Eighth Power Residue Double Circulant Self-Dual Codes

Changsong Jiang[1,3], Yuhua Sun[1,2], and Xueting Liang[1]
(Corresponding author: Yuhua Sun)

College of Science, China University of Petroleum[1]
Qingdao, Shandong 266580, China
Provincial Key Laboratory of Applied Mathematics, Putian University, Putian, Fujian 351100, China[2]
School of Computer Science and Engineering, University of Electronic Science and Technology of China[3]
(Email: sunyuhua_1@163.com)

(Received Mar. 1, 2019; Revised and Accepted Sept. 16, 2019; First Online Jan. 23, 2020)

Abstract

Self-dual codes are one of the most important classes of linear codes. Power residue classes are widely used in the constructions of linear codes and pseudo-random sequences. In this paper, we give new constructions of self-dual codes over GF(2) and GF(4) by eighth power residues. We get multiple pure double circulant codes and bordered double circulant codes. Some of these new self-dual codes have large minimum distances.

Keywords: Cyclotomic Number; Double Circulant Code; Eighth Power Residues; Self-Dual Code

1 Introduction

The famous paper "A mathematical theory of communication" [26] by Shannon marked the beginning of coding theory. Codes with good properties have many applications in cryptography and communication systems. Most of the codes constructed in the initial stage were binary codes. Now, codes over finite fields and over finite rings are very common in both mathematical and engineering literatures. Thanks to having neat mathematical structure and being easy to code and decode, linear codes play a decisive role in coding theory. It is worth noting that, among linear codes, there is one class of special codes, *i.e.*, self-dual codes which are widely used in data transmission and have become important tools to construct quantum error-correcting codes. Therefore various methods of construction and analysis of self-dual codes have been presented by coding researchers and various classes of linear codes with self-dual property appeared successively in many literatures. For example, readers can refer to [1–6, 9, 11, 17–19, 22, 24, 25, 28, 29] or can also refer to the survey paper [13] for the advances of early research in this field. It is well known that power residue classes have become an important tool to construct stream cipher sequences with good pseudo-random properties (for example, see [7, 23, 27]). In fact, they have also been used to construct error-correcting codes, and a very interesting method of constructing linear codes or self-dual codes is combining double circulant matrices and residue classes to give the generator matrix of codes(for example, see [8, 10, 12, 16, 21])). But, in most of the relevant literatures at present, the residue being used to construct codes are mainly quadratic residue.

Recently, Zhang and Ge introduced fourth power residue double circulant and obtained several new infinite families of classes of self-dual codes over GF(2), GF(3), GF(4), GF(8), GF(9) [30]. Some of these codes have better minimum weight than previously known codes. In this paper, inspired by their methods, we construct double circulant self-dual codes by by higher power residues, especially eighth power residues. We give new constructions of self-dual codes over GF(2) and GF(4) by prime p of the form $16f + 9$, and some of these codes have good parameters. Examples of such codes are binary self-dual [82, 41, 14] code, quaternary self-dual [82, 41, 14] code and quaternary self-dual [84, 42, 12] code. All computation have been done by MATLAB R2017b and MAGMA V2.12 on a 2.50 GHz CPU.

The paper is organized as follows. In Section 2, we give the relevant knowledge of double circulant codes and self-dual codes. In Section 3, we describe the detailed process of constructing linear codes by eighth power residues and discuss the parameter conditions satisfying self-dual property. Section 4 considers the constructions over GF(2) and GF(4) respectively. A conclusion is given in Section 5.

2 Preliminaries

Self-Dual Codes. A linear $[n, k]$ code C of length n and dimension k over the Galois field with q elements GF(q) is a linear subspace of dimension k of

$GF(q)^n$, where q is a prime power. An element of the code C is called a codeword of C. A generator matrix of C is a matrix whose rows generate C. Let $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$ be two codewords of $GF(q)^n$. The Euclidean inner product is defined by $(x, y) = \sum_{i=1}^{n} x_i y_i$. For a linear code C, the code $C^\perp = \{x \in GF(q)^n | (x, c) = 0 \text{ for all } c \in C\}$ is called its Euclidean dual code. And we say C is self-orthogonal if $C \subseteq C^\perp$ and C is self-dual if $C = C^\perp$.

Definition 1. *[30]: Let $P_n(R)$ and $B_n(R)$ be codes with generator matrices of the form*

$$\begin{pmatrix} I_n & R \end{pmatrix} \tag{1}$$

and

$$\left(\begin{array}{c|cccc} & \alpha & 1 & \cdots & 1 \\ & -1 & & & \\ I_{n+1} & \vdots & & R & \\ & -1 & & & \end{array}\right) \tag{2}$$

respectively, where $\alpha \in GF(q)$, I is the identity matrix and R is an $n \times n$ circulant matrix. An n by n circulant matrix has the form

$$\begin{pmatrix} r_0 & r_1 & r_2 & \cdots & r_{n-1} \\ r_{n-1} & r_0 & r_1 & \cdots & r_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{pmatrix} \tag{3}$$

so that each successive row is a cyclic shift of the previous one. The codes $P_n(R)$ and $B_n(R)$ are called pure double circulant and bordered double circulant, respectively.

The (Hamming) distance between two codewords x and y denoted by $d(x, y)$, is defined to be the number of places at which x and y differ. The Hamming weight of a codeword is the number of non-zero components. And the minimum distance $d(C)$ of C is defined by $d(C) = \min\{d(x, y) | x \neq y \in C\}$, and it also equals to the minimum weight of the codewords of C except for 0.

