On self-dual and LCD quasi-twisted codes of index two over a special chain ring

Minjia Shi, Liqin Qian, Patrick Sole

Cryptography and Communications (2019) 11:717–734
https://doi.org/10.1007/s12095-018-0322-5

On self-dual and LCD quasi-twisted codes of index two over a special chain ring

Liqin Qian[2] · Minjia Shi[1,2] · Patrick Solé[3]

Received: 26 April 2018 / Accepted: 25 July 2018 / Published online: 13 August 2018

Abstract

Let q be a prime power, and let $\mathbb{F}_q$ denote the finite field of order q. Consider the chain ring $R_k = \mathbb{F}_q[u]/\langle u^k\rangle$ with $k \geq 1$ an integer. We study self-dual and LCD quasi-twisted codes of index two and twisting constant λ over R_k for the metric induced by the standard Gray map. Some special factorizations of $x^m - \lambda$ over R_k are studied. By random coding, we obtain four classes of asymptotically good self-dual λ-circulant codes and four classes of asymptotically good LCD λ-circulant codes over R_k.

Keywords Double circulant codes · Gray map · Self-dual codes · LCD codes · Quasi-twisted codes

Mathematics Subject Classification (2010) 94 B15 · 94 B25 · 05 E30

This research is supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

✉ Minjia Shi
smjwcl.good@163.com

Liqin Qian
qianliqin_1108@163.com

Patrick Solé
sole@enst.fr

[1] Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, Anhui University, No.3 Feixi Road, Hefei, Anhui, 230039, China

[2] School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China

[3] CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France

1 Introduction

Self-dual codes are important for a number of practical and theoretical reasons, as witnessed by [1, 3, 12]. Another important class of codes defined by their duality properties is that of Linear codes with Complementary Duals (LCD), which were introduced by Massey in 1992 for information theoretic reasons (see [18]). They have found applications recently in Boolean masking [6, 7]. Massey [18] shows that LCD codes are asymptotically good. LCD codes are universal: for $q > 3$ there is an algorithm that turns any linear code into an equivalent LCD code [5]. Still, it is of interest to find direct methods of construction of LCD codes as in [4]. One such method is to use quasi-cyclic and quasi-twisted codes. In that direction, self-dual double circulant (resp. double negacirculant) codes over finite fields have been studied recently in [1, 3], from the viewpoint of enumeration and asymptotic performance. Some classes of quasi-twisted codes have been studied over finite chain rings in [19]. In [2], A. Alahmadi et al. have studied the linear complementary-dual multinegacirculant codes. Motivated by the techniques in [1–3, 8, 19, 20], we use the Chinese Remainder Theorem (CRT) approach to quasi-twisted codes as introduced in [11, 13, 14]. In particular, we study two classes of self-dual (resp. LCD) negacirculant codes of index 2 over R_k. Combining with [19], we study two families of factorizations of $x^m - \lambda$ over R_k with m an odd prime, $\gcd(m, q) = 1$. When these special factorizations are thus enforced, we derive exact enumeration formulae, and obtain asymptotic lower bounds on the minimum Hamming distance of the Gray image of these codes.

The material is arranged as follows. In Section 2, we give some background materials on the ring R_k and study the case when the element -1 is a square in R_k. In Section 3, we derive the enumeration formulae of self-dual (resp. LCD) double circulant and double negacirculant codes of co-index m and we study the special factorizations of $x^m - \lambda$ with m an odd prime, and $\gcd(m, q) = 1$. Then, we also obtain the enumeration formulae of self-dual (resp. LCD) double λ-circulant codes. In Section 4, we derive a modified Varshamov-Gilbert bound on the relative distance of the codes considered, building on exact enumeration results. Finally, Section 5 contains conclusions and open problems.

2 Preliminaries

2.1 The ring $R_k = \mathbb{F}_q[u]/\langle u^k \rangle$

Let q be a prime power, and let $\mathbb{F}_q$ denote the finite field of order q. Consider the local ring $R_k = \mathbb{F}_q[u]/\langle u^k \rangle$ where $u^k = 0$ with unique maximal ideal $\langle u \rangle$. In double λ-circulant codes case, we will consider the chain ring $R_k = \mathbb{F}_q[u]/\langle u^k \rangle$ when it contains a square root of -1.

Theorem 2.1 *If $a_0 + ua_1 + \cdots + u^{k-1}a_{k-1} \in R_k = \mathbb{F}_q[u]/\langle u^k \rangle$ is a square root of -1 if and only if*

(1) *q is a power of 2, $a_0^2 = -1, a_1 = a_2 = \cdots = a_{\frac{k-2}{2}} = 0$, where $a_{\frac{k}{2}}, a_{\frac{k+2}{2}}, \cdots, a_{k-1} \in \mathbb{F}_q$ when k is even; $a_0^2 = -1, a_1 = a_2 = \cdots = a_{\frac{k-1}{2}} = 0, a_{\frac{k+1}{2}}, a_{\frac{k+2}{2}}, \cdots, a_{k-1} \in \mathbb{F}_q$, when k is odd; or*

(2) *$q = p^{\kappa}$ where $p \equiv 1 (mod\ 4)$ or $q = p^{2\kappa}$ where $p \equiv 3 (mod\ 4)$, $a_0^2 = -1, a_1 = a_2 = \cdots = a_{k-1} = 0$.*

Proof Note that the condition is obviously sufficient. To prove its necessity, when q is a power of 2, we have $(a_0 + a_1u + \cdots + a_{k-1}u^{k-1})^2 = a_0^2 + a_1^2u^2 + \cdots + a_{k-1}^2u^{2(k-1)} = -1$,when k is even, $a_0^2 = -1, a_1 = a_2 = \cdots = a_{\frac{k-2}{2}} = 0, a_{\frac{k}{2}}, a_{\frac{k+2}{2}}, \cdots, a_{k-1} \in \mathbb{F}_q$; when k is odd, $a_0^2 = -1, a_1 = a_2 = \cdots = a_{\frac{k-1}{2}} = 0, a_{\frac{k+1}{2}}, a_{\frac{k+2}{2}}, \cdots, a_{k-1} \in \mathbb{F}_q$. When q is a power of an odd prime, we have $(a_0 + a_1u + \cdots + a_{k-1}u^{k-1})^2 = a_0^2 + 2a_0a_1u + (2a_0a_2 + a_1^2)u^2 + \cdots + (a_0a_{k-1} + a_1a_{k-2} + \cdots + a_{k-1}a_0)u^{k-1} = -1$,where $a_i \in \mathbb{F}_q, 0 \le i \le k-1$. Then we get $a_0^2 = -1, a_1 = a_2 = \cdots = a_{k-1} = 0$. Thus a_0 is a square root of -1 over $\mathbb{F}_q$ if and only if $q \equiv 1 (\mathrm{mod}\ 4)$. □

2.2 Codes

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

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i,$$

and their Hermitian scalar inner product is defined by

$$\langle x, y\rangle_H = \sum_{i=1}^{n} x_i \bar{y}_i,$$

where the operation is performed in R_k. For all $z = z_0 + uz_1 + \cdots + u^{k-1}z_{k-1} \in \mathbb{F}_{q^{2Q}} + u\mathbb{F}_{q^{2Q}} + \cdots + u^{k-1}\mathbb{F}_{q^{2Q}}$, the conjugation of z over $\mathbb{F}_{q^{2Q}} + u\mathbb{F}_{q^{2Q}} + \cdots + u^{k-1}\mathbb{F}_{q^{2Q}}$ is $\overline{z} = z_0^{q^Q} + uz_1^{q^Q} + \cdots + u^{k-1}z_{k-1}^{q^Q}$, where Q is a positive integer. The Euclidean (resp. Hermitian) dual code of C is denoted by $C^{\perp}$ (resp. $C^{\perp_H}$) and defined as $C^{\perp} = \{y \in R_k^n \mid \langle x, y\rangle = 0, \forall x \in C\}$ (resp. $C^{\perp_H} = \{y \in R_k^n \mid \langle x, y\rangle_H = 0, \forall x \in C\}$).

A linear code C of length n over R_k is called a **self-dual code** (**resp. Hermitian self-dual code**) if $C = C^{\perp}$ (resp. $C = C^{\perp_H}$). A linear code C of length n over R_k is called a **linear code with complementary dual (LCD)** if $C \bigcap C^{\perp} = \{0\}$ or $C \bigcap C^{\perp_H} = \{0\}$.

A matrix A over R_k is said to be λ**-circulant** if its rows are obtained by successive λ-shifts from the first row. In this paper, we consider double λ-circulant codes over R_k, that is $[2m, m]$ codes with generator matrices $G = (I, A)$ with A an $m \times m$ λ-circulant matrix, we can view such a code as an R_k-module in R_k^2, generated by $(1, h)$ with the first row of A being the x-expansion of h in the ring $\frac{R_k[x]}{\langle x^m - \lambda\rangle}$.

If $C(m)$ is a family of codes with parameters $[m, k_m, d_m]$ over $\mathbb{F}_q$, the rate ρ and relative distance δ are defined as $\rho = \limsup\limits_{m\to\infty} \frac{k_m}{m}$ and $\delta = \liminf\limits_{m\to\infty} \frac{d_m}{m}$, respectively. A family of codes is **good** if $\rho\delta > 0$.

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 [16]. This was proved conditionally under the Generalized Riemann Hypothesis (GRH) by Hooley [9]. Hence, we can get infinite families of double λ-circulant codes $C(m)$ over R_k where the analysis is made for $x^m - 1$ with a special factorization.

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

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

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 $\tilde{t}m$ is asymptotically equivalent, up to subexponential terms, to $q^{mH_q(\tilde{t})}$, when $0 < \tilde{t} < 1$, and m goes to infinity [10, Lemma 2.10.3].

