Quadruple Bordered Constructions of Self-Dual Codes from Group Rings

Steven T. Dougherty *

Department of Mathematics University of Scranton

Scranton, PA 18510

USA

Joseph Gildea †,

University of Chester

Department of Mathematics

Chester, UK

Abidin Kaya ‡

Sampoerna Academy, L'Avenue Campus

12780, Jakarta, Indonesia

April 2, 2019

Abstract

In this paper, we introduce a new bordered construction for self-dual codes using group rings. We consider constructions over the binary field, the family of rings R_k and the ring $\mathbb{F}_4 + u\mathbb{F}_4$. We use groups of order 4, 12 and 20. We construct some extremal self-dual codes and non-extremal self-dual codes of length 16, 32, 48, 64 and 68. In particular, we construct 33 new extremal self-dual codes of length 68.

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

*steven.dougherty@scranton.edu,prof.steven.dougherty@gmail.com

†J.Gildea@chester.ac.uk

‡abidinkaya@gmail.com

1 Introduction

Self-dual codes are one of the most widely studied families of codes. There are many reasons for this including their connection to designs and lattices as well as their importance as codes. Numerous techniques have been given to find self-dual codes and a great deal of attention has been paid to determining the existence of extremal self-dual codes, that is codes meeting a bound which comes from the application of invariant theory. In this paper, we shall show why new techniques are needed and we shall give a new construction which produces many interesting codes.

The techniques that we shall describe for constructing self-dual codes are generally concerned with circulant matrices. We recall the definition of a circulant matrix.

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

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

where $a_i \in R$. A reverse circulant matrix over a ring R is a square $n \times n$ matrix, which takes the form

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

where $a_i \in R$.

The most widely applied construction for self-dual codes is to use matrices of the form $(I_n|A)$ where A is a circulant matrix satisfying $AA^T = -I_n$. Numerous combinatorial and algebraic techniques have been applied to this case to produce interesting circulant matrices.

This technique, known as the double circulant construction was first introduced in the 1960s, (see [3, 25] for example). This method has been used extensively to create self-dual codes since it's inception (see [16, 17, 18, 19, 20] for example). MacWilliams and Sloane ([26]) extended this technique to the single bordered construction where the matrix A is replaced with

$$\begin{pmatrix} \gamma & \alpha & \ldots & \alpha \\ \hline \alpha & & & \\ \vdots & & B & \\ \alpha & & & \end{pmatrix}$$

where B is a circulant matrix.

In [24], Kaya et. al. modified the pure circulant construction where A is replaced with

$$\left(\begin{array}{cc|cc} 1 & 1 & \mathbf{x} & \mathbf{y} \\ 1 & 1 & \mathbf{y} & \mathbf{x} \\ \hline \mathbf{z^T} & \mathbf{t^T} & A & B \\ \mathbf{t^T} & \mathbf{z^T} & B & A \end{array} \right)$$

where A is an $n \times n$ circulant matrix, B is a $n \times n$ reverse circulant matrix and $\mathbf{y}$, $\mathbf{x}$, $\mathbf{z}$, $\mathbf{t}$ are vectors of length n. In this work, we shall extend the double circulant construction where A is replaced with the matrix:

$$\left[\begin{array}{cccc|c} a_1 & a_2 & a_3 & a_4 & \mathbf{a_5}\ \mathbf{a_6}\ \mathbf{a_7}\ \mathbf{a_8} \\ a_4 & a_1 & a_2 & a_3 & \mathbf{a_8}\ \mathbf{a_5}\ \mathbf{a_6}\ \mathbf{a_7} \\ a_3 & a_4 & a_1 & a_2 & \mathbf{a_7}\ \mathbf{a_8}\ \mathbf{a_5}\ \mathbf{a_6} \\ a_2 & a_3 & a_4 & a_1 & \mathbf{a_6}\ \mathbf{a_7}\ \mathbf{a_8}\ \mathbf{a_5} \\ \hline \mathbf{a_5^T a_8^T a_7^T a_6^T} & & & & \\ \mathbf{a_6^T a_5^T a_8^T a_7^T} & & & & B \\ \mathbf{a_7^T a_6^T a_5^T a_8^T} & & & & \\ \mathbf{a_8^T a_7^T a_6^T a_5^T} & & & & \end{array} \right]$$

where $\mathbf{a_5}$, $\mathbf{a_6}$, $\mathbf{a_7}$ and $\mathbf{a_8}$ are vectors of length n. In particular, we will consider matrices B that arise from a group ring construction.

Group rings have been used in the literature to construct self-dual codes using a different technique. In [1], an ideal of the group algebra $\mathbb{F}_2 S_4$ was used to construct the famous binary extended Golay code where $\mathbb{F}_2$ is the Galois field of 2 elements and S_4 is the symmetric group on 4 elements. In [22], 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 [23, 30]. In [29], McLoughlin found that the $[48, 24, 12]$ Type II code is a dihedral code. In [6, 8], the idea was extended to any group G and G-codes were defined as codes that are ideals in the group ring RG, where R is a finite Frobenius ring. In [15], a connection between certain group ring elements called unitary units and self-dual codes was established (under a certain construction). Under this construction, it was also highlighted that certain well established techniques are naturally derived from group rings.

