

# Composite Constructions of Self-Dual Codes from Group Rings and New Extremal Self-Dual Binary Codes of Length 68.

Steven T. Dougherty  
Department of Mathematics  
University of Scranton  
Scranton, PA 18510  
USA

Joe Gildea, Adrian Korban  
University of Chester  
Chester, UK  
Abidin Kaya

Department of Mathematics Education  
Sampoerna University  
12780, Jakarta, Indonesia

September 16, 2019

## Abstract

We describe eight composite constructions from group rings where the orders of the groups are 4 and 8, which are then applied to find self-dual codes of length 16 over  $\mathbb{F}_4$ . These codes have binary images with parameters  $[32, 16, 8]$  or  $[32, 16, 6]$ . These are lifted to codes over  $\mathbb{F}_4 + u\mathbb{F}_4$ , to obtain codes with Gray images extremal self-dual binary codes of length 64. Finally, we use a building-up method over  $\mathbb{F}_2 + u\mathbb{F}_2$  to obtain new extremal binary self-dual codes of length 68. We construct 11 new codes via the building-up method and 2 new codes by considering possible neighbors.

**Key Words:** Group rings; self-dual codes; codes over rings.

# 1 Introduction

A very well known technique for producing extremal binary self-dual codes over rings has been to consider generator matrices of the form  $(I_n|A)$  where  $A$  is a circulant or reverse circulant matrix satisfying  $AA^T = -I_n$ . In fact, this is probably the most common technique for producing self-dual codes. A major feature with this technique is that it produces codes whose automorphism group must contain certain groups as subgroups, see [6] for details. This technique was extended, so that the matrix  $A$  was replaced with  $\sigma(v)$ , i.e.,

$$(I_n \mid \sigma(v)) \tag{1}$$

where  $\sigma(v)$  is the image of a unitary unit in a group ring under a map that sends group ring elements to matrices. Examples of this approach where different groups of different sizes are used can be found in [11] and [9]. The main motivation for this approach is to obtain codes whose structure is not attainable from the classical techniques. Specifically, this means that we wish to find codes, whose automorphism groups are distinct from the automorphism groups that are usually obtained via this construction. We do this to find new codes which have been missed by a more classical approach.

We want to continue in this vein, by giving new constructions which will produce codes with significantly different structures. With this in mind, we modify Matrix 1, by considering group rings where the orders of the groups are 4 and 8. By applying the map  $\sigma(v)$  to different groups of orders 4 and 8 we get different block-matrix constructions which we combine together to form new matrices which we then use to find extremal binary self-dual codes. In fact, all the constructions from group rings, where the orders of the groups are 4 and 8 are  $2 \times 2$  block matrices as we will see later. We now define the composite constructions.

- (1) Take a  $2 \times 2$  block constructed from a group ring of order 8,

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$$

where  $A_1, A_2, A_3, A_4$  are special matrices (depending on the group these will differ).

- (2) Use the first row of each of the matrices  $A_1, A_2, A_3, A_4$  and apply to each, a construction from a group ring of order 4 to get a  $4 \times 4$  block matrix,

$$\begin{pmatrix} B_1 & B_2 & B_5 & B_6 \\ B_3 & B_4 & B_7 & B_8 \\ B_9 & B_{10} & B_{13} & B_{14} \\ B_{11} & B_{12} & B_{15} & B_{16} \end{pmatrix}.$$

We construct 12,  $4 \times 4$  block matrices, but some of them turn out to be equivalent constructions, i.e., one can be obtained from the other. Therefore, we only construct and

focus on 8 constructions which we use later to find extremal binary self-dual codes. We use these constructions over  $\mathbb{F}_4$  to find extremal binary images of codes with parameters  $[32, 16, 8]$  or  $[32, 16, 6]$  which we then lift over  $\mathbb{F}_4 + u\mathbb{F}_4$ , to obtain the extremal binary images of self-dual codes of length 64. We also apply the extension method to find new extremal binary self-dual codes of length 68.

The rest of the work is organized as follows. In Section 2, we give preliminary definitions and results on group rings, self-dual codes and the alphabets which we use. In the same section, we also give the  $2 \times 2$  block matrices obtained from group rings where the orders of the groups are 4 and 8. In Section 3, we give new constructions which are in fact  $4 \times 4$  block matrices. We use them to define generator matrices for which we give necessary conditions in order to be able to apply them to find extremal binary self-dual codes. We also show which constructions are equivalent and how they are equivalent. In Section 4, we tabulate all the results from applying the generator matrices from the previous section to  $\mathbb{F}_4$  and  $\mathbb{F}_4 + u\mathbb{F}_4$ . In Section 5, we find new extremal binary codes of length 68 by applying the extension methods to the codes found in Section 4.

## 2 Preliminaries

### 2.1 Self-Dual Codes, the Field $\mathbb{F}_4$ and the Ring $\mathbb{F}_4 + u\mathbb{F}_4$

We begin by recalling the standard definitions from coding theory. In this paper, all rings are assumed to be commutative, finite, Frobenius rings with a multiplicative identity. Denote the character module of  $R$  by  $\widehat{R}$ . A code  $C$  of length  $n$  over a Frobenius ring  $R$  is a subset of  $R^n$ . For a finite ring  $R$  the following are equivalent:

- (1)  $R$  is a Frobenius ring;
- (2) As a left module,  $\widehat{R} \cong {}_R R$ ;
- (3) As a right module  $\widehat{R} \cong R_R$ .

We consider codes over Frobenius rings since such rings have good duality properties which are reflected by the equivalent statements above. If the code is a submodule of  $R^n$  then we say that the code is linear. For a full description of Frobenius rings and codes over Frobenius rings, see [3]. Elements of the code  $C$  are called codewords of  $C$ . Let  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  and  $\mathbf{y} = (y_1, y_2, \dots, y_n)$  be two elements of  $R^n$ . The duality is understood in terms of the Euclidean inner product, namely:

$$\langle \mathbf{x}, \mathbf{y} \rangle_E = \sum x_i y_i.$$

The dual  $C^\perp$  of the code  $C$  is defined as

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

We say that  $C$  is self-orthogonal if  $C \subseteq C^\perp$  and is self-dual if  $C = C^\perp$ .

We now describe the alphabets we use in this paper. We take the standard representation of the field with 4 elements, namely we let  $\mathbb{F}_4 = \mathbb{F}_2(\omega)$  be the quadratic field extension of  $\mathbb{F}_2$ , where  $\omega^2 + \omega + 1 = 0$ . The ring  $\mathbb{F}_4 + u\mathbb{F}_4 = \mathbb{F}_4[u]/\langle u^2 \rangle$  is a commutative ring of size 16 with characteristic 2. 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  $\langle u \rangle = \{0, u, u\omega, u + u\omega\}$ . This gives that the ring is a commutative chain ring and as such is a Frobenius ring. Moreover, it is a self-dual code of length 1, that is  $\langle u \rangle^\perp = \langle u \rangle$ . It is immediate from this fact that there are self-dual codes of every length over this ring by taking direct products of the self-dual code of length 1.

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  $\bar{\omega} = \omega^2$ , since  $\omega \in \mathbb{F}_4$  and  $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$ . Let us recall the following Gray Maps from [12] and [4]:

$$\begin{array}{l|l} \psi_{\mathbb{F}_4} : (\mathbb{F}_4)^n \rightarrow (\mathbb{F}_2)^{2n} & \varphi_{\mathbb{F}_2+u\mathbb{F}_2} : (\mathbb{F}_2 + u\mathbb{F}_2)^n \rightarrow \mathbb{F}_2^{2n} \\ a\omega + b\bar{\omega} \mapsto (a, b), \ a, b \in \mathbb{F}_2^n & a + bu \mapsto (b, a + b), \ a, b \in \mathbb{F}_2^n. \end{array}$$

In [15], these maps were generalized to the following Gray maps:

$$\begin{array}{l|l} \psi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow (\mathbb{F}_2 + u\mathbb{F}_2)^{2n} & \varphi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow \mathbb{F}_4^{2n} \\ a\omega + b\bar{\omega} \mapsto (a, b), \ a, b \in (\mathbb{F}_2 + u\mathbb{F}_2)^n & a + bu \mapsto (b, a + b), \ a, b \in \mathbb{F}_4^n. \end{array}$$

Note that these Gray maps preserve orthogonality in their respective alphabets, for details we refer to [15]. Let  $C \subseteq (\mathbb{F}_4 + u\mathbb{F}_4)^n$ , then the binary codes  $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  and  $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  are equivalent to each other, please see [12] and [15] for more details. 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 maps. A self-dual code in  $R^n$  where  $R$  is equipped with a Gray map to the binary Hamming space 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. Of course, it is then trivial to note that the image of a Type II code is a binary Type II code and the image of a Type I code is a binary Type I code in the traditional definition. We explain this completely in the following proposition from [15].

**Proposition 2.1.** (*[15]*) *Let  $C$  be a code over  $\mathbb{F}_4 + u\mathbb{F}_4$ . If  $C$  is self-orthogonal, then so are  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  and  $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ . The code  $C$  is a Type I (resp. Type II) code over  $\mathbb{F}_4 + u\mathbb{F}_4$  if and only if  $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  is a Type I (resp. Type II)  $\mathbb{F}_4$ -code, if and only if  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  is a Type I (resp. Type II)  $\mathbb{F}_2 + u\mathbb{F}_2$ -code. Furthermore, the minimum Lee weight of  $C$  is the same as the minimum Lee weight of  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  and  $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ .*

The next corollary follows immediately from the proposition and we will use this result repeatedly to produce binary codes.

**Corollary 2.2.** *Suppose that  $C$  is a self-dual code over  $\mathbb{F}_4+u\mathbb{F}_4$  of length  $n$  and minimum Lee distance  $d$ . Then  $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  is a binary  $[4n, 2n, d]$  self-dual code. Moreover, the Lee weight enumerator of  $C$  is equal to the Hamming weight enumerator of  $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ . If  $C$  is Type I (Type II), then so is  $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ .*

An upper bound on the minimum Hamming distance of a binary self-dual code was given in [16]. Specifically, let  $d_I(n)$  and  $d_{II}(n)$  be the minimum distance of a Type I and Type II binary code of length  $n$ , respectively. Then

$$d_{II}(n) \leq 4\lfloor \frac{n}{24} \rfloor + 4$$

and

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

Self-dual codes meeting these bounds are called *extremal*. Throughout the text we obtain extremal binary codes of different lengths. Self-dual codes which are the best possible for a given set of parameters are said to be optimal. Extremal codes are necessarily optimal but optimal codes are not necessarily extremal.

## 2.2 Group Rings

We need to define a circulant matrix, a reverse circulant matrix and a block circulant matrix before we introduce group rings.

**Definition 1.** *A circulant matrix over a ring  $R$  is a square  $n \times n$  matrix, which takes the form*

$$\text{circ}(a_1, a_2, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}$$

where  $a_i \in R$ .

**Definition 2.** *A reverse circulant matrix over a ring  $R$  is a square  $n \times n$  matrix, which takes the form*

$$\text{rcirc}(a_1, a_2, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_3 & a_4 & \dots & a_1 \\ a_3 & a_4 & a_5 & \dots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_1 & a_2 & \dots & a_{n-1} \end{pmatrix}$$

where  $a_i \in R$ .

**Definition 3.** A block circulant matrix over a ring  $R$  is a square  $kn \times kn$  matrix, which takes the form

$$\text{CIRC}(A_1, A_2, \dots, A_n) = \begin{pmatrix} A_1 & A_2 & A_3 & \dots & A_n \\ A_n & A_1 & A_2 & \dots & A_{n-1} \\ A_{n-1} & A_n & A_1 & \dots & A_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & A_4 & \dots & A_1 \end{pmatrix}$$

where each  $A_i$  is a  $k \times k$  matrix over  $R$ .

We shall use group rings in our constructions, therefore we shall give the standard definition of a group ring. While group rings can be given for infinite rings and infinite groups, we are only concerned with group rings where both the ring and the group are finite. Let  $G$  be a finite group of order  $n$ , then the group ring  $RG$  consists of  $\sum_{i=1}^n \alpha_i g_i$ ,  $\alpha_i \in R$ ,  $g_i \in G$ .

Addition in the group ring is done by coordinate addition, namely

$$\sum_{i=1}^n \alpha_i g_i + \sum_{i=1}^n \beta_i g_i = \sum_{i=1}^n (\alpha_i + \beta_i) g_i. \quad (2)$$

The product of two elements in a group ring is given by

$$\left( \sum_{i=1}^n \alpha_i g_i \right) \left( \sum_{j=1}^n \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \quad (3)$$

It follows that the coefficient of  $g_k$  in the product is  $\sum_{g_i g_j = g_k} \alpha_i \beta_j$ .

