An Altered Four Circulant Construction for Self-Dual Codes from Group Rings and New Extremal Binary Self-dual Codes I

Joe Gildea,
University of Chester
Department of Mathematics
Chester, UK

Abidin Kaya
Department of Mathematics Education
Sampoerna University, 12780, Jakarta, Indonesia

Bahattin Yildiz *
Department of Mathematics & Statistics
Northern Arizona University
Flagstaff, AZ 86001, USA
bahattin.yildiz@nau.edu

Abstract

We introduce an altered version of the four circulant construction over group rings for self-dual codes. We consider this construction over the binary field, the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$; using groups of order 4 and 8. Through these constructions and their extensions, we find binary self-dual codes of lengths 16, 32, 48, 64 and 68, many of which are extremal. In particular, we find forty new extremal binary self-dual codes of length 68, including twelve new codes with $\gamma = 5$ in $W_{68,2}$, which is the first instance of such a γ value in the literature.

Key Words: Group rings; self-dual codes; codes over rings; extremal codes; four circulant constructions.

*Corresponding Author

1 Introduction

Self-dual codes are one of the most well-known families of codes and as such have received an extensive interest in the coding theory community. The connection of self-dual codes to such combinatorial objects as designs and association schemes as well as their connection to lattices, invariant theory, cryptography have made them the focus of many researchers. The classification of extremal binary self-dual codes, and the discovery of extremal binary self-dual codes with new weight enumerators are active areas of research on self-dual codes.

There have been some well known construction methods for self-dual codes. The so-called pure double circulant or simply double circulant construction was first introduced in the 1960's ([4, 24]). It is a classical technique for producing self-dual codes and it considers generator matrices of the form $(I_n|A)$ where A is a circulant matrix satisfying $AA^T = -I_n$. This method has been used extensively to construct self-dual codes since its inception ([17, 18, 19]). In [16], this method was extended to consider matrices A that arise from group rings. Group rings have been used in the literature to construct self-dual codes from different angles. In [1], an ideal of the group algebra $\mathbb{F}_2S_4$ was used to construct the well-known binary extended Golay code where S_4 is the symmetric group on 4 elements. In [21], an isomorphism between a group ring and a certain subring of the $n \times n$ matrices over the ring was established. This isomorphism was used to produce self-dual codes in [22, 28]. In [27], McLoughlin found that the $[48, 24, 12]$ Type II code is a dihedral code.

Recently, in [9], the idea of using group ring elements to construct codes was extended to any group G and consequently, G-codes were defined as codes that are ideals in the group ring RG, where R is a finite Frobenius ring. In [16], a connection between certain group ring elements called unitary units and self-dual codes was established and the connection was used to produce many self-dual codes.

The double circulant matrix construction is one of the few well-known constructions that use the idea of circulant matrices to reduce the search field. The bordered double circulant construction is a variant while, the so-called four-circulant construction is a different variation of the same idea, which was first introduced in [2]: Let G be the matrix

$$\left[\begin{array}{c|cc} I_{2n} & A & B \\ & -B^T & A^T \end{array}\right]$$

where A and B are circulant matrices. Then the code generated by G over $\mathbb{F}_p$ is self-dual if and only if $AA^T + BB^T = -I_n$. Note that when the alphabet is a ring of characteristic 2, then the matrix and the conditions can be written in an alternative form, where the negative signs disappear.

In this work, we will consider constructing self dual codes from the following variation of the four-circulant matrix. Consider the matrix

$$\left[\begin{array}{c|cc} I_{2n} & A & B \\ & B^T & A^T \end{array}\right]$$

where both A and B are matrices that arise from group rings. Depending on the groups, the matrices will usually not be circulant matrices, which is a variation from the usual four-circulant construction. Under this construction, we establish the link between units/non-units in the group ring and corresponding self-dual codes. Using this connection for some particular examples of groups over the field $\mathbb{F}_2$ and the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ we are able to construct many extremal binary self-dual codes of different lengths. In particular we construct forty new binary extremal self-dual codes of length 68. Of these forty, twelve have parameters $\gamma = 5$ in $W_{68,2}$. These are the first examples of codes with such a γ value in the literature.

The rest of the work is organized as follows. In section 2, we give the necessary background on codes, the alphabets we use and the group rings. In section 3, we give the constructions and the theoretical results about the group ring elements that lead to self-dual codes. In sections 4 and 5, we apply the construction methods to produce the numerical results, using MAGMA ([25]). The paper ends with concluding remarks and possible further research directions.

2 Preliminaries

In this section, we will define self-dual codes over Frobenius rings of characteristic 2. We will recall some of the properties of the family of rings called R_k and the ring $\mathbb{F}_4 + u\mathbb{F}_4$. This section concludes with an introduction to group rings and an established isomorphism between a group ring and a certain subring of the $n \times n$ matrices over a ring.