Let C be a self-dual code over $GF(q)$ of length n and minimum distance d(C). Then the following bounds are known in [14, 22, 24, 25]. For binary self-dual codes:

$$d(C) \leq \begin{cases} 4[\frac{n}{24}] + 4, & if\ n \neq 22 \pmod{24}, \\ 4[\frac{n}{24}] + 6, & if\ n = 22 \pmod{24}. \end{cases}$$

The minimum distance of a self-dual ternary code C satisfies: $d(C) \leq 3[\frac{n}{12}] + 3$ and for quaternary Euclidean self-dual codes: $d(C) \leq 4[\frac{n}{12}] + 4$. The code C is called extremal if the equality holds. If a code has the highest possible minimum weight for its length and dimension, we call it optimal.

In this paper, we construct a circulant matrix R by eighth power residue and get a necessary condition such that the corresponding codes are self-dual. Further, under this condition, we get two kinds of codes called pure eighth power residue double circulant code and bordered eighth power residue double circulant code, respectively. Some codes have large minimum distances, and almost reach the bounds of the minimum distance.

3 Generator Matrices of Eighth Power Residue Double Circulant Self-Dual Codes

Let $p = Nf + 1$ be a prime with a fixed primitive root g over $GF(q)$. We define the Nth cyclotomic classes $C_0, C_1, ..., C_{N-1}$ of $GF(p)$ by

$$C_i = \left\{ g^{jN+i} | 0 \leq j \leq f - 1 \right\},$$

where $0 \leq i \leq N - 1$. Then we call C_0 is the Nth power residues modulo p, and $C_i = g^i C_0$ where $0 \leq i \leq N - 1$. Define the cyclotomic number (i, j) of order N to be the number of integers $n \pmod{p}$ which satisfy

$$n \equiv g^{16s+i}, \quad 1 + n \equiv g^{16t+j} \pmod{p},$$

where s, t in $\{0, 1, 2, ..., f - 1\}$.

In order to give the necessary conditions, we give the eighth power residue cyclotomic numbers and derive the relationships between them when p is an odd prime of the form $16l + 9$.

Lemma 1. *[15]: Let $p = ef + 1$ be an odd prime. Then*

1) $(i, j)_e = (i', j')_e$, when $i \equiv i' \pmod{e}$ and $j \equiv j' \pmod{e}$.

2) $$(i, j)_e = (e - i, j - i)_e = \begin{cases} (j, i)_e; & if\ f\ even. \\ (j + \frac{e}{2}, i + \frac{e}{2})_e; & if\ f\ odd. \end{cases}$$

3) $\sum_{i=0}^{e-1} (i, j)_e = f - \delta_j$, where $\delta_j = 1$ if $j \equiv 0 \pmod{e}$; otherwise $\delta_j = 0$.

Let p be a prime of the form $p = 16l + 9$, where l is a positive integer. From Lemma 1, the relationships of cyclotomic numbers of order 8 are

$$\begin{cases} (0,0)_8 = (4,0)_8 = (4,4)_8, & (0,1)_8 = (3,7)_8 = (5,4)_8, \\ (0,2)_8 = (2,6)_8 = (6,4)_8, & (0,3)_8 = (1,5)_8 = (7,4)_8, \\ (0,4)_8, & (0,5)_8 = (1,4)_8 = (7,3)_8, \\ (0,6)_8 = (2,4)_8 = (6,2)_8, & (0,7)_8 = (3,4)_8 = (5,1)_8, \\ \multicolumn{2}{l}{(1,0)_8 = (3,3)_8 = (4,1)_8 = (4,5)_8 = (5,0)_8 = (7,7)_8,} \\ \multicolumn{2}{l}{(1,1)_8 = (3,0)_8 = (4,3)_8 = (4,7)_8 = (5,5)_8 = (7,0)_8,} \\ \multicolumn{2}{l}{(1,2)_8 = (2,7)_8 = (3,6)_8 = (5,3)_8 = (6,5)_8 = (7,1)_8,} \\ \multicolumn{2}{l}{(1,3)_8 = (1,6)_8 = (2,5)_8 = (6,3)_8 = (7,2)_8 = (7,5)_8,} \\ \multicolumn{2}{l}{(1,7)_8 = (2,3)_8 = (3,5)_8 = (5,2)_8 = (6,1)_8 = (7,6)_8,} \\ \multicolumn{2}{l}{(2,0)_8 = (2,2)_8 = (4,2)_8 = (4,6)_8 = (6,0)_8 = (6,6)_8,} \\ \multicolumn{2}{l}{(2,1)_8 = (3,1)_8 = (3,2)_8 = (5,6)_8 = (5,7)_8 = (6,7)_8.} \end{cases} \tag{4}$$

Remark 1. *For simplicity, in the next we denote*

$$\begin{cases} A := (0,0)_8, & B := (0,1)_8, & C := (0,2)_8, \\ D := (0,3)_8, & E := (0,4)_8, & F := (0,5)_8, \\ G := (0,6)_8, & H := (0,7)_8, & I := (1,0)_8, \\ J := (1,1)_8, & K := (1,2)_8, & L := (1,3)_8, \\ M := (1,7)_8, & N := (2,0)_8, & O := (2,1)_8. \end{cases} \tag{5}$$