In the following sections, we will provide important concepts required for later sections. We will then introduce a new construction and some associated theory. We will finish the article with the implementation of this technique to find certain known and unknown self-dual codes using MAGMA (see [27] for a complete description of this computer algebra system).

2 Preliminaries

In this section, we will define self-dual codes over Frobenius rings of characteristic 2. We will introduce a 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 paper, all rings are assumed to be commutative, finite, Frobenius rings with a multiplicative identity. A complete description of Frobenius rings can be found in [6].

A code C over a finite commutative ring R is said to be any subset of R^n. If the code is a submodule of the ambient space then the code is said to be linear. We attach the usual inner-product to the ambient space, namely $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$. The orthogonal with respect to this inner-product is defined as $C^\perp = \{\mathbf{w} \mid \mathbf{w} \in R^n,\ [\mathbf{w}, \mathbf{w}] = 0, \forall \mathbf{v} \in C\}$. The orthogonal code $C^\perp$ is linear whether or not C is. Since the ring is Frobenius we have that for all linear codes over R, $|C||C^\perp| = |R|^n$. The proof of this fact and a complete description of codes over rings can be found in [6].

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. It follows immediately from the fact that $|C||C^\perp| = |R|^n$, that if C is a self-dual code of length n over the finite commutative Frobenius ring R then $|C| = |R|^{\frac{n}{2}}$. For binary codes, a self-dual code where all weights are congruent to 0 (mod 4) is said to be Type II and the code is said to be Type I otherwise. The bounds on the minimum distances for self-dual codes are:

Theorem 2.1. ([31]) *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

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

Self-dual codes that meet these bounds are called *extremal*. The search for extremal codes is one of the major open questions of algebraic coding theory.

2.2 A Family of Rings

We now define a family of rings of characteristic 2 which we shall use in our constructions. These rings are denoted by R_k, for $k \geq 1$, and were defined in [12] and [13]. For $k \geq 1$,

define

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle. \tag{1}$$

We can also define the rings recursively as:

$$R_k = R_{k-1}[u_k]/\langle u_k^2, u_k u_j - u_j u_k \rangle = R_{k-1} + u_k R_{k-1}. \tag{2}$$

For any subset $A \subseteq \{1, 2, \ldots, k\}$ we will fix

$$u_A := \prod_{i \in A} u_i \tag{3}$$

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

$$\sum_{A \subseteq \{1,\ldots,k\}} c_A u_A, \qquad c_A \in \mathbb{F}_2. \tag{4}$$

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 [12] that the ring R_k is a commutative Frobenius ring with $|R_k| = 2^{(2^k)}$. The ring is a local ring with maximal ideal $\langle u_1, u_2, \ldots, u_k \rangle$. The proof of the following lemma can be found in [12].

Lemma 2.2. *An element γ of R_k if and only if $\gamma^2 = 1$. An element α of R_k is a non-unit if and only if $\alpha^2 = 0$.*

We note then that if $\mathfrak{m}$ is the maximal ideal of R_k then $\alpha \in \mathfrak{m}$ if and only if α is a non-unit. Therefore, if $\alpha \in \mathfrak{m}$ then $\alpha^2 = 0$ and if $\alpha \notin \mathfrak{m}$ then $\alpha^2 = 1$.

We shall now given the definition of a Gray map from R_k to $\mathbb{F}_2^{2^k}$, which was previously defined in [12]. For R_1 we have the following map: $\phi_1(a + bu_1) = (b, a + b)$. Then let $c \in R_k$, c can be written as $c = a + bu_k, a, b \in R_{k-1}$. Then

$$\phi_k(c) = (\phi_{k-1}(b), \phi_{k-1}(a + b)). \tag{5}$$

The map ϕ_k is a distance preserving map and the following is shown in [13].

Theorem 2.3. *Let C be a self-dual code over R_k, then $\phi_k(C)$ is a binary self-dual code of length $2^k n$.*

The next result which was introduced in [11] proves very useful when extending codes over R_1.

Theorem 2.4. *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 $\mathbb{F}_4 + u\mathbb{F}_4$

We shall now define the ring $\mathbb{F}_4 + u\mathbb{F}_4$, which we shall also use to construct self-dual codes. 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 as $\mathbb{F}_4[u]/\langle u^2 \rangle$. Note that $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2 + u\mathbb{F}_2$ and so we can describe any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $\omega a + \bar{\omega} b$ uniquely, where $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$. In order to fit the upcoming tables we use hexadecimals to denote the elements of $\mathbb{F}_4 + u\mathbb{F}_4$ with the ordered basis $\{u\omega, \omega, u, 1\}$.

