Math. Commun. **25**(2020), 213–226

New binary self-dual codes via a variation of the four-circulant construction

Joe Gildea[1], Abidin Kaya[2] and Bahattin Yildiz[3,*]

[1] *Department of Mathematics, University of Chester, Parkgate Rd, Chester CH1 4BJ, UK*
[2] *Department of Engineering Fundamentals, Faculty of Engineering and Technology, Sampoerna University, L'Avenue Campus 12 780, Jakarta, Indonesia*
[3] *Department of Mathematics and Statistics, Northern Arizona University, Flagstaff, AZ 86 011, USA*

Received September 4, 2019; accepted May 12, 2020

Abstract. In this work, we provide a variation of the four-circulant construction for self-dual codes. By applying the constructions over the alphabets $\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2$, $\mathbb{F}_4 + u\mathbb{F}_4$, we were able to obtain extremal binary self-dual codes of lengths 40, 64 including new extremal binary self-dual codes of length 68. More precisely, 43 new extremal binary self-dual codes of length 68 with new parameters have been constructed.

AMS subject classifications: 94B05, 15B33

Key words: circulant matrices, extremal self-dual codes, Gray maps

1. Introduction

Binary self-dual codes have generated a considerable amount of interest in the literature for decades for their connections to many other mathematical structures and applications. They have an upper bound on their minimum distance, which is given by Conway and Sloane in [4], and finalized by Rains in [19] as $d \leq 4\lfloor \frac{n}{24} \rfloor + 6$, when $n \equiv 22 \pmod{24}$ and $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$, otherwise, where n is the length of the self-dual code. Self-dual codes meeting these bounds are called *extremal*.

There is an extensive literature on constructions for extremal binary self-dual codes. One of the main directions of research in the literature has been to construct extremal binary self-dual codes whose weight enumerators have new parameters that were not known to exist before. This comes from the works by Conway and Sloane in [4] and Dougherty et al. in [5], in which the possible weight enumerators of all extremal self-dual codes of lengths up to 100 were classified.

While the tools in constructing extremal binary self-dual codes may differ from taking a special matrix construction considering a certain automorphism or the neighboring construction, in all of these cases the final step is to do a computer search over a reduced set of possible inputs. Using the aforementioned tools reduces the search field considerably so that the search is now feasible within a reasonable time.

*Corresponding author. *Email addresses:* j.gildea@chester.ac.uk (J. Gildea), abidin.kaya@sampoernauniversity.ac.id (A. Kaya), bahattin.yildiz@nau.edu (B. Yildiz)

For most known constructions of self-dual codes, one of the key concepts is "circulant" matrices. It is well-known that circulant matrices are determined uniquely by their first rows and that they commute in matrix multiplication. The double-circulant, bordered double-circulant and four-circulant constructions are some of the well-known construction methods in the literature that make use of circulant matrices. Through these constructions the search field for a self-dual code of length $2n$ usually reduces to a constant multiple of 2^n, which makes it feasible to search for self-dual codes of lengths up to 88 for example.

In this work, we will be considering a generalized version of the four-circulant construction over the alphabets $\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ to construct extremal binary self-dual codes. Our construction, in general, is different than the four-circulant construction and we will be giving the comparative results. Using this construction, we are able to construct many extremal binary self-dual codes of lengths 40 and 64, and in particular, we are able to construct 43 new extremal binary self-dual codes of length 68 with new weight enumerators in $W_{68,2}$. The exact parameters in the weight enumerators are given in section 5.

The rest of the paper is organized as follows. In section 2, we give the preliminaries on the alphabets to be used, special types of matrices that we use in our constructions and the well known four-circulant construction. In section 3, we introduce our variation of the four-circulant construction and give theoretical results as to when they lead to self-dual codes as well as their connection to the ordinary four-circulant construction. In section 4, we give the numerical results of extremal binary self-dual codes of lengths 40 and 64 that we obtain by a direct application of our constructions over different alphabets together with a comparison with the usual four-circulant construction. In section 5, we apply the neighboring construction as well as extensions to the codes obtained in section 4 to find new extremal binary self-dual codes of length 68. We finish with concluding remarks and directions for possible future research.

2. Preliminaries

Let $\mathcal{R}$ be a commutative Frobenius ring of characteristic 2. A code $\mathcal{C}$ of length n over $\mathcal{R}$ is an $\mathcal{R}$-submodule of $\mathcal{R}^n$. Elements of the code $\mathcal{C}$ are called codewords of $\mathcal{C}$. Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of $\mathcal{R}^n$. The duality is understood in terms of the Euclidean inner product; $\langle x, y \rangle_E = \sum x_i y_i$. The dual $\mathcal{C}^\perp$ of the code $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp = \{x \in \mathcal{R}^n \mid \langle x, y \rangle_E = 0 \text{ for all } y \in \mathcal{C}\}.$$

We say that $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^\perp$.

Two self-dual binary codes of dimension k are said to be neighbors if their intersection has dimension $k - 1$.

