Fourth Power Residue Double Circulant Self-Dual Codes

Tao Zhang and Gennian Ge

Abstract—**Quadratic residue codes are a well-known class of codes. In this paper, we consider the constructions of self-dual codes by higher power residues, especially fourth power residues. New infinite families of self-dual codes over GF(2), GF(3), GF(4), GF(8), and GF(9) are introduced. Some of them have better minimum weight than previously known codes. We also give general results related to the automorphism group of some of these codes.**

Index Terms—**Self-dual code, double circulant code, fourth power residues, cyclotomic number.**

I. INTRODUCTION

SELF-DUAL codes are one of the most interesting classes of linear codes, which include the best-known error-correcting codes, such as the extended Hamming codes, the extended Golay codes, and certain extended quadratic residue codes. These codes have important applications in data transmission [17], [32], [37]. Self-dual codes also have strong connections to several other areas including stabilizer quantum error-correcting codes [8], designs [2], [3], projective planes [26], lattices [11], and invariant theory [31]. Therefore, constructing good self-dual codes has been an important research problem. There have been a number of papers devoted to classifying or constructing self-dual codes (see [1], [6], [7], [16], [20], [21], [23], [24], [35] and the references therein).

Another interesting class of codes is the class of quadratic residue codes. They have rate close to $1/2$ and large minimum distance. They also have a powerful decoding method named permutation decoding, which makes use of the fact that these codes have large automorphism groups. While initially researchers focused on the quadratic residue codes, there have been recent developments in the higher power residue codes [10], [13], [36].

The connections between self-dual codes and quadratic residue codes were introduced by Karlin [25]. He considered binary double circulant codes based on quadratic residues. Later, Pless [33] considered ternary double circulant codes from quadratic residues, producing the famous Pless symmetry codes. In 2002, Gaborit [14] introduced quadratic double circulant codes including Karlin's construction and the Pless symmetry codes. He also constructed new infinite families of self-dual codes over GF(4), GF(5), GF(7) and GF(9).

Our goal is to construct double circulant self-dual codes by higher power residues, especially fourth power residues. We give new constructions for infinite families of self-dual codes over GF(2), GF(3), GF(4), GF(8) and GF(9), some of which lead to new codes with better parameters than previously known codes. Examples of such codes are ternary self-dual $[124, 62, 24]$ code, quaternary self-dual $[76, 38, 19]$ code, self-dual $[58, 29, 18]$ code over GF(8) and self-dual $[58, 29, 18]$ code over GF(9). We also give general results related to the automorphism group of some of these codes. All computations have been done by MAGMA V2.20-4 [5] on a 3.40 GHz CPU.

This paper is organized as follows. In Section II, we present definitions and some results about self-dual codes and cyclotomy. We also give general results about fourth power residue double circulant self-dual codes. In Section III, we give two infinite families of binary self-dual codes, four infinite families of quaternary self-dual codes and an infinite family of self-dual codes over GF(8) from the 4th cyclotomic classes. In Section IV, two infinite families of ternary self-dual codes and two infinite families of self-dual codes over GF(9) are given. Section V investigates the automorphism group of some of these codes. In Section VI, we give an infinite family of binary four circulant self-dual codes. Section VII concludes the paper. Proofs for most lemmas are presented in the appendix.

Manuscript received October 24, 2014; revised March 21, 2015; accepted June 8, 2015. Date of publication June 17, 2015; date of current version July 10, 2015. The work of G. Ge was supported in part by the Scientific and Technological Innovation Capacity Enhancement Program of Beijing Municipal Institutions, in part by the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions, and in part by the National Natural Science Foundation of China under Grant 61171198 and Grant 11431003.

T. Zhang is with the School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China (e-mail: tzh@zju.edu.cn).

G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China, and also with the Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China (e-mail: gnge@zju.edu.cn).

Communicated by Y. Mao, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2015.2446468

II. DEFINITIONS AND GENERAL RESULTS

A. Self-Dual Codes

A linear code C of length n and dimension k over finite field GF(q) is a k-dimensional subspace of GF$(q)^n$, where q is a prime power. A generator matrix G of the code C is a $k \times n$ matrix whose row span equals the code. The Euclidean inner product is defined by

$$(x, y) = \sum_{i=1}^{n} x_i y_i,$$

where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. For a linear code C of length n, the code

$$C^{\perp} = \{x \in \mathrm{GF}(q)^n | (x, c) = 0 \quad \text{for all } c \in C\}$$

is called its Euclidean dual code. $C^{\perp}$ is linear, and we have $\dim(C)+\dim(C^{\perp}) = n$. C is called Euclidean self-orthogonal if $C \subseteq C^{\perp}$ and Euclidean self-dual if $C = C^{\perp}$. From now on, what we mean by self-dual is Euclidean self-dual. Note that a self-dual code always has even length n and the dimension $n/2$. Hence, we usually do not state the dimension for a self-dual code explicitly.

The (Hamming) distance between two codewords $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, denoted by $d(x, y)$, is defined to be the number of places at which x and y differ. The (Hamming) weight $w(x)$ of a codeword $x = (x_1, \ldots, x_n)$ is $w(x) = d(x, 0)$ and the minimum distance $d(C)$ of a code C is defined by $d(C) = \min\{d(x, y)|x \neq y \in C\}$. Then for the self-dual codes, we have the following result.

Theorem 1 [24], [30], [34], [35]: Let C be a self-dual code over GF(q) *of length n and minimum distance* $d(C)$. *Then we have*

(i) *If* $q = 2$, *then*

$$d(C) \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4; & \text{if } n \not\equiv 22 \pmod{24}, \\ 4\lfloor \frac{n}{24} \rfloor + 6; & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

(ii) *If* $q = 3$, *then* $d(C) \leq 3\lfloor \frac{n}{12} \rfloor + 3$.

(iii) *If* $q = 4$, *then* $d(C) \leq 4\lfloor \frac{n}{12} \rfloor + 4$.

(iv) $d(C) \leq \lfloor \frac{n}{2} \rfloor + 1$ *for* $q \neq 2,\ 3,\ 4$.

The code C is called extremal if the above equality holds. A self-dual code is called optimal if it has the highest possible minimum distance for its length. An extremal code is automatically optimal.

B. Power Residues, Cyclotomy and Cyclotomic Number

Let p be an odd prime and γ be a fixed primitive element of GF(p). Let $N > 1$ be a divisor of $p - 1$. We define the Nth cyclotomic classes $C_0, C_1, \ldots, C_{N-1}$ of GF(p) by

$$C_i = \left\{ \gamma^{jN+i} | 0 \leq j \leq \frac{p-1}{N} - 1 \right\},$$

where $0 \leq i \leq N - 1$. That is, C_0 is the Nth power residues modulo p, and $C_i = \gamma^i C_0$, $1 \leq i \leq N - 1$. For integers m, n with $0 \leq m, n < N$, the cyclotomic number of order N is defined by

$$(m, n)_N = |(C_m + 1) \bigcap C_n|.$$

The following lemma summarizes some basic properties of cyclotomic numbers.

Lemma 2 [4]: Let $p = ef + 1$ *be some odd prime. Then*

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

2)

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

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

In the sequel, we need the following exact values of the cyclotomic numbers of order 4 determined by a fixed primitive root.