The following construction of a matrix was first given for codes over fields by Hurley in [13]. It was extended to Frobenius rings in [6]. Let  $R$  be a finite commutative Frobenius ring and let  $G = \{g_1, g_2, \dots, g_n\}$  be a group of order  $n$ . Let  $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \dots + \alpha_{g_n} g_n \in RG$ . Define the matrix  $\sigma(v) \in M_n(R)$  to be

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1} g_1} & \alpha_{g_1^{-1} g_2} & \alpha_{g_1^{-1} g_3} & \dots & \alpha_{g_1^{-1} g_n} \\ \alpha_{g_2^{-1} g_1} & \alpha_{g_2^{-1} g_2} & \alpha_{g_2^{-1} g_3} & \dots & \alpha_{g_2^{-1} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1} g_1} & \alpha_{g_n^{-1} g_2} & \alpha_{g_n^{-1} g_3} & \dots & \alpha_{g_n^{-1} g_n} \end{pmatrix}. \quad (4)$$

We note that the elements  $g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}$  are the elements of the group  $G$  in a some given order. We will now describe  $\sigma(v)$  for the following group rings  $RG$  where  $G \in \{C_2 \times C_2, C_4, C_8, C_4 \times C_2, D_8, Q_8\}$ .

- Let  $G = \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle \cong C_2 \times C_2$ . If  $v = \sum_{i=0}^1 \sum_{j=0}^1 \alpha_{i+2j+1} x^i y^j \in R(C_2 \times C_2)$ , then

$$\sigma(v) = CIRC(A, B)$$

where  $A = circ(\alpha_1, \alpha_2)$ ,  $B = circ(\alpha_3, \alpha_4)$  and  $\alpha_i \in R$ .

- Let  $G = \langle x \mid x^4 = 1 \rangle \cong C_4$ . If  $v = \sum_{i=0}^1 \sum_{j=0}^1 \alpha_{i+2j+1} x^{2i+j} \in RC_4$ , then

$$\sigma(v) = \begin{pmatrix} A & B \\ B' & A \end{pmatrix}$$

where  $A = circ(\alpha_1, \alpha_2)$ ,  $B = circ(\alpha_3, \alpha_4)$ ,  $B' = circ(\alpha_4, \alpha_3)$  and  $\alpha_i \in R$ .

- Let  $G = \langle x \mid x^8 = 1 \rangle \cong C_8$ . If  $v = \sum_{i=0}^3 \sum_{j=0}^1 \alpha_{i+4j+1} x^{2i+j} \in RC_8$ , then

$$\sigma(v) = \begin{pmatrix} A & B \\ B' & A \end{pmatrix}$$

where  $A = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$ ,  $B' = circ(\alpha_8, \alpha_5, \alpha_6, \alpha_7)$  and  $\alpha_i \in R$ .

- Let  $G = \langle x, y \mid x^4 = y^2 = 1, xy = yx \rangle \cong C_4 \times C_2$ . If  $v = \sum_{i=0}^3 \sum_{j=0}^1 \alpha_{i+4j+1} x^i y^j \in R(C_4 \times C_2)$ , then

$$\sigma(v) = CIRC(A, B)$$

where  $A = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$  and  $\alpha_i \in R$ .

- Let  $G = \langle x, y \mid x^4 = y^2 = (yx)^2 = 1 \rangle \cong D_8$ .

- (1) If  $v = \sum_{i=0}^3 \sum_{j=0}^1 \alpha_{i+4j+1} y^j x^i \in RD_8$ , then

$$\sigma(v) = CIRC(A, B)$$

where  $A = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = rcirc(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$  and  $\alpha_i \in R$ .

- (2) If  $v = \sum_{i=0}^3 \sum_{j=0}^1 \alpha_{i+4j+1} x^i y^j \in RD_8$ , then

$$\sigma(v) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$$

where  $A = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$  and  $\alpha_i \in R$ .

- Let  $G = \langle x, y \mid x^4 = 1, x^2 = y^2, yx = xy^{-1} \rangle \cong Q_8$ .

(1) If  $v = \sum_{i=0}^3 \sum_{j=0}^1 \alpha_{i+4j+1} y^j x^i \in RQ_8$ , then

$$\sigma(v) = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$$

where  $A = \text{circ}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = \text{rcirc}(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$ ,  $C = \text{rcirc}(\alpha_7, \alpha_8, \alpha_5, \alpha_6)$  and  $\alpha_i \in R$ .

(2) If  $v = \sum_{i=0}^3 \sum_{j=0}^1 \alpha_{i+4j+1} x^i y^j \in RQ_8$ , then

$$\sigma(v) = \begin{pmatrix} A & B \\ C & A^T \end{pmatrix}$$

where  $A = \text{circ}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = \text{circ}(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$ ,  $C = \text{circ}(\alpha_7, \alpha_6, \alpha_5, \alpha_8)$  and  $\alpha_i \in R$ .

### 3 New constructions from Group Rings where the orders of the groups are 4 and 8

In [14], the authors have applied the four circulant construction, i.e.,

$$G = \left[ I_{2n} \mid \begin{array}{cc} A & B \\ B^T & A^T \end{array} \right],$$

over  $\mathbb{F}_4$  to search for codes whose binary images have parameters [32, 16, 8 or 6]. They then lift the  $\mathbb{F}_4$  codes to  $\mathbb{F}_4 + u\mathbb{F}_4$  to obtain extremal binary self-dual codes of length 64, which then are extended to find new extremal self-dual codes of length 68. We amend the four circulant construction by considering the composite matrices derived from group rings. The motivation for the composite constructions comes from the fact that the four circular construction can be derived from group rings:

$$G = (I_{2n} \mid \sigma(v)) = \left[ I_{2n} \mid \begin{array}{cc} A & B \\ B^T & A^T \end{array} \right],$$

where  $v \in RD_{2n}$ . Please see [11] for details. What we also achieve by amending the four circulant construction in this way, is that we find more new extremal self-dual binary codes of length 68 that were not obtained by the authors in [14]. We tabulate the results in



Sections 4 and 5. We also present other composite constructions which we apply to search for extremal self-dual binary codes later in the work. We only consider certain matrices which we derived from group rings in Section 2. We restrict our attention to some groups of orders 4 and 8, but the composite constructions can be extended so that groups of higher orders are employed.

We now define the composite constructions which are  $4 \times 4$  block matrices with blocks being special type of matrices. The obtained block matrices can be applied to search for new extremal self-dual binary codes. The technique for finding new block matrices is as follows.

- (1) Take each  $2 \times 2$  block matrix from group rings where the group has order 8, which we found in the previous section, (six  $2 \times 2$  block matrices were found).
- (2) In each  $2 \times 2$  block matrix from group rings where the group has order 8, we replace the submatrices with the  $2 \times 2$  block matrices from group rings, where the group has order 4 (two such matrices were found).

Following the above two steps we should end up with twelve new  $4 \times 4$  block matrices of order 8 but some of the constructions are equivalent. Therefore we end up with eight  $4 \times 4$  block matrices. We shall show which ones are equivalent. We show, with necessary and different conditions that each one of the new eight block matrices can be applied to search for the extremal binary self-dual codes. We give a complete characterization of these matrices in order to aid the construction of the codes later in the work. Also, the composite matrices can not be obtained directly from an element in  $RG$ , therefore we give a detailed proof of each construction stating all the necessary conditions that each generator matrix has to meet in order to generate a self-dual code. The proofs are the same but the conditions for the matrices are different. Our construction gives codes with potentially different automorphism groups than those constructed by similar methods, thus enabling our search for new codes. We split the new constructions into subsections.

### 3.1 The group $C_8$ replaced with groups $C_2 \times C_2$ and $C_4$

First, we construct a  $4 \times 4$  block matrix by combining the two block matrices obtained from the group rings  $RC_8$  and  $R(C_2 \times C_2)$  in Section 2:

$$\begin{pmatrix} A & B \\ B' & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{pmatrix}, \quad (5)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $A_3 = \text{circ}(\alpha_8, \alpha_5)$  and  $B_3 = \text{circ}(\alpha_6, \alpha_7)$ . Now, we give the following results using the  $4 \times 4$  block matrix in (5).

**Theorem 3.1.** *The matrix*

$$G = \left[ \begin{array}{c|cc} & A_1 & B_1 & A_2 & B_2 \\ I_8 & B_1 & A_1 & B_2 & A_2 \\ & A_3 & B_3 & A_1 & B_1 \\ & B_3 & A_3 & B_1 & A_1 \end{array} \right], \quad (6)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $A_3 = \text{circ}(\alpha_8, \alpha_5)$  and  $B_3 = \text{circ}(\alpha_6, \alpha_7)$ , is the generator matrix of a self-dual code over  $R$ , if and only if the following equations hold in  $R$ :

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (7)$$

$$2A_1B_1 + 2A_2B_2 = 0, \quad (8)$$

$$A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0, \quad (9)$$

$$A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 = 0, \quad (10)$$

$$A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2, \quad (11)$$

$$2A_1B_1 + 2A_3B_3 = 0. \quad (12)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \left[ \begin{array}{cc|cc} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{array} \right],$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{bmatrix} \begin{bmatrix} A_1 & B_1 & A_3 & B_3 \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_3 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & 2A_1B_1 + 2A_2B_2 \\ 2A_1B_1 + 2A_2B_2 & A_1^2 + A_2^2 + B_1^2 + B_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 & A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 \\ A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 & A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_1^2 + A_3^2 + B_1^2 + B_3^2 & 2A_1B_1 + 2A_3B_3 \\ 2A_1B_1 + 2A_3B_3 & A_1^2 + A_3^2 + B_1^2 + B_3^2 \end{bmatrix}.$$

This will equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $2A_1B_1 + 2A_2B_2 = 0$ ,  $A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0$ ,  $A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 = 0$ ,  $A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2$  and  $2A_1B_1 + 2A_3B_3 = 0$ .

□

Now, we construct a  $4 \times 4$  block matrix by combining the two block matrices obtained from the group rings  $RC_8$  and  $RC_4$  in Section 2:

$$\begin{pmatrix} A & B \\ B' & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B'_3 & A_3 & B'_1 & A_1 \end{pmatrix}, \quad (13)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ ,  $A_3 = \text{circ}(\alpha_8, \alpha_5)$ ,  $B_3 = \text{circ}(\alpha_6, \alpha_7)$  and  $B'_3 = \text{circ}(\alpha_7, \alpha_6)$ . Now we give the following results using the  $4 \times 4$  block matrix in (13).

**Theorem 3.2.** *The matrix*

$$G = \left[ \begin{array}{c|cc} I_8 & A_1 & B_1 & A_2 & B_2 \\ & B'_1 & A_1 & B'_2 & A_2 \\ & A_3 & B_3 & A_1 & B_1 \\ & B'_3 & A_3 & B'_1 & A_1 \end{array} \right], \quad (14)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ ,  $A_3 = \text{circ}(\alpha_8, \alpha_5)$ ,  $B_3 = \text{circ}(\alpha_6, \alpha_7)$  and  $B'_3 = \text{circ}(\alpha_7, \alpha_6)$ , is the generator matrix of a self-dual code over  $R$ , if and only if the following equations hold:

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (15)$$

$$A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 = 0, \quad (16)$$

$$B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2, \quad (17)$$

$$A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0, \quad (18)$$

$$A_2B'_1 + A_3B_1 + A_1B'_3 + A_1B_2 = 0, \quad (19)$$

$$A_3B'_1 + A_2B_1 + A_1B'_2 + A_1B_3 = 0, \quad (20)$$

$$B'_1B'_2 + B'_1B'_3 + A_1A_2 + A_1A_3 = 0, \quad (21)$$

$$A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2, \quad (22)$$

$$A_1B'_1 + A_1B_1 + A_3B'_3 + A_3B_3 = 0, \quad (23)$$

$$B_1'^2 + B_3'^2 + A_1^2 + A_3^2 = -I_2. \quad (24)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B'_3 & A_3 & B'_1 & A_1 \end{bmatrix},$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B'_3 & A_3 & B'_1 & A_1 \end{bmatrix} \begin{bmatrix} A_1 & B'_1 & A_3 & B'_3 \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B'_2 & A_1 & B'_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix},$$

where

$$\begin{aligned} X_1 &= \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 \\ A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 & B_1'^2 + B_2'^2 + A_1^2 + A_2^2 \end{bmatrix}, \\ X_2 &= \begin{bmatrix} A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 & A_2B'_1 + A_3B_1 + A_1B'_3 + A_1B_2 \\ A_3B'_1 + A_2B_1 + A_1B'_2 + A_1B_3 & B'_1B'_2 + B'_1B'_3 + A_1A_2 + A_1A_3 \end{bmatrix}, \\ X_3 &= \begin{bmatrix} A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 & A_3B'_1 + A_2B_1 + A_1B'_2 + A_1B_3 \\ A_2B'_1 + A_3B_1 + A_1B'_3 + A_1B_2 & B'_1B'_2 + B'_1B'_3 + A_1A_2 + A_1A_3 \end{bmatrix}, \\ X_4 &= \begin{bmatrix} A_1^2 + A_3^2 + B_1^2 + B_3^2 & A_1B'_1 + A_1B_1 + A_3B'_3 + A_3B_3 \\ A_1B'_1 + A_1B_1 + A_3B'_3 + A_3B_3 & B_1'^2 + B_3'^2 + A_1^2 + A_3^2 \end{bmatrix}. \end{aligned}$$

This will be equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 = 0$ ,  $B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2$ ,  $A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0$ ,  $A_2B'_1 + A_3B_1 + A_1B'_3 + A_1B_2 = 0$ ,  $A_3B'_1 + A_2B_1 + A_1B'_2 + A_1B_3 = 0$ ,  $B'_1B'_2 + B'_1B'_3 + A_1A_2 + A_1A_3 = 0$ ,  $A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2$ ,  $A_1B'_1 + A_1B_1 + A_3B'_3 + A_3B_3 = 0$  and  $B_1'^2 + B_3'^2 + A_1^2 + A_3^2 = -I_2$ .  $\square$

### 3.2 The group $C_4 \times C_2$ replaced with groups $C_2 \times C_2$ and $C_4$

First we construct a  $4 \times 4$  block matrix by combining the two block matrices obtained from the group rings  $R(C_4 \times C_2)$  and  $R(C_2 \times C_2)$  in Section 2:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{pmatrix}, \quad (25)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$  and  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ . Now we give the following results using the  $4 \times 4$  block matrix in (25).

