ON THE HULL AND COMPLEMENTARITY OF CERTAIN QUASI-CYCLIC CODES

by

Zohreh Aliabadi

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Sabancı University

July 2022

On the Hull and Complementarity of Certain Quasi-Cyclic Codes

Zohreh Aliabadi

Mathematics, PhD Thesis, July 2022

Thesis Supervisor: Prof. Dr. Cem Güneri

Keywords: Hull of a code, linear complementary dual (LCD) code, linear complementary pair (LCP) of codes, quasi-cyclic code, double circulant code, four circulant code.

Abstract

Linear codes with small hull dimension have been of interest due to their applications to various problems in coding theory and cryptography. Linear complementary dual codes, which are codes with zero hull dimension, and their generalization called linear complementary pair of codes have also been studied widely in the literature. We study these notions for quasi-cyclic codes. We show that all admissible hull dimensions for quasi-cyclic codes, according to their CRT decomposition, are attained. We pay particular attention to double and four circulant codes, which are one and two generator quasi-cyclic codes of special form. We formulate the hull dimension for these families in terms of the polynomials involved in their generating elements. We obtain results on possible hull dimensions, such as the hull of a four circulant code being even and the nonexistence of hull dimension one double circulant codes over $\mathbb{F}_q$ if $q \equiv 3 \pmod 4$. We present numerical results on the parameters of double and four circulant codes with extra conditions, such as having fixed small hull dimension or being complementary dual. We also enumerate double and four circulant codes with zero or the smallest possible positive hull dimension and prove that double circulant codes with zero or one hull dimension are asymptotically good.

BAZI SANKİ-DEVİRSEL KODLARIN KABUKLARI VE BÜTÜNLEYİCİ ÖZELLİKLERİ

Zohreh Aliabadi

Matematik, Doktora Tezi, Temmuz 2022

Tez Danışmanı: Prof. Dr. Cem Güneri

Anahtar Kelimeler: Kod kabuğu, doğrusal bütünleyici dual kod, doğrusal bütünleyici kod çifti, sanki-devirsel kod, çift devirli kod, dört devirli kod.

Özet

Küçük kabuk boyutuna sahip doğrusal kodlar, kodlama teorisinde çeşitli problemlere ve kriptografiye uygulamaları sebebiyle ilgi çekmektedirler. Sıfır kabuk boyutuna sahip doğrusal bütünleyeci dual kodlar ve genellemeleri olan doğrusal bütünleyici kod çiftleri de literatürde çokça çalışılmaktadırlar. Bu tezde bahsi geçen kavramlar sanki-devirsel kodlar için çalışılmıştır. Sanki-devirsel kodların CRT parçalanışlarına göre mümkün olan tüm kabuk boyutlarının realize edildikleri gösterilmiştir. Bu kod ailelerinin kabuk boyutları, üreteçlerinde yer alan polinomlar cinsinden ifade edilmiştir. Dört devirli kodların çift boyutlu kabukları olması, $\mathbb{F}_q$ üzerinde tanımlı çift devirli kodlar için $q \equiv 3 \pmod 4$ durumunda 1 boyutlu kabuğun mümkün olmaması gibi kabuk boyutlarına dair sonuçlar elde edilmiştir. Küçük kabuk boyutlu olmak, doğrusal bütünleyici dual gibi ek şartlar sağlayan çift ve dört devirli kodların sayıları verilmiş, ayrıca 0 ve 1 kabuk boyutlu çift kodların asimptotik olarak iyi oldukları gösterilmiştir.

To my beloved Mohammad and my family

Acknowledgements

First of all, I would like to thank my advisor Prof. Dr. Cem Güneri, for all his guidance and support toward my P.hD. journey.
I also thank Assoc. Prof. Dr. Kağan Kurşungöz, Prof. Dr. Albert Levi, Prof. Dr. Ferruh Özbudak, Assoc. Prof. Dr. Seher Tutdere for being on my jury committee and their insightful comments.
It was a big chance to pursue my P.hD. degree as a member of SabancıUniversity. I would like to thank Sabancı, FENS graduate school, and all the people in the Mathematics department who helped me and the ones I learned a lot from them.
I am most grateful to my dear friends Prof. Nürdagul Anbar, Prof. Suha Orhun Mutluergil, and Dr. Canan Kaşıkcı who have been there for me all the times. My special thanks to Dr. Tekgül Kalaycı for her enormous help and contribution to my PhD. life, there is no word that I can express my appreciation to her.
Last but not least, I would like to thank my family for their love and support in my entire life. I am so lucky to have my beloved Mohammad by my side, my biggest thanks to him for supporting and encouraging me in all my ups and downs.

Table of Contents

List of Tables

Introduction

The hull of a linear code C is defined as $C \cap C^{\perp}$, where $C^{\perp}$ is the Euclidean dual code. The hull can also be defined with respect to other inner products, such as the Hermitian inner product, if C is defined over a finite field $\mathbb{F}_q$ with square cardinality. This concept was introduced by Assmus and Key in ([?]) in order to classify finite projective planes. The hull of a linear code has found applications such as determining permutation equivalence between codes, determining the automorphism group of a code and construction of quantum error-correcting codes ([?], [?], [?], [?]).

Sendrier determined the number of linear codes with given hull dimension in [?], where he also showed that the hull dimension is usually small. He also proved that linear codes with fixed hull dimension meet the Gilbert-Varshamov Bound ([?]). We also refer to [?], where the hull of algebraic code families, namely cyclic and negacyclic codes, are investigated.

For applications, codes with small hull dimension are desired. The smallest positive hull dimension is 0, and codes having trivial hull are called linear complementary dual (LCD) codes. LCD codes were introduced by Massey in [?], where he also showed that this class of codes is asymptotically good. Of course, Sendrier's stronger asymptotic observation mentioned above also implies this. Note that the name LCD is justified, since $C \oplus C^{\perp} = \mathbb{F}_q^n$ for an LCD code $C \subseteq \mathbb{F}_q^n$. Let us note that LCD codes have been generalized to linear complementary pair (LCP) of codes, where a pair (C, D) of linear codes in $\mathbb{F}_q^n$ is called LCP if $C \oplus D = \mathbb{F}_q^n$. Note that an LCD code amounts to $(C, C^{\perp})$ being LCP.

There is yet another motivation to study LCD and LCP of codes, which stem from cryptography. It has been observed that certain cryptosystems, which are defined via linear codes, are more secure against attacks if one uses LCD or LCP of codes in their construction ([?], [?], [?]). The security parameter of an LCP (C, D) of codes is defined as $\min\{d(C), d(D^{\perp})\}$, which is simply $d(C)$ in the case of LCD codes. LCD and LCP of codes have been very actively studied in the recent literature ([?], [?], [?], [?], [?], [?], [?], [?]).

The next smallest possible hull dimension is 1 and due to above-mentioned motivations, construction of codes with 1 dimensional hull also found interest in recent literature ([?], [?], [?]).

This thesis studies concepts described above for general and also some special classes of quasi-cyclic (QC) codes. QC codes are natural generalization of the well-known family of cyclic codes. A linear code C is called QC of index l if it is closed under l-shift of codewords, and l is the smallest such number. The case $l = 1$ clearly amounts to cyclic codes. Like cyclic codes, QC codes also come with nice algebraic structure ([?], [?]). Finally, double and four circulant codes are special types of QC codes. We prove results on hulls and LCD/LCP classes for aforementioned code families. We also present some numerical results on the parameters of codes studied.

Chapter 1 introduces the required background on the hull of linear codes and LCD/LCP codes. Chapter 2 starts by introducing QC codes and their CRT decomposition. Decomposition of the code and its dual yield a natural formula for the hull dimension of a QC code. The rest of this chapter is devoted to showing that all admissible hull dimensions for a QC code are attained. Chapter 3 studies special classes of QC codes, namely double-circulant (DC) and four-circulant (FC) codes. For general 1-generator QC codes, results on their hull dimension and LCD/LCP features are proved. Results on these concepts are also obtained for DC and FC codes, as well as the enumeration of DC code, with small hull dimension and the asymptotic consequences. Chapter 3 also provides numerical result on the code families studied.

CHAPTER 1

Background

We give basic definitions and facts on linear codes, which will be used in the thesis. Throughout the thesis $\mathbb{F}_q$ denotes a finite field with q elements.

1.1 Linear Codes and Their Duals

For $x \in (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, the Hamming distance is defined as

$$d(x, y) := \#\{1 \le i \le n \ ; \ x_i \ne y_i\}.$$

The Hamming weight of an element is defined as

$$\mathrm{wt}(x) := d(x, 0) = \#\{1 \le i \le n \ ; \ x_i \ne 0\}.$$

An $[n, k, d]$ linear code over $\mathbb{F}_q$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$ with minimum distance d. The minimum distance is defined by

$$d = d(C) := \min\{d(x, y) \ ; \ x, y \in C \ , \ x \ne y\}.$$

For a linear code it is easy to see that the minimum distance is the same as the minimum weight among nonzero elements of the code.

The dual $C^\perp$ of a linear code can be defined with respect to various inner products on $\mathbb{F}_q^n$. $C^\perp$ is another linear code, whose dimension is $n-k$. We will be interested in Euclidean and Hermitian duals in this thesis, which are defined as follows:

$$C^\perp := \{x \in \mathbb{F}_q \; ; \; < c, x >= \sum_{i=1}^{n} c_i x_i = 0 \quad \forall c \in C\}$$

$$C^{\perp_h} := \{x \in \mathbb{F}_{q^2}^n \; ; \; < c, x >_h = \sum_{i=1}^{n} c_i \bar{x}_i = 0 \quad \forall c \in C\}$$

We note that Hermitian dual is only defined over a square field $\mathbb{F}_{q^2}$. We also note that $\bar{a}$ denotes the $\mathbb{F}_q$-conjugate a^q for an element $a \in \mathbb{F}_{q^2}$.

A $k \times n$ matrix G, whose rows consist of basis elements of an $[n,k]$ linear code C, is called a generator matrix of C. A $(n-k) \times n$ generator matrix H for the dual code $C^\perp$ is called a parity check matrix of C. It is clear that we have

$$GH^T = 0.$$

If $G = [Id_k \; : \; A]$ is a generator matrix in systematic form, then we have $H = [-A^T \; : \; Id_{n-k}]$. Note that the parity check matrix for the Hermitian inner product is $\bar{H} = [-\bar{A}^T \; : \; Id_{n-k}]$, where $\bar{A}$ denotes the matrix obtained from A by $\mathbb{F}_q$-conjugate in each entry.

1.2 Hull of a Linear Code

Let C be an $[n,k,d]_q$ linear code. Hull of C is defined as

$$\mathrm{Hull}(C) := C \cap C^\perp.$$

Let $h(C) = \dim(\mathrm{Hull}(C))$. If q is square one can define the Hermitian hull of C as

$$\mathrm{Hull}_h(C) := C \cap C^{\perp_h}$$

and denote its dimesion by $h_h(C) = \dim(\mathrm{Hull}_h(C))$.

Proposition 1.2.1. *(Proposition 3.1 [?])*

i: Let C be an $[n,k]_q$ linear code with generator matrix G and parity check matrix H. Then

$$h(C) = k - rank(GG^T).$$

ii: Let C be an $[n,k]_{q^2}$ linear code with generator matrix G and parity check matrix H. Then

$$h_h(C) = k - rank(G\bar{G}^T).$$

We will denote the dimension of the intersection of $C_1 \cap C_2^{\perp}$ for two linear codes C_1 and C_2 by $h(C_1, C_2)$. Note that $h(C) = h(C, C)$.