2.3 Gray map

Any integer z can be written uniquely in base p as $z = p_0(z) + pp_1(z) + p^2 p_2(z) + \cdots$, where $0 \le p_i(z) \le p-1, i = 0, 1, 2, \ldots$. The **Gray map** $\Phi : R \to \mathbb{F}_p^{p^{k-1}}$ is defined as follows:

$$\Phi(a) = (b_0, b_1, b_2, \ldots, b_{p^{k-1}-1}),$$

where $a = a_0 + a_1 u + \cdots + a_{k-1}u^{k-1}$. Then for all $0 \le i \le p^{k-2} - 1, 0 \le \tau \le p-1$,we have

$$b_{ip+\tau} = \begin{cases} a_{k-1} + \sum\limits_{l=1}^{k-2} p_{l-1}(i)a_l + \tau a_0, & \text{if } k \ge 3, \\ a_1 + \tau a_0, & \text{if } k = 2. \end{cases}$$

Note that, more generally, Gray maps have been defined at the level of finite chain rings in [15, 23], linking codes over rings to codes over finite fields. For instance, when $p = k = 2$, it is easy to check that the Gray map adopted in the trace codes of [21] is the same as the Gray map defined here. As an additional example, when $p = k = 3$, write $\Phi(a_0 + a_1 u + a_2 u^2) = (b_0, b_1, b_2, \cdots, b_8)$. According to the definition above, we have $0 \le i \le 2, 0 \le \tau \le 2$ and $\sum\limits_{l=1}^{k-2} p_{l-1}(i)a_l = p_0(i)a_1 = ia_1$. Then we get

$$b_0 = a_2, b_1 = a_2 + a_0, b_2 = a_2 + 2a_0, b_3 = a_2 + a_1, b_4 = a_2 + a_1 + a_0,$$

$$b_5 = a_2 + a_1 + 2a_0, b_6 = a_2 + 2a_1, b_7 = a_2 + 2a_1 + a_0, b_8 = a_2 + 2a_1 + 2a_0.$$

It is easy to extend the Gray map from R_k^m to $\mathbb{F}_p^{p^{k-1}m}$, and we also know from [22] that Φ is injective and linear.

3 Algebraic structure of λ-circulant codes of index two

In this section, we study the exact enumeration of the double self-dual and LCD λ-circulant codes over R_k.

3.1 Double circulant codes (λ = 1)

In this subsection, we assume m is an odd integer and $\gcd(m, q) = 1$. We can cast the factorization of $x^m - 1$ into distinct basic irreducible polynomials over $R_k = \mathbb{F}_q[u]/\langle u^k \rangle$ in the form

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

where δ is a unit in R_k, the polynomial $g_i(x)$ is self-reciprocal of degree $2e_i$ for $2 \le i \le s$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ with degree d_j for $1 \le j \le t$. By the Chinese Remainder Theorem (CRT), we have

$$\begin{aligned}\frac{R_k[x]}{\langle x^m-1\rangle} &\simeq \frac{R_k[x]}{\langle x-1\rangle} \oplus \left(\bigoplus_{i=2}^{s} R_k[x]/\langle g_i(x)\rangle\right) \oplus \left(\bigoplus_{j=1}^{t}\Big(R_k[x]/\langle h_j(x)\rangle \oplus R_k[x]/\langle h_j^*(x)\rangle\Big)\right)\\ &\simeq \frac{\mathbb{F}_q[u,x]}{\langle u^k, x-1\rangle} \oplus \left(\bigoplus_{i=2}^{s} \frac{\mathbb{F}_q[u,x]}{\langle u^k, g_i(x)\rangle}\right) \oplus \left(\bigoplus_{j=1}^{t}\left(\frac{\mathbb{F}_q[u,x]}{\langle u^k, h_j(x)\rangle} \oplus \frac{\mathbb{F}_q[u,x]}{\langle u^k, h_j^*(x)\rangle}\right)\right)\\ &\simeq R_k \oplus \left(\bigoplus_{i=2}^{s}(\mathbb{F}_{q^{2e_i}} + u\mathbb{F}_{q^{2e_i}} + \cdots + u^{k-1}\mathbb{F}_{q^{2e_i}})\right) \oplus \left(\bigoplus_{j=1}^{t}\Big(\big(\mathbb{F}_{q^{d_j}} + u\mathbb{F}_{q^{d_j}} + \cdots\right.\\ &\qquad \left. + u^{k-1}\mathbb{F}_{q^{d_j}}\big) \oplus (\mathbb{F}_{q^{d_j}} + u\mathbb{F}_{q^{d_j}} + \cdots + u^{k-1}\mathbb{F}_{q^{d_j}})\Big)\right)\\ &:= R_k \oplus \left(\bigoplus_{i=2}^{s} R_{k(2e_i)}\right) \oplus \left(\bigoplus_{j=1}^{t}(R_{k(d_j)} \oplus R_{k(d_j)})\right).\end{aligned}$$

Note that all of these rings are extensions of R_k. This decomposition naturally extends to $(\frac{R_k[x]}{\langle x^m-1\rangle})^2$ as

$$\left(\frac{R_k[x]}{\langle x^m-1\rangle}\right)^2 \simeq R_k \oplus \left(\bigoplus_{i=2}^{s} R_{k(2e_i)}^2\right) \oplus \left(\bigoplus_{j=1}^{t}\Big(R_{k(d_j)}^2 \oplus R_{k(d_j)}^2\Big)\right).$$

In particular, each linear code C of length 2 over $\frac{R_k[x]}{\langle x^m-1\rangle}$ 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_k of length 2, C_i is a linear code over $R_{k(2e_i)}$ of length 2 for each $2 \le i \le s$, and C_j' and C_j'' are linear codes over $R_{k(d_j)}$ of length 2 for each $1 \le j \le t$, which are called the constituents of C.

Lemma 3.1 *Keep the same notations as above, then*

(1) *C_1 is LCD if and only if $1 + r^2 \in R_k^\times$ with $C_1 = \langle(1, r)\rangle$;*
(2) *C_i is LCD if and only if $1 + \eta\bar{\eta} \in R_{k(2e_i)}^\times$ with $C_i = \langle(1, \eta)\rangle$;*
(3) *$C_j' \oplus C_j''$ are LCD if and only if $1 + \eta'\eta'' \in R_{k(d_j)}^\times$ with $C_j' = \langle(1, \eta')\rangle$ and $C_j'' = \langle(1, \eta'')\rangle$.*

Proof (1) " $\Longrightarrow$ " If C_1 is LCD, suppose $1 + r^2 \notin R_k^\times$, then $1 + r^2 \in \langle u\rangle$. We have $u^{k-1}(1 + r^2) = 0$,i.e., $\langle u^{k-1}(1, r), (1, r)\rangle = 0$,then $u^{k-1}(1, r) \in C_1^\perp$,which implies $u^{k-1}(1, r) \in C_1 \cap C_1^\perp$, a contradiction.

"$\Longleftarrow$" If $1+r^2 \in R_k^\times$, assume C_1 is not LCD, then $C_1 \cap C_1^\perp \neq \{0\}$. Hence, there exists $r' \in R_k^\times$ such that $r'(1,r) \in C_1 \cap C_1^\perp$, then $\langle r'(1,r),(1,r)\rangle = r'(1+r^2) = 0$,since $1+r^2 \in R_k^\times$, then $r'=0$, a contradiction.

(2) "$\Longrightarrow$" If C_i is LCD, suppose $1+\eta\bar{\eta} \notin R_{k(2e_i)}^\times$, then $1+\eta\bar{\eta} \in \langle u\rangle$. We have $u^{k-1}(1+\eta\bar{\eta}) = 0$,i.e., $\langle u^{k-1}(1,\eta),(1,\eta)\rangle_H = 0$,then $u^{k-1}(1,\eta) \in C_i^{\perp_H}$,which implies $u^{k-1}(1,\eta) \in C_i \cap C_i^{\perp_H}$, a contradiction.

"$\Longleftarrow$" If $1+\eta\bar{\eta} \in R_{k(2e_i)}^\times$, assume C_i is not LCD, then $C_i \cap C_i^{\perp_H} \neq \{0\}$. If $\eta \in R_{k(2e_i)}^\times$,then $C_i^{\perp_H} = \langle(1,-\frac{1}{\bar{\eta}})\rangle$,there exist $k_1,k_2 \in R_{k(2e_i)}^\times$ such that $k_1(1,\eta) = k_2(1,-\frac{1}{\bar{\eta}})$,i.e., $k_1(1+\eta\bar{\eta}) = 0$. And $1+\eta\bar{\eta} \in R_{k(2e_i)}^\times$, then $k_1 = 0$, a contradiction. If $\eta \in \langle u\rangle$,we can let $\eta = ua_1 + u^2a_2 + \cdots + u^{k-1}a_{k-1}$, $a_i \in \mathbb{F}_{q^{2e_i}}$, $0 \le i \le k-1$,then the generator matrix of $C_i^{\perp_H}$ is of the form

$$\begin{pmatrix} -(u\bar{a}_1 + u^2\bar{a}_2 + \cdots + u^{k-1}\bar{a}_{k-1}) & 1 \\ 0 & u^{k-1}k_3 \end{pmatrix},$$

where $k_3 \in \mathbb{F}_{q^{2e_i}}$. Thus, there exist $k_4,k_5,k_6 \in R_{k(2e_i)}^\times$ such that $k_4(1, ua_1+u^2a_2+\cdots+u^{k-1}a_{k-1}) = k_5(-(u\bar{a}_1+u^2\bar{a}_2+\cdots+u^{k-1}\bar{a}_{k-1}),1) + k_6(0,u^{k-1}k_3)$,we then obtain

$$\begin{cases} k_4 = -(u\bar{a}_1 + u^2\bar{a}_2 + \cdots + u^{k-1}\bar{a}_{k-1})k_5, \\ (ua_1 + u^2a_2 + \cdots + u^{k-1}a_{k-1})k_4 = k_5 + u^{k-1}k_3k_6, \end{cases} \tag{2}$$

by (2), we get $k_4 \in R_{k(2e_i)}^\times$,but $-(u\bar{a}_1 + u^2\bar{a}_2 + \cdots + u^{k-1}\bar{a}_{k-1})k_5 \in \langle u\rangle$, a contradiction.

