G by $\mathbf{u}$ and the word in the second row of G by $\mathbf{v}$, Also we will call the submatrix A of G the extension part of G and the digits of $\mathbf{u}$ and $\mathbf{v}$ that are in A the extension digits of $\mathbf{u}$ and $\mathbf{v}$.

Proposition 5.3. [11, Proposition 2.2] For any integer $r \geq 0$ we have :

$$LD_2(6r+3,2) \geq 4r+2$$

$$LD_2(6r+4,2) \geq 4r+2$$

$$LD_2(6r+5,2) \geq 4r+2$$

$$LD_2(6r+6,2) \geq 4r+3$$

$$LD_2(6r+7,2) \geq 4r+4$$

$$LD_2(6r+8,2) \geq 4r+5$$

Proof. For any integer $r \geq 0$ and $s \in \{3, 4, 5\}$ let C be the code with generator matrix in standard form

$$G = \left[\begin{array}{cc|c|cc|ccc} 1 & 0 & ... & 1 & 0 & 1 & ... & 1 \\ 0 & 1 & ... & 0 & 1 & 1 & ... & 1 \end{array}\right].$$

$$\underbrace{\hphantom{1 \quad 0 \mid ... \mid 1 \quad 0}}_{\substack{2r+1\ I_2's \\ = 4r+2 \text{ digits}}} \qquad \underbrace{\hphantom{1 \ ... \ 1}}_{\substack{2r+s-2 \\ \text{ones}}}$$

Then $\text{wt}(\mathbf{u}) = \text{wt}(\mathbf{v}) = 4r + s - 1$ and $\text{wt}(\mathbf{u} + \mathbf{v}) = 4r + 2$, so that $d = 4r + 2$. Using the block multiplication of matrices we conclude from Theorem 5.1 that C is LCD. Hence the first three inequalities hold.

For any integer $r \geq 0$ and $s \in \{6, 7, 8\}$ let C be the code with generator matrix in standard form

$$G = \left[\begin{array}{cc|c|cc|ccc} 1 & 0 & ... & 1 & 0 & 1 & ... & 1 \\ 0 & 1 & ... & 0 & 1 & 1 & ... & 1 \end{array}\right].$$

$$\underbrace{\hphantom{1 \quad 0 \mid ... \mid 1 \quad 0}}_{\substack{2r+3\ I_2's \\ = 4r+6 \text{ digits}}} \qquad \underbrace{\hphantom{1 \ ... \ 1}}_{\substack{2r+s-6 \\ \text{ones}}}$$

Thus, $\text{wt}(\mathbf{u}) = \text{wt}(\mathbf{v}) = 4r + s - 3$ and $\text{wt}(\mathbf{u} + \mathbf{v}) = 4r + 6$, so that $d = 4r + s - 3$. Using the block multiplication of matrices we conclude from Theorem 5.1 that C is LCD. Hence the last three inequalities hold. □

Proposition 5.4. [11, Proposition 2.3] For any integer $r \geq 0$ we have :

$$\mathrm{LD}_2(6r+3,2) < 4r+3$$

$$\mathrm{LD}_2(6r+4,2) < 4r+3$$

$$\mathrm{LD}_2(6r+7,2) < 4r+5$$

$$\mathrm{LD}_2(6r+8,2) < 4r+6$$

Proof. If $r = 0$ each inequality is clearly true. Assume $r \geq 1$ and suppose to the contrary. Let C be an LCD $[6r+3,2]$ code with $d \geq 4r+3$. Up to permutation equivalence we may assume that the generator matrix G of C is in standard form. Then $\mathbf{u}$ and $\mathbf{v}$ have at least $4r+2$ extension digits which are one. Up to permutation equivalence we may assume that the first $4r+2$ extension digits of $\mathbf{u}$ are ones and that the first $2r+3$ extension digits of $\mathbf{v}$ are ones. so we have

$$G = \left[\begin{array}{c|c|c|c} \begin{matrix}1 & 0\\ 0 & 1\end{matrix} & \underbrace{\begin{matrix}1 & \dots & 1\\ 1 & \dots & 1\end{matrix}}_{2r+3} & \underbrace{\begin{matrix}1 & \dots & 1\\ & \dots & \end{matrix}}_{2r-1} & \underbrace{\begin{matrix}\quad\dots\quad\\ \quad\dots\quad\end{matrix}}_{2r-1} \end{array}\right].$$

now $\mathbf{u}+\mathbf{v}$ can have at most $2+(2r-1)+(2r-1) = 4r$ ones, contradicting the assumption $d \geq 4r+3$. The first inequality is proved. The proofs of the remaining three inequalities go along the same lines. Assume $r \geq 1$ and suppose to the contrary. Let C be an LCD $[6r+4,2]$ code with $d \geq 4r+3$. Up to permutation equivalence we may assume that the generator matrix G of C is in standard form. Then $\mathbf{u}$ and $\mathbf{v}$ have at least $4r+2$ extension digits which are one. Up to permutation equivalence we may assume that the first $4r+2$ extension digits of $\mathbf{u}$ are ones and that the first $2r+3$ extension digits of $\mathbf{v}$ are ones. so we have

$$G = \left[\begin{array}{cc|ccc|ccc|c} 1 & 0 & 1 & \dots & 1 & 1 & \dots & 1 & \dots \\ 0 & 1 & 1 & \dots & 1 & & \dots & & \dots \\ & & \multicolumn{3}{c}{\underbrace{\hspace{2.5cm}}_{2r+3}} & \multicolumn{3}{c}{\underbrace{\hspace{2cm}}_{2r-1}} & \underbrace{\hspace{1.5cm}}_{2r} \end{array}\right].$$

now $\mathbf{u}+\mathbf{v}$ can have at most $2+(2r-1)+(2r) = 4r+1$ ones, contradicting the assumption $d \geq 4r+3$. The second inequality is proven. Assume $r \geq 1$ and suppose to the contrary. Let C be an LCD $[6r+7, 2]$ code with $d \geq 4r+5$. Up to permutation equivalence we may assume that the generator matrix G of C is in standard form. Then $\mathbf{u}$ and $\mathbf{v}$ have at least $4r+4$ extension digits which are one. Up to permutation equivalence we may assume that the first $4r+4$ extension digits of $\mathbf{u}$ are ones and that the first $2r+5$ extension digits of $\mathbf{v}$ are ones. so we have

$$G = \left[\begin{array}{cc|ccc|ccc|c} 1 & 0 & 1 & \dots & 1 & 1 & \dots & 1 & \dots \\ 0 & 1 & 1 & \dots & 1 & & \dots & & \dots \\ & & \multicolumn{3}{c}{\underbrace{\hspace{2.5cm}}_{2r+5}} & \multicolumn{3}{c}{\underbrace{\hspace{2cm}}_{2r-1}} & \underbrace{\hspace{1.5cm}}_{2r+1} \end{array}\right].$$

now $\mathbf{u}+\mathbf{v}$ can have at most $2+(2r)+(2r) = 4r+2$ ones, contradicting the assumption $d \geq 4r+5$. The third inequality is proven.

