On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q

Preprint · June 2018

CITATIONS
0

READS
206

5 authors, including:

Minjia Shi
Anhui University
154 PUBLICATIONS **528** CITATIONS
SEE PROFILE

Hongwei Zhu
Anhui University
5 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Liqin Qian
Nanjing University of Aeronautics & Astronautics
13 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Lin Sok
Institut Mines-Télécom
27 PUBLICATIONS **136** CITATIONS
SEE PROFILE

On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$ *

Minjia Shi,†Hongwei Zhu,‡Liqin Qian,§Lin Sok,¶and Patrick Solé‖

Abstract

Double circulant codes of length $2n$ over the semilocal ring $R = \mathbb{F}_q + u\mathbb{F}_q$, $u^2 = u$, are studied when q is an odd prime power, and -1 is a square in $\mathbb{F}_q$. Double negacirculant codes of length $2n$ are studied over R when n is even and q is an odd prime power. Exact enumeration of self-dual and LCD such codes for given length $2n$ is given. Employing a duality-preserving Gray map, self-dual and LCD codes of length $4n$ over $\mathbb{F}_q$ are constructed. Using random coding and the Artin conjecture, the relative distance of these codes is bounded below. The parameters of examples of the modest length are computed. Several such codes are optimal.

Keywords: double circulant codes, double negacirculant codes, codes over rings, self-dual codes, LCD codes, Artin conjecture

MSC(2010): 94 B15, 94 B25, 05 E30

*This research is supported by National Natural Science Foundation of China (61672036), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133) and the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

†Minjia Shi, Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, Anhui University, No.3 Feixi Road, Hefei, Anhui, 230039, China, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China and National Mobile Communications Research Laboratory, Southeast University, China, smjwcl.good@163.com

‡Hongwei Zhu, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, zhwgood66@163.com

§Liqin Qian, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, qianliqin_1108@163.com

¶Lin Sok, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601 and Department of Mathematics, Royal University of Phnom Penh, 12156 Phnom Penh, Cambodia, sok.lin@rupp.edu.kh

‖Patrick Solé, CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France, sole@enst.fr

1 Introduction

Double circulant and double negacirculant self-dual codes over finite fields have been studied recently in [1] and [3], respectively, from the viewpoint of enumeration and asymptotic performance. The main tool there is the CRT approach to quasi-cyclic codes as introduced in [12], and generalized to quasi-twisted codes in [10]. It is natural to extend these results to other classes of ring alphabets, beyond finite fields, building on the theory developed in [13]. Double circulant self-dual codes over a commutative ring can only exist if there is a square root of -1 over that ring [13]. For the ring $R = \mathbb{F}_q + u\mathbb{F}_q$, $u^2 = u$, a ring of current interest [18], this requirement leads to the condition that -1 is a square in $\mathbb{F}_q$. This ring is studied here because of a duality preserving Gray map that turns self-dual codes into self-dual codes, and similarly, LCD codes into LCD codes. While this Gray map was defined already in [20], its duality properties were not considered there. LCD codes are defined as codes intersecting trivially with their dual. They enjoy a wealth of combinatorial and algebraic properties [5, 7]. In particular quasi-cyclic codes over fields have been proved to contain infinite families of good long LCD codes [7]. In this paper we study both self-dual and LCD double circulant and double negacirculant codes over R and show that all four families contain arbitrarily long codes with fixed rate and with relative distance of the Gray image bounded below by a nonzero constant. These results are based on the complete enumeration of the codes in these four families for given length $2n$. While, for asymptotic purposes, only the case of n a prime with q primitive modulo n is needed, the counting results are developed for all n's. The said arithmetic condition holds for infinitely many n's by Artin conjecture [15], which is proved conditionally under GRH [8]. In the case of negacirculant codes, n is supposed to be a power of 2 for asymptotics, and the truth of Artin conjecture is not needed. The factorization of $x^n + 1$ in that case depends on properties of Dickson polynomials.

The material is organized as follows. Section 2 contains the preliminary requisite necessary to the further sections. Section 3 develops the machinery of the CRT approach to double circulant and double negacirculant codes, and derives the main enumeration results. Section 4 is dedicated to asymptotic bounds on the relative Hamming distance of the Gray image of these codes when their lengths tends to infinity. Section 5 computes some numerical examples. Section 6 concludes the article and discusses open problems.

2 Preliminaries

2.1 The Ring $\mathbb{F}_q + u\mathbb{F}_q$

Let q be a prime power, and let $\mathbb{F}_q$ be the finite field of order q. Consider the ring $R = \mathbb{F}_q + u\mathbb{F}_q$ where $u^2 = u$. It is semi-local with maximal ideals (u) and $(u-1)$. The group of units R^* is isomorphic, as a multiplicative group, to the product of two cyclic groups of order $(q-1)$. To construct double circulant codes, we need to know when the ring $R = \mathbb{F}_q + u\mathbb{F}_q$ contains a square root of -1.

THEOREM 2.1. *The ring R contains a square root of -1 if one and only one of the following three conditions is true:*

- *q is a power of 2;*
- *$q = p^b$, where p is a prime congruent to $1 \mod 4$;*
- *$q = p^{2b}$, where p is a prime congruent to $3 \mod 4$, and $b \geq 1$ is an integer.*

Proof. Note first that $\mathbb{F}_q$ contains a square root of -1 iff one of the above three conditions is true [13]. The condition is sufficient. If one of the three cases is true, then $\mathbb{F}_q$, a subring of R, already contains such a root. The condition is necessary. Write such a root as $x + uy$ with $x, y \in \mathbb{F}_q$. Then $(x+uy)^2 = x^2 + u(y^2 + 2xy)$, showing that $x^2 = -1$, and that x is a square root of -1 in $\mathbb{F}_q$. □

Remark: Note that for each x in the above proof there are two possible value of y that is $y = 0$, or $y = -2x$. There are thus zero or four distinct square roots of -1 in R.

2.2 Norm Function over Finite Field

For all $x \in \mathbb{F}_{q^n}$, the norm of x over $\mathbb{F}_q$ is a map **Norm**: $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ defined by

$$Norm(x) = x^{(q^n-1)/(q-1)}.$$

Moreover, Norm is a multiplicative homomorphism which is surjective ([11, Theorem 2.28]). $Norm(0) = 0$, so it maps $\mathbb{F}_{q^n}^*$ onto $\mathbb{F}_q^*$, where each nonzero element in $\mathbb{F}_q^*$ has a preimage of size $(q^n-1)/(q-1)$ in $\mathbb{F}_{q^n}^*$.

2.3 Codes

A **linear code** C over R of length n is an R-submodule of R^n. If $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are two elements of R^n, their standard (Euclidean) inner product

is defined by $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$, where the operation is performed in R. The Euclidean dual code of C is denoted by $C^{\perp}$ and defined as $C^{\perp} = \{y \in R^n \mid \langle x, y\rangle = 0, \forall x \in C\}$. A linear code C of length n over R is called **self-dual** if $C = C^{\perp}$. A linear code C of length n over R is called **linear complementary dual (LCD)** if $C \cap C^{\perp} = \{\mathbf{0}\}$.

A matrix A over R is said to be **circulant** (*resp.* **negacirculant**) if its rows are obtained by successive shifts (*resp.* **negashifts**) from the first row. A code C is called **double circulant** (*resp.* **double negacirculant**) over R if its generator matrix G will be of the form $G = (I, A)$, where I is the identity matrix of order n and A is a circulant (*resp.* negacirculant) matrix of the same order.

If $C(n)$ is a family of codes with parameters $[n, k_n, d_n]$ over $\mathbb{F}_q$, the rate ρ and relative distance δ are defined as $\rho = \limsup_{n\to\infty} \frac{k_n}{n}$ and $\delta = \liminf_{n\to\infty} \frac{d_n}{n}$, respectively. A family of code is **good** if $\rho\delta > 0$. Both limits are finite as limits of bounded quantities.

