Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(9): 21636–21643.
DOI: 10.3934/math.20231103
Received: 01 May 2023
Revised: 24 June 2023
Accepted: 28 June 2023
Published: 07 July 2023

Research article

Double circulant complementary dual codes over $\mathbb{F}_4$

Hatoon Shoaib*

Department of Mathematics, King Abdulaziz University, Jeddah, Saudi Arabia

* **Correspondence:** Email: hashoaib@kau.edu.sa; Tel: +966504661124.

Abstract: Linear codes with complementary-duals (LCD codes) are linear codes that trivially intersect with their dual (Massey, 1992). In this paper, we study double circulant codes (DC codes), which are a special class of quasi-cyclic codes, over $\mathbb{F}_4$ that are LCD. The main techniques used are as follows: Chinese reminder theory (CRT) decomposition in the line of (Ling et al. 2001), explicit enumeration, and asymptotics. In particular, we show that the class of codes considered here is asymptotically good.

Keywords: Artin's conjecture; double circulant code; LCD codes
Mathematics Subject Classification: 94B15

1. Introduction

Linear codes with complementary-duals (LCD codes) were introduced by Massey in 1992 to solve an information theory problem [10]. In the last decade, they gained a lot of attention due to their importance in Boolean masking, which is an important countermeasure against side-channel attacks in cryptography [2]. A survey of the mathematical problems raised by LCD codes, algebraic constructions and possibility bounds is given in [3]. Very recently, the notion was generalized to additive codes over $\mathbb{F}_4$ under the name of additive complementary-dual (ACD) codes [12] .

In the present paper, we study LCD codes over $\mathbb{F}_4$ with a quasi-cyclic structure. Note that the existence of an algorithm to turn any quaternary linear code into an equivalent LCD code [1] should not deter researchers from looking for quaternary LCD codes with a special structure. In particular, we study the family of double circulant codes, which is a family of quasi-cyclic codes of index two. We enumerate the codes of this family for a given length by using the Chinese reminder theory (CRT) approach given in [8]. For a similar approach with a different CRT decomposition, the reader is referred to [5]. Building on these enumeration results, we show that the family of double circulant (DC) LCD codes is asymptotically good by the standard expurgated random coding method, a classical example of which is found in [9]. To simplify matters, we require the primitive root conjecture of Artin [10] to ensure that $x^n - 1$ has only three irreducible factors over $\mathbb{F}_4[x]$ for infinitely many primes n. This asymptotic performance is confirmed by numerical examples of modest lengths.

The rest of the paper is organized as follows: Section 2 contains the basic notions and notations needed for the other sections. Section 3 develops the CRT methodology in our context. Section 4 builds on the previous section to enumerate the family of DC LCD codes over $\mathbb{F}_4$. Section 5 establishes the asymptotic performance of the said family. Section 6 collects numerical examples. Section 7 concludes the paper, and points out some challenging open problems.

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. *A* ***generator matrix*** *of a linear code C of parameters $[N, K]$ over $\mathbb{F}_4$ is a $K \times N$ generator matrix G with entries in $\mathbb{F}_4$ such that $C = \{xG : x \in \mathbb{F}_4^K\}$.*

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:*

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

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 $\mathbb{F}_q[x]/(x^n - 1)$.

Definition 2.3. *A linear block code 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 $c \in C$, there exists a number l such that the codeword obtained by l cyclic shifts is also a codeword in C. That is,*

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

The ***index*** *of C is the smallest $l > 0$ that satisfies this definition.*

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 C is a linear code over $\mathbb{F}_4$ with a generator matrix $G = (I, A)$ where I is the identity matrix and A is circulant.*

Thus, C is a QC code of even length of index $l = 2$. Note that not all QC codes of index 2 can afford such a generator matrix.

If A has order n, then C has a size of 4^n since its generator matrix has rank n. We refer to C as a $[2n, n]$ code.

Definition 2.6. *The* ***dual*** *$C^\perp$ of a linear code C of length n over $\mathbb{F}_4$ is defined as follows:*

$$C^\perp = \{u \in \mathbb{F}_4^n \mid \forall v \in C,\ (u, v) = 0\},$$

where $(u, v) = \sum_{i=1}^{n} u_i v_i$ is the standard inner product of $u, v \in \mathbb{F}_4^n$.

