第48卷第11期 中国科学技术大学学报 Vol. 48, No. 11
2018年11月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Nov. 2018

文章编号:0253-2778(2018)11-0890-08

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

LU Yaqi, SHI Minjia, WU Wenting, XIAO Aqing

(*School of Mathematical Sciences, Anhui University, Hefei* 230601, *China*)

Abstract: Double circulant codes of length $2n$ over a non-chain ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$, $u^2=v^2=0$, $uv=vu$, were studied when q was a prime power. Exact enumerations of self-dual and LCD double circulant codes for a positive integer n were given. Using a distance-preserving Gray map, self-dual and LCD codes of length $8n$ over $\mathbb{F}_q$ were constructed when q was even. Using random coding and the Artin conjecture, the modified Varshamov-Gilbert bounds were derived on the relative distance of the codes considered, building on exact enumeration results for given n and q.

Key words: double circulant codes; self-dual codes; LCD codes; Artin conjecture

CLC number: TP391 **Document code**: A doi: 10.3969/j.issn.0253-2778.2018.11.004

2010 Mathematics Subject Classification: 94B15; 94B25; 05E30

Citation: LU Yaqi, SHI Minjia, WU Wenting, et al. On self-dual and LCD double circulant codes over $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$[J]. Journal of University of Science and Technology of China, 2018,48(11):890-897.
卢亚琪,施敏加,伍文婷,等. $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$上的自对偶和LCD双循环码[J]. 中国科学技术大学学报,2018,48(11):890-897.

$\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$上的自对偶和LCD双循环码

卢亚琪,施敏加,伍文婷,肖阿琴

(安徽大学数学科学学院,安徽合肥 230601)

摘要:主要研究 q 为素数的方幂时非链环$\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$, $u^2=v^2=0$,$uv=vu$ 上长度为 $2n$ 的双循环码. 对于给定的正整数 n,给出了自对偶和LCD双循环码个数的精确计算公式. 利用保距的Gray映射,构造了 q 为偶数时有限域$\mathbb{F}_q$上长度为 $8n$ 的自对偶码和LCD码. 基于给定的 n 和 q 的精确计数公式,由随机编码理论和Artin猜想,得到了关于所研究码的相对距离的修订Varshamov Gilbert界.

关键词:双循环码;自对偶码;LCD码;Artin猜想

0 Introduction

Linear complementary dual (LCD) circulant codes are linear codes that meet their duals trivially. In 1992, Massey[1] introduced LCD codes and showed the asymptotically good property of LCD codes. Quasi-cyclic complementary dual codes were studied in Ref.[2]. Recently, self-dual double circulant (negacirculant) codes and self-dual four negacirculant codes over finite fields, and

Received: 2018-02-04; **Revised**: 2018-04-11

Foundation item: Supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province(1808085J20).

Biography: LU Yaqi, female, born in 1994, master. Research field: Algebraic coding. E-mail: lyqSunshine8@163.com

Corresponding author: SHI Minjia, PhD/Prof. E-mail: mjshi@ahu.edu.cn

double circulant self-dual and LCD codes over Galois rings have been studied in Refs. [3-6], the authors derived the modified Varshamov-Gilbert bounds on the relative distance of the codes considered, building on exact enumeration results for given n and q. But the case over non-chain rings are not as well-studied yet.

Codes over the non-chain ring $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$, $u^2=v^2=0$, $uv=vu$, were considered by a lot of literatures, such as Refs. [7-8]. The aim of this work is to study double circulant self-dual codes and double circulant LCD codes over the ring R. The main tool is the Chinese Remainder Theorem (CRT) approach to quasi-cyclic codes as introduced in Ref. [9], and generalized to quasi-twisted codes in Ref. [10]. Based on the theory developed in Ref. [11], we extend the method to the ring R. By the Gray map in Ref. [7], we also derive the modified Varshamov-Gilbert bounds on the relative distance of the codes considered, building on exact enumeration results for given n and q.

The material is organised as follows. The next section contains the preliminaries of the ring R. We use the CRT to study algebraic structure of double circulant codes and derive the main enumeration results in Section 2. Section 3 is dedicated to asymptotic bounds on the relative distance of the double circulant codes. Section 4 concludes the paper.

1 Preliminaries

1.1 The ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$

Consider the ring $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$, where $u^2=v^2=0$, $uv=vu$. It is a non-chain ring which has maximal ideal $\langle u,v\rangle$. Let R^* be the set which consists of all units in R, that is to say, $R^*=R\backslash\langle u,v\rangle$. The following result gives the number of square roots of -1 in R.

Proposition 1.1 (i) Let q be a power of 2. Then the number of square roots of -1 in R is q^3. (ii) Let q be a power of an odd prime with $q\equiv 1 \pmod 4$. Then the number of square roots of -1 in R is 2.

Proof (i) Assume q is a power of 2, for $r=a+bu+cv+duv\in R$, if $r^2=a^2=-1$, then $a=1$ and $b,c,d\in\mathbb{F}_q$. Thus the number of square roots of -1 in R is q^3.