Let $p \equiv 1 (\mathrm{mod}\ 8)$ be a prime. Its 8th cyclotomic classes are $C_0, C_1, C_2, C_3, C_4, C_5, C_6$ and C_7. Suppose $m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8$ are the elements of $\mathrm{GF}(q)$. Then we construct the matrix $C_p(m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8)$ which is a $p \times p$ matrix on $\mathrm{GF}(q)$. The component c_{ij}, $1 \le i, j \le p$, defines

$$\begin{cases} m_0; & \text{if} \quad j = i, \\ m_1; & \text{if} \quad j - i \in C_0, \\ m_2; & \text{if} \quad j - i \in C_1, \\ m_3; & \text{if} \quad j - i \in C_2, \\ m_4; & \text{if} \quad j - i \in C_3, \\ m_5; & \text{if} \quad j - i \in C_4, \\ m_6; & \text{if} \quad j - i \in C_5, \\ m_7; & \text{if} \quad j - i \in C_6, \\ m_8; & \text{if} \quad j - i \in C_7. \end{cases} \tag{6}$$

Let I_n be the identity matrix and J_n be the all-one square matrix, so that $C_p(1,0,0,0,0,0,0,0,0) = I_p$ and $C_p(1,1,1,1,1,1,1,1,1) = J_p$. Denote

$$\begin{array}{ll} A_1 := C_p(0,1,0,0,0,0,0,0,0), & A_2 := C_p(0,0,1,0,0,0,0,0,0), \\ A_3 := C_p(0,0,0,1,0,0,0,0,0), & A_4 := C_p(0,0,0,0,1,0,0,0,0), \\ A_5 := C_p(0,0,0,0,0,1,0,0,0), & A_6 := C_p(0,0,0,0,0,0,1,0,0), \\ A_7 := C_p(0,0,0,0,0,0,0,1,0), & A_8 := C_p(0,0,0,0,0,0,0,0,1). \end{array} \tag{7}$$

And the construction of the $n \times n$ circulant matrix R is given as follows:

$$\begin{aligned} R = m_0 I_p + m_1 A_1 + m_2 A_2 + m_3 A_3 + m_4 A_4 + \\ m_5 A_5 + m_6 A_6 + m_7 A_7 + m_8 A_8 \end{aligned} \tag{8}$$

Lemma 2. *Let $p = 16l + 9$ be a prime, then the matrices in equation (7) have the following relationships.*

