Double Circulant Additive Complementary Dual Codes over $\mathbb{F}_4$

Hatoon Shoaib*

Keywords: Additive code, Double circulant code, Complementary dual code.

1 Introduction

Linear codes with complementary-duals (LCD) are linear codes that intersect with their dual trivially [2]. Weakening the linearity condition, an additive code over $\mathbb{F}_4$ is additive complementary dual (ACD) if it intersects its dual trivially. The cyclic subclass was investigated recently [3]. In this paper, we study double circulant (DC) codes over $\mathbb{F}_4$ that are ACD. All methodologies and issues employed in the study of DC codes may be applicable to ACD codes: CRT decomposition, explicit enumeration, asymptotics [1]. In particluar, we show that the class of codes considered here is asymptotically good.

2 Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of order 2 and $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$ represent the finite field of order 4, where $\overline{\omega} = \omega^2 = \omega + 1, \omega^3 = 1$.

Definition 2.1 *An **additive codes** $\mathcal{C}$ over $\mathbb{F}_4$ is $\mathbb{F}_4$-code that is closed by its codewords under addition.*

An additive code $\mathcal{C}$ over $\mathbb{F}_4$ of length n is an additive subgroup of $\mathbb{F}_4^n$.

Definition 2.2 *An $n \times n$-matrix is called a **circulant matrix** if each row is obtained from the previous one by a cyclic shift over one position to the right.*

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ . & . & & . & . \\ . & . & & . & . \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{bmatrix}$$

*Math. Dept., King Abdulaziz University, Jeddah, Saudi Arabia, Email: hashoaib@kau.edu.sa

Definition 2.3 *A linear block code $\mathcal{C}$ of length $n = ml$ over a finite field $\mathbb{F}_q$ is called a **quasi-cyclic** (QC) code of index l if for every codeword $c \in \mathcal{C}$ there exists a number l such that the codeword obtained by l cyclic shift is also a codeword in $\mathcal{C}$. That is,*

$$c = (c_0, c_1, ..., c_{n-1}) \in \mathcal{C} \Rightarrow c' = (c_{n-l}, ..., c_0, ..., c_{n-l-1}) \in \mathcal{C}.$$

Where l is defined as the smallest number of cyclic shifts where the code is invariant.

Remark 2.4 *Quasi-cyclic codes are a generalization of cyclic codes; that is, cyclic codes are quasi-cyclic codes with $l = 1$.*

Definition 2.5 *A **double-circulant** (DC) code $\mathcal{C}$ is a quasi-cyclic code of even length with $l = 2$.*

Definition 2.6 *A **Complementary Dual Codes** are non-linear codes that intersect with their dual trivially.*

$\mathcal{C}$ has a size of 4^n since it is a free $\mathbb{F}_2$-module. We refer to $\mathcal{C}$ as a $(2n, 4^n)$ code. The basis for additive complementary dual codes over $\mathbb{F}_4$ is an $\mathbb{F}_2$-module with $2n$ basis vectors. The similarity between additive codes and quantum codes as discussed in [2] has generated interest in these codes over $\mathbb{F}_4$.
The additive codes that result from the trace map have a natural inner product.
The trace map $Tr : \mathbb{F}_4 \to \mathbb{F}_2$ is defined by

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

In particular $Tr(0) = Tr(1) = 0$ and $Tr(\omega) = Tr(\overline{\omega}) = 1$.

Definition 2.7 *A **generator matrix** of a $(2n, 4^n)$ additive double circulant code $\mathcal{C}$ over $\mathbb{F}_4$ is a $2n \times 2n$ circulant matrix G with entries in $\mathbb{F}_4$ such that $\mathcal{C} = \{xG : x \in \mathbb{F}_2^{2n}\}$.*

Definition 2.8 *An additive code over $\mathbb{F}_4$ is **additive complementary dual** (ACD) if it intersect with their dual trivially. $\mathcal{C} \bigcap \mathcal{C}^{\perp} = \phi$*

Let $\mathbf{x} = (x_1, x_2, ..., x_n)$ and $\mathbf{y} = ((y_1, y_2, ..., y_n)$ are in $\mathbb{F}_4^n$, we have the Hermitian inner product is defined as:

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i \overline{y_i},$$

the trace Hermitian inner product is defined as:

$$\mathbf{x} \star \mathbf{y} = \sum_{i=1}^{n} Tr(x_i \overline{y_i}),$$

and the trace Euclidean inner is defined as:

$$\mathbf{x} \diamond \mathbf{y} = \sum_{i=1}^{n} Tr(x_i y_i).$$

If $\mathcal{C}$ is an $(2n, 4^n)$ additive double circulant code, the dual of $\mathcal{C}$ with respect to Hermitian inner product is $\mathcal{C}^{\perp_H} = \{x \in \mathbb{F}_4^{2n} \mid x.y = 0 \text{ for all } y \in \mathcal{C}\}$, the trace Hermitian inner product is $\mathcal{C}^{\perp_{TrH}} = \{x \in \mathbb{F}_4^{2n} \mid x \star y = 0 \text{ for all } y \in \mathcal{C}\}$, and the trace Euclidean inner product is $\mathcal{C}^{\perp_{TrE}} = \{x \in \mathbb{F}_4^{2n} \mid x \diamond y = 0 \text{ for all } y \in \mathcal{C}\}$.
Hence, $\mathcal{C}^{\perp_H}, \mathcal{C}^{\perp_{TrH}}$ and $\mathcal{C}^{\perp_{TrE}}$ are $(2n, 8^n)$ additive codes.
It is well known that the algebra of $n \times n$ circulant matrices over the field $\mathbb{F}_q$ is isomorphic to the algebra of polynomials in the ring $\mathbb{F}_q[x]/(x^n - 1)$.

As we know that if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, then $\mathcal{C}$ is self-orthogonal. Any linear code over $\mathbb{F}_4$ is self-orthogonal under the Hermitian inner product if and only if a self-orthogonal additive double circulant code under trace inner product.
By a code of length n over $\mathbb{F}_4$, we have code is linear if it is a $\mathbb{F}_4$-vector subspace of $\mathbb{F}_4^n$. However, a code's three parameters are concisely expressed as (N, k, d). We expand this notation to a $\mathcal{C}$ code that may be nonlinear such that $\mathcal{C} \subseteq \mathbb{F}_4^n$, where $k = \log_4(|\mathcal{C}|)$, and d is the smallest pairwise distance between two nonzero codewords. Then we have the rate is $R(\mathcal{C}) = \frac{\log_4 4^{\frac{n}{2}}}{2n} = \frac{1}{4}$, and the relative distance $\delta = \frac{d}{2n}$.

If $\mathcal{C}_m$ is a family of codes of parameters (m, k_m, d_m) the rate R and relative distance δ are defined as:

$$R = \limsup_{m \to \infty} \frac{k_m}{m}$$

$$\delta = \liminf_{m \to \infty} \frac{d_m}{m}$$

Such a family of codes is said to be **good** if $R\delta \neq 0$.

Recall that the 4-ary **entropy function** $H_4 : [0, 1] \to \mathbb{R}$ as follows:

$$H_4(y) = y \log_4 3 - y \log_4(y) - (1 - y) \log_4(1 - y).$$

3 Algebraic Structure

In this paper, we assume that $gcd(n, 4) = 1$. Every double circulant code of length $2n$ may be thought of as a code of length 2 over the ring $R = \mathbb{F}_4/(x^n - 1)$, as stated in this paper "Ling S., Solé P.: On the algebraic structure of quasi-cyclic codes I".

We consider double circulant (DC) codes over $\mathbb{F}_4$. These are $(n, 4^{\frac{n}{2}})$ codes over $\mathbb{F}_4$, where the codewords are closed under two shifts. In other words, a double circulant code is an index 2 quasi-cyclic code.

We assume that the factorization of $x^n - 1$ into irreducible polynomials over $\mathbb{F}_4$ is of the form:

$$x^n - 1 = \alpha(x-1)\prod_{i=2}^{s} g_i(x)\prod_{j=1}^{t} h_j(x)h_j^*(x)$$

Where $\alpha \in \mathbb{F}_4^*, g_i$ a self-reciprocal polynomial with degree $2d_i$, the polynomial h_j is of degree e_j and $*$ denoted reciprocation.
We next use the Chinese Remainder Theorem to break down this ring by (CRT), we have

$$R \simeq \left(\bigoplus_{i=1}^{s} \frac{\mathbb{F}_4}{< g_i(x) >}\right) \oplus \left(\bigoplus_{j=1}^{t} (\frac{\mathbb{F}_4}{< h_j(x) >} \oplus \frac{\mathbb{F}_4}{< h_j^*(x) >}\right).$$