Proposition 1.2.2. *(Theorem 2.1 [?]): For $i \in \{1,2\}$, let C_i be a linear $[n,k_i]_q$ code with parity check matrix H_i and generator matrix G_i. If $\dim(C_1, C_2) = \ell$, then*

$$rank(G_1 H_2^T) = k_1 - \ell,$$

and

$$rank(G_2 H_1^T) = k_2 - \ell.$$

As a consequence of Proposition **??**, we can write

$$h(C_1, C_2) = k_1 - \operatorname{rank}(G_1 G_2^T) \qquad \textit{and} \qquad h(C_2, C_1) = k_2 - \operatorname{rank}(G_2 G_1^T)$$

1.3 LCD and LCP of Linear Codes

Definition 1.3.1. *i: An $[n,k]_q$ linear code is called a linear complementary dual (LCD) code, if Hull(C) $= \{0\}$.*

ii: A pair (C, D) of linear codes of length n over $\mathbb{F}_q$ is called linear complementary pair (LCP) of codes if $C \oplus D = \mathbb{F}_q^n$.

Note that LCP of codes can be considered as a generalization of LCD codes. Namely if C is an LCD code, the pair $(C, C^{\perp})$ is LCP.
The following is a consequence of Proposition **??** and **??**. We note that the characterization of LCD codes in (i) was first given by Massey in ([?]).

Proposition 1.3.1. *i: A linear code C with a generator matrix G is LCD if and only if GG^T is non-singular.*

ii: Let C_i be an $[n,k_i]$ linear code, for $i = 1,2$, with generator and parity check matrices G_i, H_i, respectively. Then (C_1, C_2) is LCP of codes if and only if $k_1 + k_2 = n$ and $G_1 H_2^T$ is non-singular.

LCD and LCP of codes drew attention recently due to their cryptographic applications ([?], [?]). In this respect, the security parameter of an LCP (C, D) of codes is defined as

$$\min\{d(C), d(D^{\perp})\}.$$

Note that if C is LCD (i.e. $D = C^{\perp}$ above), the security parameter is simply $d(C)$. It has been shown that if (C, D) is LCP of abelian codes (or, group codes more generally), we also have $d(C)$ as the security parameter. This is established by showing that C and $D^{\perp}$ are equivalent codes ([?], [?], [?]).

CHAPTER 2

Quasi-Cyclic Codes

This chapter presents the algebraic structure of quasi-cyclic (QC) codes. We also provide a proof for the existence of QC codes of given hull dimension.

2.1 QC Codes

An $[n, k]_q$ linear code is called a QC code of index l, if its codewords are invariant under shift by l units, and l is the smallest positive integer with this property. It is known that the index of a QC code is a divisor of its length, say $n = ml$. We refer to the QC code of index l as l-QC code for simplicity. The well-known cyclic codes correspond to QC codes of index 1. As in cyclic codes, QC codes can also be viewed algebraically.

Let C be an l-QC code of length ml over $\mathbb{F}_q$, and write its codewords in $m \times l$ array form

$$\overrightarrow{c} = \begin{pmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,l-1} \end{pmatrix}.$$

In this representation, note that being invariant under shift by l units amounts to being invariant under row shift.

Let $R_m := \frac{\mathbb{F}_q[x]}{<x^m-1>}$ and consider the map

$$\begin{aligned} \phi \; : \; \mathbb{F}_q^{ml} \; &\rightarrow \; R_m^l \\ \overrightarrow{c} \; &\mapsto \; (c_0(x), \ldots, c_{l-1}(x)), \end{aligned} \tag{2.1}$$

where $c_j(x) = \sum_{i=0}^{m-1} c_{i,j}x^i \in R_m$ for $0 \leq j \leq l-1$. In other words each column in $\overrightarrow{c}$ produces an entry for $\phi(\overrightarrow{c}) \in R_m^l$.

Proposition 2.1.1. *i: ([?] Lemma 3.1) The map ϕ induces a 1-1 correspondence between l-QC codes over $\mathbb{F}_q$ of length ml and linear codes over R_m of length l (i.e. R_m-submodule in R_m^l).*

ii: ([?], Corollary 3.3) Under this correspondence, we have $\phi(C^\perp) = \phi(C)^\perp$. Here duality in $\mathbb{F}_q^{ml}$ is with respect to the Euclidean inner product. Duality in R_m^l is with respect to the inner product

$$(a_0(x), \ldots, a_{l-1}(x)).(b_0(x), \ldots, b_{l-1}(x)) = \sum_{i=0}^{l-1} a_i(x)\bar{b}_i(x),$$

where $\bar{b}_i(x) = b_i(x^{-1}) = b_i(x^{m-1})$.

From now on, we assume that q and m are relatively prime. With this assumption we have the following factorization into distinct polynomials.

$$x^m - 1 = \prod_{i=1}^{s} g_i(x) \prod_{j=1}^{t} (h_j(x)h_j^*(x)).$$

Here $g_i(x)$ is self-reciprocal for $1 \leq i \leq s$ and $h_j(x)$ and $h_j^*(x)$ are reciprocal pairs for $1 \leq j \leq t$, where the reciprocal of a monic polynomial $f(x)$ with non-zero constant term is defined as

$$f^*(x) = f(0)^{-1}x^{\deg f} f(x^{-1}).$$

By the Chinese Remainder Theorem (CRT), R_m decomposes as follows:

$$R_m = (\bigoplus_{i=1}^{s} \mathbb{G}_i) \bigoplus (\bigoplus_{j=1}^{t} (\mathbb{H}'_j \bigoplus \mathbb{H}''_j)),$$

where for $1 \leq i \leq s$, $\mathbb{G}_i = \frac{\mathbb{F}_q[x]}{<g_i(x)>}$, and for $1 \leq j \leq t$, $\mathbb{H}'_j = \frac{\mathbb{F}_q[x]}{<h_j(x)>}$ and $\mathbb{H}''_j = \frac{\mathbb{F}_q[x]}{<h_j^*(x)>}$. Thus

$$R_m^l = (\bigoplus_{i=1}^{s} \mathbb{G}_i^l) \bigoplus (\bigoplus_{j=1}^{t} (\mathbb{H}'^l_j \bigoplus \mathbb{H}''^l_j)).$$

Let ξ be a primitive m^{th} root of unity and ξ^{u_i}, ξ^{v_j} and ξ^{-v_j} be roots of $g_i(x)$, $h_j(x)$ and $h_j^*(x)$, respectively. Then we have

$$\mathbb{G}_i \cong \mathbb{F}_q(\xi^{u_i}) \cong \mathbb{F}_{q^{2d_i}},\ \mathbb{H}'_j \cong \mathbb{F}_q(\xi^{v_j}) \cong \mathbb{F}_{q^{d_j}},\ \mathbb{H}''_j \cong \mathbb{F}_q(\xi^{-v_j}) \cong \mathbb{F}_{q^{d_j}}$$

where $2d_i = \deg g_i(x)$ and $d_j = \deg h_j(x) = \deg h_j^*(x)$. Note that we use the fact that the degree of a self-reciprocal polynomial is even.

Via the CRT decomposition of R_m^l, any QC code C can be decomposed as

$$C = (\bigoplus_{i=1}^{s} C_i) \bigoplus (\bigoplus_{j=1}^{t} (C'_j \bigoplus C''_j)), \tag{2.2}$$

where C_i, C'_j, C''_j are linear codes of length l over the fields $\mathbb{G}_i, \mathbb{H}'_j, \mathbb{H}''_j$, respectively. They are called the constituents of C. Moreover, we have

$$\dim(C) = \sum_{i=1}^{s} \deg g_i(x) \dim(C_i) + \sum_{j=1}^{t} \deg h_j(x)[\dim(C'_j) + \dim(C''_j)].$$

It is well-known that the dual of an l-QC code is also an l-QC code of length ml and it has the following CRT decomposition

$$C^{\perp} = (\bigoplus_{i=1}^{s} C_i^{\perp_h}) \bigoplus (\bigoplus_{j=1}^{t} (C''^{\perp}_j \bigoplus C'^{\perp}_j)), \tag{2.3}$$

where $C_i^{\perp_h}$ denotes the Hermitian dual of C_i in $\mathbb{F}_{q^{\deg g_i}}$. Hence we have

$$\mathrm{Hull}(C) = C \cap C^{\perp} = (\bigoplus_{i=1}^{s} (C_i \cap C_i^{\perp_h})) \bigoplus (\bigoplus_{j=1}^{t} (C'_j \cap C''^{\perp}_j) \bigoplus (C''_j \cap C_j^{\perp})), \tag{2.4}$$

and the hull dimension is

$$h(C) = \sum_{i=1}^{s} \deg g_i(x)\ h_h(C_i) + \sum_{j=1}^{t} \deg h_j(x)[h(C'_j, C''_j) + h(C''_j, C'_j)]$$

Hence the hull of an l-QC code C over $\mathbb{F}_q$ is formulated in terms of Hermitian hulls and pairwise intersection of its constituent codes and their duals, which are codes of length l over various field extensions of $\mathbb{F}_q$. Let

$$\ell = t_1 + \sum_{i=2}^{s} 2d_i t_i + \sum_{j=1}^{t} d'_j (t'_j + t''_j) \qquad \textit{if } m \textit{ is odd} \tag{2.5}$$

$$\ell = t_1 + t_2 + \sum_{i=3}^{s} 2d_i t_i + \sum_{j=1}^{t} d'_j (t'_j + t''_j) \qquad \textit{if } m \textit{ is even} \tag{2.6}$$

be integers, with $t_i \leq k_i$, $t'_j \leq k'_j$ and $t''_j \leq k''_j$, where $k_i = \dim(C_i)$, $k'_j = \dim(C'_j)$ and $k''_j = \dim(C''_j)$. Note that these express possible hull dimensions for QC codes. Our aim is to understand whether all such hull dimensions can be realized by l-QC codes.

2.2 Linear and QC Codes with Arbitrary Hull Dimension

In order to understand possible hull dimension for QC codes, we investigate existence of linear codes with arbitrary Euclidean and Hermitian hull dimensions.

Proposition 2.2.1. *Let n, k be positive integers such that $2k \leq n$. Then for any $t \leq k$, there exists an $[n,k]_q$ linear code with t-dimensional hull.*

Proof. Define the matrix

$$G_t = \left[\begin{array}{c|c} Id_{k-t} & O \\ \hline O & D \end{array}\right] \in M_{k\times n}(\mathbb{F}_q)$$

where $D \in M_{(t\times(n-(k-t)))}(\mathbb{F}_q)$. Note that $\operatorname{rank}(G_tG_t^T) = k-t$ if and only if $DD^T = 0$. The following choices of the matrix D give us $DD^T = 0$.

i: $q = 2^r$ for some $r \geq 1$:

$$D = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 & \dots & 0 \end{pmatrix}$$

ii: $q \equiv 1 \pmod 4$: In such finite fields -1 is a quadratic residue, i.e., there exists $\alpha \in \mathbb{F}_q^*$ such that $\alpha^2 = -1$. Take

$$D = \begin{pmatrix} 1 & \alpha & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \alpha & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & \alpha & \dots & 0 \end{pmatrix}$$

Then $DD^T = 0$.