Theorem 3 [4]: Let p be a prime of the form $p = 8l + 5$. *Let g be a primitive root of p. Then the cyclotomic numbers of order* 4 *are*

$$\begin{aligned} (0,0)_4 &= (2,0)_4 = (2,2)_4 = \frac{p - 7 + 2x}{16}, \\ (0,1)_4 &= (1,3)_4 = (3,2)_4 = \frac{p + 1 + 2x - 4y}{16}, \\ (0,2)_4 &= \frac{p + 1 - 6x}{16}, \\ (0,3)_4 &= (1,2)_4 = (3,1)_4 = \frac{p + 1 + 2x + 4y}{16}, \\ (1,0)_4 &= (1,1)_4 = (2,1)_4 = (2,3)_4 = (3,0)_4 = (3,3)_4 \\ &= \frac{p - 3 - 2x}{16}, \end{aligned}$$

with the integers x and y given uniquely by

$$p = x^2 + y^2,\ x \equiv 1 \pmod 4,\ y \equiv g^{\frac{p-1}{4}} x \pmod p.$$

Remark 4: For simplicity, in the following sections, we denote $A := (0, 0)_4$, $B := (0, 1)_4$, $C := (0, 2)_4$, $D := (0, 3)_4$ *and* $E := (1, 0)_4$.

C. General Results

Let p be an odd prime of the form $4k+1$ for some integer k with its 4th cyclotomic classes being C_0, C_1, C_2 and C_3. Let m_0, m_1, m_2, m_3 and m_4 be elements of GF(q). We now set the matrix $C_p(m_0, m_1, m_2, m_3, m_4)$ to be the $p \times p$ matrix on GF(q) with components c_{ij}, $1 \leq i, j \leq p$, where

$$c_{ij} = \begin{cases} m_0; & \text{if } j = i, \\ m_1; & \text{if } j - i \in C_0, \\ m_2; & \text{if } j - i \in C_1, \\ m_3; & \text{if } j - i \in C_2, \\ m_4; & \text{if } j - i \in C_3. \end{cases}$$

We define by I_n and J_n the identity and the all-one square $n \times n$ matrices, respectively. Then $C_p(1, 0, 0, 0, 0) = I_p$ and $C_p(1, 1, 1, 1, 1) = J_p$. Denote $A_1 := C_p(0, 1, 0, 0, 0)$, $A_2 := C_p(0, 0, 1, 0, 0)$, $A_3 := C_p(0, 0, 0, 1, 0)$ and $A_4 := C_p(0, 0, 0, 0, 1)$. Noting that the 4th cyclotomic classes form a 4-class association scheme [12], we obtain the following result.

Lemma 5: If p is a prime of the form $8l + 5$, *then*

$$\begin{aligned} &A_1 = A_3^t \text{ and } A_2 = A_4^t, \\ &A_1^2 = AA_1 + BA_2 + CA_3 + DA_4, \\ &A_2^2 = DA_1 + AA_2 + BA_3 + CA_4, \\ &A_3^2 = CA_1 + DA_2 + AA_3 + BA_4, \\ &A_4^2 = BA_1 + CA_2 + DA_3 + AA_4, \\ &A_1A_2 = A_2A_1 = AA_1 + EA_2 + DA_3 + BA_4, \\ &A_1A_3 = A_3A_1 = (2l + 1)I_p + AA_1 + EA_2 + AA_3 + EA_4, \\ &A_1A_4 = A_4A_1 = EA_1 + DA_2 + BA_3 + EA_4, \\ &A_2A_3 = A_3A_2 = BA_1 + EA_2 + EA_3 + DA_4, \end{aligned}$$

$$A_2A_4 = A_4A_2 = (2l+1)I_p + EA_1 + AA_2 + EA_3 + AA_4,$$
$$A_3A_4 = A_4A_3 = DA_1 + BA_2 + EA_3 + EA_4.$$

Proof: The proof is straightforward from the definition of A_i and Theorem 3. ■

The following result will be needed in the sequel.

Lemma 6: If p is a prime of the form $8l+5$, then

$$\begin{aligned}(m_0I_p &+ m_1A_1 + m_2A_2 + m_3A_3 + m_4A_4)(m_0I_p + m_1A_1\\ &+ m_2A_2 + m_3A_3 + m_4A_4)^t\\ &= a_0I_p + a_1A_1 + a_2A_2 + a_3A_3 + a_4A_4,\end{aligned}$$

where

$$\begin{aligned}a_0 &= m_0^2 + (\frac{p-1}{4})(m_1^2+m_2^2+m_3^2+m_4^2),\\ a_1 &= a_3 = m_0m_3 + m_0m_1 + (m_1m_3 + m_1^2 + m_3^2)A\\ &\quad + (m_2m_4 + m_1m_2 + m_3m_4)B + m_1m_3C\\ &\quad + (m_2m_4 + m_2m_3 + m_1m_4)D + (m_1m_2 + m_3m_4 + m_1m_4\\ &\quad + m_2m_3 + m_2^2 + m_4^2)E,\\ a_2 &= a_4 = m_0m_4 + m_0m_2 + (m_2^2 + m_4^2 + m_2m_4)A\\ &\quad + (m_1m_3 + m_2m_3 + m_1m_4)B + m_2m_4C\\ &\quad + (m_1m_2 + m_3m_4 + m_1m_3)D + (m_1m_4 + m_2m_3 + m_1m_2\\ &\quad + m_3m_4 + m_1^2 + m_3^2)E.\end{aligned}$$

Proof: The result comes from Lemma 5 and a lengthy routine computation. ■

For convenience, we denote

$$\begin{aligned}\overrightarrow{m} &:= (m_0, m_1, m_2, m_3, m_4) \in \mathrm{GF}(q)^5,\\ D_0(\overrightarrow{m}) &:= m_0^2 + (\frac{p-1}{4})(m_1^2+m_2^2+m_3^2+m_4^2),\\ D_1(\overrightarrow{m}) &:= m_0m_3 + m_0m_1 + (m_1m_3 + m_1^2 + m_3^2)A\\ &\quad + (m_2m_4 + m_1m_2 + m_3m_4)B + m_1m_3C\\ &\quad + (m_2m_4 + m_2m_3 + m_1m_4)D\\ &\quad + (m_1m_2 + m_3m_4 + m_1m_4 + m_2m_3 + m_2^2\\ &\quad + m_4^2)E,\\ D_2(\overrightarrow{m}) &:= m_0m_4 + m_0m_2 + (m_2^2 + m_4^2 + m_2m_4)A\\ &\quad + (m_1m_3 + m_2m_3 + m_1m_4)B + m_2m_4C\\ &\quad + (m_1m_2 + m_3m_4 + m_1m_3)D\\ &\quad + (m_1m_4 + m_2m_3 + m_1m_2 + m_3m_4 + m_1^2\\ &\quad + m_3^2)E.\end{aligned}$$

Definition 7: Let $P_n(R)$ and $B_n(\alpha, R)$ be codes with generator matrices of the form

$$\begin{pmatrix} I_n & R \end{pmatrix},$$

and

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

*respectively, where $\alpha \in \mathrm{GF}(q)$ and R is an $n \times n$ circulant matrix. The codes $P_n(R)$ and $B_n(\alpha, R)$ are called **pure double circulant codes** and **bordered double circulant codes**, respectively.*

Let

$$\begin{aligned}P_p(\overrightarrow{m}) &:= P_p(m_0I_p + m_1A_1 + m_2A_2 + m_3A_3 + m_4A_4),\\ B_p(\alpha, \overrightarrow{m}) &:= B_p(\alpha, m_0I_p + m_1A_1 + m_2A_2 + m_3A_3\\ &\qquad + m_4A_4).\end{aligned}$$

*Then the codes with generator matrices $P_p(\overrightarrow{m})$ and $B_p(\alpha, \overrightarrow{m})$ are called **fourth power residue double circulant codes**.*