For simplicity we let $G_i = \frac{\mathbb{F}_4}{<g_i(x)>}, H_j' = \frac{\mathbb{F}_4}{<h_j(x)>}, H_j'' = \frac{\mathbb{F}_4}{<h_j^*(x)>}$. This decomposition naturally extends to R^2 as

$$R^2 \simeq \left(\bigoplus_{i=1}^{s} G_i^2\right) \oplus \left(\bigoplus_{j=1}^{t} (H_j'^2 \oplus H_j''^2\right).$$

In particulart,

$$R^2 \simeq \left(\bigoplus_{i=1}^{s} \mathcal{C}_i\right) \oplus \left(\bigoplus_{j=1}^{t} (\mathcal{C}_j' \oplus \mathcal{C}_j''\right),$$

where $\mathcal{C}_i$ is a linear code over G_i of length 2 for each $1 \leq i \leq s$, and $\mathcal{C}_j'$ is a linear code over H_j' of length 2 and $\mathcal{C}_j''$ is a linear code over H_j'' of length 2for each $1 \leq j \leq t$. These codes are called the constituents of $\mathcal{C}$.

However, If $\mathcal{C}$ is self-orthogonal additive DC code if and only if $\mathcal{C}_i$ is self-orthogonal additive DC code relative to the trace inner product in G_i^2 for each $1 \leq i \leq s$, and $\mathcal{C}_j' \bigcap \mathcal{C}_j''^{\perp_{TrH}} \neq \{0\}$, $\mathcal{C}_j'' \bigcap \mathcal{C}_j'^{\perp_{TrH}} \neq \{0\}$.

4 Enumeration

We provide enumerative findings for self-orthogonal additive double circulant codes in this section.

Theorem 4.1 *Let n denote an odd prime. If $x^n - 1$ factors as a product of two irreducible polynomials over $\mathbb{F}_4$, then the number of self-orthogonal double circulant codes of lenght $2n$ is $2^{n-1} + 1$.*

Proof. We use the algebraic Structure from the pervious section, where $x^n - 1$ is factored into irreducible polynomials as:

$$x^n - 1 = (x-1)(x_{n-1} + ... + x + 1),$$

Then if $s = 2$ and $t = 0$, here we have: $G_1 = \mathbb{F}_4$, and $G_2 = \mathbb{F}_4^{n-1}$. Since $t = 0$ then H'_j and H''_j are undefined. By Chines Reminder Theorem (CRT), we get that any 2-quasi cyclic code of length $2n$ over $\mathbb{F}_4$ decomposes as the sum of self-orthogonal additive DC code $\mathcal{C}$ of length 2 over $\mathbb{F}_4$ and of a hermition additive DC code $\mathcal{C}$ of length 2 over $\mathbb{F}_4^{n-1}$.
To get an additive DC code in systematic form, We must make sure that the only possibility for $\mathcal{C}_1$ is the code spanned by $[1, 1]$, and for $\mathcal{C}_n$ the generator matrix is $[1, a]$, with a is $1+a^{1+r} = 0$ with $4^{n-1} = r^2$. To count the solution of the equation $1+a^{1+r} = 0$ over $\mathbb{F}_4^{n-1}$ by finite field theory, it can be seen that this equation has $1 + r$ solutions.

5 Asymptotics

In this section, we assume that n be an odd prime such that $x^n - 1$ has only two irreducible factors as

$$x^n - 1 = (x - 1)(x_{n-1} + ... + x + 1).$$

Theorem 5.1 *For every $\epsilon > 0$, is a sequence of double circulant ACD codes with relative distance*

$$\delta \geq H_4^{-1}(3/4) + \epsilon.$$

References

[1] Adel Alahmadi, Funda Ozdemir, Patrick Solé On self-dual double circulant codes. Des. Codes Cryptogr. **86**(6), (2018), 1257–1265.

[2] Steven T. Dougherty, Jon-Lark Kim, Buket Ozkaya, Lin Sok, Patrick Solé, The combinatorics of LCD codes: linear programming bound and orthogonal matrices. Int. J. Inf. Coding Theory **4**(2/3), (2017), 116–128.

[3] Minjia Shi, Na Liu, Ferruh Ozbudak, Patrick Solé Additive cyclic complementary dual codes over F4. Finite Fields Their Appl. **83** 102087 (2022)