Let $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ be the quadratic field extension of the binary field $\mathbb{F}_2 = \{0, 1\}$, where $\omega^2 + \omega + 1 = 0$. The ring $\mathbb{F}_4 + u\mathbb{F}_4$ defined via $u^2 = 0$ is a commutative binary ring of size 16. We may easily observe that it is isomorphic to $\mathbb{F}_2[\omega, u] / \langle u^2, \omega^2 + \omega + 1 \rangle$. The ring has a unique non-trivial ideal $\langle u \rangle = \{0, u, u\omega,$

$u + u\omega\}$. Note that $\mathbb{F}_4+u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2+u\mathbb{F}_2$ and so we can describe any element of $\mathbb{F}_4+u\mathbb{F}_4$ in the form $\omega a+\bar{\omega}b$ uniquely, where $a, b \in \mathbb{F}_2+u\mathbb{F}_2$.

$$\begin{array}{ccc} (\mathbb{F}_4+u\mathbb{F}_4)^n & \xrightarrow{\psi_{\mathbb{F}_4+u\mathbb{F}_4}} & (\mathbb{F}_2+u\mathbb{F}_2)^{2n} \\ \downarrow \varphi_{\mathbb{F}_4+u\mathbb{F}_4} & & \downarrow \varphi_{\mathbb{F}_2+u\mathbb{F}_2} \\ \mathbb{F}_4^{2n} & \xrightarrow{\psi_{\mathbb{F}_4}} & \mathbb{F}_2^{4n} \end{array}$$

Let us recall the following Gray maps from [8, 18] and [6];

$$\begin{aligned} \psi_{\mathbb{F}_4} &: a\omega + b\overline{\omega} \mapsto (a, b)\,, \quad a, b \in \mathbb{F}_2^n \\ \varphi_{\mathbb{F}_2+u\mathbb{F}_2} &: a + bu \mapsto (b, a + b)\,, \quad a, b \in \mathbb{F}_2^n \\ \psi_{\mathbb{F}_4+u\mathbb{F}_4} &: a\omega + b\overline{\omega} \mapsto (a, b)\,, \quad a, b \in (\mathbb{F}_2+u\mathbb{F}_2)^n \\ \varphi_{\mathbb{F}_4+u\mathbb{F}_4} &: a + bu \mapsto (b, a + b)\,, \quad a, b \in \mathbb{F}_4^n \end{aligned}$$

Note that these Gray maps preserve orthogonality in the respective alphabets; for the details we refer to [18]. The binary codes $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ are equivalent. The Lee weight of an element in $\mathbb{F}_4 + u\mathbb{F}_4$ is defined to be the Hamming weight of its binary image under any of the previously mentioned compositions of the maps. A self-dual code is said to be of Type II if the Lee weights of all codewords are multiples of 4, otherwise it is said to be of Type I.

Proposition 1 (see [18])**.** *Let $\mathcal{C}$ be a code over $\mathbb{F}_4 + u\mathbb{F}_4$. If $\mathcal{C}$ is self-orthogonal, so are $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$. The code $\mathcal{C}$ is a Type I (resp. Type II) code over $\mathbb{F}_4 + u\mathbb{F}_4$ if and only if $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a Type I (resp. Type II) $\mathbb{F}_4$-code, if and only if $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a Type I (resp. Type II) $\mathbb{F}_2 + u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of $\mathcal{C}$ is the same as the minimum Lee weight of $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$.*

Corollary 1. *Suppose that $\mathcal{C}$ is a self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$ of length n and the minimum Lee distance d. Then $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a binary $[4n, 2n, d]$ self-dual code. Moreover, $\mathcal{C}$ and $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ have the same weight enumerator. If $\mathcal{C}$ is Type I (Type II), then so is $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$.*

In subsequent sections we will write tables in which vectors with elements from the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ will appear. In order to avoid writing long vectors with elements that can be confused with other elements, we will describe the elements of this ring in a shorthand way, which will make the tables more compact.

For the elements of $\mathbb{F}_2 + u\mathbb{F}_2$, we will use $0 \to 0, 1 \to 1, u \to u$ and $1 + u \to 3$.

For the elements of $\mathbb{F}_4+u\mathbb{F}_4$, we use the ordered basis $\{u\omega, \omega, u, 1\}$ to express the elements of $\mathbb{F}_4+u\mathbb{F}_4$ as binary strings of length 4. Then we will use the hexadecimal number system to describe each element:

$0 \leftrightarrow 0000$, $1 \leftrightarrow 0001$, $2 \leftrightarrow 0010$, $3 \leftrightarrow 0011$, $4 \leftrightarrow 0100$, $5 \leftrightarrow 0101$, $6 \leftrightarrow 0110$, $7 \leftrightarrow 0111$, $8 \leftrightarrow 1000$, $9 \leftrightarrow 1001$, A $\leftrightarrow 1010$, B $\leftrightarrow 1011$, C $\leftrightarrow 1100$, D $\leftrightarrow 1101$, E $\leftrightarrow 1110$, F $\leftrightarrow 1111$.

For example, $1+u\omega$ corresponds to 1001, which is represented by the hexadecimal 9, while $\omega + u\omega$ corresponds to 1100, which is represented by C.

We are going to use the following extension method for computational results.

Theorem 1 (see [7]). *Let R be a commutative ring of characteristic 2 with identity. Let C be a self-dual code over R of length n and let $G = (r_i)$ be a $k \times n$ generator matrix for C, where r_i is the i-th row of G, $1 \leq i \leq k$. Let c be a unit in R such that $c^2 = 1$ and let X be a vector in R^n with $\langle X, X \rangle = 1$. Let $y_i = \langle r_i, X \rangle$ for $1 \leq i \leq k$. Then the following matrix*

$$\left[\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array}\right],$$

generates a self-dual code D over R of length $n + 2$.

2.1. Special matrices

Circulant matrices play an important role in many applications. In this section, we briefly recall circulant matrices and its variations in the form of reverse-circulant and λ-circulant matrices.