Note that in both cases above at least $2t$ columns are needed to define D. We have $2k \leq n$ and $t \leq k \leq n-k$. Therefor $2t \leq n-(k-t)$, so D is well-defined. Also it is clear that in both cases $\operatorname{rank}(D) = t$.

iii: $q \equiv 3\ (mod\ 4)$

Consider the curve χ over $\mathbb{F}_q$ defined by

$$\chi : x^2 + y^2 + (a - x)^2 = 0$$

over $\mathbb{F}_q$, where $a \in \mathbb{F}_q^{\times}$. If we study the points at infinity, we have

$$2x^2 + y^2 = 0 \qquad so \qquad y^2 = -2x^2.$$

If -2 is a quadratic residue in $\mathbb{F}_q$ then χ has two points at infinity. This means that χ has at least $q-1$ affine rational points, since it is of genus 0 and has $q+1$ rational points.

Note that for $q \equiv 3 \pmod 4$, a self-dual linear code exists only when $n \equiv 0 \pmod 4$ (see the proof of Proposition 6.3 in ([?])). Also for a self-dual code we have $h(C) = t = k = \frac{n}{2}$, which means that length is even. For this reason we distinguish between the even and odd t.

- t is even:

$$D = \begin{pmatrix} \alpha & \beta & a-\alpha & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \alpha - a & \beta & -\alpha & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \alpha & \beta & a-\alpha & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha - a & \beta & -\alpha & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & \alpha & \beta & a-\alpha & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & \alpha - a & \beta & -\alpha & \dots & 0 \end{pmatrix}$$

  In this case again we need at least $2t$ columns and as before D is well-defined with rank t.

- t is odd:

$$D = \begin{pmatrix} \alpha & \beta & a-\alpha & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \alpha - a & \beta & -\alpha & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \alpha & \beta & a-\alpha & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha - a & \beta & -\alpha & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & \alpha & \beta & a-\alpha & 0 & \dots & 0 \end{pmatrix}$$

  First note that, at least $2t+2$ columns are needed to define D. We have $t \leq k-1$, and $2k \leq n$ which means that $2k+1 < n$. All together we obtain that $2t+2 < n-(k-t)$, thus D is well-defined with rank t.

In all the cases, where the description of D in G_t is given, rows of G_t are linearly independent. Hence $\text{rank}(G_t) = k$. The code C generated by G_t is an $[n,k]_q$ linear code with t-dim hull. $\square$

The next step is to show the existence of linear codes over square fields of given t-dimensional Hermitian hull.

Proposition 2.2.2. *Let q be a square, and n, k be positive integers such that $2k \leq n$. Then for any $t \leq k$, there exists an $[n,k]_q$ linear code with t-dimensional Hermitian hull.*

Proof. As in the proof of Proposition **??** define the matrix

$$G_t = \left[\begin{array}{c|c} Id_{k-t} & 0 \\ \hline 0 & D \end{array}\right] \in M_{k\times n}(\mathbb{F}_q),$$

where $A = Id_{k-t}$, and $D \in M_{(t\times(n-(k-t)))}(\mathbb{F}_q)$. Note that $rank(G_t\bar{G}_t^T) = k-t$ if and only if $D\bar{D}^T = 0$.

The following choices of the matrix D gives us $D\bar{D}^T = 0$.

i: $q = 2^r$, where r is an even integer: Let α be an element of $\mathbb{F}_q$, and $\beta \in \mathbb{F}_q^*$ be its conjugate, i.e. $\bar{\alpha} = \alpha^{\sqrt{q}} = \beta$. Take

$$D = \begin{pmatrix} \alpha & \beta & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \alpha & \beta & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & \alpha & \beta & \dots & 0 \end{pmatrix}$$

Then

$$\bar{D} = \begin{pmatrix} \beta & \alpha & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \beta & \alpha & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & \beta & \alpha & \dots & 0 \end{pmatrix}$$

and $D\bar{D}^T = 0$.

ii: $q = s^r$, with s an odd prime and r an even integer:

$|\mathbb{F}_q^*| = q-1 = (\sqrt{q}-1)(\sqrt{q}+1)$, so we have $2(\sqrt{q}+1) \mid |\mathbb{F}_q^*|$. Thus, there exists $\beta \in \mathbb{F}_q^*$ such that $| < \beta > | = 2(\sqrt{q}+1)$. Take

$$D = \begin{pmatrix} 1 & \beta & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \beta & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & \beta & \dots & 0 \end{pmatrix}.$$

Then

$$\bar{D} = \begin{pmatrix} 1 & \beta^{\sqrt{q}} & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \beta^{\sqrt{q}} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & \beta^{\sqrt{q}} & \dots & 0 \end{pmatrix}$$

and we have

$$D\bar{D}^T = \begin{pmatrix} 1+\beta^{\sqrt{q}+1} & 0 & \dots & 0 & \dots & 0 \\ 0 & 1+\beta^{\sqrt{q}+1} & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & 0 \\ 0 & 0 & \dots & 1+\beta^{\sqrt{q}+1} & \dots & 0 \end{pmatrix}$$

As $\beta^{2(\sqrt{q}+1)} = 1$, we have $\beta^{\sqrt{q}+1} = -1$. Therefore $D\bar{D}^T = 0$.

Like the Euclidean case, D is a well-defined matrix of rank t. Thus G_t generates an $[n,k]_q$ linear code of t-dimensional Hermitian hull. $\square$

Note that the hull of a QC code also involves intersection of two vector spaces. Although finding spaces that intersect at desired dimension is clearly achievable, we show the details in the following. Let C_1 and C_2 be two linear codes over a finite field. Then

$$h(C_1,C_2) + h(C_2,C_1) = k_1 - \text{rank}(G_1G_2^T) + k_2 - \text{rank}(G_2G_1^T) = k_1 + k_2 - 2\text{rank}(G_1G_2^T).$$

Without loss of generality assume that $k_1 \leq k_2$. For the constituents coming from reciprocal pairs, we need to find matrices G_1 and G_2 such that $rank(G_1G_2^T) = t$, where $t \leq k_1$. Let C_1 and C_2 be linear codes generated as follows

$$C_1 = < e_1, \dots, e_{k_1} >,$$

$$C_2 =< e_1, \ldots, e_t, e_{k_1+1}, \ldots, e_{k_2}, e_{k_2+1}, \ldots, e_{k_2+k_1-t} > .$$

By Sylvester's inequality we have

$$k_1 + k_2 - n \leq t \;\Rightarrow\; k_2 + k_1 - t \leq n.$$

Also, the number of vectors in the basis of C_2 is

$$t + (k_2 - (k_1 + 1) + 1) + (k_2 + k_1 - t - (k_2 + 1) + 1) = k_2$$

It is clear that all vectors are distinct, thus the basis is well-defined.

Therefore

$$G_1 = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_t \\ e_{t+1} \\ \vdots \\ e_{k_1} \end{pmatrix} \qquad \textit{and} \qquad G_2 = \begin{pmatrix} e_1 \\ \vdots \\ e_t \\ e_{k_1+1} \\ \vdots \\ e_{k_2} \\ \vdots \\ e_{k_2+k_1-t} \end{pmatrix}$$

For the standard vectors e_i's, we have

$$e_i.e_j^T = \delta_{ij}.$$

Therefor the i^{th}-row of $G_1G_2^T$ is

$$e_iG_2^T = \begin{pmatrix} e_ie_1^T & \ldots & e_ie_t^T & e_ie_{k_1+1}^t & \ldots & e_ie_{k_2+k_1-t}^T, \end{pmatrix},$$

and

$$G_1G_2^T = \begin{pmatrix} e_1 \\ \vdots \\ e_t \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

which has rank t.

Note that, by Proposition 6.3 in [?], there is no self-dual l-QC codes of length ml when l is odd and $q \equiv 3 \pmod 4$. In such case there exists self-dual l-QC code if and only if l is a multiple of 4.

From the discussion above, we reach the following consequence, which is the main result of this section.

Theorem 2.2.3. *Let $\mathbb{F}_q$ be a finite field, m a positive integer relatively prime to q, $0 < k \leq ml$ and $\ell \leq k$. Then there exists an $[ml, k]_q$ l-QC code with ℓ-dimensional hull if ℓ can be written as in **??** or **??**, with the exception of $\ell = k$ is odd and $q \equiv 3 \pmod 4$.*

CHAPTER 3

Double and Four Circulant Codes

The hull and LCP properties of a special class of one and two generator QC codes are investigated in this chapter.

3.1 1-Generator QC Codes

Let C be a ρ-generator l-QC code of length ml over $\mathbb{F}_q$, which is generated by

$$\{(a_{1,1}(x),\dots,a_{1,l}(x)),\dots,(a_{\rho,1}(x),\dots,a_{\rho,l}(x))\}$$

in R_m^l. Via CRT decomposition, one can write spanning sets for its constituents:

$$C_i := Span_{\mathbb{G}_i}\{(a_{b,1}(\xi^{u_i}),\dots,a_{b,l}(\xi^{u_i}))\ :\ 1\le b\le \rho\} \quad for \quad 1\le i\le s$$

$$C'_j := Span_{\mathbb{H}'_j}\{(a_{b,1}(\xi^{v_j}),\dots,a_{b,l}(\xi^{v_j}))\ :\ 1\le b\le \rho\} \quad for \quad 1\le j\le t$$

$$C''_j := Span_{\mathbb{H}''_j}\{(a_{b,1}(\xi^{-v_j}),\dots,a_{b,l}(\xi^{-v_j}))\ :\ 1\le b\le \rho\} \quad for \quad 1\le j\le t$$

.

We will consider 1-generator QC codes.

Definition 3.1.1. *Let $C =< (a_1(x),\dots,a_l(x)) >$ be a 1-generator l-QC code over $\mathbb{F}_q$.*

i: The generator polynomial of C is defined by

$$g(x) := \gcd(a_1(x),\dots,a_l(x),x^m-1).$$

ii: A monic polynomial $h(x)$ of the least degree is called the parity check polynomial of C if $h(x)a_i(x) = 0$ for all $1 \leq i \leq l$.

The polynomials $g(x)$ and $h(x)$ are unique ([?], Lemma 2) and they satisfy

$$h(x)g(x) = x^m - 1.$$

Lemma 3.1.1. *([?], Lemma 1) Let $C =< a_1(x), \dots, a_l(x)) >$ be a 1-generator l-QC code of length ml over $\mathbb{F}_q$. Then*

$$\dim C = m - \deg g(x) = \deg h(x).$$

Definition 3.1.2. *An $[ml, k]_q$ 1-generator l-QC code is called maximal if $k = m$.*

If C is a maximal 1-generator l-QC code, we clearly have

$$g(x) = 1 \qquad \& \qquad h(x) = x^m - 1.$$

A class of such codes, namely Double Circulant (DC) codes, will be discussed later in this chapter.

3.1.1 LCD 1-generator l-QC Codes

Let C be an $[ml, k]_q$, l-QC code with the CRT decomposition as in (??). Then its dual decomposes as in (??). A characterization of LCD QC codes has been provided as follows.