$$\begin{aligned}
& A_1 = A_5^t, A_2 = A_6^t, A_3 = A_7^t, A_4 = A_8^t, \\
A_1^2 &= AA_1 + BA_2 + CA_3 + DA_4 + EA_5 + FA_6 + GA_7 + HA_8, \\
A_2^2 &= HA_1 + AA_2 + BA_3 + CA_4 + DA_5 + EA_6 + FA_7 + GA_8, \\
A_3^2 &= GA_1 + HA_2 + AA_3 + BA_4 + CA_5 + DA_6 + EA_7 + FA_8, \\
A_4^2 &= FA_1 + GA_2 + HA_3 + AA_4 + BA_5 + CA_6 + DA_7 + EA_8, \\
A_5^2 &= EA_1 + FA_2 + GA_3 + HA_4 + AA_5 + BA_6 + CA_7 + DA_8, \\
A_6^2 &= DA_1 + EA_2 + FA_3 + GA_4 + HA_5 + AA_6 + BA_7 + CA_8, \\
A_7^2 &= CA_1 + DA_2 + EA_3 + FA_4 + GA_5 + HA_6 + AA_7 + BA_8, \\
A_8^2 &= BA_1 + CA_2 + DA_3 + EA_4 + FA_5 + GA_6 + HA_7 + AA_8, \\
A_1A_2 &= A_2A_1 = IA_1 + JA_2 + KA_3 + LA_4 + FA_5 + DA_6 + LA_7 + MA_8, \\
A_1A_3 &= A_3A_1 = NA_1 + OA_2 + NA_3 + MA_4 + GA_5 + LA_6 + CA_7 + KA_8, \\
A_1A_4 &= A_4A_1 = JA_1 + OA_2 + OA_3 + IA_4 + HA_5 + MA_6 + KA_7 + BA_8, \\
A_1A_5 &= A_5A_1 = (2l+1)I_p + AA_1 + IA_2 + AA_3 + JA_4 + AA_5 + IA_6 \\
&\qquad + NA_7 + JA_8, \\
A_1A_6 &= A_6A_1 = IA_1 + HA_2 + MA_3 + KA_4 + BA_5 + JA_6 + OA_7 + OA_8, \\
A_1A_7 &= A_7A_1 = NA_1 + MA_2 + GA_3 + LA_4 + CA_5 + KA_6 + NA_7 + OA_8, \\
A_1A_8 &= A_8A_1 = JA_1 + AA_2 + LA_3 + FA_4 + DA_5 + LA_6 + MA_7 + IA_8, \\
A_2A_3 &= A_3A_2 = MA_1 + IA_2 + JA_3 + KA_4 + LA_5 + FA_6 + DA_7 + LA_8, \\
A_2A_4 &= A_4A_2 = KA_1 + NA_2 + OA_3 + NA_4 + MA_5 + GA_6 + LA_7 + CA_8, \\
A_2A_5 &= A_5A_2 = BA_1 + JA_2 + OA_3 + OA_4 + IA_5 + HA_6 + MA_7 + KA_8, \\
A_2A_6 &= A_6A_2 = JA_1 + AA_2 + IA_3 + NA_4 + JA_5 + AA_6 + IA_7 + NA_8, \\
A_2A_7 &= A_7A_2 = OA_1 + IA_2 + AA_3 + MA_4 + KA_5 + BA_6 + JA_7 + OA_8, \\
A_2A_8 &= A_8A_2 = OA_1 + NA_2 + MA_3 + GA_4 + LA_5 + CA_6 + KA_7 + NA_8, \\
A_3A_4 &= A_4A_3 = LA_1 + MA_2 + IA_3 + JA_4 + KA_5 + LA_6 + FA_7 + DA_8, \\
A_3A_5 &= A_5A_3 = CA_1 + KA_2 + NA_3 + OA_4 + NA_5 + MA_6 + GA_7 + LA_8, \\
A_3A_6 &= A_6A_3 = KA_1 + BA_2 + JA_3 + OA_4 + OA_5 + IA_6 + HA_7 + MA_8, \\
A_3A_7 &= A_7A_3 = (2l+1)I_p + NA_1 + JA_2 + AA_3 + IA_4 + NA_5 + JA_6 \\
&\qquad + AA_7 + IA_8, \\
A_3A_8 &= A_8A_3 = OA_1 + OA_2 + IA_3 + HA_4 + MA_5 + KA_6 + BA_7 + JA_8, \\
A_4A_5 &= A_5A_4 = DA_1 + MA_2 + LA_3 + IA_4 + JA_5 + KA_6 + LA_7 + FA_8, \\
A_4A_6 &= A_6A_4 = LA_1 + CA_2 + KA_3 + NA_4 + OA_5 + NA_6 + MA_7 + GA_8, \\
A_4A_7 &= A_7A_4 = MA_1 + KA_2 + BA_3 + JA_4 + OA_5 + OA_6 + IA_7 + HA_8, \\
A_4A_8 &= A_8A_4 = (2l+1)I_p + IA_1 + NA_2 + JA_3 + AA_4 + IA_5 + NA_6 \\
&\qquad + JA_7 + AA_8, \\
A_5A_6 &= A_6A_5 = FA_1 + DA_2 + LA_3 + MA_4 + IA_5 + JA_6 + KA_7 + LA_8, \\
A_5A_7 &= A_7A_5 = GA_1 + LA_2 + CA_3 + KA_4 + NA_5 + OA_6 + NA_7 + MA_8, \\
A_5A_8 &= A_8A_5 = HA_1 + MA_2 + KA_3 + BA_4 + JA_5 + OA_6 + OA_7 + IA_8, \\
A_6A_7 &= A_7A_6 = LA_1 + FA_2 + DA_3 + LA_4 + MA_5 + IA_6 + JA_7 + KA_8, \\
A_6A_8 &= A_8A_6 = MA_1 + GA_2 + LA_3 + CA_4 + KA_5 + NA_6 + OA_7 + NA_8, \\
A_7A_8 &= A_8A_7 = KA_1 + LA_2 + FA_3 + DA_4 + LA_5 + MA_6 + IA_7 + JA_8.
\end{aligned} \tag{9}$$

Proof. The proof is straightforward from the definition of A_i and lemma 1. □

Lemma 3. *If $p = 16l + 9$ is a prime, then*

$$\begin{aligned} RR^t = \alpha_0 I_p + \alpha_1 A_1 + \alpha_2 A_2 + \alpha_3 A_3 + \alpha_4 A_5 + \\ \alpha_5 A_5 + \alpha_6 A_6 + \alpha_7 A_7 + \alpha_8 A_8 \end{aligned} \tag{10}$$