(ii) Assume q is a power of an odd prime with $q\equiv 1 \pmod 4$, for $r=a+bu+cv+duv\in R$, then $r^2=a^2+2abu+2acv+2(ad+bc)uv$. Note that $r^2=-1$ if and only if $a^2=-1$ and $b=c=d=0$, thus the number of square roots of -1 in R is 2.

1.2 Norm function and trace function over finite fields

Given a positive integer m, there exists an extension field $\mathbb{F}_{q^m}$. For $x\in\mathbb{F}_{q^m}$, the trace $\mathrm{Tr}(x)$ of x over $\mathbb{F}_q$ is defined by

$$\mathrm{Tr}(x)=x+x^q+\cdots+x^{q^{m-1}}.$$

For $x\in\mathbb{F}_{q^m}$, the norm $N(x)$ of x over $\mathbb{F}_q$ is defined by

$$N(x)=x^{(q^m-1)/(q-1)}.$$

In fact, for the norm function, each nonzero element in $\mathbb{F}_q^*$ has a preimage of size $(q^m-1)/(q-1)$ in $\mathbb{F}_{q^m}^*$. For the trace function, each nonzero element in $\mathbb{F}_q^*$ has a preimage of size q^{m-1} in $\mathbb{F}_{q^m}^*$.

1.3 Codes

A linear code C of length n over R is an R-submodule of R^n. For $x=(x_1,x_2,\cdots,x_n)$, $y=(y_1,y_2,\cdots,y_n)\in C$, the Euclidean inner product of x and y is defined as $[x,y]=\sum_{i=1}^{n}x_iy_i$. The dual code of C denoted by $C^\perp$, is defined by

$$C^\perp=\{y\in R^n \mid [x,y]=0,\ \forall x\in C\}.$$

A linear code C of length n over R is called a self-dual code if $C=C^\perp$. Moreover, a linear code C of length n over R is called an LCD code (a linear code with complementary dual) if $C\cap C^\perp=\{\mathbf{0}\}$, which is equivalent to $C\oplus C^\perp=R^n$.

Let $\mathbb{F}_q$ be the finite field of order q, where q is a power of a prime p, i. e., $q=p^l$ with a positive integer l. In particular, when $\gcd(2,l)=2$, for $z=z_1+uz_2+vz_3+uvz_4\in R$ with $z_1,z_2,z_3,z_4\in\mathbb{F}_q$, the conjugation of z over R is defined by $\bar{z}=z_1^{\sqrt{q}}+uz_2^{\sqrt{q}}+vz_3^{\sqrt{q}}+uvz_4^{\sqrt{q}}$, and the Hermitian inner product is defined by $[x,y]_H=[x,\bar{y}]$, where x, $y\in R$.

Here, we use a circulant matrix to describe a double circulant code. A matrix A over R is said to be circulant if its rows are obtained by successive shifts from the first row. A code C is a double circulant code 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 matrix of order n.

1.4 Gray map

The Gray map ϕ from R to $\mathbb{F}_q^4$ is defined by

$$\phi(a+ub+vc+uvd)=(d,c+d,b+d,\ a+b+c+d)$$

in Ref.[7]. In fact, the Gray map ϕ is a bijection from R to $\mathbb{F}_q^4$, and it is a distance-preserving map, which can be extended naturally into a map from R^n to $\mathbb{F}_q^{4n}$ as $\phi((x_1,x_2,\cdots,x_n))=(\phi(x_1),\phi(x_2),\cdots,\phi(x_n))$, where $x_i\in R$ for $1\leqslant i\leqslant n$.

Theorem 1.1 Let q be a power of 2, then we have the following properties.

(i) If C is a self-dual code of length n over R, then $\phi(C)$ is a self-dual code of length $4n$ over $\mathbb{F}_q$.

(ii) If C is an LCD code of length n over R, then $\phi(C)$ is also an LCD code of length $4n$ over $\mathbb{F}_q$.

Proof For $x=(x_1,x_2,\cdots,x_n)$, $y=(y_1,y_2,\cdots,y_n)\in C$, where $x_i=a_i+b_iu+c_iv+d_iuv$, $y_i=a'_i+b'_iu+c'_iv+d'_iuv$ with $a_i,b_i,c_i,d_i,a'_i,b'_i,c'_i,d'_i\in\mathbb{F}_q$, for $1\leqslant i\leqslant n$. If C is self-dual, then

$$[x,y]=\sum_{i=1}^{n}(a_ia'_i+(a_ib'_i+a'_ib_i)u+(a_ic'_i+a'_ic_i)v+(a_id'_i+b_ic'_i+c_ib'_i+d_ia'_i)uv)=0.$$

It means that

$$\sum_{i=1}^{n}a_ia'_i=\sum_{i=1}^{n}(a_ib'_i+a'_ib_i)=\sum_{i=1}^{n}(a_ic'_i+a'_ic_i)=\sum_{i=1}^{n}(a_id'_i+b_ic'_i+c_ib'_i+d_ia'_i)=0.$$