**Theorem 3.3.** *The matrix*

$$G = \left[ \begin{array}{c|cc} I_8 & A_1 & B_1 & A_2 & B_2 \\ \hline & B_1 & A_1 & B_2 & A_2 \\ & A_2 & B_2 & A_1 & B_1 \\ & B_2 & A_2 & B_1 & A_1 \end{array} \right], \quad (26)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$  and  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ , is the generator matrix of a self-dual code over  $R$ , if and only if the following equations hold in  $R$ :

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (27)$$

$$2A_1B_1 + 2A_2B_2 = 0, \quad (28)$$

$$2A_1A_2 + 2B_1B_2 = 0, \quad (29)$$

$$2A_1B_2 + 2A_2B_1 = 0. \quad (30)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix},$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix} \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_1 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & 2A_1B_1 + 2A_2B_2 \\ 2A_1B_1 + 2A_2B_2 & A_1^2 + A_2^2 + B_1^2 + B_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} 2A_1A_2 + 2B_1B_2 & 2A_1B_2 + 2A_2B_1 \\ 2A_1B_2 + 2A_2B_1 & 2A_1A_2 + 2B_1B_2 \end{bmatrix}.$$

This will equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $2A_1B_1 + 2A_2B_2 = 0$ ,  $2A_1A_2 + 2B_1B_2 = 0$  and  $2A_1B_2 + 2A_2B_1 = 0$ .  $\square$

Secondly, we construct a  $4 \times 4$  block matrix by combining the two block matrices obtained from the group rings  $R(C_4 \times C_2)$  and  $RC_4$  in Section 2:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_2 & B_2 & A_1 & B_1 \\ B'_2 & A_2 & B'_1 & A_1 \end{pmatrix}, \quad (31)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$  and  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ . Now we give the following results using the  $4 \times 4$  block matrix in (32).

**Theorem 3.4.** *The matrix*

$$G = \left[ \begin{array}{c|cc} I_8 & A_1 & B_1 \\ & B'_1 & A_1 \\ & A_2 & B_2 \\ & B'_2 & A_2 \end{array} \right], \quad (32)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$  and  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ , generates a self-dual code over  $R$ , if and only if the following equations hold:

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (33)$$

$$A_1 B'_1 + A_1 B_1 + A_2 B'_2 + A_2 B_2 = 0, \quad (34)$$

$$B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2, \quad (35)$$

$$2A_1 A_2 + 2B_1 B_2 = 0, \quad (36)$$

$$A_2 B'_1 + A_2 B_1 + A_1 B'_2 + A_1 B_2 = 0, \quad (37)$$

$$2B_1' B_2' + 2A_1 A_2 = 0. \quad (38)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \left[ \begin{array}{cc|cc} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ \hline A_2 & B_2 & A_1 & B_1 \\ B'_2 & A_2 & B'_1 & A_1 \end{array} \right],$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \left[ \begin{array}{cc|cc} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ \hline A_2 & B_2 & A_1 & B_1 \\ B'_2 & A_2 & B'_1 & A_1 \end{array} \right] \left[ \begin{array}{cc|cc} A_1 & B'_1 & A_2 & B'_2 \\ B_1 & A_1 & B_2 & A_2 \\ \hline A_2 & B'_2 & A_1 & B'_1 \\ B_2 & A_2 & B_1 & A_1 \end{array} \right] = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_1 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & A_1 B'_1 + A_1 B_1 + A_2 B'_2 + A_2 B_2 \\ A_1 B'_1 + A_1 B_1 + A_2 B'_2 + A_2 B_2 & B_1'^2 + B_2'^2 + A_1^2 + A_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} 2A_1 A_2 + 2B_1 B_2 & A_2 B'_1 + A_2 B_1 + A_1 B'_2 + A_1 B_2 \\ A_2 B'_1 + A_2 B_1 + A_1 B'_2 + A_1 B_2 & 2B_1' B_2' + 2A_1 A_2 \end{bmatrix}.$$

This will equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $A_1 B'_1 + A_1 B_1 + A_2 B'_2 + A_2 B_2 = 0$ ,  $B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2$ ,  $2A_1 A_2 + 2B_1 B_2 = 0$ ,  $A_2 B'_1 + A_2 B_1 + A_1 B'_2 + A_1 B_2 = 0$  and  $2B_1' B_2' + 2A_1 A_2 = 0$ .  $\square$

### 3.3 The group $D_8$ replaced with groups $C_2 \times C_2$ and $C_4$

In this section we amend the four circulant construction (Case 2 below) that the authors applied in [14]. As a result we obtain new extremal self-dual codes of length 68- see Sections 4 and 5.

We have two cases here, as we have seen in Section 2. Two  $2 \times 2$  block matrices can be obtained from the dihedral group of order 8.

Case 1: Here we consider the block matrix:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}, \quad (39)$$

where  $A = \text{circ}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = \text{rcirc}(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$ .

Now, combining the matrix (39) with the two matrices obtained from group rings  $R(C_2 \times C_2)$  and  $RC_4$  we get the following two constructions:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{pmatrix}, \quad (40)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$  and  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ . And,

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_2 & B_2 & A_1 & B_1 \\ B'_2 & A_2 & B'_1 & A_1 \end{pmatrix}, \quad (41)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$  and  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ . But matrices (40) and (41) are the same as matrices (25) and (31), therefore case 1 has not produced new constructions. We move now to case 2:

Case 2: Here, we consider the matrix

$$\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}, \quad (42)$$

where  $A = \text{circ}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = \text{circ}(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$ .

First, we construct a  $4 \times 4$  block matrix by combining the matrix in (42) with a block matrix obtained from the group ring  $R(C_2 \times C_2)$  in Section 2:

$$\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3 & A_3 & B_4 & A_4 \end{pmatrix}, \quad (43)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $A_3 = \text{circ}(\alpha_5, \alpha_8)$ ,  $B_3 = \text{circ}(\alpha_7, \alpha_6)$ ,  $A_4 = \text{circ}(\alpha_1, \alpha_4)$  and  $B_4 = \text{circ}(\alpha_3, \alpha_2)$ . Now we give the following results using the  $4 \times 4$  block matrix in (43).

**Theorem 3.5.** *The matrix*

$$G = \left[ \begin{array}{c|cc} I_8 & A_1 & B_1 & A_2 & B_2 \\ \hline & B_1 & A_1 & B_2 & A_2 \\ & A_3 & B_3 & A_4 & B_4 \\ & B_3 & A_3 & B_4 & A_4 \end{array} \right], \quad (44)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $A_3 = \text{circ}(\alpha_5, \alpha_8)$ ,  $B_3 = \text{circ}(\alpha_7, \alpha_6)$ ,  $A_4 = \text{circ}(\alpha_1, \alpha_4)$  and  $B_4 = \text{circ}(\alpha_3, \alpha_2)$ , is the generator matrix of a self-dual code over  $R$ , if and only if the following equations hold:

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (45)$$

$$2A_1B_1 + 2A_2B_2 = 0, \quad (46)$$

$$A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 = 0, \quad (47)$$

$$A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 = 0, \quad (48)$$

$$A_3^2 + A_4^2 + B_3^2 + B_4^2 = -I_2, \quad (49)$$

$$2A_3B_3 + 2A_4B_4 = 0. \quad (50)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3 & A_3 & B_4 & A_4 \end{bmatrix},$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3 & A_3 & B_4 & A_4 \end{bmatrix} \begin{bmatrix} A_1 & B_1 & A_3 & B_3 \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B_2 & A_4 & B_4 \\ B_2 & A_2 & B_4 & A_4 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_3 \end{bmatrix},$$



where

$$\begin{aligned}
X_1 &= \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & 2A_1B_1 + 2A_2B_2 \\ 2A_1B_1 + 2A_2B_2 & A_1^2 + A_2^2 + B_1^2 + B_2^2 \end{bmatrix}, \\
X_2 &= \begin{bmatrix} A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 & A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 \\ A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 & A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 \end{bmatrix}, \\
X_3 &= \begin{bmatrix} A_3^2 + A_4^2 + B_3^2 + B_4^2 & 2A_3B_3 + 2A_4B_4 \\ 2A_3B_3 + 2A_4B_4 & A_3^2 + A_4^2 + B_3^2 + B_4^2 \end{bmatrix}.
\end{aligned}$$

This will equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $2A_1B_1 + 2A_2B_2 = 0$ ,  $A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 = 0$ ,  $A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 = 0$ ,  $A_3^2 + A_4^2 + B_3^2 + B_4^2 = -I_2$  and  $2A_3B_3 + 2A_4B_4 = 0$ .  $\square$

Now, we construct a  $4 \times 4$  block matrix by combining the matrix (43) with a block matrix obtained from the group ring  $RC_4$  in Section 2:

$$\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B'_3 & A_3 & B'_4 & A_4 \end{pmatrix}, \quad (51)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ ,  $A_3 = \text{circ}(\alpha_5, \alpha_8)$ ,  $B_3 = \text{circ}(\alpha_7, \alpha_6)$ ,  $B'_3 = \text{circ}(\alpha_6, \alpha_7)$ ,  $A_4 = \text{circ}(\alpha_1, \alpha_4)$ ,  $B_4 = \text{circ}(\alpha_3, \alpha_2)$ ,  $B'_4 = \text{circ}(\alpha_2, \alpha_3)$ . Now we give the following results using the  $4 \times 4$  block matrix in (51).