2.1 Self-Dual codes

Throughout this work, all rings are assumed to be commutative, finite, Frobenius rings with a multiplicative identity.

A code over a finite commutative ring R is said to be any subset C of R^n. When the code is a submodule of the ambient space then the code is said to be linear. To the ambient space, we attach the usual inner-product, specifically $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$. The orthogonal with respect to this inner-product is defined as $C^\perp = \{\mathbf{w} \mid \mathbf{w} \in R^n,\ [\mathbf{w}, \mathbf{w}] = 0, \forall \mathbf{v} \in C\}$. Since the ring is Frobenius we have that for all linear codes over R, $|C||C^\perp| = |R|^n$. If a code satisfies $C = C^\perp$ then the code C is said to be self-dual. If $C \subseteq C^\perp$ then the code is said to be self-orthogonal.

For binary codes, a self-dual code where all weights divisible by 4, is said to be Type II and the code is said to be Type I otherwise. 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, the bounds on the minimum distances for self-dual codes are ([29]):

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

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 that meet these bounds are called *extremal*. In section 4, we will construct extremal binary self-dual codes. The weight enumerator $W(y)$ of a code is given by $W(y) = \sum_{i=0}^{n} A_i y$ where A_i is the number of codewords of weight i. The possible weight enumerators for extremal Type I codes of lengths 66 - 100 were determined in [11].

2.2 R_k family of rings

One of the The alphabets that we will use in this work, namely $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ is a special member of a more general family of rings characteristic 2 (R_k), which were defined in [13] and [14]. For $k \geq 1$, define $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$ which can also be defined recursively as $R_k = R_{k-1}[u_k]/\langle u_k^2 = 0, u_k u_j = u_j u_k \rangle = R_{k-1} + u_k R_{k-1}$. For any subset $A \subseteq \{1, 2, \ldots, k\}$ we will fix

$$u_A := \prod_{i \in A} u_i$$

with the convention that $u_\emptyset = 1$. Then any element of R_k can be represented as

$$\sum_{A \subseteq \{1,\ldots,k\}} c_A u_A$$

where $c_A \in \mathbb{F}_2$. An advantage of representing elements with this notation is that we can easily observe that

$$u_A u_B = \begin{cases} 0 & \text{if } A \cap B \neq \emptyset \\ u_{A \cup B} & \text{if } A \cap B = \emptyset \end{cases}.$$

This leads to

$$\left(\sum_A c_A u_A \right) \left(\sum_B d_B u_B \right) = \sum_{A,B \subseteq \{1,\ldots,k\}, A \cap B = \emptyset} c_A d_B u_{A \cup B}.$$

It is shown in [13] that the ring family R_k is a commutative ring with $|R_k| = 2^{(2^k)}$. A Gray map from R_k to $\mathbb{F}_2^{2^k}$ was defined inductively starting with the map on R_1: $\phi_1(a + bu_1) = (b, a + b)$. We recall that $c \in R_k$, c can be written as $c = a + bu_{k-1}, a, b \in R_{k-1}$. Then

$$\phi_k(c) = (\phi_{k-1}(b), \phi_{k-1}(a + b)).$$

The map ϕ_k is a distance preserving map and the following is shown in [14]. Let C be a self-dual code over R_k, it is well known that $\phi_k(R_k)$ is a binary self-dual code of length $2^k n$ ([14]). The next result which was introduced in [12] proves to be useful when extending codes over R_1:

Theorem 2.1. *([12]) Let $\mathcal{C}$ be a self-dual code over R_k of length n and $G = (r_i)$ be a $j \times n$ generator matrix for $\mathcal{C}$, where r_i is the i-th row of G, $1 \leq i \leq k$. Let c be a unit in R_k and X be a vector in R_k^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 $\mathcal{C}'$ over R_k of length $n+2$.

2.3 The ring $\mathbb{F}_4 + u\mathbb{F}_4$

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 $\mathbb{F}_4 + u\mathbb{F}_4$ is defined via $u^2 = 0$. Note that $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ 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 $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$.

A linear code C of length n over $\mathbb{F}_4 + u\mathbb{F}_4$ is an $(\mathbb{F}_4 + u\mathbb{F}_4)$-submodule of $(\mathbb{F}_4 + u\mathbb{F}_4)^n$. In [15] and [7] the following Gray maps were introduced;

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

Those were generalized to the following maps in [26];

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

These maps preserve orthogonality in the corresponding alphabets. The binary images $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ are equivalent. The Lee weight of an element is defined to be the Hamming weight of its binary image.