On the other hand, according to the definition of Gray map ϕ, we have

$$[\phi(x),\phi(y)]=\sum_{i=1}^{n}(a_ia'_i+(a_ib'_i+a'_ib_i)+(a_ic'_i+a'_ic_i)+(a_id'_i+b_ic'_i+c_ib'_i+d_ia'_i))=0.$$

It implies that $\phi(C^{\perp})\subseteq\phi(C)^{\perp}$. Since the Gray map ϕ is a bijection from R^n to $\mathbb{F}_q^{4n}$, then $\phi(C^{\perp})=\phi(C)^{\perp}$. If C is an LCD code over R, then $C\cap C^{\perp}=\{\mathbf{0}\}$. It follows that $\phi(C\cap C^{\perp})\subseteq\phi(C)\cap\phi(C^{\perp})$. Since ϕ is a bijection from R^n to $\mathbb{F}_q^{4n}$, we find that $\phi(C)\cap\phi(C)^{\perp}=\phi(C)\cap\phi(C^{\perp})=\phi(C\cap C^{\perp})=\{\mathbf{0}\}$. Thus $\phi(C)$ is an LCD code of length $4n$ over $\mathbb{F}_q$.

2 Algebraic structure of double circulant codes

In this section, let n be an odd integer with $\gcd(n,q)=1$. Let $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ with $a_n\neq 0$. Then the reciprocal polynomial $f^*(x)$ of $f(x)$ is defined by $f^*(x)=x^nf(\frac{1}{x})=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$. Furthermore, $f(x)$ is called self-reciprocal if $f^*(x)=f(x)$. Now, the ploynomial $x^n-1\in R[x]$ can be represented in the form

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

over R with $\alpha\in R^*$, where $g_i(x)$ is a self-reciprocal basic irreducible polynomial with degree $2e_i$ for $2\leqslant i\leqslant s$, and $h_j^*(x)$ is the reciprocal basic irreducible polynomial of $h_j(x)$ with degree d_j for $1\leqslant j\leqslant t$. By the CRT, we get

$$\frac{R[x]}{(x^n-1)}\simeq\frac{R[x]}{(x-1)}\oplus(\bigoplus_{i=2}^{s}R[x]/(g_i(x)))\oplus(\bigoplus_{j=1}^{t}(R[x]/(h_j(x))\oplus R[x]/(h_j^*(x))))\simeq$$
$$R\oplus(\bigoplus_{i=2}^{s}\mathbb{F}_{q^{2e_i}}+u\,\mathbb{F}_{q^{2e_i}}+v\,\mathbb{F}_{q^{2e_i}}+uv\,\mathbb{F}_{q^{2e_i}})\oplus(\bigoplus_{j=1}^{t}((\mathbb{F}_{q^{d_j}}+u\mathbb{F}_{q^{d_j}}+v\mathbb{F}_{q^{d_j}}+uv\mathbb{F}_{q^{d_j}})\oplus(\mathbb{F}_{q^{d_j}}+u\mathbb{F}_{q^{d_j}}+v\mathbb{F}_{q^{d_j}}+uv\mathbb{F}_{q^{d_j}})))\,:=$$
$$R\oplus(\bigoplus_{i=2}^{s}R_{2e_i})\oplus(\bigoplus_{j=1}^{t}(R_{d_j}\oplus R_{d_j})).$$

Obviously, all of these are extention rings of R. This decomposition naturally extends to $\left(\frac{R[x]}{(x^n-1)}\right)^2$ as

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

A linear code C of length 2 over $\frac{R[x]}{(x^n-1)}$ can be decomposed in the form of $C\simeq C_1\oplus(\bigoplus_{i=2}^{s}C_i)\oplus(\bigoplus_{j=1}^{t}(C'_j\oplus C''_j))$, where C_1 is a linear code over R of length 2, C_i is a linear code over R_{2e_i} for each $2\leqslant i\leqslant s$, and for each $1\leqslant j\leqslant t$, C'_j and C''_j are both linear codes over R_{d_j} of length 2, which are called the constituents of C.

Theorem 2.1 Let n be a positive odd integer. Assume that the factorization of x^n-1 into basic 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

(i) if q is a power of an odd prime with $q\equiv1\pmod 4$, the total number of self-dual double circulant codes over R is $2\prod_{i=2}^{s}q^{3e_i}(q^{e_i}+1)\prod_{j=1}^{t}q^{3d_j}(q^{d_j}-1)$;

(ii) if q is a power of 2, the total number of self-dual double circulant codes over R is $q^3\prod_{i=2}^{s}q^{3e_i}(q^{e_i}+1)\prod_{j=1}^{t}q^{3d_j}(q^{d_j}-1)$.