2.4 Gray Map

2.4.1 q Odd

The Gray map ϕ over the ring R is defined by $\phi(a + ub) = (-b, 2a + b)$ for $a, b \in \mathbb{F}_q$ from R to $\mathbb{F}_q^2$. Clearly, ϕ is a bijection from R to $\mathbb{F}_q^2$, which extends naturally to a map from R^n to $\mathbb{F}_q^{2n}$. Adopting the idea of [5, Theorem 2.10.3], we can prove the following result.

THEOREM 2.2. *If C is a self-dual (resp. LCD) code of length n over R, then $\phi(C)$ is a self-dual (resp. LCD) code of length $2n$ over $\mathbb{F}_q$.*

Proof. Consider a pair of codewords $w = (w_1, w_2, \ldots, w_n)$, $v = (v_1, v_2, \ldots, v_n) \in C$, where $w_i = a_i + b_i u$, $v_i = c_i + d_i u$ and $a_i, b_i, c_i, d_i \in \mathbb{F}_q$ for $1 \le i \le n$. If C is a self-dual code over R, then $\langle w, v\rangle = \sum_{i=1}^{n} (a_i + b_i u)(c_i + d_i u) = \sum_{i=1}^{n} (a_i c_i + (a_i d_i + b_i c_i + b_i d_i)u) = 0$, which implies that

$$\sum_{i=1}^{n} a_i c_i = 0 \text{ and } \sum_{i=1}^{n} (a_i d_i + b_i c_i + b_i d_i) = 0.$$

According to the definition of the Gray map, we have

$$\begin{aligned} \langle \phi(w), \phi(v)\rangle &= \langle \phi(a_1 + b_1 u, \ldots, a_n + b_n u), \phi(c_1 + d_1 u, \ldots, c_n + d_n u)\rangle \\ &= \sum_{i=1}^{n} (b_i d_i + 4a_i c_i + 2a_i d_i + 2b_i c_i + b_i d_i) \\ &= \sum_{i=1}^{n} (4a_i c_i + 2(a_i d_i + b_i c_i + b_i d_i)) = 0. \end{aligned}$$

It implies that $\phi(C^\perp) \subseteq \phi(C)^\perp$. Since the Gray map ϕ is a bijection from R to $\mathbb{F}_q^2$, then $\phi(C^\perp) = \phi(C)^\perp$.

If C is a LCD code over R, then $C \cap C^\perp = \{\mathbf{0}\}$. We can easily obtain that $\phi(C \cap C^\perp) \subseteq \phi(C) \cap \phi(C^\perp)$. Because ϕ is a bijection from R to $\mathbb{F}_q^2$, equality holds in the preceding inclusion and

$$\phi(C) \cap \phi(C)^\perp = \phi(C) \cap \phi(C^\perp) = \phi(C \cap C^\perp) = \{\mathbf{0}\}.$$

Thus $\phi(C)$ is a LCD code of length $2n$ over $\mathbb{F}_q$. □

2.4.2 q Arbitrary

We can generalize the map β of [4] as follows. Define a map $\beta : R \to \mathbb{F}_q^2$ by the formula $\beta(a + ub) = (a, a + b)$, for all $a, b \in \mathbb{F}_q$.

THEOREM 2.3. *If C is a self-dual (resp. LCD) code of length n over R, then $\beta(C)$ is a self-dual (resp. LCD) code of length $2n$ over $\mathbb{F}_q$.*

Proof. We claim that $\beta(C^\perp) = \beta(C)^\perp$. The rest of the proof follows in the same way as the proof of Theorem 2.2. To prove the claim note that if $\langle w, v \rangle = 0$ like in the said proof, then

$$\langle \beta(w), \beta(v) \rangle = \sum_{i=1}^{n} a_i c_i + (a_i + b_i)(c_i + d_i) = \sum_{i=1}^{n} a_i d_i + b_i c_i + b_i d_i = 0.$$

This shows that $\beta(C^\perp) \subseteq \beta(C)^\perp$, and β being bijective, that $\beta(C^\perp) = \beta(C)^\perp$. □

3 Algebraic Structure of Double Circulant and Double Negacirculant Codes

3.1 Double Circulant Codes of Odd Length

In this subsection, we assume that n is an odd integer, q is a prime power and $\gcd(n, q) = 1$. We can cast the factorization of $x^n - 1$ into distinct irreducible polynomials over R in 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 $\alpha \in R^*$, $g_i(x)$ is a self-reciprocal polynomial with degree $2e_i$ for $2 \leq i \leq s$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ with degree d_j for $1 \leq j \leq t$. By the Chinese

Remainder Theorem (CRT), we have

$$\begin{aligned}
\frac{R[x]}{(x^n-1)} &\simeq \frac{R[x]}{(x-1)} \oplus \left(\bigoplus_{i=2}^{s} R[x]/(g_i(x)) \right) \oplus \left(\bigoplus_{j=1}^{t} (R[x]/(h_j(x)) \oplus (R[x]/(h_j^*(x)))) \right) \\
&\simeq R \oplus \left(\bigoplus_{i=2}^{s} \frac{\mathbb{F}_q[u,x]}{(u^2-u, g_i(x))} \right) \oplus \left(\bigoplus_{j=1}^{t} \frac{\mathbb{F}_q[u,x]}{(u^2-u, h_j(x))} \oplus \frac{\mathbb{F}_q[u,x]}{(u^2-u, h_j^*(x))} \right) \\
&\simeq R \oplus \left(\bigoplus_{i=2}^{s} \mathbb{F}_{q^{2e_i}} + u\mathbb{F}_{q^{2e_i}} \right) \oplus \left(\bigoplus_{j=1}^{t} (\mathbb{F}_{q^{d_j}} + u\mathbb{F}_{q^{d_j}}) \oplus (\mathbb{F}_{q^{d_j}} + u\mathbb{F}_{q^{d_j}}) \right) \\
&:= R \oplus \left(\bigoplus_{i=2}^{s} R_{2e_i} \right) \oplus \left(\bigoplus_{j=1}^{t} R_{d_j} \oplus R_{d_j} \right),
\end{aligned}$$

where we let $R_\ell = \mathbb{F}_{q^\ell} + u\mathbb{F}_{q^\ell}$, for any nonegative integer ℓ. Note that all of these rings are extensions of R. This decomposition naturally extends to $\left(\frac{R[x]}{(x^n-1)}\right)^2$ as

$$\left(\frac{R[x]}{(x^n-1)}\right)^2 \simeq R^2 \oplus \left(\bigoplus_{i=2}^{s} (R_{2e_i})^2 \right) \oplus \left(\bigoplus_{j=1}^{t} (R_{d_j})^2 \oplus (R_{d_j})^2 \right).$$

In particular, each linear code C of length 2 over $\frac{R[x]}{(x^n-1)}$ can be decomposed as the "CRT sum"

$$C \simeq C_1 \oplus \left(\bigoplus_{i=2}^{s} C_i \right) \oplus \left(\bigoplus_{j=1}^{t} (C_j' \oplus C_j'') \right),$$

where C_1 is a linear code over R, for each $2 \le i \le s$, C_i is a linear code over R_{2e_i}, and for each $1 \le j \le t$, C_j' and C_j'' are linear codes over R_{d_j}, which are called the constituents of C.

In self-reciprocal case, we give the definition of the Hermitian inner product over R_{2e_i}. For all $z = z_1 + uz_2 \in R_{2e_i}$, where $z_1, z_2 \in \mathbb{F}_{q^{2e_i}}$, the conjugate of z over R_{2e_i} is $\overline{z} = z_1^{q^{e_i}} + uz_2^{q^{e_i}}$, and the Hermitian inner product is defined as: $(z, z') \cdot (w, w') = z\overline{w} + z'\overline{w'}$, where $z, z', w, w' \in R_{2e_i}$.