Let C be a self-orthogonal code over $\mathbb{F}_4 + u\mathbb{F}_4$. It is shown in ([26]) that $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ are also self-orthogonal. It is also shown that if 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. Additionally, they prove that 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 $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.

To shorten the notation when using in the tables in subsequent sections, we use the ordered basis $\{u\omega, \omega, u, 1\}$ to express the elements of $\mathbb{F}_4 + u\mathbb{F}_4$ in hexadecimals. For instance, $1 + u\omega$ corresponds to 1001, which is represented by the hexadecimal 9, while $1 + \omega + u\omega$ corresponds to 1101, which is represented by D.

2.4 Certain Matrices and Group Rings

Before we introduce group rings, we need to define a circulant matrix and a block circulant. For further details on circulant matrices see [6]. Note that $\text{circ}(a_1, a_2, \ldots, a_n)$ means the circulant matrix whose first row is $(a_1, a_2, \ldots, a_n)$ and $\text{CIRC}(A_1, A_2, \ldots, A_n)$ represents a block circulant matrix whose first row of block matrices are $A_1, A_2, \ldots, A_n$.

Let G be a finite group or 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

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

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

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

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

The following construction of a matrix was first given by Hurley in [21]. Let R be a finite commutative Frobenius ring of characteristic 2 and let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be $\sigma(v) = (\alpha_{g_i^{-1} g_j})$ where $i, j \in \{1, 2, \cdots, n\}$.

We note that the elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are the elements of the group G in a given order. We will now describe $\sigma(v)$ for the group ring RG where $G = C_{4n}$. Let $G = \langle x \mid x^{4n} = 1 \rangle \cong C_{4n}$. If $v = \sum_{i=0}^{2n-1} \alpha_{i+j+1}(\alpha_{i+1} x^{2i} + \alpha_{i+2n+1} x^{2i+1}) \in RC_{4n}$, then

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

where $A = circ(\alpha_1, \ldots, \alpha_{2n})$, $B = circ(\alpha_{2n+1}, \ldots, \alpha_{4n})$, $B' = circ(\alpha_{4n}, \alpha_{2n+1}, \ldots, \alpha_{4n-1})$ and $\alpha_i \in R$.

3 The Construction

Let $v \in RG$ where R is a finite commutative Frobenius ring of characteristic 2 and G is a finite group of order $4n$. Define the following matrix:

$$M(\sigma) = \left[\begin{array}{c|c|c} & \sigma(v) & \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix} \\ I_{8n} & & \\ & \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T & \sigma(v)^T \end{array}\right]$$

Let C_σ be a code that is generated by the matrix $M(\sigma)$. Then, the code C_σ has length $16n$. We will now provide conditions when the above construction produces self-dual codes. We also provide a connection (when using this construction) between self-dual codes and units and non-units in a group ring.

Theorem 3.1. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite group of order $4n$. If $I + \sigma(v)\sigma(v)^T + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T = 0$ and $\sigma(v)$ commutes with $\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}$ then C_σ is a self-dual code of length $16n$.*

Proof. Clearly, C_σ has free rank $8n$ as the left hand side of the generator matrix is the $8n$ by $8n$ identity matrix. Now,

$$\begin{aligned} M(\sigma)M(\sigma)^T &= \begin{pmatrix} I + \sigma(v)\sigma(v)^T + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T & \sigma(v)\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix} + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}\sigma(v) \\ \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T\sigma(v)^T + \sigma(v)^T\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T & I + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix} + \sigma(v)^T\sigma(v) \end{pmatrix} \\ &= \begin{pmatrix} I + \sigma(vv^*) + \begin{pmatrix} A_1A_1^T + A_2A_2^T & A_1(A_2'^T + A_2A_1^T \\ A_2'A_1^T + A_1A_2^T & A_2'(A_2'^T + A_1A_1^T \end{pmatrix} & \sigma(v)\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix} + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}\sigma(v) \\ \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T\sigma(v)^T + \sigma(v)^T\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T & I + \begin{pmatrix} A_1^TA_1 + (A_2'^TA_2' & A_1^TA_2 + (A_2'^TA_1 \\ A_2^TA_1 + A_1^TA_2' & A_2^TA_2 + A_1^TA_1 \end{pmatrix} + \sigma(v^*v) \end{pmatrix}. \end{aligned}$$

If $I + \sigma(v)\sigma(v)^T + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T = 0$ and $\sigma(v)$ commutes with $\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}$ then C_σ is self-orthogonal and so C_σ is self-dual.