**Theorem 3.6.** *The matrix*

$$G = \left[ \begin{array}{c|cc} I_8 & A_1 & B_1 & A_2 & B_2 \\ \hline & B'_1 & A_1 & B'_2 & A_2 \\ & A_3 & B_3 & A_4 & B_4 \\ & B'_3 & A_3 & B'_4 & A_4 \end{array} \right], \quad (52)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ ,  $A_3 = \text{circ}(\alpha_5, \alpha_8)$ ,  $B_3 = \text{circ}(\alpha_7, \alpha_6)$ ,  $B'_3 = \text{circ}(\alpha_6, \alpha_7)$ ,  $A_4 = \text{circ}(\alpha_1, \alpha_4)$ ,  $B_4 = \text{circ}(\alpha_3, \alpha_2)$ ,  $B'_4 = \text{circ}(\alpha_2, \alpha_3)$ , generates a self-dual code over  $R$ , if and only if the following equations hold:

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (53)$$

$$A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 = 0, \quad (54)$$

$$B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2, \quad (55)$$

$$A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 = 0, \quad (56)$$

$$A_1B'_3 + A_2B'_4 + A_3B_1 + A_4B_2 = 0, \quad (57)$$

$$A_3B'_1 + A_4B'_2 + A_1B_3 + A_2B_4 = 0, \quad (58)$$

$$B'_1B'_3 + B'_2B'_4 + A_1A_3 + A_2A_4 = 0, \quad (59)$$

$$A_3^2 + A_4^2 + B_3^2 + B_4^2 = -I_2, \quad (60)$$

$$A_3B'_3 + A_3B_3 + A_4B'_4 + A_4B_4 = 0, \quad (61)$$

$$B_3'^2 + B_4'^2 + A_3^2 + A_4^2 = -I_2. \quad (62)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B'_3 & A_3 & B'_4 & A_4 \end{bmatrix},$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B'_3 & A_3 & B'_4 & A_4 \end{bmatrix} \begin{bmatrix} A_1 & B'_1 & A_3 & B'_3 \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B'_2 & A_4 & B'_4 \\ B_2 & A_2 & B_4 & A_4 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 \\ A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 & B_1'^2 + B_2'^2 + A_1^2 + A_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 & A_1B'_3 + A_2B'_4 + A_3B_1 + A_4B_2 \\ A_3B'_1 + A_4B'_2 + A_1B_3 + A_2B_4 & B'_1B'_3 + B'_2B'_4 + A_1A_3 + A_2A_4 \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 & A_3B'_1 + A_4B'_2 + A_1B_3 + A_2B_4 \\ A_1B'_3 + A_2B'_4 + A_3B_1 + A_4B_2 & B'_1B'_3 + B'_2B'_4 + A_1A_3 + A_2A_4 \end{bmatrix},$$

$$X_4 = \begin{bmatrix} A_3^2 + A_4^2 + B_3^2 + B_4^2 & A_3B'_3 + A_3B_3 + A_4B'_4 + A_4B_4 \\ A_3B'_3 + A_3B_3 + A_4B'_4 + A_4B_4 & B_3'^2 + B_4'^2 + A_3^2 + A_4^2 \end{bmatrix}.$$

This will equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 = 0$ ,  $B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2$ ,  $A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 = 0$ ,  $A_1B'_3 + A_2B'_4 + A_3B_1 + A_4B_2 = 0$ ,  $A_3B'_1 + A_4B'_2 + A_1B_3 + A_2B_4 = 0$ ,  $B'_1B'_3 + B'_2B'_4 + A_1A_3 + A_2A_4 = 0$ ,  $A_3^2 + A_4^2 + B_3^2 + B_4^2 = -I_2$ ,  $A_3B'_3 + A_3B_3 + A_4B'_4 + A_4B_4 = 0$  and  $B_3'^2 + B_4'^2 + A_3^2 + A_4^2 = -I_2$ .  $\square$

### 3.4 The group $Q_8$ replaced with groups $C_2 \times C_2$ and $C_4$

Here we also have two cases:

Case 1: The first matrix we consider is

$$\begin{pmatrix} A & B \\ C & A \end{pmatrix} \quad (63)$$

where  $A = \text{circ}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = \text{rcirc}(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$  and  $C = \text{rcirc}(\alpha_7, \alpha_8, \alpha_5, \alpha_6)$ . First we construct a  $4 \times 4$  block matrix by combining the matrix in (63) with a block matrix obtained from the group ring  $R(C_2 \times C_2)$  in Section 2:

$$\begin{pmatrix} A & B \\ C & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{pmatrix}, \quad (64)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $A_3 = \text{circ}(\alpha_7, \alpha_8)$  and  $B_3 = \text{circ}(\alpha_5, \alpha_6)$ . Now we give the following results using the  $4 \times 4$  block matrix in (64).

**Theorem 3.7.** *The matrix*

$$G = \left[ \begin{array}{c|cc} I_8 & A_1 & B_1 & A_2 & B_2 \\ & B_1 & A_1 & B_2 & A_2 \\ & A_3 & B_3 & A_1 & B_1 \\ & B_3 & A_3 & B_1 & A_1 \end{array} \right], \quad (65)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $A_3 = \text{circ}(\alpha_7, \alpha_8)$  and  $B_3 = \text{circ}(\alpha_5, \alpha_6)$ , is the generator matrix of a self-dual code over  $R$ , if and only if the following equations hold in  $R$ :

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (66)$$

$$2A_1B_1 + 2A_2B_2 = 0, \quad (67)$$

$$A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0, \quad (68)$$

$$A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 = 0, \quad (69)$$

$$A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2, \quad (70)$$

$$2A_1B_1 + 2A_3B_3 = 0. \quad (71)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{bmatrix},$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{bmatrix} \begin{bmatrix} A_1 & B_1 & A_3 & B_3 \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_3 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & 2A_1B_1 + 2A_2B_2 \\ 2A_1B_1 + 2A_2B_2 & A_1^2 + A_2^2 + B_1^2 + B_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 & A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 \\ A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 & A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_1^2 + A_3^2 + B_1^2 + B_3^2 & 2A_1B_1 + 2A_3B_3 \\ 2A_1B_1 + 2A_3B_3 & A_1^2 + A_3^2 + B_1^2 + B_3^2 \end{bmatrix}.$$

This will equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $2A_1B_1 + 2A_2B_2 = 0$ ,  $A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0$ ,  $A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 = 0$ ,  $A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2$  and  $2A_1B_1 + 2A_3B_3 = 0$ .  $\square$

Now, we construct a  $4 \times 4$  block matrix by combining the matrix (64) with a block matrix obtained from the group ring  $RC_4$  in Section 2:

$$\begin{pmatrix} A & B \\ C & A \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B'_3 & A_3 & B'_1 & A_1 \end{pmatrix}, \quad (72)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ ,  $A_3 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B_3 = \text{circ}(\alpha_5, \alpha_6)$  and  $B'_3 = \text{circ}(\alpha_6, \alpha_5)$ . Now we give the following results using the  $4 \times 4$  block matrix in (72).

**Theorem 3.8.** *The matrix*

$$G = \left[ \begin{array}{c|cc} I_8 & A_1 & B_1 & A_2 & B_2 \\ \hline & B'_1 & A_1 & B'_2 & A_2 \\ & A_3 & B_3 & A_1 & B_1 \\ & B'_3 & A_3 & B'_1 & A_1 \end{array} \right], \quad (73)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ ,  $A_3 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B_3 = \text{circ}(\alpha_5, \alpha_6)$  and  $B'_3 = \text{circ}(\alpha_6, \alpha_5)$ , generates a self-dual code of length 16 over  $R$ , if and only if the following equations hold in  $R$ :

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2, \quad (74)$$

$$A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 = 0, \quad (75)$$

$$B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2, \quad (76)$$

$$A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0, \quad (77)$$

$$A_2B'_1 + A_3B_1 + A_1B'_3 + A_1B_2 = 0, \quad (78)$$

$$A_3B'_1 + A_2B_1 + A_1B'_2 + A_1B_3 = 0, \quad (79)$$

$$B'_1B'_2 + B'_1B'_3 + A_1A_2 + A_1A_3 = 0, \quad (80)$$

$$A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2, \quad (81)$$

$$A_1B'_1 + A_1B_1 + A_3B'_3 + A_3B_3 = 0, \quad (82)$$

$$B_1'^2 + B_3'^2 + A_1^2 + A_3^2 = -I_2. \quad (83)$$

*Proof.* The code  $C$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Let

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B'_3 & A_3 & B'_1 & A_1 \end{bmatrix},$$

we have to show that  $XX^T = -I_8$ . Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B'_3 & A_3 & B'_1 & A_1 \end{bmatrix} \begin{bmatrix} A_1 & B'_1 & A_3 & B'_3 \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B'_2 & A_1 & B'_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 \\ A_1B'_1 + A_1B_1 + A_2B'_2 + A_2B_2 & B_1'^2 + B_2'^2 + A_1^2 + A_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 & A_2B'_1 + A_3B_1 + A_1B'_3 + A_1B_2 \\ A_3B'_1 + A_2B_1 + A_1B'_2 + A_1B_3 & B'_1B'_2 + B'_1B'_3 + A_1A_2 + A_1A_3 \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 & A_3B'_1 + A_2B_1 + A_1B'_2 + A_1B_3 \\ A_2B'_1 + A_3B_1 + A_1B'_2 + A_1B_3 & B'_1B'_2 + B'_1B'_3 + A_1A_2 + A_1A_3 \end{bmatrix},$$

$$X_4 = \begin{bmatrix} A_1^2 + A_3^2 + B_1^2 + B_3^2 & A_1B_1' + A_1B_1 + A_3B_3' + A_3B_3 \\ A_1B_1' + A_1B_1 + A_3B_3' + A_3B_3 & B_1'^2 + B_3'^2 + A_1^2 + A_3^2 \end{bmatrix}.$$

This will equal to  $-I_8$  only if  $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$ ,  $A_1B_1' + A_1B_1 + A_2B_2' + A_2B_2 = 0$ ,  $B_1'^2 + B_2'^2 + A_1^2 + A_2^2 = -I_2$ ,  $A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0$ ,  $A_2B_1' + A_3B_1 + A_1B_3' + A_1B_2 = 0$ ,  $A_3B_1' + A_2B_1 + A_1B_2' + A_1B_3 = 0$ ,  $B_1'B_2' + B_1'B_3' + A_1A_2 + A_1A_3 = 0$ ,  $A_1^2 + A_3^2 + B_1^2 + B_3^2 = -I_2$ ,  $A_1B_1' + A_1B_1 + A_3B_3' + A_3B_3 = 0$  and  $B_1'^2 + B_3'^2 + A_1^2 + A_3^2 = -I_2$ .  $\square$

Case 2: Here we consider the matrix

$$\begin{pmatrix} A & B \\ C & A^T \end{pmatrix}, \quad (84)$$

where  $A = \text{circ}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ,  $B = \text{circ}(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$ ,  $C = \text{circ}(\alpha_7, \alpha_6, \alpha_5, \alpha_8)$ . Now, combining the matrix (84) with the block matrix obtained from the group ring  $R(C_2 \times C_2)$  we get:

$$\begin{pmatrix} A & B \\ C & A^T \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3 & A_3 & B_4 & A_4 \end{pmatrix}, \quad (85)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $A_3 = \text{circ}(\alpha_7, \alpha_6)$ ,  $B_3 = \text{circ}(\alpha_5, \alpha_8)$ ,  $A_4 = \text{circ}(\alpha_1, \alpha_4)$  and  $B_4 = \text{circ}(\alpha_3, \alpha_2)$ . If we apply the following permutation

$$\begin{pmatrix} A_3 & B_3 \\ \downarrow & \downarrow \\ B_3 & A_3 \end{pmatrix}$$

to the symbols in the ninth and tenth positions of the matrix (85), we get

$$\begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ B_3 & A_3 & A_4 & B_4 \\ A_3 & B_3 & B_4 & A_4 \end{pmatrix}, \quad (86)$$

which is the same as matrix (43).

Similarly, combining matrix (43) with a block matrix obtained from the group ring  $RC_4$  in Section 2:

$$\begin{pmatrix} A & B \\ C & A^T \end{pmatrix} \rightarrow \begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1' & A_1 & B_2' & A_2 \\ A_3 & B_3 & A_4 & B_4 \\ B_3' & A_3 & B_4' & A_4 \end{pmatrix}, \quad (87)$$

where  $A_1 = \text{circ}(\alpha_1, \alpha_2)$ ,  $B_1 = \text{circ}(\alpha_3, \alpha_4)$ ,  $B'_1 = \text{circ}(\alpha_4, \alpha_3)$ ,  $A_2 = \text{circ}(\alpha_5, \alpha_6)$ ,  $B_2 = \text{circ}(\alpha_7, \alpha_8)$ ,  $B'_2 = \text{circ}(\alpha_8, \alpha_7)$ ,  $A_3 = \text{circ}(\alpha_7, \alpha_6)$ ,  $B_3 = \text{circ}(\alpha_5, \alpha_8)$ ,  $B'_3 = \text{circ}(\alpha_8, \alpha_5)$ ,  $A_4 = \text{circ}(\alpha_1, \alpha_4)$ ,  $B_4 = \text{circ}(\alpha_3, \alpha_2)$  and  $B'_4 = \text{circ}(\alpha_2, \alpha_3)$ . If we apply the following permutation

$$\begin{pmatrix} A_3 & B_3 & B'_3 \\ \downarrow & \downarrow & \downarrow \\ B_3 & A_3 & A'_3 \end{pmatrix}$$

to the symbols in the ninth and tenth positions of the matrix (87), we get

$$\begin{pmatrix} A_1 & B_1 & A_2 & B_2 \\ B'_1 & A_1 & B'_2 & A_2 \\ B_3 & A_3 & A_4 & B_4 \\ A'_3 & B_3 & B'_4 & A_4 \end{pmatrix}, \quad (88)$$

where  $A'_3 = \text{circ}(\alpha_6, \alpha_7)$ , which is the same as matrix (51). So we have shown that matrices (85) and (87) are equivalent to matrices (43) and (51) respectively.

## 4 $[64, 32, 12]_2$ Singly-Even Codes as Images of $\mathbb{F}_4 + u\mathbb{F}_4$ -Lifts of Codes Over $\mathbb{F}_4$

In this section, we apply each result from the previous section to the ring  $\mathbb{F}_4$  to obtain self-dual codes of length 32 with minimum Lee weight  $\geq 6$ . We then lift the  $\mathbb{F}_4$  codes to  $\mathbb{F}_4 + u\mathbb{F}_4$  to obtain extremal self-dual binary images of codes with parameters  $[64, 32, 12]_2$ .

