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

Hatoon A. Shoaib

King Abdulaziz University, Mathematics Department

ALCOCRYPT
Marseille, France, February 2023

Outline

- Introduction
- History
- CRT
- New Results
- Conclusion
- Future Work

Double CirculantComplementary Dual Codes over $\mathbb{F}_4$

(DC Code)

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.

(Circulant Matrix)

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.

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

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

(LCD Code)

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

Introduction

- LCD codes were introduced by Massey in 1992 to solve an Information Theory problem [1].
- In the last decade, they gained a lot of attention due to their importance in Boolean masking, 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 ACD codes [4].
- Today we study such LCD codes with a quasi-cyclic structure.

[1] J. L. Massey, Linear codes with complementary duals, Discrete Math. **106-107** : 337-342, 1992.
[2] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks. Coding Theory and Applications. Raquel Pinto, Paula Rocha-Malonek, Paolo Vettori eds, Springer, CIMSMS, **3** : 97–105, 2015.
[3] S. T. Dougherty, J. Kim, B. Ozkaya, L. Sok, P. Solé, The combinatorics of LCD codes : linear programming bound and orthogonal matrices. Int. J. Inf. Coding Theory **4**(2/3), (2017), 116–128.
[4] M. Shi, N. Liu, F. Ozbudak, P. Solé Additive cyclic complementary dual codes over F4. Finite Fields Their Appl. **83** 102087 (2022).

History

” Are long cyclic codes good” ?

Assmus-Mattson-Turyn (1966)

If $C(n)$ is a family of codes of parameters $[n, k_n, d_n]$, the **rate** r **is**

$$r = \limsup_{n\to\infty} \frac{k_n}{n},$$

relative distance δ **is**

$$\delta = \liminf_{n\to\infty} \frac{d_n}{n}.$$

A family of codes is said to be good iff $r\delta > 0$.

A Brief History of Good Codes :

- **Forty years ago**, quasi cyclic codes were proved good in the asymptotic sense.
- **Eighteen years ago**, it was shown that even the self-dual subclass is good.
- **Seven years ago**, it was proved that the class of quasi-cyclic linear complementary dual codes are good.
- **Recently**, we studied the class of double circulant complementary dual codes over $\mathbb{F}_4$, emphasizing the aspects of :
  - Enumeration.
  - Asymptotic performance.

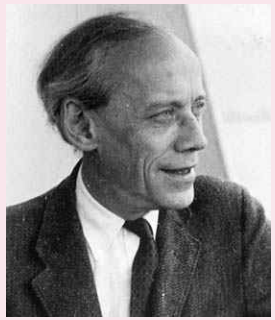
How to have only three factors ?

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.

In number theory, **Artin's conjecture**, proved under the Generalized Riemann Hypothesis (GRH) by
Hooley in 1967, and "almost proved" by
Heath-Brown [5], there are infinitely many primes n which satisfy this condition [6]. In that situation, it can be seen that

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

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



Emil Artin

[5] D.R. Heath-Brown, ARTIN'S CONJECTURE FOR PRIMITIVE ROOTS, The Quarterly Journal of Mathematics, Volume 37, Issue 1, March 1986, Pages 27â38.
[6] P. Moree, Artin's Primitive Root Conjecture â A Survey Integers https://doi.org/10.1515/integers-2012-0043.

Chinese Remainder Theorem :

1. 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

$$R = \mathbb{F}_4/(x^n - 1).$$

2. We use the Chinese Remainder Theorem to break down this ring

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

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

Chinese Remainder Theorem : continued

1. In particular,

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

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.

Lemma

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').

Enumeration

First, exact enumeration for self-orthogonal double circulant codes and LCD double circulant codes are derived.

Proposition

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

Proposition

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 $2(4^{\frac{n-1}{2}} - 1)(4^{\frac{n-1}{2}} - 2)$.

Covering lemma

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 generator matrix $[1, a] \in R^{1\times 2}$.

Lemma

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

The proof uses the CRT decomposition of $R(n; \mathbb{F}_4)$.

Asymptotic Bound I

The 4-ary **entropy function** $H_4 : [0, 3/4] \to \mathbb{R}$ is defined as follows :

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

Denote by $B_q(n, t)$ the volume of the Hamming ball of radius t in $\mathbb{F}_q^n$.
Up to constant multipliers for $n \to \infty$ we have

$$B_q(n, t) \sim \frac{q^{nH_q(t))}}{\sqrt{n}}.$$

Asymptotic Bound II

Now, are now ready for the main result :

Theorem

For every $\epsilon > 0$, 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.

This shows that there are infinite families of LCD double circulant codes with relative distance satisfying a modified Gilbert-Varshamov bound.

Gilbert-Varshamov bound

(Gilbert-Varshamov bound)

Let $q \geq 2$. For every $0 \leq \delta \leq 1 - \frac{1}{q}$. Then there exist a linear code with rate $R \geq 1 - H_q(\delta)$ and relative distance δ.

Conclusion :

- Describes the factorization of $x^n - 1$ over $\mathbb{F}_4$.
- We enumerate the codes of this family for given length using the CRT.
- Building on that enumeration, we show that the family of DC LCD codes is good.
- In the last Theorem, We derived a modified GV bound for this class of codes.

Future Work :

- 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.
- Maybe we can think of the four circulant constructions studied in [7] to construct self-dual codes.

[7] M. Shi, H. Zhu, L. Qian, P. Solé On Self-Dual Four Circulant Codes. Int. J. Found. Comput. Sci. 29(7) : 1143-1150 (2018).

Thank You

For Your Attention

Any Questions?

NO?

SUPER!