Corollary 3.2. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order $4n$. Let C_σ be self-dual. If $A_1A_1^T + A_2A_2^T = 0$, $A_1(A_2')^T + A_2A_1^T = 0$ and $A_2'(A_2')^T + A_1A_1^T = 0$, then $v \in RG$ is a unitary unit.*

Proof. If C_σ is self-dual, clearly $\sigma(vv^*) = I + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T$. If $A_1A_1^T + A_2A_2^T = 0$, $A_1(A_2')^T + A_2A_1^T = 0$ and $A_2'(A_2')^T + A_1A_1^T = 0$, then $\sigma(vv^*) = I$. Therefore $vv^* = 1$ and v is unitary unit.

Corollary 3.3. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order $4n$. Let C_σ be self-dual. If $A_1A_1^T + A_2A_2^T = I$, $A_1(A_2')^T + A_2A_1^T = 0$ and $A_2'(A_2')^T + A_1A_1^T = I$, then $v \in RG$ is a non-unit.*

Proof. If C_σ is self-dual, clearly $\sigma(vv^*) = I + \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix} \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}^T$. If $A_1A_1^T + A_2A_2^T = I$, $A_1(A_2')^T + A_2A_1^T = 0$ and $A_2'(A_2')^T + A_1A_1^T = I$, then $\sigma(vv^*) = 0$. Now, vv^* is a non-unit by Corollary 3 in [21]. Therefore, $v \in RG$ is a non-unit.

4 Extremal binary self-dual codes from the constructions

In this section, we will present the results obtained using the construction described in section 3, to construct self-dual codes for certain groups of order 4 and 8. We finish with constructing new extremal self-dual codes of length 68.

4.1 Construction coming from C_4

Here we present the results for the above construction using the group C_4. We construct self-dual codes of length 64 by considering this construction over $\mathbb{F}_4 + u\mathbb{F}_4$. Note that $(\alpha_1, \ldots, \alpha_{4n})$ represents the first row of the image of $\sigma(v)$ (for a given group ring RG) and $(a_1, \ldots, a_{4n})$ represents the first row of the matrix $\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}$.

We recall that the possible weight enumerators for a self-dual Type I $[64, 32, 12]$-code is given in [5, 11] as:

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

With the most updated information, the existence of codes is known for β =14, 18, 22, 25, 29, 32, 35, 36, 39, 44, 46, 53, 59, 60, 64 and 74 in $W_{64,1}$ and for β =0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, ..., 25, 28, 19, 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 apply the construction C_4 over the ring $\mathbb{F}_4 + u\mathbb{F}_4$ to generate self-dual codes of length 16, whose Gray images are extremal binary self-dual codes of length 64. The codes in the following table all have weight enumerators in $W_{64,2}$.

Table 1: Extremal binary self-dual codes of length 64 from self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$ of length 16 via C_4

$\mathcal{C}_i$	$(\alpha_1, \ldots, \alpha_4)$	$(a_1, \ldots, a_4)$	$\lvert Aut(C)\rvert$	β	$\mathcal{C}_i$	$(\alpha_1, \ldots, \alpha_4)$	$(a_1, \ldots, a_4)$	$\lvert Aut(C)\rvert$	β
1	$(0,1,A,9)$	$(2,4,3,4)$	2^4	0	2	$(0,9,4,F)$	$(2,4,2,5)$	2^5	0
3	$(2,1,2,1)$	$(0,6,9,4)$	2^6	0	4	$(0,1,A,9)$	$(8,6,B,6)$	2^4	4
5	$(A,9,A,9)$	$(0,6,B,6)$	2^5	4	6	$(0,2,0,6)$	$(8,7,1,B)$	2^4	8
7	$(0,8,0,4)$	$(8,7,9,B)$	2^5	8	8	$(0,1,2,9)$	$(8,6,9,6)$	2^4	12
9	$(0,9,0,9)$	$(8,6,B,C)$	2^5	12	10	$(0,2,A,6)$	$(8,5,1,B)$	2^4	16
11	$(A,9,A,9)$	$(2,4,3,E)$	2^5	16	12	$(0,9,2,1)$	$(A,6,1,6)$	2^4	20
13	$(2,9,2,9)$	$(A,4,9,E)$	2^5	20	14	$(0,1,0,9)$	$(A,6,9,4)$	2^4	24
15	$(2,9,2,9)$	$(1,C,9,F)$	2^5	24	16	$(0,9,8,9)$	$(2,6,1,6)$	2^4	28
17	$(0,6,9,E)$	$(4,7,C,D)$	2^5	28	18	$(2,9,4,7)$	$(9,4,3,F)$	2^4	32
19	$(A,9,8,9)$	$(2,4,9,E)$	2^5	32	20	$(0,9,A,9)$	$(0,6,1,4)$	2^4	36
21	$(0,9,0,9)$	$(A,4,9,E)$	2^5	36	22	$(0,8,2,4)$	$(8,7,1,3)$	2^5	40
23	$(2,4,9,4)$	$(6,5,6,5)$	2^5	44	24	$(A,1,6,5)$	$(0,4,0,7)$	$2^4 \cdot 3$	48
25	$(8,1,8,1)$	$(0,6,9,4)$	2^5	48	26	$(A,1,A,1)$	$(A,1,A,1)$	2^5	52