A 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 [14] and [7] the following Gray maps were introduced:

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

Those were generalized to the following maps in [28]:

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

These maps preserve orthogonality in the corresponding alphabets. Moreover, 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 under the Gray map. we have the following result from [28].

Proposition 2.5. *([28]) Let C be a code over $\mathbb{F}_4 + u\mathbb{F}_4$. If C is self-orthogonal, 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 Type I (resp. Type II) 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 $\varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$.*

Corollary 2.6. *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, C and $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ have the same weight enumerator. If C is Type I (Type II), then so is $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

2.4 Certain Matrices and Group Rings

In this section, we shall introduce group rings and a special isomorphism between the group ring a certain subring of $n \times n$ matrices over a ring. Before we introduce group rings, we need to define a block circulant. For further details on circulant matrices see [5].

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

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

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

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

$$
\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i. \tag{6}
$$

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

$$
\left(\sum_{i=1}^{n} \alpha_i g_i \right) \left(\sum_{j=1}^{n} \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \tag{7}
$$

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

We shall restrict ourselves to finite groups since we are using these to construct codes of finite lengths, however group rings can be defined for infinite groups as well. Throughout, we shall use e_G to denote the identity element of any group G.

The following construction of a matrix was first given by Hurley in [22]. 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

$$
\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1} g_1} & \alpha_{g_1^{-1} g_2} & \alpha_{g_1^{-1} g_3} & \cdots & \alpha_{g_1^{-1} g_n} \\ \alpha_{g_2^{-1} g_1} & \alpha_{g_2^{-1} g_2} & \alpha_{g_2^{-1} g_3} & \cdots & \alpha_{g_2^{-1} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1} g_1} & \alpha_{g_n^{-1} g_2} & \alpha_{g_n^{-1} g_3} & \cdots & \alpha_{g_n^{-1} g_n} \end{pmatrix}. \tag{8}
$$

The elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are simply the elements of the group G in a specific order. The construction in the next section depends on group rings where the order of the group is $4p$ and p is odd. In this paper, we consider RC_{4p}, RD_{4p} and RA_4 where C_{4p} is the cyclic group of order $4p$, D_{4p} is the dihedral group of order $4p$ and A_4 is the alternating group on 4 elements. We shall now describe $\sigma(v)$ for each case.

1. Let $C_{4p} = \langle x \mid x^{4p} = 1 \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{3} \alpha_{i+pj+1} x^{4i+j} \in RC_{4p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4' & A_1 & A_2 & A_3 \\ A_3' & A_4' & A_1 & A_2 \\ A_2' & A_3' & A_4' & A_1 \end{pmatrix}$$

where $A_i = circ(\alpha_{(i-1)p+1}, \ldots, \alpha_{ip})$ and $A_i' = circ(\alpha_{ip}, \alpha_{(i-1)p+1}, \ldots, \alpha_{ip-1})$.

2. Let $D_{4p} = \langle x, y \mid x^{2p} = y^2 = 1, x^y = x^{-1} \rangle$ and

$$v = \sum_{i=0}^{p-1} x^{2i} (\alpha_{i+1} + \alpha_{i+p+1} x + \alpha_{i+2p+1} y + \alpha_{i+3p+1} xy) \in RD_{4p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2' & A_1 & A_4' & A_3 \\ A_3^T & A_4'^T & A_1^T & A_2'^T \\ A_4^T & A_3^T & A_2^T & A_1^T \end{pmatrix}$$

where $A_i = circ(\alpha_{(i-1)p+1}, \ldots, \alpha_{ip})$ and $A_i' = circ(\alpha_{ip}, \alpha_{(i-1)p+1}, \ldots, \alpha_{ip-1})$.

3. Let $a = (1,2)(3,4)$, $b = (1,3)(2,4)$ and $c = (1,2,3)$ where $a, b, c \in A_4$. If

$$v = \sum_{i=0}^{2} (\alpha_{i+1} + \alpha_{i+4} a + \alpha_{i+7} b + \alpha_{i+10} ab) c^i \in RA_4$$