With R a commutative ring with identity, let σ be the permutation on R^n that corresponds to the right shift, i.e.

$$\sigma(a_1, a_2, \ldots, a_n) = (a_n, a_1, \ldots, a_{n-1}).$$

A circulant matrix is a square matrix where each row is a right-circular shift of the previous row. In other words, if $\overline{r}$ is the first row, a typical circulant matrix is of the form

$$\left[\begin{array}{c} \overline{r} \\ \hline \sigma(\overline{r}) \\ \hline \sigma^2(\overline{r}) \\ \hline \vdots \\ \hline \sigma^{n-1}(\overline{r}) \end{array}\right].$$

It is clear that, with T denoting the permutation matrix corresponding to the n-cycle $(123...n)$, a circulant matrix with the first row $(a_1, a_2, \ldots, a_n)$ can be expressed as a polynomial in T as:

$$a_1 I_n + a_2 T + a_3 T^2 + \cdots + a_n T^{n-1},$$

with $T^n = I_n$. This shows that circulant matrices commute.

A reverse-circulant matrix is a square matrix where each row is a left-circular shift of the previous row. It is clear to see that if $\overline{r}$ is the first row, a reverse-circulant matrix is of the form

$$\left[\begin{array}{c} \overline{r} \\ \hline \sigma^{-1}(\overline{r}) \\ \hline \sigma^{-2}(\overline{r}) \\ \hline \vdots \\ \hline \sigma^{-(n-1)}(\overline{r}) \end{array}\right].$$

An $n \times n$ square matrix A is called λ-circulant if every row is a λ-cyclic shift of the previous one, in other words, A is in the following form;

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ \lambda a_n & a_1 & a_2 & \cdots & a_{n-1} \\ \lambda a_{n-1} & \lambda a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda a_2 & \lambda a_3 & \lambda a_4 & \cdots & a_1 \end{pmatrix}.$$

λ-circulant matrices are an immediate generalization of circulant matrices and like circulant matrices, two λ-circulant matrices also commute. Recently, λ-circulant matrices were used in [17] to construct formally self-dual codes.

λ-reverse-circulant matrices can also be defined in exactly the same way as an extension of reverse circulant matrices.

The following lemma gives us an important result that will be used in the upcoming sections.

Lemma 1 (see [16]). *Let A and C be λ-circulant matrices. Then $C' = CR$ is a λ-reverse-circulant matrix and it is symmetric. Here R is a back-diagonal matrix. Moreover, $AC' - C'A^T = 0$. Equivalently, $ARC^T - CRA^T = 0$.*

A special case of Lemma 1 is as follows;

Lemma 2. *Symmetric circulant matrices commute with reverse circulant matrices.*

2.2. On the four-circulant construction

The four-circulant construction, which was inspired by orthogonal designs, was introduced in [2]:

Theorem 2 (see [2]). *Let A and B be $n \times n$ circulant matrices over $\mathbb{F}_p$ such that $AA^T + BB^T = -I_n$. Then the matrix*

$$G = \left(I_{2n} \,\middle|\, \begin{matrix} A & B \\ -B^T & A^T \end{matrix} \right)$$

generates a self-dual code over $\mathbb{F}_p$.

Recently, the four-circulant construction was applied on $\mathbb{F}_2 + u\mathbb{F}_2$ in [12], which resulted in a new binary self-dual code of length 64.

The following is a variation of the four-circulant construction, which was used in [16] to obtain new extremal binary self-dual codes.

Theorem 3 (see [16]). *Let λ be a unit of the commutative Frobenius ring $\mathcal{R}$, A a λ-circulant matrix and B a λ-reverse-circulant matrix with $AA^T + BB^T = -I_n$. Then the matrix*

$$G = \left(I_{2n} \,\middle|\, \begin{matrix} A & B \\ -B & A \end{matrix} \right)$$

generates a self-dual code $\mathcal{C}$ over $\mathcal{R}$.

3. A variation of the four-circulant construction

In this section, we propose a modification of the four-circulant construction. We also propose two specific variations of the construction.

Theorem 4. *Let $\mathcal{R}$ be a commutative Frobenius ring of characteristic 2, A and B circulant matrices and C a reverse circulant matrix. Then the code generated by*

$$G := \left(\begin{array}{c|cc} I_{2n} & \begin{matrix} A & B+C \\ B^T+C & A^T \end{matrix} \end{array} \right)$$

is self-dual when $AA^T + BB^T + C^2 = I_n$ and $AC = CA$.

Proof. Let $M := \begin{pmatrix} A & B+C \\ B^T+C & A^T \end{pmatrix}$. We are to show that $MM^T = I_{2n}$ under the given conditions. Indeed

$$\begin{aligned} MM^T &= \begin{pmatrix} AA^T + BB^T + BC + CB^T + C^2 & AB + AC + BA + CA \\ B^TA^T + CA^T + A^TB^T + A^TC & B^TB + B^TC + CB + C^2 + A^TA \end{pmatrix} \\ &= \begin{pmatrix} AA^T + BB^T + C^2 & AC + CA \\ CA^T + A^TC & B^TB + C^2 + A^TA \end{pmatrix} = \begin{pmatrix} I_n & 0_n \\ 0_n & I_n \end{pmatrix}. \end{aligned}$$

The above equality holds because we have $AB = BA$ and $A^TB^T = B^TA^T$ since circulant matrices commute and also because by Lemma 1 $BC + CB^T = 0$ and $B^TC + CB = 0$. □

Remark 1. *Note that when $C = 0$ in Theorem 4 we get the ordinary four-circulant construction. Hence, the variation is also a generalization of the four-circulant construction when the characteristic is 2.*

We obtain the following corollary when A is a symmetric circulant matrix:

Corollary 2. *Let $\mathcal{R}$ be a commutative Frobenius ring of characteristic 2, A a symmetric circulant matrix, B a circulant matrix and C a reverse circulant matrix. Then the code generated by*

$$G := \left(\begin{array}{c|cc} I_{2n} & \begin{matrix} A & B+C \\ B^T+C & A \end{matrix} \end{array} \right)$$

is a self-dual code over $\mathcal{R}$ whenever $A^2 + BB^T + C^2 = I_n$.