**Theorem 4.1.** *Let  $M = (I \mid A)$  be a  $\frac{n}{2} \times n$  generator matrix in the finite Frobenius ring  $S$ . Let  $S$  be a subring of the Frobenius ring  $R$ . If  $M$  generates a self-dual code of length  $n$  over  $S$  then  $M$  generates a self-dual code over  $R$ .*

*Proof.* Since any two rows of  $M$  are orthogonal over  $S$  then they are orthogonal over  $R$ . Then the free rank of  $\langle M \rangle$  over  $R$  is  $\frac{n}{2}$  which gives that  $\langle M \rangle$  has cardinality  $|R|^{\frac{n}{2}}$ . It follows that  $C$  is self-dual, since  $C$  is self-orthogonal, i.e.  $C \subseteq C^\perp$  and  $|C| = |C^\perp| = |R|^{\frac{n}{2}}$ .  $\square$

The technique we use here is the following. We begin with a matrix  $M$  of the form  $M = (I \mid A)$  which generates a self-dual code of length  $n$  over  $\mathbb{F}_2$ . Then this lifts via the previous theorem to the field  $\mathbb{F}_4$  and then to the ring  $\mathbb{F}_4 + u\mathbb{F}_4$ . Following this we use the Gray map  $(\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow \mathbb{F}_2^{4n}$  which gives a binary self-dual code of length  $4n$ . We see this in the following diagram:

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

If  $M$  is the original matrix used then we define  $\Omega(M)$  to be the matrix which generates the self-dual code over  $\mathbb{F}_2$  of length  $4n$ . We note that this matrix can be put in to the form  $(I | A)$  since  $\mathbb{F}_2$  is a field.

Let  $M$  be a matrix that generates a self-dual code  $C$  in  $\mathbb{F}_2^n$ . Then this code lifts to a code  $D$  in  $\mathbb{F}_4^n$  and then to a code  $D'$  in  $(\mathbb{F}_4 + u\mathbb{F}_4)^n$ . Applying the Gray map to the code  $D'$  gives a self-dual code  $C'$  in  $\mathbb{F}_2^{4n}$ . This self-dual binary code  $C'$  has a generator matrix, call it  $\Omega(M)$ , since it came from the matrix  $M$ . Then this process can be done again to produce a self-dual code  $C''$  in  $\mathbb{F}_2^{4(4n)}$ , which has a generator matrix  $\Omega^2(M) = \Omega(\Omega(M))$ . Then the matrix  $\Omega^i(M) = \Omega(\Omega(\Omega(\dots(\Omega(M))))))$  generates a self-dual code in  $\mathbb{F}_2^{4^i n}$ . This leads to the following theorem.

**Theorem 4.2.** *Any generator matrix of a binary self-dual code gives rise to an infinite family of binary self-dual codes.*

*Proof.* Given a matrix  $M$  generating a binary self-dual code, the family  $\Omega^i(M)$  is an infinite family of binary self-dual codes.  $\square$

There are two possibilities for the weight enumerators of extremal singly-even  $[64, 32, 12]_2$  codes ([2]):

$$W_{64,1} = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \dots, \quad 14 \leq \beta \leq 284,$$

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

With the most updated information, the existence of codes is known for  $\beta = 14, 18, 22, 25, 29, 32, 35, 36, 39, 44, 46, 53, 59, 60, 64$  and  $74$  in  $W_{64,1}$  and for  $\beta = 0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, \dots, 25, 28, 29, 30, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120$  and  $184$  in  $W_{64,2}$ .

We now implement the search for self dual codes by applying the composite matrices from Section 3 to the ring  $\mathbb{F}_4$  to obtain self-dual codes of length 32 with minimum Lee weight  $\geq 6$ . We then lift the  $\mathbb{F}_4$  codes to  $\mathbb{F}_4 + u\mathbb{F}_4$  to obtain extremal self-dual binary images of codes with parameters  $[64, 32, 12]$ . The search is implemented using *MAGMA* ([1]).

In the coming tables,  $r_{A_1}, r_{B_1}, r_{A_2}, r_{B_2}, r_{A_3}, r_{B_3}, r_{A_4}, r_{B_4}$  are the first rows of the matrices  $A_1, B_1, A_2, B_2, A_3, B_3, A_4, B_4$  respectively that we have used in the appropriate theorem in Section 4. In order to fit the upcoming tables regarding the results, we label the elements of  $\mathbb{F}_4 + u\mathbb{F}_4$  as follows:



$z_1$	0	$a_1$	1	$b_1$	$\omega$	$c_1$	$1 + \omega$
$z_2$	$u$	$a_2$	$1 + u$	$b_2$	$\omega + u$	$c_2$	$1 + \omega + u$
$z_3$	$u\omega$	$a_3$	$1 + u\omega$	$b_3$	$\omega + u\omega$	$c_3$	$1 + \omega + u\omega$
$z_4$	$u + u\omega$	$a_4$	$1 + u + u\omega$	$b_4$	$\omega + u + u\omega$	$c_4$	$1 + \omega + u + u\omega$

The groups we use are not necessarily of interest from the point of view of group theory, they are generally used because they produce interesting codes. We split the rest of this section into subsection to make the tabulated results easy to read.

#### 4.1 $C_8$ replaced with groups $C_2 \times C_2$ and $C_4$

We now apply Theorem 3.1 from Section 3 over  $\mathbb{F}_4$ .

Table 1: Theorem 3.1 over  $\mathbb{F}_4$

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 0)	(1, 1)	( $\omega$ , 1)	( $\omega + 1$ , 1)	(1, $\omega$ )	(1, $\omega + 1$ )	$[32, 16, 8]_{II}$	$2^9 3^{25}$
$C_2$	(0, $\omega$ )	(1, $\omega + 1$ )	(0, 0)	( $\omega + 1$ , $\omega$ )	( $\omega$ , 0)	(0, $\omega + 1$ )	$[32, 16, 8]_{II}$	$2^{15} 3^{25} \cdot 7$
$C_3$	(0, 0)	(1, 1)	(0, $\omega$ )	(1, $\omega$ )	( $\omega$ , 0)	( $\omega$ , 1)	$[32, 16, 6]_I$	$2^8 3$
$C_4$	(0, 0)	(1, 1)	( $\omega$ , 0)	( $\omega + 1$ , 0)	(0, $\omega$ )	(0, $\omega + 1$ )	$[32, 16, 6]_I$	$2^9 3^{25}$
$C_5$	(0, 1)	( $\omega$ , $\omega + 1$ )	(0, 1)	( $\omega$ , $\omega$ )	( $\omega$ , 0)	(1, $\omega$ )	$[32, 16, 6]_I$	$2^7 3$
$C_6$	(0, $\omega$ )	(1, $\omega + 1$ )	(0, 1)	( $\omega + 1$ , $\omega + 1$ )	( $\omega + 1$ , 0)	(1, $\omega + 1$ )	$[32, 16, 6]_I$	$2^{11} 3$

We now lift the  $\mathbb{F}_4$ -codes in Table 1 to  $\mathbb{F}_4 + u\mathbb{F}_4$ , as a result we obtain extremal binary self-dual codes of length 64 as given in Table 2.

Table 2: The  $\mathbb{F}_4 + u\mathbb{F}_4$ -lifts of  $C_i$  and the  $\beta$  values of the binary images

code		$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$\beta$ in $W_{64,2}$	$ Aut(C) $
$I_1$	$C_5$	( $z_4$ , $a_3$ )	( $b_1$ , $c_2$ )	( $z_3$ , $a_1$ )	( $b_2$ , $b_1$ )	( $b_1$ , $z_3$ )	( $a_1$ , $b_2$ )	8	$2^4$
$I_2$	$C_5$	( $z_3$ , $a_1$ )	( $b_3$ , $c_1$ )	( $z_2$ , $a_3$ )	( $b_4$ , $b_3$ )	( $b_3$ , $z_2$ )	( $a_3$ , $b_4$ )	8	$2^5$
$I_3$	$C_2$	( $z_1$ , $b_1$ )	( $a_2$ , $c_2$ )	( $z_4$ , $z_2$ )	( $c_1$ , $b_1$ )	( $b_1$ , $z_4$ )	( $z_2$ , $c_1$ )	12	$2^4$
$I_4$	$C_2$	( $z_1$ , $b_1$ )	( $a_3$ , $c_3$ )	( $z_2$ , $z_4$ )	( $c_1$ , $b_2$ )	( $b_2$ , $z_2$ )	( $z_4$ , $c_1$ )	24	$2^4$
$I_5$	$C_2$	( $z_1$ , $b_1$ )	( $a_4$ , $c_4$ )	( $z_2$ , $z_4$ )	( $c_2$ , $b_2$ )	( $b_2$ , $z_2$ )	( $z_4$ , $c_2$ )	24	$2^5$
$I_6$	$C_2$	( $z_1$ , $b_1$ )	( $a_3$ , $c_3$ )	( $z_4$ , $z_2$ )	( $c_2$ , $b_2$ )	( $b_2$ , $z_4$ )	( $z_2$ , $c_2$ )	28	$2^4$
$I_7$	$C_2$	( $z_1$ , $b_1$ )	( $a_4$ , $c_4$ )	( $z_2$ , $z_3$ )	( $c_2$ , $b_1$ )	( $b_1$ , $z_2$ )	( $z_3$ , $c_2$ )	32	$2^5$
$I_8$	$C_2$	( $z_1$ , $b_2$ )	( $a_4$ , $c_4$ )	( $z_3$ , $z_4$ )	( $c_2$ , $b_4$ )	( $b_4$ , $z_3$ )	( $z_4$ , $c_2$ )	32	$2^6$
$I_9$	$C_5$	( $z_2$ , $a_1$ )	( $b_1$ , $c_2$ )	( $z_4$ , $a_1$ )	( $b_4$ , $b_4$ )	( $b_4$ , $z_4$ )	( $a_1$ , $b_4$ )	40	$2^5$

We now apply Theorem 3.2 from Section 3 over  $\mathbb{F}_4$ .

Table 3: Theorem 3.2 over  $\mathbb{F}_4$ 

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 0)	(1, $\omega$ )	( $\omega + 1$ , 1)	(1, 1)	(1, $\omega + 1$ )	(1, 1)	$[32, 16, 8]_{II}$	$2^9 3^{25}$
$C_2$	(0, 1)	(1, 0)	(1, $\omega$ )	(1, $\omega + 1$ )	( $\omega + 1$ , 1)	( $\omega$ , 1)	$[32, 16, 8]_{II}$	$2^{15} 3^{25} \cdot 7$
$C_3$	( $\omega, \omega + 1$ )	( $\omega + 1, \omega$ )	( $\omega$ , 0)	( $\omega$ , 1)	(1, $\omega$ )	(0, $\omega$ )	$[32, 16, 8]_I$	$2^{12} 3 \cdot 7$
$C_4$	(0, 0)	(0, $\omega$ )	(0, $\omega + 1$ )	( $\omega + 1, \omega + 1$ )	( $\omega + 1$ , 0)	( $\omega + 1, \omega + 1$ )	$[32, 16, 6]_I$	$2^9 3^{25}$
$C_5$	(0, 0)	(0, $\omega$ )	(1, $\omega$ )	( $\omega$ , $\omega$ )	( $\omega$ , 1)	( $\omega$ , $\omega$ )	$[32, 16, 6]_I$	$2^8 3$
$C_6$	(0, 1)	(1, 0)	( $\omega$ , 0)	( $\omega$ , 1)	(1, $\omega$ )	(0, $\omega$ )	$[32, 16, 6]_I$	$2^6$

We now lift the  $\mathbb{F}_4$ -codes in Table 3 to  $\mathbb{F}_4 + u\mathbb{F}_4$ , as a result we obtain extremal binary self-dual codes of length 64 as given in Table 4.