THEOREM 3.1. *Let n denote a positive odd integer, and let q be a prime power coprime with n. Assume that the factorization of $x^n - 1$ into irreducible polynomials over R is of the form*

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

with $\alpha \in R^*$, $n = 1 + \sum_{i=2}^{s} 2e_i + 2\sum_{j=1}^{t} d_j$. *Then the total number of self-dual double circulant codes over* R *is*

$$4\prod_{i=2}^{s}(1+q^{e_i})^2\prod_{j=1}^{t}\left(q^{d_j}-1\right)^2.$$

Proof. We can count the number of self-dual double circulant codes by counting their constituent codes. There are four self-dual codes C_1 of length 2 over R, whose generators are $(1,\omega)$, $(1,-\omega)$, $(1,\omega(1-2u))$ and $(1,\omega(2u-1))$, respectively, where $\omega^2=-1$ and $\omega \in \mathbb{F}_q$. More generally, a factor $g_i(x)$ of degree $2e_i$ leads to counting self-dual Hermitian codes C_i of length 2 over R_{2e_i}. If $(1, c_{e_i})$ is the generator of C_i then $(1, c_{e_i}) \cdot (1, c_{e_i}) = 1 + c_{e_i}\overline{c_{e_i}} = 1 + c_{e_i}c_{e_i}{}^{q^{e_i}} = 0$. Let $c_{e_i} = x + uy$, where $x, y \in \mathbb{F}_{q^{2e_i}}$, we then have

$$1+(x+uy)(x^{q^{e_i}}+uy^{q^{e_i}})=0 \Longleftrightarrow \begin{cases} x\cdot x^{q^{e_i}}=-1, \\ (x+y)(x+y)^{q^{e_i}}=-1, \end{cases} \Longleftrightarrow \begin{cases} Norm(x)=-1, \\ Norm(x+y)=-1, \end{cases}$$

where $Norm$ is a map from $\mathbb{F}_{q^{2e_i}}$ to $\mathbb{F}_{q^{e_i}}$. So there are $q^{e_i}+1$ roots for $Norm(x) = -1$ and $q^{e_i}+1$ roots for $Norm(x+y) = -1$. Therefore, the number of ordered pairs (x, y) is equal to $(q^{e_i}+1)^2$.

In the last case about reciprocal pairs, note that $h_j(x)$ and $h_j^*(x)$ of both degree d_j leads to counting dual pairs of codes (for the Euclidean inner product) of length 2 over R_{d_j}, that is to count the number of solutions of the equation $1 + c'_{d_j}c''_{d_j} = 0$, where $(1, c'_{d_j})$ and $(1, c''_{d_j})$ are the generators of C'_j and C''_j, respectively. If $c'_{d_j} \in R^*_{d_j}$, then $c''_{d_j} = -\frac{1}{c'_{d_j}}$. There are $|R^*_{d_j}| = (q^{d_j}-1)^2$ choices for (c'_{d_j}, c''_{d_j}). If $c'_{d_j} \in R_{d_j}\backslash R^*_{d_j}$, then $c'_{d_j} = ux \in (u)$ or $c'_{d_j} = (u-1)x \in (u-1)$. In this case, we claim that $1+c'_{d_j}c''_{d_j} = 0$ cannot occur. Otherwise, by reducing the equation modulo u or $u-1$, we would get $1 = 0$ in $\mathbb{F}_{q^{d_j}}$, contradiction. The proof of the theorem is now completed. □

THEOREM 3.2. *Keep the same notations as above, then the total number of LCD double circulant codes over* R *is*

$$(q^2-4)\prod_{i=2}^{s}(q^{4e_i}-(q^{e_i}+1)^2)\prod_{j=1}^{t}(q^{4d_j}-2q^{3d_j}+3q^{2d_j}-2q^{d_j}+1).$$

Proof. Like in the self-dual case, we can count the number of LCD double circulant codes C by considering each constituent of C. Note that if a double circulant code of length 2 over some extension of R is not self-dual, then it is LCD because of having single-row generator matrix. Combined with the results of Theorem 3.1, the total number of LCD double circulant constituent codes C_1 over R is q^2-4 and the total number of LCD double circulant constituent codes C_i over R_{2e_i} is $q^{4e_i}-(q^{e_i}+1)^2$.

In the last case about reciprocal pairs, note that $h_j(x)$ and $h_j^*(x)$ of degree d_j leads to counting pairs of codes of length 2 over R_{d_j} with certain intersection properties [7]. Let $(1, a)$ and $(1, b)$ be the generators of C'_j and C''_j, respectively.

$$\begin{cases} C'_j \cap C''^{\perp}_j = \{0\}, \\ C''_j \cap C'^{\perp}_j = \{0\}. \end{cases} \iff 1 + ab \in R^*_{d_j}.$$

Without loss of generality, we discuss on the unit character of a as follows.

- If $a \in R^*_{d_j}$, then $b \in \frac{-1}{a} + R^*_{d_j}$ and $|\frac{-1}{a} + R^*_{d_j}| = |R^*_{d_j}|$. In this case, we have $|R^*_{d_j}|^2 = (q^{d_j} - 1)^4$ choices for (a, b).

- If $a \in R_{d_j} \backslash \{R^*_{d_j} \cup \{0\}\}$, then $a = u\alpha$ or $a = (u-1)\alpha$. Let $b = \beta' + u\beta''$, where $\alpha \in \mathbb{F}^*_{q^{d_j}}$ and $\beta', \beta'' \in \mathbb{F}_{q^{d_j}}$. When $a = u\alpha$, we then have

  $$1 + ab = 1 + u\alpha(\beta' + u\beta'') = 1 + u\alpha(\beta' + \beta'') \in R^*_{d_j}.$$

  This is equivalent to $\alpha(\beta' + \beta'') \neq -1$. There are $q^{d_j}(q^{d_j} - 1)^2$ choices for $(\alpha, \beta', \beta'')$. When $a = (u-1)\alpha$, then we have

  $$1 + ab = 1 + (u-1)\alpha(\beta' + u\beta'') = 1 + (u-1)\alpha\beta' \in R^*_{d_j}.$$

  This is equivalent to $\alpha\beta' \neq 1$ and β'' is arbitrary in $\mathbb{F}_{q^{d_j}}$. There are also $q^{d_j}(q^{d_j} - 1)^2$ choices for $(\alpha, \beta', \beta'')$.

- If a is zero, then b is arbitrary in R_{d_j}. There are q^{2d_j} choices for b.

Hence, the number of the last case about reciprocal pairs is $(q^{d_j} - 1)^4 + q^{d_j}(q^{d_j} - 1)^2 + q^{d_j}(q^{d_j} - 1)^2 + q^{2d_j} = q^{4d_j} - 2q^{3d_j} + 3q^{2d_j} - 2q^{d_j} + 1$. The proof of the theorem is now completed. □

3.2 Double Negacirculant Codes of Even Length

For our purpose, we assume in this subsection that n is an even integer, q is an odd prime power, and that $\gcd(n, q) = 1$. We can cast the factorization of $x^n + 1$ into distinct irreducible polynomials over R in the form

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

where $\alpha \in R^*$, $g_i(x)$ is a self-reciprocal polynomial with degree $2e_i$ for $1 \leq i \leq s$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ with degree d_j for $1 \leq j \leq t$. Using the same notations

and arguments as above, we can easily carry out the results as follows:

$$\frac{R[x]}{(x^n+1)} \simeq \left(\bigoplus_{i=1}^{s} R_{2e_i}\right) \oplus \left(\bigoplus_{j=1}^{t} R_{d_j} \oplus R_{d_j}\right),$$

and

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

Similar to the proof of Theorem 3.1 and Theorem 3.2, we have the following two enumeration results. Their proofs are omitted.