then

$$\sigma(v) = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} \\ \alpha_3 & \alpha_1 & \alpha_2 & \alpha_{12} & \alpha_{10} & \alpha_{11} & \alpha_6 & \alpha_4 & \alpha_5 & \alpha_9 & \alpha_7 & \alpha_8 \\ \alpha_2 & \alpha_3 & \alpha_1 & \alpha_8 & \alpha_9 & \alpha_7 & \alpha_{11} & \alpha_{12} & \alpha_{10} & \alpha_5 & \alpha_6 & \alpha_4 \\ \alpha_4 & \alpha_5 & \alpha_6 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_7 & \alpha_8 & \alpha_9 \\ \alpha_{12} & \alpha_{10} & \alpha_{11} & \alpha_3 & \alpha_1 & \alpha_2 & \alpha_9 & \alpha_7 & \alpha_8 & \alpha_6 & \alpha_4 & \alpha_5 \\ \alpha_8 & \alpha_9 & \alpha_7 & \alpha_2 & \alpha_3 & \alpha_1 & \alpha_5 & \alpha_6 & \alpha_4 & \alpha_{11} & \alpha_{12} & \alpha_{10} \\ \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\ \alpha_6 & \alpha_4 & \alpha_5 & \alpha_9 & \alpha_7 & \alpha_8 & \alpha_3 & \alpha_1 & \alpha_2 & \alpha_{12} & \alpha_{10} & \alpha_{11} \\ \alpha_{11} & \alpha_{12} & \alpha_{10} & \alpha_5 & \alpha_6 & \alpha_4 & \alpha_2 & \alpha_3 & \alpha_1 & \alpha_8 & \alpha_9 & \alpha_7 \\ \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_9 & \alpha_7 & \alpha_8 & \alpha_6 & \alpha_4 & \alpha_5 & \alpha_{12} & \alpha_{10} & \alpha_{11} & \alpha_3 & \alpha_1 & \alpha_2 \\ \alpha_5 & \alpha_6 & \alpha_4 & \alpha_{11} & \alpha_{12} & \alpha_{10} & \alpha_8 & \alpha_9 & \alpha_7 & \alpha_2 & \alpha_3 & \alpha_1 \end{pmatrix}.$$

2.5 Motivation

In this subsection, we shall describe the motivation for the construction given in the next section. We begin with a lemma.

Lemma 2.7. *Let R be a finite commutative Frobenius ring of characteristic 2. Let C be the code generated by a matrix M of the form*

$$\begin{pmatrix} I_k & B \\ B^T & I_k \end{pmatrix},$$

where B is a k by k matrix. If the free rank of C is k then C is self-dual.

Proof. Let the code D be defined by $D = \langle (I_k|B) \rangle$ and $D' = \langle (B^T|I_k) \rangle$. The inner-product of the i-th row of $(I_k|B)$ and the j-th row of $(B^T|I_k)$ is $B_{i,j} + B^T_{j,i} = B_{i,j} + B_{i,j} = 0$ since the characteristic is 2. Therefore $D' = D^\perp$ since $|D||D'| = |R|^n$.

Let the code C be defined by $C = \langle D, D^\perp \rangle$. If $D \neq D^\perp$ then $|C| > |D|$. However, we are assuming that the free rank of C is k. Hence $C = D = D^\perp$. This gives that C is a self-dual code. $\square$

Let D_{2k} be the dihedral group of order $2k$. We describe the group by $D_{2k} = \langle a, b \mid a^2 = b^k = 1, ab = b^{-1}a \rangle$.

We shall take a different ordering of the elements of the group than was given in [8]. Here the ordering of the elements for the map σ is $1, b^{k-1}, b^{k-2}, \ldots, b^2, b^1, a, ab, ab^2, \ldots, ab^{k-1}$.

Let $v = \sum \alpha_{a^i b^j} a^i b^j$. With this ordering for the first row but multiplying in the order $1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}$ on the left, the matrix $\sigma(v)$ is of the form:

$$\begin{pmatrix}
\alpha_1 & \alpha_{b^{k-1}} & \alpha_{b^{k-2}} & \cdots & \alpha_b & \alpha_a & \alpha_{ab} & \alpha_{ab^2} & \cdots & \alpha_{ab^{k-1}} \\
\alpha_b & \alpha_1 & \alpha_{b^{k-1}} & \cdots & \alpha_{b^2} & \alpha_{ab^{k-1}} & \alpha_a & \alpha_{ab} & \cdots & \alpha_{ab^{k-2}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{b^{k-1}} & \alpha_{b^{k-2}} & \alpha_{b^{k-3}} & \cdots & \alpha_1 & \alpha_{ab} & \alpha_{ab^2} & \alpha_{ab^3} & \cdots & \alpha_a \\
\alpha_a & \alpha_{ab^{k-1}} & \alpha_{ab^{k-2}} & \cdots & \alpha_{ab} & \alpha_1 & \alpha_b & \alpha_{b^2} & \cdots & \alpha_{b^{k-1}} \\
\alpha_{ab} & \alpha_a & \alpha_{ab^{k-1}} & \cdots & \alpha_{ab^2} & \alpha_{b^{k-1}} & \alpha_1 & \alpha_b & \cdots & \alpha_{b^{k-2}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{ab^{k-1}} & \alpha_{ab^{k-2}} & \alpha_{ab^{k-3}} & \cdots & \alpha_{ab^{k-2}} & \alpha_b & \alpha_{b^2} & \alpha_{b^3} & \cdots & \alpha_1
\end{pmatrix}. \tag{9}$$

This gives that $\sigma(v)$ is of the form:

$$\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$$

where A and B are circulant matrices.