Table 4: The  $\mathbb{F}_4 + u\mathbb{F}_4$ -lifts of  $C_i$  and the  $\beta$  values of the binary images

code	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$\beta$ in $W_{64,2}$	$ Aut(C) $
$J_1$	$C_6$ ( $z_2, a_1$ )	( $a_1, z_2$ )	( $b_1, z_4$ )	( $b_1, a_2$ )	( $a_2, b_1$ )	( $z_4, b_1$ )	0	$2^6$
$J_2$	$C_6$ ( $z_4, a_3$ )	( $a_3, z_4$ )	( $b_2, z_1$ )	( $b_2, a_4$ )	( $a_4, b_2$ )	( $z_1, b_2$ )	4	$2^5$
$J_3$	$C_6$ ( $z_3, a_1$ )	( $a_1, z_3$ )	( $b_2, z_1$ )	( $b_2, a_4$ )	( $a_4, b_2$ )	( $z_1, b_2$ )	12	$2^5$
$J_4$	$C_2$ ( $z_4, a_1$ )	( $a_1, z_4$ )	( $a_3, b_4$ )	( $a_3, c_2$ )	( $c_2, a_3$ )	( $b_4, a_3$ )	24	$2^5$
$J_5$	$C_3$ ( $b_1, c_2$ )	( $c_2, b_1$ )	( $b_2, z_1$ )	( $b_2, a_4$ )	( $a_4, b_2$ )	( $z_1, b_2$ )	28	$2^5$
$J_6$	$C_3$ ( $b_2, c_1$ )	( $c_1, b_2$ )	( $b_1, z_2$ )	( $b_1, a_3$ )	( $a_3, b_1$ )	( $z_2, b_1$ )	44	$2^5$
$J_7$	$C_3$ ( $b_2, c_4$ )	( $c_4, b_2$ )	( $b_1, z_4$ )	( $b_1, a_2$ )	( $a_2, b_1$ )	( $z_4, b_1$ )	48	$2^5$
$J_8$	$C_3$ ( $b_1, c_3$ )	( $c_3, b_1$ )	( $b_2, z_1$ )	( $b_2, a_4$ )	( $a_4, b_2$ )	( $z_1, b_2$ )	52	$2^5$

## 4.2 $C_4 \times C_2$ replaced with groups $C_2 \times C_2$ and $C_4$

Here we apply Theorem 3.3 and Theorem 3.4 Section 3 over  $\mathbb{F}_4$ .

Table 5: Theorem 3.3 over  $\mathbb{F}_4$ 

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 0)	(0, $\omega$ )	(1, $\omega$ )	( $\omega + 1, \omega + 1$ )	$[32, 16, 8]_{II}$	$2^9 3^{25}$
$C_2$	(0, 0)	(0, 1)	(0, 1)	( $\omega, \omega + 1$ )	$[32, 16, 6]_I$	$2^9 3^{25}$
$C_3$	(0, 0)	(0, $\omega$ )	(1, 1)	(1, $\omega$ )	$[32, 16, 6]_I$	$2^8 3$

Table 6: Theorem 3.4 over  $\mathbb{F}_4$ 

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 0)	(0, $\omega$ )	( $\omega + 1, \omega + 1$ )	(1, $\omega$ )	$[32, 16, 8]_{II}$	$2^9 3^2 5$
$C_2$	(0, 0)	(0, $\omega$ )	(1, 1)	(0, $\omega + 1$ )	$[32, 16, 6]_I$	$2^9 3^2 5$
$C_3$	(0, 0)	(0, $\omega$ )	(1, 1)	(1, $\omega$ )	$[32, 16, 6]_I$	$2^8 3$

Unfortunately, we were unable to find any codes of length 64 by lifting the  $\mathbb{F}_4$ -codes in Tables 5 and 6 to  $\mathbb{F}_4 + u\mathbb{F}_4$ .

### 4.3 $D_8$ replaced with groups $C_2 \times C_2$ and $C_4$

We now apply Theorem 3.5 from Section 3 over  $\mathbb{F}_4$ .

Table 7: Theorem 3.5 over  $\mathbb{F}_4$ 

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$r_{A_4}$	$r_{B_4}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 0)	(0, $\omega$ )	( $\omega + 1, 1$ )	( $\omega + 1, \omega$ )	( $\omega + 1, \omega$ )	( $\omega + 1, 1$ )	(0, $\omega$ )	(0, 0)	$[32, 16, 8]_{II}$	$2^9 3^2 5$
$C_2$	(0, 0)	(1, $\omega$ )	(0, $\omega$ )	( $\omega + 1, \omega + 1$ )	(0, $\omega + 1$ )	( $\omega + 1, \omega$ )	(0, $\omega$ )	(1, 0)	$[32, 16, 8]_{II}$	$2^5 3 \cdot 5 \cdot 31$
$C_3$	(0, 1)	(1, $\omega$ )	(1, 0)	( $\omega + 1, 1$ )	(1, 1)	( $\omega + 1, 0$ )	(0, $\omega$ )	(1, 1)	$[32, 16, 8]_{II}$	$2^{15} 3^2 5 \cdot 7$
$C_4$	(0, $\omega$ )	( $\omega, \omega + 1$ )	( $\omega, 1$ )	( $\omega + 1, \omega$ )	( $\omega, \omega$ )	( $\omega + 1, 1$ )	(0, $\omega + 1$ )	( $\omega, \omega$ )	$[32, 16, 8]_I$	$2^{12} 3 \cdot 7$
$C_5$	(0, 0)	(0, $\omega$ )	(1, 0)	(1, $\omega + 1$ )	(1, $\omega + 1$ )	(1, 0)	(0, $\omega$ )	(0, 0)	$[32, 16, 6]_I$	$2^9 3^2 5$
$C_6$	(0, 0)	(0, $\omega$ )	(1, 1)	(1, $\omega$ )	(1, $\omega$ )	(1, 1)	(0, $\omega$ )	(0, 0)	$[32, 16, 6]_I$	$2^8 3$
$C_7$	(0, 0)	(1, $\omega$ )	(1, 0)	( $\omega, 1$ )	(1, 1)	( $\omega, 0$ )	(0, $\omega$ )	(1, 0)	$[32, 16, 6]_I$	$2^6$
$C_8$	(0, 0)	(1, $\omega$ )	(1, $\omega$ )	( $\omega, \omega + 1$ )	(1, $\omega + 1$ )	( $\omega, \omega$ )	(0, $\omega$ )	(1, 0)	$[32, 16, 6]_I$	$2^3 3$
$C_9$	(0, 1)	(1, $\omega$ )	(1, $\omega$ )	( $\omega + 1, \omega + 1$ )	(1, $\omega + 1$ )	( $\omega + 1, \omega$ )	(0, $\omega$ )	(1, 1)	$[32, 16, 6]_I$	$2^5$

We now lift the  $\mathbb{F}_4$ -codes in Table 7 to  $\mathbb{F}_4 + u\mathbb{F}_4$ , as a result we obtain extremal binary self-dual codes of length 64 as given in Table 8.

Table 8: The  $\mathbb{F}_4 + u\mathbb{F}_4$ -lifts of  $C_i$  and the  $\beta$  values of the binary images

code		$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$r_{A_4}$	$r_{B_4}$	$\beta$ in $W_{64,2}$	$ Aut(C) $
$K_1$	$C_2$	$(z_1, z_2)$	$(a_3, b_1)$	$(z_2, b_1)$	$(c_1, c_4)$	$(z_2, c_4)$	$(c_1, b_1)$	$(z_1, b_1)$	$(a_3, z_2)$	0	$2^5$
$K_2$	$C_3$	$(z_1, a_1)$	$(a_3, b_1)$	$(a_3, z_2)$	$(c_2, a_2)$	$(a_3, a_2)$	$(c_2, z_2)$	$(z_1, b_1)$	$(a_3, a_1)$	0	$2^4$
$K_3$	$C_9$	$(z_1, a_1)$	$(a_3, b_2)$	$(a_1, b_1)$	$(c_2, c_4)$	$(a_1, c_4)$	$(c_2, b_1)$	$(z_1, b_2)$	$(a_3, a_1)$	0	$2^5$
$K_4$	$C_7$	$(z_1, z_1)$	$(a_1, b_2)$	$(a_1, z_3)$	$(b_2, a_4)$	$(a_1, a_4)$	$(b_2, z_3)$	$(z_1, b_2)$	$(a_1, z_1)$	0	$2^4$
$K_5$	$C_4$	$(z_2, b_2)$	$(b_1, c_2)$	$(b_2, a_2)$	$(c_2, b_4)$	$(b_2, b_4)$	$(c_2 a_2)$	$(z_2, c_2)$	$(b_1, b_2)$	0	$2^6$
$K_6$	$C_4$	$(z_2, b_1)$	$(b_2, c_4)$	$(b_2, a_1)$	$(c_1, b_2)$	$(b_2, b_2)$	$(c_1, a_1)$	$(z_2, c_4)$	$(b_2, b_1)$	4	$2^4$
$K_7$	$C_7$	$(z_4, z_1)$	$(a_3, b_2)$	$(a_3, z_4)$	$(b_4, a_4)$	$(a_3, a_4)$	$(b_4, z_4)$	$(z_4, b_2)$	$(a_3, z_1)$	4	$2^5$
$K_8$	$C_1$	$(z_1, z_2)$	$(z_3, b_1)$	$(c_1, a_1)$	$(c_4, b_4)$	$(c_1, b_4)$	$(c_4, a_1)$	$(z_1, b_1)$	$(z_3, z_2)$	8	$2^5$
$K_9$	$C_1$	$(z_2, z_4)$	$(z_3, b_2)$	$(c_1, a_3)$	$(c_2, b_4)$	$(c_1, b_4)$	$(c_2, a_3)$	$(z_2, b_2)$	$(z_3, z_4)$	8	$2^4$
$K_{10}$	$C_2$	$(z_1, z_2)$	$(z_3, b_1)$	$(z_2, b_1)$	$(c_4, c_3)$	$(z_2, c_3)$	$(c_4, b_1)$	$(z_1, b_1)$	$(a_3, z_2)$	12	$2^4$
$K_{11}$	$C_4$	$(z_4, b_1)$	$(b_1, c_4)$	$(b_1, a_3)$	$(c_4, b_4)$	$(b_1, b_4)$	$(c_4, a_3)$	$(z_4, c_4)$	$(b_1, b_1)$	12	$2^5$
$K_{12}$	$C_1$	$(z_1, z_1)$	$(z_3, b_2)$	$(c_1, a_3)$	$(c_4, b_4)$	$(c_1, b_4)$	$(c_4, a_3)$	$(z_1, b_2)$	$(z_3, z_1)$	16	$2^6$
$K_{13}$	$C_1$	$(z_1, z_3)$	$(z_4, b_2)$	$(c_1, a_1)$	$(c_2, b_2)$	$(c_1, b_2)$	$(c_2, a_1)$	$(z_1, b_2)$	$(z_4, z_3)$	16	$2^4$
$K_{14}$	$C_1$	$(z_1, z_3)$	$(z_3, b_2)$	$(c_2, a_1)$	$(c_3, b_3)$	$(c_2, b_3)$	$(c_3, a_1)$	$(z_1, b_2)$	$(z_3, z_3)$	16	$2^5$
$K_{15}$	$C_2$	$(z_2, z_2)$	$(a_1, b_1)$	$(z_3, b_1)$	$(c_2, c_4)$	$(z_3, z_4)$	$(c_2, b_1)$	$(z_2, b_1)$	$(a_1, z_2)$	20	$2^4$
$K_{16}$	$C_3$	$(z_2, a_1)$	$(a_3, b_2)$	$(a_3, z_2)$	$(c_4, a_4)$	$(a_3, a_4)$	$(c_4, z_2)$	$(z_2, b_2)$	$(a_3, a_1)$	20	$2^5$
$K_{17}$	$C_1$	$(z_1, z_2)$	$(z_3, b_2)$	$(c_1, a_3)$	$(c_4, b_2)$	$(c_1, b_2)$	$(c_4, a_3)$	$(z_1, b_2)$	$(z_3, z_2)$	24	$2^5$
$K_{18}$	$C_1$	$(z_2, z_2)$	$(z_3, b_2)$	$(c_1, a_1)$	$(c_2, b_1)$	$(c_1, b_1)$	$(c_2, a_1)$	$(z_2, b_2)$	$(z_3, z_2)$	24	$2^4$
$K_{19}$	$C_2$	$(z_2, z_1)$	$(a_1, b_2)$	$(z_4, b_2)$	$(c_1, c_3)$	$(z_4, c_3)$	$(c_1, b_2)$	$(z_2, b_2)$	$(a_1, z_1)$	28	$2^4$
$K_{20}$	$C_4$	$(z_1, b_1)$	$(b_2, c_2)$	$(b_1, a_4)$	$(c_2, b_2)$	$(b_1, b_2)$	$(c_2, a_4)$	$(z_1, c_2)$	$(b_2, b_1)$	28	$2^5$
$K_{21}$	$C_1$	$(z_1, z_2)$	$(z_3, b_2)$	$(c_1, a_1)$	$(c_4, b_3)$	$(z_1, b_3)$	$(a_4, a_1)$	$(z_1, b_2)$	$(z_3, z_2)$	32	$2^5$
$K_{22}$	$C_4$	$(z_4, b_2)$	$(b_1, c_1)$	$(b_2, a_1)$	$(c_3, b_1)$	$(b_2, b_1)$	$(c_3, a_1)$	$(z_4, c_1)$	$(b_1, b_2)$	32	$2^4$
$K_{23}$	$C_7$	$(z_1, z_1)$	$(a_3, b_2)$	$(a_1, z_4)$	$(b_1, a_3)$	$(a_1, a_3)$	$(b_1, z_4)$	$(z_1, b_2)$	$(a_3, z_1)$	36	$2^4$
$K_{24}$	$C_4$	$(z_3, b_1)$	$(b_2, c_4)$	$(b_1, a_4)$	$(c_4, b_3)$	$(b_1, b_3)$	$(c_4, a_4)$	$(z_3, c_4)$	$(b_2, b_1)$	36	$2^5$
$K_{25}$	$C_5$	$(z_1, z_4)$	$(z_4, b_2)$	$(a_1, z_2)$	$(a_2, c_1)$	$(a_1, c_1)$	$(a_2, z_2)$	$(z_1, b_2)$	$(z_4, z_4)$	40	$2^5$
$K_{26}$	$C_2$	$(z_4, z_1)$	$(a_1, b_1)$	$(z_1, b_2)$	$(c_2, c_1)$	$(z_1, c_1)$	$(c_2, b_2)$	$(z_4, b_1)$	$(a_1, z_1)$	44	$2^4 3$
$K_{27}$	$C_4$	$(z_2, b_2)$	$(b_1, c_1)$	$(b_2, a_3)$	$(c_1, b_1)$	$(b_2, b_1)$	$(c_1, a_3)$	$(z_2, c_1)$	$(b_1, b_2)$	44	$2^5$
$K_{28}$	$C_4$	$(z_4, b_2)$	$(b_1, c_4)$	$(b_2, a_2)$	$(c_4, b_1)$	$(b_2, b_1)$	$(c_4, a_2)$	$(z_4, c_4)$	$(b_1, b_2)$	48	$2^5$
$K_{29}$	$C_4$	$(z_1, b_1)$	$(b_2, c_3)$	$(b_1, a_4)$	$(c_3, b_2)$	$(b_1, b_2)$	$(c_3, a_4)$	$(z_1, c_3)$	$(b_2, b_1)$	52	$2^5$