THEOREM 3.3. *Let n denote a positive even integer, and q a prime power coprime with n. Assume that the factorization of x^n+1 into irreducible polynomials over $R = \mathbb{F}_q + u\mathbb{F}_q$ is of the form*

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

with $\alpha \in R^*$, $n = \sum_{i=1}^{s} 2e_i + 2\sum_{j=1}^{t} d_j$. Then the total number of self-dual double negacirculant codes over R is

$$\prod_{i=1}^{s} (1+q^{e_i})^2 \prod_{j=1}^{t} (q^{d_j}-1)^2.$$

THEOREM 3.4. *Keep the same notations as above, then the total number of LCD double negacirculant codes over R is*

$$\prod_{i=1}^{s} (q^{4e_i} - (q^{e_i}+1)^2) \prod_{j=1}^{t} (q^{4d_j} - 2q^{3d_j} + 3q^{2d_j} - 2q^{d_j} + 1).$$

4 Distance Bound

4.1 Distance Bound for Double Circulant Codes

Let q be a primitive root mod n and n be an odd prime. Recall that $x^n - 1 = (x-1)(x^{n-1} + \ldots + x + 1) = (x-1)h(x)$. Note that $h(x)$ is irreducible over R, because $\mathbb{F}_q$ is a subring of R, and $h(x)$ is irreducible over $\mathbb{F}_q$.

By the Chinese Remainder Theorem (CRT), we have

$$\frac{R[x]}{(x^n-1)} \simeq \frac{R[x]}{(x-1)} \oplus \frac{R[x]}{(h(x))} \simeq R \oplus \frac{\mathbb{F}_q[u,x]}{(u^2-u, h(x))} \simeq R \oplus \mathbb{F}_{q^{n-1}} + u\mathbb{F}_{q^{n-1}}.$$

Let $\mathcal{R}$ denote the ring $\frac{R[x]}{(h(x))}$, so R is a subring of $\mathcal{R}$. The nonzero codewords of the cyclic code of length n generated by $h(x)$ is called **constant vector**.

LEMMA 4.1. *If the nonzero vector $z = (e, f)$ with e not a constant vector, then there are at most q^{n+1} generators $(1, a)$ such that $z \in C_a$ and C_a is a double circulant code over R.*

Proof. By the Chinese Remainder Theorem (CRT), $(e, f) \simeq (e_1, f_1) \oplus (e_2, f_2)$. Since $(e, f) \in C_a$, then $f = ea$, $f_1 = e_1 a_1$ and $f_2 = e_2 a_2$, where e_1, f_1, $a_1 \in R$ and e_2, f_2, $a_2 \in \mathcal{R}$. Let $a_1 = a_1' + ua_1''$, $a_2 = a_2' + ua_2''$, where $a_1', a_1'' \in \mathbb{F}_q$ and $a_2', a_2'' \in \mathbb{F}_{q^{n-1}}$.

In the first constituent of C_a, we discuss on the unit character of e_1 as follows.

- If $e_1 \in R^*$, there exists only one solution for $a_1 = \frac{f_1}{e_1}$.
- If $e_1 \in (u)\backslash\{0\}$, then $e_1 = ue_1'$ and $f_1 = uf_1'$, where $e_1' \in \mathbb{F}_q^*$, $f_1' \in \mathbb{F}_q$. Since $u^2 = u$, then $f_1 = uf_1' = ue_1'a_1 = ue_1'(a_1' + ua_1'') = ue_1'a_1' + ue_1'a_1'' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1' + a_1''$. There are q choices for a_1.
- If $e_1 \in (u-1)\backslash\{0\}$, then $e_1 = (u-1)e_1{}'$ and $f_1 = (u-1)f_1'$, where $e_1' \in \mathbb{F}_q^*$, $f_1' \in \mathbb{F}_q$. Since $u^2 = u$, then $f_1 = (u-1)f_1' = (u-1)e_1'a_1 = (u-1)e_1'(a_1' + ua_1'') = (u-1)e_1'a_1' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1'$ and a_1'' is arbitrary in $\mathbb{F}_q$. There are q choices for a_1.
- If e_1=0, then a_1 is arbitrary in R, there are q^2 choices for a_1.

In the second constituent of C_a, we discuss on the unit character of e_2 as follows.

- If $e_2 \in \mathcal{R}^*$, there exists only one solution of a_2.
- If $e_2 \in (u)\backslash\{0\}$, then $e_2 = ue_2'$ and $f_2 = uf_2'$, where $e_2' \in \mathbb{F}_{q^{n-1}}^*$, $f_2' \in \mathbb{F}_{q^{n-1}}$. Since $u^2 = u$, then $f_2 = uf_2' = ue_2'a_2 = ue_2'(a_2' + ua_2'') = ue_2'a_2' + ue_2'a_2'' \Longleftrightarrow \frac{f_2'}{e_2'} = a_2' + a_2''$. There are q^{n-1} choices for a_2.
- If $e_2 \in (u-1)\backslash\{0\}$, then $e_2 = (u-1)e_2{}'$ and $f_2 = (u-1)f_2'$, where $e_2' \in \mathbb{F}_{q^{n-1}}^*$, $f_2' \in \mathbb{F}_{q^{n-1}}$. Since $u^2 = u$, then $f_2 = (u-1)f_2' = (u-1)e_2'a_2 = (u-1)e_2'(a_2' + ua_2'') = (u-1)e_2'a_2' \Longleftrightarrow \frac{f_2'}{e_2'} = a_2'$ and a_2'' is arbitrary in $\mathbb{F}_{q^{n-1}}$. There are q^{n-1} choices for a_2.
- If $e_2 = 0$, then $e \equiv 0 \mod h(x)$, then e is a constant vector, contradiction.

Thus, there are at most q^{n+1} generators $(1, a)$ such that $z \in C_a$. □

LEMMA 4.2. *If $z = (e, f) \in R^{2n}$ with e is not a constant vector, then there are at most $4(1 + q^{\frac{n-1}{2}})$ generators $(1, a)$ such that $z \in C_a$ and C_a is a self-dual double circulant code over R.*

Proof. Keep the same notations as Lemma 4.1. In the first constituent of C_a, there are at most 4 generators $(1, a_1)$ such that C_1 is self-dual double circulant code over R due to Theorem 3.1.

In the second constituent of C_a, let $a_2 = a_2' + ua_2''$, where a_2', $a_2'' \in \mathbb{F}_{q^{n-1}}$, we discuss on the unit character of e_2 as follows.