Definition 2.7. *A linear code over $\mathbb{F}_4$ is* ***linear complementary dual*** *(LCD) if it intersects with its dual trivially: $C \bigcap C^{\perp} = \{0\}$.*

Definition 2.8. *A code C is* ***self-dual*** *iff $C = C^{\perp}$.*

Classically, the three parameters of a linear code are concisely expressed as $[N, k, d]$. Here, d is the smallest pairwise Hamming distance between two nonzero codewords.

If C_m is a family of linear codes of parameters $[m, k_m, d_m]$, the rate R and relative distance δ are defined as follows:

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

and

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

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

Recall from [7, Section 2.10.3] that the 4-ary **entropy function** H_4: $[0, 3/4] \to \mathbb{R}$ is defined 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 n is odd. Every double circulant code of length $2n$ may be thought of as a code of length 2 over the ring $R = \mathbb{F}_4[x]/(x^n - 1)$, as stated in [8].

We consider DC codes of length $2n$ and index 2 over $\mathbb{F}_4$. These are $(2n, 4^{\frac{n}{2}})$ codes over $\mathbb{F}_4$, where the codewords are closed under two shifts. In other words, a DC 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 following 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 CRT to break down this ring, we have

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

For simplicity, we let

$$G_i = \frac{\mathbb{F}_4[x]}{< g_i(x) >},\ H_j' = \frac{\mathbb{F}_4[x]}{< h_j(x) >},\ H_j'' = \frac{\mathbb{F}_4[x]}{< h_j^*(x) >}.$$

This decomposition naturally extends to R^2 as

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

In particular,

$$R^2 \simeq \Big(\bigoplus_{i=1}^{s} C_i\Big) \oplus \Big(\bigoplus_{j=1}^{t} (C'_j \oplus C''_j)\Big),$$

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

The next result is essential to characterize the duality properties of our QC codes in terms of their constituent codes. For the definition of the hermitian inner product used in that characterization, we refer to [8].

Lemma 3.1. *A QC DC code is:*

(1) ***Self-dual*** *if the constituents C_i are self-dual for the hermitian inner product and (C'_i, C''_i) are dual pairs for the Euclidean inner product.*

(2) ***LCD*** *if the constituents C_i are LCD for the hermitian inner product and C'_i (resp. C''_i) has trivial intersection with the dual of C''_i (resp. the dual of C'_i).*

The first assertion follows [8]. The second assertion is the index 2 case of [5, Theorem 3.1].

4. Enumeration

In this section, we provide enumerative findings for self-orthogonal double circulant codes and LCD double circulant codes.

In order to simplify the analysis, we are looking for integers n that minimize the number of irreducible factors $x^n - 1$. Note that $x^n - 1$ factors as a product of two irreducible polynomials over the binary field $\mathbb{F}_2$ iff n is an odd prime, for which 2 is a primitive root. Upon assuming Artin's conjecture, proved under generalized Riemann hypothesis (GRH) by Hooley, and "almost proved" by Heath-Brown [6], there are infinitely many primes n which satisfy this condition [11]. In that situation, it can be seen that

$$x^n - 1 = (x + 1)h'h''$$

over $\mathbb{F}_4$ with h', h'' of degree $\frac{(n-1)}{2}$.

Proposition 4.1. *Let n denote an odd prime. If $x^n - 1$ factors as a product of three irreducible polynomials over $\mathbb{F}_4$, then the number of self-dual double circulant codes of length $2n$ is $4^{\frac{n-1}{2}} - 1$.*

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

$$x^n - 1 = (x - 1)h'h''$$

with h, h'' of degree $\frac{(n-1)}{2}$. Then, if $s = 1$ and $t = 1$, here we have: $G_1 \simeq \mathbb{F}_4$ and $H'_1 \simeq H''_1 \simeq \mathbb{F}_Q$, with

$$Q = 4^{\frac{n-1}{2}}.$$

Now, we apply (1) of Lemma 3.1. There is only one possibility for C_1: the repetition code of length 2. Writing

$$C'_1 =< [1, A'] >$$

and

$$C_1'' =< [1, A''] >,$$

we see that these two codes are dual pairs iff $A'A'' = 1$. Since A' is arbitrary nonzero in $\mathbb{F}_Q$ the result follows. □

The counterpart for LCD codes is as follows:

Proposition 4.2. *Let n denote an odd prime. If $x^n - 1$ factors as a product of three irreducible polynomials over $\mathbb{F}_4$, then the number of LCD double circulant codes over $\mathbb{F}_4$ of length $2n$ is* $2(4^{\frac{n-1}{2}} - 1)(4^{\frac{n-1}{2}} - 2)$.