Assume $r \geq 1$ and suppose to the contrary. Let C be an LCD $[6r+8, 2]$ code with $d \geq 4r+6$. Up to permutation equivalence we may assume that the generator matrix G of C is in standard form. Then $\mathbf{u}$ and $\mathbf{v}$ have at least $4r+5$ extension digits which are one. Up to permutation equivalence we may assume that the first $4r+5$ extension digits of $\mathbf{u}$ are ones and that the first $2r$ extension digits of $\mathbf{v}$ are ones. so we have

$$G=\left[\begin{array}{c|c|c|c} \begin{matrix}1&0\\0&1\end{matrix} & \underbrace{\begin{matrix}1&\dots&1\\1&\dots&1\end{matrix}}_{2r+5} & \underbrace{\begin{matrix}1&\dots&1\\ &\dots& \end{matrix}}_{2r} & \underbrace{\begin{matrix}\dots\\ \dots\end{matrix}}_{2r+1}\end{array}\right].$$

now $\mathbf{u}+\mathbf{v}$ can have at most $2+(2r)+(2r+1)=4r+3$ ones, contradicting the assumption $d \geq 4r+6$. □

Proposition 5.5. [11, Proposition 2.4] For any integer $r \geq 0$ we have :

$$\mathrm{LD}_2(6r+6,2) < 4r+4$$

Proof. Suppose to the contrary. Let C be an LCD $[6r+6,2]$ code with $d \geq 4r+4$. Up to permutation equivalence we may assume that the generator matrix G of C is in standard form. Them $\mathbf{u}$ and $\mathbf{v}$ have at least $4r+3$ extension digits of $\mathbf{u}$ are ones and that the first $2r+2$ extension digits of $\mathbf{v}$ are ones. So we have

$$G=\left[\begin{array}{c|c|c|c} \begin{matrix}1&0\\0&1\end{matrix} & \underbrace{\begin{matrix}1&\dots&1\\1&\dots&1\end{matrix}}_{2r+2} & \underbrace{\begin{matrix}1&\dots&1\\ &\dots& \end{matrix}}_{\substack{\text{2r+1}\\ \text{Block A}}} & \underbrace{\begin{matrix}\dots\\ \dots\end{matrix}}_{\substack{\text{2r+1}\\ \text{Block B}}}\end{array}\right].$$

Note the following two facts:

1. $\mathbf{u}+\mathbf{v}$ has at least $4r+4$ ones, hence all digits of v in the blocks A and B are opposite to the digits of $\mathbf{u}$.

2. At least $2r+1$ digits of $\mathbf{v}$ in the blocks A and B are ones.

The facts above force G to have the following form:

$$G = \left[\begin{array}{cc|c|c|c} 1 & 0 & 1 \ \ldots \ 1 & 1 \ \ldots \ 1 & 0 \ \ldots \ 0 \\ 0 & 1 & \underbrace{1 \ \ldots \ 1}_{2r+2} & \underbrace{0 \ \ldots \ 0}_{2r+1} & \underbrace{1 \ \ldots \ 1}_{2r+1} \end{array}\right].$$

Hence up to permutation equivalence

$$G = \left[\begin{array}{cc|c|cc|c} 1 & 0 & \ldots & 1 & 0 & 1 \ \ldots \ 1 \\ 0 & 1 & \ldots & 0 & 1 & \underbrace{1 \ \ldots \ 1}_{\substack{\text{2r+2} \\ \text{ones}}} \end{array}\right].$$

Using the block multiplication of matrices we conclude from Theorem 5.1 that C is not LCD. We get a contradiction, the inequality is proven. □

Proposition 5.6. [11, Proposition 2.5] For any integer $r \geq 0$ we have :

$$\mathrm{LD}_2(6r+5, 2) < 4r+3$$

Proof. Suppose to the contrary. Let C be an LCD $[6r+5, 2]$ code with $d \geq 4r+3$. Up to permutation equivalence we may assume that the generator matrix G of C is in standard form. Then $\mathbf{u}$ and $\mathbf{v}$ have at least $4r+2$ extension digits one. Up to permutation equivalence we may assume that the first $4r+2$ extension digits of $\mathbf{u}$ are ones and that the first $2r+1$ extension digits $\mathbf{v}$ are ones. So we have

$$G = \left[\begin{array}{cc|c|c|c} 1 & 0 & 1 \ \ldots \ 1 & 1 \ \ldots \ 1 & \ldots \\ 0 & 1 & \underbrace{1 \ \ldots \ 1}_{2r+1} & \underbrace{\ \ \ldots \ \ }_{\substack{\text{2r+1} \\ \text{Block A}}} & \underbrace{\ \ \ldots \ \ }_{\substack{\text{2r+1} \\ \text{Block B}}} \end{array}\right].$$

Consider the following:

1. $\mathbf{u} + \mathbf{v}$ has at least $4r + 3$ ones, hence all digits of v in the blocks A and B, except at most one, are opposite to the digits of $\mathbf{u}$.
2. At least $2r + 1$ digits of $\mathbf{v}$ in the blocks A and B are ones.

Hence, up to permutation equivalence, G has the following form:

$$G = \left[\begin{array}{cc|ccc|cccc|ccccc} 1 & 0 & 1 & \dots & 1 & 1 & \dots & 1 & 1 & b_1 & b_2 & \dots & b_{2r} & c \\ 0 & 1 & 1 & \dots & 1 & 0 & \dots & 0 & a & \overline{b_1} & \overline{b_2} & \dots & \overline{b_{2r}} & d \\ \multicolumn{2}{c}{} & \multicolumn{3}{c}{\underbrace{\hphantom{1 \ \dots \ 1}}_{2r+1}} & \multicolumn{4}{c}{\underbrace{\hphantom{1 \ \dots \ 1 \ 1}}_{\substack{\text{2r+1} \\ \text{Block A}}}} & \multicolumn{5}{c}{\underbrace{\hphantom{b_1 \ b_2 \ \dots \ b_{2r} \ c}}_{\substack{\text{2r+1} \\ \text{Block B}}}} \end{array}\right]$$

where the overline denotes the opposite digit. If $r = 0$, we have

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & c \\ 0 & 1 & 1 & a & d \end{array}\right].$$

By (2) at least a or d is 1. If $a = 1$, then (1) implies $d = \overline{c}$, so that

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & c \\ 0 & 1 & 1 & 1 & \overline{c} \end{array}\right],$$

but then GG^T is equal to either

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ or } G = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

so that, by Theorem 5.1, C is not LCD, a contradiction. If $a = 0$, then (2) implies $d = 1$ so that

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & c \\ 0 & 1 & 1 & 0 & 1 \end{array}\right],$$

but then GG^T is equal to either

$$G = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \text{ or } G = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

so that, by Theorem 5.1, C is not LCD, a contradiction.