4.2 Construction coming from C_8

Here we present the results for the above construction using $G = C_8$. We construct self-dual codes of length 64 by considering this construction over $\mathbb{F}_2 + u\mathbb{F}_2$. Again, $(\alpha_1, \ldots, \alpha_{4n})$ represents the first row of the image of $\sigma(v)$ (for a given group ring RG) and $(a_1, \ldots, a_{4n})$ represents the first row of the matrix $\begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}$. We replace 3 with $u+1$ to save space.

Table 2: Type I Extremal binary self-dual codes of length 64 from self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length 32 via C_8.

$\mathcal{D}_i$	$(\alpha_1, \ldots, \alpha_8)$	$(a_1, \ldots, a_8)$	$\lvert Aut(C)\rvert$	$W_{64,2}$	$\mathcal{D}_i$	$(\alpha_1, \ldots, \alpha_8)$	$(a_1, \ldots, a_8)$	$\lvert Aut(C)\rvert$	$W_{64,2}$
1	$(u,u,0,1,0,1,u,3)$	$(u,u,1,1,u,u,3,1)$	2^5	0	2	$(u,0,0,u,u,u,1,3)$	$(u,u,1,1,u,1,1,3)$	2^5	16
3	$(u,u,u,0,u,u,1,3)$	$(u,0,1,3,u,1,1,3)$	2^6	16	4	$(0,0,0,u,0,0,1,3)$	$(u,0,1,3,u,1,1,3)$	2^7	16
5	$(u,0,u,u,u,0,1,1)$	$(u,0,1,3,0,1,1,3)$	2^5	32	6	$(0,0,0,u,u,0,1,1)$	$(u,0,1,3,0,1,3,3)$	2^5	48
7	$(u,0,u,u,0,0,1,3)$	$(u,0,1,3,u,1,3,3)$	2^7	80					

5 New Codes of length 68

In this section, we construct forty new extremal self-dual codes of length 68 by extending certain previously constructed codes of length 64 (using Theorem 2.1) from Tables 1 & 2. In particular we construct the first examples of codes with $\gamma = 5$ in $W_{68,2}$.

5.1 New Codes of length 68 from $(\mathbb{F}_4 + u\mathbb{F}_4)C_4$

The possible weight enumerator of an extremal binary self-dual $[68, 34, 12]$-code is in one of the following forms by [11, 3, 20, 10]:

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

where $0 \leq \gamma \leq 9$. Recently, Yankov et al. constructed the first examples of codes with a weight enumerator for $\gamma = 7$ in $W_{68,2}$ ([30]). In [10] and [8], more unknown $W_{68,2}$ codes were constructed. Together with these, the existence of the codes in $W_{68,2}$ is known for;

γ = 0, β = 0, 7, 11, 14, 17, 21, 22, 28, 33, 35, 42, 44, ..., 158,159, 161, 163, 165, 175, 187, 189, 203, 209, 221, 231, 255, 303 or

$\beta \in \{2m | m = 17, 20, 102, 110, 119, 136, 165 \text{ or } 80 \leq m \leq 99\}$;

γ = 1, β = 49,51,53,55, 57, 59, ..., 160,161,163,165,167,169,171 or

$\beta \in \{2m | m = 22,24, \ldots, 29, 81, \ldots, 90, 92, \ldots, 96\}$;

γ = 2, β = 58,65,69,71,73,75,77,79,81,157,159, 206, 208 or $\beta \in \{2m | 30 \leq m \leq 100\}$ or

$\beta \in \{2m + 1 | 41 \leq m \leq 77\}$;

γ = 3, β = 87,89,95,97,99,101,103,105,107,109,111,113,115,117,119,121,123,125,127,129, 131,133, 135,137, 139, 141, 143, 145,147,149,151,153, 155, 159, 161,193 or

$\beta \in \{2m\,| m = 41, \ldots, 92, 94, 95, 97, 98, 101, 102\}$;

γ = 4, β = 129, 139, 141, 143, 145, 149, 157, 161 or

$\beta \in \{2m\,| m = 43, 48, 49,50, 51, 52, 54, 55, 56, 58, 60, \ldots, 78,79, 80,81,85, 87, 97, 98\}$;

γ = 6 with $\beta \in \{2m | m = 69, 77, 78, 79, 81, 88\}$

γ = 7 with $\beta \in \{7m | m = 14, \ldots, 39, 42\}$.