(3) "$\Longrightarrow$" If $C_j' \oplus C_j''$ is LCD, assume $1+\eta'\eta'' \notin R_{k(d_j)}^\times$, then $1+\eta'\eta'' \in \langle u\rangle$. We have $u^{k-1}(1+\eta'\eta'') = 0$,i.e., $\langle u^{k-1}(1,\eta'),(1,\eta'')\rangle = 0$,then $u^{k-1}(1,\eta') \in C_j''^\perp$ (or $u^{k-1}(1,\eta'') \in C_j'^\perp$), which implies $u^{k-1}(1,\eta') \in C_j' \cap C_j''^\perp$ (or $u^{k-1}(1,\eta'') \in C_j'' \cap C_j'^\perp$), a contradiction.

"$\Longleftarrow$" If $1+\eta'\eta'' \in R_{k(d_j)}^\times$, assume $C_j' \oplus C_j''$ is not LCD, then

$$\begin{cases} C_j' \cap C_j''^\perp \neq \{0\}, \\ C_j'' \cap C_j'^\perp \neq \{0\}. \end{cases}$$

If $C_j' \cap C_j''^\perp \neq \{0\}$, then there exists $k' \in R_{k(d_j)}^\times$ such that $k'(1,\eta') \in C_j' \cap C_j''^\perp$,i.e., $\langle k'(1,\eta'),(1,\eta'')\rangle = k'(1+\eta'\eta'') = 0$, a contradiction. □

Theorem 3.2 *Let m denote a positive odd integer, and q a prime coprime with m. If $x^m - 1$ can be factored into irreducible polynomials over R_k as in* (1)*, where $m = 1 + \sum_{i=2}^{s} 2e_i + 2\sum_{j=1}^{t} d_j$. Then*

(1) *the total number of self-dual double circulant codes over R_k is*

$$B\prod_{i=2}^{s}(q^{e_i}+1)q^{e_i(k-1)}\prod_{j=1}^{t}(q^{d_j}-1)q^{d_j(k-1)}, \textit{where}$$

1) *when q is a power of 2, $B = 2q^{\frac{k}{2}}$, k is even, or $B = 2q^{\frac{k-1}{2}}$, k is odd;*

2) *when q is a power of odd prime, $B = 2$.*

(2) *the total number of LCD double circulant codes over R_k is*

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

Proof (1) We can count the number of self-dual double circulant codes by counting their constituent codes.

Let $(1, r)$ be the generator of the self-dual code C_1 over R_k. By Theorem 2.1, when q is a power of 2, the number of r is equal to $2q^{\frac{k}{2}}$, where k is even ($2q^{\frac{k-1}{2}}$,where k is odd); when q is a power of odd prime, the number of choices for r is equal to 2.

Let $(1, c_{e_i})$ be the generators of Hermitian self-dual codes C_i over $R_{k(2e_i)}$, $2 \le i \le s$, then $\langle(1, c_{e_i}), (1, c_{e_i})\rangle_H = 1 + c_{e_i}\overline{c}_{e_i} = 0$. Let $c_{e_i} = c_0 + uc_1 + \cdots + u^{k-1}c_{k-1}$, where $c_\ell \in \mathbb{F}_{q^{2e_i}}$, $0 \le \ell \le k-1$, we then have

$$\begin{cases} c_0c_0^{q^{e_i}} = -1, \\ c_0c_1^{q^{e_i}} + c_1c_0^{q^{e_i}} = 0, \\ c_0c_2^{q^{e_i}} + c_1c_1^{q^{e_i}} + c_2c_0^{q^{e_i}} = 0, \\ c_0c_3^{q^{e_i}} + c_1c_2^{q^{e_i}} + c_2c_1^{q^{e_i}} + c_3c_0^{q^{e_i}} = 0, \\ c_0c_4^{q^{e_i}} + c_1c_3^{q^{e_i}} + c_2c_2^{q^{e_i}} + c_3c_1^{q^{e_i}} + c_4c_0^{q^{e_i}} = 0, \\ \vdots \\ c_0c_{k-1}^{q^{e_i}} + c_1c_{k-2}^{q^{e_i}} + \cdots + c_{k-1}c_0^{q^{e_i}} = 0. \end{cases} \tag{3}$$

$$\Longleftrightarrow \begin{cases} Norm(c_0) = -1, \\ Tr(c_0c_1^{q^{e_i}}) = 0, \\ Tr(c_0c_2^{q^{e_i}}) + Norm(c_1) = 0, \\ Tr(c_0c_3^{q^{e_i}}) + Tr(c_1c_2^{q^{e_i}}) = 0, \\ Tr(c_0c_4^{q^{e_i}}) + Tr(c_1c_3^{q^{e_i}}) + Norm(c_2) = 0, \\ \vdots \\ Tr(c_0c_{k-1}^{q^{e_i}}) + Tr(c_1c_{k-2}^{q^{e_i}}) + \cdots + Tr(c_{\frac{k-2}{2}}c_{\frac{k}{2}}) = 0, \text{ when } k \text{ is even, or} \\ Tr(c_0c_{k-1}^{q^{e_i}}) + Tr(c_1c_{k-2}^{q^{e_i}}) + \cdots + Tr(c_{\frac{k-3}{2}}c_{\frac{k+1}{2}}) + Norm(c_{\frac{k-1}{2}}) = 0, \text{ when } k \text{ is odd,} \end{cases}$$

where the $Norm()$ and $Tr()$ are maps norm and trace from $\mathbb{F}_{q^{2e_i}}$ to $\mathbb{F}_{q^{e_i}}$. So there are $q^{e_i} + 1$ roots for $Norm(c_0) = -1$ and q^{e_i} choices for c_i for $1 \le \ell \le k-1$. Clearly, the number of solutions of (3) is equal to $(q^{e_i} + 1)q^{e_i(k-1)}$.

As for reciprocal pairs, note that a pair $(h_j(x), h_j^*(x))$ both of degree d_j leads to counting dual pairs of codes (for the Euclidean inner product) of length 2 over $R_{k(d_j)}$, that is to count the number of solutions of $1 + c'_{d_j}c''_{d_j} = 0$, where $(1, c'_{d_j})$ and $(1, c''_{d_j})$ are the generators of C'_j and C''_j, respectively. If $c'_{d_j} \in R^\times_{k(d_j)}$, then $c''_{d_j} = -\frac{1}{c'_{d_j}}$, there are $|R^\times_{k(d_j)}| = (q^{d_j} - 1)q^{d_j(k-1)}$ choices for (c'_{d_j}, c''_{d_j}). If $c'_{d_j} \in R_{k(d_j)} \backslash R^\times_{k(d_j)}$, then $c'_{d_j} = ux_1 + u^2x_2 + \cdots + u^{k-1}x_{k-1} \in \langle u\rangle$. In this case, $1 + c'_{d_j}c''_{d_j} = 0$, which is impossible.

(2) The code C_1 is an LCD code, by Lemma 3.1 (1), we can get $1 + r^2 \in R_k^\times$. Let $r = r_0+ur_1+\cdots+u^{k-1}r_{k-1} \in R_k$,then $1+r^2 = 1+(r_0+ur_1+u^2r_2+\cdots+u^{k-1}r_{k-1})^2 =$

$1+r_0^2+2r_0r_1u+(2r_0r_2+r_1^2)u^2+\cdots+(r_0r_{k-1}+r_1r_{k-2}+\cdots+r_{k-1}r_0)u^{k-1} \in R_k^\times$. Hence, the number of r is equal to $(q-2)q^{k-1}$.

The code C_i is an LCD code, by Lemma 3.1 (2), we can get $1+\eta\bar{\eta} \in R^\times_{k(2e_i)}$. Let $\eta = \eta_0+u\eta_1+\cdots+u^{k-1}\eta_{k-1}$, then $1+\eta\bar{\eta} = 1+(\eta_0+u\eta_1+\cdots+u^{k-1}\eta_{k-1})(\eta_0^{q^{e_i}} + u\eta_1^{q^{e_i}} +\cdots+u^{k-1}\eta_{k-1}^{q^{e_i}}) = 1+\eta_0^{q^{e_i}+1} + u(\eta_0\eta_1^{q^{e_i}} + \eta_1\eta_0^{q^{e_i}}) + \cdots + u^{k-1}(\eta_0\eta_{k-1}^{q^{e_i}} + \eta_1\eta_{k-2}^{q^{e_i}} + \cdots + \eta_{k-1}\eta_0^{q^{e_i}}) \in R^\times_{k(2e_i)}$. Hence, the number of η is equal to $(q^{2e_i}-(q^{e_i}+1))q^{2(k-1)e_i}$.