Proof. Similar to the previous proof, we have $G_1 \simeq \mathbb{F}_4$ and $H_1' \simeq H_1'' \simeq \mathbb{F}_Q$, with $Q = 4^{\frac{n-1}{2}}$. Now, we apply (2) of Lemma 3.1.

There are two possible LCD codes for C_1: $< [1, \omega] >$ and $< [1, \omega^2] >$. Writing

$$C_1' =< [1, A'] >$$

and

$$C_1'' =< [1, A''] >,$$

we see that these two codes satisfy the said condition iff $A'A'' \neq 1$. □

5. Asymptotics

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

$$x^n - 1 = (x - 1)h'h''.$$

Let $a(x)$ denote a polynomial of $\mathbb{F}_4[x]$, and let C_a be the LCD double circulant code with the generator matrix $[1, a] \in R^{1\times 2}$.

Lemma 5.1. *If $v = (f, g) \in R^2$, with f, g non zero, then there are at most* $4^{\frac{n+1}{2}}$ *polynomials a such that*

$$v \in C_a =< [1, a] > .$$

Proof. Let $v = (f, g)$, with f, g are in R. By the CRT, the condition $v \in C_a$ is equivalent to the system of equations

$$g(1) = a(1)f(1),$$

$$g(\xi) = a(\xi)f(\xi),$$

$$g(\xi^2) = a(\xi^2)f(\xi^2),$$

where $\xi \in \mathbb{F}_{4^{n-1}}$, $h'(\xi) = 0$. Since the third equation is the conjugate of the second, it can be forgotten in the following discussion. For the rest of the proof, for simplicity, we write $g' = g(\xi)$, $g'' = g(\xi^2)$ and so on. To determine a', we distinguish the following cases:

(a) If $f' \neq 0$, then $a' = \frac{g'}{f'}$ has a unique solution.

(b) If $f' = 0$, then

   (i) If $g' \neq 0$, we have no solution.

(ii) If $g' = 0$, then a' is undetermined and we have at most $4^{\frac{n-1}{2}}$ choices for a'.

By definition, we have at most 4 values for $a(1)$. Hence, we have at most $4^{\frac{n+1}{2}}$ choices for a. □

Now, we can state and prove the main result of this section.

Theorem 5.2. *For every $\epsilon > 0$, there is a sequence of LCD double circulant codes with relative distance*

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

and rate $1/2$. This family of codes is asymptotically good.

Proof. The number of double circulant codes containing a vector of weight $d \simeq 2\delta n$ or less are by standard entropic estimates of Hamming balls volumes [7, Lemma 2.10.3] and Lemma 5.1 of the order $O(4^{n/2+2nH_4(\delta)})$ up to subexponential terms. This number will be less than the total number of LCD double circulant codes, which is by Proposition 4.2 of the order of $\Omega(4^n)$, provided that

$$4^n > 4^{n/2+2nH_4(\delta)+\epsilon}$$

holds for $n \to \infty$.

This condition reduces, after taking $\log_4$, dividing by n, and taking limits, to the condition

$$-\frac{1}{2} + 2H_4(\delta) \leq -\epsilon$$

for all $\epsilon > 0$.

The first assertion follows and implies the second since our codes have constant rate $1/2$. □

6. Numerical examples

In view of [1], we should expect the minimum distance d of $[2n, n]$ LCD codes over $\mathbb{F}_4$ to be as high as that of the best linear $[2n, n]$ codes over $\mathbb{F}_4$, denoted here by d_G, as listed in [4]. In Table 1, we give these three parameters for a DC code with generator matrix $(1, a(x))$. The vector of coefficients of $a(x)$ is denoted by **a**.