- If $e_2 \in \mathcal{R}^*$, then there exists a unique solution of $a_2 = \frac{f_2}{e_2}$.
- If $e_2 \in (u)\backslash\{0\}$, then $e_2 = ue_2'$, $f_2 = uf_2'$ and

$$f_2 = ua_2e_2' = u(a_2' + ua_2'')e_2' = u(a_2' + a_2'')e_2' \Longleftrightarrow a_2' + a_2'' = \frac{f_2'}{e_2'},$$

  where $e_2' \in \mathbb{F}_{q^{n-1}}^*$ and $f_2' \in \mathbb{F}_{q^{n-1}}$. Since C_a is a self-dual double circulant code, then $(1, a_2) \cdot (1, a_2) = 1 + a_2\overline{a_2} = 1 + a_2{a_2}^{q^{\frac{n-1}{2}}} = 0$. This is equivalent to

$$\begin{cases} a_2'{a_2'}^{q^{\frac{n-1}{2}}} = -1, \\ (a_2' + a_2'')({a_2'}^{q^{\frac{n-1}{2}}} + {a_2''}^{q^{\frac{n-1}{2}}}) = -1. \end{cases} \Longleftrightarrow \begin{cases} Norm(a_2') = -1, \\ Norm(a_2' + a_2'') = -1, \end{cases}$$

  where $Norm$ is a map from $\mathbb{F}_{q^{n-1}}$ to $\mathbb{F}_{q^{\frac{n-1}{2}}}$. So there are $q^{\frac{n-1}{2}}+1$ roots for $Norm(a_2') = -1$ and $q^{\frac{n-1}{2}} + 1$ roots for $Norm(a_2' + a_2'') = -1$. But a_2'' is determined by a_2', then there are at most $1 + q^{\frac{n-1}{2}}$ choices for a_2', hence for a_2.
- If $e_2 \in (u-1)\backslash\{0\}$, then $e_2 = (u-1)e_2'$ and $f_2 = (u-1)f_2'$, where $e_2' \in \mathbb{F}_{q^{n-1}}^*$ and $f_2' \in \mathbb{F}_{q^{n-1}}$, which implies that

$$f_2 = (u-1)a_2e_2' = (u-1)(a_2' + ua_2'')e_2' \Longleftrightarrow a_2' = \frac{f_2'}{e_2'}.$$

  Since C_a is a self-dual double circulant code, using the same procedure as above, we have

$$\begin{cases} Norm(a_2') = -1, \\ Norm(a_2' + a_2'') = -1. \end{cases}$$

  Hence, there are $1 + q^{\frac{n-1}{2}}$ choices for a_2 because $a_2' = \frac{f_2'}{e_2'}$ and $1 + q^{\frac{n-1}{2}}$ roots for a_2''.
- If $e_2 = 0$, then $e \equiv 0 \mod h(x)$, then e is a constant vector, contradiction.

So there are at most $4(1+q^{\frac{n-1}{2}})$ generators $(1, a)$ such that $z \in C_a$. The proof is done. □

In number theory, Artin's conjecture on primitive roots states that a given integer q which is neither a perfect square nor -1 is a primitive root modulo infinitely many primes l [15]. This was proved conditionally under the Generalized Riemann Hypothesis (GRH) by Hooley [8]. Hence we can get infinite families of double circulant codes $C(2n)$ over R where the analysis made for $x^n - 1$ with only two irreducible factors applies.

Recall the q-ary entropy function defined for $0 \leq t \leq \frac{q-1}{q}$ by

$$H_q(t) = \begin{cases} 0, & \text{if } \ t = 0, \\ t\log_q(q-1) - t\log_q(t) - (1-t)\log_q(1-t), & \text{if } \ 0 < t \leq \frac{q-1}{q}. \end{cases}$$

This quantity is instrumental in the estimation of the volume of high-dimensional Hamming balls when the base field is $\mathbb{F}_q$. The result we are using is that the volume of the Hamming ball of radius tn is asymptotically equivalent, up to subexponential terms, to $q^{nH_q(t)}$, when $0 < t < 1$, and n goes to infinity [9, Lemma 2.10.3]. The main result obtained in this paper is as follows.

THEOREM 4.3. *Let n be an odd prime, $n > q$, and q be a primitive root modulo n. The family of Gray images of self-dual double circulant codes over R of length $2n$, of relative distance δ, and rate $1/2$, satisfies $H_q(\delta) \geq \frac{1}{8}$. The family of Gray images of LCD double circulant codes over R of length $2n$, of relative distance δ, and rate $1/2$, satisfies $H_q(\delta) \geq \frac{1}{4}$. In particular, both families codes are good.*

Proof. Let Ω_n denote the size of the family. Thus, for $n \to \infty$, we have, by Theorem 3.1, $\Omega_n \sim 4q^{n-1}$ for self-dual double circulant codes, and by Theorem 3.2, $\Omega_n \sim q^{2n-2}$ for LCD double circulant codes. Assume we can prove that for n large enough $\Omega_n > \lambda_n B(d_n)$, where $B(r)$ denotes the number of vectors in R^{2n} with Hamming weight of their $\mathbb{F}_q$ image $< r$. Here $\lambda_n = 4(1 + q^{(n-1)/2})$ for self-dual codes, and $\lambda_n = q^{n+1}$ for LCD codes.

This would imply, by Lemmas 4.1 and 4.2, that there are codes of length $2n$ in the family with minimum Hamming distance of their $\mathbb{F}_q$ image $\geq d_n$. Denote by δ the relative distance of this family of q-ary codes.

If we take d_n the largest number satisfying $\Omega_n > \lambda_n B(d_n)$, and assume a growth of the form $d_n \sim 4\delta_0 n$, and thus $\Omega_n \sim \lambda_n B(d_n)$, for $n \to \infty$ then, using an entropic estimate for $B(d_n) \sim q^{4nH_q(\delta_0)}$ [9, Lemma 2.10.3] yields, with the said values of Ω_n and λ_n the estimate $H_q(\delta_0) = \frac{1}{8}$ for self-dual codes and $H_q(\delta_0) = \frac{1}{4}$ for LCD codes. The result follows by observing that, by the definition of δ, we have $\delta \geq \delta_0$. □

4.2 Distance Bound for Double Negacirculant Codes

4.2.1 Factorization of $x^n + 1$

In order to describe the factorization of $x^n + 1$ over R, where $n = 2^a$, we first recall the definition of **Dickson polynomials**. For $\alpha \in R$, we define the Dickson polynomial of

paramater α and degree n as

$$D_n(x,\alpha) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j}\binom{n-j}{j}(-\alpha)^j x^{n-2j}.$$

The complete factorization of $x^{2^n}+1$ over $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ is given in the following theorem [14].

THEOREM 4.4. *[14] Let $q \equiv 3$ (mod 4), where $q = 2^A m - 1, A \geq 2$ and m is an odd integer. Let $n \geq 2$,*

(a) if $n < A$, then $x^{2^n}+1$ is the product of 2^{n-1} irreducible trinomials over $\mathbb{F}_q$

$$x^{2^n}+1 = \prod_{\gamma \in \Gamma}(x^2+\gamma x+1),$$

where Γ is the set of all roots of $D_{2^{n-1}}(x,1)$.

(b) if $n \geq A$, then $x^{2^n}+1$ is the product of 2^{A-1} irreducible trinomials over $\mathbb{F}_q$

$$x^{2^n}+1 = \prod_{\delta \in \triangle}(x^{2^{n-A+1}}+\delta x^{2^{n-A}}-1),$$

where $\triangle$ is the set of all roots of $D_{2^{A-1}}(x,-1)$.

EXAMPLE 4.5. *If $q = 3$, i.e., $q \equiv 3$ (mod 4), then $q = 2^2 \cdot 1 - 1$. This implies $A = 2, m = 1$, and $D_2(x,-1) = 0$, i.e., $\triangle = \{1,2\}$. By Theorem 4.4*

$$x^{2^n}+1 = (x^{2^{n-1}}+x^{2^{n-2}}-1)(x^{2^{n-1}}+2x^{2^{n-2}}-1).$$

EXAMPLE 4.6. *If $q = 11$, i.e., $q \equiv 3$ (mod 4), then $q = 2^2 \cdot 3 - 1$. This implies $A = 2, m = 3$, and $D_2(x,-1) = 0$, i.e., $\triangle = \{3,8\}$. By Theorem 4.4*

$$x^{2^n}+1 = (x^{2^{n-1}}+3x^{2^{n-2}}-1)(x^{2^{n-1}}+8x^{2^{n-2}}-1).$$

EXAMPLE 4.7. *If $q = 7$, i.e., $q \equiv 3$ (mod 4), then $q = 2^3 \cdot 1 - 1$. This implies $A = 3, m = 1$, and $D_4(x,-1) = 0$, i.e., $\triangle = \{1,3,4,6\}$. By Theorem 4.4*

$$x^{2^n}+1 = (x^{2^{n-2}}+x^{2^{n-3}}-1)(x^{2^{n-2}}+3x^{2^{n-3}}-1)(x^{2^{n-2}}+4x^{2^{n-3}}-1)(x^{2^{n-2}}+6x^{2^{n-3}}-1).$$

Next, we need the analogous factorization theorem when $q \equiv 1 \pmod 4$ as follows.