Next, we count the number of LCD double circulant codes of length 2 over $R_{k(d_j)}$ for the pairs $h_j(x)$ and $h_j^*(x)$ with $\deg(h_j(x)) = \deg(h_j^*(x)) = d_j$. By Lemma 3.1 (3), we then get

$$\begin{cases} C'_j \bigcap C''^{\perp}_j = \{0\}, \\ C''_j \bigcap C'^{\perp}_j = \{0\}. \end{cases} \Longleftrightarrow 1+\eta'\eta'' \in R^\times_{k(d_j)}.$$

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

1) If $\eta' \in R^\times_{k(d_j)}$, then $\eta'' \in -\frac{1}{\eta'}+R^\times_{k(d_j)}$ and $|\frac{-1}{\eta'}+R^\times_{k(d_j)}| = |R^\times_{k(d_j)}| = q^{(k-1)d_j}(q^{d_j}-1)$. Hence, there are $|R^\times_{k(d_j)}|^2 = q^{2(k-1)d_j}(q^{d_j}-1)^2$ choices for (η',η'').
2) If $\eta' \in R_{k(d_j)}\backslash\{R^\times_{k(d_j)}\cup\{0\}\}$, let $\eta'' = \eta''_0+u\eta''_1+\cdots+u^{k-1}\eta''_{k-1}$, then $\eta' = u\eta'_1+u^2\eta'_2+\cdots+u^{k-1}\eta'_{k-1}$, where η'_{ℓ_1} can't be all zero, $1\le \ell_1 \le k-1$, $\eta''_{\ell_2} \in \mathbb{F}_{q^{d_j}}$, $0\le \ell_2\le k-1$. We then have $1+\eta'\eta'' = 1+u\eta'_1\eta''_0+u^2(\eta'_1\eta''_1+\eta'_2\eta''_0)+\cdots+u^{k-1}(\eta'_1\eta''_{k-2}+\eta'_2\eta''_{k-3}+\cdots+\eta'_{k-1}\eta''_0) \in R^\times_{k(d_j)}$. Thus, there are $(q^{(k-1)d_j}-1)q^{kd_j}$ choices for (η',η'').
3) If $\eta'=0$, then $\eta'' \in R_{k(d_j)}$, thus there are q^{kd_j} choices for η''.

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

3.2 Double negacirculant codes ($\lambda = -1$)

In this subsection, assume m is an even integer and $\gcd(m,q)=1$, where q is a prime power. We can cast the factorization of x^m+1 into distinct basic irreducible polynomials over R_k as follows.

$$x^m+1 = \epsilon\prod_{i=1}^{s} g_i(x)\prod_{j=1}^{t} h_j(x)h_j^*(x), \tag{4}$$

where $\epsilon \in R_k^\times$, $g_i(x) = g_i^*(x)$ with $\deg(g_i(x)) = 2e_i$, $1\le i\le s$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ with $\deg(h_j(x)) = \deg(h_j^*(x)) = d_j$, $1\le j\le t$. Using the same notations and argument as in Subsection 3.1, we can easily carry out the result as follows:

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

and

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

Theorem 3.3 *Let m denote a positive even integer, and q a prime power coprime with m. The factorization of x^m+1 over R_k is of the form (4) with $m=\sum_{i=1}^{s}2e_i+2\sum_{j=1}^{t}d_j$. Then*

(1) *the total number of self-dual double negacirculant codes over R_k is*

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

(2) *the total number of LCD double negacirculant codes over R_k is*

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

Proof This proof is similar to that of Theorem 3.2, so we omitted it here. □

Now, we consider a special factorization of x^m+1, where m is a power of 2, q is an odd prime. According to [17, Theorem 1] and [2, Theorems 5.1,5.3], we know that x^m+1 can be factored into two (resp. four) basic irreducible polynomials, which are reciprocal of each other over R_k, by limiting the size of $\triangle$ and U, because $\mathbb{F}_q$ is a subring of R_k. We can get the following lemma.

Lemma 3.4 *Let m be a power of 2, $q\equiv\pm1(mod\,4)$.*

(1) *If $q=2^2e\pm1$, e is odd, then x^m+1 factors into two basic irreducible polynomials over R_k as follows.*

$$x^m+1=h(x)h^*(x)$$

with $deg(h(x))=deg(h^*(x))=\frac{m}{2}$. In this case, the number of self-dual (resp. LCD) double negacirculant codes over R_k is

$$(q^{\frac{m}{2}}-1)q^{\frac{m(k-1)}{2}}(resp.q^{km}-q^{m(k-1)}(q^{\frac{m}{2}}-1))).$$

(2) *If $q=2^3e\pm1$, e is odd, then x^m+1 factors into four basic irreducible polynomials over R_k as follows.*

$$x^m+1=h_1(x)h_1^*(x)h_2(x)h_2^*(x) \tag{5}$$

with $deg(h_1(x))=deg(h_1^*(x))=deg(h_2(x))=deg(h_2^*(x))=\frac{m}{4}$. In this case, the number of self-dual (resp. LCD) double negacirculant codes over R_k is

$$(q^{\frac{m}{4}}-1)^2q^{\frac{m(k-1)}{2}}(resp.(q^{\frac{km}{2}}-q^{\frac{m(k-1)}{2}}(q^{\frac{m}{4}}-1))^2).$$

3.3 Quasi-twisted codes of index two ($\lambda=1+\omega u^t$)

In this subsection, we focus on the case $(1+\omega u^t)=(1+\omega u^t)^{-1}=(1-\omega u^t)$. According to [19], $x^m-(1+\omega u^t)$ can be uniquely expressed as

$$x^m-(1+\omega u^t)=\varsigma g_1(x)\prod_{i=2}^{s}g_i(x)\prod_{j=1}^{t}h_j(x)h_j^*(x), \tag{6}$$

where m is an odd, then $g_1(x)=x-(1+\omega u^t)$, $\varsigma\in R_k^\times$, $g_i(x)=g_i^*(x)$ with $\deg(g_i(x))=2e_i$, $2\le i\le s$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ with $\deg(h_j(x))=\deg(h_j^*(x))=d_j$, $1\le j\le t$.

In fact, we notice that a $(1+\omega u^{\mathrm{t}})$-QT code over R_k is self-dual only if $1+\omega u^{\mathrm{t}} = 1-\omega u^{\mathrm{t}}$, i.e., $2\omega u^{\mathrm{t}} = 0 \Longrightarrow \mathrm{char}(R_k) = 2$ over R_k.

Conjecture 3.5 Assume that m is an odd prime and $\gcd(m, q) = 1$, where q is a prime power. Let $\alpha \mid (m-1)$ and $\mathrm{ord}_m(q) = \frac{m-1}{\alpha}$, we can cast the factorization of $x^m - \lambda$ into distinct basic irreducible polynomials over $R_k = \frac{\mathbb{F}_q[u]}{\langle u^k \rangle}$ as follows.

(1) If α is an odd integer, then we have $x^m - \lambda = A(x) \prod_{i=1}^{\alpha} g_i(x)$,where $g_i(x) = g_i^*(x)$, $\deg(g_i(x)) = \frac{m-1}{\alpha}$;

(2) If α is an even integer, then we have $x^m - \lambda = A(x) \prod_{j=1}^{\frac{\alpha}{2}} h_j(x)h_j^*(x)$,where $\deg(h_j(x))$ $=\deg(h_j^*(x)) = \frac{m-1}{\alpha}$; if

(i) $\lambda = 1$, $A(x) = x - 1$, or
(ii) $\lambda = -1$, $A(x) = x + 1$, or
(iii) $\lambda = 1 + \omega u^{\mathrm{t}}$, q is a power of 2, $A(x) = x + 1 + \omega u^{\mathrm{t}}$, where $\mathrm{t} \geq \lceil \frac{k}{2} \rceil$, $\omega \in R_k^{\times}$.

Now, we only give some examples to illustrate its correctness. In fact, we have tried a lot of examples by Magma, the conjecture is also correct. But we fail to prove it. Thus we would like to put it here as a conjecture.

Example 3.6 Let $R_k = \mathbb{F}_3[u]/\langle u^k \rangle, m = 11, \alpha = 2$ be an even integer, implies $\alpha \mid (m-1) = 2 \mid 10$,$\mathrm{ord}_{11}(3) = \frac{m-1}{\alpha} = 5$, then by Conjecture 3.5,

$$\begin{aligned} x^{11} - 1 &= (x-1)(x^5 + 2x^3 + x^2 + 2x + 2)(x^5 + x^4 + 2x^3 + x^2 + 2), \\ x^{11} + 1 &= (x+1)(x^5 + 2x^3 + 2x^2 + 2x + 1)(x^5 + 2x^4 + 2x^3 + 2x^2 + 1). \end{aligned}$$

Example 3.7 Let $R_k = \mathbb{F}_2[u]/\langle u^k \rangle, m = 5, u^k = 0, \mathrm{t} \geq \lceil \frac{k}{2} \rceil, \alpha = 1$ be an odd integer, implies $\alpha \mid (m-1) = 1 \mid 4$,$\mathrm{ord}_5(2) = \frac{m-1}{\alpha} = 4$, then by Conjecture 3.5,

$$\begin{aligned} x^5 - 1 &= (x-1)(x^4 + x^3 + x^2 + x + 1), \\ x^5 - (1 + u^{\mathrm{t}}) &= (x + 1 + u^{\mathrm{t}})(x^4 + (1 + u^{\mathrm{t}})x^3 + x^2 + (1 + u^{\mathrm{t}})x + 1). \end{aligned}$$

Example 3.8 Let $R_k = \mathbb{F}_4[u]/\langle u^k \rangle, m = 7, u^k = 0, \mathrm{t} \geq \lceil \frac{k}{2} \rceil, \alpha = 2$ be an even integer, implies $\alpha \mid (m-1) = 2 \mid 6$,$\mathrm{ord}_7(4) = \frac{m-1}{\alpha} = 3$, then by Conjecture 3.5,

$$\begin{aligned} x^7 - 1 &= (x-1)(x^3 + x + 1)(x^3 + x^2 + 1), \\ x^7 - (1 + u^{\mathrm{t}}) &= (x + 1 + u^{\mathrm{t}})(x^3 + x + 1 + u^{\mathrm{t}})(x^3 + (1 + u^{\mathrm{t}})x^2 + 1 + u^{\mathrm{t}}). \end{aligned}$$

The proof of Theorem 3.9 is similar to that of Theorem 3.2, and is omitted.