where

$$\begin{aligned}
\alpha_0 &= m_0^2 + \tfrac{p-1}{8}(m_1^2 + m_2^2 + m_3^2 + m_4^2 + m_5^2 + m_6^2 + m_7^2 + m_8^2), \\
\alpha_1 &= \alpha_5 = (m_0m_1 + m_0m_5) + (m_1^2 + m_1m_5 + m_5^2)A \\
&\quad + (m_1m_2 + m_4m_8 + m_5m_6)B + (m_1m_3 + m_3m_7 + m_5m_7)C \\
&\quad + (m_1m_4 + m_2m_6 + m_5m_8)D + m_1m_5E \\
&\quad + (m_1m_6 + m_2m_5 + m_4m_8)F + (m_1m_7 + m_3m_5 + m_3m_7)G \\
&\quad + (m_1m_8 + m_2m_6 + m_4m_5)H \\
&\quad + (m_1m_2 + m_1m_6 + m_2m_5 + m_4^2 + m_5m_6 + m_8^2)I \\
&\quad + (m_1m_4 + m_1m_8 + m_2^2 + m_4m_5 + m_5m_8 + m_6^2)J \\
&\quad + (m_2m_3 + m_2m_8 + m_3m_8 + m_4m_6 + m_4m_7 + m_6m_7)K \\
&\quad + (m_2m_4 + m_2m_7 + m_3m_6 + m_3m_8 + m_4m_7 + m_6m_8)L \\
&\quad + (m_2m_7 + m_2m_8 + m_3m_4 + m_3m_6 + m_4m_6 + m_7m_8)M \\
&\quad + (m_1m_3 + m_1m_7 + m_3^2 + m_3m_5 + m_5m_7 + m_7^2)N \\
&\quad + (m_2m_3 + m_2m_4 + m_3m_4 + m_6m_7 + m_6m_8 + m_7m_8)O, \\
\alpha_2 &= \alpha_6 = (m_0m_2 + m_0m_6) + (m_2^2 + m_2m_6 + m_6^2)A \\
&\quad + (m_1m_5 + m_2m_3 + m_6m_7)B + (m_2m_4 + m_4m_8 + m_6m_8)C \\
&\quad + (m_1m_6 + m_2m_5 + m_3m_7)D + m_2m_6E \\
&\quad + (m_1m_5 + m_2m_7 + m_3m_6)F + (m_2m_8 + m_4m_6 + m_4m_8)G \\
&\quad + (m_1m_2 + m_3m_7 + m_5m_6)H \\
&\quad + (m_1^2 + m_2m_3 + m_2m_7 + m_3m_6 + m_5^2 + m_6m_7)I \\
&\quad + (m_1m_2 + m_1m_6 + m_2m_5 + m_3^2 + m_5m_6 + m_7^2)J \\
&\quad + (m_1m_3 + m_1m_4 + m_3m_4 + m_5m_7 + m_5m_8 + m_7m_8)K \\
&\quad + (m_1m_4 + m_1m_7 + m_3m_5 + m_3m_8 + m_4m_7 + m_5m_8)L \\
&\quad + (m_1m_3 + m_1m_8 + m_3m_8 + m_4m_5 + m_4m_7 + m_5m_7)M \\
&\quad + (m_2m_4 + m_2m_8 + m_4^2 + m_4m_6 + m_6m_8 + m_8^2)N \\
&\quad + (m_1m_7 + m_1m_8 + m_3m_4 + m_3m_5 + m_4m_5 + m_7m_8)O, \\
\alpha_3 &= \alpha_7 = (m_0m_3 + m_0m_7) + (m_3^2 + m_3m_7 + m_7^2)A \\
&\quad + (m_2m_6 + m_3m_4 + m_7m_8)B + (m_1m_5 + m_1m_7 + m_3m_5)C \\
&\quad + (m_2m_7 + m_3m_6 + m_4m_8)D + m_3m_7E \\
&\quad + (m_2m_6 + m_3m_8 + m_4m_7)F + (m_1m_3 + m_1m_5 + m_5m_7)G \\
&\quad + (m_2m_3 + m_4m_8 + m_6m_7)H \\
&\quad + (m_2^2 + m_3m_4 + m_3m_8 + m_4m_7 + m_6^2 + m_7m_8)I \\
&\quad + (m_2m_3 + m_2m_7 + m_3m_6 + m_4^2 + m_6m_7 + m_8^2)J \\
&\quad + (m_1m_6 + m_1m_8 + m_2m_4 + m_2m_5 + m_4m_5 + m_6m_8)K \\
&\quad + (m_1m_4 + m_1m_6 + m_2m_5 + m_2m_8 + m_4m_6 + m_5m_8)L \\
&\quad + (m_1m_2 + m_1m_4 + m_2m_4 + m_5m_6 + m_5m_8 + m_6m_8)M \\
&\quad + (m_1^2 + m_1m_3 + m_1m_7 + m_3m_5 + m_5^2 + m_5m_7)N \\
&\quad + (m_1m_2 + m_1m_8 + m_2m_8 + m_4m_5 + m_4m_6 + m_5m_6)O,
\end{aligned}$$

$$
\begin{aligned}
\alpha_4 = \alpha_8 = {} & (m_0m_4 + m_0m_8) + (m_4^2 + m_4m_8 + m_8^2)A \\
& +(m_1m_8 + m_3m_7 + m_4m_5)B + (m_2m_6 + m_2m_8 + m_4m_6)C \\
& +(m_1m_5 + m_3m_8 + m_4m_7)D + m_4m_8E \\
& +(m_1m_4 + m_3m_7 + m_5m_8)F + (m_2m_4 + m_2m_6 + m_6m_8)G \\
& +(m_1m_5 + m_3m_4 + m_7m_8)H \\
& +(m_1m_4 + m_1m_8 + m_3^2 + m_4m_5 + m_5m_8 + m_7^2)I \\
& +(m_1^2 + m_3m_4 + m_3m_8 + m_4m_7 + m_5^2 + m_7m_8)J \\
& +(m_1m_2 + m_1m_7 + m_2m_7 + m_3m_5 + m_3m_6 + m_5m_6)K \\
& +(m_1m_3 + m_1m_6 + m_2m_5 + m_2m_7 + m_3m_6 + m_5m_7)L \\
& +(m_1m_6 + m_1m_7 + m_2m_3 + m_2m_5 + m_3m_5 + m_6m_7)M \\
& +(m_2^2 + m_2m_4 + m_2m_8 + m_4m_6 + m_6^2 + m_6m_8)N \\
& +(m_1m_2 + m_1m_3 + m_2m_3 + m_5m_6 + m_5m_7 + m_6m_7)O.
\end{aligned}
$$

Proof. The result comes from Lemma 2, Lemma 3 and a complex computation. □

In order to facilitate, we denote

$$
\begin{aligned}
& \overrightarrow{m} := (m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8) \in \mathrm{GF}(q)^9, \\
& D_0(\overrightarrow{m}) := \alpha_0, \\
& D_1(\overrightarrow{m}) := \alpha_1 = \alpha_5, \\
& D_2(\overrightarrow{m}) := \alpha_2 = \alpha_6, \\
& D_3(\overrightarrow{m}) := \alpha_3 = \alpha_7, \\
& D_4(\overrightarrow{m}) := \alpha_4 = \alpha_8.
\end{aligned} \tag{11}
$$