Theorem 3.1.2. *([?], Theorem 3.1) Let C be an l-QC code of length ml over $\mathbb{F}_q$. Then C is LCD if and only if $C_i \cap C_i^{\perp_h} = \{0\}$ for all $1 \leq i \leq s$, and $C'_j \cap C''^{\perp}_j = C''_j \cap C'^{\perp}_j = \{0\}$ for all $1 \leq j \leq t$.*

LCD 1-generator QC codes can be characterized as follows.

Theorem 3.1.3. *Let $C =< (a_1(x), \dots, a_l(x)) >$ be a 1-generator l-QC code of length ml over $\mathbb{F}_q$. Then C is LCD if and only if*

$$\gcd\left(\sum_{r=1}^{l} a_r(x)a_r(x^{m-1}), h(x)\right) = 1.$$

Proof. Note that the constituents of C are either 0 or 1-dimensional codes over their field of definition. So the intersections we have to understand are either trivial or 1-dimensional.

- $C_i \cap C_i^{\perp_h} \neq \{0\}$ if and only if
  - $C_i \neq \{0\}$, which means $g_i(x) \mid h(x)$,
  - $C_i \subseteq C_i^{\perp_h}$ which means that $\sum_{r=1}^{l} a_r(\xi^{u_i})a_r(\xi^{-u_i}) = 0$. This implies that $g_i(x) \mid \sum_{r=1}^{l} a_r(x)a_r(x^{m-1})$.
- $C'_j \cap C''^{\perp}_j \neq \{0\}$ if and only if
  - $C'_j \neq \{0\}$, which means $h_j(x) \mid h(x)$,
  - $C'_j \subseteq C''^{\perp}_j$, which means that $\sum_{r=1}^{l} a_r(\xi^{v_j})a_r(\xi^{-v_j}) = 0$. This implies $h_j(x) \mid \sum_{r=1}^{l} a_r(x)a_r(x^{m-1})$.
- Using the same argument, $C''_j \cap C'^{\perp}_j \neq \{0\}$ if and only if $h_j^* \mid h(x)$ and $h_j^*(x) \mid \sum_{r=1}^{l} a_r(x)a_r(x^{m-1})$.

Hence, C is LCD if and only if the factors of x^m-1 divide either $h(x)$ or $\sum_{r=1}^{l} a_r(x)a_r(x^{m-1})$, but not both. □

Remark 3.1.1. *LCD characterization for a special class of maximal 1-generator 2-QC codes (namely, double circulant codes), is given in ([?], Theorem 5.1). Theorem* **??** *generalizes this result.*

Tables 3.1 and 3.2 illustrate binary and ternary LCD maximal 1-generator 2-QC codes of length $2m$. The search is done by the MAGMA software [?] for random $a_1(x), a_2(x) \in R_m$ satisfying $\gcd(a_1(x)a_1(x^{m-1}) + a_2(x)a_2(x^{m-1}), x^m - 1) = 1$. In these two tables d presents the best possible minimum distance which can be attained by an LCD maximal 1-generator 2-QC code $C =< a_1(x), a_2(x)) >$, d^* represents optimal minimum distance for binary or ternary linear codes of length $2m$ and dimension m, according to code tables [?].

m	d	d^*	$a_1(x)$	$a_2(x)$
3	2	3	$x+1$	x^2+x+1
5	3	4	x^3+1	x^2+x+1
7	4	4	x^2+1	x^3+x+1
9	5	6	x^5+x+1	x^5+x^2+x+1
11	6	7	x^4+1	$x^8+x^7+x^6+x^2+1$
13	7	7	x^5+1	$x^{11}+x^9+x^6+x^3+1$
15	7	8	x^6+x^2+x+1	x^5+x+1
17	8	8	x^6+x^4+x+1	$x^5+x^4+x^3+x+1$

Table 3.1: Binary LCD maximal 1-generator 2-QC Codes.

m	d	d^*	$a_1(x)$	$a_2(x)$
4	4	4	$x+1$	$x+2$
5	4	5	$x+2$	$2x+2$
7	6	6	$2x+1$	x^3+2x^2+x+2
8	6	6	x^3+2x+2	xx^2+2x+2
10	6	7	x^3+x+1	x^2+2x+1
11	7	8	x^3+2x+2	x^3+2x^2+2x+1
13	8	8	x^3+x^2+x+1	x^4+x^2+2x+2
14	8	9	x^4+x^2+x+2	x^3+2x^2+x+1

Table 3.2: Ternary LCD maximal 1-generator 2-QC Codes.

As it is mentioned before, cyclic codes are 1-QC codes. It has been shown that a cyclic code is LCD if and only if its generator polynomial is self-reciprocal ([?]). The next proposition states that self-reciprocal generator polynomial is a necessary condition for being LCD for 1-generator QC codes.

Proposition 3.1.4. *Let $C =< (a_1(x), \ldots, a_l(x)) >$ be a 1-generator l-QC code with generator polynomial $g(x)$. If C is LCD then $g(x)$ is self-reciprocal.*

Proof. Assume that $g(x)$ is not self-reciprocal. This implies that there exists $h_j(x)$ such that $h_j(x) \mid g(x)$ but $h_j^*(x) \nmid g(x)$ (hence, $h_j^*(x) \mid h(x)$). Since $h_j(x) \mid g(x)$, we have that $h_j(x) \mid a_u(x)$, for all $1 \leq u \leq l$. Therefore $h_j^*(x) \mid a_u(x^{m-1})$ for all u. Hence

$$h_j(x) \mid \gcd(\sum_{r=1}^{l} a_r(x)a_r(x^{m-1}), h(x))$$

which contradicts the assumption that C is LCD. $\square$

The following example shows that the converse of Proposition **??** need not hold.

Example 3.1.1. *Let $C =< (x^2 + x, x^2 + 1 >)$ be $[6, 2]_2$ 1-generator 2-QC code. Note that $g(x) = x + 1$ and $h(x) = x^2 + x + 1$, and both are self-reciprocal polynomials. However $h(C) = 2$, and hence it is not LCD.*

Determining the hull of 1-generator l-QC codes is an immediate consequence of Theorem **??**.

Corollary 3.1.5. *Let $C =< (a_1(x), \ldots, a_l(x)) >$ be a 1-generator l-QC code of length ml over $\mathbb{F}_q$. Then $h(C) = \deg u(x)$, where*

$$u(x) = \gcd\left(\sum_{r=1}^{l} a_r(x)a_r(x^{m-1}), h(x)\right).$$

Proof. The proof of Theorem **??** showed that a constituent of C contributes to the hull dimension if and only if the corresponding irreducible factor of x^m-1 $(g_i(x), h_j(x), h_j^*(x))$ does not divide $g(x)$, hence divides $h(x)$, and the same irreducible factor divides $\sum_{r=1}^{l} a_r(x)a_r(x^{m-1})$. Since the contribution of any constituent is at most 1 over its field of definition, this contribution is the degree of irreducible factor dividing $u(x)$. Hence the result follows. $\square$

3.1.2 LCP 1-Generator l-QC Codes

We start with a bound on the intersection dimension of two 1-generator l-QC codes.

Proposition 3.1.6. *Let $C =< (a_1(x), \ldots, a_l(x)) >$ and $D =< (b_1(x), \ldots, b_l(x)) >$ be two 1-generator l-QC codes of length ml over $\mathbb{F}_q$. If C and D are linear ℓ-intersection pair of codes then $\ell \leq m - \gcd(e_1(x), \ldots, e_l(x), x^m - 1)$, where $e_i(x) = \mathrm{lcm}(a_i(x), b_i(x))$.*

Proof. Let $E :=< (e_1(x), \ldots, e_l(x)) >$, E is a 1-generator l-QC code and

$$\dim(E) = m - \deg(\gcd(e_1(x), \ldots, e_l(x), x^m - 1)).$$

Claim: $C \cap D \subseteq E$.

Take $d(x) = (d_1(x), \ldots, d_l(x)) \in C \cap D$. Then each coordinate of $d(x)$ is divisible by the corresponding coordinate of $a(x)$ and $b(x)$. Hence, $e_i(x) \mid d_i(x)$ for all $1 \leq i \leq l$, and we have $d(x) \in E$. Hence

$$\dim(C \cap D) \leq \dim E = m - \deg g_E(x)$$

□

Next, we observe that LCP of 1-generator QC codes are rather constrained.

Proposition 3.1.7. *i: If (C, D) is LCP of 1-generator l-QC codes, then $l = 2$ and both C and D are maximal.*

ii: For $C =< (a_1(x), a_2(x)) >$ and $D =< (b_1(x), b_2(x)) >$, if $x^m - 1 \mid \operatorname{lcm}(a_i(x), b_i(x))$ for $i = 1, 2$, then (C, D) is LCP.

Proof. i: By definition we have

$$\dim(C) + \dim(D) = ml$$

for an LCP of codes. For a 1-generator QC code, the maximal dimension is m. Therefor, $2m \geq ml$. On the other hand, l is at least 2. Hence we obtain $l = 2$. Since $\dim(C) = \dim(D)$ is required for an LCP, we also see that both C and D are maximal.

ii: Since $x^m - 1 \mid \operatorname{lcm}(a_i(x), b_i(x))$, we have $E = \{0\}$, where E is defined as in the proof of Proposition **??**. Since $C \cap D \subseteq E$, we reach the conclusion.

□

A characterization of LCP of l-QC codes is given in [**?**] as follows:

Theorem 3.1.8. *(Theorem 3.1, [**?**]) Let C and D be l-QC codes of length ml over $\mathbb{F}_q$. Suppose that the CRT decomposition of C and D are as in (**??**).Then (C, D) is LCP if and only if (C_i, D_i) is LCP in $\mathbb{G}_i^l$ (for all $1 \leq i \leq s$), (C'_j, D'_j) is LCP in $\mathbb{H}'^l_j$ (for all $1 \leq j \leq t$) and (C''_j, D''_j) is LCP in $\mathbb{H}''^l_j$ (for all $1 \leq j \leq t$).*

We now characterize LCP of maximal 1-generator 2-QC codes.