Theorem 3.9 *Assume that the factorization of $x^m - \lambda$ into basic irreducible polynomials over $R_k = \frac{\mathbb{F}_q[u]}{\langle u^k \rangle}$ is of the form of*

1) *case (1) in Conjecture 3.5, the total number of self-dual (resp. LCD) double λ-circulant codes over R_k is*

$$Bq^{\frac{(m-1)(k-1)}{2}}(q^{\frac{m-1}{2\alpha}} + 1)^{\alpha}(resp. (q-2)q^{m(k-1)}(q^{\frac{m-1}{\alpha}} - (q^{\frac{m-1}{2\alpha}} + 1))^{\alpha}).$$

2) *case (2) in Conjecture 3.5, the total number of self-dual (resp. LCD) double λ-circulant codes over* R_k *is*

$$Bq^{\frac{(m-1)(k-1)}{2}}(q^{\frac{m-1}{\alpha}}-1)^{\frac{\alpha}{2}}(resp.(q-2)q^{k-1}(q^{\frac{2k(m-1)}{\alpha}}-q^{\frac{2(m-1)(k-1)}{\alpha}}(q^{\frac{m-1}{\alpha}}-1))^{\frac{\alpha}{2}}).$$

4 Main results

Firstly, we give some lemmas as follows.

A. Case (1) in Lemma 3.4 In this case, by the Chinese Remainder Theorem (CRT), we have

$$\begin{aligned}\frac{R_k[x]}{\langle x^m+1\rangle} &\simeq \frac{R_k[x]}{\langle h(x)\rangle}\oplus\frac{R_k[x]}{\langle h^*(x)\rangle}\\ &\simeq \frac{\mathbb{F}_q[u,x]}{\langle u^k,h(x)\rangle}\oplus\frac{\mathbb{F}_q[u,x]}{\langle u^k,h^*(x)\rangle}\\ &\simeq (\mathbb{F}_{q^{n-1}}+u\mathbb{F}_{q^{n-1}}+\cdots+u^{k-1}\mathbb{F}_{q^{n-1}})\oplus(\mathbb{F}_{q^{n-1}}+u\mathbb{F}_{q^{n-1}}+\cdots+u^{k-1}\mathbb{F}_{q^{n-1}})\\ &\simeq R_{k(\frac{m}{2})}\oplus R_{k(\frac{m}{2})}.\end{aligned}$$

Lemma 4.1 *If* $0\neq\varepsilon=(\mu,\nu)\in C$*, and* $C=\langle(1,h)\rangle$ *is a double negacirculant code over* R_k*. Then*

(1) *there are at most* $q^{\frac{m(2k-1)}{2}}$ *generators* $(1,h)$ *such that* $\varepsilon=(\mu,\nu)\in C$.
(2) *there are at most* $q^{\frac{m(k-1)}{2}}$ *generators* $(1,h)$ *such that* $\varepsilon=(\mu,\nu)\in C$ *and* $C=C^{\perp}$.
(3) *there are at most* $q^{\frac{m(2k-1)}{2}}$ *generators* $(1,h)$ *such that* $\varepsilon=(\mu,\nu)\in C$ *and* $C\cap C^{\perp}=\{0\}$.

Proof By the CRT, $(\mu,\nu)=(\mu',\nu')\oplus(\mu'',\nu'')$. Since $(\mu,\nu)\in C$, then $\nu=\mu h$, $\nu'=\mu'h'$ and $\nu''=\mu''h''$, where μ', ν', $h'\in R_k[x]/\langle h(x)\rangle=R_{k(\frac{m}{2})}$ and μ'', ν'', $h''\in R_k[x]/\langle h^*(x)\rangle=R_{k(\frac{m}{2})}$. Let $h'=h'^{(0)}+uh'^{(1)}+\cdots+u^{k-1}h'^{(k-1)}$ and $h''=h''^{(0)}+uh''^{(1)}+\cdots+u^{k-1}h''^{(k-1)}$, where $h'^{(i)},h''^{(i)}\in\mathbb{F}_{q^{\frac{m}{2}}}$, $0\le i\le k-1$.

(1) In the first constituent of C, we discuss on the unit character of μ' as follows.

- If $\mu'\in R^{\times}_{k(\frac{m}{2})}$, there exists only one solution $h'=\frac{\nu'}{\mu'}$.
- If $\mu'\in R_{k(\frac{m}{2})}\backslash\{R^{\times}_{k(\frac{m}{2})}\cup\{0\}\}$, then $\mu'=u^l\mu'^{(l)}+u^{l+1}\mu'^{(l+1)}+\cdots+u^{k-1}\mu'^{(k-1)}$ where $1\le l\le k-1$, $\mu'^{(l)}\in\mathbb{F}^*_{q^{\frac{m}{2}}}$, $\mu'^{(i)}\in\mathbb{F}_{q^{\frac{m}{2}}}$, $l+1\le i\le k-1$ and $\nu'=u^l\nu'^{(l)}+u^{l+1}\nu'^{(l+1)}+\cdots+u^{k-1}\nu'^{(k-1)}$ where $\nu'^{(j)}\in\mathbb{F}_{q^{\frac{m}{2}}}$, $l\le j\le k-1$. Since $\nu'=\mu'h'$, $u^k=0$, then $\nu'=u^l\nu'^{(l)}+u^{l+1}\nu'^{(l+1)}+\cdots+u^{k-1}\nu'^{(k-1)}=(u^l\mu'^{(l)}+u^{l+1}\mu'^{(l+1)}+\cdots+u^{k-1}\mu'^{(k-1)})h'=u^l\mu'^{(l)}h'^{(0)}+u^{l+1}(\mu'^{(l+1)}h'^{(0)}+\mu'^{(l)}h'^{(1)})+\cdots+u^{k-1}(\mu'^{(k-1)}h'^{(0)}+\mu'^{(k-2)}h'^{(1)}+\cdots+\mu'^{(l)}h'^{(k-1-l)})$. Hence, we have

$$\begin{cases}\nu'^{(l)}=\mu'^{(l)}h'^{(0)},\\ \nu'^{(l+1)}=\mu'^{(l+1)}h'^{(0)}+\mu'^{(l)}h'^{(1)},\\ \cdots\\ \nu'^{(k-1)}=\mu'^{(k-1)}h'^{(0)}+\mu'^{(k-2)}h'^{(1)}+\cdots+\mu'^{(l)}h'^{(k-1-l)}.\end{cases}\qquad(7)$$

By (7), we can get

$$\begin{pmatrix} \mu'^{(l)} & 0 & \cdots & 0 \\ \mu'^{(l+1)} & \mu'^{(l)} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \mu'^{(k-1)} & \mu'^{(k-2)} & \cdots & \mu'^{(l)} \end{pmatrix}. \tag{8}$$

Since $\mu'^{(l)} \in \mathbb{F}^*_{q^{\frac{m}{2}}}$, the determinant of the matrix (8) is not equal to 0, then $h'^{(0)}, h'^{(1)}, \cdots, h'^{(k-1-l)}$ have a unique solution, $h'^{(k-l)}, h'^{(k-l+1)}, \cdots, h'^{(k-1)} \in \mathbb{F}_{q^{\frac{m}{2}}}$. Thus there are at most $q^{\frac{ml}{2}}$ choices for h'. When $l = k-1$, we can get the maximum possible for h', i.e., there are at most $q^{\frac{m(k-1)}{2}}$ choices for h'.

- If $\mu' = 0$, then $h' \in R_{k(\frac{m}{2})}$, there are $q^{\frac{km}{2}}$ choices for h'.

Using the same argument as above in the second constituent of C, there are also at most $q^{\frac{km}{2}}$ choices for h''. But $\varepsilon \neq 0$,then μ' and μ'' can not be zero simultaneously. Hence there are at most $q^{\frac{m(k-1)}{2}} \times q^{\frac{km}{2}}$ generators $(1, h)$ such that $\varepsilon \in C$.