Table 1. Parameters of LCD DC codes.

n	d_G	d	**a**
3	4	4	$(\omega, 1, 1)$
4	4	4	$(1, 0, 1, \omega^2)$
5	5	5	$(0, \omega^2, \omega, 1, \omega)$
6	5	5	$(\omega^2, 1, \omega^2, 0, 1, 0)$
7	6	6	$(\omega, 1, 1, \omega, \omega^2, \omega^2, \omega^2)$
8	6	6	$(0, \omega, \omega^2, \omega, 0, \omega^2, \omega, \omega)$
9	8	6	$(\omega^2, \omega^2, 0, \omega, \omega, 0, 1, 0, \omega^2)$
10	8	7	$(\omega, 0, 0, \omega, 0, \omega, \omega^2, \omega, \omega^2, 0)$
11	8-9	7	$(0, \omega^2, 1, 1, \omega^2, \omega, \omega, \omega^2, 1, \omega, \omega^2)$
12	8	8	$(\omega^2, 1, 0, \omega^2, 0, 1, \omega, 0, \omega^2, 1, 1, \omega)$
13	10	8	$(\omega^2, 0, \omega^2, 0, \omega, \omega^2, \omega, \omega^2, 1, \omega, 0, 0, \omega^2)$
14	11	9	$(0, 1, \omega, \omega, \omega, \omega, \omega^2, \omega^2, \omega, \omega, 0, 1, \omega, 0)$

7. Conclusions and open problems

In this paper, we have investigated thr enumeration, and asymptotic performance of the class of LCD double circulant codes over $\mathbb{F}_4$. The analysis of quasi-cyclic codes by the CRT method of [8] has been the main technical tool. We derived a modified GV bound for this class of codes (Theorem 5.2). Proving similar asymptotic results for self-dual double circulant codes would require a sharpening of Lemma 5.1, in view of the small quantity of self-dual codes (Proposition 4.1) .

One avenue of research includes the extension of this work to other finite fields and to Galois rings. Staying over $\mathbb{F}_4$ but changing the index, and therefore the rate of the codes considered, is also worthy of attention. For example, we are thinking of the four circulant constructions studied in [13] to construct linear complementary dual codes.

Use of AI tools declaration

I declare that I have not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The author declares no conflict of interest in this paper.

References

1. C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, *IEEE Trans. Inf. Theory*, **64** (2018), 3010–3017. https://doi.org/10.1109/TIT.2018.2789347
2. C. Carlet, S. Guilley, *Coding theory and applications*, Springer, 2015. https://doi.org/10.1007/978-3-319-17296-5-9
3. S. T. Dougherty, J. L. Kim, B. Ozkaya, L. Sok, P. Solé, The combinatorics of LCD codes: linear programming bound and orthogonal matrices, *Int. J. Inf. Coding Theory*, **4** (2017), 116–128. https://doi.org/10.1504/IJICOT.2017.083827
4. *Bounds on the minimum distance of linear codes and quantum codes*, Markus Grassl, 2023. Available from: http://www.codetables.de.
5. C. Güneri, B. Özkaya, P. Solé, Quasi-cyclic complementary dual codes, *Finite Fields Appl.*, **42** (2016), 67–80. https://doi.org/10.1016/j.ffa.2016.07.005
6. D. R. Heath-Brown, Artin's conjecture for primitive roots, *Q. J. Math.*, **37** (1986), 27–38.
7. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.
8. S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, *IEEE Trans. Inf. Theory*, **47** (2001), 2751–2760. https://doi.org/10.1109/18.959257
9. F. J. MacWilliams, N. J. A. Sloane, J. G. Thompson, Good self dual codes exist, *Discrete Math.*, **3** (1972), 153–162. https://doi.org/10.1016/0012-365X(72)90030-1

10. J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, **106-107** (1992), 337–342. https://doi.org/10.1016/0012-365X(92)90563-U

11. P. Moree, Artin's primitive root conjecture–a survey, *Integers*, **12** (2012), 0043. https://doi.org/10.1515/integers-2012-0043

12. M. Shi, N. Liu, F. Özbudak, P. Solé, Additive cyclic complementary dual codes over $\mathbb{F}_4$, *Finite Fields Appl.*, **83** (2022), 102087. https://doi.org/10.1016/j.ffa.2022.102087

13. M. Shi, H. Zhu, L. Qian, P. Solé, On self-dual four circulant codes, *Int. J. Found. Comput. Sci.*, **29** (2018), 1143–1150. https://doi.org/10.1142/S0129054118500259