Theorem 3.1.9. *Let $C =< (a_1(x), a_2(x)) >$ and $D =< (b_1(x), b_2(x)) >$ be two maximal 1-generator 2-QC codes. Then (C, D) is LCP of codes if and only if*

$$\gcd(a_1(x)b_2(x) - a_2(x)b_1(x), x^m - 1) = 1.$$

Proof. Let C and D have the following CRT decompositions:

$$C = (\bigoplus_{i=1}^{s} C_i) \bigoplus (\bigoplus_{j=1}^{t} (C'_j \bigoplus C''_j)),$$

$$D = (\bigoplus_{i=1}^{s} D_i) \bigoplus (\bigoplus_{j=1}^{t} (D'_j \bigoplus D''_j)).$$

Generator matrices of the constituents are as follows:

$$G_{C_i} = [a_1(\xi^{u_i}) \quad a_2(\xi^{u_i})] \qquad , \qquad G_{C'_j} = [a_1(\xi^{v_j}) \quad a_2(\xi^{v_j})]$$

$$G_{C''_j} = [a_1(\xi^{-v_j}) \quad a_2(\xi^{-v_j})]$$

$$G_{D_i} = [a_1(\xi^{u_i}) \quad a_2(\xi^{u_i})] \qquad , \qquad G_{D'_j} = [a_1(\xi^{v_j}) \quad a_2(\xi^{v_j})]$$

$$G_{D''_j} = [a_1(\xi^{-v_j}) \quad a_2(\xi^{-v_j})]$$

Moreover, parity check matrices for the constituents of D are easy to write as follows:

$$\bar{H}_{D_i} = [-b_2(\xi^{u_i}) \quad b_1(\xi^{u_i})] \qquad , \qquad H_{D'_j} = [-b_2(\xi^{-v_j}) \quad b_1(\xi^{-v_j})]$$

$$H_{D''_j} = [-b_2(\xi^{v_j}) \quad b_1(\xi^{v_j})]$$

By Proposition **??**, we have

$$\dim(C_i \cap D_i) = 0 \iff \operatorname{rank}(G_{C_i}\bar{H}^T_{D_i}) = 1 \iff a_1(\xi^{u_i})b_2(\xi^{u_i}) - a_2(\xi^{u_i})b_1(\xi^{u_i})) \neq 0$$

$$\dim(C'_j \cap D'_j) = 0 \iff \operatorname{rank}(G_{C'_j}\bar{H}^T_{D'_j}) = 1 \iff a_1(\xi^{v_j})b_2(\xi^{v_j}) - a_2(\xi^{v_j})b_1(\xi^{v_j})) \neq 0$$

$$\dim(C''_j \cap D''_j) = 0 \iff \operatorname{rank}(G_{C''_j}\bar{H}^T_{D''_j}) = 1 \iff a_1(-\xi^{v_j})b_2(-\xi^{v_j}) - a_2(-\xi^{v_j})b_1(-\xi^{v_j})) \neq 0$$

Combining these observations, we obtain that (C, D) is LCP if and only if no irreducible factor of $x^m - 1$ divide the polynomial $a_1(x)b_2(x) - a_2(x)b_1(x)$. $\square$

3.2 Double Circulant Codes

A 1-generator 2-QC code of the form $C =< (1, a(x)) >\subseteq R_m^2$ is called a double circulant (DC) code. Note that $[Id_m \mid A]$ is a generator matrix of C, where A is the $m \times m$ circulant matrix associated to the polynomial $a(x) = a_0 + a_1(x) + \ldots + a_{m-1}x^{m-1}$:

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_{m-1} & a_0 & \cdots & a_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

A DC code is clearly a maximal 2-QC code. By Corollary **??**, we have the following:

Proposition 3.2.1. *Let* $C =< (1, a(x)) >$. *Then*

i: $h(C) = \deg \gcd(1 + a(x)a(x^{m-1}), x^m - 1)$.

ii: If $D =< (1, b(x)) >$, *then* (C, D) *is LCP if and only if* $\gcd(b(x) - a(x), x^m - 1) = 1$.

Let us note that $h = 0$ (LCD) case of (i) was obtained in ([**?**], Theorem 5.1). Part (ii) was given in ([**?**], Proposition 3.2).

Since small hulls are of interest, as described in the Introduction, we focus on DC codes with hull dimension 1.

Proposition 3.2.2. *There exists a DC code with 1-dimensional hull over* $\mathbb{F}_q$ *if and only if* $q \equiv 1$ *(mod 4) or* q *is even.*

Proof. By the CRT decomposition, a 1-dimensional hull is possible only in the case that $\mathbb{F}_q$ contains a square root of -1, which is possible if q is even or $q \equiv 1 \pmod 4$. For the converse, let us construct $a(x)$ so that the resulting DC code has 1-dimensional hull. In the case $q \equiv 1 \pmod 4$, let $\alpha \in \mathbb{F}_q^\times$ such that $\alpha^2 = -1$. Let $a(x) = x - (\alpha + 1)$. Then

$$1 + a(x)a(x^{m-1}) = (\alpha + (2 - x - x^{m-1}))$$

An m^{th} root of unity ζ is a root of this polynomial if and only if

$$\zeta^{-1} + \zeta - 2 = 0 \iff \zeta^2 - 2\zeta + 1 = (\zeta - 1)^2 = 0 \iff \zeta = 1.$$

Hence

$$\deg\left(\gcd\left(1 + a(x)a(x^{m-1}), x^m - 1\right)\right) = 1.$$

For q even, let $h(x) = \frac{x^m-1}{x-1}$ and set $\beta = h(1) \neq 0$. If we set $a(x) = h(x) + \beta + 1$ and $v(x) = 1 + a(x)a(x^{m-1})$, we have

$$v(1) = 1 + (h(1) + \beta + 1)(h(1) + \beta + 1) = 1 + (2\beta + 1) = 1 + 1 = 0.$$

On the other hand, if $\zeta \neq 1$ is another m^{th} root of unity, we have

$$v(\zeta) = 1 + (h(\zeta) + \beta + 1)(h(\zeta^{-1}) + \beta + 1).$$

Since $h(\zeta) = h(\zeta^{-1}) = 0$, we obtain

$$v(\zeta) = 1 + (\beta + 1)^2 = 1 + \beta^2 + 1 = \beta^2.$$

Since $\beta \neq 0$, $v(\zeta) \neq 0$. We have

$$\deg\left(\deg\left(1 + a(x)a(x^{m-1}), x^m - 1\right)\right) = 1.$$

Take $a(x) = h(x) + \beta + 1$.

$$1 + a(x)a(x^{-1}) = 1 + (h(x) + \beta + 1)(h(x^{-1}) + \beta + 1)$$

$$1 + a(1)a(1^{-1}) = 1 + (\beta + \beta + 1)(\beta + \beta + 1) = 0$$

So, $x - 1 \mid u(x)$.
Let δ be another m-th root of unity.

$$1 + a(\delta)a(\delta^{-1}) = 1 + (h(\delta) + \beta + 1)(h(\delta^{-1}) + \beta + 1)$$

$$1 + (\beta + 1)(\beta + 1) = 1 + \beta^2 + 1 = \beta^2$$

Since β is nonzero, $u(x)$ and $h(x)$ are relatively prime.

$\square$

Tables 3.3, 3.4 present the best possible distance for binary and quinary DC codes with 1-dimensional hull. Here d^* is the optimal minimum distance or the best known minimum distance for binary or quinary linear codes of length $2m$ and dimension m, according to codes tables [?], d is the best possible minimum distance which can be attained by 1-dimensional hull DC code $C =< 1, a(x) >$.

m	d	d^*	a(x)
3	2	3	x^2+x+1
5	4	4	x^4+x^2+1
7	4	4	x^6+x^3+1
9	6	6	$x^8+x^7+x^5+x^3+x^2$
11	6	7	$x^{10}+x^8+x^5+x^2+1$
13	6	7	$x^{12}+x^4+x^3+x+1$
15	8	8	$x^{14}+\cdots+x^7+x^4+x^3+x$
17	8	8	$x^{16}+\cdots+x^{11}+x^5+x^3+x+1$

Table 3.3: Binary DC Codes with 1-dimensional hull.

m	d	d^*	a(x)
3	3	4	x^2+x+1
4	4	4	x^3+x^2+3x+3
6	6	6	$x^5+x^3+2x^2+2x+1$
7	6	6	$x^4+x^3+x^2+2x+3$
8	7	7	$x^5+2x^4+4x^3+2x^2+2x+2$
9	6	7	$x^5+x^4+x^3+2x^2+x+2$
11	8	8	$x^6+x^5+x^4+2x^3+x^2+4x+2$
12	8	8	$x^7+x^6+4x^5+2x^4+4x^3+4x^2+3x+4$

Table 3.4: Quinary DC Codes with 1-dimensional hull.

We provide ternary LCP of DC codes with good security parameter in Table 3.5. Here, d represents the security parameter of the pair and d^* is the best minimum distance for $[2m, m]_3$ linear codes according to [**?**].

The following statement also holds and can be proved as in Proposition **??**.

Corollary 3.2.3. *A DC code with odd-dim hull over $\mathbb{F}_q$ exists if and only if $q \equiv 1 \pmod 4$ or q is even.*

An example of a ternary DC code of length 8 with possible hull dimensions and the best minimum distance is given in the following example.

m	d	d^*	a(x)	$b(x) = -a(x^{m-1})$
4	4	4	$x^3 + 2x + 1$	$x^3 + 2x + 2$
5	4	5	$x^4 + x + 2$	$x^4 + 2x + 1$
7	5	6	$x^6 + x^3 + x + 1$	$2x^6 + 2x^4 + 2x + 2$
8	6	6	$x^7 + x^3 + x^2 + 2x + 2$	$x^7 + 2x^6 + 2x^5 + 2x + 1$
10	7	7	$x^9 + x^5 + x^4 + x^2 + x + 2$	$2x^9 + 2x^8 + 2x^6 + 2x^5 + 2x + 1$
11	7	8	$2x^{10} + 2x^9 + 2x^8 + x^5 + x^2 + 2$	$2x^9 + 2x^6 + x^3 + x^2 + x + 1$

Table 3.5: Ternary LCP DC Codes.

Example 3.2.1. *Let $q = 3$, $m = 8$. Then*

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

*Note that (x^2+1) is self-reciprocal and $(x^2+x+2), (x^2+2x+2)$ are reciprocal to each other. By Corollary **??**, possible hull dimensions for the $[16,8]_3$ DC code are 2,4,6.The following choices of $a(x)$ give a DC code with the highest possible minimum distance for such codes.*

- *$a(x) = 2x^6 + x^4 + x^2 + 2x + 1$, gives a $[16,8,6]_3$ DC code with 2-dimensional hull.*
- *$a(x) = x^4 + x^3 + x + 1$, gives a $[16,8,6]_3$ DC code with 4-dimensional hull.*
- *$a(x) = x^4 + x^3 + 2x + 1$, gives a $[16,8,6]_3$ DC code with 6-dimensional hull.*

3.3 Four Circulant Codes

We now investigate a class of 2-generator 4-QC codes. The code

$$C = < (1, 0, a_1(x), a_2(x)), (0, 1, -a_2(x^{m-1}), a_1(x^{m-1})) > \in R_m^4$$

is called a four circulant (FC) code. Via the identification between $\mathbb{F}_q^{4m}$ and R_m^4 (**??**), it is easy to see that the following is a generator matrix for C, when it is viewed as a subspace of $\mathbb{F}_q^{4m}$:

$$G = \begin{pmatrix} Id_m & 0 & A_1 & A_2 \\ 0 & Id_m & -A_2^T & A_1^T \end{pmatrix}$$

Here, A_i represents the circulant matrix corresponding to the polynomial $a_i(x)$ (for $i = 1, 2$).

It is also easy to see that the following matrices are generators for the 2-dimensional constituents of C:

$$G_i = \begin{pmatrix} 1 & 0 & a_1(\xi^{u_i}) & a_2(\xi^{u_i}) \\ 0 & 1 & -a_2(\xi^{-u_i}) & a_1(\xi^{-u_i}) \end{pmatrix} \qquad \textit{for } 1 \leq i \leq s$$

$$G'_j = \begin{pmatrix} 1 & 0 & a_1(\xi^{v_j}) & a_2(\xi^{v_j}) \\ 0 & 1 & -a_2(\xi^{-v_j}) & a_1(\xi^{-v_j}) \end{pmatrix} \qquad \textit{for } 1 \leq j \leq t$$

$$G''_j = \begin{pmatrix} 1 & 0 & a_1(\xi^{-v_j}) & a_2(\xi^{-v_j}) \\ 0 & 1 & -a_2(\xi^{v_j}) & a_1(\xi^{v_j}) \end{pmatrix} \qquad \textit{for } 1 \leq j \leq t$$

The next result characterizes LCD FC codes.