(2) Since C is a self-dual double negacirculant code, then

$$\langle (1, h'), (1, h'') \rangle = 1 + h'h'' = 0. \tag{9}$$

It is equivalent to

$$\begin{cases} h'^{(0)}h''^{(0)} = -1, \\ h'^{(0)}h''^{(1)} + h'^{(1)}h''^{(0)} = 0, \\ h'^{(0)}h''^{(2)} + h'^{(1)}h''^{(1)} + h'^{(2)}h''^{(0)} = 0, \\ \cdots \\ h'^{(0)}h''^{(k-1)} + h'^{(1)}h''^{(k-2)} + \cdots + h'^{(k-1)}h''^{(0)} = 0. \end{cases} \tag{10}$$

Combining with the proof of (1), we have:

- if $\mu', \mu'' \in R^{\times}_{k(\frac{m}{2})}$, we know that $h' = \frac{\nu'}{\mu'}$ and $h'' = \frac{\nu''}{\mu''}$, then there are at most one generator $(1, h)$.
- if $\mu' \in R^{\times}_{k(\frac{m}{2})}$, $\mu'' \in R_{k(\frac{m}{2})} \backslash \{R^{\times}_{k(\frac{m}{2})} \cup \{0\}\}$, we know that $h' = \frac{\nu'}{\mu'}$,by (9), h'' can be uniquely fixed, then there are at most one generator $(1, h)$.
- if $\mu' \in R^{\times}_{k(\frac{m}{2})}$, $\mu'' = 0$, we know that $h' = \frac{\nu'}{\mu'}$ and h'' is free, by (10), then there are at most one generator $(1, h)$.
- if $\mu', \mu'' \in R_{k(\frac{m}{2})} \backslash \{R^{\times}_{k(\frac{m}{2})} \cup \{0\}\}$, we know that $h'^{(0)}$ can be uniquely fixed, $h'^{(1)}, h'^{(2)}, \cdots, h'^{(k-1)} \in \mathbb{F}_{q^{\frac{m}{2}}}$, $h''^{(0)}$ can be uniquely fixed, $h''^{(1)}, h''^{(2)}, \cdots, h''^{(k-1)} \in \mathbb{F}_{q^{\frac{m}{2}}}$, and because of (10), then there are at most $q^{\frac{m(k-1)}{2}}$ generators $(1, h)$.
- if $\mu' \in R_{k(\frac{m}{2})} \backslash \{R^{\times}_{k(\frac{m}{2})} \cup \{0\}\}$, $\mu'' = 0$, we know that $h'^{(0)}$ can be uniquely fixed, $h'^{(1)}, h'^{(2)}, \cdots, h'^{(k-1)} \in \mathbb{F}_{q^{\frac{m}{2}}}$, $h'' \in R_{k(\frac{m}{2})}$, and because of (10), then there are at most $q^{\frac{m(k-1)}{2}}$ generators $(1, h)$.

(3) Since C is an LCD double negacirculant code, then

$$\langle (1, h'), (1, h'') \rangle = 1 + h'h'' \in R^{\times}_{k(\frac{m}{2})}. \tag{11}$$

Using the similar way, there are at most $q^{\frac{m(2k-1)}{2}}$ generators $(1, h)$ such that $\varepsilon = (\mu, \nu) \in C$ and $C \cap C^{\perp} = \{0\}$. We have thus proved the lemma. □

B. Case (2) in Lemma 3.4 In this case, by the CRT, we have

$$\begin{aligned}\frac{R_k[x]}{\langle x^m+1\rangle} &\simeq \bigoplus_{i=1}^{2}\left(\frac{R_k[x]}{\langle h_i(x)\rangle}\oplus\frac{R_k[x]}{\langle h_i^*(x)\rangle}\right)\\ &\simeq \bigoplus_{i=1}^{2}\left(\frac{\mathbb{F}_q[u,x]}{\langle u^2,h_i(x)\rangle}\oplus\frac{\mathbb{F}_q[u,x]}{\langle u^2,h_i^*(x)\rangle}\right)\\ &\simeq R_{k(\frac{m}{4})}\oplus R_{k(\frac{m}{4})}\oplus R_{k(\frac{m}{4})}\oplus R_{k(\frac{m}{4})}.\end{aligned}$$

Lemma 4.2 *If $C=\langle(1,h)\rangle$ is a double negacirculant code over R_k, and $0\neq\varepsilon=(\mu,\nu)\in C$, then*

(1) *there are at most $q^{\frac{m(4k-1)}{4}}$ generators $(1,h)$ such that $\varepsilon=(\mu,\nu)\in C$.*
(2) *there are at most $q^{\frac{m(2k-1)}{4}}$ generators $(1,h)$ such that $\varepsilon=(\mu,\nu)\in C$ and $C=C^{\perp}$.*
(3) *there are at most $q^{\frac{m(4k-3)}{4}}(q^{\frac{m}{2}}-q^{\frac{m}{4}}+1)$ generators $(1,h)$ such that $\varepsilon=(\mu,\nu)\in C$ and $C\cap C^{\perp}=\{0\}$.*

Proof By the CRT, $(\mu,\nu)=\bigoplus_{i=1}^{2}\left((\mu_i',\nu_i')\oplus(\mu_i'',\nu_i'')\right)$. Since $(\mu,\nu)\in C$, then $\nu=\mu h$, $\nu_i'=\mu_i'h_i'$ and $\nu_i''=\mu_i''h_i''$, where μ_i', ν_i', $h_i'\in R_{k(\frac{m}{4})}$ and μ_i'', ν_i'', $h_i''\in R_{k(\frac{m}{4})}$. Let $h_i'=h_i'^{(0)}+uh_i'^{(1)}+\cdots+u^{k-1}h_i'^{(k-1)}$ and $h_i''=h_i''^{(0)}+uh_i''^{(1)}+\cdots+u^{k-1}h_i''^{(k-1)}$, where $h_i'^{(j)}, h_i''^{(j)}\in\mathbb{F}_{q^{\frac{m}{4}}}$, $1\le i\le 2, 0\le j\le k-1$.

(1) In the first constituent of C, we discuss on the unit character of μ_1' as follows.

- If $\mu_1'\in R^{\times}_{k(\frac{m}{4})}$, there exists only one solution $h_1'=\frac{\nu_1'}{\mu_1'}$.
- If $\mu_1'\in R_{k(\frac{m}{4})}\backslash\{R^{\times}_{k(\frac{m}{4})}\cup\{0\}\}$, then $\mu_1'=u^l\mu_1'^{(l)}+u^{l+1}\mu_1'^{(l+1)}+\cdots+u^{k-1}\mu_1'^{(k-1)}$, $1\le l\le k-1$, $\mu_1'^{(l)}\in\mathbb{F}^*_{q^{\frac{m}{4}}}$, $\mu_1'^{(i)}\in\mathbb{F}_{q^{\frac{m}{4}}}$, $l+1\le i\le k-1$ and $\nu_1'=u^l\nu_1'^{(l)}+u^{l+1}\nu_1'^{(l)}+\cdots+u^{k-1}\nu_1'^{(k-1)}$, $\nu_1'^{(j)}\in\mathbb{F}_{q^{\frac{m}{4}}}$, $l\le i\le k-1$. Since $\nu_1'=\mu_1'h_1', u^k=0$, then $\nu_1'=u^l\nu_1'^{(l)}+u^{l+1}\nu_1'^{(l)}+\cdots+u^{k-1}\nu_1'^{(k-1)}=(u^l\mu_1'^{(l)}+u^{l+1}\mu_1'^{(l+1)}+\cdots+u^{k-1}\mu_1'^{(k-1)})h_1'=u^l\mu_1'^{(l)}h_1'^{(0)}+u^{l+1}(\mu_1'^{(l+1)}h_1'^{(0)}+\mu_1'^{(l)}h_1'^{(1)})+\cdots+u^{k-1}(\mu_1'^{(k-1)}h_1'^{(0)}+\mu_1'^{(k-2)}h_1'^{(1)}+\cdots+\mu_1'^{(l)}h_1'^{(k-1-l)})$. Hence, we obtain

$$\begin{cases}\nu_1'^{(l)}=\mu_1'^{(l)}h_1'^{(0)},\\ \nu_1'^{(l+1)}=\mu_1'^{(l+1)}h_1'^{(0)}+\mu_1'^{(l)}h_1'^{(1)},\\ \cdots\\ \nu_1'^{(k-1)}=\mu_1'^{(k-1)}h_1'^{(0)}+\mu_1'^{(k-2)}h_1'^{(1)}+\cdots+\mu_1'^{(l)}h_1'^{(k-1-l)}.\end{cases}\tag{12}$$

By (12), we can get

$$\begin{pmatrix}\mu_1'^{(l)} & 0 & \cdots & 0\\ \mu_1'^{(l+1)} & \mu_1'^{(l)} & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots\\ \mu_1'^{(k-1)} & \mu_1'^{(k-2)} & \cdots & \mu_1'^{(l)}\end{pmatrix}.\tag{13}$$

Since $\mu_1'^{(l)} \in \mathbb{F}^*_{q^{\frac{m}{4}}}$, the determinant of the matrix (13) is not equal to 0, then $h_1'^{(0)}, h_1'^{(1)}, \cdots, h_1'^{(k-1-l)}$ have a unique solution, $h_1'^{(k-l)}, h_1'^{(k-l+1)}, \cdots, h_1'^{(k-1)} \in \mathbb{F}_{q^{\frac{m}{4}}}$. Thus, there are at most $q^{\frac{ml}{4}}$ choices for h_1'. When $l = k-1$, we can get the maximum possible for h_1', i.e., there are at most $q^{\frac{m(k-1)}{4}}$ choices for h_1'.
- If $\mu_1' = 0$, then $h_1' \in R_{k(\frac{m}{4})}$, there are $q^{\frac{km}{4}}$ choices for h_1'.

Using the same argument as above in the other constituent of C, there are also at most $q^{\frac{km}{4}}$ choices for h_2', h_1'', h_2''. But $\varepsilon \neq 0$,then μ_1', μ_2', μ_1'' and μ_2'' can not be zero simultaneously. Hence, there are at most $q^{\frac{m(k-1)}{4}} \times (q^{\frac{km}{4}})^3$ generators $(1, h)$ such that $\varepsilon \in C$.

(2) Since C is a self-dual double negacirculant code, then

$$\begin{cases} \langle (1, h_1'), (1, h_1'') \rangle = 0, \\ \langle (1, h_2'), (1, h_2'') \rangle = 0. \end{cases} \tag{14}$$

Combining with the proof of (1), similar to the discussion of (2) in Lemma 4.1, there are at most $q^{\frac{(2k-1)m}{4}}$ generators $(1, h)$ such that $\varepsilon = (\mu, \nu) \in C$ and $C = C^{\perp}$.