The main theorem of this section is:

Theorem 8: Let p be an odd prime of the form $8l+5$ and q be a prime power. Let $\alpha \in \mathrm{GF}(q)$, $\overrightarrow{m} \in \mathrm{GF}(q)^5$. Then

1) *the code with generator matrix $P_p(\overrightarrow{m})$ is self-dual over $\mathrm{GF}(q)$ if and only if the following holds:*
   a) $D_0(\overrightarrow{m}) = -1$,
   b) $D_1(\overrightarrow{m}) = 0$,
   c) $D_2(\overrightarrow{m}) = 0$;
2) *the code with generator matrix $B_p(\alpha, \overrightarrow{m})$ is self-dual over $\mathrm{GF}(q)$ if and only if the following holds:*
   a) $\alpha + p = -1$,
   b) $-\alpha + m_0 + \frac{p-1}{4}(m_1 + m_2 + m_3 + m_4) = 0$,
   c) $D_0(\overrightarrow{m}) = -2$,
   d) $D_1(\overrightarrow{m}) = -1$,
   e) $D_2(\overrightarrow{m}) = -1$.

Proof: The result follows from

$$\begin{aligned}P_p(\overrightarrow{m})&P_p(\overrightarrow{m})^t\\ &= I_p + D_0(\overrightarrow{m})I_p + D_1(\overrightarrow{m})A_1 + D_2(\overrightarrow{m})A_2\\ &\quad + D_1(\overrightarrow{m})A_3 + D_2(\overrightarrow{m})A_4,\end{aligned}$$

and

$$B_p(\alpha, \overrightarrow{m})B_p(\alpha, \overrightarrow{m})^t = I_{p+1} + \begin{pmatrix} \alpha + p & S \cdots S\\ S & \\ \vdots & X\\ S & \end{pmatrix},$$

where $X = J_p + D_0(\overrightarrow{m})I_p + D_1(\overrightarrow{m})A_1 + D_2(\overrightarrow{m})A_2 + D_1(\overrightarrow{m})A_3 + D_2(\overrightarrow{m})A_4$ and $S = -\alpha + m_0 + \frac{p-1}{4}(m_1 + m_2 + m_3 + m_4)$. ■

III. Fourth Power Residue Double Circulant Self-Dual Codes Over Fields With Characteristic 2

A. Self-Dual Codes Over GF(2)

In this subsection, we construct two infinite families of self-dual codes over GF(2). As a preparation, we have the following two lemmas.

Lemma 9: Let p be an odd prime having the form $16k+5$, where k is a nonnegative integer. Suppose g is a fixed primitive root of p. If $p = x^2 + y^2$, $x \equiv 1 \pmod 4$, $y \equiv g^{\frac{p-1}{4}}x \pmod p$. Then $x = 8t+1$, $y = 4s+2$ and $k \equiv t \pmod 2$ for some integers t, s. In particular, we can attain one of the following equations:

1) $A \equiv C \equiv D \equiv E \equiv 0 \pmod 2$, $B \equiv 1 \pmod 2$,
2) $A \equiv B \equiv C \equiv E \equiv 0 \pmod 2$, $D \equiv 1 \pmod 2$.

Proof: See the Appendix. ■

TABLE I
SOME CODES OBTAINED BY CONSTRUCTIONS $P_p(0,0,1,1,1)$ AND $B_p(0,1,0,1,1,1)$ OVER GF(2)

Code	Construction	Comments
$[12,6,4]$	$B_5(0,1,0,1,1,1)$	extremal
$[26,13,6]$	$P_{13}(0,0,1,1,1)$	optimal [15]
$[58,29,10]$	$P_{29}(0,0,1,1,1)$	optimal [15]
$[108,54,16]$	$B_{53}(0,1,0,1,1,1)$	highest known [15]
$[122,61,20]$	$P_{61}(0,0,1,1,1)$	highest known [22]

Lemma 10: Let p be an odd prime having the form $16k+13$, where k is a nonnegative integer. Suppose g is a fixed primitive root of p. If $p = x^2 + y^2$, $x \equiv 1 \pmod 4$, $y \equiv g^{\frac{p-1}{4}} x \pmod p$. Then $x = 8t+5$, $y = 4s+2$ and $k+t \equiv 1 \pmod 2$ for some integers t, s. In particular, we can attain one of the following equations:

1) $A \equiv C \equiv D \equiv 0 \pmod 2$, $B \equiv E \equiv 1 \pmod 2$,
2) $A \equiv B \equiv C \equiv 0 \pmod 2$, $D \equiv E \equiv 1 \pmod 2$.

Proof: See the Appendix. ■

Now we obtain the following result:

Theorem 11: Let p be an odd prime, then the following holds:

1) *if p has the form $16k+5$, then the code with generator matrix $B_p(0,1,0,1,1,1)$ over GF(2) is self-dual of length $2p+2$;*
2) *if p has the form $16k+13$, then the code with generator matrix $P_p(0,0,1,1,1)$ over GF(2) is self-dual of length $2p$.*

Proof: If p has the form $16k+5$, then from Lemma 9, we have

$$\begin{aligned}
&\alpha + p = 16k+5 \equiv 1 \pmod 2,\\
&-\alpha + m_0 + (\frac{p-1}{4})(m_1+m_2+m_3+m_4) \equiv 0 \pmod 2,\\
&D_0(1,0,1,1,1) = 1 + (4k+1)(1+1+1) \equiv 0 \pmod 2,\\
&D_1(1,0,1,1,1) = 1 + A + 2B + 2D + 4E \equiv 1 \pmod 2,\\
&D_2(1,0,1,1,1) = 2 + 3A + B + C + D + 3E \equiv 1 \pmod 2.
\end{aligned}$$

By Theorem 8, the code with generator matrix $B_p(0,1,0,1,1,1)$ over GF(2) is self-dual of length $2p+2$.

If p has the form $16k+13$, then by Lemma 10, we have

$$\begin{aligned}
&D_0(0,0,1,1,1) = (4k+3)(1+1+1) \equiv 1 \pmod 2,\\
&D_1(0,0,1,1,1) = A + 2B + 2D + 4E \equiv 0 \pmod 2,\\
&D_2(0,0,1,1,1) = 3A + B + C + D + 3E \equiv 0 \pmod 2.
\end{aligned}$$

By Theorem 8, we get that the code with generator matrix $P_p(0,0,1,1,1)$ over GF(2) is self-dual of length $2p$. ■

By the Dirichlet Theorem, there are infinitely many primes of the form $16k+5$ or $16k+13$. Therefore the two families described in Theorem 11 are infinite families. Most of the codes obtained by these constructions are extremal, optimal or the best-known codes with these parameters (see Table I). In particular the $[12,6,4]$ and $[122,61,20]$ codes also achieve the best-known lower bound on the minimum distance of general linear codes [18]. Table I lists the codes built by Theorem 11.

*Remark 12: In the following tables, we will denote by **highest known** the fact that the code meets the highest known minimum distance for its parameters, and we will denote by **exceeds before** the fact that the code has a better minimum distance than any previously known code with these parameters.*

B. Self-Dual Codes Over GF(4)

In this subsection, we give four constructions of infinite families of self-dual codes over GF(4). Let ζ be the fixed primitive element of GF(4) satisfying $\zeta^2+\zeta+1=0$, then we have the following theorems.

Theorem 13: Let p be an odd prime having the form $16k+5$, then the code with generator matrix $P_p(0,1,\zeta^2,1,\zeta)$ on GF(4) is self-dual of length $2p$.