Theorem 2.8. *Let R be a finite commutative Frobenius ring of characteristic 2 and let $v \in RD_{2k}$ with $v = \sum \alpha_{a^i b^j} a^i b^j$ where only $\alpha_{a^0 b}$ is 1 and $\alpha_{a^0 b^i}$ is 0 for $i \neq 1$. Let $C_v = \langle \sigma(v) \rangle$. If C_v has free rank k, then C_v is a self-dual code.*

Proof. Since $\alpha_{a^0 v}$ is 1 and $\alpha_{a^0 b^i}$ is 0 for $i \neq 1$, the generator matrix of C_v is of the form:

$$\begin{pmatrix} I_k & B \\ B^T & I_k \end{pmatrix}.$$

Then, by Lemma 2.7, we have the result. $\qquad\square$

Corollary 2.9. *Let C be a self-dual code over a finite commutative Frobenius ring of characteristic 2 of length $2k$ generated by $(I_k|A)$ where A is a circulant matrix. Then C is an ideal in RD_{2k} and D_{2k} is a subgroup of the automorphism group of C.*

Proof. The orthogonal of the code generated by $(I_k|A)$ is the code generated by $(A^T|I_k)$. Since C is self-dual then the code generated by $\begin{pmatrix} I_k & A \\ A^T & I_k \end{pmatrix}$ where A is a circulant matrix is the self-dual code C. Therefore $C = \langle \sigma(v) \rangle$ for some $v \in RD_{2k}$.

The fact that the code has D_{2k} as a subgroup of its automorphism group follows from Corollary 2.2 in [8]. $\qquad\square$

The implication of this corollary is that if you are simply searching for self-dual codes generated by $(I_k|A)$ where A is a circulant matrix then you will only be finding codes with a fairly significant restriction on their automorphism group. Additionally, it was shown in [8] that if A is a reverse circulant matrix that it will correspond to an ideal in the same group algebra with a different ordering of the elements. This means that, in either case, you will only be finding codes which correspond to ideals in in the group ring RD_{2k}. One implication of this is that you can only find self-dual codes where $2k$ divides the order of the automorphism group. Therefore, if we wish to find all interesting self-dual codes of a given length (for example the extremal codes) then we need to expand the structure of matrices that we use to construct the codes. This is precisely what we do in this paper. We give new structures for matrices to obtain codes that were previously missed by other constructions.

3   Construction

Let $v \in RG$ where R is a finite commutative ring and G is a finite group. If $v = \sum_g a_g g$ then $v^* = \sum_g a_g g^{-1}$. We say that v is a unitary unit in RG if $vv^* = 1$.

Let $v \in RG$ where R is a finite commutative Frobenius ring of characteristic 2 and G is a finite group of order $4p$ where p is odd. Let $a_i \in R$ and $\mathbf{a_{i+4}} = (a_{i+4}, \dots, a_{i+4}) \in R^p$ for $1 \leq i \leq 4$. Define the following matrix:

$$M(\sigma) = \begin{bmatrix} & & \begin{array}{cccc|cccc} a_1 & a_2 & a_3 & a_4 & \mathbf{a_5} & \mathbf{a_6} & \mathbf{a_7} & \mathbf{a_8} \\ a_4 & a_1 & a_2 & a_3 & \mathbf{a_8} & \mathbf{a_5} & \mathbf{a_6} & \mathbf{a_7} \\ a_3 & a_4 & a_1 & a_2 & \mathbf{a_7} & \mathbf{a_8} & \mathbf{a_5} & \mathbf{a_6} \\ a_2 & a_3 & a_4 & a_1 & \mathbf{a_6} & \mathbf{a_7} & \mathbf{a_8} & \mathbf{a_5} \\ \hline \mathbf{a_5^T}\,\mathbf{a_8^T}\,\mathbf{a_7^T}\,\mathbf{a_6^T} & & & & & & \\ \mathbf{a_6^T}\,\mathbf{a_5^T}\,\mathbf{a_8^T}\,\mathbf{a_7^T} & & & & & \sigma(v) & \\ \mathbf{a_7^T}\,\mathbf{a_6^T}\,\mathbf{a_5^T}\,\mathbf{a_8^T} & & & & & & \\ \mathbf{a_8^T}\,\mathbf{a_7^T}\,\mathbf{a_6^T}\,\mathbf{a_5^T} & & & & & & \end{array} \end{bmatrix}$$

Let C_σ be a code that is generated by the matrix $M(\sigma)$. Then, the code C_σ has length $8p + 8$. We want to investigate when this construction yields self-dual codes. Consequently, we will now consider $M(\sigma)M(\sigma)^T$.