(3) Since C is an LCD double negacirculant code, then

$$\langle (1, h_i'), (1, h_i'') \rangle = 1 + h_i' h_i'' \in R^{\times}_{k(\frac{m}{4})}, i = 1, 2. \tag{15}$$

Using the similar way, there are at most $q^{\frac{m(4k-3)}{4}}(q^{\frac{m}{2}} - q^{\frac{m}{4}} + 1)$ generators $(1, h)$ such that $\varepsilon = (\mu, \nu) \in C$ and $C \cap C^{\perp} = \{0\}$. We have thus proved the lemma. □

C. Case (1) in Theorem 3.9

Lemma 4.3 *If $0 \neq \varepsilon = (\mu, \nu) \in C$, and if there exists a positive integer i such that μ is not generated by $g_i(x)$, and if, furthermore, $C = \langle (1, h) \rangle$ is a double λ-circulant code over R_k, then*

(1) *there are at most $q^{\frac{m(k\alpha-1)+1}{\alpha}}$ generators $(1, h)$ such that $\varepsilon \in C$.*
(2) *there are at most $Bq^{\frac{(m-1)(k-1)}{2}}(q^{\frac{m-1}{2\alpha}} + 1)^{\alpha-1}$ generators $(1, h)$ such that $\varepsilon \in C$ and $C = C^{\perp}$.*
(3) *there are at most $(q-2)q^{m(k-1)}(q^{\frac{m-1}{\alpha}} - q^{\frac{m-1}{2\alpha}} - 1)^{\alpha-1}$ generators $(1, h)$ such that $\varepsilon = (\mu, \nu) \in C$ and $C \cap C^{\perp} = \{0\}$.*

Proof By the CRT, we have $(\mu, \nu) \simeq (\mu_0, \nu_0) \oplus \left(\bigoplus_{i=1}^{\alpha} (\mu_i, \nu_i) \right)$. Since $\varepsilon = (\mu, \nu) \in C$, then $\nu = \mu h$, $\nu_0 = \mu_0 h_0$ and $\nu_i = \mu_i h_i$, where $\mu_0, \nu_0, h_0 \in R_k = R_k[x]/\langle A(x) \rangle$ and μ_i, ν_i, $h_i \in R_{k(\frac{m-1}{\alpha})} = R_k[x]/\langle g_i(x) \rangle$. Let $h_0 = h_0^{(0)} + uh_0^{(1)} + \cdots + u^{k-1}h_0^{(k-1)}$ and $h_i = h_i^{(0)} + uh_i^{(1)} + \cdots + u^{k-1}h_i^{(k-1)}$, where $h_0^{(j)} \in \mathbb{F}_q$, $h_i^{(j)} \in \mathbb{F}_{q^{\frac{m-1}{\alpha}}}$, $1 \leq i \leq \alpha$, $0 \leq j \leq k-1$.

(1) In the first constituent of C, we discuss on the unit character of μ_0 as follows.

- If $\mu_0 \in R_k^{\times}$, there exists unique solution $h_0 = \frac{\nu_0}{\mu_0}$.
- If $\mu_0 \in R_k \backslash \{R_k^{\times} \cup \{0\}\}$, similar to discuss in Lemma 4.1, there are at most q^{k-1} choices for h_0.
- If μ_0=0, then h_0 is arbitrary in R_k, there are q^k choices for h_0.

In the ith constituent of C, we discuss on the unit character of μ_i as follows.

- If $\mu_i \in R^{\times}_{k(\frac{m-1}{\alpha})}$, there exists only one solution $h_i = \frac{\nu_i}{\mu_i}$.
- If $\mu_i \in R_{k(\frac{m-1}{\alpha})} \backslash \{R^{\times}_{k(\frac{m-1}{\alpha})} \cup \{0\}\}$, this case can be discussed similarly. Hence, there are at most $q^{\frac{(m-1)(k-1)}{\alpha}}$ choices for h_i.
- If $\mu_i = 0$, there are $q^{\frac{k(m-1)}{\alpha}}$ choices for h_1'.

Thus there are at most $q^{\frac{m(k\alpha-1)+1}{\alpha}}$ generators $(1, h)$ such that $\varepsilon \in C$.

(2) In the first constituent of C, there are at most B generators $(1, h_0)$ such that C_0 is a self-dual double λ-circulant code over R_k by Theorem 3.2.

In the ith constituent of C, combining with (1), we can get

- if $\mu_i \in R^{\times}_{k(\frac{m-1}{\alpha})}$, there exists only one solution $h_i = \frac{\nu_i}{\mu_i}$.
- if $\mu_i \in R_{k(\frac{m-1}{\alpha})} \backslash \{R^{\times}_{k(\frac{m-1}{\alpha})} \cup \{0\}\}$, $h_i^{(0)}$ can be uniquely fixed, $h_i^{(1)}, h_i^{(2)} \cdots, h_i^{(k-1)} \in \mathbb{F}_{q^{\frac{m-1}{\alpha}}}$. And because C is a self-dual double λ-circulant code, then $\langle (1, h_i) \cdot (1, h_i) \rangle_H = 1 + h_i \overline{h_i} = 0$, which implies

$$\begin{cases} h_i^{(0)} h_i^{(0) q^{\frac{m-1}{2\alpha}}} = -1, \\ h_i^{(0)} h_i^{(1) q^{\frac{m-1}{2\alpha}}} + h_i^{(1)} h_i^{(0) q^{\frac{m-1}{2\alpha}}} = 0, \\ h_i^{(0)} h_i^{(2) q^{\frac{m-1}{2\alpha}}} + h_i^{(1)} h_i^{(1) q^{\frac{m-1}{2\alpha}}} + h_i^{(2)} h_i^{(0) q^{\frac{m-1}{2\alpha}}} = 0, \\ \cdots \\ h_i^{(0)} h_i^{(k-1) q^{\frac{m-1}{2\alpha}}} + h_i^{(1)} h_i^{(k-2) q^{\frac{m-1}{2\alpha}}} + \cdots + h_i^{(k-1)} h_i^{(0) q^{\frac{m-1}{2\alpha}}} = 0. \end{cases} \Longleftrightarrow$$

$$\begin{cases} Norm(h_i^{(0)}) = -1, \\ Tr(h_i^{(0)} h_i^{(1) q^{\frac{m-1}{2\alpha}}}) = 0, \\ Tr(h_i^{(0)} h_i^{(2) q^{\frac{m-1}{2\alpha}}}) + Norm(h_i^{(1)}) = 0, \\ \cdots \\ Tr(h_i^{(0)} h_i^{(k-1) q^{\frac{m-1}{2\alpha}}}) + Tr(h_i^{(1)} h_i^{(k-2) q^{\frac{m-1}{2\alpha}}}) + \cdots + Tr(h_i^{(\frac{k-2}{2})} h_i^{(\frac{k}{2}) q^{\frac{m-1}{2\alpha}}}) = 0, \\ \text{when } k \text{ is even , or} \\ Tr(h_i^{(0)} h_i^{(k-1) q^{\frac{m-1}{2\alpha}}}) + \cdots + Tr(h_i^{(\frac{k-3}{2})} h_i^{(\frac{k+1}{2}) q^{\frac{m-1}{2\alpha}}}) + Norm(h_i^{(\frac{k-1}{2})}) = 0, \\ \text{when } k \text{ is odd ,} \end{cases}$$

then there are at most $q^{\frac{(m-1)(k-1)}{2\alpha}}$ choices for h_i.

- if $\mu_i = 0$, since C is a self-dual double λ-circulant code, there are at most $q^{\frac{(m-1)(k-1)}{2\alpha}} (q^{\frac{m-1}{2\alpha}} + 1)$ choices for h_i.

Thus there are at most $Bq^{\frac{(m-1)(k-1)}{2}} (q^{\frac{m-1}{2\alpha}} + 1)^{\alpha-1}$ generators $(1, h)$ such that $\varepsilon \in C$ and $C = C^{\perp}$.

(3) Since C is an LCD double λ-circulant code, then

$$\langle (1, h_i), (1, h_i) \rangle_H = 1 + h_i \bar{h}_i \in R_k^{\times}, i = 1, 2, \cdots, \alpha. \quad (16)$$

Hence, there are at most $(q-2)q^{m(k-1)}(q^{\frac{m-1}{\alpha}} - q^{\frac{m-1}{2\alpha}} - 1)^{\alpha-1}$ generators $(1, h)$ such that $\varepsilon = (\mu, \nu) \in C$ and $C \cap C^{\perp} = \{0\}$. □

D. Case (2) in Theorem 3.9

Lemma 4.4 *If $C = \langle(1, h)\rangle$ is a double λ-circulant code over R_k, such that $0 \neq \varepsilon = (\mu, \nu) \in C$, and that there exists a positive integer i such that μ is not generated by $h_i(x)$, then*

(1) *there are at most $q^{\frac{m(k\alpha-1)+1}{\alpha}}$ generators $(1, h)$ such that $\varepsilon \in C$.*
(2) *there are at most $Bq^{\frac{(m-1)(k\alpha-2)}{2\alpha}}$ generators $(1, h)$ such that $\varepsilon \in C$ and $C = C^{\perp}$.*
(3) *there are at most $(q-2)q^{\frac{(m-1)(\alpha k-\alpha+1)}{\alpha}}(q^{\frac{2(m-1)}{\alpha}} - q^{\frac{m-1}{\alpha}} + 1)^{\frac{\alpha}{2}-1}$ generators $(1, h)$ such that $\varepsilon = (\mu, \nu) \in C$ and $C \cap C^{\perp} = \{0\}$.*