Recall that the previously constructed codes of length 64 (from Table 1) are codes over $\mathbb{F}_4 + u\mathbb{F}_4$. In order to apply Theorem 2.1, it requires the codes to be over $\mathbb{F}_2 + u\mathbb{F}_2$. Before considering extensions of these codes, we need to use the Gray map $\psi_{\mathbb{F}_4 + u\mathbb{F}_4}$ to convert them to a code over $\mathbb{F}_2 + u\mathbb{F}_2$. The following table details the new extremal self-dual codes of length 68. For each new code constructed we note the original code of length 64 from Table 1, the unit $c \in \mathbb{F}_2 + u\mathbb{F}_2$, the vector X required to apply Theorem 2.1. Again, we replace $u + 1$ with 3 to save space.

Table 3: Type I Extremal Self-dual codes of length 68 as extensions.

$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β	$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β
$\mathcal{C}_{68,1}$	1	1	$(u301013311u33uu03030303u31uuuu00)$	**4**	**97**	$\mathcal{C}_{68,2}$	1	1	$(u3u1u01030u33333u0uu1u303u1u11uu)$	**4**	**99**
$\mathcal{C}_{68,3}$	1	1	$(013u00uu330330u3330000uu1u3011u0)$	**4**	**101**	$\mathcal{C}_{68,4}$	1	3	$(303u003131031u3u3100u331113u3u3u)$	**4**	**103**
$\mathcal{C}_{68,5}$	1	3	$(1u1u0u3u3uu1uu003331000u1313uuuu)$	**4**	**105**	$\mathcal{C}_{68,6}$	1	1	$(10u1110001010uu1uu30u11131u3313u)$	**4**	**111**
$\mathcal{C}_{68,7}$	1	3	$(033u13u03303013u31111130u111103u)$	**4**	**117**	$\mathcal{C}_{68,8}$	1	1	$(00301u333u0u1111010331u03u1u303u)$	**4**	**121**
$\mathcal{C}_{68,9}$	1	1	$(u1u0u33u3u0u0113uu03130u33110311)$	**4**	**123**	$\mathcal{C}_{68,10}$	1	1	$(333300u013uu133uu3u1130000113100)$	**4**	**125**
$\mathcal{C}_{68,11}$	3	3	$(u33u3u0u10100u1000u10uu133031111)$	**3**	**80**	$\mathcal{C}_{68,12}$	4	1	$(01uu1313u3003u0u3u1001u1u1u1u330)$	**3**	**93**
$\mathcal{C}_{68,13}$	12	1	$(31u1u3u011u31013u10003uu311u0103)$	**4**	**137**	$\mathcal{C}_{68,14}$	14	1	$(3uu30u333u3u0300uu33u030u0110uu3)$	**5**	**164**
$\mathcal{C}_{68,15}$	20	3	$(3u0311u0uuu30311uu0313u110u13013)$	**3**	**167**	$\mathcal{C}_{68,16}$	21	1	$(130u133uu3u1u1u31001u1101311u13u)$	**4**	**170**
$\mathcal{C}_{68,17}$	22	3	$(u03101u313u3u3100300u111u00u1133)$	**4**	**164**	$\mathcal{C}_{68,18}$	22	1	$(13u01300011301u10300u330310001uu)$	**4**	**172**
$\mathcal{C}_{68,19}$	22	1	$(331u3u333u00310uuuuu01u110u30130)$	**4**	**176**	$\mathcal{C}_{68,20}$	22	1	$(u30uu1331333u3113103uu000101331u)$	**4**	**178**
$\mathcal{C}_{68,21}$	22	3	$(1u1110u03301133330u113330311u01u)$	**4**	**180**	$\mathcal{C}_{68,22}$	22	1	$(33uu3303uu1u1u310u11u31u30uu0uu1)$	**4**	**182**
$\mathcal{C}_{68,23}$	22	1	$(133u33301u01u01u3uu1111001u0u1u3)$	**4**	**184**						

5.2 New Codes of length 68 from R_1C_8

We now consider extensions of the previously constructed codes of length 64 from Table 2. The following table records newly constructed extremal self-dual codes of length 68. Again, we note the original code of length 64 from Table 2, the unit $c \in \mathbb{F}_2 + u\mathbb{F}_2$, the vector X required to apply Theorem 2.1. Recall that we replace $u+1$ with 3 to save space.

Table 4: Type I Extremal Self-dual code of length 68 from C_8 over R_1.