Assume now that $r \geq 1$. Because of (1) we have either $a = 0$ or $d = \bar{c}$. Because of (2), among the digits $a, b_1, b_2, ..., b_{2r}, d$ the word $\mathbf{v}$ has at least $2r+1$ ones. Hence among the digits $\overline{b_1}, \overline{b_2}, ..., \overline{b_{2r}}$, the word $\mathbf{v}$ has at least $2r-1$ ones. Hence, up to permutation equivalence, G has the following form:

$$G = \left[\begin{array}{c|c|cc|ccc} \begin{matrix}1 & 0\\ 0 & 1\end{matrix} & \underbrace{\begin{matrix}1 & \dots & 1\\ 1 & \dots & 1\end{matrix}}_{2r+1} & \underbrace{\begin{matrix}1 & \dots & 1\\ 0 & \dots & 0\end{matrix}}_{2r} & \begin{matrix}1\\ a\end{matrix} & \underbrace{\begin{matrix}0 & \dots & 0\\ 1 & \dots & 1\end{matrix}}_{2r-1} & \begin{matrix}b_{2r}\\ \overline{b_{2r}}\end{matrix} & \begin{matrix}c\\ d\end{matrix} \end{array}\right].$$

Hence because of (1) either $a = 0$ or $d = \bar{c}$, and because of (2), at least two digits $a, \overline{b_{2r}}, d$ are ones. Thus we have the following options:

i. $a = 0$, $\overline{b_{2r}} = d = 1$ (so that $b_{2r} = 0$);

ii. $a = 1$, $d = \bar{c}$, and $d = 1$ (so that $c = 0$);

iii. $a = 1$, $d = \bar{c}$, and $\overline{b_{2r}} = 1$.

This implies that for the matrix G, we respectively, have the following options:

i.

$$G = \left[\begin{array}{c|c|cc|ccc} \begin{matrix}1 & 0\\ 0 & 1\end{matrix} & \underbrace{\begin{matrix}1 & \dots & 1\\ 1 & \dots & 1\end{matrix}}_{2r+1} & \underbrace{\begin{matrix}1 & \dots & 1\\ 0 & \dots & 0\end{matrix}}_{2r} & \begin{matrix}1\\ 0\end{matrix} & \underbrace{\begin{matrix}0 & \dots & 0\\ 1 & \dots & 1\end{matrix}}_{2r-1} & \begin{matrix}0\\ 1\end{matrix} & \begin{matrix}c\\ 1\end{matrix} \end{array}\right]$$

ii.

$$G = \left[\begin{array}{c|c|cc|ccc} \begin{matrix}1 & 0\\ 0 & 1\end{matrix} & \underbrace{\begin{matrix}1 & \dots & 1\\ 1 & \dots & 1\end{matrix}}_{2r+1} & \underbrace{\begin{matrix}1 & \dots & 1\\ 0 & \dots & 0\end{matrix}}_{2r} & \begin{matrix}1\\ 1\end{matrix} & \underbrace{\begin{matrix}0 & \dots & 0\\ 1 & \dots & 1\end{matrix}}_{2r-1} & \begin{matrix}b_{2r}\\ \overline{b_{2r}}\end{matrix} & \begin{matrix}0\\ 1\end{matrix} \end{array}\right]$$

iii.

$$G = \left[\begin{array}{c|c|cc|ccc} \begin{matrix}1 & 0\\ 0 & 1\end{matrix} & \underbrace{\begin{matrix}1 & \dots & 1\\ 1 & \dots & 1\end{matrix}}_{2r+1} & \underbrace{\begin{matrix}1 & \dots & 1\\ 0 & \dots & 0\end{matrix}}_{2r} & \begin{matrix}1\\ 1\end{matrix} & \underbrace{\begin{matrix}0 & \dots & 0\\ 1 & \dots & 1\end{matrix}}_{2r-1} & \begin{matrix}0\\ 1\end{matrix} & \begin{matrix}c\\ \bar{c}\end{matrix} \end{array}\right]$$

Option(i): In this option, up to permutation equivalence, the matrix G has the form

$$G = \left[\begin{array}{c|c|c|c} \begin{matrix}1 & 0\\ 0 & 1\end{matrix} & \underbrace{\begin{matrix}1 & \dots & 1\\ 1 & \dots & 1\end{matrix}}_{2r+1} & \underbrace{\begin{matrix}1 & 0 & \dots & 1 & 0\\ 0 & 1 & \dots & 0 & 1\end{matrix}}_{2rI_2's} & \begin{matrix}1 & c\\ 0 & 1\end{matrix}\end{array}\right].$$

Notice that

$$\begin{bmatrix}1 & c\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & c\\ 0 & 1\end{bmatrix}^T \text{ is equal to either } \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \text{ or } \begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}.$$

Hence using the block multiplication of matrices, we conclude that GG^T is equal to either

$$\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} \text{ or } \begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}.$$

So by Theorem 5.1 the code C is not LCD and we have a contradiction.

Option(ii): In this option, up to permutation equivalence, the matrix G has the form:

$$G = \left[\begin{array}{c|c|c|c} \begin{matrix}1 & 0\\ 0 & 1\end{matrix} & \underbrace{\begin{matrix}1 & \dots & 1\\ 1 & \dots & 1\end{matrix}}_{2r+1} & \underbrace{\begin{matrix}1 & 0 & \dots & 1 & 0\\ 0 & 1 & \dots & 0 & 1\end{matrix}}_{2rI_2's} & \begin{matrix}1 & b_{2r}\\ 1 & \overline{b_{2r}}\end{matrix}\end{array}\right].$$

With reasoning similar as in option(ii) we conclude that GG^T is equal to either

$$\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix} \text{ or } \begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}.$$

So by Theorem 5.1 the code C is not LCD and we have a contradiction.

Option(iii): This option is analyzed in the same way as in option (ii). Since we got a contradiction with the assumption that C is LCD, the inequality is proven. □

Thus we conclude with the following theorem:

Theorem 5.7. *[11, 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:

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

Proof. The theorem follows from the previous propositions. □

Remark 5.8. Note that the last equality of the above theorem holds for $r = -1$ which yields that: $\mathrm{LD}_2(2, 2) = 1$. Also, if you replace r with $r - 1$ you have the following:

$$\mathrm{LD}_2(6r - 3, 2) = 4r - 2$$

$$\mathrm{LD}_2(6r - 2, 2) = 4r - 2$$

$$\mathrm{LD}_2(6r - 1, 2) = 4r - 2$$

$$\mathrm{LD}_2(6r + 0, 2) = 4r - 1$$

$$\mathrm{LD}_2(6r + 1, 2) = 4r + 0$$

$$\mathrm{LD}_2(6r + 2, 2) = 4r + 1.$$

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

In this section we make a correction of the statement to [23, Theorem 4.2] and give a different proof. We also provide a different proof of [23, 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

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

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

Lemma 5.9. [23, 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 5.10. 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 5.11. Let C be an $[n, 2, d]$ binary linear code. Then $d \leq \lfloor \frac{2n}{3} \rfloor$

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

The following Theorem is a correction of the statement of [23, Theorem 4.2]. It also includes the statement of [23, Theorem 4.3]. The proofs of both of the theorems are different.