Proof: If p is an odd prime of the form $16k+5$, then from Lemma 9,

$$\begin{aligned}
&D_0(0,1,\zeta^2,1,\zeta) = (4k+1)(1+\zeta+1+\zeta^2) \equiv 1 \pmod 2,\\
&D_1(0,1,\zeta^2,1,\zeta) = 3A + C + (3\zeta^2+3\zeta)E \equiv 0 \pmod 2,\\
&D_2(0,1,\zeta^2,1,\zeta) = C \equiv 0 \pmod 2.
\end{aligned}$$

By Theorem 8, we have that the code with generator matrix $P_p(0,1,\zeta^2,1,\zeta)$ over GF(4) is self-dual of length $2p$. ■

Theorem 14: Let p be an odd prime having the form $16k+5$. Suppose the cyclotomic number $(0,1)_4$ is odd, then the code with generator matrix $B_p(0,\zeta,1,\zeta^2,0,0)$ on GF(4) is self-dual of length $2p+2$.

Proof: If p is an odd prime of the form $16k+5$ and the cyclotomic number $(0,1)_4$ is odd, that is $B = (0,1)_4 \equiv 1 \pmod 2$. Then by Lemma 9, we get that

$$\begin{aligned}
&\alpha + p = 16k+5 \equiv 1 \pmod 2,\\
&-\alpha + m_0 + (\frac{p-1}{4})(m_1+m_2+m_3+m_4) \equiv 0 \pmod 2,\\
&D_0(\zeta,1,\zeta^2,0,0) = -4k\zeta^2 \equiv 0 \pmod 2,\\
&D_1(\zeta,1,\zeta^2,0,0) = \zeta + A + \zeta^2 B + E \equiv 1 \pmod 2,\\
&D_2(\zeta,1,\zeta^2,0,0) = 1 + \zeta A + \zeta^2 D + \zeta E \equiv 1 \pmod 2.
\end{aligned}$$

From Theorem 8, the code with generator matrix $B_p(0,\zeta,1,\zeta^2,0,0)$ over GF(4) is self-dual of length $2p+2$. ■

Theorem 15: Let p be an odd prime of the form $16k+13$. Suppose the cyclotomic number $(0,1)_4$ is odd, then the codes with generator matrices $P_p(\zeta,\zeta,\zeta,\zeta^2,0)$ and $B_p(0,\zeta,1,\zeta,\zeta,\zeta^2)$ on GF(4) are self-dual codes of lengths $2p$ and $2p+2$, respectively.

Proof: If p is an odd prime of the form $16k+13$ and the cyclotomic number $(0,1)_4$ is odd, that is $B = (0,1)_4 \equiv 1 \pmod 2$. By Lemma 10, we have

$$\begin{aligned}
&D_0(\zeta,\zeta,\zeta,\zeta^2,0) = \zeta^2 + (4k+3)(2\zeta^2+\zeta) \equiv 1 \pmod 2,\\
&D_1(\zeta,\zeta,\zeta,\zeta^2,0) = \zeta + \zeta^2 B + C + D + E \equiv 0 \pmod 2,\\
&D_2(\zeta,\zeta,\zeta,\zeta^2,0) = \zeta^2 + \zeta^2 A + 2B\\
&\qquad + \zeta D + \zeta^2 E \equiv 0 \pmod 2.
\end{aligned}$$

From Theorem 8, the code with generator matrix $P_p(\zeta,\zeta,\zeta,\zeta^2,0)$ over GF(4) is self-dual of length $2p$.

TABLE II
SOME CODES OBTAINED BY CONSTRUCTIONS $P_p(0,1,\zeta^2,1,\zeta)$, $P_p(\zeta,\zeta,\zeta,\zeta^2,0)$, $B_p(0,\zeta,1,\zeta^2,0,0)$ AND $B_p(0,\zeta,1,\zeta,\zeta,\zeta^2)$ OVER GF(4)

Code	Construction	Comments
$[10,5,4]$	$P_5(0,1,\zeta^2,1,\zeta)$	extremal
$[26,13,8]$	$P_{13}(\zeta,\zeta,\zeta,\zeta^2,0)$	highest known [15]
$[58,29,15]$	$P_{29}(\zeta,\zeta,\zeta,\zeta^2,0)$	highest known [15]
$[60,30,16]$	$B_{29}(0,\zeta,1,\zeta,\zeta,\zeta^2)$	highest known [19]
$[74,37,18]$	$P_{37}(0,1,\zeta^2,1,\zeta)$	highest known [19]
$[76,38,19]$	$B_{37}(0,\zeta,1,\zeta^2,0,0)$	exceeds before [19]

Since we have

$$\begin{aligned}
&\alpha+p=16k+13\equiv 1 \pmod 2,\\
&-\alpha+m_0+(\frac{p-1}{4})(m_1+m_2+m_3+m_4)\equiv 0 \pmod 2,\\
&D_0(\zeta,1,\zeta,\zeta,\zeta^2)=(4k+4)\zeta^2\equiv 0 \pmod 2,\\
&D_1(\zeta,1,\zeta,\zeta,\zeta^2)=-1+(2+\zeta)B+\zeta C+(1+2\zeta^2)D\\
&\qquad\qquad+(2\zeta^2+\zeta)E\equiv 1 \pmod 2,\\
&D_2(\zeta,1,\zeta,\zeta,\zeta^2)=-\zeta+(\zeta+2\zeta^2)B+C+(1+2\zeta)D\\
&\qquad\qquad+(1+2\zeta^2)E\equiv 1 \pmod 2.
\end{aligned}$$

Then by Theorem 8 again, the code with generator matrix $B_p(0,\zeta,1,\zeta,\zeta,\zeta^2)$ over GF(4) is self-dual of length $2p+2$. ■

Table II gives examples of codes constructed by the above three theorems, and all the codes are either extremal or the best-known codes with these parameters. In particular, the code $[76,38,19]$ has a better minimum distance than any previously known codes [19]. Moreover, the codes $[74,37,18]$ and $[76,38,19]$ achieve the best-known lower bound on the minimum distance of general linear codes [18].

C. Self-Dual Codes Over GF(8)

In this subsection, we give a construction of self-dual codes over GF(8). Let ζ be the fixed primitive element of GF(8) satisfying $\zeta^3+\zeta+1=0$, then we have the following result.

Theorem 16: Let p be an odd prime of the form $16k+13$, then the code with generator matrix $P_p(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$ on GF(8) *is self-dual of length $2p$.*

Proof: If $p=16k+13$, then by Lemma 10,

$$\begin{aligned}
&D_0(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)=(4k+2)\zeta+1\equiv 1 \pmod 2,\\
&D_1(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)=\zeta^2+A+\zeta^2B+\zeta^3C\\
&\qquad\qquad+\zeta^2D\equiv 0 \pmod 2,\\
&D_2(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)=\zeta^6A+\zeta B+\zeta^6C+\zeta D\\
&\qquad\qquad+\zeta E\equiv 0 \pmod 2.
\end{aligned}$$

Using Theorem 8, we get that the code with generator matrix $P_p(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$ over GF(8) is self-dual of length $2p$. ■

Table III gives examples of such codes. The code $[26,13,10]$ achieves the best-known lower bound on the minimum distance of general linear codes [18], and the code of length 58 is new.