Theorem 1. *Let p be an odd prime of the form $16l+9$ and q be a prime power. Suppose $\alpha \in \mathrm{GF}(q)$, $\overrightarrow{m} \in \mathrm{GF}(q)^9$. Then*

(1) pure eighth power residue double circulant code $P_p(\overrightarrow{m})$ is self-dual over $\mathrm{GF}(q)$ when the following conditions hold:

$$
\begin{cases}
D_0(\overrightarrow{m}) = -1, \\
D_1(\overrightarrow{m}) = 0, \\
D_2(\overrightarrow{m}) = 0, \\
D_3(\overrightarrow{m}) = 0, \\
D_4(\overrightarrow{m}) = 0.
\end{cases} \tag{12}
$$

(2) bordered eighth power residue double circulant code $B_p(\alpha, \overrightarrow{m})$ is self-dual over $\mathrm{GF}(q)$ when the following conditions hold:

$$
\begin{cases}
\alpha^2 + p = -1, \\
-\alpha + m_0 + \frac{p-1}{8}(m_1 + m_2 + m_3 + \\
\qquad m_4 + m_5 + m_6 + m_7 + m_8) = 0, \\
D_0(\overrightarrow{m}) = -2, \\
D_1(\overrightarrow{m}) = -1, \\
D_2(\overrightarrow{m}) = -1, \\
D_3(\overrightarrow{m}) = -1, \\
D_4(\overrightarrow{m}) = -1.
\end{cases} \tag{13}
$$

Proof. According to Lemma 3,

$$
\begin{aligned}
P_p(\overrightarrow{m})P_p(\overrightarrow{m})^t = {} & I_p + D_0(\overrightarrow{m})I_p + D_1(\overrightarrow{m})A_1 + D_2(\overrightarrow{m})A_2 \\
& +D_3(\overrightarrow{m})A_3 + D_4(\overrightarrow{m})A_4 + D_1(\overrightarrow{m})A_5 \\
& +D_2(\overrightarrow{m})A_6 + D_3(\overrightarrow{m})A_7 + D_4(\overrightarrow{m})A_8,
\end{aligned} \tag{14}
$$

and

$$
B_p(\overrightarrow{m})B_p(\overrightarrow{m})^t = (I_{p+1} \quad K)\begin{pmatrix} I_{p+1} \\ K^t \end{pmatrix} = I_{p+1} + KK^t, \tag{15}
$$

where

$$
\begin{aligned}
KK^t &= \begin{pmatrix} \alpha & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & R & \\ -1 & & & \end{pmatrix} \cdot \begin{pmatrix} \alpha & -1 & \cdots & -1 \\ 1 & & & \\ \vdots & & R^t & \\ 1 & & & \end{pmatrix} \\
&= \begin{pmatrix} \alpha^2 + p & S & \cdots & S \\ S & & & \\ \vdots & & X & \\ S & & & \end{pmatrix}_{(p+1)\times(p+1)}
\end{aligned} \tag{16}
$$

and

$$
\begin{aligned}
& X = J_p + D_0(\overrightarrow{m})I_p + D_1(\overrightarrow{m})A_1 + D_2(\overrightarrow{m})A_2 + D_3(\overrightarrow{m})A_3 \\
& +D_4(\overrightarrow{m})A_4 + D_1(\overrightarrow{m})A_5 + D_2(\overrightarrow{m})A_6 + D_3(\overrightarrow{m})A_7 + D_4(\overrightarrow{m})A_8, \\
& S = -\alpha + m_0 + \frac{p-1}{8}(m_1 + m_2 + m_3 + m_4 \\
& \qquad + m_5 + m_6 + m_7 + m_8).
\end{aligned} \tag{17}
$$

□

The result can be obtained by the definition of self-dual codes.

4 Eighth Power Residue Double Circulant Self-Dual Codes Over GF(2) and GF(4)

In this section, we give some constructions of self-dual codes over GF(2) and GF(4) by MATLAB and MAGMA. And the corresponding minimum hamming distances are solved. Some codes have good minimum distances, even almost satisfy the bounds.

Theorem 2. *Let p be an odd prime of the form $16l + 9$, several pure eighth power residue double circulant self-dual codes whose generator matrix satisfies the form of $P_p(m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8)$ of length $2p$ over $\mathrm{GF}(2)$ are obtained. The parameters that satisfy the conditions are listed in the following table when $p = 41 = 16 \times 2 + 9$.*

When $p = 41$, the length n of the code is 82, so that the bound of the minimum hamming distance is 16. By our method, the minimum hamming distance of the codes has a maximum of 14, which almost satisfies the bound. The self-dual [82, 41, 14] codes over GF(2) with a good property are obtained.