Proof Again using the CRT, we have $(\mu, \nu) \simeq (\mu_0, \nu_0) \oplus \left(\bigoplus_{j=1}^{\alpha/2}\left((\mu'_j, \nu'_j) \oplus (\mu''_j, \nu''_j)\right)\right)$. Since $\varepsilon = (\mu, \nu) \in C$, then $\nu = \mu h$, $\nu_0 = \mu_0 h_0$, $\nu'_j = \mu'_j h'_j$ and $\nu''_j = \mu''_j h''_j$, where μ_0, ν_0, $h_0 \in R_k = R_k[x]/\langle A(x)\rangle$, $\mu'_j, \nu'_j, h'_j \in R_{k(\frac{m-1}{\alpha})} = R_k[x]/\langle h_j(x)\rangle$ and $\mu''_j, \nu''_j, h''_j \in R_{k(\frac{m-1}{\alpha})} = R_k[x]/\langle h^*_j(x)\rangle$. Let $h_0 = h_0^{(0)} + uh_0^{(1)} + \cdots + u^{k-1}h_0^{(k-1)}$, $h'_j = h_j'^{(0)} + uh_j'^{(1)} + \cdots + u^{k-1}h_j'^{(k-1)}$, $h''_j = h_j''^{(0)} + uh_j''^{(1)} + \cdots + u^{k-1}h_j''^{(k-1)}$, where $h_0^{(0)}, h_0^{(1)}, \cdots, h_0^{(k-1)} \in \mathbb{F}_q$, $h_j'^{(0)}, h_j'^{(1)}, \cdots, h_j'^{(k-1)}\mathbb{F}_{q^{\frac{m-1}{\alpha}}}$, $h_j''^{(0)}, h_j''^{(1)}, \cdots, h_j''^{(k-1)} \in \mathbb{F}_{q^{\frac{m-1}{\alpha}}}$.

(1) Since $0 \neq \varepsilon \in C$, there are at most $q^{\frac{m(k\alpha-1)+1}{\alpha}}$ generators $(1, h)$.
(2) In the first constituent of C, there are at most B generators $(1, h_0)$ such that C_0 is a self-dual double λ-circulant code over R_k according to Theorem 3.2.
    In the jth constituent of C, we have a similar discussion for pairs (μ'_j, μ''_j), there are at most $Bq^{\frac{(m-1)(k\alpha-2)}{2\alpha}}$ generators $(1, h)$ such that $\varepsilon \in C$ and $C = C^{\perp}$.
(3) Since C is an LCD double λ-circulant code, then

$$\langle(1, h'_j), (1, h''_j)\rangle = 1 + h'_j h''_j \in R^{\times}_{k(\frac{m-1}{\alpha})}, \; j = 1, 2, \cdots, \frac{\alpha}{2}. \tag{17}$$

Hence, there are at most $(q-2)q^{\frac{(m-1)(\alpha k-\alpha+1)}{\alpha}}(q^{\frac{2(m-1)}{\alpha}} - q^{\frac{m-1}{\alpha}} + 1)^{\frac{\alpha}{2}-1}$ generators $(1, h)$ such that $\varepsilon = (\mu, \nu) \in C$ and $C \cap C^{\perp} = \{0\}$. □

We are now ready for the main result of this paper.

Theorem 4.5 *If q is a power of prime, then there are infinite families of:*

(1) *self-dual (resp. LCD) negacirculant codes of index 2 over R_k of relative distance δ satisfying $H_q(\delta) \geq \frac{1}{4p^{k-1}}$ $(resp. H_q(\delta) \geq \frac{1}{4p^{k-1}})$ for case (1) in Lemma 3.4;*
(2) *self-dual (resp. LCD) negacirculant codes of index 2 over R_k of relative distance δ satisfying $H_q(\delta) \geq \frac{1}{8p^{k-1}}$ $(resp. H_q(\delta) \geq \frac{1}{8p^{k-1}})$ for case (2) in Lemma 3.4;*
(3) *self-dual (resp. LCD) λ-circulant codes of index 2 over R_k of relative distance δ satisfying $H_q(\delta) \geq \frac{1}{4\alpha p^{k-1}}$ $(resp. H_q(\delta) \geq \frac{1}{2\alpha p^{k-1}})$ for case (1) in Theorem 3.9;*
(4) *self-dual (resp. LCD) λ-circulant codes of index 2 over R_k of relative distance δ satisfying $H_q(\delta) \geq \frac{1}{2\alpha p^{k-1}}$ $(resp. H_q(\delta) \geq \frac{1}{2\alpha p^{k-1}})$ for case (2) in Theorem 3.9.*

Proof By the Gray map over R_k, we see that the Gray image of the several families of codes of length $2m$ are linear codes of length $2mp^{k-1}$. Combining Lemmas 3.4, 4.1, 4.2, 4.3, 4.4 and Theorem 3.9, the result follows by the same method as Theorem 5.2 in [20], so we omit the detailed proof here. □

5 Conclusion

In the present paper, we have studied self-dual (resp. LCD) double λ-circulant codes over the ring $R_k = \mathbb{F}_p[u]/\langle u^k \rangle$,i.e., index 2 quasi-twisted codes with twisting constant $\lambda = \pm 1$ and $\lambda = 1 + wu^t$.

We not only have considered the special factorization of $x^m + 1$ to construct the double negacirculant codes when it factors into two (resp. four) basic irreducible factors reciprocal of each other for m a power of 2 in [1, 2], but also have studied another special kind of factorization, for m odd prime, and $(m, q) = 1$ when $x^m - \lambda$ factors into $\alpha + 1$ basic irreducible polynomials with $\alpha \mid (m - 1)$ and $\mathrm{ord}_m(q) = \frac{m-1}{\alpha}$. With this particular factorization, we have constructed self-dual (resp. LCD) quasi-twisted codes of index 2 over R_k, and derived an exact enumeration formula for this family of codes. Further, we have derived a modified Varshamov-Gilbert bound on the relative distance of the codes considered, building on exact enumeration results.

The main open problem is Conjecture 3.5. More general directions are quasi-twisted codes of index > 2 and replacing R_k by a general chain ring.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Alahmadi, A., Güneri, C., Özkaya, B., Shoaib, H., Solé, P.: On self-dual double negacirculant codes. Discret. Appl. Math. **222**, 205–212 (2017)
2. Alahmadi, A., Güneri, C., Özkaya, B., Shoaib, H., Solé, P.: On linear complementary-dual multinegacirculant codes, Cryptography and Communications (2017)
3. Alahmadi, A., Özdemir, F., Solé, P.: On self-dual double circulant codes, Designs, Codes and Cryptography. https://doi.org/10.1007/s10623-017-0393-x (2017)
4. Carlet, C., Güneri, C., Özbudak, F., Solé, P.: A new concatenated type construction for LCD codes and isometry codes. Discret. Math. **341**(3), 830–835 (2018)
5. Carlet, C., Mesnager, S., Tang, C.M., Qi, Y.F., Pellikaan, R.: Linear Codes Over $\mathbb{F}_q$ Are Equivalent to LCD Codes for $q > 3$. IEEE Trans. Inf. Theory **64**(4), 3010–3017 (2018)
6. Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**, 131–150 (2016)
7. Carlet, C., Guilley, S.: Statistical properties of side-channel and fault injection attacks using coding theory. Cryptogr. Commun. **10**, 909–933 (2018)
8. Güneri, C., Özkaya, B., Solé, P.: Quasi-cyclic complementary dual codes. Finite Fields Appl. **42**, 67–80 (2016)
9. Hooley, C.: On Artin's conjecture. J. Fur Die Reine Und Angewandte Mathematik **225**, 209–220 (1967)
10. Huffman, W.C., Pless, V.: Fundamentals of error correcting codes. Cambridge University Press, Cambridge (2003)
11. Jia, Y.: On quasi-twisted codes over finite fields. Finite Fields Appl. **18**, 237–257 (2012)
12. Kaya, A., Yildiz, B., Pasa, A.: New extremal binary self-dual codes from a modified four circulant construction. Discret. Math. **339**, 1086–1094 (2016)
13. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes I: finite fields. IEEE Trans. Inf. Theory **47**, 2751–2760 (2001)

14. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes II: Chain rings, Des. Codes Crypt. **30**(1), 113–130 (2003)
15. Ling, S., Blackford, T.: $\mathbb{Z}_{p^{k+1}}$-linear codes. IEEE Trans. Inf. Theory **48**(9), 2592–2605 (2002)
16. Moree, P.: Artin's primitive root conjecture a survey. Integers **10**(6), 1305–1416 (2012)
17. Meyn, H.: Factorization of the cyclotomic polynomial $x^{2^n}+1$ over finite fields. Finite Fields Their Appl **2**, 439–442 (1996)
18. Massey, J.L.: Linear codes with complementary duals. Discret. Math. **106**(/107), 337–342 (1992)
19. Saleh, A., Esmaeili, M.: Some classes of quasi-twisted codes over finite chain rings, Journal of Applied Mathematics and Computing. https://doi.org/10.1007/s12190-017-1125-0 (2017)
20. Shi, M.J., Qian, L.Q., Solé, P.: On self-dual negacirculant codes of index two and four, Designs, Codes and Cryptography. https://doi.org/10.1007/s10623-017-0455-0 (2018)
21. Shi, M.J., Liu, Y., Solé, P.: Optimal two-weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Commun. Lett. **20**(12), 2346–2349 (2016)
22. Shi, M.J., Zhu, S.X., Yang, S.L.: A class of optimal p-ary codes from one-weight codes over $\mathbb{F}_p[u]/(u^m)$. J. Franklin Inst. **350**(5), 929–937 (2013)
23. Shi, M.J., Wu, R.S., Liu, Y., Solé, P.: Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$. Cryptogr. Commun. **9**, 637–646 (2017)