$\mathcal{C}_{68,i}$	$\mathcal{D}_i$	c	X	γ	β	$\mathcal{C}_{68,i}$	$\mathcal{D}_i$	c	X	γ	β
$\mathcal{C}_{68,24}$	1	3	$(310013u13uu13uu1u1u33103u0u3103u)$	**0**	**41**	$\mathcal{C}_{68,25}$	1	1	$(101u303u0300001u133u13311u3uu000)$	**0**	**43**
$\mathcal{C}_{68,26}$	7	3	$(3u011301uuuuu3130311u00u3u111031)$	**1**	**182**	$\mathcal{C}_{68,27}$	7	3	$(0030000u0011033103300u0uu3133131)$	**1**	**194**
$\mathcal{C}_{68,28}$	7	1	$(30130u00uu1u110011u110u133010u01)$	**1**	**196**	$\mathcal{C}_{68,29}$	7	1	$(3100131u10uu1303uuu101u3310u0311)$	**1**	**198**

5.3 New self-dual codes of length 68 from Neighboring construction

Two self-dual binary codes of dimension k are said to be neighbors if their intersection has dimension $k-1$. Let $C = \mathcal{C}_{68,14}$ be the code with weight enumerator for $\gamma = 5$, $\beta = 164$ in Table 3 In order to reduce down the search field without loss of generality, we consider the standard form of the generator matrix of C. Let $x \in \mathbb{F}_2^n - C$ then $D = \left\langle \langle x \rangle^{\perp} \cap C, x \right\rangle$ is a neighbour of C. The first 34 entries of x are set to be 0, the rest of the vectors are listed in Table 5. As neighbors of C we obtain eleven new codes with weight enumerator $\gamma = 5$ in $W_{68,2}$, which are listed in Table 5.

Table 5: New codes of length 68 with $\gamma = 5$ as neighbors of $\mathcal{C}_{68,14}$

$\mathcal{N}_{68,i}$	$(x_{35}, x_{36}, ..., x_{68})$	β	$\mathcal{N}_{68,i}$	$(x_{35}, x_{36}, ..., x_{68})$	β
$\mathcal{N}_{68,1}$	(01101010100101000110010101110101 00)	**158**	$\mathcal{N}_{68,2}$	(01111100100000100001100100011000 11)	**159**
$\mathcal{N}_{68,3}$	(00110010100001110111010111000010 10)	**160**	$\mathcal{N}_{68,4}$	(00110010011110111100001000100010 11)	**161**
$\mathcal{N}_{68,5}$	(11110101001111001010100101011101)	**162**	$\mathcal{N}_{68,6}$	(10110001100111100010000010111011 00)	**163**
$\mathcal{N}_{68,7}$	(01000001011010101100111001001010 11)	**165**	$\mathcal{N}_{68,8}$	(00111011101101001011010111001010 00)	**166**
$\mathcal{N}_{68,9}$	(01010000001100001000111111011010 00)	**167**	$\mathcal{N}_{68,10}$	(00101001010000101110110100000111 11)	**168**
$\mathcal{N}_{68,11}$	(10001111100011101010011000111010 10)	**169**			

6 Conclusion

In this work, we introduced a new construction for constructing self-dual codes using group rings. We provided certain conditions when this construction produces self-dual codes and we established a link between units/non-units and self-dual codes. We demonstrated the relevance of this new construction by constructing many extremal binary self-dual codes, including new extremal self-dual codes of length 68. All the new codes have an automorphism group of order 2. In particular, we were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{68,2}$, including the first instances of $\gamma = 5$ in the literature:

$$
\begin{aligned}
&(\gamma = 0, \quad \beta = \{41, 43\}),\\
&(\gamma = 1, \quad \beta = \{182, 194, 196, 198\}),\\
&(\gamma = 3, \quad \beta = \{80, 93, 167\}),\\
&(\gamma = 4, \quad \beta = \{97, 99, 101, 103, 105, 111, 117, 121, 123, 125, 137, 164, 170, 172, 176,\\
&\qquad\qquad 178, 180, 182, 184\}) \text{ and}\\
&(\gamma = 5, \quad \beta = \{158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169\}).
\end{aligned}
$$

Because of the computational limitations that the construction method brings, we were able to consider the groups of order 4 and 8. However, a look at larger groups may lead to further results with a higher computational power. Another direction of research could be considering other families of rings.

References

[1] F. Bernhardt, P. Landrock, and O. Manz, "The extended Golay codes considered as ideals", *J. Combin. Theory Ser. A*, Vol. 55, no. 2, pp. 235–246, 1990.

[2] K. Betsumiya, S. Georgiou, T. A. Gulliver, M. Harada and C. Koukouvinos, "On self-dual codes over some prime fields ", *Discrete Math.*, vol. 262, no. 1–3, pp. 37–58, 2003.

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

[4] C.L. Chen, W.W. Peterson and E.J. Weldon, "Some results on quasi-cyclic codes", *Information and Control*, vol. 15, pp. 407–423, 1969.