Proof (i) We prove it by counting their constituent codes. Using Proposition 1.1 (ii), there are 2 self-dual codes C_1 of length 2 over R, whose generators are $(1,\eta)$, $(1,-\eta)$, where $\eta^2=-1$, $\eta\in\mathbb{F}_q$. For constituent codes C_i of C, suppose that $(1,\beta_i)$ is the generator of C_i, and let $\beta_i=a+ub+vc+uvd\in R_{2e_i}$, then

$$[(1,\beta_i),(1,\beta_i)]_H=1+\beta_i\overline{\beta_i}=0.$$

Hence we get $1+(a+ub+vc+uvd)(a^{q^{e_i}}+ub^{q^{e_i}}+vc^{q^{e_i}}+uvd^{q^{e_i}})=0$, and thus $(1+a^{q^{e_i}+1})+u(ab^{q^{e_i}}+ba^{q^{e_i}})+v(ac^{q^{e_i}}+ca^{q^{e_i}})+uv(ad^{q^{e_i}}+bc^{q^{e_i}}+cb^{q^{e_i}}+da^{q^{e_i}})=0$.

$$\begin{cases}1+a^{q^{e_i}+1}=0,\\ ab^{q^{e_i}}+ba^{q^{e_i}}=0,\\ ac^{q^{e_i}}+ca^{q^{e_i}}=0,\\ ad^{q^{e_i}}+bc^{q^{e_i}}+cb^{q^{e_i}}+da^{q^{e_i}}=0,\end{cases}\Leftrightarrow\begin{cases}N(a)=-1,\\ \mathrm{Tr}(ab^{q^{e_i}})=0,\\ \mathrm{Tr}(ac^{q^{e_i}})=0,\\ \mathrm{Tr}(ad^{q^{e_i}}+bc^{q^{e_i}})=0.\end{cases}$$

By the definition of the norm function from $\mathbb{F}_{q^{2e_i}}$ to $\mathbb{F}_{q^{e_i}}$, there are $q^{e_i}+1$ different choices for a. Similarly, by the definition of the trace function from $\mathbb{F}_{q^{2e_i}}$ to $\mathbb{F}_{q^{e_i}}$, so there are q^{e_i} different choices for b, c and d, respectively. Thus the choices of β_i are equal to $q^{3e_i}(q^{e_i}+1)$.

By what we have already known, 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_{d_j}. Our goal is looking for the total number of (β'_j,β''_j) such that $1+\beta'_j\beta''_j=0$, where $(1,\beta'_j)$ and $(1,\beta''_j)$ are the generators of C'_j and C''_j, respectively. We discuss the choices of (β'_j,β''_j) by its characterization of unit. If $\beta'_j\in R_{d_j}^*$, then $\beta''_j=-\frac{1}{\beta'_j}$, there are $|R_{d_j}^*|=(q^{d_j}-1)q^{3d^j}$ choices for (β'_j,β''_j). If $\beta'_j\in R_{d_j}\setminus R_{d_j}^*$, then $\beta'_j\in\langle u,v\rangle$, it is a contradiction with $1+\beta'_j\beta''_j=0$.

(ii) It follows from (i) by considering Proposition 1.1 (i).

Lemma 2.1 Consider the constituents C_1, C_i, C'_j and C''_j of C, then

(i) C_1 is an LCD code over R with the generator $(1,\eta)$ if and only if $1+\eta^2\in R^*$.

(ii) C_i is an LCD code over R_{2e_i} with the generator $(1,\beta_i)$ if and only if $1+\beta_i\overline{\beta_i}\in R_{2e_i}^*$.

(iii) $C'_j\oplus C''_j$ is an LCD code over R_{d_j} with $C'_j=\langle(1,\beta'_j)\rangle$ and $C''_j=\langle(1,\beta''_j)\rangle$ if and only if $1+\beta'_j\beta''_j\in R_{d_j}^*$.

Proof It suffices to prove (i), because the proofs of (ii) and (iii) are similar to that of (i). Suppose that $1+\eta^2\in R\setminus R^*$, then $[uv(1,\eta),(1,\eta)]=0$, which implies $uv(1,\eta)\in C_1^{\perp}$. It means that $uv(1,\eta)\in C_1^{\perp}\cap C_1$, which means that C_1 is not an LCD code, a contradiction. Conversely, suppose that $1+\eta^2\in R^*$, then $a(1+\eta^2)\neq 0$ for $a\in R\backslash\{0\}$. Hence, $a(1,\eta)\notin C_1^{\perp}$. Because $(1,\eta)$ is a generator of C_1, it follows that $C_1\cap C_1^{\perp}=\{\mathbf{0}\}$. Therefore, C_1 is an LCD code over R.