TABLE III
SOME CODES OBTAINED BY CONSTRUCTION $P_p(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$ OVER GF(8)

Code	Construction	Comments
$[26,13,10]$	$P_{13}(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$	highest known [19]
$[58,29,18]$	$P_{29}(\zeta^5,\zeta,\zeta^3,\zeta^2,\zeta^3)$	

IV. FOURTH POWER RESIDUE DOUBLE CIRCULANT SELF-DUAL CODES OVER FIELDS WITH CHARACTERISTIC 3

A. Self-Dual Codes Over GF(3)

In this subsection, we give two constructions $B_p(1,1,0,1,2,1)$ and $B_p(1,1,0,0,1,1)$ for self-dual codes over GF(3), we also list some examples of these constructions. As a preparation, we give the following lemma.

Lemma 17: Let p be an odd prime having the form $24k+13$, where k is a nonnegative integer. Suppose g is a primitive root of p. If $p=x^2+y^2$, $x\equiv 1 \pmod 4$, $y\equiv g^{\frac{p-1}{4}}x \pmod p$. Then $x=4m+1$, $y=4n+2$ for some integers m, n satisfying $m\equiv 2 \pmod 3$ or $n\equiv 1 \pmod 3$. Moreover,

1) *if $m\equiv 2 \pmod 3$, then $A\equiv 0 \pmod 3$, $C+1\equiv 0 \pmod 3$ and $2B+C+2D+2E\equiv 0 \pmod 3$;*
2) *if $n\equiv 1 \pmod 3$, then $2+A+B+2E\equiv 0 \pmod 3$ and $2+A+D+2E\equiv 0 \pmod 3$.*

Proof: See the Appendix. ■

As an application of the above lemma, we have the following theorem.

Theorem 18: Let p be an odd prime having the form $24k+13$. Then $p=x^2+y^2$, where $x=4m+1$, $y=4n+2$ for some integers m, n satisfying $m\equiv 2 \pmod 3$ or $n\equiv 1 \pmod 3$. Furthermore,

1) *if $m\equiv 2 \pmod 3$, then the code with generator matrix $B_p(1,1,0,1,2,1)$ is self-dual over* GF(3)*;*
2) *if $n\equiv 1 \pmod 3$, then the code with generator matrix $B_p(1,1,0,0,1,1)$ is self-dual over* GF(3).

Proof: Let p be an odd prime having the form $24k+13$. Assume $m\equiv 2 \pmod 3$, then from Lemma 17, we have

$$\begin{aligned}
&\alpha+p=24k+14\equiv 2 \pmod 3,\\
&-\alpha+m_0+(\frac{p-1}{4})(m_1+m_2+m_3+m_4)\equiv 0 \pmod 3,\\
&D_0(1,0,1,2,1)=36k+19\equiv 1 \pmod 3,\\
&D_1(1,0,1,2,1)=2+4A+3B+3D+6E\equiv 2 \pmod 3,\\
&D_2(1,0,1,2,1)=2+3A+2B\\
&\qquad\qquad+C+2D+8E\equiv 2 \pmod 3.
\end{aligned}$$

By Theorem 8, we have that the code with generator matrix $B_p(1,1,0,1,2,1)$ is self-dual over GF(3).

Assume $n\equiv 1 \pmod 3$, then by Lemma 17 again,

$$\begin{aligned}
&\alpha+p=24k+14\equiv 2 \pmod 3,\\
&-\alpha+m_0+(\frac{p-1}{4})(m_1+m_2+m_3+m_4)\equiv 0 \pmod 3,\\
&D_0(1,0,0,1,1)=12k+7\equiv 1 \pmod 3,\\
&D_1(1,0,0,1,1)=1+A+B+2E\equiv 2 \pmod 3,\\
&D_2(1,0,0,1,1)=1+A+D+2E\equiv 2 \pmod 3.
\end{aligned}$$

TABLE IV
SOME CODES OBTAINED BY CONSTRUCTIONS $B_p(1,1,0,1,2,1)$ AND $B_p(1,1,0,0,1,1)$ OVER GF(3)

Code	Construction	Comments
$[28,14,9]$	$B_{13}(1,1,0,1,2,1)$	extremal
$[76,38,18]$	$B_{37}(1,1,0,0,1,1)$	highest known [15]
$[124,62,24]$	$B_{61}(1,1,0,0,1,1)$	highest known [18]

From Theorem 8, the code with generator matrix $B_p(1,1,0,0,1,1)$ is self-dual over GF(3). ■

Table IV gives examples of such codes. Note that all the codes in Table IV achieve the best-known lower bound on the minimum distance of general linear codes [18].

B. Self-Dual Codes Over GF(9)

In this subsection, we give two constructions of infinite families of self-dual codes over GF(9). Let ζ be the fixed primitive element of GF(9) satisfying the equation $\zeta^2+2\zeta+2=0$, then we have the following lemma.

Lemma 19: Let p be an odd prime having the form $24k+5$, where k is a nonnegative integer. Then $C\equiv 0 \pmod 3$ and $2+B+D+2E\equiv 0 \pmod 3$.

Proof: See the Appendix. ■

Then we have the following theorem.

Theorem 20: Let p be an odd prime having the form $24k+5$, where k is a nonnegative integer. Then the code with generator matrix $P_p(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7)$ is self-dual over GF(9) of length $2p$.

Proof: If $p=24k+5$, by Lemma 19 we have,

$$\begin{aligned} D_0(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7) &= 2,\\ D_1(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7) &= \zeta^7+\zeta^3B+\zeta^2C+\zeta^3D\\ &\quad +\zeta^7E\equiv 0 \pmod 3,\\ D_2(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7) &= \zeta^5+\zeta B+\zeta^6C+\zeta D\\ &\quad +\zeta^5E\equiv 0 \pmod 3. \end{aligned}$$

From Theorem 8, the code with generator matrix $P_p(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7)$ over GF(9) is self-dual of length $2p$. ■

For the case p is an odd prime of the form $24k+13$, we have the following theorem.

Theorem 21: Let p be an odd prime having the form $24k+13$. Then $p=x^2+y^2$, where $x=4m+1$, $y=4n+2$ for some integers $m,\ n$ satisfying $m\equiv 2 \pmod 3$ or $n\equiv 1 \pmod 3$. If $m\equiv 2 \pmod 3$ then the code with generator matrix $P_p(\zeta^2,1,\zeta^7,\zeta^5,\zeta^7)$ is self-dual over GF(9) of length $2p$.

Proof: If $p=24k+13$ and $m\equiv 2 \pmod 3$, then from Lemma 17,

$$\begin{aligned} D_0(\zeta^2,1,\zeta^7,\zeta^5,\zeta^7) &= 2+(6k+3)\zeta^5\equiv 2 \pmod 3,\\ D_1(\zeta^2,1,\zeta^7,\zeta^5,\zeta^7) &= \zeta^5+2A+\zeta^5C\equiv 0 \pmod 3,\\ D_2(\zeta^2,1,\zeta^7,\zeta^5,\zeta^7) &= \zeta^5+B+\zeta^6C\\ &\quad +D+E\equiv 0 \pmod 3. \end{aligned}$$

By Theorem 8, we get that the code with generator matrix $P_p(\zeta^2,1,\zeta^7,\zeta^5,\zeta^7)$ over GF(9) is self-dual of length $2p$. ■

TABLE V
SOME CODES OBTAINED BY CONSTRUCTIONS $P_p(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7)$ AND $P_p(\zeta^2,1,\zeta^7,\zeta^5,\zeta^7)$ OVER GF(9)

Code	Construction	Comments
$[10,5,6]$	$P_5(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7)$	extremal
$[26,13,10]$	$P_{13}(\zeta^2,1,\zeta^7,\zeta^5,\zeta^7)$	highest known [19]
$[58,29,18]$	$P_{29}(\zeta^2,\zeta,\zeta^7,\zeta,\zeta^7)$	highest known [18]

Table V gives examples of codes constructed by previous two theorems. The codes $[10,5,6]$ and $[58,29,18]$ achieve the best-known lower bound on the minimum distance of general linear codes [18].