Theorem 5.12. *Let C be a binary LCD $[n, 2]$ code with maximal possible d that meets the Griesmer Bound. Then $n \equiv 2(mod\ 6)$ or $n \equiv 3(mod\ 6)$ and in both cases the code C is unique up to equivalence. Conversely, if $n \equiv 2(mod\ 6)$ or $n \equiv 3(mod\ 6)$ there exists one and only one (up to equivalence) binary LCD $[n, 2]$ code with maximal possible d, that meets Griesmer Bound.*

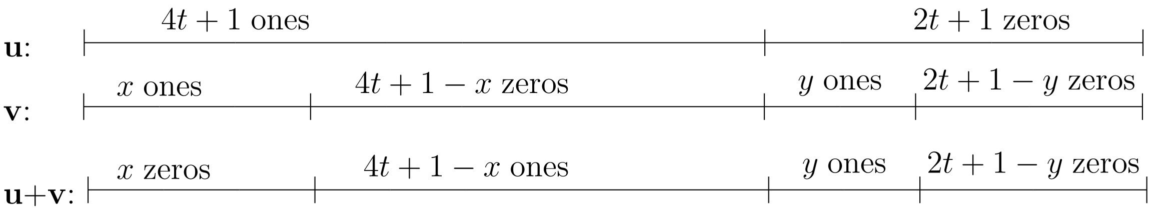
Proof. Let C be an LCD binary $[n, 2, d]$ code wit maximal possible d (i.e., such that $d = \mathrm{LD}_2(n, 2)$).

- 1st case: $n \equiv 0(\text{mod } 6)$. We can write $n = 6t$ for some $t \geq 1$. Since, by Lemma 5.11, $d \leq \lfloor \frac{2n}{3} \rfloor$, 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 Theorem 5.7 , $d = 4t - 1$. Hence no LCD code C with maximal d meets the Griesmer Bound in this case.

- 2nd case: $n \equiv 1(\text{mod } 6)$. We can write $n = 6t + 1$ for some $t \geq 0$. Since by, Lemma 5.11, $d \leq \lfloor \frac{2n}{3} \rfloor$, 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.

- 3rd case: $n \equiv 2(\text{mod } 6)$. We can write $n = 6t + 2$ for some $t \geq 0$. Since, by Lemma 5.11, $d \leq \lfloor \frac{2n}{3} \rfloor$, 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 theorem 5.7 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

$$y \geq x$$

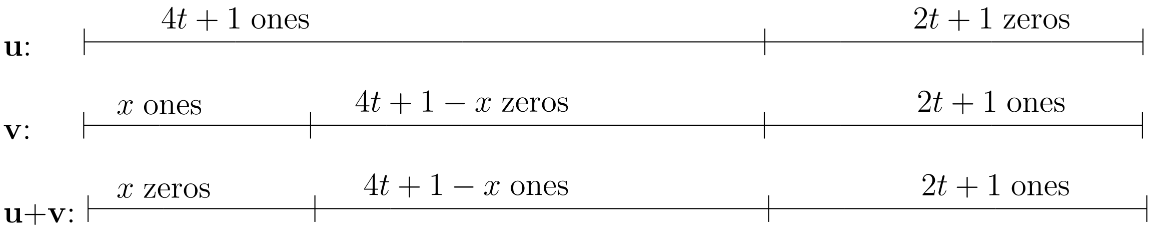
then this and the first inequality imply

$$y \geq 2t+1$$

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

$$x \geq 2t$$

$$x \leq 2t + 1$$

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 (by Lemma 5.10). These codes are LCD as GG^T (from $\mathbf{u}$, $\mathbf{v}$ in case $x = 2t$) looks like

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

- 4th case: $n \equiv 3 (\text{mod } 6)$. Reasoning like in the 3rd case, we conclude that there is, up to equivalence, exactly one LCD $[n, 2]$ code with maximal d, which meets the Griesmer Bound.

- 5th case: $n \equiv 4 (\text{mod } 6)$. Reasoning like in the 2nd case, we conclude that there is no $[6t + 4, 2]$ code which meets the Griesmer Bound.

- 6th case: $n \equiv 5 (\text{mod } 6)$. 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.

□

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

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

Definition 5.13. $\mathrm{LD}_3(n,k) = \max\{d \mid \text{there exists a ternary } [n,k,d] \text{ LCD code}\}$

Theorem 5.14. *[23, 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 5.15. *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 $d \leq \lfloor \frac{3n}{4} \rfloor$.

- 1st case: $n \equiv 0 (\mathrm{mod}\ 4)$. 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, $\mathrm{LD}_3(n,2) = \lfloor \frac{3n}{4} \rfloor - 1$, so no ternary $LCD[n,2,d]$ code with $d = \mathrm{LD}_3(n,2)$ can meet the Griesmer Bound in this case.

- 2nd case: $n \equiv 1 (\mathrm{mod}\ 4)$. 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 $\mathrm{LD}_3(n,2) = 3t$ we conclude that no ternary LCD $[n,2,d]$ code with $d = \mathrm{LD}_3(n,2)$ can meet the Griesmer Bound in this case too.

- 3rd case: $n \equiv 2 (\mathrm{mod}\ 4)$. 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 $\mathrm{LD}_3(n,2) = \lfloor \frac{3n}{4} \rfloor = 3t+1$, by Theorem 5.14 we conclude that any ternary LCD $[n,2,d]$ code with $d = \mathrm{LD}_3(n,2)$ meets the Griesmer Bound in this case.

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

□

Let C be a ternary linear $[n, 2]$ code. Let $\mathbf{u} = (u_1, u_2, \dots, u_n)$ and $\mathbf{v} = (v_1, v_2, \dots, v_n)$ 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 [23, 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 5.16. [23, Page 6] Let C be a ternary linear $[n, 2]$ code with generator matrix G whose rows are $\mathbf{u} = (u_1, u_2, \dots, u_n)$ and $\mathbf{v} = (v_1, v_2, \dots, v_n)$. 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 5.17. 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 Theorem 5.14. 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 [23].