We now apply Theorem 3.6 from Section 3 over  $\mathbb{F}_4$ .

Table 9: Theorem 3.6 over  $\mathbb{F}_4$

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$r_{A_4}$	$r_{B_4}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 1)	(0, 1)	(1, $\omega$ )	(1, $\omega + 1$ )	(1, $\omega + 1$ )	(1, $\omega$ )	(0, 1)	(0, 1)	$[32, 16, 8]_{II}$	$2^{15}3^{25} \cdot 7$
$C_2$	(0, $\omega$ )	( $\omega$ , $\omega$ )	( $\omega$ , 1)	(1, 1)	( $\omega$ , 1)	(1, 1)	(0, $\omega$ )	( $\omega$ , $\omega$ )	$[32, 16, 8]_{II}$	$2^9 3^{25}$
$C_3$	( $\omega$ , 0)	( $\omega$ , 1)	( $\omega$ , $\omega + 1$ )	( $\omega$ , $\omega + 1$ )	( $\omega$ , $\omega + 1$ )	( $\omega$ , $\omega + 1$ )	( $\omega$ , 1)	( $\omega$ , 0)	$[32, 16, 8]_I$	$2^{12}3 \cdot 7$
$C_4$	(0, 0)	(0, $\omega$ )	(1, 1)	(1, $\omega$ )	(1, $\omega$ )	(1, 1)	(0, $\omega$ )	(0, 0)	$[32, 16, 6]_I$	$2^8 3$
$C_5$	(0, 0)	(0, $\omega$ )	( $\omega + 1$ , 0)	( $\omega + 1$ , $\omega + 1$ )	( $\omega + 1$ , $\omega + 1$ )	( $\omega + 1$ , 0)	(0, $\omega$ )	(0, 0)	$[32, 16, 6]_I$	$2^9 3^{25}$
$C_6$	(0, 1)	(0, 1)	( $\omega$ , 0)	( $\omega$ , 1)	( $\omega$ , 1)	( $\omega$ , 0)	(0, 1)	(0, 1)	$[32, 16, 6]_I$	$2^6$

We now lift the  $\mathbb{F}_4$ -codes in Table 9 to  $\mathbb{F}_4 + u\mathbb{F}_4$ , as a result we obtain extremal binary self-dual codes of length 64 as given in Table 10.

Table 10: The  $\mathbb{F}_4 + u\mathbb{F}_4$ -lifts of  $C_i$  and the  $\beta$  values of the binary images

code		$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$r_{A_4}$	$r_{B_4}$	$\beta$ in $W_{64,2}$	$ Aut(C) $
$L_1$	$C_6$	( $z_2, a_1$ )	( $z_2, a_1$ )	( $b_1, z_4$ )	( $b_1, a_2$ )	( $b_1, a_2$ )	( $b_1, z_4$ )	( $z_2, a_1$ )	( $z_2, a_1$ )	0	$2^6$
$L_2$	$C_6$	( $z_4, a_3$ )	( $z_4, a_3$ )	( $b_2, z_1$ )	( $b_2, a_4$ )	( $b_2, a_4$ )	( $b_2, z_1$ )	( $z_4, a_3$ )	( $z_4, a_3$ )	4	$2^5$
$L_3$	$C_4$	( $z_2, z_4$ )	( $z_2, b_2$ )	( $a_1, a_2$ )	( $a_1, b_1$ )	( $a_1, b_1$ )	( $a_1, a_2$ )	( $z_2, b_2$ )	( $z_2, z_4$ )	8	$2^5$
$L_4$	$C_6$	( $z_3, a_1$ )	( $z_3, a_1$ )	( $b_2, z_1$ )	( $b_2, a_4$ )	( $b_2, a_4$ )	( $b_2, z_1$ )	( $z_3, a_1$ )	( $z_3, a_1$ )	12	$2^5$
$L_5$	$C_5$	( $z_2, z_3$ )	( $z_2, b_1$ )	( $c_1, z_4$ )	( $c_1, c_3$ )	( $c_1, c_3$ )	( $c_1, z_4$ )	( $z_2, b_1$ )	( $z_2, z_3$ )	16	$2^4$
$L_6$	$C_3$	( $b_2, z_3$ )	( $b_2, a_2$ )	( $b_1, c_1$ )	( $b_1, c_3$ )	( $b_1, c_3$ )	( $b_1, c_1$ )	( $b_2, a_2$ )	( $b_2, z_3$ )	20	$2^4$
$L_7$	$C_3$	( $b_2, z_1$ )	( $b_2, a_1$ )	( $b_1, c_1$ )	( $b_1, c_2$ )	( $b_1, c_2$ )	( $b_1, c_1$ )	( $b_2, a_1$ )	( $b_2, z_1$ )	24	$2^4$
$L_8$	$C_4$	( $z_1, z_3$ )	( $z_1, b_1$ )	( $a_3, a_4$ )	( $a_3, b_2$ )	( $a_3, b_2$ )	( $a_3, a_4$ )	( $z_1, b_1$ )	( $z_1, z_3$ )	24	$2^5$
$L_9$	$C_3$	( $b_1, z_2$ )	( $b_1, a_1$ )	( $b_2, c_2$ )	( $b_2, c_3$ )	( $b_2, c_3$ )	( $b_2, c_2$ )	( $b_1, a_1$ )	( $b_1, z_2$ )	28	$2^4$
$L_{10}$	$C_3$	( $b_2, z_1$ )	( $b_2, a_4$ )	( $b_1, c_2$ )	( $b_1, c_2$ )	( $b_1, c_2$ )	( $b_1, c_2$ )	( $b_2, a_4$ )	( $b_2, z_1$ )	28	$2^5$
$L_{11}$	$C_3$	( $b_1, z_4$ )	( $b_1, a_1$ )	( $b_2, c_1$ )	( $b_2, c_3$ )	( $b_2, c_3$ )	( $b_2, c_1$ )	( $b_1, a_1$ )	( $b_1, z_4$ )	32	$2^4$
$L_{12}$	$C_4$	( $z_3, z_1$ )	( $z_3, b_1$ )	( $a_3, a_4$ )	( $a_3, b_1$ )	( $a_3, b_1$ )	( $a_3, a_4$ )	( $z_3, b_1$ )	( $z_3, z_1$ )	40	$2^5$
$L_{13}$	$C_3$	( $b_1, z_2$ )	( $b_1, a_3$ )	( $b_2, c_1$ )	( $b_2, c_1$ )	( $b_2, c_1$ )	( $b_2, c_1$ )	( $b_1, a_3$ )	( $b_1, z_2$ )	44	$2^5$
$L_{14}$	$C_3$	( $b_1, z_4$ )	( $b_1, a_2$ )	( $b_2, c_4$ )	( $b_2, c_4$ )	( $b_2, c_4$ )	( $b_2, c_4$ )	( $b_1, a_2$ )	( $b_1, z_4$ )	48	$2^4$
$L_{15}$	$C_3$	( $b_2, z_1$ )	( $b_2, a_4$ )	( $b_1, c_3$ )	( $b_1, c_3$ )	( $b_1, c_3$ )	( $b_1, c_3$ )	( $b_2, a_4$ )	( $b_2, z_1$ )	52	$2^5$

#### 4.4 $Q_8$ replaced with groups $C_2 \times C_2$ and $C_4$

We now apply Theorem 3.7 from Section 3 over  $\mathbb{F}_4$ .

Table 11: Theorem 3.7 over  $\mathbb{F}_4$

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 1)	(0, 1)	(1, 1)	$(\omega, \omega + 1)$	$(\omega, \omega + 1)$	(1, 1)	$[32, 16, 8]_{II}$	$2^9 3^{25}$
$C_2$	(0, 0)	$(\omega, \omega + 1)$	(0, 1)	(0, 1)	(0, 1)	(0, 1)	$[32, 16, 6]_I$	$2^9 3^{25}$
$C_3$	(0, 1)	(0, 1)	(0, 1)	$(\omega, \omega)$	$(\omega, \omega)$	(0, 1)	$[32, 16, 6]_I$	$2^8 3$

Unfortunately, we were unable to find any codes of length 64 by lifting the  $\mathbb{F}_4$ -codes in Table 11 to  $\mathbb{F}_4 + u\mathbb{F}_4$ .

Here, we apply Theorem 3.8 from Section 3 over  $\mathbb{F}_4$ .

Table 12: Theorem 3.8 over  $\mathbb{F}_4$

$C_i$	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$\psi_{\mathbb{F}_4}(C)$	$ Aut(C) $
$C_1$	(0, 1)	(0, 1)	(1, $\omega$ )	(1, $\omega + 1$ )	(1, $\omega + 1$ )	(1, $\omega$ )	$[32, 16, 8]_{II}$	$2^{15} 3^{25} \cdot 7$
$C_2$	$(\omega, \omega + 1)$	$(\omega, \omega + 1)$	(0, $\omega$ )	(1, $\omega$ )	(1, $\omega$ )	(0, $\omega$ )	$[32, 16, 8]_I$	$2^{12} 3 \cdot 7$
$C_3$	$(\omega, \omega + 1)$	$(\omega, \omega + 1)$	(1, $\omega$ )	(1, $\omega + 1$ )	(1, $\omega + 1$ )	(1, $\omega$ )	$[32, 16, 8]_{II}$	$2^9 3^{25}$
$C_4$	(0, 1)	(0, 1)	(0, $\omega$ )	(1, $\omega$ )	(1, $\omega$ )	(0, $\omega$ )	$[32, 16, 6]_I$	$2^6$
$C_5$	$(\omega, \omega + 1)$	$(\omega, \omega + 1)$	(0, $\omega$ )	(0, $\omega + 1$ )	(0, $\omega + 1$ )	(0, $\omega$ )	$[32, 16, 6]_I$	$2^9 3^{25}$

We now lift the  $\mathbb{F}_4$ -codes in Table 12 to  $\mathbb{F}_4 + u\mathbb{F}_4$ , as a result we obtain extremal binary self-dual codes of length 64 as given in Table 13.