Remark 22: We believe that it is also possible to obtain double circulant construction for the case $p=24k+13=x^2+y^2$, where $x=4m+1$, $y=4n+2$ for some integers $m,\ n$ satisfying $n\equiv 1 \pmod 3$. But the minimum prime satisfying this condition is 37, and it is difficult to determine the minimum distance of a self-dual $[74,37]$ code over GF(9).

Remark 23: It is also possible to obtain other pure double circulant (bordered double circulant) codes over GF(2), GF(3), GF(4), GF(8) and GF(9), but we only list the code having a good minimum distance.

V. AUTOMORPHISM GROUP

In this section we prove results concerning the permutation group of the double circulant codes. We first consider the automorphism group of the code constructed by $B_p(0,m_0,m_1,m_2,m_3,m_4)$ over GF(q), where p has the form $8k+5$ and q is a prime power. Following [14] we consider a linear space V_{p+1} of dimension $p+1$ over GF(q) and a set of its basis vectors: $e_\infty=(1,0,\ldots,0)$, $e_0=(0,1,\ldots,0),\ldots,\ e_{p-1}=(0,0,\ldots,1)$. Let g be the primitive element of GF(p) and

$$\chi(a)=\begin{cases} m_0; & \text{if } a=0,\\ m_1; & \text{if } a=g^{4i} \text{ for some } i,\\ m_2; & \text{if } a=g^{4i+1} \text{ for some } i,\\ m_3; & \text{if } a=g^{4i+2} \text{ for some } i,\\ m_4; & \text{if } a=g^{4i+3} \text{ for some } i. \end{cases}$$

We define the transformation S_p which acts on V_{p+1} as:

$$e_\infty S_p=\sum_{j=0}^{p-1}e_j,\ e_iS_p=\sum_{j=0}^{p-1}\chi(j-i)e_j,\ i=0,\ldots,p-1.$$

Now for any b in GF(p) we define $S(b)$ the shift transformation as:

$$e_\infty S(b)=e_\infty,\ e_iS(b)=e_{i+b},\ i=0,\ldots,p-1.$$

For $s\neq 0$, we define the biquadratic transformation $T(s^4)$ as:

$$e_\infty T(s^4)=e_\infty,\ e_iT(s^4)=e_{is^4},\ i=0,\ldots,p-1.$$

Then we have the following proposition.

Proposition 24: For any $b\in$ GF(p), $0\neq s\in$ GF(p) and for the transformation S_p defined on GF(q),

$$S_pS(b)=S(b)S_p \text{ and } S_pT(s^4)=T(s^4)S_p.$$

Proof: To prove the equalities we only need to compute separately the effect of the left hand side and the right hand side on the basis vectors:

$$e_\infty S_p S(b) = \sum_{j=0}^{p-1} e_j S(b) = \sum_{j=0}^{p-1} e_{j+b},$$
$$e_\infty S(b) S_p = e_\infty S_p = \sum_{j=0}^{p-1} e_j.$$

These two vectors are equal since $j+b$ ranges over all elements in GF(p) as j ranges over all values in GF(p). For $i = 0, \ldots, p-1$,

$$e_i S_p S(b) = \sum_{j=0}^{p-1} \chi(j-i) e_j S(b) = \sum_{j=0}^{p-1} \chi(j-i) e_{j+b},$$
$$e_i S(b) S_p = e_{i+b} S_p = \sum_{j=0}^{p-1} \chi(j-i-b) e_j,$$

these two vectors are equal. Hence $S_p S(b) = S(b) S_p$.

Since

$$e_\infty S_p T(s^4) = \sum_{j=0}^{p-1} e_j T(s^4) = \sum_{j=0}^{p-1} e_{js^4},$$
$$e_\infty T(s^4) S_p = e_\infty S_p = \sum_{j=0}^{p-1} e_j,$$

and for $i = 0, \ldots, p-1$,

$$e_i S_p T(s^4) = \sum_{j=0}^{p-1} \chi(j-i) e_j T(s^4) = \sum_{j=0}^{p-1} \chi(j-i) e_{js^4},$$
$$e_i T(s^4) S_p = e_{is^4} S_p = \sum_{j=0}^{p-1} \chi(j - is^4 - b) e_j,$$

hence $S_p T(s^4) = T(s^4) S_p$. ■

Now we define a group $R(p)$ (p has the form $8k+5$) generated by the following types of transformations:

1) the cyclic shifts: $x \mapsto x+b$, for b in GF(p),
2) the biquadratic transformations: $x \mapsto s^4 x$, for $s \neq 0$ in GF(p).

Then we have the following results:

Theorem 25: Any code over GF(q) *with generator matrix of the form* $B_p(0, m_0, m_1, m_2, m_3, m_4)$ *is invariant under the monomial group* $R(p)$ *applied simultaneously to both halves of the generator matrix* $B_p(0, m_0, m_1, m_2, m_3, m_4)$.

Proof: Since $B_p(0, m_0, m_1, m_2, m_3, m_4) = \begin{pmatrix} I & S_p \end{pmatrix}$. Then applying any transformation M among $S(b)$ and $T(s^4)$ we obtain by Proposition 24,

$$\begin{pmatrix} I & S_p \end{pmatrix} \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix} = \begin{pmatrix} M & S_p M \end{pmatrix} = \begin{pmatrix} M & M S_p \end{pmatrix}$$
$$= M \begin{pmatrix} I & S_p \end{pmatrix}.$$

This proves our result. ■

Theorem 26: The automorphism group of the code over GF(q) *with generator matrix of the form* $P_p(m_0, m_1, m_2, m_3, m_4)$ *contains a group of order* $\frac{p(p-1)}{4}$.

Proof: By construction the cyclic shifts: $x \to x+b$, for b in GF(p) and the biquadratic transformations: $x \to s^4 x$, for $s \neq 0$ in GF(p) can be applied simultaneously to both parts of the generator matrix and they form a group of order $\frac{p(p-1)}{4}$. ■

VI. Binary Fourth Power Residue Four Circulant Self-Dual Codes

In this section we define fourth power residue four circulant codes. In the same way we get an infinite family of binary self-dual codes.

Definition 27: Let $F_n(R_1, R_2)$ *be codes with generator matrix of the form*

$$\begin{pmatrix} & R_1 & R_2 \\ I_{2n} & & \\ & R_2^t & R_1^t \end{pmatrix},$$

where R_1, R_2 *are* $n \times n$ *circulant matrices. The code* $F_n(R_1, R_2)$ *is called a* ***four circulant code****. Suppose* p *is an odd prime of form* $8k+5$, R_1 *and* R_2 *are of the form* $m_0 I_p + m_1 A_1 + m_2 A_2 + m_3 A_3 + m_4 A_4$, *where* $m_i \in$ GF(q), $i = 0, 1, 2, 3, 4, 5$. *Then the code* $F_p(R_1, R_2)$ *is called* ***fourth power residue four circulant code****.*

Now we have the following theorem.

Theorem 28: Let p *be an odd prime of the form* $16k+13$, *then the code with generator matrix* $F_p(A_4, I_p + A_2 + A_3 + A_4)$ *over* GF(2) *is self-dual of length* $4p$.