Theorem 5.18. *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 Theorem 5.14 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:

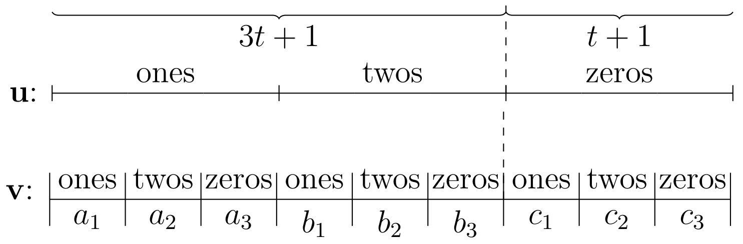

$3t+1$
$t+1$
ones
twos
zeros
$\mathbf{u}$:
$\mathbf{v}$:
ones | twos | zeros | ones | twos | zeros | ones | twos | zeros
a_1 a_2 a_3 b_1 b_2 b_3 c_1 c_2 c_3

Diagram 5.3.1

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

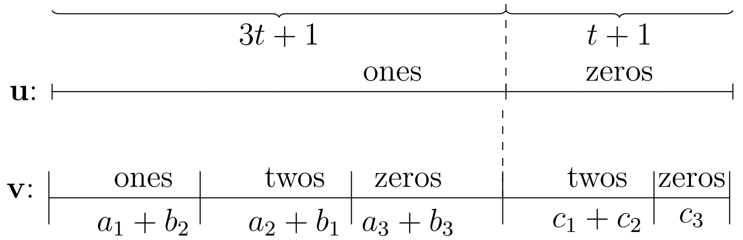

$3t+1$
$t+1$
ones
zeros
$\mathbf{u}$:
$\mathbf{v}$:
ones | twos | zeros | twos | zeros
$a_1 + b_2$ $a_2 + b_1$ $a_3 + b_3$ $c_1 + c_2$ c_3

Diagram 5.3.2

The word $\mathbf{u} + \mathbf{v}$ from Diagram 5.3.2 has the following form:

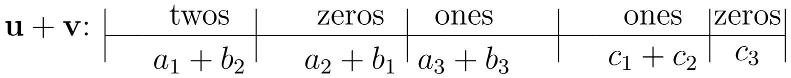

$\mathbf{u} + \mathbf{v}$:
twos | zeros | ones | ones | zeros
$a_1 + b_2$ $a_2 + b_1$ $a_3 + b_3$ $c_1 + c_2$ c_3

Diagram 5.3.3

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

$$a_1 + a_2 + a_3 + b_1 + b_2 + b_3 = 3t + 1 \tag{5.1}$$

$$a_1 + a_2 + b_1 + b_2 + c_1 + c_2 \geq 3t + 1 \tag{5.2}$$

$$a_1 + a_3 + b_1 + b_3 + c_1 + c_3 \geq 3t + 1 \tag{5.3}$$

From (5.1) and (5.2) we get

$$c_1 + c_2 \geq a_3 + b_3 \tag{5.4}$$

and from (5.1) and (5.3) we get

$$c_1 + c_2 \geq a_2 + b_1 \tag{5.5}$$

The word $2\mathbf{u} + \mathbf{2v}$ from Diagram 5.3.2 has the following form:

$2\mathbf{u} + 2\mathbf{v}$:	ones	zeros	twos	twos	zeros
	$a_1 + b_2$	$a_2 + b_1$	$a_3 + b_3$	$c_1 + c_2$	c_3

Counting ones and twos we get

$$a_1 + b_2 + a_3 + b_3 + c_1 + c_2 \geq 3t + 1 \tag{5.6}$$

which together with (5.1) implies

$$c_1 + c_2 \geq a_1 + b_2 \tag{5.7}$$

If we consider other linear combinations of $\mathbf{u}$ and $\mathbf{v}$ from Diagram 5.3.2 and do a similar reasoning, we end up with one of the inequalities (5.4), (5.5), (5.7) or with the inequality (5.1). Note that there are exactly 8 non-zero linear combinations, each of the relations (5.1), (5.4), (5.5), (5.7) would be yielded from exactly two linear combinations. If we add (5.4), (5.5), and (5.7) 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 **u** in Diagram 5.3.2 we can see that

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

Hence

$$c_1 + c_2 = t + 1 c_3 = 0 \tag{5.8}$$

Now (5.4), (5.5), (5.7), and (5.8) imply:

$$a_1 + b_2 \leq t + 1 \tag{5.9}$$

$$a_2 + b_1 \leq t + 1 \tag{5.10}$$

$$a_3 + b_3 \leq t + 1 \tag{5.11}$$

Adding (5.9) and (5.10) we get

$$a_1 + b_2 + a_2 + b_1 \leq 2t + 2 \tag{5.12}$$

which together with (5.1) implies

$$a_3 + b_3 \geq t - 1 \tag{5.13}$$

Similarly we get

$$a_1 + b_2 \geq t - 1 \tag{5.14}$$

$$a_2 + b_1 \leq t - 1 \tag{5.15}$$

Now from (5.9),(5.10), (5.11), (5.13), (5.14), and (5.15) we conclude

$$a_1 + b_2 \in \{t - 1, t, t + 1\}, \tag{5.16}$$

$$a_2 + b_1 \in \{t - 1, t, t + 1\}, \tag{5.17}$$

$$a_3 + b_3 \in \{t - 1, t, t + 1\} \tag{5.18}$$

The relations (5.16), (5.17), (5.18), and (5.1) imply that there are six possible cases:

$$a_1 + b_2 = t - 1,\ a_2 + b_1 = a_3 + b_3 = t + 1 \tag{5.19}$$

$$a_2 + b_1 = t - 1,\ a_1 + b_2 = a_3 + b_3 = t + 1 \tag{5.20}$$

$$a_3 + b_3 = t - 1,\ a_1 + b_2 = a_2 + b_1 = t + 1 \tag{5.21}$$

$$a_1 + b_2 = a_2 + b_1 = t,\ a_1 + b_2 = t + 1 \tag{5.22}$$

$$a_1 + b_2 = a_3 + b_3 = t,\ a_2 + b_1 = t + 1 \tag{5.23}$$

$$a_2 + b_1 = a_3 + b_3 = t,\ a_1 + b_2 = t + 1 \tag{5.24}$$

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 Diagram 5.3.2, we use Lemma 5.16 to calculate GG^T. For example, in case (5.19) 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 LCD by Theorem 5.1. Similarly, the codes (5.20) and (5.22) are not LCD. In the case (5.21) 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 (5.23) and (5.24) 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 **u**, and **v** from Diagram 5.3.2, with the parameters a_1, a_2, a_3, b_1, b_2, b_3, c_1, and c_2 satisfying (5.8), (5.21), (5.23), and (5.24). We not consider the equivalence of these 3 codes. The code (5.21) 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 (5.23) or (5.24). The reason is the fact that the codes (5.23) and (5.24) 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 (5.23) and (5.24) are equivalent since the generator matrix with rows **u**, and **v** for the code (5.23) is equal to the generator matrix with rows $\mathbf{u}$, and $2\mathbf{u} + \mathbf{v}$ for the code (5.24). 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.