Table 13: The  $\mathbb{F}_4 + u\mathbb{F}_4$ -lifts of  $C_i$  and the  $\beta$  values of the binary images

code	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$\beta$ in $W_{64,2}$	$ Aut(C) $	
$M_1$	$C_2$	$(b_1, c_2)$	$(b_1, c_2)$	$(z_2, b_1)$	$(a_2, b_4)$	$(a_2, b_4)$	$(z_2, b_1)$	0	$2^5$
$M_2$	$C_2$	$(b_2, c_2)$	$(b_2, c_2)$	$(z_2, b_1)$	$(a_2, b_4)$	$(a_2, b_4)$	$(z_2, b_1)$	0	$2^6$
$M_3$	$C_3$	$(b_1, c_1)$	$(b_1, c_1)$	$(a_1, b_2)$	$(a_1, c_4)$	$(a_1, c_4)$	$(a_1, b_2)$	4	$2^5$
$M_4$	$C_2$	$(b_1, c_4)$	$(b_1, c_4)$	$(z_4, b_1)$	$(a_3, b_4)$	$(a_3, b_4)$	$(z_4, b_1)$	12	$2^5$
$M_5$	$C_3$	$(b_2, c_2)$	$(b_2, c_2)$	$(a_1, b_3)$	$(a_2, c_4)$	$(a_2, c_4)$	$(a_1, b_3)$	16	$2^5$
$M_6$	$C_1$	$(z_2, a_3)$	$(z_2, a_3)$	$(a_1, b_2)$	$(a_4, c_1)$	$(a_4, c_1)$	$(a_1, b_2)$	20	$2^5$
$M_7$	$C_1$	$(z_2, a_3)$	$(z_2, a_3)$	$(a_1, b_3)$	$(a_3, c_4)$	$(a_3, c_4)$	$(a_1, b_3)$	24	$2^5$
$M_8$	$C_2$	$(b_1, c_2)$	$(b_1, c_2)$	$(z_1, b_2)$	$(a_4, b_2)$	$(a_4, b_2)$	$(z_1, b_2)$	28	$2^5$
$M_9$	$C_3$	$(b_1, c_1)$	$(b_1, c_1)$	$(a_1, b_2)$	$(a_2, c_3)$	$(a_2, c_3)$	$(a_1, b_2)$	32	$2^6$
$M_{10}$	$C_2$	$(b_1, c_4)$	$(b_1, c_4)$	$(z_3, b_2)$	$(a_4, b_3)$	$(a_4, b_3)$	$(z_3, b_2)$	36	$2^5$
$M_{11}$	$C_2$	$(b_1, c_2)$	$(b_1, c_2)$	$(z_4, b_1)$	$(a_1, b_2)$	$(a_1, b_2)$	$(z_4, b_1)$	44	$2^5$
$M_{12}$	$C_2$	$(b_2, c_4)$	$(b_2, c_4)$	$(z_4, b_1)$	$(a_2, b_1)$	$(a_2, b_1)$	$(z_4, b_1)$	48	$2^5$
$M_{13}$	$C_2$	$(b_1, c_3)$	$(b_1, c_3)$	$(z_1, b_2)$	$(a_4, b_2)$	$(a_4, b_2)$	$(z_1, b_2)$	52	$2^5$

## 5 New Extremal Binary Self-Dual Codes of Length 68 from $\mathbb{F}_2 + u\mathbb{F}_2$ Extensions and Neighbors

In the sequel, let  $R$  be a commutative Frobenius ring with identity. Here, we define a well known extension method ([8]) which we then apply to the codes of length 64 tabulated in the previous section, to search for new extremal binary self dual codes with parameters  $[68, 34, 12]_2$ . The weight enumerator of a self-dual  $[68, 34, 12]_2$  code is in one of the following forms ([7]):

$$W_{68,1} = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \dots,$$

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

where  $\beta$  and  $\gamma$  are parameters and  $0 \leq \gamma \leq 0$ . The existence of the codes in  $W_{68,2}$  is known for [14, 5]:

$\gamma = 0, \beta = 0, 7, 11, 14, 17, 21, 22, 28, 33, 35, 42, \dots, 158, 161, 165,$   
 $175, 187, 189, 203, 209, 221, 231, 255, 303$  or  
 $\beta \in \{2m | m = 17, 20, 102, 110, 119, 136, 165 \text{ or } 80 \leq m \leq 99\};$   
 $\gamma = 1, \beta = 49, 51, 53, 55, 57, \dots, 160$  or  
 $\beta \in \{2m | m = 22, 24, \dots, 29, 81, \dots, 99\};$   
 $\gamma = 2, \beta = 65, 69, 71, 73, 75, 77, 79, 81, 141, 159, 166, 167, 168, 169, 171, 206, 208$  or  
 $\beta \in \{2m | 29 \leq m \leq 68, 70 \leq m \leq 100\}$  or  $\beta \in \{2m + 1 | 41 \leq m \leq 69, 71 \leq m \leq 77\};$   
 $\gamma = 3, \beta \in \{2m + 1 | m = 43, 44, 47, \dots, 77, 79, 80, 81, 83, 96\}$  or  
 $\beta \in \{2m | m = 40, \dots, 92, 94, 95, 97, 98, 101, 102\};$   
 $\gamma = 4, \beta = 103, 105, 113, 117, 121, 129, 139, 141, 143, 145, 149, 157, 161$  or  
 $\beta \in \{2m | m = 43, 48, 49, 51, 52, 54, 55, 56, 58, 60, \dots, 90, 92, 97, 98\};$   
 $\gamma = 5$  with  $\beta \in \{m | m = 158, \dots, 169\}$   
 $\gamma = 6$  with  $\beta \in \{2m | m = 69, 77, 78, 79, 81, 88\}$   
 $\gamma = 7$  with  $\beta \in \{7m | m = 14, \dots, 39, 42\}.$

**Theorem 5.1.** ([8]) *Let  $C$  be a self-dual code of length  $n$  over  $R$  and  $G = (r_i)$  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  $X$  be a vector in  $S^n$  with  $\langle X, X \rangle = -1$ . Let  $y_i = \langle r_i, X \rangle$  for  $1 \leq i \leq k$ . 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  $n + 2$ .*

Theorem 5.1 is applied to the  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}$ -images of the codes in tables 2,4,8,10,13. The results are tabulated in Table 14, where  $1 + u$  in  $\mathbb{F}_2 + u\mathbb{F}_2$  is denoted as 3.

We observe that the first 16 columns of  $G$  are linearly independent. Without loss of generality we assume that the first 16 entries of the extension vector  $X$  are 0, which narrows down the search field remarkably from  $4^{32}$  to  $4^{16}$ .

Two binary self-dual codes of length  $2k$  are said to be neighbors if their intersection has dimension  $k - 1$ . Let  $C$  be a binary self-dual code of length  $2k$  and  $x \in \mathbb{F}_2^{2k} - C$  then  $D = \langle \langle x \rangle^\perp \cap C, x \rangle$  is a neighbor of  $C$ . As neighbors of codes in Table 14 we obtain two new codes, which are listed in Table 15. Before applying the method we use the standard form of a generator matrix of  $C$ . Therefore, the first 34 columns are linearly independent. Without loss of generality we assume that the first 34 entries of  $x$  are 0, the last half of  $x$  is given in the table.



Table 14: New codes of length 68 from Theorem 5.1

$D$	$C$	$(x_{17}, x_{18}, \dots, x_{32})$	$c$	$\gamma$	$\beta$ in $W_{68,2}$
$C_{68,1}$	$I_2$	$(u, 0, 0, 3, u, 1, 3, u, 3, 3, 1, 1, 3, 0, 1, 0)$	$u + 1$	0	38
$C_{68,2}$	$K_3$	$(3, 1, 1, 3, u, u, 0, u, 0, 0, 0, 3, 1, 1, 1, 3)$	1	1	38
$C_{68,3}$	$K_3$	$(3, 3, 1, 1, 0, u, 0, u, 0, u, 0, 3, 1, 1, 3, 3)$	1	1	46
$C_{68,4}$	$K_2$	$(u, 1, u, u, 1, 3, 3, 3, u, 1, 1, u, u, 0, 3, 3)$	$u + 1$	2	67
$C_{68,5}$	$K_1$	$(0, 0, 1, 0, 1, 3, u, 3, u, 0, u, 0, 3, 0, 3, 1)$	$u + 1$	3	77
$C_{68,6}$	$K_1$	$(1, 1, 0, 3, 0, u, u, u, 1, 1, 1, 0, 1, 3, 0, 3)$	$u + 1$	3	78
$C_{68,7}$	$I_1$	$(1, 3, 1, 3, 1, 0, 1, 0, 1, 3, 1, 3, u, 1, 0, 0)$	1	3	81
$C_{68,8}$	$K_{23}$	$(0, u, 1, 1, u, 3, 0, 1, 0, 1, 1, 3, u, 1, 3, u)$	$u + 1$	3	179
$C_{68,9}$	$K_3$	$(1, 0, 0, 3, u, 3, u, 3, 1, 3, 3, 3, 1, 1, 1, u)$	1	4	92
$C_{68,10}$	$K_3$	$(u, u, 3, 3, 1, 1, 1, 1, 3, 0, 3, 3, 1, 1, 0, u)$	1	4	94
$C_{68,11}$	$K_4$	$(1, u, 1, 0, u, u, 1, u, 1, 1, 0, u, u, u, 1, 1)$	1	4	119

Table 15: New codes of length 68 as neighbors

$D$	$C$	$x$	$\gamma$	$\beta$
$C_{68,12}$	$C_{68,11}$	$(10101101010001100000011111110000011)$	4	107
$C_{68,13}$	$C_{68,10}$	$(1011111011101111011000100111110111)$	4	115

## 6 Conclusion

In this work, we define new composite constructions from group rings, where the orders of the groups are 4 and 8. The composite constructions, together with an extension method, are used to search for extremal binary self-dual codes of length 68. In particular, we construct the following unknown  $W_{68,2}$  codes:

$$\begin{aligned}
&(\gamma = 0, \beta = \{38\}), \\
&(\gamma = 1, \beta = \{38, 46\}), \\
&(\gamma = 2, \beta = \{67\}), \\
&(\gamma = 3, \beta = \{77, 78, 81, 179\}), \\
&(\gamma = 4, \beta = \{92, 94, 107, 115, 119\}).
\end{aligned}$$

The binary generator matrices of new extremal self-dual codes are available online at [10]. A suggestion for further work would be to consider group rings, where the orders of the groups are 16, 8 and 4. This would lead to more composite constructions. Another suggestion is to work on the theoretical analysis of the composite constructions derived from group rings to see if there are any specific groups of interest from the point of view of group theory.

## References

- [1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, Vol. 24 (1997), 235-265.
- [2] J.H. Conway, N.J.A. Solane, “A new upper bound on the minimal distance of self-dual codes”, *IEEE Trans. Inform. Theory*, Vol. 36, 6, 1319-1333, 1990.
- [3] S.T. Dougherty, “Algebraic Coding Theory over Finite Commutative Rings”, Springer Briefs in Mathematics. Springer, 2017.
- [4] S.T. Dougherty, P. Gaborit, M. Harada, P. Sole, “Type II codes over  $\mathbb{F}_2 + u\mathbb{F}_2$ ”, *IEEE Trans. Inform. Theory*, Vol. 45, 32-45, 1999.
- [5] S.T. Dougherty, J. Gildea, A. Kaya, “Quadruple bordered constructions of self-dual codes from group rings over Frobenius rings”, *Cryptogr. Commun.* (2019). <https://doi.org/10.1007/s12095-019-00380-8>.
- [6] S.T. Dougherty, J. Gildea, R. Taylor and A. Tylyshchak, “group rings, G-codes and constructions of self-dual and formally self-dual codes”, *Des., Codes and Cryptog.*, Vol. 86, no. 9, 2115-2138, 2018.
- [7] S.T. Dougherty, T.A. Gulliver, M. Harada, “Extremal binary self dual codes”, *IEEE Trans. Inform. Theory*, Vol. 43, 2036-2047, 1997.
- [8] S.T. Dougherty, J.-L. Kim, H. Kulosman and H. Liu, “Self-dual codes over commutative Frobenius rings”, *Finite Fields Appl.*, Vol. 16, No. 1, pp. 14-26, 2010.
- [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 Appl.*, Vol. 57, 108-127, 2019.
- [10] S. T. Dougherty, J. Gildea, A. Korban and A. Kaya “Binary generator matrices for extremal binary self-dual codes of length 68”, available online at <http://abidinkaya.wixsite.com/math/adrian1>.
- [11] J. Gildea, A. Kaya, R. Taylor and B. Yildiz, “Constructions for self-dual codes induced from group rings”, *Finite Fields Appl.*, Vol. 51, 71-92, 2018.
- [12] P. Gaborit, V. Pless, P. Sole and O. Atkin, “Type II codes over  $\mathbb{F}_4$ ”, *Finite Fields Appl.*, Vol. 8, 171-183, 2002.
- [13] T. Hurley, “Group Rings and Rings of Matrices”, *Int. Jour. Pure and Appl. Math.*, Vol. 31, no. 3, 319-335, 2006.

- [14] A. Kaya, B. Yildiz, “Various constructions for self-dual codes over rings and new binary self-dual codes”, *Discrete Mathematics*, Vol. 339, Issue 2, 460-469, 2016
- [15] S. Ling, P. Sole, “Type II Codes Over  $\mathbb{F}_4 + u\mathbb{F}_4$ ”, *Europ. J. Combinatorics*, Vol. 22, 983-997, 2001.
- [16] E.M. Rains, “Shadow Bounds for Self-Dual Codes”, *IEEE Trans. Inf. Theory*, Vol. 44, 134-139, 1998.