Theorem 2.2 Let n be a positive odd integer. Assume that the factorization of x^n-1 into basic 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 we have

(i) if q is a power of an odd prime with $q\equiv 1 \pmod 4$, the number of LCD double circulant codes over R is $q^3(q-2)\prod_{i=2}^{s}(q^{8e_i}-q^{7e_i}-q^{6e_i})\cdot\prod_{j=1}^{t}(q^{8d_j}-q^{7d_j}+q^{6d_j})$;

(ii) if q is a power of 2, the number of LCD double circulant codes over R is

$$q^3(q-1)\prod_{i=2}^{s}(q^{8e_i}-q^{7e_i}-q^{6e_i})\cdot\prod_{j=1}^{t}(q^{8d_j}-q^{7d_j}+q^{6d_j}).$$

Proof (i) We can also count the number of LCD double circulant codes by counting constituent codes of C. For the constituent code C_1 of C, let $(1,\eta)$ be the generator of C_1. According to Lemma 2.1 (i), we know that C_1 is an LCD code if and only if $1+\eta^2\in R^*$. Next, we discuss the unit character of η as follows:

If $\eta\in R^*$, we write $\eta=\eta_1+\eta_2u+\eta_3v+\eta_4uv$, where $\eta_1,\eta_2,\eta_3,\eta_4\in\mathbb{F}_q$ and $\eta_1\neq 0$, then $1+\eta^2=(1+\eta_1^2)+2\eta_1\eta_2u+2\eta_1\eta_3v+2(\eta_1\eta_4+\eta_2\eta_3)uv$. Suppose that $1+\eta^2\in R^*$, then we must have $1+\eta_1^2\neq 0$. Therefore there are $(q-3)q^3$ choices for η.

If $\eta\in R\backslash R^*$, then $1+\eta^2\in R^*$. It is easy to see that there are q^3 choices for η.

For the constituent codes C_i of C, let $(1,\beta_i)$ be the generators of C_i with $2\leqslant i\leqslant s$. By Lemma 2.1 (ii), C_i is an LCD code if and only if $1+\beta_i\overline{\beta_i}\in R_{2e_i}^*$. Put $\beta_i=\beta_{i1}+u\beta_{i2}+v\beta_{i3}+uv\beta_{i4}$ with $\beta_{i1},\beta_{i2},\beta_{i3},\beta_{i4}\in\mathbb{F}_{q^{2e_i}}$, then we get $1+\beta_i\overline{\beta_i}=1+\beta_{i1}^{q^{e_i}+1}+u(\beta_{i1}\beta_{i2}^{q^{e_i}}+\beta_{i2}\beta_{i1}^{q^{e_i}})+v(\beta_{i1}\beta_{i3}^{q^{e_i}}+\beta_{i3}\beta_{i1}^{q^{e_i}})+uv(\beta_{i1}\beta_{i4}^{q^{e_i}}+\beta_{i2}\beta_{i3}^{q^{e_i}}+\beta_{i3}\beta_{i2}^{q^{e_i}}+\beta_{i4}\beta_{i1}^{q^{e_i}})$.

If $1+\beta_i\overline{\beta_i}\in R_{2e_i}^*$, then we obtain $1+\beta_{i1}^{q^{e_i}+1}\neq 0$. Therefore, there are $q^{2e_i}-q^{e_i}-1$ different choices for β_{i1}. Thus there are $q^{8e_i}-q^{7e_i}-q^{6e_i}$ different choices for β_i such that C_i is an LCD code.

For the constituent codes $C_j'\oplus C_j''$ of C, let $(1,\beta_j')$ and $(1,\beta_j'')$ be the generators of C_j' and C_j'' with $1\leqslant j\leqslant t$, respectively. By Lemma 2.1 (iii), we get $C_j'\oplus C_j''$ is an LCD code if and only if $1+\beta_j'\beta_j''\in R_{d_j}^*$. Without loss of generality, we discuss the unit character of β_j' as follows:

If $\beta_j'\in R_{d_j}^*$, then $\beta_j''\in-\frac{1}{\beta_j'}+R_{d_j}^*$, we note that $\left|-\frac{1}{\beta_j'}+R_{d_j}^*\right|=|R_{d_j}^*|$. Therefore, in this case, we have $|R_{d_j}^*|^2=[(q^{d_j}-1)q^{3d_j}]^2=q^{8d_j}-2q^{7d_j}+q^{6d_j}$. So there are $q^{8d_j}-2q^{7d_j}+q^{6d_j}$ different choices for (β_j',β_j'').

If $\beta_j'\in R_{d_j}\backslash R_{d_j}^*$, let $\beta_j'=u\beta_{j2}'+v\beta_{j3}'+uv\beta_{j4}'$, $\beta_j''=\beta_{j1}''+u\beta_{j2}''+v\beta_{j3}''+uv\beta_{j4}''$, where $\beta_{j2}',\beta_{j3}',\beta_{j4}',\beta_{j1}'',\beta_{j2}'',\beta_{j3}'',\beta_{j4}''\in\mathbb{F}_{q^{d_j}}$. Then $1+\beta_j'\beta_j''=1+u\beta_{j2}'\beta_{j1}''+v\beta_{j3}'\beta_{j1}''+uv(\beta_{j2}'\beta_{j3}''+\beta_{j3}'\beta_{j2}''+\beta_{j4}'\beta_{j1}'')$, we must have $1+\beta_j'\beta_j''\in R_{d_j}^*$. In this case, the number of (β_j',β_j'') that satisfies $1+\beta_j'\beta_j''\in R_{d_j}^*$ is equal to q^{7d_j}.