Proof. It follows by Theorem 4 and Lemma 2. □

We may also propose another special case of Theorem 4.

Corollary 3. *Let $\mathcal{C}$ be a self-dual four-circulant code of length $4n$ over $\mathcal{R}$ (of characteristic 2) generated by*

$$G := \left(\begin{array}{c|cc} I_{2n} & \begin{matrix} A & B \\ B^T & A^T \end{matrix} \end{array} \right).$$

Then for any reverse circulant matrix C, which commutes with A and satisfies $C^2 = 0$, the matrix

$$\left(\begin{array}{c|cc} I_{2n} & A & B+C \\ & B^T+C & A^T \end{array} \right)$$

generates a self-dual code $\mathcal{C}'$.

Corollary 3 allows us to reduce the size of the search field for that specific variation. We may consider a four-circulant code and search for reverse circulant matrices C under the restrictions.

Example 1. *Let $n = 7$ and $\mathcal{C}$ be the four-circulant code where $A = I_7$ and $B = 0_7$, i.e. $r_A = (1,0,0,0,0,0,0)$ and $r_B = (0,0,0,0,0,0,0)$. The code $\mathcal{C}$ is binary self-dual with parameters $[28,14,2]$. Let C be the reverse circulant matrix with the first row $r_C = (1110100)$ which satisfies $C^2 = 0_7$, and obviously it commutes with A. Then the code $\mathcal{C}'$ obtained by Corollary 3 is an extremal binary self-dual $[28,14,6]$ code with an automorphism group of order $2^6 \times 3 \times 7$.*

4. Computational results

In this section, we provide examples to demonstrate the effectiveness of the methods introduced in Section 3. We also compare the methods with the well known four-circulant construction for various lengths over the alphabets $\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$.

4.1. Applying constructions over $\mathbb{F}_2$ for length 40

We construct Type I self-dual codes of length 40 by the four-circulant construction and also by the methods given in Section 3. The weight enumerator of a singly even binary self-dual code of parameters $[40,20,8]$ is in the following form:

$$W_{40} = 1 + (125 + 16\beta)\, y^8 + (1664 - 64\beta)\, y^{10} + \cdots, 0 \leq \beta \leq 10.$$

The nonexistence of a code with $\beta = 9$ has been proven in [10]. The codes exist for all possible weight enumerators. In Table 1, we list four-circulant self-dual binary codes of length 40.

$\mathcal{C}_{40,i}$	r_A	r_B	$\lvert Aut(\mathcal{C}_{40,i})\rvert$	β in W_{40}
$\mathcal{C}_{40,1}$	(0100001110)	(0100110011)	$2^2 \times 5$	0
$\mathcal{C}_{40,2}$	(0000110011)	(0010111001)	$2^3 \times 5$	0
$\mathcal{C}_{40,3}$	(0101100111)	(1111001011)	$2^3 \times 3 \times 5$	0
$\mathcal{C}_{40,4}$	(1001000100)	(0101101101)	$2^{14} \times 3 \times 5$	10
$\mathcal{C}_{40,5}$	(1000000010)	(1101011101)	$2^{16} \times 3^3 \times 5^2$	10

Table 1: $[40,20,8]$ *four-circulant codes*

We apply Corollary 3 to $\mathcal{C}_{40,4}$ from Table 1. In other words, we fix the circulant matrices A and B and search for reverse circulant matrices which satisfy the given conditions. The results are given in Table 2. The results have shown the method to be quite effective.

$\mathcal{E}_{40,i}$	r_C	$\lvert Aut(\mathcal{E}_{40,i})\rvert$	β in W_{40}
$\mathcal{E}_{40,1}$	(1101011010)	2^3	0
$\mathcal{E}_{40,2}$	(1100011000)	2^2	2
$\mathcal{E}_{40,3}$	(0111001110)	2^3	2
$\mathcal{E}_{40,3}$	(0100001000)	2^8	2
$\mathcal{E}_{40,4}$	(0011100111)	2^{13}	2
$\mathcal{E}_{40,5}$	(0111101111)	2^{11}	4
$\mathcal{E}_{40,6}$	(1010010100)	2^8	6
$\mathcal{E}_{40,7}$	(1101011010)	$2^8 \times 3$	6
$\mathcal{E}_{40,8}$	(1000110001)	2^{15}	10
$\mathcal{E}_{40,9}$	(1111011110)	2^{16}	10

Table 2: $[40, 20, 8]$ *codes by Corollary 3 for* $\mathcal{C}_{40,4}$

4.2. Applying constructions over $\mathbb{F}_2$ for length 64

There are two possibilities for the weight enumerators of extremal Type I self-dual codes of length 64 (hence of parameters $[64, 32, 12]$) ([4]):

$$W_{64,1} = 1 + (1312 + 16\beta)\, y^{12} + (22016 - 64\beta)\, y^{14} + \cdots, 14 \leq \beta \leq 284,$$
$$W_{64,2} = 1 + (1312 + 16\beta)\, y^{12} + (23040 - 64\beta)\, y^{14} + \cdots, 0 \leq \beta \leq 277.$$

With the most updated information, [1, 14], extremal singly even self-dual codes with weight enumerator $W_{64,1}$ are known for

$$\beta \in \left\{ \begin{array}{l} 14, 16, 18, 20, 22, 24, 25, 26, 28, 29, 30, 32, 34 \\ 35, 36, 38, 39, 44, 46, 48, 50, 53, 59, 60, 64, 74 \end{array} \right\}$$

and extremal self-dual codes with weight enumerator $W_{64,2}$ are known for

$$\beta \in \left\{ \begin{array}{l} 0, 1, ..., 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 65, \\ 72, 80, 88, 96, 104, 108, 112, 114, 118, 120, 184 \end{array} \right\} \setminus \{31, 39\}.$$

Self-dual four-circulant $[64, 32, 12]_2$ Type I codes exist for weight enumerators $\beta = 0, 8, 16, 24, 32, 40, 48, 56, 64$ and 72 in $W_{64,2}$. We provide codes obtained from Corollary 2 in Table 3. The results show that the limited version of the generalized four-circulant construction gives some codes which do not have four-circulant representation (The ones with $\beta = 4, 10, 12, 13, 17, 18, 20, 28, 34$.)