□

5.4 $\mathrm{LD}_3(n, n-i) = 2$ under certain assumptions

Theorem 5.19. *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

$$1 + 2n + \cdots + 2^t\tbinom{n}{t} \leq 3^i. \tag{5.1}$$

When $n \geq \frac{3^i+1}{2}$, $1 + 2n \geq 3^i + 2$. Hence (5.1) 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 $i \equiv 0 (\mathrm{mod}\ 3)$, let

$$G = \left[I_{n-i} \,\middle|\, \underbrace{\mathbb{1} \;\; \mathbb{1} \;\; \ldots \;\; \mathbb{1}}_{i} \right], \quad \text{where } \mathbb{1} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \}n-i.$$

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

- If $i \equiv 1 (\mathrm{mod}\ 3)$, let

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

  Using the same Reasoning as the previous case we see that $GG^T = I_{n-i}$.

- Finally if $i \equiv 2 (\mathrm{mod}\ 3)$, let

$$G = \left[I_{n-i} \,\middle|\, \underbrace{\mathbb{1} \;\; \mathbb{1} \;\; \ldots \;\; \mathbb{1} \;\; \mathbf{0} \;\; \mathbf{0}}_{i} \right].$$

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 Theorem 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. □

5.5 Nonexistence of certain LCD ternary codes

Theorem 5.20. *Suppose $i, k \geq 1$*

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

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

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

Before the proof of Theorem 5.20 is given we will prove the following lemma:

Lemma 5.21. 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 Massey's Theorem C is not LCD, a contradiction. □

Proof. (for Theorem 5.20)

(a) • For $k = 1$, there is no $[n, 1, n-3i]$ LCD ternary code by Lemma 5.21

since $n \equiv 0 \pmod 3$.

- 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 Theorem 5.14, $\mathrm{LD}_3(12i, 2) = \lfloor \frac{3 \cdot 12i}{4} \rfloor - 1 = 9i - 1$. 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.

(b)

- For $k = 1$, there is no $[n, 1, n-3i-1]$ LCD ternary code by Lemma 5.21 since $n \equiv 0 \pmod 3$.

- 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 Theorem 5.14, $\mathrm{LD}_3(12i + 4, 2) = 9i + 2$ 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.

(c)

- For $k=1$, there is no $[n,1,n-3i-2]$ LCD ternary code by Lemma 5.21 since $n \equiv 0 (\mathrm{mod}\ 3)$.

- 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 Theorem 5.14, $\mathrm{LD}_3(12i+8,2) = 9i+2$ 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.

□

5.6 The relation $\mathrm{LD}_q(n,k) \leq \mathrm{LD}_q(n,k-1)$

For binary codes the relation $\mathrm{LD}_2(n,k) \leq \mathrm{LD}_2(n,k-1)$ for any $2 \leq k \leq n$ was proved in [4, Theorem 8]. For ternary codes a proof was given in [14]. 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 [23], but it is not correct since [23, 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 5.22. *[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*

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

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 5.23. *[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 $GG^T = diag[1, 1, \ldots, 1, \delta]$, where $\delta \in \mathbb{F}_q \setminus \{0\}$.*

Theorem 5.24. *We have*

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

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 ([2, Theorem 25]) 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 $G_1 G_1^T = I_{k-1}$. Since $d(C_1) \geq d(C)$, we in particular have $\mathrm{LD}_q(n, k) \leq \mathrm{LD}_q(n, k-1)$. □

Corollary 5.25. Suppose $2 \leq k \leq n$. Then

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

for any q.

Proof. For $q = 2$ see [4, Theorem 8]. For q a power of an odd prime, see Theorem 5.24. 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 $\mathrm{LD}_q(n, k) \leq \mathrm{LD}_q(n, k-1)$. □

5.7 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 [14, 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 5.26. *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 5.27. 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 $\mathbf{x} \in C^\perp$ such that $\langle \mathbf{x}, \mathbf{x} \rangle = 1$

Proof. By Massey's Theorem, $C^\perp$ is an LCD $[n, n-k]$ code. By Theorem 5.23 it has a generator matrix G such that $GG^T = \mathrm{diag}[1, 1, \ldots, 1, \delta]$, $\delta \in \mathbb{F}_q \setminus \{0\}$ 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 Massey's Theorem, $C^\perp$ is an LCD $[n, n-k]$ code. Hence by the Corollary 5.27, 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 LCD by Massey's Theorem and C is a subcode of C'.

□

Remark 5.28. The difference between this proof and the proof in [14] is in the way the word $\mathbf{x}$ is produced. In [14, Lemma 3(i)] a theorem about self-orthogonality of ternary codes was used, so the constructive proof given in [14, 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.

CHAPTER 6

CONCLUSIONS

The study and classification of LCD codes remain to be a very active area in algebraic coding theory. LCD codes give an optimum solution to the two-user binary adder channel. In [3] Carlet and Guilley discuss how LCD codes with large minimum distance defend against two main attacks in cryptography, namely fault-injection and side-channel attacks. It has also recently been shown that LCD codes have applications for error-correcting quantum codes.

The characterization for a cyclic LCD code over a field was given in [27] and codes over $\mathbb{Z}_4$ were thoroughly investigated in [13]. In Chapter 3 we use the characterization of the hull of a cyclic code over $\mathbb{Z}_4$, provided in [18], to give a characterization for a cyclic LCD code over $\mathbb{Z}_4$, which is also given in our paper [10]. This result is expanded in Chapter 4 by using results from [22], were we gave a characterization for cyclic codes over $R = \big(R, (\gamma), \kappa\big)$ with $\nu(\gamma) = 2$ to be an LCD code. From our results it can be concluded that the condition for cyclic code to be LCD over R is surprisingly very similar to the condition provided by Massey and Yang for cyclic codes over fields.

In Chapter 5 we explored the definition in [6] for the maximum minimum distance that an LCD code exists given a fixed n and $k = 2$. We expanded on the results in [6] and provide a formula for the maximum minimum distance that an LCD code exists given $k = 2$. This result is also discussed in our paper [11]. We provide a correction to the theorem in [23] and provide a proof for a binary

LCD $[n, k]$ to meet the Griesmer bound. Using results from [23] we also provide a theorem for ternary LCD $[n, k]$ codes to meet the Griesmer Bound. Using the Sphere Packing Bound we showed that the maximum minimum distance for certain ternary LCD codes is 2 and provided a theorem for the non-existence of certain LCD ternary codes. Lastly, we improved the result of [14] for any prime power q by providing a constructive proof and correct a relation in [23].