Thus there are $q^{8d_j}-q^{7d_j}+q^{6d_j}$ choices for (β_j',β_j'') such that $C_j'\oplus C_j''$ are LCD codes.

(ii) This follows from (i) and the result is proven.

3 Distance bound

Let q be a primitive root modulo n, where n is an odd prime. Since $\mathbb{F}_q$ is a subring of R and $h(x)=x^{n-1}+\cdots+x+1$ is irreducible over $\mathbb{F}_q$. Then we have $x^n-1=(x-1)h(x)$ and $h(x)$ is a basic irreducible polynomial over R.

By the CRT, we have

$$\frac{R[x]}{(x^n-1)}\simeq\frac{R[x]}{(x-1)}\oplus\frac{R[x]}{(h(x))}\simeq$$

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

Let $\mathscr{R}$ be the ring $\frac{R[x]}{(h(x))}$, so R is a subring of $\mathscr{R}$.

Lemma 3.1 If a nonzero vector $z=(e,f)\in C_a$ and f is not generated by $h(x)$, where C_a is a double circulant code over R, then there are at most q^{3n+1} generators $(1,a)$ such that $z\in C_a$.

Proof By the CRT, $(e,f)\simeq(e_1,f_1)\oplus(e_2,f_2)$. Since $(e,f)\in C_a$, then $f=ea$, $f_1=e_1a_1$ and $f_2=e_2a_2$, where $e_1, f_1, a_1\in R$ and $e_2, f_2, a_2\in\mathscr{R}$. Let $a_1=a_{11}+ua_{12}+va_{13}+uva_{14}$, $a_2=a_{21}+ua_{22}+va_{23}+uva_{24}$, where $a_{11}, a_{12}, a_{13}, a_{14}\in\mathbb{F}_q$, $a_{21}, a_{22}, a_{23}, a_{24}\in\mathbb{F}_{q^{n-1}}$. Now, writing $R'_1=R$, $R'_2=\mathscr{R}$, consider two constituents of C_a, we discuss the unit character of e_i for $1\leqslant i\leqslant 2$ as follows:

① If $e_1=0$, $f_1=e_1a_1$, then a_1 is an arbitrary element in R, thus there are q^4 different choices for a_1.

② If $e_i\in {R'_i}^{*}$ for $1\leqslant i\leqslant 2$, there exists only one solution for $a_i=\frac{f_i}{e_i}$.

③ If $e_i\in\langle(u,v)\rangle\backslash\{0\}$ for $1\leqslant i\leqslant 2$, let $e_i=ue_{i2}+ve_{i3}+uve_{i4}$ with $(e_{i2}, e_{i3}\, e_{i4})\neq(0,0,0)$ and $f_i=uf_{i2}+vf_{i3}+uvf_{i4}$ for $1\leqslant i\leqslant 2$, where $e_{12}, e_{13}, e_{14}, f_{12}, f_{13}, f_{14}\in\mathbb{F}_q$, $e_{22}, e_{23}, e_{24}, f_{22}, f_{23}, f_{24}\in\mathbb{F}_{q^{n-1}}$. Since $f_i=e_ia_i$, we have

$$uf_{i2}+vf_{i3}+uvf_{i4}=(ue_{i2}+ve_{i3}+uve_{i4})(a_{i1}+ua_{i2}+va_{i3}+uva_{i4})=ue_{i2}a_{i1}+ve_{i3}a_{i1}+uv(e_{i2}a_{i3}+e_{i3}a_{i2}+e_{i4}a_{i1}).$$

Through a comparison of coefficients, we have $f_{i2}=e_{i2}a_{i1}$, $f_{i3}=e_{i3}a_{i1}$, $f_{i4}=e_{i2}a_{i3}+e_{i3}a_{i2}+e_{i4}a_{i1}$. In the case of $e_{12}=0$, $e_{13}=0$, $e_{14}\neq 0$, then $a_{11}=\frac{f_{14}}{e_{14}}$, $a_{12}, a_{13}, a_{14}\in\mathbb{F}_q$. Therefore, there are at most q^3 choices for a_1. Similarly, there are at most q^{3n-3} choices for a_1 when $e_{22}=e_{23}=0, e_{24}\neq 0$.

In summary, there are at most q^4 different choices for a_1 and at most q^{3n-3} different choices for a_2. Then the result follows.

Lemma 3.2 If a nonzero vector $z=(e,f)\in C_a$ and f is not generated by $h(x)$, where C_a is a self-dual double circulant code over R. Then

(i) if q is a power of an odd prime with $q\equiv 1 \pmod 4$, there are at most $2q^{\frac{3n-3}{2}}$ generators $(1,a)$ such that $z\in C_a$.