Theorem 3.3.1. *Let $C =< (1, 0, a_1(x), a_2(x)), (0, 1, -a_2(x^{m-1}), a_1(x^{m-1}) >$ be an FC code over $\mathbb{F}_q$. Then C is LCD if and only if*

$$\gcd(1 + a_1(x)a_1(x^{m-1}) + a_2(x)a_2(x^{m-1}), x^m - 1) = 1.$$

Proof. For the constituents C_i corresponding to self-reciprocal factors of $x^m - 1$, we have

$$G_i\bar{G}_i^T = \begin{pmatrix} 1 & 0 & a_1(\xi^{u_i}) & a_2(\xi^{u_i}) \\ 0 & 1 & -a_2(\xi^{-u_i}) & a_1(\xi^{-u_i}) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a_1(\xi^{-u_i}) & -a_2(\xi^{u_i}) \\ a_2(\xi^{-u_i}) & a_1(\xi^{u_i}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 + a_1(\xi^{u_i})a_1(\xi^{-u_i}) + a_2(\xi^{u_i})a_2(\xi^{-u_i}) & 0 \\ 0 & 1 + a_1(\xi^{u_i})a_1(\xi^{-u_i}) + a_2(\xi^{u_i})a_2(\xi^{-u_i}) \end{pmatrix}.$$

This matrix has nonzero (in fact, 2) rank if and only if

$$1 + a_1(\xi^{u_i})a_1(\xi^{-u_i}) + a_2(\xi^{u_i})a_2(\xi^{-u_i}) \neq 0.$$

This is equivalent to saying that $g_i(x)$ does not divide the polynomial

$$1 + a_1(x)a_1(x^{m-1}) + a_2(x)a_2(x^{m-1}).$$

Since $h_h(C_i) = 2 - \operatorname{rank}(G_i\bar{G}_i^T)$, this is the condition for constituents C_i to be LCD. For the constituents C'_j, C''_j of C, we have

$$h(C'_j, C''_j) = \dim(C'_j \cap C''^{\perp}_j) = 2 - \operatorname{rank}(G'_jG''^T_j).$$

We have

$$G'_j G''^T_j = \begin{pmatrix} 1 & 0 & a_1(\xi^{v_j}) & a_2(\xi^{v_j}) \\ 0 & 1 & -a_2(\xi^{-v_j}) & a_1(\xi^{-v_j}) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a_1(\xi^{-v_j}) & -a_2(\xi^{v_j}) \\ a_2(\xi^{-v_j}) & a_1(\xi^{v_j}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 + a_1(\xi^{v_j})a_1(\xi^{-v_j}) + a_2(\xi^{v_j})a_2(\xi^{-v_j}) & 0 \\ 0 & 1 + a_1(\xi^{v_j})a_1(\xi^{-v_j}) + a_2(\xi^{v_j})a_2(\xi^{-v_j}) \end{pmatrix}.$$

Hence $h(C'_j, C''_j) = 0$ if and only if $h_j(x)$ does not divide

$$1 + a_1(x)a_1(x^{m-1}) + a_2(x)a_2(x^{m-1}).$$

The same analysis, can be carried out for $h(C''_j, C'_j)$, which yields the result. □

The following immediately follows, using arguments in the proof of Theorem **??**.

Corollary 3.3.2. *Let* $C =< (1, 0, a_1(x), a_2(x)), (0, 1, -a_2(x^{m-1}), a_1(x^{m-1}) >$ *be a FC code over* $\mathbb{F}_q$*. Then*

i: $h(C) = 2 \deg u(x)$*, where* $u(x) = \gcd(1 + a_1(x)a_1(x^{m-1}) + a_2(x)a_2(x^{m-1}), x^m - 1)$*.*

ii: There exists no FC code with odd hull dimension.

Tables 3.6 and 3.7 present the best possible distances of binary and ternary LCD FC codes. Again, d presents the best possible minimum distance which can be attained by binary or ternary LCD FC codes, and d^* presents optimal minimum distance for binary or ternary $[4m, 2m]$ linear codes, according to code tables [**?**].

m	d	d^*	$a_1(x)$	$a_2(x)$
3	2	4	$x + 1$	$x^2 + x$
5	5	6	x^2	$x^2 + x + 1$
7	6	8	$x^6 + x^5 + x^4 + x^3$	$x + 1$
9	8	8	$x^7 + x^6 + x^5 + x^3 + x$	$x^3 + x + 1$
11	9	10	$x^5 + x^3 + x^2$	$x^7 + x^6 + x^5 + x + 1$
13	10	10	$x^7 + x^6 + x + 1$	$x^4 + x^3 + x^2 + 1$

Table 3.6: Binary LCD FC codes.

m	d	d^*	$a_1(x)$	$a_2(x)$
4	6	6	$2x^3+x^2+1$	$2x^3+1$
5	7	7	x^4+2x^2+x+2	$2x^4+2x^2+1$
7	8	9	$x^6+2x^5+x^3+x$	$2x^5+x^4+x^3+2$
8	9	10	$2x^5+x^2+1$	$x^5+x^4+x^3+2x+1$
10	11	12	$2(x^7+\ldots+x)+1$	$x^7+2x^5+2x^4+x^2+2x+1$

Table 3.7: Ternary LCD FC codes.

Our next result characterizes LCP of FC codes.

Theorem 3.3.3. *Let* $C =< (1,0,a_1(x),a_2(x)),(0,1,-a_2(x^{m-1}),a_1(x^{m-1}) >$ *and* $D =< (1,0,b_1(x),b_2(x)),(0,1,-b_2(x^{m-1}),b_1(x^{m-1}) >$ *be two FC codes of length* $4m$ *over* $\mathbb{F}_q$*.* (C,D) *is LCP if and only if*

$$\gcd\left(\sum_{r=1}^{2}[(a_r(x)-b_r(x))(a_r(x^{m-1})-b_r(x^{m-1})],x^m-1\right)=1.$$

Proof. Let C and D have the following CRT decompositions:

$$C=(\bigoplus_{i=1}^{s}C_i)\bigoplus(\bigoplus_{j=1}^{t}(C'_j\bigoplus C''_j))$$

$$D=(\bigoplus_{i=1}^{s}D_i)\bigoplus(\bigoplus_{j=1}^{t}(D'_j\bigoplus D''_j))$$

Generator matrices of the constituents are as follows:

$$G_{C_i}=\begin{pmatrix}1 & 0 & a_1(\xi^{u_i}) & a_2(\xi^{u_i})\\ 0 & 1 & -a_2(\xi^{-u_i}) & a_1(\xi^{-u_i})\end{pmatrix}\quad,\quad G_{C'_j}=\begin{pmatrix}1 & 0 & a_1(\xi^{v_j}) & a_2(\xi^{v_j})\\ 0 & 1 & -a_2(\xi^{-v_j}) & a_1(\xi^{-v_j})\end{pmatrix}$$

$$G_{C''_j}=\begin{pmatrix}1 & 0 & a_1(\xi^{-v_j}) & a_2(\xi^{-v_j})\\ 0 & 1 & -a_2(\xi^{v_j}) & a_1(\xi^{v_j})\end{pmatrix}$$

$$D_{C_i}=\begin{pmatrix}1 & 0 & b_1(\xi^{u_i}) & b_2(\xi^{u_i})\\ 0 & 1 & -b_2(\xi^{-u_i}) & b_1(\xi^{-u_i})\end{pmatrix}\quad,\quad G_{C'_j}=\begin{pmatrix}1 & 0 & b_1(\xi^{v_j}) & b_2(\xi^{v_j})\\ 0 & 1 & -b_2(\xi^{-v_j}) & b_1(\xi^{-v_j})\end{pmatrix}$$

$$G_{C''_j}=\begin{pmatrix}1 & 0 & b_1(\xi^{-v_j}) & b_2(\xi^{-v_j})\\ 0 & 1 & -b_2(\xi^{v_j}) & b_1(\xi^{v_j})\end{pmatrix}$$

Moreover, parity check matrices for the constituents of D are easy to write as follows:

$$\bar{H}_{D_i} = \begin{pmatrix} -b_1(\xi^{-u_i}) & b_2(\xi^{u_i}) & 1 & 0 \\ -b_2(\xi^{-u_i}) & -b_1(\xi^{u_i}) & 0 & 1 \end{pmatrix} \quad , \quad H_{D'_j} = \begin{pmatrix} -b_1(\xi^{v_j}) & b_2(\xi^{-v_j}) & 1 & 0 \\ -b_2(\xi^{v_j}) & -b_1(\xi^{-v_j}) & 0 & 1 \end{pmatrix}$$

$$H_{D''_j} = \begin{pmatrix} -b_1(\xi^{-v_j}) & b_2(\xi^{v_j}) & 1 & 0 \\ -b_2(\xi^{-v_j}) & -b_1(\xi^{v_j}) & 0 & 1 \end{pmatrix}$$

By Proposition **??** we have

$$\dim(C_i \cap D_i) = 0 \iff \operatorname{rank}(G_{C_i}\bar{H}_{D_i}) = 2 \iff \det(G_{C_i}\bar{H_{D_i}}^T) \neq 0$$
$$\iff \sum_{r=1}^{2}[a_r(\xi^{u_i})a_r(\xi^{-u_i}) + b_r(\xi^{u_i})b_r(\xi^{-u_i}) - a_r(\xi^{u_i})b_r(\xi^{-u_i}) - a_r(\xi^{-u_i})b_r(\xi^{u_i})] \neq 0$$

$$\dim(C'_j \cap D'_j) = 0 \iff \operatorname{rank}(G_{C'_j}H^T_{D'_j}) = 2 \iff \det(G_{C'_j}H^T_{D'_j}) \neq 0$$
$$\iff \sum_{r=1}^{2}[a_r(\xi^{v_j})a_r(\xi^{-v_j}) + b_r(\xi^{v_j})b_r(\xi^{-v_j}) - a_r(\xi^{v_j})b_r(\xi^{-v_j}) - a_r(\xi^{-v_j})b_r(\xi^{v_j})] \neq 0$$

$$\dim(C''_j \cap D''_j) = 0 \iff \operatorname{rank}(G_{C''_j}H^T_{D''_j}) = 2 \iff \det(G_{C''_j}H^T_{D''_j}) \neq 0$$
$$\iff \sum_{r=1}^{2}[a_r(\xi^{v_j})a_r(\xi^{-v_j}) + b_r(\xi^{v_j})b_r(\xi^{-v_j}) - a_r(\xi^{v_j})b_r(\xi^{-v_j}) - a_r(\xi^{-v_j})b_r(\xi^{v_j})] \neq 0$$

Combining these together, we obtain (C, D) is LCP if and only if no irreducible factor of $x^m - 1$ is a divisor of $\sum_{r=1}^{2}[(a_r(x) - b_r(x))(a_r(x^{m-1}) - b_r(x^{m-1})]$. $\square$

Table 3.8 presents ternary LCP of FC codes with good security parameter.

m	d	d^*	$a_1(x)$	$a_2(x)$
4	6	6	$2x^3 + 2x^2 + x$	$x^2 + 1$
5	7	7	$x^2 + 2x + 1$	$2x^3 + x + 1$
7	9	9	$x^3 + 2x^2 + 1$	$2x^5 + 2x^3 + 2x^2 + x + 1$
8	9	10	$x^3 + x^2 + x + 2$	$x^4 + x^2 + 2x + 1$

Table 3.8: Ternary LCP of FC codes.