$\mathcal{C}_i$	r_A	r_B	r_C	$\lvert Aut(\mathcal{C}_i)\rvert$	β
$\mathcal{C}_1$	(101001111)	(0001111001100011)	(1101001110011001)	2^3	4
$\mathcal{C}_2$	(001101011)	(0101001000001001)	(0101011110111101)	2^4	8
$\mathcal{C}_3$	(111101110)	(0011110000111101)	(0101011110111101)	2^5	8
$\mathcal{C}_4$	(111101011)	(0000100001000001)	(0100000011001101)	2^3	10
$\mathcal{C}_5$	(101101111)	(1000101000101000)	(0010111110100010)	2^4	12
$\mathcal{C}_6$	(100110100)	(0001001001111111)	(0101011110111101)	2^3	13
$\mathcal{C}_7$	(100011101)	(1010110001101011)	(1100111001100100)	2^4	16
$\mathcal{C}_8$	(110001001)	(0010111110100010)	(1100011011111000)	2^3	17
$\mathcal{C}_9$	(000011110)	(0000011101110111)	(0100000011001101)	2^3	18
$\mathcal{C}_{10}$	(101101100)	(1111001000100111)	(1100101101001011)	2^4	20
$\mathcal{C}_{11}$	(000011100)	(0010001101001111)	(0101011110111101)	2^3	24
$\mathcal{C}_{12}$	(010111001)	(1010000110110000)	(0100010001011111)	2^4	24
$\mathcal{C}_{13}$	(010010011)	(0000000100000101)	(0101011110111101)	2^4	28
$\mathcal{C}_{14}$	(111011011)	(0100000101111111)	(0001010001000001)	2^4	32
$\mathcal{C}_{15}$	(011111000)	(1000101000100010)	(0001001101000011)	2^3	34

Table 3: *Type I extremal self-dual codes of length 64 by Corollary 2* ($W_{64,2}$)

Remark 2. *The first code with weight enumerator $\beta = 34$ in $W_{64,2}$ has been recently constructed in [1]. Here we give an alternative construction.*

4.3. Applying constructions over $\mathbb{F}_2 + u\mathbb{F}_2$

In this section, we compare two methods: four-circulant construction and a variation of the four-circulant construction over $\mathbb{F}_2 + u\mathbb{F}_2$ for length 32. A complete classification of four-circulant codes of length 32 over $\mathbb{F}_2 + u\mathbb{F}_2$ is given by Karadeniz et al. in [12]. Four-circulant type I codes of length 32 have binary images corresponding to weight enumerators with $\beta = 0, 16, 32, 48$ and 80 in $W_{64,2}$. In Table 4, we provide codes obtained by the main construction. It is observed that the latter method is more efficient as it produces many more codes of length 64 with parameters that could not be obtained by the ordinary four-circulant construction.

$\mathcal{F}_i$	r_A	r_B	r_C	$\lvert Aut(\mathcal{F}_i)\rvert$	β
1	$(0,u,0,0,1,u,3,0)$	$(u,u,u,0,0,1,1,3)$	$(0,u,3,0,0,u,3,0)$	2^4	0
2	$(u,u,0,u,1,u,1,u)$	$(u,u,u,0,0,1,1,3)$	$(0,0,3,0,0,0,3,0)$	2^5	0
3	$(u,u,u,u,1,u,3,u)$	$(u,u,u,0,0,1,1,3)$	$(u,u,1,u,u,u,1,u)$	2^6	0
4	$(u,0,u,0,0,1,u,3)$	$(u,u,u,u,0,1,1,1)$	$(1,u,3,0,3,u,1,0)$	2^3	4
5	$(u,u,u,u,1,1,3,1)$	$(u,u,0,1,0,0,1,3)$	$(u,u,0,u,u,u,0,u)$	2^4	4
6	$(0,u,0,u,1,u,3,u)$	$(u,u,u,0,0,1,1,3)$	$(u,0,3,0,u,0,3,0)$	2^5	4
7	$(0,u,0,u,1,1,0,1)$	$(u,u,0,u,1,1,1,3)$	$(u,0,u,0,u,3,u,3)$	2^3	8
8	$(u,0,0,u,1,u,1,0)$	$(u,u,u,u,0,1,1,1)$	$(u,0,1,0,u,0,1,0)$	2^4	8
9	$(u,u,u,u,1,1,u,1)$	$(u,u,u,u,u,1,0,1)$	$(u,0,u,u,1,3,1,1)$	2^5	8
10	$(u,u,0,0,1,1,0,3)$	$(u,u,0,u,1,1,1,3)$	$(u,u,0,u,u,1,0,1)$	2^3	12
11	$(u,u,u,u,0,1,0,3)$	$(u,u,u,u,0,1,1,1)$	$(1,u,3,u,1,u,3,u)$	2^4	12