(ii) if q is a power of 2, there are at most $q^{\frac{3n+3}{2}}$ generators $(1,a)$ such that $z\in C_a$.

Proof Using the same notations as Lemma 3.1.

(i) Based on the proof of Lemma 3.1. In the first constituent of C_a, $[(1,a_1),(1,a_1)]=1+a_1^2=0$. By Proposition 1.1 (ii), then there are 2 choices for a_1.

In the second constituent of C_a,

$$[(1,a_2)(1,a_2)]_H=1+a_2\overline{a_2}=0,$$

then

$$\begin{cases}1+a_{21}^{q^{\frac{n-1}{2}}+1}=0,\\ a_{21}a_{22}^{q^{\frac{n-1}{2}}}+a_{22}a_{21}^{q^{\frac{n-1}{2}}}=0,\\ a_{21}a_{23}^{q^{\frac{n-1}{2}}}+a_{23}a_{21}^{q^{\frac{n-1}{2}}}=0,\\ a_{21}a_{24}^{q^{\frac{n-1}{2}}}+a_{22}a_{23}^{q^{\frac{n-1}{2}}}+a_{23}a_{22}^{q^{\frac{n-1}{2}}}+a_{24}a_{21}^{q^{\frac{n-1}{2}}}=0,\end{cases} \Longleftrightarrow \begin{cases}N(a_{21})=-1,\\ \mathrm{Tr}(a_{21}a_{22}^{q^{\frac{n-1}{2}}})=0,\\ \mathrm{Tr}(a_{21}a_{23}^{q^{\frac{n-1}{2}}})=0,\\ \mathrm{Tr}(a_{21}a_{24}^{q^{\frac{n-1}{2}}}+a_{22}a_{23}^{q^{\frac{n-1}{2}}})=0.\end{cases}$$

It means that there are $1+q^{\frac{n-1}{2}}$, $q^{\frac{n-1}{2}}$, $q^{\frac{n-1}{2}}$, $q^{\frac{n-1}{2}}$ choices for a_{21}, a_{22}, a_{23}, a_{24}, respectively. Using the proof of Lemma 3.1, there are $q^{\frac{3n-3}{2}}$ choices for a_2.

(ii) This follows from (i) and Proposition 1.1 (i), the result follows.

Lemma 3.3 If a nonzero vector $z=(e,f)\in C_a$ and f is not generated by $h(x)$, where C_a is an

LCD double circulant code over R. Then

(i) if q is a power of an odd prime with $q\equiv 1 \pmod 4$, there are at most $(q-2)q^{3n}$ generators $(1,a)$ such that $z\in C_a$.

(ii) if q is a power of 2, there are at most $(q-1)q^{3n}$ generators $(1,a)$ such that $z\in C_a$.

Proof Using the same notations as Lemma 3.1.

(i) Based on the proof of Lemma 3.1, for the first constituent of C_a, it is an LCD code if and only if $1+a_1^2\in R^*$. If $1+a_1^2\in R^*$, then $1+a_{11}^2\neq 0$, a_{12}, a_{13}, $a_{14}\in \mathbb{F}_q$. Thus there are $(q-2)q^3$ choices for a_1.

For the second constituent of C_a, it is an LCD code if and only if $1+a_2\overline{a_2}\in \mathcal{R}^*$. if $1+a_2\overline{a_2}\in \mathcal{R}^*$, then we get $1+a_{21}{}^{q^{\frac{n-1}{2}}+1}\neq 0$, a_{22}, a_{23}, $a_{24}\in \mathbb{F}_{q^{n-1}}$. It means that there are $q^{n-1}-q^{\frac{n-1}{2}}-1$, q^{n-1}, q^{n-1}, q^{n-1} choices for a_{21}, a_{22}, a_{23}, a_{24}, respectively. Using the proof of Lemma 3.1, there are q^{3n-3} choices for a_2.

(ii) This follows from (i) and Proposition 1.1 (i).

If $C(n)$ is a family of codes with parameters $[n, k_n, d_n]$ over $\mathbb{F}_q$. We say that a family of codes is good if $\rho\delta>0$, where $\rho=\limsup\limits_{n\to\infty}\frac{k_n}{n}$ is rate, and $\delta=\liminf\limits_{n\to\infty}\frac{d_n}{n}$ is relative distance.

In number theory, Artin's conjecture on primitive roots[12] states that a given integer q which is neither a perfect square nor -1 is a primitive root modulo infinitely many primes. This was proved conditionally under the generalized Riemann hypothesis (GRH)[13].

Recall the q-ary entropy function defined for $0\leqslant t\leqslant \frac{q-1}{q}$ by Ref. [14, Chapter 2.10.3]

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

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.

Now we are ready to present the main results.

Theorem 3.1 Let n be an odd prime with $n>q$, and q be a primitive root modulo n. The family of Gray images of self-dual (resp. LCD) double circulant codes over R of length $2n$, of relative distance δ, and rate 1/2, satisfies $H_q(\delta)\geqslant\frac{1}{16}$ (resp. $H_q(\delta)\geqslant\frac{1}{8}$). In particular, both families of codes are good.