Let $A = circ(a_1, a_2, a_3, a_4)$ and $B = CIRC(\mathbf{a_5}, \mathbf{a_6}, \mathbf{a_7}, \mathbf{a_8})$. Then

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

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

$$= \begin{pmatrix} AA^T + BB^T + I & AB + B\sigma(v^*) \\ B^T A^T + \sigma(v)B^T & B^T B + \sigma(vv^*) + I \end{pmatrix}.$$

Now, $AA^T = circ\left(\sum_{i=1}^{4} a_i^2, (a_1 + a_3)(a_2 + a_4), 0, (a_1 + a_3)(a_2 + a_4)\right)$ and

$$BB^T = circ\left(p\sum_{i=1}^{4} a_{i+4}^2, p(a_5 + a_7)(a_6 + a_8), 0, p(a_5 + a_7)(a_6 + a_8)\right)$$

$$= circ\left(\sum_{i=1}^{4} a_{i+4}^2, (a_5 + a_7)(a_6 + a_8), 0, (a_5 + a_7)(a_6 + a_8)\right).$$

Therefore

$$AA^T + BB^T + I = circ\left(1 + \sum_{i=1}^{8} a_i^2, \gamma, 0, \gamma\right)$$

where $\gamma = (a_1 + a_3)(a_2 + a_4) + (a_5 + a_7)(a_6 + a_8)$. Additionally,

$$B^T B = CIRC\left(\sum_{i=1}^{4} a_{i+4}\left(circ(\underbrace{1, \ldots, 1}_{p-\text{times}})\right), \delta\left(circ(\underbrace{1, \ldots, 1}_{p-\text{times}})\right), 0, \delta\left(circ(\underbrace{1, \ldots, 1}_{p-\text{times}})\right)\right)$$

where $\delta = (a_5 + a_7)(a_6 + a_8)$.

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.

11

Theorem 3.1. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite group of order $4p$ where p is odd. If $AA^T + BB^T + I = 0$, $AB + B\sigma(v^*) = 0$ and $B^T B + \sigma(vv^*) + I = 0$ then C_σ is a self-dual code of length $8p + 8$.*

Proof. Clearly, C_σ has free rank $4p + 4$ as the left hand side of the generator matrix is the $4p + 4$ by $4p + 4$ identity matrix. If $AA^T + BB^T + I = 0$, $AB + B\sigma(v^*) = 0$ and $B^T B + \sigma(vv^*) + I = 0$ then C_σ is self-orthogonal and C_σ is self-dual. $\square$

Corollary 3.2. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order $4p$ where p is odd. Let $v \in RG$ be a unitary unit. If $a_5 = a_7$, $a_6 = a_8$, $a_1 = a_3$ and $a_2 + a_4 = 1$ or $a_5 = a_7$, $a_6 = a_8$, $a_1 + a_3 = 1$ and $a_2 = a_4$ then C_σ is a self-dual code of length $8p + 8$.*

Proof. If $a_5 = a_7$, $a_6 = a_8$, $a_1 = a_3$ and $a_2 + a_4 = 1$ or $a_5 = a_7$, $a_6 = a_8$, $a_1 + a_3 = 1$ and $a_2 = a_4$ then $AA^T + BB^T + I = 0$ and $B^T B + \sigma(vv^*) + I = \sigma(vv^*) + I = 2I = 0$ since I is unitary. Therefore C_σ is self-dual. $\square$

Corollary 3.3. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order $4p$ where p is odd. Let C_σ be self-dual. If $\sum_{i=1}^{4} a_{i+4} = 1$, then $v \in RG$ is a non-unit.*

Proof. If C_σ is self-dual, clearly $\sigma(vv^*) = B^T B + I$. If $\sum_{i=1}^{4} a_{i+4} = 1$, then $I + B^T B = CIRC(A_1, A_2, 0, A_2)$ where $A_1 = circ(0, \underbrace{1, \ldots, 1}_{(p-1)-\text{times}})$ and $A_2 = circ(\underbrace{\delta, \ldots, \delta}_{p-\text{times}})$. Let $C = CIRC(A_1, A_2, 0, A_2)$. For each $2 \leq i \leq 4p$, add the i-th row of C to the first row of C. Then the first row becomes

$$\underbrace{((p-1) + 2p\delta, (p-1) + 2p\delta, \ldots (p-1) + 2p\delta)}_{4p-\text{times}} = \underbrace{(0, 0, \ldots, 0)}_{4p-\text{times}}.$$

Since p is odd and the ring has characteristic 2, then $det(CIRC(A_1, A_2, 0, A_2)) = 0$. Therefore, $det(I + B^T B) = 0$ and vv^* is a non-unit by Corollary 3 in [22]. Therefore, $v \in RG$ is a non-unit. $\square$

We can use the structure of the family of rings R_s to get an infinite number of binary self-dual codes from a single matrix M satisfying the conditions of Theorem 3.1.

Theorem 3.4. *If M is a matrix satisfying the conditions in Theorem 3.1 over R_k, then M generates a self-dual code over R_s for all $s \geq k$.*

Proof. If $k \leq s$ then the ring R_k is a subring of the ring R_s. The matrix M has free rank $4p + 4$ over any ring where it is defined and if $\mathbf{v}$ and $\mathbf{w}$ are orthogonal over R_k then they are orthogonal over R_s as well since R_k is a subring of R_s. Therefore, the code generated by M over R_s is a self-dual code of length $8p + 8$. $\square$

This leads immediately to the following corollary.

Corollary 3.5. *Let M be a matrix satisfying the conditions in Theorem 3.1 over R_k. Let C_s be the code generated by M over R_s. Then $\phi_s(C_s)$ is a binary self-dual code of length $2^s(8p + 8)$.*

Similarly, we have the following.