In terms of future work, I want to identify double cyclic codes over R that are LCD codes for specified length/dimension and characterize when double cyclic codes are LCD codes. Double cyclic codes have only been studied over the past few years. These codes can be defined in the following way: for positive integers r, s such that r+s=n, a double cyclic code over R of length (r, s) is a R-submodule of R^{r+s} which has the property that for any $\mathbf{c} = (c_{1,0}, ..., c_{1,r-1} | c_{2,0}, .., c_{2,s-1}) \in C$ the double cyclic shift is: $T(\mathbf{c}) = (c_{1,r-1}, c_{1,0}, .., , c_{1,r-2} | c_{2,s-1}, , c_{2,0} .., c_{2,s-2}) \in C$. It would also be of interest to characterize the hulls of double cyclic codes over R. This result would be of importance because the dimension of the hull of a code is used to determine the complexity of algorithms in coding theory. More specifically, codes with large hulls do not work with such algorithms. Another goal is to improve the table for the lower bounds on $\mathrm{LD}_2(n, K)$ provided in [6], where $\mathrm{LD}_2(n, k) = \max\{k|$there exists a binary $[n, k, d]$ LCD code$\}$. It would also be of interest to look at properties of $\mathrm{LD}_q(n, k) = \max\{k|$there exists a q-ary $[n, k, d]$ LCD code$\}$ where q is any prime power.

REFERENCES

[1] Alexis Bonnecaze and Parampalli Udaya, *Cyclic and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Transactions on Information Theory **45** (1999), no. 4, 1250–1255.

[2] A Robert Calderbank and Neil JA Sloane, *Modular and p-adic cyclic codes*, Designs, codes and Cryptography **6** (1995), no. 1, 21–35.

[3] Claude Carlet and Sylvain Guilley, *Complementary dual codes for counter-measures to side-channel attacks*, Advances in Mathematics of Communications **10** (2016), no. 1, 131.

[4] Claude Carlet, Sihem Mesnager, Chunming Tang, and Yanfeng Qi, *New characterization and parametrization of LCD codes*, IEEE Transactions on Information Theory **65** (2018), no. 1, 39–49.

[5] Claude Carlet, Sihem Mesnager, Chunming Tang, Yanfeng Qi, and Rudd Pellikann, *Linear codes over* $\mathbb{F}_q$ *are equivalent to LCD codes for* $q > 3$, IEEE Transactions on Information Theory **64** (2018), no. 4, 3010–3017.

[6] Steven T Dougherty, Jon-Lark Kim, Buket Ozkaya, Lin Sok, and Patrick Solé, *The combinatorics of LCD codes: linear programming bound and orthogonal matrices*, International Journal of Information and Coding Theory **4** (2017), no. 2-3, 116–128.

[7] Yilmaz Durgun, *On LCD codes over finite chain rings*, Bulletin of the Korean Mathematical Society **57** (2020), no. 1, 37–50.

[8] Yun Fan, San Ling, and Hongwei Liu, *Matrix product codes over finite commutative frobenius rings*, Designs, codes and cryptography **71** (2014), no. 2, 201–227.

[9] Philippe Gaborit, *Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings*, IEEE Transactions on Information Theory **42** (1996), no. 4, 1222–1228.

[10] Seth Gannon and Hamid Kulosman, *The condition for a cyclic code over $\mathbb{Z}_4$ of odd length to have a complementary dual*, arXiv preprint arXiv:1905.12309 (2019).

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

[12] Kenza Guenda, Somphong Jitman, and T Aaron Gulliver, *Constructions of good entanglement-assisted quantum error correcting codes*, Designs, Codes and Cryptography **86** (2018), no. 1, 121–136.

[13] A Roger Hammons, P Vijay Kumar, A Robert Calderbank, Neil JA Sloane, and Patrick Solé, *The $_4$-linearity of kerdock, preparata, goethals, and related codes*, IEEE Transactions on Information Theory **40** (1994), no. 2, 301–319.

[14] Masaaki Harada and Ken Saito, *Remark on subcodes of linear complementary dual codes*, Information Processing Letters **159** (2020), 105963.

[15] Raymond Hill, *A first course in coding theory*, Oxford University Press, 1986.

[16] W Cary Huffman and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge university press, 2010.

[17] Yan Jia, San Ling, and Chaoping Xing, *On self-dual cyclic codes over finite fields*, IEEE Transactions on Information Theory **57** (2011), no. 4, 2243–2251.

[18] Somphong Jitman, Ekkasit Sangwisut, and Patanee Udomkavanich, *Hulls of cyclic codes over* $\mathbb{Z}_4$, Discrete Mathematics **343** (2020), no. 1, 111621.

[19] San Ling and Patrick Sole, *Duadic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, Applicable algebra in engineering, communication and computing **12** (2001), no. 5, 365–379.

[20] Xiusheng Liu and Hualu Liu, *LCD codes over finite chain rings*, Finite Fields and Their Applications **34** (2015), 1–19.

[21] James L Massey, *Linear codes with complementary duals*, Discrete Mathematics **106** (1992), 337–342.

[22] Graham H Norton and Ana Sălăgean, *On the structure of linear and cyclic codes over a finite chain ring*, Applicable algebra in engineering, communication and computing **10** (2000), no. 6, 489–506.

[23] Binbin Pang, Shixin Zhu, and Xiaoshan Kai, *Some new bounds on LCD codes over finite fields*, Cryptography and Communications **12** (2020), no. 4, 743–755.

[24] Ekkasit Sangwisut, Somphong Jitman, San Ling, and Patanee Udomkavanich, *Hulls of cyclic and negacyclic codes over finite fields*, Finite Fields and Their Applications **33** (2015), 232–257.

[25] Gintaras Skersys, *The average dimension of the hull of cyclic codes*, Discrete applied mathematics **128** (2003), no. 1, 275–292.

[26] Zhe-Xian Wan, *Quaternary codes*, vol. 8, World Scientific, 1997.

[27] X. Yang and J.L. Massey, *The condition for a cyclic codes to have a complementary dual*, Discrete Math. **126** (1994), 391–393.

CURRICULUM VITAE

Dalton Seth Gannon
dalton.gannon@louisville.edu
802 East Madison Street., Apt B
Louisville, KY 40204
(859) 317-0198

EDUCATION

University of Louisville, Louisville, KY
Ph.D. in Applied and Industrial Mathematics — Expected, August 2022
Master of Arts in Mathematics — December 2018

University of Dayton, Dayton, OH
Master of Science in Applied Mathematics — May 2017
Concentrations in Discrete Mathematics & Applied Statistics

Transylvania University, Lexington, KY
Bachelor of Arts in Mathematics — May 2015
Minor in Interdisciplinary Business

TEACHING EXPERIENCE

Lecturer of Statistics, Bluegrass Community & Technical College June 2020 - July 2022

- Courses Taught:

Courses Taught:	Semester(s) Taught:
Finite Math and Applications	Summer'21
Applied Mathematics	Fall'21
Contemporary Mathematics	Spring'21
Mathematical Literacy	Spring'21
College Algebra Workshop	Fall'20, Fall'21
College Algebra	Fall'20, Fall'21, Spring'22
Introduction to Statistical Reasoning	Summer'20, Fall'20, Spring'21, Fall'21, Spring'22
Introduction to Statistical Reasoning (KSP Academy)	Fall'20, Fall'21
Statistics	Fall'20, Summer'21