Proof: If p has the form $16k+13$, then

$$F_p(A_4, I_p + A_2 + A_3 + A_4) F_p(A_4, I_p + A_2 + A_3 + A_4)^t$$
$$= I_{2p} + \begin{pmatrix} X & Y \\ Y & X \end{pmatrix},$$

where $X = (1 + A + 2B + 2D + 5E)(A_1 + A_3) + (2 + 4A + B + C + D + 3E)(A_2 + A_4) + (16k+13) I_p$ and $Y = 2A_4(I_p + A_2 + A_3 + A_4)$. Then by Lemma 10, $F_p(A_4, I_p + A_2 + A_3 + A_4) F_p(A_4, I_p + A_2 + A_3 + A_4)^t = 0$ over GF(2). So the code with generator matrix $F_p(A_4, I_p + A_2 + A_3 + A_4)$ over GF(2) is self-dual of length $4p$. ■

Example 29: Let $p = 13$. *Applying Theorem 28, we obtain a binary self-dual* [52, 26, 10] *code, which is optimal [15].*

VII. Conclusion

While self-dual codes are useful in data transmission, it is not easy to construct such codes with a large minimum distance. We even do not know any family of asymptotic good self-dual codes, although it has been proved to exist [27], [29]. The best-known infinite family of self-dual codes is the quadratic double circulant self-dual code, which has a square root bound for the minimum distance [9]. In this paper, we construct several infinite families of self-dual codes based on fourth power residues. Some of them lead to new codes with better parameters than previously known codes. Numerical experiments show the hint that our codes may have a similar bound as that of quadratic double circulant self-dual codes. These enrich the choices of methods to construct good self-dual codes.

We know that the most powerful decoding method for quadratic residue codes is permutation decoding, which makes use of the fact that these codes have large automorphism groups [28]. In Section V, we proved that the codes constructed in this paper have a large automorphism group, as well. It is very likely that our codes may also have a good decoding method.

Another notable point is that, in Section VI, we give an infinite family of binary four circulant self-dual codes from fourth power residues. Certainly we can also give similar constructions over other finite fields. We believe that these constructions will also lead to good self-dual codes, although we cannot give any examples since the lengths of codes have become very large.

It seems that the construction method by higher power residues is a rich source to obtain codes with good parameters. We expect that more good codes can be produced via this approach.

Appendix

A. Proof of the Lemma 9

Proof: Let $p = 16k + 5 = x^2 + y^2$, $x \equiv 1 \pmod 4$, $y \equiv g^{\frac{p-1}{4}} x \pmod p$. Then $x^2 \equiv 1 \pmod 8$, and so $y^2 \equiv 4 \pmod 8$, $y \equiv 2 \pmod 4$.

Suppose $x = 4m + 1$ and $y = 4s + 2$, then

$$16k + 5 = 16m^2 + 8m + 1 + 16s^2 + 16s + 4,$$

that is,

$$2k = 2m^2 + m + 2s^2 + 2s,$$

so $m \equiv 0 \pmod 2$, then there exists an integer t such that $m = 2t$.

Therefore,

$$2k = 8t^2 + 2t + 2s^2 + 2s,$$

i.e.,

$$k - t = 4t^2 + s^2 + s,$$

we get $k \equiv t \pmod 2$.

Hence, by Theorem 3, if $y \equiv 2 \pmod 8$, then

$$A \equiv C \equiv D \equiv E \equiv 0 \pmod 2,\ B \equiv 1 \pmod 2.$$

If $y \equiv 6 \pmod 8$, then

$$A \equiv B \equiv C \equiv E \equiv 0 \pmod 2,\ D \equiv 1 \pmod 2.$$

■

B. Proof of the Lemma 10

Proof: Assume that $p = 16k + 13 = x^2 + y^2$, $x \equiv 1 \pmod 4$, $y \equiv g^{\frac{p-1}{4}} x \pmod p$. We have $x^2 \equiv 1 \pmod 8$, and so $y^2 \equiv 4 \pmod 8$, $y \equiv 2 \pmod 4$.

Suppose $x = 4m + 1$ and $y = 4s + 2$, then

$$16k + 13 = 16m^2 + 8m + 1 + 16s^2 + 16s + 4,$$

it follows that,

$$2k + 1 = 2m^2 + m + 2s^2 + 2s,$$

which gives $m \equiv 1 \pmod 2$, thus there exists an integer t such that $m = 2t + 1$.

Therefore,

$$2k + 1 = 8t^2 + 8t + 2 + 2t + 1 + 2s^2 + 2s,$$

that is,

$$k = 4t^2 + 5t + s^2 + s + 1,$$

so $k + t \equiv 1 \pmod 2$.

Hence by Theorem 3, if $y \equiv 2 \pmod 8$, then

$$A \equiv C \equiv D \equiv 0 \pmod 2,\ B \equiv E \equiv 1 \pmod 2.$$

If $y \equiv 6 \pmod 8$, then

$$A \equiv B \equiv C \equiv 0 \pmod 2,\ D \equiv E \equiv 1 \pmod 2.$$

■

C. Proof of the Lemma 17

Proof: Suppose $m \not\equiv 2 \pmod 3$, then

$$24k + 13 = 16m^2 + 8m + 1 + 16n^2 + 16n + 4,$$

that is,

$$3k + 1 = 2m^2 + m + 2n^2 + 2n.$$

Then $n \equiv 1 \pmod 3$ since

$$2m^2 + m = \begin{cases} 0; & \text{if } m \equiv 0, 1 \pmod 3, \\ 1; & \text{if } m \equiv 2 \pmod 3, \end{cases}$$

and

$$2n^2 + 2n = \begin{cases} 0; & \text{if } n \equiv 0, 2 \pmod 3, \\ 1; & \text{if } n \equiv 1 \pmod 3. \end{cases}$$

If $m \equiv 2 \pmod 3$, then $4A = \frac{p-7+2x}{4} = \frac{24k+13-7+8m+2}{4} \equiv 0 \pmod 3$ and $16(C + 1) = 24k + 13 + 1 - 6x + 16 \equiv 0 \pmod 3$. Since A and $C + 1$ are integers, we see that $A \equiv 0 \pmod 3$ and $C + 1 \equiv 0 \pmod 3$. Furthermore,

$$\begin{aligned} &2(2B + C + 2D + 2E) \\ &\quad = \frac{2p + 2 + 4x}{4} + \frac{p + 1 - 6y}{8} + \frac{p - 3 - 2x}{4} \\ &\quad = 21k - m + 11 \\ &\quad \equiv 0 \pmod 3, \end{aligned}$$

and $2B+C+2D+2E$ is an integer, we have $2B+C+2D+2E \equiv 0 \pmod 3$.

If $n \equiv 1 \pmod 3$, then

$$\begin{aligned} &2(2 + A + B + 2E) \\ &\quad = 4 + \frac{p - 7 + 2x}{8} + \frac{p + 1 + 2x - 4y}{8} + \frac{p - 3 - 2x}{4} \\ &\quad = 12k - 2n + 8 \\ &\quad \equiv 0 \pmod 3, \end{aligned}$$

and

$$\begin{aligned}
&2(2+A+D+2E)\\
&\quad = 4+\frac{p-7+2x}{8}+\frac{p+1+2x+4y}{8}+\frac{p-3-2x}{4}\\
&\quad = 12k+2n+10\\
&\quad \equiv 0 \pmod 3.
\end{aligned}$$

Since $2+A+B+2E$ and $2+A+D+2E$ are integers, we have $2+A+B+2E \equiv 0 \pmod 3$ and $2+A+D+2E \equiv 0 \pmod 3$. ∎

D. Proof of the Lemma 19

Proof: Let $p = x^2 + y^2$ and $x \equiv 1 \pmod 4$. Assume $x = 4m + 1$ for some integer m. If $p = 24k + 5$ then by Theorem 3,

$$16C = p + 1 - 6x = 24k + 6 - 6x \equiv 0 \pmod 3.$$

Since C is an integer, then $C \equiv 0 \pmod 3$. Similarly, we have

$$\begin{aligned}
2+B+D+2E &= 2+\frac{p+1+2x}{8}+\frac{p-3-2x}{8}\\
&= 2+\frac{p-1}{4}\\
&= 6k+3\\
&\equiv 0 \pmod 3.
\end{aligned}$$

∎

ACKNOWLEDGMENTS

The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which were very helpful to the improvement of the presentation of this paper, and to Dr. Yongyi Mao, the associate editor, for his excellent editorial job.