Theorem 3.6. *If M is a matrix satisfying the conditions in Theorem 3.1 over R_1, then M generates a self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$.*

Proof. The ring R_1 is a subring of the ring $\mathbb{F}_4 + u\mathbb{F}_4$. Therefore the proof follows exactly as the proof of Theorem 3.4. □

This leads naturally to the following corollary using the result in Corollary 2.6.

Corollary 3.7. *Let M be a matrix satisfying the conditions in Theorem 3.1 over R_1. Let C be the code generated by M over $\mathbb{F}_4 + u\mathbb{F}_4$. Then $(\phi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4})(C)$ is a binary self-dual code of length $4(8p + 8)$.*

4   Results

In this section, we will present the results obtained using this construction to construct self-dual codes for certain groups of order 4, 12 and 20.

4.1   Constructions coming from a group of order 4

Here we present the results for the above construction using $G = C_4$. We construct self-dual codes of length 16, 32 and 64 by considering this construction over $\mathbb{F}_2$, $\mathbb{F}_4$ and $\mathbb{F}_4 + u\mathbb{F}_4$. Finally, we construct new extremal self-dual codes of length 68 by extending certain extremal self-dual codes of length 64.

The possible weight enumerators for a self-dual Type I $[64, 32, 12]$-code is given in [4, 10] as:

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

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, . . . , 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 $W_{64,2}$.

Table 1: Self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$ of length 64 from C_4 where each code is of type $W_{64,2}$

C_i	$(a_1,\ldots,a_8)$	$(\alpha_1,\ldots,\alpha_4)$	$\lvert Aut(C)\rvert$	β	C_i	$(a_1,\ldots,a_8)$	$(\alpha_1,\ldots,\alpha_4)$	$\lvert Aut(C)\rvert$	β
1	$(0,9,6,4,2,4,3,5)$	$(9,D,F,0)$	2^4	0	2	$(0,4,9,F,1,1,6,7)$	$(0,F,9,4)$	2^5	0
3	$(2,2,1,1,0,9,6,4)$	$(2,1,1,2)$	2^6	0	4	$(0,9,6,E,A,4,3,F)$	$(1,D,7,A)$	2^3	2
5	$(2,8,4,5,6,6,F,F)$	$(4,3,2,E)$	2^4	2	6	$(0,9,6,E,2,4,1,5)$	$(5,1,3,6)$	2^3	4
7	$(2,4,1,F,9,9,E,D)$	$(2,F,1,4)$	2^4	4	8	$(A,A,9,9,0,9,E,E)$	$(A,9,9,A)$	2^5	4
9	$(2,9,4,6,0,4,1,D)$	$(7,1,1,E)$	2^3	6	10	$(0,A,6,7,A,A,9,9)$	$(6,1,0,C)$	2^4	6
11	$(0,1,6,6,8,6,B,7)$	$(9,D,F,A)$	2^3	8	12	$(2,4,9,F,1,9,6,7)$	$(2,F,9,4)$	2^4	8
13	$(0,0,2,6,1,7,E,D)$	$(0,6,2,0)$	2^5	8	14	$(2,2,4,7,2,4,3,F)$	$(4,3,2,6)$	2^3	10
15	$(A,0,4,7,6,6,D,D)$	$(6,B,8,C)$	2^4	10	16	$(0,9,6,E,8,4,9,7)$	$(5,1,3,6)$	2^3	12
17	$(0,4,1,D,9,3,E,7)$	$(0,D,1,4)$	2^4	12	18	$(2,2,4,5,4,C,5,F)$	$(9,C,F,B)$	2^5	12
19	$(0,A,6,7,2,4,1,7)$	$(8,F,E,2)$	2^3	14	20	$(A,8,4,5,6,E,F,5)$	$(6,1,8,C)$	2^4	14
21	$(0,1,6,4,8,4,9,F)$	$(3,D,5,8)$	2^3	16	22	$(2,4,9,5,1,9,C,D)$	$(2,5,9,4)$	2^4	16
23	$(A,A,9,9,2,1,C,6)$	$(A,9,9,A)$	2^5	16	24	$(0,1,6,C,2,6,3,7)$	$(D,1,B,C)$	2^3	18
25	$(8,A,6,7,4,C,D,7)$	$(4,3,A,E)$	2^4	18	26	$(2,4,1,5,9,9,4,7)$	$(2,5,1,4)$	2^4	20
27	$(2,2,9,9,1,B,6,5)$	$(2,9,9,2)$	2^5	20	28	$(0,1,4,C,2,6,1,F)$	$(9,F,D,2)$	2^3	22
29	$(0,8,6,5,6,6,D,D)$	$(1,4,7,9)$	2^4	22	30	$(2,4,1,D,9,B,4,F)$	$(2,D,1,4)$	2^4	24
31	$(2,2,9,9,1,9,C,F)$	$(2,9,9,2)$	2^5	24	32	$(2,9,4,4,8,6,1,F)$	$(F,9,9,4)$	2^3	26

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

The possible weight enumerator of a self-dual $[68,34,12]_2$ -code is in one of the following forms by [2, 21, 9]:

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

where $0 \le \gamma \le 9$. Recently, Yankov et. al. constructed the first examples of codes with a weight enumerator for $\gamma = 7$ in $W_{68,2}$. In [9], more unknown $W_{68,2}$ codes were constructed.