THEOREM 4.8. *[2] Let $q \equiv 1$ (mod 4), where $q = 2^{A+1}m + 1, A \geq 1, m$ is an odd integer. Denote the set of all primitive 2^k-th roots of unity in $\mathbb{F}_q$ by U_k. If $n \geq 2$, then*

(a) if $n \leq A$, then $ord_{2^{n+1}}(q) = 1$, $x^{2^n} + 1$ is the product of 2^n linear factors over $\mathbb{F}_q$

$$x^{2^n} + 1 = \prod_{u \in U_{n+1}} (x + u).$$

(b) if $n \geq A+1$, then $ord_{2^{n+1}}(q) = 2^{n-A}$, $x^{2^n}+1$ is the product of 2^A irreducible binomials over $\mathbb{F}_q$ of degree 2^{n-A}

$$x^{2^n} + 1 = \prod_{u \in U_{A+1}} (x^{2^{n-A}} + u).$$

EXAMPLE 4.9. *If $q = 5$, i.e., $q \equiv 1 \ (mod\ 4)$, then $q = 2^2 \cdot 1 + 1$. This implies $A = 1, m = 1$, and $U_2 = \{2, 3\}$. By Theorem 4.8*

$$x^{2^n} + 1 = (x^{2^{n-1}} + 2)(x^{2^{n-1}} + 3).$$

EXAMPLE 4.10. *If $q = 13$, i.e., $q \equiv 1 \ (mod\ 4)$, then $q = 2^2 \cdot 3 + 1$. This implies $A = 1, m = 3$, and $U_2 = \{5, 8\}$. By Theorem 4.8*

$$x^{2^n} + 1 = (x^{2^{n-1}} + 5)(x^{2^{n-1}} + 8).$$

EXAMPLE 4.11. *If $q = 41$, i.e., $q \equiv 1 \ (mod\ 4)$, then $q = 2^3 \cdot 5 + 1$. This implies $A = 2, m = 5$, and $U_3 = \{3, 14, 27, 38\}$. By Theorem 4.8*

$$x^{2^n} + 1 = (x^{2^{n-2}} + 3)(x^{2^{n-2}} + 14)(x^{2^{n-2}} + 27)(x^{2^{n-2}} + 38).$$

Remark: There is an error in the case (b) of Theorem 4 in [1], i.e., "$x^{2^n} + 1 = \prod_{\gamma \in \triangle} (x^{n-A+1} + \delta x^{n-A} - 1)$" should be changed to "$x^{2^n} + 1 = \prod_{\gamma \in \triangle} (x^{2^{n-A+1}} + \delta x^{2^{n-A}} - 1)$". According to [14], there is another error of Theorem 6 in [1], "$q = 2^A m + 1, A \geq 2$" should be changed to "$q = 2^{A+1} m + 1, A \geq 1$".

So we can cast the factorization $x^n + 1$ over $\mathbb{F}_q$ into two or four irreducible polynomials by limiting the size of $\triangle$ and U in Theorems 4.4 and 4.8. This factorization carries over R because $\mathbb{F}_q$ is subring of R.

The polynomial $x^n + 1$ factors into two irreducible polynomials that are reciprocal of each other over R, this is the case if $q \equiv \pm 1 \pmod 4$, where $q = 2^2 m \pm 1, m$ odd, it happens if $q = 3, 5, 11, 13, 19, 27, 29, 37,$ etc. The polynomial $x^n + 1$ factors into four irreducible polynomials which are pairwise reciprocal of each other over R, this is the case if $q \equiv \pm 1 \pmod 4$, where $q = 2^3 m \pm 1, m$ odd, it happens if $q = 7, 23, 25, 41,$ etc.

4.2.2 Distance Bounds for Decomposition I and II

Decomposition I: If $x^n + 1 = h(x)h^*(x)$, where $h(x)$ and $h^*(x)$ are irreducible polynomials and reciprocal of each other, where $\deg(h(x)) = \frac{n}{2}$, then $R[x]/(h(x)) \simeq R[x]/(h^*(x)) \simeq$

$\mathbb{F}_{q^{\frac{n}{2}}} + u\mathbb{F}_{q^{\frac{n}{2}}}$. For convenience, $K_1 = R[x]/(h(x))$ and $K_2 = R[x]/(h^*(x))$. We have provided several examples of that situation, such as Examples 4.5, 4.6, 4.9 and 4.10.

LEMMA 4.12. *Let q be odd, n be a power of 2, x^n+1 with **Decomposition I**. If $z = (e, f) \in R^{2n}$ is a nonzero vector, then there are at most $q^{\frac{3n}{2}}$ generators $(1, a)$ such that $z \in C_a$ and C_a is a double negacirculant code over R.*

Proof. By the Chinese Remainder Theorem (CRT), $(e, f) = (e_1, f_1) \oplus (e_2, f_2)$. Since $(e, f) \in C_a$, then $f = ea$, $f_1 = e_1a_1$ and $f_2 = e_2a_2$, where e_1, f_1, $a_1 \in K_1$ and e_2, f_2, $a_2 \in K_2$. Let $a_1 = a_1' + ua_1''$, $a_2 = a_2' + ua_2''$, where a_1', a_1'', a_2', $a_2'' \in \mathbb{F}_{q^{\frac{n}{2}}}$.

In the first constituent of C_a, we discuss on the unit character of e_1 as follows.

- If $e_1 \in K_1^*$, there exists only one solution for $a_1 = \frac{f_1}{e_1}$.
- If $e_1 \in (u)\backslash\{0\}$, then $e_1 = ue_1'$ and $f_1 = uf_1'$, where $e_1' \in \mathbb{F}^*_{q^{\frac{n}{2}}}$, $f_1' \in \mathbb{F}_{q^{\frac{n}{2}}}$. Since $u^2 = u$, then $f_1 = uf_1' = ue_1'a_1 = ue_1'(a_1' + ua_1'') = ue_1'a_1' + ue_1'a_1'' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1' + a_1''$. There are $q^{\frac{n}{2}}$ choices for a_1.
- If $e_1 \in (u-1)\backslash\{0\}$, then $e_1 = (u-1)e_1{}'$ and $f_1 = (u-1)f_1'$, where $e_1' \in \mathbb{F}^*_{q^{\frac{n}{2}}}$, $f_1' \in \mathbb{F}_{q^{\frac{n}{2}}}$. Since $u^2 = u$, then $f_1 = (u-1)f_1' = (u-1)e_1'a_1 = (u-1)e_1'(a_1' + ua_1'') = (u-1)e_1'a_1' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1'$ and a_1'' is arbitrary in $\mathbb{F}_q$. There are $q^{\frac{n}{2}}$ choices for a_1.
- If $e_1 = 0$, then a_1 is arbitrary in K_1, there are q^n choices for a_1.