[5] J.H. Conway and N.J.A. Sloane, "A new upper bound on the minimal distance of self-dual codes", *IEEE Trans. Inform. Theory*, vol. 36, no. 6, pp. 1319–1333, 1990.

[6] P.J. Davis, "Circulant Matrices", Chelsea Publishing New York, 1979.

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

[8] S.T. Dougherty, J. Gildea and A. Kaya, "Quadruple Bordered Constructions of Self-Dual Codes from Group Rings", **submittted**.

[9] S.T. Dougherty, J. Gildea, R. Taylor and A. Tylshchak, "Group rings, G-codes and constructions of self-dual and formally self-dual codes", *Des. Codes Cryptogr.*, vol. 86, no. 9, pp. 2115–2138, 2018.

[10] S.T. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylshchak, and B. Yildiz, "Bordered Constructions of Self-Dual Codes from Group Rings", *Finite Fields Appl.*, vol. 57, pp. 108–127, 2019.

[11] S.T. Dougherty, M. Harada, and T.A. Gulliver, "Extremal Binary Self-dual Codes", *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 2036–2047, 1997.

[12] S.T.Dougherty, J. -L.Kim, H.Kulosman and H. Liu, "Self-dual codes over commutative Frobenius rings", *Finite Fields Appl.*, vol. 16, pp. 14–26, 2010.

[13] S.T. Dougherty, B. Yildiz and S. Karadeniz, "Codes over R_k, Gray maps and their Binary Images", *Finite Fields Appl.*, vol. 17, no. 3, pp. 205–219, 2011.

[14] S.T. Dougherty, B. Yildiz and S. Karadeniz, "Self-dual Codes over R_k and Binary Self-Dual Codes", *European Journal of Pure and Applied Mathematics*, vol. 6, no. 1, pp. 89–106, 2013.

[15] P. Gaborit, V. Pless, P. Sole and O. Atkin, "Type II codes over $\mathbb{F}_4$", *Finite Fields Appl.*, vol. 8, no. 2, pp. 171–183, 2002.

[16] J. Gildea, A. Kaya, R. Taylor and B. Yildiz, "Constructions for self-dual codes induced from group rings", *Finite Fields Appl.*, vol. 51, pp. 71–92, 2018).

[17] T.A. Gulliver and M. Harada, "Weight enumerators of double circulant codes and new extremal self-dual codes", *Des. Codes Cryptogr.*, vol. 11, no. 2, pp. 141–150, 1997.

[18] T.A. Gulliver and M. Harada, "Classification of extremal double circulant formally self-dual even codes", *Des. Codes Cryptogr.*, vol. 11, no. 1, pp. 25–35, 1997.

[19] T.A. Gulliver and M. Harada, "On double circulant doubly even self-dual $[72, 36, 12]$ codes and their neighbors", *Australas. J. Combin.*, vol. 40, pp. 137–144, 2008.

[20] M. Harada and A. Munemasa, "Some restrictions on weight enumerators of singly even self-dual codes", *IEEE Trans. Inform. Theory*, vol. 52, pp. 1266–1269, 2006.

[21] T. Hurley, "Group Rings and Rings of Matrices", *Int. Jour. Pure and Appl. Math.*, vol. 31, no. 3, pp. 319–335, 2006.

[22] T. Hurley, "Self-dual, dual-containing and related quantum codes from group rings", arXiv:0711.3983, 2007.

[23] A. Kaya, B. Yildiz and A. Pasa, "New extremal binary self-dual codes from a modified four circulant construction", *Discrete Math.*, vol. 339, no.3, pp. 1086–1094, 2016.

[24] M. Karlin, "New binary coding results by circulants", *IEEE Trans. Inform. Theory*, vol. 15, pp. 81–92, 1969.

[25] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), "Handbook of Magma functions", Edition 2.16 ,2010.

[26] S. Ling and P. Sole, "Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$", *Europ. J. Combinatorics*, vol. 22, pp. 983–997, 2001.

[27] I. McLoughlin, "A group ring construction of the $[48, 24, 12]$ Type II linear block code", *Des. Codes Cryptogr.*, vol. 63, no. 1, pp. 29–41, 2012.

[28] I. McLoughlin and T. Hurley, "A group ring construction of the extended binary Golay code", *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4381–4383, 2008.

[29] E.M. Rains, "Shadow Bounds for Self Dual Codes", *IEEE Trans. Inform. Theory*, vol. 44, pp.134–139, 1998.

[30] N. Yankov, M. Ivanova, M.H. Lee, "Self-dual codes with an automorphism of order 7 and s-extremal codes of length 68", *Finite Fields Appl.*, vol. 51, no. 5, pp. 17–30, 2018.