3.4 Enumeration and Asymptotics

We present enumeration results on DC and FC codes with small hull dimension. We also study the asymptotic performance of DC codes with 0 or 1 dimensional hull.
For DC codes with small hull dimension (i.e. 0 or 1) over $\mathbb{F}_q$, we need to count the number of LCD (for 0 dimension) or self-dual (for 1 dimension) codes over $\mathbb{F}_q$, the number of Hermitian LCD codes over square extensions of $\mathbb{F}_q$, and the number of pair (C_1, C_2) of codes over extensions of $\mathbb{F}_q$, such that $C_1 \cap C_2^{\perp} = C_2 \cap C_1^{\perp} = \{0\}$.

Lemma 3.4.1. *The number of solutions in $\mathbb{F}_q$ of the equation*

$$1 + x^2 = 0$$

is 1 if q is even and 2 if $q \equiv 1$ (mod 4).

Proof. If q is even then

$$1 + x^2 = (1 + x)^2.$$

Clearly $x = 1$ is the only root of this equation.
If $q \equiv 1 \pmod 4$, there exits $\alpha \in \mathbb{F}_q^{\times}$ such that $\alpha^2 = -1$. Then α and $-\alpha$ are the roots of $1 + x^2$. $\square$

Lemma 3.4.2. *The number of solutions x in $\mathbb{F}_{q^2}$ of the equation*

$$1 + x^{q+1} = 0$$

is $q + 1$.

Proof. Let $f(x) = 1 + x^{q+1}$. First note that $f(x)$ has at most $q+1$ roots in the algebraic closure $\bar{\mathbb{F}}_{q^2}$. We also have $f'(x) = x^q$. Since $\gcd(f, f') = 1$ this equation has no repeated root.

We need to show that, every root of $f(x)$ is in $\mathbb{F}_{q^2}$. Let $f(\alpha) = 0$. Then we have $\alpha^{q+1} = -1$.

If q is odd, we have

$$(\alpha^{q+1})^{q-1} = 1 \implies \alpha^{q^2-1} = 1 \implies \alpha \in \mathbb{F}_{q^2}.$$

If q is even, we have

$$\alpha^{q+1} = -1 = 1 \implies (\alpha^{q+1})^{q-1} = 1 \implies \alpha^{q^2-1} = 1 \implies \alpha \in \mathbb{F}_{q^2}.$$

$\square$

Lemma 3.4.3. *(Lemma 2.10 [?]) The number of solutions of* $1+x_1y_1+\ldots,x_{t-1}y_{t-1} = 0$ *is*

$$q^{2t-3} - q^{t-2}.$$

The enumeration results are as follows:

Proposition 3.4.4. *The number of LCD DC codes of length* $2m$ *over* $\mathbb{F}_q$ *is*

- $(q-2)\prod_{i=2}^{s}(q^{2d_i} - q^{d_i} - 1)\prod_{j=1}^{t}(q^{2d'_j+} - q^{d'_j} + 1)$ *if* m *is odd and* $q \equiv 1$ *(mod 4)*
- $(q-2)^2\prod_{i=3}^{s}(q^{2d_i} - q^{d_i} - 2)\prod_{j=1}^{t}(q^{2d'_j} - q^{d'_j} + 1)$, *if* m *is even and* $q \equiv 1$ *(mod 4)*
- $(q-1)\prod_{i=2}^{s}(q^{2d_i} - q^{d_i} - 1)\prod_{j=1}^{t}(q^{2d'_j} - 2q^{d'_j} + 1)$ *if* m *is odd and* q *is even.*
- $q\prod_{i=2}^{s}(q^{2d_i} - q^{d_i} - 1)\prod_{j=1}^{t}(q^{2d'_j} - 2q^{d'_j} + 1)$ *if* m *is odd and* $q \equiv 3$ *(mod 4)*
- $q^2\prod_{i=3}^{s}(q^{2d_i} - q^{2d_i} - 1)\prod_{j=1}^{t}(q^{2d'_j} - q^{d'_j} + 1)$ *if* m *is even and* $q \equiv 3$ *(mod 4)*

Proof. We use the CRT decomposition of R_m. To count LCD DC codes over $\mathbb{F}_q$, we are reduced to counting the number of $[2,1]$ codes over some extension fields $\mathbb{F}_Q$ of $\mathbb{F}_q$. If m is odd, then $x-1$ is the only self-reciprocal linear factor. By Lemma **??**, the number of self-dual $[2,1]_q$ linear codes is equal to 1 and 2, when q is even and $q \equiv 1$ (mod 4), respectively. We obtain $(q-1)$ and $(q-2)$, $[2,1]$ LCD linear codes of the form $[1\ a]$, for q is even and $q \equiv 1$ (mod 4), respectively.

If m is even, then we have $x+1$ as another linear factor also we have $q \equiv 1 \pmod 4$. In this case, we obtain $(q-2)^2$, $[2,1]$ LCD linear codes of the form $[1\ a]$.
Over extension fields corresponding to the self-reciprocal factor $g_i(x)$, we have $Q = q^{2d_i}$, where $2d_i = \deg g_i(x)$. The number of $[2,1]$ Hermitian self-dual linear codes of the form $[1\ a_i]$ over $\mathbb{F}_q$ is equivalent to counting the number of solutions of the equation

$$1 + x^{q^{d_i}},$$

which by ?? is $q^{d_i}+1$. Thus we obtain $q^{2d_i} - q^{d_i} - 1$, $[2,1]_Q$ Hermitian LCD codes over $\mathbb{F}_Q$.
A pair $h_j(x)$ and $h^*j(x)$ leads us to the extension $\mathbb{F}_Q$, with $Q = q^{d'_j}$, here $d'_j = \deg h'_j(x)$. The number of pair (C'_j, C''_j) of linear codes of the form $[1\ a'_j]$ and $[1\ a''_j]$ satisfying $C'_j = C''^{\perp}_j$ is equivalent to counting the number of solutions of the equation

$$1 + xy = 0,$$

which by ?? is $q^{d'_j} - 1$. Thus we obtain $q^{2d'_j} - q^{d'_j} + 1$ of pair (C'_j, C''_j) such that $C'_j \cap C''_j = C''_j \cap C'_j = \{0\}$.

□

Proposition 3.4.5. *Let q be a prime power, $q \equiv 1 \pmod 4$ or q is even, m an integer relatively prime to q. Then the number of DC codes of length $2m$ with 1-dimensional hull is equal to*

i: $2\prod_{j=2}^{s}(q^{2d_i} - q^{d_i} - 1)\prod_{j=1}^{t}(q^{2d'_j} - q^{d'_j} + 1)$ *if m is odd and $q \equiv 1 \pmod 4$.*

ii: $4(q-2)\prod_{j=3}^{s}(q^{2d_i} - q^{d_i} - 1)\prod_{j=1}^{t}(q^{2d'_j} - q^{d'_j} + 1)$, *if m is even and $q \equiv 1 \pmod 4$.*

iii: $\prod_{j=2}^{s}(q^{2d_i} - q^{d_i} - 1)\prod_{j=1}^{t}(q^{2d'_j} - q^{d'_j} + 1)$ *if m is odd and q is even.*

Proof. The proof is similar to the proof of Proposition ??, with the difference that in this case we have self-dual codes over field $\mathbb{G}_1$ or $\mathbb{G}_2$, depending on the parity of m. □

To count the number of LCD FC and FC codes with 2-dimensional hull, we need to count the number of LCD (for 0 dimension) or self-dual (for 2 dimension) codes over $\mathbb{F}_q$, the number of Hermitian LCD codes over square extensions of $\mathbb{F}_q$, and the number of pair (C_1, C_2) of codes over extensions of $\mathbb{F}_q$, such that $C_1 \cap C_2^{\perp} = C_2 \cap C_1^{\perp} = \{0\}$. For the enumeration we use the following results from [?]:

Lemma 3.4.6. *(Lemma 2.7, [?]) If q is odd, then the number of solutions (x, y) in $\mathbb{F}_{q^2}$ of the equation $1 + x^{1+q} + y^{1+q} = 0$ is*

$$q^3 - q.$$

Lemma 3.4.7. *(Corollary 2.9, [?]) If q is odd, then the number of solutions (x, y) in $\mathbb{F}_q$ of the equation $1 + x^2 + y^2 = 0$ is*

$$q - \eta(-1),$$

where $\eta(x)$ is the quadratic character of $\mathbb{F}_q$ defined as

$$\eta(x) = \begin{cases} 1 & x \text{ is square} \\ 0 & x = 0 \\ -1 & x \text{ is non-square} \end{cases}.$$

Note that the constituents of a FC code C are either 0 or 2-dimensional over the field they are defined.

- Let C be a linear code with generator matrix $G_C = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix}$ over $\mathbb{F}_q$. Then, $h(C) = 2$ if and only if

  $$1 + a^2 + b^2 = 0.$$

  By Lemma **??**, there are $q - \eta(-1)$ such codes. Thus there are $q^2 - q + \eta(-1)$ LCD codes with the generator matrix as G_C.

- Let C be a linear code with generator matrix $G_C = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b^q & a^q \end{pmatrix}$ over $\mathbb{F}_{q^2}$. Then, $h(C) = 2$ if and only if

  $$1 + a^{q+1} + b^{q+1} = 0.$$

  By Lemma **??**, there are $q^3 - q$ such codes. Thus there are $q^4 - q^3 + q$ LCD codes with generator matrix as G_C.

- Let C and D be two linear codes with generator matrices

  $$G_C = \begin{pmatrix} 1 & 0 & a_1 & a_2 \\ 0 & 1 & -b_2 & b_1 \end{pmatrix} \qquad G_D = \begin{pmatrix} 1 & 0 & b_1 & b_2 \\ 0 & 1 & -a_2 & a_1 \end{pmatrix}.$$

Then, $h(C,D)=2$ if and only if $\mathrm{rank}(G_C G_D^T)=0$:

$$\begin{pmatrix} 1 & 0 & a_1 & a_2 \\ 0 & 1 & -b_2 & b_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ b_1 & -a_2 \\ b_2 & a_1 \end{pmatrix} = \begin{pmatrix} 1+a_1b_1+a_2b_2 & -a_1a_2+a_1a_2 \\ -b_1b_2+b_1b_2 & 1+a_1b_1+a_2b_2 \end{pmatrix}$$

This matrix has rank 0 if and only if

$$1+a_1b_1+a_2b_2=0.$$

By Lemma **??**, there are q^3-q of such pair of codes. Thus the number of (C,D) such that $C=D^{\perp}$ is q^4-q^3+q.

Theorem 4.3 in ([**?**]), gave enumeration results for LCD FC codes. While we were trying to examine our enumeration results for LCD case, it did not match their result. After carefully checking, we found their missing point and revised the enumeration result as follow.