Using the same argument as above in the second constituent of C_a, there are also at most q^n choices for a_2. But if z is not zero, then e_1 and e_2 cannot both be zero. Hence there are only at most $q^{\frac{3n}{2}}$ generators $(1, a)$ such that $z \in C_a$. We have thus proved the lemma. □

LEMMA 4.13. *Let q be odd, n be a power of 2. Assume $x^n + 1$ satisfies decomposition I. If $z = (e, f) \in R^{2n}$ is a nonzero vector, then there are at most $q^{\frac{n}{2}}$ generators $(1, a)$ such that $z \in C_a$ and that C_a is self-dual double negacirculant code of length $2n$ over R.*

Proof. Keep the same notations as Lemma 4.12. Since C_a is a self-dual code, then $\langle (1, a_1), (1, a_2) \rangle = 1 + a_1a_2 = 0$. Clearly, a_1, a_2 are units and a_2 is determined by a_1. Since e_1 and e_2 can not both be zero, without loss of generality, we may assume $e_1 \neq 0$, then we just need to consider the first constituent of C_a by symmetry. Next, we discuss on the unit character of e_1 as follows.

- If $e_1 \in K_1^*$, there exists only one solution of $a_1 = \frac{f_1}{e_1}$.

- If $e_1 \in (u)\backslash\{0\}$, then $e_1 = ue_1'$ and $f_1 = uf_1'$, where $e_1' \in \mathbb{F}^*_{q^{\frac{n}{2}}}$ and $f_1' \in \mathbb{F}_{q^{\frac{n}{2}}}$. Since $u^2 = u$, then $f_1 = uf_1' = ue_1'a_1 = ue_1'(a_1' + ua_1'') = ue_1'a_1' + ue_1'a_1'' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1' + a_1''$. There are $q^{\frac{n}{2}}$ choices for a_1.

- If $e_1 \in (u-1)\backslash\{0\}$, then $e_1 = (u-1)e_1{}'$ and $f_1 = (u-1)f_1'$, where $e_1' \in \mathbb{F}^*_{q^{\frac{n}{2}}}$ and $f_1' \in \mathbb{F}_{q^{\frac{n}{2}}}$. Since $u^2 = u$, then $f_1 = (u-1)f_1' = (u-1)e_1'a_1 = (u-1)e_1'(a_1' + ua_1'') = (u-1)e_1'a_1' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1'$ and a_1'' is arbitrary in $\mathbb{F}_q$. There are $q^{\frac{n}{2}}$ choices for a_1.

Hence there are at most $q^{\frac{n}{2}}$ generators $(1, a)$ such that $z \in C_a$. We have thus proved the lemma. □

Decomposition II: If $x^n + 1 = u_1(x)u_1^*(x)u_2(x)u_2^*(x)$, where $u_1(x)$ (*resp.* $u_2(x)$) and $u_1^*(x)$ (*resp.* $u_2^*(x)$) are irreducible polynomials and reciprocal of each other, $\deg(u_i(x)) = q^{\frac{n}{4}}, i = \{1, 2\}$, then $R[x]/(u_1(x)) \simeq R[x]/(u_1^*(x)) \simeq R[x]/(u_2(x)) \simeq R[x]/(u_2^*(x)) \simeq \mathbb{F}_{q^{\frac{n}{4}}} + u\mathbb{F}_{q^{\frac{n}{4}}}$. For convenience, let $I_1 = R[x]/(u_1(x))$, $I_2 = R[x]/(u_1^*(x))$, $I_3 = R[x]/(u_2(x))$ and $I_4 = R[x]/(u_2^*(x))$. We have provided several examples of that situation, such as Examples 4.7 and 4.11.

LEMMA 4.14. *Let q be odd, n be a power of 2, and $x^n + 1$ satisfying Decomposition II . If $z = (e, f) \in R^{2n}$ is a nonzero vector, then there are at most $q^{\frac{7n}{4}}$ generators $(1, a)$ such that $z \in C_a$ and C_a is a double negacirculant code of length $2n$ over R.*

Proof. By the Chinese Remainder Theorem (CRT), $(e, f) = (e_1, f_1) \oplus (e_2, f_2) \oplus (e_3, f_3) \oplus (e_4, f_4)$. Since $(e, f) \in C_a$, then $f = ea$, $f_1 = e_1a_1$, $f_2 = e_2a_2$, $f_3 = e_3a_3$ and $f_4 = e_4a_4$, where e_1, f_1, $a_1 \in I_1$, e_2, f_2, $a_2 \in I_2$, e_3, f_3, $a_3 \in I_3$ and e_4, f_4, $a_4 \in I_4$.

In the first constituent of C_a, Let $a_1 = a_1' + ua_1''$, where a_1', $a_1'' \in \mathbb{F}_{q^{\frac{n}{4}}}$, we discuss on the unit character of e_1 as follows.

- If $e_1 \in I_1^*$, then there exists only one solution for a_1 that is $a_1 = \frac{f_1}{e_1}$.

- If $e_1 \in (u)\backslash\{0\}$, then $e_1 = ue_1'$ and $f_1 = uf_1'$, where $e_1' \in \mathbb{F}^*_{q^{\frac{n}{4}}}$ and $f_1' \in \mathbb{F}_{q^{\frac{n}{4}}}$. Since $u^2 = u$, then $f_1 = uf_1' = ue_1'a_1 = ue_1'(a_1' + ua_1'') = ue_1'a_1' + ue_1'a_1'' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1' + a_1''$. There are $q^{\frac{n}{4}}$ choices for a_1.

- If $e_1 \in (u-1)\backslash\{0\}$, then $e_1 = (u-1)e_1{}'$ and $f_1 = (u-1)f_1'$, where $e_1' \in \mathbb{F}^*_{q^{\frac{n}{4}}}$ and $f_1' \in \mathbb{F}_{q^{\frac{n}{4}}}$. Since $u^2 = u$, then $f_1 = (u-1)f_1' = (u-1)e_1'a_1 = (u-1)e_1'(a_1' + ua_1'') = (u-1)e_1'a_1' \Longleftrightarrow \frac{f_1'}{e_1'} = a_1'$, while a_1'' is arbitrary in $\mathbb{F}_q$. Thus there are $q^{\frac{n}{4}}$ choices for a_1.

- If $e_1 = 0$, then a_1 is arbitrary in I_1, there are $q^{\frac{n}{2}}$ choices for a_1.

Using the same argument as above in the three remaining constituents of C_a. There are also at most $q^{\frac{n}{2}}$ choices for a_i, where $i = 2, 3, 4$. But z is not zero, then e_1, e_2, e_3 and e_4 can not be zero at the same time. Hence there are at most $q^{\frac{3n}{2}} \times q^{\frac{n}{4}}$ generators $(1, a)$ such that $z \in C_a$. We have thus proved the lemma. □

LEMMA 4.15. *Let q be odd, n be a power of 2, and $x^n + 1$ satisfying Decomposition II. If $z = (e, f) \in R^{2n}$ is a nonzero vector, then there are at most $q^{\frac{3n}{4}}$ generators $(1, a)$ such that $z \in C_a$, and C_a is a self-dual double negacirculant code over R.*

Proof. Keep the same notations as Lemma 4.14. Since C_a is a self-dual code, we then have

$$\begin{cases} \langle (1, a_1), (1, a_2) \rangle = 0, \\ \langle (1, a_3), (1, a_4) \rangle = 0. \end{cases} \iff \begin{cases} 1 + a_1 a_2 = 0, \\ 1 + a_3 a_4 = 0. \end{cases}$$

So we just need to consider a_1 and a_3, because a_2 and a_4 are determined by a_1 and a_3, respectively. Since z is not zero, then we may assume $e_1 \neq 0$. Using a similar argument as in the proof of Lemma 4.13, we see that there are only at most $q^{\frac{n}{4}}$ choices for a_1 and $q^{\frac{n}{2}}$ choices for a_3. Hence, there are at most $q^{\frac{3n}{4}}$ generators such that $z \in C_a$. □

The following results can be proved by the same method as employed in the last subsection.