Proof Let p_1 be an odd prime, and Ω_n be the size of the family codes. The numberical value of λ_n is equal to the results of Lemmas 3.2 and 3.3, respectively. For $n\to\infty$, Using Theorems 2.1 and 2.3, we obtain Tab. 1 as follows.

Tab. 1 Enumeration results of self-dual and LCD double circulant codes

	self-dual		LCD	
	Ω_n	λ_n	Ω_n	λ_n
$q=p_1{}^l$	$2q^{2n-2}+2q^{\frac{3n-3}{2}}$	$2q^{\frac{3n-3}{2}}$	$(q-2)(q^{4n-1}-q^{\frac{7n-1}{2}}-q^{3n})$	$(q-2)q^{3n}$
$q=2^l$	$q^{2n+1}+q^{\frac{3n+3}{2}}$	$q^{\frac{3n+3}{2}}$	$(q-1)(q^{4n-1}-q^{\frac{7n-1}{2}}-q^{3n})$	$(q-1)q^{3n}$

Assume that we can prove that $\Omega_n>\lambda_n B(d_n)$ is n large enough, where $B(r)$ denotes the number of vectors in R^{2n} with Hamming weight of their $\mathbb{F}_q$ image $<r$. This would imply, by Lemmas 3.2 and 3.3, that there are codes of length $2n$ in the family with minimum Hamming distance of their $\mathbb{F}_q$ image $\geqslant d_n$.

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 suppose that a growth of the form $d_n \sim 8\delta_0 n$, then, using an entropic estimate for $B(d_n) \sim q^{8nH_q(\delta_0)}$ [14, Lemma 2.10.3] yields, with the said values of Ω_n and λ_n the estimate $H_q(\delta_0) = \frac{1}{16}$ for self-dual codes and $H_q(\delta_0) = \frac{1}{8}$ for LCD codes. The result follows by observing that, by definition of δ, we have $\delta \geqslant \delta_0$.

4 Conclusion

In this paper, we mainly studied self-dual and LCD double circulant codes of length $2n$ over the ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$. The exact enumerations of self-dual and LCD double circulant codes have been given. This paper have clearly proved that these two families of image codes are asymptotically good over $\mathbb{F}_q$. Moreover, the complicated proofs and calculations of this ring might be worthy studying other rings or defining by many variables.

References

[1] MASSEY J L. Linear codes with complementary duals [J]. Discrete Mathematics, 1992,106-107: 337-342.

[2] GÜNERI C, ÖZKAYA B, SOLÉ P. Quasi-cyclic complementary dual codes[J]. Finite Fields and Their Applications, 2016, 42: 67-80.

[3] ALAHMADI A, GÜNERI C, ÖZKAYA B, et al. On self-dual double negacirculant codes [J]. Discrete Applied Mathematics, 2017, 222: 205-212.

[4] ALAHMADI A, OZDEMIR F, SOLÉ P. On self-dual double circulant codes [J]. Designs, Codes and Cryptography, 2018, 86:1257-1265.

[5] SHI M J, HUANG D T, SOK L, et al. Double circulant self-dual and LCD codes over Galois rings [EB/OL]. [2018-02-01] https://arxiv. org/abs/1801. 06624.

[6] SHI M J, QIAN L Q, SOLÉ P. On self-dual negacirculant codes of index two and four[J]. Designs, Codes and Cryptography, 2018, 86: 2485-2494.

[7] LIU Y, SHI M J, SOLÉ P. Two-weight and three-weight codes from trace codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$ [J]. Discrete Mathematics, 2018, 341: 350-357.

[8] ZHU S X, KAI X S. (1-uv)-constacyclic codes over $\mathbb{F}_p+u\mathbb{F}_p+v\mathbb{F}_p+uv\mathbb{F}_p$[J]. Journal of Systems Science Complexity, 2014, 27(4): 811-816.

[9] LING S, SOLÉ P. On the algebraic structure of quasi-cyclic codes Ⅰ: Finite fields[J]. IEEE Transactions on Information Theory, 2001, 47: 2751-2760.

[10] JIA Y. On quasi-twisted codes over finite fields[J]. Finite Fields and Their Applications, 2012, 18: 237-257.

[11] LING S, SOLÉ P. On the algebraic structure of quasi-cyclic codes Ⅱ: Chain rings[J]. Designs, Codes and Cryptography, 2003, 30(1): 113-130.

[12] MOREE P. Artin's primitive root conjecture a survey [J]. Integers, 2012, 10(6): 1305-1416.

[13] HOOLEY C. On Artin's conjecture[J]. Journal Für Die Reine Und Angewandte Mathematik, 1967, 225: 209-220.

[14] HUFFMAN W C, PLESS V. Fundamentals of Error-Correcting Codes [M]. Cambridge: Cambridge University Press, 2003.