REFERENCES

[1] K. T. Arasu and T. A. Gulliver, "Self-dual codes over F_p and weighing matrices," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2051–2055, Jul. 2001.

[2] E. F. Assmus, Jr., and J. D. Key, *Designs and Their Codes* (Cambridge Tracts in Mathematics), vol. 103. Cambridge, U.K.: Cambridge Univ. Press, 1992.

[3] E. F. Assmus, Jr., and H. F. Mattson, Jr., "New 5-designs," *J. Combinat. Theory*, vol. 6, no. 2, pp. 122–151, 1969.

[4] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums* (Canadian Mathematical Society Series of Monographs and Advanced Texts). New York, NY, USA: Wiley, 1998.

[5] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, 1997.

[6] S. Bouyuklieva and I. Bouyukliev, "An algorithm for classification of binary self-dual codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3933–3940, Jun. 2012.

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

[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[9] R. Calderbank, "A square root bound on the minimum weight in quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 332–337, May 1983.

[10] P. Charters, "Generalizing binary quadratic residue codes to higher power residues over larger fields," *Finite Fields Appl.*, vol. 15, no. 3, pp. 404–413, 2009.

[11] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups* (Grundlehren der Mathematischen Wissenschaften), vol. 290, 3rd ed. New York, NY, USA: Springer-Verlag, 1999.

[12] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Rep. Suppl.*, vol. 10, no. 10, p. vi+97, 1973.

[13] C. Ding, "Cyclic codes from cyclotomic sequences of order four," *Finite Fields Appl.*, vol. 23, pp. 8–34, Sep. 2013.

[14] P. Gaborit, "Quadratic double circulant codes over fields," *J. Combinat. Theory, A*, vol. 97, no. 1, pp. 85–107, 2002.

[15] P. Gaborit and A. Otmani. *Tables of Self-Dual Codes*. [Online]. Available: http://www.unilim.fr/pages_perso/philippe.gaborit/SD/index.html, accessed Mar. 9, 2015.

[16] P. Gaborit and A. Otmani, "Experimental constructions of self-dual codes," *Finite Fields Appl.*, vol. 9, no. 3, pp. 372–394, 2003.

[17] M. Garcia-Rodriguez, Y. Yañez, M. J. Garcia-Hernandez, J. Salazar, A. Turo, and J. A. Chavez, "Application of Golay codes to improve the dynamic range in ultrasonic Lamb waves air-coupled systems," *NDT E Int.*, vol. 43, no. 8, pp. 677–686, 2010.

[18] M. Grassl. (2007). *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. [Online]. Available: http://www.codetables.de, accessed Mar. 9, 2015.

[19] M. Grassl and T. A. Gulliver, "On circulant self-dual codes over small fields," *Designs, Codes Cryptogr.*, vol. 52, no. 1, pp. 57–81, 2009.

[20] T. A. Gulliver and M. Harada, "Classification of extremal double circulant self-dual codes of lengths 74–88," *Discrete Math.*, vol. 306, no. 17, pp. 2064–2072, 2006.

[21] M. Harada, "The existence of a self-dual [70, 35, 12] code and formally self-dual codes," *Finite Fields Appl.*, vol. 3, no. 2, pp. 131–139, 1997.

[22] M. Harada, M. Kiermaier, A. Wassermann, and R. Yorgova, "New binary singly even self-dual codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1612–1617, Apr. 2010.

[23] W. C. Huffman, "Automorphisms of codes with applications to extremal doubly even codes of length 48," *IEEE Trans. Inf. Theory*, vol. 28, no. 3, pp. 511–521, May 1982.

[24] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Appl.*, vol. 11, no. 3, pp. 451–490, 2005.

[25] M. Karlin, "New binary coding results by circulants," *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 81–92, Jan. 1969.

[26] C. W. H. Lam, L. Thiel, and S. Swiercz, "The nonexistence of finite projective planes of order 10," *Can. J. Math.*, vol. 41, no. 6, pp. 1117–1123, 1989.

[27] S. Ling and P. Solé, "Good self-dual quasi-cyclic codes exist," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1052–1053, Apr. 2003.

[28] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Mathematical Library), vol. 16. Amsterdam, The Netherlands: North Holland, 1977.

[29] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self dual codes exist," *Discrete Math.*, vol. 3, nos. 1–3, pp. 153–162, 1972.

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

[31] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory* (Algorithms and Computation in Mathematics), vol. 17. Berlin, Germany: Springer-Verlag, 2006.

[32] T. L. O'Donovan, P. A. Contla, and D. K. Das-Gupta, "Application of Golay codes and piezoelectric ultrasound transducer to biomedical noninvasive measurement," *IEEE Trans. Electr. Insul.*, vol. 28, no. 1, pp. 93–100, Feb. 1993.

[33] V. Pless, "Symmetry codes over GF(3) and new five-designs," *J. Combinat. Theory, A*, vol. 12, no. 1, pp. 119–142, 1972.

[34] E. M. Rains, "Shadow bounds for self-dual codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 134–139, Jan. 1998.

[35] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, vol. 2. Amsterdam, The Netherlands: North Holland, 1998, pp. 177–294.

[36] D. N. Semënovykh, "A generalization of quadratic residue codes to the case of residues of degrees three and four," *Diskret. Mat.*, vol. 17, no. 4, pp. 143–149, 2005.

[37] I. Trots, Y. Tasinkevych, A. Nowicki, and M. Lewandowski, "Golay coded sequences in synthetic aperture imaging systems," *Arch. Acoust.*, vol. 36, no. 4, pp. 913–926, 2011.

Tao Zhang is currently a Ph.D. student at Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include combinatorial design theory, coding theory, algebraic combinatorics, and their interactions.

Gennian Ge received the M.S. and Ph.D. degrees in mathematics from Suzhou University, Suzhou, Jiangsu, P. R. China, in 1993 and 1996, respectively. After that, he became a member of Suzhou University. He was a postdoctoral fellow in the Department of Computer Science at Concordia University, Montreal, QC, Canada, from September 2001 to August 2002, and a visiting assistant professor in the Department of Computer Science at the University of Vermont, Burlington, Vermont, USA, from September 2002 to February 2004. He was a full professor in the Department of Mathematics at Zhejiang University, Hangzhou, Zhejiang, P. R. China, from March 2004 to February 2013. Currently, he is a full professor in the School of Mathematical Sciences at Capital Normal University, Beijing, P. R. China. His research interests include the constructions of combinatorial designs and their applications to codes and crypts.

Dr. Ge is on the Editorial Board of *Journal of Combinatorial Designs*, *Science China Mathematics*, and *Applied Mathematics—A Journal of Chinese Universities*. He received the 2006 Hall Medal from the Institute of Combinatorics and its Applications.