THEOREM 4.16. *Under the condition of the **Decomposition I** (resp. **Decomposition II**), if q is an odd prime power, and n is a power of 2, then the family of Gray images of self-dual double negacirculant codes over R of length $2n$, of relative distance δ, and rate $1/2$, satisfies $H_q(\delta) \geq \frac{1}{8}$ (resp. $H_q(\delta) \geq \frac{1}{16}$). In particular, these families of codes are good.*

Proof. The proof follows the method of the proof of Theorem 4.3 with $\Omega_n \sim q^n$ for both Decomposition I and Decomposition II, by Theorem 3.4 and $\lambda_n = q^{\frac{n}{2}}$ and $\lambda_n = q^{\frac{3n}{4}}$ by Lemmas 4.13 and 4.15, respectively. The details are omitted. □

THEOREM 4.17. *Under the condition of the **Decomposition I** (resp. **Decomposition II**), if q is an odd prime power, and n is a power of 2, then the family of Gray images of LCD double negacirculant codes over R of length $2n$, of relative distance δ, and rate $1/2$, satisfies $H_q(\delta) \geq \frac{1}{8}$ (resp. $H_q(\delta) \geq \frac{1}{16}$). In particular, these families of codes are good.*

Proof. The proof follows the method of the proof of Theorem 4.3 with $\Omega_n \sim q^{2n}$ for both Decomposition I and Decomposition II, by Theorem 3.4 and $\lambda_n = q^{\frac{3n}{2}}$ and $\lambda_n = q^{\frac{7n}{4}}$ by Lemmas 4.12 and 4.14, respectively. The details are omitted. □

Table 1: Gray image of LCD double circulant codes over $\mathbb{F}_5 + u\mathbb{F}_5$, *: optimal codes

n	$a_1(x)$	$a_2(x)$	**Parameters over $\mathbb{F}_5$**	**Distance [6]**
2	40	42	$[8, 4, 4]^*$	4
3	121	402	$[12, 6, 6]^*$	6
4	0334	3242	$[16, 8, 6]$	7
5	43030	04131	$[20, 10, 8]^*$	8
6	010044	132202	$[24, 12, 8]$	9
7	1402124	2113424	$[28, 14, 10]$	11
8	34430110	24023121	$[32, 16, 11]^*$	11
9	033302122	314321000	$[36, 18, 12]^*$	12

5 Numerical Examples

We need the following lemma, before doing any computation.

LEMMA 5.1. *If C has generator matrix $G = (I, A)$, with $A = A_1 + uA_2$, where A_1, A_2 are q-ary matrices of order n, and I denotes the identity matrix of order n, then $\phi(C)$ has generator matrix*

$$\begin{pmatrix} -I & I & -A_1 - A_2 & A_1 + A_2 \\ 0 & 2I & -A_2 & 2A_1 + A_2 \end{pmatrix}.$$

Proof. The first row of the first matrix is $\phi(uG)$, and its second row is $\phi(G)$. The matrix spans subsets of $\phi(C)$. Since the rank is $2n$, the result follows. □

In Table 1 and Table 2, we have provided some examples of LCD and self-dual double circulant codes respectively with the best parameters obtained by Magma search and Lemma 5.1. The coefficients of degree n polynomial $a_1(x)$ and $a_2(x)$ in $\mathbb{F}_5[x]$ are written in decreasing powers of x. For example for $n = 3$, the entry 311 means $3x^2 + x + 1$. The parameters over $\mathbb{F}_5$ are given in the form $[4n, 2n, d]$ where d is the minimum distance. The entry in the rightmost column is the best known distance of a $[4n, 2n]$ (self-dual) code over $\mathbb{F}_5$, obtained by looking up the tables in [6] and [19]. When the distance of the code constructed reaches that value the parameters are starred.

6 Conclusion and Open Problems

In this paper we have studied double circulant and double negacirculant codes over the ring $R = \mathbb{F}_q + u\mathbb{F}_q$. It might be worth looking at quasi-cyclic codes of higher index, or more

Table 2: Gray image of self-dual double circulant codes over $\mathbb{F}_5 + u\mathbb{F}_5$, *: optimal codes

n	$a_1(x)$	$a_2(x)$	**Parameters over $\mathbb{F}_5$**	**Distance [19]**
2	20	32	$[8, 4, 4]^*$	4
3	313	240	$[12, 6, 4]$	6
4	4144	2020	$[16, 8, 4]$	7
5	22314	12003	$[20, 10, 8]^*$	8
6	031243	032004	$[24, 12, 8]$	9
7	2220222	1214201	$[28, 14, 8]$	10
8	03310024	24022212	$[32, 16, 8]$	10
9	331421003	423002122	$[36, 18, 10]$	12

generally, at quasi-twisted codes of higher index. Four-circulant or four-negacirculant codes are natural candidates for this exploration [17].

While passing from fields to rings increases significantly the complexity of the proofs and calculations, it might still be worth looking at other polynomial rings with u having a minimal polynomial of higher degree, or defined by several variables.

References

[1] A. Alahmadi, C. G*ü*neri, B. *Ö*zkaya, H. Shoaib, P. Sol*é*, On self-dual double negacirculant codes, Discrete Applied Mathematics, **222**, pp. 205–212, 2017.

[2] A. Alahmadi, C. G*ü*neri, B. *Ö*zkaya, H. Shoaib, P. Sol*é*, On linear complementary-dual multinegacirculant codes, arXiv:1703.03115v1 [cs.IT], 2017.

[3] A. Alahmadi, F. Ozdemir, P. Sol*é*, On self-dual double circulant codes, Designs Codes & Cryptography, DOI `10.1007/s10623-017-0393-x`, 2017.

[4] S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, P. Solé, Type IV codes over rings, IEEE Transactions on Information Theory, **45**(7), pp. 2345–2360, 1999.

[5] S.T. Dougherty, J.L. Kim, B. Özkaya, L. Sok, P. Solé, The combinatorics of LCD codes: linear programming bound and orthogonal matrices, International Journal of Information and Coding Theory, **4**(2/3), pp. 116–128, 2017.

[6] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes." Online available at http://www.codetables.de.

[7] C. Güneri, B. Özkaya, P. Solé, Quasi-cyclic complementary dual codes, Finite Fields and Their Applications, **42**, pp. 67–80, 2016.

[8] C. Hooley, On Artin's conjecture, J. Reine Angew. Math, **225**, pp. 209–220, 1967.

[9] W.C. Huffman, V. Pless, *Fundamentals of error correcting codes*, Cambridge University Press, 2003.

[10] Y. Jia, On quasi-twisted codes over finite fields, Finite Fields and Their Applications, **18**, pp. 237–257, 2012.

[11] R. Lidl, H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

[12] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Transactions on Information Theory, **47**(7), pp. 2751–2760, 2001.

[13] S. Ling, P. Solé, On the Algebraic Structure of Quasi-cyclic Codes II: Chain Rings, Designs Codes & Cryptography, **30**(1), pp. 113–130, 2003.

[14] H. Meyn, Factorization of the cyclotomic polynomial $x^{2^n}+1$ over finite fields, Finite Fields and Their Applications, **2**, pp. 439–442, 1996.

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

[16] `http://magma.maths.usyd.edu.au/magma/`

[17] M.J. Shi, H.W. Zhu, P. Solé, On the self-dual four-circulant codes, International Journal on Foundations of Computer Science, to appear, `https://arxiv.org/pdf/1709.07548.pdf`, 2017.

[18] M.J. Shi, Y. Guan, P. Solé, Two new families of two-weight codes, IEEE Transactions on Information Theory, **63**(10), pp. 6240–6246, 2017.

[19] `www.unilim.fr/pages_perso/philippe.gaborit/SD/GF5/GF5.htm`

[20] S.X. Zhu, L. Wang, A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, Discrete Mathematics, **311**, pp. 2677–2682, 2011.