Theorem 3. *Let ξ be the fixed primitive element of $\mathrm{GF}(4)$ satisfying $\xi^2+\xi+1 = 0$ and p be an odd prime of the form $16l + 9$, pure eighth power residue double circulant self-dual codes $P_p(\overrightarrow{m})$ of length $2p$ over $\mathrm{GF}(4)$ and bordered eighth power residue double circulant codes $B_p(\alpha, \overrightarrow{m})$ of length $2(p+1)$ over $\mathrm{GF}(4)$ can be obtained. Furthermore, it is obvious that equation $\alpha^2 + p = -1$ holds if and only if $\alpha = 0$, because p is an odd prime. And the parameter values except α that meet the conditions are listed in the following table when $p = 41 = 16 \times 2 + 9$ and $p = 73 = 16 \times 4 + 9$.*

Table 1: The parameters of P_p over GF(2) with $p = 41$

Serial number	m_0	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	Min-distance
1	0	0	0	1	1	1	0	1	1	10
2	0	0	1	1	0	0	1	1	1	10
3	0	1	0	0	1	1	1	0	1	10
4	0	1	1	0	1	1	0	0	1	10
5	1	0	0	0	1	0	1	1	1	14
6	1	0	0	1	0	1	1	1	0	14
7	1	0	0	1	1	0	1	0	1	12
8	1	0	1	0	1	0	0	1	1	12
9	1	0	1	1	1	0	0	0	1	14
10	1	1	1	0	1	0	1	0	0	12

Table 2: The parameters of P_p over GF(4) with $p = 41$

Serial number	m_0	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	Min-distance
1	1	1	1	1	ξ	1	1	1	ξ^2	14
2	1	1	ξ	1	ξ^2	0	0	ξ^2	ξ	12
3	1	1	0	0	0	1	0	1	1	14
4	ξ	1	ξ	1	0	0	1	ξ^2	ξ^2	14
5	0	ξ	0	ξ	ξ^2	ξ	ξ^2	ξ^2	0	14

Table 3: The parameters of B_p over GF(4) with $p = 41$

Serial number	m_0	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	Min-distance
1	1	1	1	ξ	1	0	ξ	ξ	ξ	12
2	1	1	ξ	1	ξ^2	ξ^2	ξ	ξ^2	ξ	8
3	1	1	ξ^2	1	0	ξ^2	ξ^2	ξ^2	1	8
4	ξ^2	1	0	0	ξ	ξ^2	ξ	1	0	12
5	0	1	ξ^2	ξ	0	ξ	0	ξ^2	1	12

Table 4: The parameters of P_p over GF(4) with $p = 73$

Serial number	m_0	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	Min-distance
1	1	1	ξ	ξ	0	1	ξ^2	ξ^2	0	12
2	1	1	ξ	0	ξ^2	1	ξ^2	0	ξ	12
3	0	ξ	ξ	ξ^2	0	ξ^2	ξ^2	ξ	0	6
4	1	1	0	ξ^2	ξ	1	0	ξ	ξ^2	12
5	1	ξ^2	ξ^2	ξ^2	ξ^2	ξ	ξ	ξ	ξ	12

Table 5: The parameters of B_p over GF(4) with $p = 73$

Serial number	m_0	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	Min-distance
1	1	1	ξ^2	ξ^2	ξ	1	ξ	ξ	ξ^2	8
2	0	1	ξ	0	ξ	1	ξ^2	0	ξ^2	12
3	0	1	0	ξ	ξ	1	0	ξ^2	ξ^2	12
4	0	ξ^2	1	0	ξ^2	ξ^2	1	0	ξ	12
5	0	ξ	ξ	1	0	ξ^2	ξ^2	1	0	12

The pure double circulant self-dual codes [82, 41, 14] codes and bordered double circulant self-dual codes self-dual [84, 42, 12] codes over GF(4) which have good property are listed, especially the values of parameters $m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8$. Besides, we get some other codes when $p = 73$.

5 Conclusion

In this paper, we construct double circulant self-dual codes by higher power residues, especially eighth power residues.

First of all, the relationship of the eighth power residue cyclotomic numbers is given. Suppose that there are eight matrices with nine parameters on the GF(q), and the expression for multiplying any two matrices is represented by the cyclotomic numbers. From the linear combination of eight circulant matrices, we can construct the circulant matrix R. Two kinds of codes are represented by R. One is pure circulant codes, and the other is bordered circulant codes. Combined with the necessary condition of self-dual code ($GG^{\mathrm{T}} = 0$), parameters can be determined to satisfy the condition of self-dual code, which renders the pure double circulant self-dual codes and bordered circulant self-dual codes can be obtained. By programming, the parameters that satisfy the conditions and the minimum hamming distance are given.

We exploit a new way to construct self-dual codes over GF(2) and GF(4) by prime p of the form $16f+9$, and some codes have good properties. Examples of such codes are binary self-dual [82, 41, 14] code, quaternary self-dual [82, 41, 14] code and quaternary self-dual [84, 42, 12] code.

Acknowledgments

The work is financially supported by National Natural Science Foundation of China (No. 61902429, No.11775306), Shandong Provincial Natural Science Foundation of China (No. ZR2017MA001, ZR2019MF070), Fundamental Research Funds for the Central Universities (No. 19CX02058A, No. 17CX02030A), the Open Research Fund from Shandong provincial Key Laboratory of Computer Networks, Grant No. SDKLCN-2017-03, Key Laboratory of Applied Mathematics of Fujian Province University (Putian University)(No.SX201702, No.SX201806), and International Cooperation Exchange Fund of China University of Petroleum (UPCIEF2019020).

References

[1] K. T. Arasu and T. A. Gulliver, "Self-dual codes over $\mathbb{F}_p$ and weighing matrices," *IEEE Transactions on Information Theory*, vol. 47, no. 5, pp. 2051-2055, 2001.