12	$(0,u,0,u,0,1,u,3)$	$(u,u,u,0,0,1,1,3)$	$(1,0,3,0,1,0,3,0)$	2^5	12
13	$(u,0,0,0,u,1,u,3)$	$(u,u,u,0,0,1,1,3)$	$(1,u,3,u,1,u,3,u)$	2^6	12
14	$(u,0,u,0,1,1,u,1)$	$(u,u,u,u,u,1,0,1)$	$(0,0,0,u,1,3,1,1)$	2^4	16
15	$(u,u,u,u,0,1,0,3)$	$(u,u,u,u,0,1,1,1)$	$(3,0,3,0,3,0,3,0)$	2^5	16
16	$(u,u,0,u,u,1,u,3)$	$(u,u,u,0,0,1,1,3)$	$(3,0,3,0,3,0,3,0)$	2^6	16
17	$(0,0,u,0,0,1,0,3)$	$(u,u,u,0,0,1,1,3)$	$(3,0,3,0,3,0,3,0)$	2^7	16
18	$(u,u,u,u,1,1,u,1)$	$(u,u,0,0,u,1,u,3)$	$(u,u,u,0,3,3,3,1)$	2^3	20
19	$(u,0,0,u,1,u,1,0)$	$(u,u,u,u,0,1,1,1)$	$(0,0,1,0,0,0,1,0)$	2^4	20
20	$(u,u,u,u,1,1,0,1)$	$(u,u,0,u,1,3,3,1)$	$(u,u,u,u,u,3,0,3)$	2^3	24
21	$(u,0,0,u,0,1,u,1)$	$(u,u,u,u,0,1,1,1)$	$(3,u,3,0,3,u,3,0)$	2^4	24
22	$(u,u,0,u,0,1,0,1)$	$(u,u,u,0,0,u,0,1)$	$(1,0,1,0,1,3,1,3)$	2^5	24
23	$(u,0,0,0,u,1,u,3)$	$(u,u,u,0,0,1,1,3)$	$(1,u,3,0,1,u,3,0)$	2^4	28
24	$(u,u,u,u,u,1,0,3)$	$(u,u,u,0,0,1,1,3)$	$(1,u,1,0,1,u,1,0)$	2^5	32
25	$(u,u,0,0,1,0,1,u)$	$(u,u,u,u,0,1,1,1)$	$(u,0,3,0,u,0,3,0)$	2^4	36
26	$(u,u,u,0,1,u,3,0)$	$(u,u,u,0,0,1,1,3)$	$(u,u,3,u,u,u,3,u)$	2^5	36
27	$(0,u,u,0,0,1,0,1)$	$(u,u,u,0,0,1,1,3)$	$(1,0,3,0,1,0,3,0)$	2^4	44
28	$(0,u,u,0,0,1,0,1)$	$(u,u,u,0,0,1,1,3)$	$(1,u,1,u,1,u,1,u)$	2^5	48
29	$(u,0,u,0,u,1,0,3)$	$(u,u,u,0,0,1,1,3)$	$(3,u,3,u,3,u,3,u)$	2^7	80

Table 4: $[64,32,12]$ *codes via Theorem 4 over* $\mathbb{F}_2+u\mathbb{F}_2$ *(*$W_{64,2}$*)*

4.4. Computational results over $\mathbb{F}_4+u\mathbb{F}_4$

Four-circulant codes of length 16 over $\mathbb{F}_4+u\mathbb{F}_4$ were studied in [15]. The binary images of these codes are Type I extremal self-dual binary codes with weight enumerators $\beta = 0,4,8,12,24,28,32,36,40,48$ and 52 in $W_{64,2}$. We apply Corollary 2 and observe that it provides many new parameters that could not be constructed from the four-circulant construction. The results are presented in Table 5. The Gray images of the codes are extremal binary self-dual codes of length 64 by Corollary 1.

$\mathcal{E}_i$	r_A	r_B	r_C	$\lvert Aut(\mathcal{E}_i)\rvert$	β in $W_{64,2}$
$\mathcal{E}_1$	(D,F,5,F)	(E,C,0,1)	(7,B,4,A)	2^3	1
$\mathcal{E}_2$	(5,B,D,B)	(A,E,B,D)	(7,F,1,8)	2^3	5
$\mathcal{E}_3$	(B,9,D,9)	(2,E,9,7)	(D,7,1,2)	2^3	9
$\mathcal{E}_4$	(D,F,F,F)	(E,E,9,8)	(A,6,9,7)	2^3	13
$\mathcal{E}_5$	(9,7,7,7)	(0,F,C,0)	(4,1,F,A)	2^3	17
$\mathcal{E}_6$	(F,9,7,9)	(2,4,3,F)	(F,5,B,8)	2^3	21
$\mathcal{E}_7$	(D,0,F,0)	(9,E,C,A)	(D,B,4,2)	2^3	29
$\mathcal{E}_8$	(5,8,6,8)	(F,5,E,8)	(0,8,9,7)	2^5	40
$\mathcal{E}_9$	(B,4,4,4)	(7,E,8,D)	(0,6,4,2)	2^5	52

Table 5: *Self-dual codes via Corollary 2 over* $\mathbb{F}_4+u\mathbb{F}_4$ *of length 16 whose binary images are self-dual codes of length 64*

Remark 3. *The codes with weight enumerators for 1, 5, 13, 17, 21, 29 and 52 were first constructed in [11] as R_3, lifts of the extended binary Hamming code. These are reconstructed by a circulant construction in Table 5.*

5. New extremal binary self-dual codes of length 68

By [3, 10], a possible weight enumerator of an extremal binary self-dual code of length 68 (of parameters $[68, 34, 12]$) is in one of the following forms:

$$W_{68,1} = 1 + (442 + 4\beta)\, y^{12} + (10864 - 8\beta)\, y^{14} + \cdots, 104 \le \beta \le 1358,$$
$$W_{68,2} = 1 + (442 + 4\beta)\, y^{12} + (14960 - 8\beta - 256\gamma)\, y^{14} + \cdots,$$

where $0 \le \gamma \le 9$. Recently, Yankov et al. constructed the first examples of codes with a weight enumerator for $\gamma = 7$ in $W_{68,2}$. Together with these, including the ones obtained in [13], the existence of codes in $W_{68,2}$ is known for many values. In order to save space we only give the lists for $\gamma = 5$ and $\gamma = 6$, which are updated in this work;

$$\gamma = 5 \text{ with } \beta \in \{113,116,...,182,187,189,191,193\};$$
$$\gamma = 6 \text{ with } \beta \in \{2m | m = 69,\ 77,\ 78,\ 79,\ 81,\ 88\}.$$

We construct 36 new codes with parameter $\gamma = 6$ and 7 codes with $\gamma = 5$ in $W_{68,2}$.