Theorem 3.4.8. *Let q be odd, then the number of LCD FC codes of length $4m$ over $\mathbb{F}_q$ is*

i: $(q^2-q+\eta(-1))\prod_{i=2}^{s}(q^{4d_i}-q^{3d_i}+q^{d_i})\prod_{j=1}^{t}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})$*,if m is odd.*

i: $(q^2-q+\eta(-1))^2\prod_{i=3}^{s}(q^{4d_i}-q^{3d_i}+q^{d_i})\prod_{j=1}^{t}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})$*,if m is even.*

Proof. Again by using the CRT decomposition of R_m, we need to count the number of codes with the 0 dimensional hull over the field they are defined.
For the constituents from $x-1$ or $x+1$, this number is $(q^2-q+\eta(-1))$.
Self-reciprocal factor $g_i(x)$, leads us to count the number of $[4,2]$ Hermitian LCD codes over $\mathbb{F}_{q^{2d_i}}$, which is equal to $(q^{4d_i}-q^{3d_i}+q^{d_i})$. A pair $h_j(x)$ and $h_j^*(x)$, leads us to the pair (C'_j, C''_j) over $\mathbb{F}_{q^{d'_j}}$ such that $h(C'_j, C''_j)=h(C''_j, C'_j)=0$, which is equal to $q^{4d'_j}-q^{3d'_j}+q^{d'_j}$. □

By Corollary **??**, 2-dimensional hull FC codes corresponds to the polynomial $a_1(x), a_2(x)$ such that

$$\gcd(1+a(x)a(x^{m-1})+b(x)b(x^{m-1}), x^m-1)=x-1,$$

or

$$\gcd(1+a(x)a(x^m-1)+b(x)b(x^{m-1}), x^m-1)=x+1,$$

depending on the parity of m.

Theorem 3.4.9. *The number of FC codes of length $4m$ and hull dimension 2 over $\mathbb{F}_q$ is*

i: $(q-\eta(-1))\prod_{i=2}^{s}(q^{4d_i}-q^{3d_i}+q^{d_i})\prod_{j=1}^{t}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})$*, if m is odd.*

i: $2(q-\eta(-1))(q^2-q+\eta(-1))\prod_{i=3}^{s}(q^{4d_i}-q^{3d_i}+q^{d_i})\prod_{j=1}^{t}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})$*, if m is even.*

Tables 3.9 and 3.10 present binary and ternary FC codes with 2-dimensional hull.

m	d	d^*	$a_1(x)$	$a_2(x)$
3	4	4	x^2+x	x^2
5	4	6	x^3+1	x^4+x^2+1
7	8	8	$x^6+x^5+x^4+x+1$	x^6+x^3
9	8	8	$x^8+\ldots+x^4$	x^8+x
11	8	10	x^3+x^2+1	x^6+x^2+x+1
13	11	8	$x^7+\ldots+x^2$	$x^12+x^7+x^3$

Table 3.9: Binary FC codes with 2-dimensional hull

m	d	d^*	$a_1(x)$	$a_2(x)$
4	6	6	$2x^4+x^2+2$	$2x+2$
5	7	7	$2x^4+2x^3+1$	x^4+x^2+2
7	8	9	$x^5+2x^3+2x^2+2$	$2x^6+x+2$
8	9	10	$x^6+2x^4+x^3+2x+1$	x^7+x^2+1
10	11	12	$x^6+x^4+x^3+x^2+2x+2$	$x^6+x^5+x^4+x^2+x+1$

Table 3.10: Ternary FC codes with 2-dimensional hull

We now turn our attention to the asymptotic performance of DC codes with small hull dimension. If $C(i)$ is a family of linear codes with parameters $[n_i, k_i, d_i]_q$, the rate and relative distance of this family is defined as

$$R = \lim_{i\to\infty} \sup \frac{k_i}{n_i},$$

and

$$\delta = \lim_{i\to\infty} \sup \frac{d_i}{i}.$$

$C(i)$ is called asymptotically good if $R\delta > 0$.

An integer g is called a primitive root modulo m if g generates the group of units $\mathbb{Z}_m^\times$ of the ring $\mathbb{Z}_m$. Artin's conjecture on primitive roots, which was proved in [**?**] under Generalized Riemann Hypothesis, states that any positive integer, which is not square, is a primitive root modulo infinitely many primes m. This implies that for a non-square q, there exists infinitely many primes m such that $x^m - 1$ factors into irreducible polynomials over $\mathbb{F}_q$ as

$$x^m - 1 = (x-1)u(x).$$

Lemma 3.4.10. *(Lemma 6, [**?**]) With above assumption, let* $0 \neq u(x) \in R_m^2$. *If* u *has Hamming weight less than* m*, then there are at most* q *polynomials such that* $u \in C_a =< (1, a(x)) >$.

The q-ary entropy function is defined for $0 < t < 1 - \frac{1}{q}$ by

$$H_q(t) = t\log_q(q-1) - t\log_q(t) - (1-t)log_q(1-t).$$

The volume of the Hamming ball of radius tn (or the number of vectors of weight $\leq tn$) is approximately $q^{nH_q(t)}$ ([**?**], Lemma 2.10.3).

Theorem 3.4.11. *i) Let* q *be a non-square,* m *an odd prime such that* $\gcd(q, m) = 1$. *Then there exit infinite families of LCD DC codes of length* $2m$ *and relative distance satisfying*

$$\delta \geq H_q^{-1}(\frac{1}{2}).$$

In particular such families are asymptotically good.

ii) Let q be a non-square which is either even or $q \equiv 1$ (mod 4), m an odd prime such that $\gcd(q, m) = 1$*. Then there exist infinite families of 1-dim hull DC codes of length $2m$ and relative distance satisfying*

$$\delta \geq H_q^{-1}(\frac{1}{2}).$$

In particular such families are asymptotically good.

Proof. With our assumption, let

$$x^m - 1 = (x - 1)u(x).$$

i) Let Γ_m denotes the number of LCD DC codes of length $2m$. Then by Proposition (**??**), $\Gamma_m \sim q^m$.

Denote the number of double circulant codes of length $2m$ containing a vector of weight $d \sim 2m\delta$ or less by γ_m. By Lemma **??** and (Lemma 2.10.3, [**?**]),

$$\gamma_m \sim q.q^{2mH_q(\delta)} \sim q^{2mH_q(\delta)}$$

If $\Gamma_m > \gamma_m$, then there exist LCD DC codes of length $2m$ and minimum distance at least $d \sim 2m\delta$. Let δ' be the largest possible number such that $\Gamma_m > \gamma_m$. Then for any $\delta \geq \delta'$ we have $\Gamma_m \sim \gamma_m$ as $m \to \infty$ or equivalently

$$2mH_q(\delta) \geq m \implies \delta \geq H_q^{-1}(\frac{1}{2})$$

Note that for such a family we have $R = \frac{1}{2}$, thus $R\delta > 0$.

ii) The proof is analogous to the proof of part (i), utilizing Proposition (**??**) this time.

□

Bibliography

[1] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib, P. Solé, *On complementary dual multinegacirculant codes*, Cryptogr. Commun., vol. 12, 101-113 (2020).

[2] A. Alahmadi, F. Özdemir, P. Solé, *On self-dual double circulant codes*, Des. Codes Cryptogr., vol. 86, 1257-1265 (2018).

[3] E.F. Assmus Jr., J.D. Key, *Affine and projective planes*, Discrete Math., vol. 83(2–3), 161-187 (1990).

[4] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada, C. Koukouvinos, *On self-dual codes over some prime fields*, Discrete Math., vol. 262, 37-58 (2003).

[5] S. Bhasin, J.L. Danger, S. Guilley, Z. Najm, X.T. Ngo, *Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses*, IEEE International Symposium on Hardware Oriented Security and Trust, 82-87 (2015).

[6] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, H. Maghrebi, *Orthogonal direct sum masking: a smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks*, WISTP, Lecture Notes in Computer Science, vol. 8501, Springer, Berlin, Heidelberg, 40-56, (2014).

[7] M. Borello, J. de Cruz, W. Willems, *A note on linear complementary pairs of group codes*, Discret. Math., vol. 343(8), 111905 (2020).

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

[9] C. Carlet, C. Li, S. Mesnager, *Linear codes with small hulls in semi-primitive case*, Des. Codes Cryptogr., vol. 87(12), 3063-3075 (2019).

[10] C. Carlet, S. Guilley, *Complementary dual codes for counter-measures to side-channel attacks*, Adv. Math. Commun., vol. 10(1), 131-150 (2014).

[11] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, P. Solé, *On linear complementary pairs of codes*, IEEE Trans. Inform. Theory, vol. 64, 6583-6589 (2018).

[12] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, *Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$*, IEEE Trans. Inform. Theory, vol. 64, no. 4, 3010-3017 (2018).

[13] M. Esmaeili, S. Yari, *On complementary-dual quasi-cyclic codes*, Finite Fields Appl., vol. 15, 375-386 (2009).

[14] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at http://www.codetables.de, Accessed on 2022-07-14.

[15] K. Guenda, T.A. Gulliver, S. Jitman, S. Thipworawimon, *Linear ℓ-intersection pairs of codes and their applications*, Des. Codes Cryptogr., vol. 88, 133-152 (2020).

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

[17] C. Güneri, B. Özkaya, S. Sayıcı, *On linear complementary pair of nD cyclic codes*, IEEE Commun. Lett., vol. 22, 2404-2406 (2018).

[18] C. Güneri, B. Özkaya, P. Solé, *Quasi-cyclic complementary dual codes*, Finite Fields Appl., vol. 42, 67-80 (2016).

[19] W.C. Huffman, V. Pless,*Fundamentals of Error Correcting Codes*, Cambridge University Press, Cambridge (2003).

[20] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. vol. 225, 209–220 (1967).

[21] J.S. Leon, *Computing automorphism groups of error-correcting codes*, IEEE Trans. Inform. Theory, vol. 28(3), 496-511 (1982).

[22] C. Li, P. Zeng, *Constructions of linear codes with one-dimensional hull*, IEEE Trans. Inform. Theory, vol. 65, no. 3, 1668-1676 (2019).

[23] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press (1986).

[24] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes I: finite fields*, IEEE Trans. Inform. Theory, vol.47, no. 7, 2751-2760 (2001).

[25] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes III: generator theory*, IEEE Trans. Inform. Theory, vol. 51, 2692-2700 (2005).

[26] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam (1977).

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

[28] P. Moree, *Artin's primitive root conjecture, a survey*, Integers 10(6), 1305-1416 (2012).

[29] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, *Hulls of cyclic and negacyclic codes over finite fields*, Finite Fields Appl. vol. 33, 232-257 (2015).

[30] G.E. Seguin, *A class of 1-generator quasi-cyclic codes*, IEEE Trans. Inform. Theory, vol. 50, 1745-1753 (2004).

[31] N. Sendrier, *On the dimension of the hull*, SIAM J. Discrete Math., vol. 10(2), 282-293 (1997).

[32] N. Sendrier, *Finding the permutation between equivalent codes: the support splitting algorithm*, IEEE Trans. Inform. Theory, vol. 46(4), 1193-1203 (2000).

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

[34] N. Sendrier, G. Skersys, *On the computation of the automorphism group of a linear code*, Proc. IEEE Int. Symp. Inf. Theory, p. 13 (2001).

[35] L. Sok, *On linear codes with one-dimensional Euclidean hull and their applications to EAQECCs*, IEEE Trans. Inform. Theory, vol. 68, no. 7, 4329-4343 (2022).

[36] X. Yang, J.L. Massey, *The condition for a cyclic code to have a complementary dual*, Discrete Math., vol. 126, 391-393 (1994).

[37] H. Zhu, M. Shi, *On linear complementary dual four circulant codes*, Bull. Aust. Math. Soc., vol. 98(1), 159-166 (2018).