[2] E. R. Berlekamp, F. J. MacWilliams and N. J. A. Sloane, "Gleason's theorem on self-dual," *IEEE Transactions on Information Theory*, vol. 18, pp. 409-414, 1972.

[3] S. Buyuklieva, "On the binary self-dual codes with an automorphism of order 2," *Designs Codes & Cryptography*, vol. 12, no. 1, pp. 39-48, 1997.

[4] S. Bouyuklieva and I. Bouyukliev, "An algorithm for classification of binary self-dual codes," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3933-3940, 2012.

[5] J. H. Convay and V. Pless, "On the enumeration of self-dual codes," *Journal of Combinatorial Theory*, vol. 28, no. 1, pp. 26-53, 1980.

[6] J. H. Convay and J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Transactions on Information Theory*, vol. 36, no. 6, pp. 1319-1333, 1990.

[7] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, 1998.

[8] S. T. Dougherty, J. L. Kim and P. Sole, "Double circulant codes from two class association schemes," *Advances in Mathematics of Communications*, vol. 1, no. 1, pp. 45-64, 2007.

[9] S. T. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylyshchak and B. Yildiz, "Bordered constructions of self-dual codes from group rings and new extremal binary self-dual codes," *Finite Fields and Their Applications*, vol. 57, pp. 108-127, 2019.

[10] P. Gaborit, "Quadratic double circulant codes over fields," *Journal of Combinatorial Theory, Series A*, vol. 97, no. 1, pp. 85-107, 2002.

[11] M. Harada, M. Kiermaier, A. Wassermann, *et al.*, "New binary singly even self-dual codes," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1612-1617, 2010.

[12] T. Helleseth, "Double circulant quadratic residue codes," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2154-2155, 2004.

[13] W. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields and Their Applications*, vol. 11, pp. 451-490, 2005.

[14] W. C. Huffman, R. A. Brualdi and V. S. Pless, *Handbook of Coding Theory*, 1998.

[15] K. Ireland and M. Rosen, "Gauss and jacobi sums," *Mathematical Gazette*, vol. 84, pp. 75-92, 1998.

[16] M. Karlin, "New binary coding results by circulants," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 81-92, 1969.

[17] A. Kaya, B. Yildiz and I. Siap, "New extremal binary self-dual codes from $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of quadratic circulant codes over $\mathbb{F}_4$," *Finite Fields and Their Applications*, vol. 35, pp. 318-329, 2015.

[18] A. Kaya, B. Yildiz, "Various constructions for self-dual codes over rings and new binary self-dual codes," *Discrete Mathematics*, vol. 339, pp. 460-469, 2016.

[19] A. Kaya, "New extremal binary self-dual codes of lengths 64 and 66 from R_2-lifts," *Finite Fields and Their Applications*, vol. 46, pp. 271-279, 2017.

[20] A. Kaya, B. Yildiz and I. Siap, "New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$," *Finite Fields and Their Applications*, vol. 29, pp. 160-177, 2014.

[21] A. Kaya, B. Yildiz and I. Siap, "New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2[\mathrm{J}]$," *Finite Fields and Their Applications*, vol. 29, pp. 160-177, 2014.

[22] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," *Information & Control*, vol. 22, no. 2, pp. 188-200, 1973.

[23] R. Meng, T. Yan, "New constructions of binary interleaved sequences with low autocorrelation," *International Journal of Network Security*, vol. 19, no. 4, pp. 546–550, 2017.

[24] V. Pless and N. J. A. Sloane, "On the classification and enumeration of self-dual codes," *Journal of Combinatorial Theory*, vol. 18, no. 3, pp. 313-335, 1975.

[25] E. M. Rains, "Shadow bounds for self-dual codes," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 134-139, 1998.

[26] C. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379-423, 1948.

[27] S. Zhang, T. Yan, Y. Sun, L. Wang, "Linear complexity of two classes of binary interleaved sequences with low autocorrelation," *International Journal of Network Security*, 2019. (`http://ijns.jalaxy.com.tw/contents/ijns-v22-n6/ijns-2020-v22-n6-p834-0.pdf`)

[28] N. J. A. Sloane and J. G. Thompson, "Cyclic self-dual codes," *IEEE Transactions on Information Theory*, vol. 29, pp. 364-366, 1983.

[29] N. Yankov, M. Ivanova and M. H. Lee, "Self-dual codes with an automorphism of order 7 and s-extremal codes of length 68," *Finite Fields and Their Applications*, vol. 51, pp. 17-30, 2018.

[30] T. Zhang and G. Ge, "Fourth power residue double circulant self-dual codes," *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4243-4252, 2015.

Biography

Changsong Jiang was born in 1997 in Sichuan Province of China. He was graduated from China University of Petroleum in 2019. He is currently studying for a postgraduate degree at University of Electronic Science and Technology of China. Email: jiangchso@163.com

Yuhua Sun was born in 1979. She was graduated from Shandong Normal University, China, in 2001. In 2004, she received the M.S. degree in mathematics from the Tongji University, Shanghai and a Ph.D. in Cryptography from the Xidian University. She is currently a lecturer of China University of Petroleum. Her research interests include cryptography, coding and information theory. Email: sunyuha_1@163.com

Xueting Liang was born in 1997 in Anhui Province of China. She is studying at China University of Petroleum. Email:13399613079@163.com