We first construct two new codes of length 68 by applying the extension method described in Theorem 1 over $\mathbb{F}_2 + u\mathbb{F}_2$ to $\mathcal{F}_2$ from Table 4.

$\mathcal{D}_{68,i}$	$\mathcal{F}_i$	c	X	γ	β
$\mathcal{D}_{68,1}$	2	1	$(31u011u30uu113u3333u11u010301101)$	**5**	**101**
$\mathcal{D}_{68,2}$	2	$1+u$	$(130031u300013101313u31uu301u3103)$	**5**	**105**

Table 6: *New codes of length* 68 *as extensions of codes in Table 4 by Theorem 1*

Now, applying the neighboring construction to the codes obtained in Table 6, we get the following new codes of length 68:

$\mathcal{N}_{68,i}$	$\mathcal{D}_{68,i}$	x	γ	β
$\mathcal{N}_{68,1}$	2	(10101110010111000101000000010000000)	**5**	**109**
$\mathcal{N}_{68,2}$	2	(00001100110110101111011100100011100)	**5**	**111**
$\mathcal{N}_{68,3}$	2	(00001111100111111111011010001100000)	**5**	**112**
$\mathcal{N}_{68,4}$	2	(11011100000010010111001011000101010)	**5**	**114**
$\mathcal{N}_{68,5}$	1	(11101101000000010011000000111001010)	**5**	**115**
$\mathcal{N}_{68,6}$	2	(10010100010101011100101111101110000)	**6**	**133**

Table 7: *New codes of length* 68 *as neighbors of codes in Table 6*

Example 2. *Let $\mathcal{C}_{68}$ be the code obtained by extending $\varphi(\mathcal{E}_6)$ over $\mathbb{F}_2 + u\mathbb{F}_2$, where $X = (3, 0, 1, 1, u, 0, u, 3, 0, 1, 1, u, 1, 0, 0, u, 3, 0, 0, u, u, u, 1, 3, 3, 0, 1, 3, 1, u, 0, 3)$, then the binary image of $\mathcal{C}_{68}$ is an extremal self-dual $[68, 34, 12]$ code with the weight*

enumerator for $\gamma = 6$ and $\beta = 157$ in $W_{68,2}$. As listed above, only 6 codes with $\gamma = 6$ were known before. So this is the first example of a self-dual code with the corresponding weight enumerator.

Without loss of generality, we consider a standard form of the generator matrix of $\varphi(\mathcal{C}_{68})$. Let $x \in \mathbb{F}_2^{68} - \varphi(\mathcal{C}_{68})$. Then $D = \left\langle \langle x \rangle^{\perp} \cap \varphi(\mathcal{C}_{68}), x \right\rangle$ is a neighbor of $\varphi(\mathcal{C}_{68})$. The first 34 entries of x are set to 0, the rest of the vectors are listed in Table 8. As neighbors of $\varphi(\mathcal{C}_{68})$, we obtain 34 new codes with weight enumerators for $\gamma = 6$ in $W_{68,2}$, which are listed in Table 8. All the codes have an automorphism group of order 2.

$\mathcal{C}_{68,i}$	X	β
$\mathcal{C}_{68,1}$	(11111111001111000011000001000000111)	137
$\mathcal{C}_{68,2}$	(01010010010011111111011100010111011)	139
$\mathcal{C}_{68,3}$	(10000011000001101101100000111100010)	140
$\mathcal{C}_{68,4}$	(00100111011101100110011101101101110)	141
$\mathcal{C}_{68,5}$	(11111111110000111111101100010011001)	142
$\mathcal{C}_{68,6}$	(10010000011111111110100100000011110)	143
$\mathcal{C}_{68,7}$	(11001000100001110011001111111110001)	144
$\mathcal{C}_{68,8}$	(00001100011101100110111011010000110)	145
$\mathcal{C}_{68,9}$	(10000101000010101101011101111110101)	146
$\mathcal{C}_{68,10}$	(11001101000000100100001100100111110)	147
$\mathcal{C}_{68,11}$	(11101010000111101001011111111101011)	148
$\mathcal{C}_{68,12}$	(01100110010011010001110101011000)	149
$\mathcal{C}_{68,13}$	(11111111001011010000000001011111000)	150
$\mathcal{C}_{68,14}$	(00001000011000101110100111111111000)	151
$\mathcal{C}_{68,15}$	(11100000101000000011101101100000101)	152
$\mathcal{C}_{68,16}$	(10101001001100111111010011010010001)	153
$\mathcal{C}_{68,17}$	(11110100100001001000001010000111101)	155
$\mathcal{C}_{68,18}$	(10000010111101111001011000000001000)	159
$\mathcal{C}_{68,19}$	(00010100010101010100100100011000010)	160
$\mathcal{C}_{68,20}$	(11000001000111101011111100010101010)	161
$\mathcal{C}_{68,21}$	(01011100111100101100001111111010011)	163
$\mathcal{C}_{68,22}$	(10000001111110000000010111100010001)	164
$\mathcal{C}_{68,23}$	(01000000010100000010011101100101110)	165
$\mathcal{C}_{68,24}$	(01110010100101000000100100101010000)	166
$\mathcal{C}_{68,25}$	(11110100110001110001011010010111100)	167
$\mathcal{C}_{68,26}$	(00101100101101000000100011110000000)	168
$\mathcal{C}_{68,27}$	(00000100110101100010100100000101001)	169
$\mathcal{C}_{68,28}$	(11101010001100000111110101010101)	170
$\mathcal{C}_{68,29}$	(11101000011001111001000000100100 10)	171