Graduate Teaching Assistant, University of Louisville August 2017 - July 2022

- Courses Independently Taught: Semester(s) Taught:

Courses Independently Taught:	Semester(s) Taught:
College Algebra	Fall'21
Math for Elementary Education II	Spring'21
Math for Elementary Education I	Fall'20
Calculus I	Summer'19, Summer'21
Elements of Calculus	Summer'18

Recitation Courses Taught:	Semester(s) Taught:
Quantitative Reasoning	Fall'18
Contemporary Mathematics	Spring'18
Elementary Statistics	Fall'19
College Algebra	Fall'17, Fall'18 Fall'19, Spring'22
Elements of Calculus	Spring'18, Spring'20

Graduate Teaching Assistant, University of Dayton August 2015 - May 2017

Courses Independently Taught:	Semester(s) Taught:
Precalculus	Fall'16, Spring'17

Recitation Courses Taught:	Semester(s) Taught:
Analytic Geometry & Calculus II	Spring'16
Analytic Geometry & Calculus III	Fall'15

RESEARCH EXPERIENCE

University of Louisville, Louisville, KY
Doctoral Research January 2018 - May 2022
Faculty Advisor: Dr. Hamid Kulosman

- Dissertation Title: Defended May 18th, 2022
  Properties and Classifications of Certain LCD Codes

- Abstract:
  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 [6] 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 this dissertation we show that a necessary and sufficient condition for a cyclic code C over $\mathbb{Z}_4$ of odd length to be an LCD code is that $C = \big(f(x)\big)$ where f is a self-reciprocal polynomial in $\mathbb{Z}_4[X]$ which is also in our paper [10]. We then extend this result and provide a necessary and sufficient condition for a cyclic code C of length N over a finite chain ring $R = \big(R, \mathfrak{m} = (\gamma), \kappa = R/\mathfrak{m}\big)$ with $\nu(\gamma) = 2$ to be an LCD code. In a different direction, we find the formula for $\mathrm{LD}_2(n,2)$ which appears in [11]. In 2020, Pang et al. defined binary LCD $[n,k]$ codes with biggest minimal distance, which meets the Griesmer bound [23]. We give a correction to and provide a different proof for

[23, Theorem 4.2], provide a different proof for [23, Theorem 4.3], examine properties of LCD ternary codes, and extend some results found in [14] for any q which is a power of an odd prime.

University of Dayton, Dayton, OH
Masters Research May 2016 - March 2017
Faculty Advisor: Dr. Maher Qumsiyeh

- Master's Thesis Title: Defended March 17th 2017
  Bootstrapping General ARIMA Models
- Abstract:
  The Bootstrap of Efron (1979) has been shown to be an effective method for estimation and testing purposes. In regression models and in autoregressive time series models we resample the residuals to create new observation and use the ARIMA model to get estimates for parameters. This will not work in a moving average or mixed ARIMA models because the residuals are correlated. Due to this a different bootstrap approach must be used to deal with the dependency, known as, the non-overlapping block bootstrap method. In this paper we show how the non-overlapping block bootstrap method can be used for parameter estimation and for forecasting in a moving average and in a mixed autoregressive-moving average models for simulated data. The non-overlapping block bootstrap method will be compared with the Box-Jenkins methodology for parameter estimation and forecasting. We also compare the length of the confidence intervals for the parameters and forecasted values using the traditional methods and the non-overlapping block bootstrap method. All programming was completed using the statistical software package (SAS).

Air force Research Laboratory , Fairborn, OH
Research for Automated Technology Center program May 2016 - July 2017
Mentor: Hyatt Baker

- Abstract:
  The primary focus of this research was to establish models that represent a subset of the Moving and Stationary Target Acquisition and Recognition Laboratory(MSTAR) platform. This was done so that a model that would output similar results to what the MSTAR platform would generate could process data that had not been processed by the MSTAR platform. These models were built using machine learning techniques such as neural networks, decision trees, and k^{th} nearest neighbor. The MSTAR data was also examined with the AYASDI software in order to apply topological data analysis to algorithm modeling.

Papers:

Gannon, S., Kulosman, H., "The Formula For the Largest Minimal Distance of Binary LCD $[n, 2]$ Codes," submitted; Cornell University Library, arXiv:1909.00253v1 (August2019).

Gannon, S., Kulosman, H., "The condition For a Cyclic Code Over $\mathbb{Z}_4$ of Odd Length to have Complementary Dual," submitted; Cornell University Library, arXiv:1905.12309v1 (May2019).

Qumsiyeh, M., Deis, R., Gannon, S. (2017). "Bootstrapping An Auto Regressive Time Series Modeling Using SAS," Advances and Applications in Statistics, 50(6), 435-467.

Conferences & Presentations:

Seth Gannon. "LCD codes and the condition for cyclic codes over $\mathbb{Z}_4$ to be LCD". Special Session on "Coding Theory, Crypography, and Number Theory" at the Fall AMS Meeting, University of Tennessee at Chattanooga(virtual) (2020, October).

Seth Gannon. "LCD codes and the condition for cyclic codes over $\mathbb{Z}_4$ to be LCD". Graduate Student Regional Research Conference (2020, February).

Seth Gannon. "The Condition for a Quaternary Cyclic Code to be LCD". 39^{th} Western Kentucky University Mathematics Symposium (2019, November).

Seth Gannon and James Ryan. "ATR Modeling, Evaluation, and Validation using Machine Learning Techniques". ATR Center Summer Briefing and Poster Presentations (2016, August).

Seth Gannon and Kelli Marquardt. “University of Dayton Crime Rate Detection Using Time Series Analysis”. University of Dayton Stander Symposium (2016, May).

TECHNICAL SKILLS

Matlab, R, SAS, C++

COMMUNITY & UNIVERSITY ENGAGEMENT

Mercy High School Assistant Tennis Coach	February 2021 - present
University of Louisville GNAS President	May 2020 - July 2021
University of Louisville AMS Chapter President	May 2019 - July 2020
University of Louisville AMS Chapter Secretary	May 2018 - July 2019
Transylvania University Varsity Tennis Player	September 2011 - May 2015

AWARDS/HONORS

- Joint Mathematics Meeting Travel Grant November 2021
- Nominated to join the Society for Collegiate Leadership & Achievement October 2020
- Nominated to join Phi Kappa Phi Academic Honor Society February 2020
- Graduate Student Council Travel Fund Grant, University of Louisville December 2019
- University of Louisville Dean’s Citation Award Recipient December 2018

PROFESSIONAL MEMBERSHIPS

- Institute of Electrical and Electronics Engineers September 2021 - present
- Mathematical Association of America August 2015 - present
- American Mathematical Society August 2015 - present