$\mathcal{C}_{68,30}$	(10000011011011100100011010101111101)	172
$\mathcal{C}_{68,31}$	(11001000011100111010010100011000000)	173
$\mathcal{C}_{68,32}$	(01000110010000110001000101001011100)	174
$\mathcal{C}_{68,33}$	(01100000011101100001111010001011)	177
$\mathcal{C}_{68,34}$	(10111110001000000010110100001010)	184

Table 8: *New extremal binary self-dual codes of length* 68 *with* $\gamma = 6$ *as neighbors of* $\mathcal{C}_{68}$

6. Conclusion

In this paper, we propose a variation of the well known four-circulant construction for constructing self-dual codes. We compare both methods to highlight the significance of the generalized construction. Additionally, we construct new codes of length 68. For codes of length 68, we constructed the following codes with new weight enumerators in $W_{68,2}$:

$$\begin{aligned}
&\gamma = 5, \quad \beta = \{101, 105, 109, 111, 112, 114, 115\}.\\
&\gamma = 6, \quad \beta = \{133, 137, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151,\\
&\qquad\quad 152, 153, 155, 157, 159, 160, 161, 163, 164, 165, 166, 167, 168, 169, 170,\\
&\qquad\quad 171, 172, 173, 174, 177, 184\}.
\end{aligned}$$

The binary generator matrices of the new codes we have constructed are available online at [9].

The results we have obtained have demonstrated the effectiveness of the new construction and the difference from the ordinary four-circulant construction. A possible direction for future research could be to apply these constructions for different rings and lengths.

References

[1] D. Anev, M. Harada, N. Yankov, *New extremal singly even self-dual codes of lengths 64 and 66*, J. Algebra Comb. Discrete Appl. **5**(2017), 143–151.

[2] K. Betsumiya, S. Georgiou, T. A. Gulliver, M. Harada, C. Koukouvinos, *On self-dual codes over some prime fields*, Discrete Math. **262**(2003), 37–58.

[3] S. Buyuklieva, I. Boukliev, *Extremal self-dual codes with an automorphism of order 2*, IEEE Trans. Inform. Theory **44**(1998), 323–328.

[4] J. H. Conway N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory **36**(1990), 1319–1333.

[5] S. T. Dougherty, T. A. Gulliver, M. Harada, *Extremal binary self dual codes*, IEEE Trans. Inform. Theory **43**(1997), 2036–2047.

[6] S. T. Dougherty, P. Gaborit, M. Harada, P. Sole, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45**(1999), 32–45.

[7] S. T. Dougherty, J. -L. Kim, H. Kulosman, H. Liu, *Self-dual codes over commutative Frobenius rings*, Finite Fields Appl. **16**(2010), 14–26.

[8] P. Gaborit, V. Pless, P. Sole, P. Atkin, *Type II codes over* $\mathbb{F}_4$, Finite Fields Appl. **8**(2002), 171–183.

[9] J. Gildea, A. Kaya, B. Yildiz, *Binary generator matrices for extremal binary self-dual codes of length* 68, available at:
`http://abidinkaya.wixsite.com/math/research6`.

[10] M. Harada, A. Munemasa, *Some restrictions on weight enumerators of singly even self-dual codes*, IEEE Trans. Inform. Theory **52**(2006), 1266–1269.

[11] S. Karadeniz, B. Yildiz, *New extremal binary self-dual codes of length* 64 *from* R_3*-lifts of the extended binary Hamming code*, Des. Codes Cryptogr. **74**(2015), 673–680.

[12] S. Karadeniz, B. Yildiz, N. Aydin, *Extremal binary self-dual codes of lengths* 64 *and* 66 *from four-circulant constructions over codes* $\mathbb{F}_2 + u\mathbb{F}_2$, FILOMAT **28**(2014), 937–945.

[13] A. Kaya, *New extremal binary self-dual codes of length 68 via short Kharaghani array over* $\mathbb{F}_2 + u\mathbb{F}_2$, Math. Commun. **22**(2017), 123–133.

[14] A. Kaya, *New extremal binary self-dual codes of lengths 64 and 66 from* R_2*-lifts*, Finite Fields Appl. **46**(2017), 271–279.

[15] A. Kaya, B. Yildiz, *Various constructions for self-dual codes over rings and new binary self-dual codes*, Discrete Math. **339**(2016), 460–469.

[16] A. Kaya, B. Yildiz, A. Pasa, *New extremal binary self-dual codes from a modified four circulant construction*, Discrete Math. **339**(2016), 1086–1094.

[17] A. Kaya, B. Yildiz, *Constructing formally self-dual codes from block* λ*-circulant matrices*, Math. Commun. **24**(2019), 91–105.

[18] S. Ling, P. Sole, *Type II codes over* $\mathbb{F}_4 + u\mathbb{F}_4$, Europ. J. Combinatorics **22**(2001), 983–997.

[19] E. M. Rains, *Shadow Bounds for Self Dual Codes*, IEEE Trans. Inform. Theory **44**(1998), 134–139.