Table 2: Self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$ of length 64 from C_4 where each code is of type $W_{64,2}$

C_i	$(a_1,\ldots,a_8)$	$(\alpha_1,\ldots,\alpha_4)$	$|Aut(C)|$	β	C_i	$(a_1,\ldots,a_8)$	$(\alpha_1,\ldots,\alpha_4)$	$|Aut(C)|$	β
33	$(2,9,4,6,8,4,9,D)$	$(B,7,D,8)$	2^3	28	34	$(2,6,9,7,1,1,4,7)$	$(2,7,9,6)$	2^4	28
35	$(2,2,4,5,6,E,7,D)$	$(9,C,F,B)$	2^5	28	36	$(0,0,6,7,4,C,D,7)$	$(1,4,7,3)$	2^4	30
37	$(2,4,9,7,9,3,4,F)$	$(2,7,9,4)$	2^4	32	38	$(A,8,9,9,2,9,4,E)$	$(A,9,9,8)$	2^5	32
39	$(A,4,9,F,1,1,4,F)$	$(A,F,9,4)$	2^4	36	40	$(0,0,9,9,A,9,4,E)$	$(0,9,9,0)$	2^5	36
41	$(0,A,2,6,1,5,6,F)$	$(0,6,2,A)$	2^5	40	42	$(A,8,4,5,4,E,F,7)$	$(3,E,D,3)$	2^4	44
43	$(0,0,4,7,A,6,1,5)$	$(0,7,4,0)$	$2^4 \cdot 3$	44	44	$(8,8,1,1,0,9,6,4)$	$(8,1,1,8)$	2^5	48
45	$(A,A,1,1,8,1,E,C)$	$(A,1,1,A)$	2^5	52					

Together with these, the existence of the codes in $W_{68,2}$ is known for;

$$\gamma \; = \; 0, \; \beta = 0, \, 7, \, 11, \, 14, \, 17, \, 21, \, 22, \, 28, \, 33, \, 35, \, 42, \, 44, \ldots, 158, \, 161, \, 165,$$
$$175, \, 187, \, 189, \, 203, \, 209, \, 221, \, 231, \, 255, \, 303 \text{ or}$$
$$\beta \; \in \; \{2m | m = 17, \, 20, \, 102, \, 110, \, 119, \, 136, \, 165 \text{ or } 80 \leq m \leq 99\} \, ;$$
$$\gamma \; = \; 1, \; \beta = 49,51,53,55, \, 57, \, 59, \ldots, 160 \text{ or}$$
$$\beta \; \in \; \{2m | m = 25, \ldots, 29, \, 81, \ldots, 90, 92, \ldots, 96\} \, ;$$
$$\gamma \; = \; 2, \; \beta = 65,69,71,73,75,77,79,81,159, \, 206, \, 208 \text{ or } \beta \in \{2m | 30 \leq m \leq 68, 70 \leq m \leq 100\} \text{ or}$$
$$\beta \; \in \; \{2m + 1 | 41 \leq m \leq 69, \; 71 \leq m \leq 77\} \, ;$$
$$\gamma \; = \; 3, \; \beta = \; 84,95,97,101,103,105,107,109,113,115,117,119,121,123,125,127,129,131,133, \, 135,$$
$$137, \, 139, \, 141, \, 143, \, 145,147,149,151,153, \, 155, \, 159, \, 161,193 \text{ or}$$
$$\beta \; \in \; \{2m \, | m = 44, \, 45, \, 47, \ldots, 84, \, 86, \ldots, 92, \, 94, \, 95, \, 97, \, 98, \, 101, \, 102\} \, ;$$
$$\gamma \; = \; 4, \; \beta = 129, \, 141, \, 145, \, 157, \, 161 \text{ or}$$
$$\beta \; \in \; \{2m \, | m = 43, \, 48, \, 49, \, 51, \, 52, \, 54, \, 55, \, 56, \, 58, \, 60, \ldots, 78, \, 80, \, 87, \, 97, \, 98\} \, ;$$
$$\gamma \; = \; 6 \text{ with } \beta \in \{2m | m = 69, \, 77, \, 78, \, 79, \, 81, \, 88\}$$
$$\gamma \; = \; 7 \text{ with } \beta \in \{7m | m = 14, \ldots, 39, \, 42\} \, .$$

Recall that the previously constructed codes of length 64 are codes over $\mathbb{F}_4 + u\mathbb{F}_4$. In order to apply Theorem 2.4, 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 the previous table, the unit $c \in \mathbb{F}_2 + u\mathbb{F}_2$, the vector X required to apply Theorem 2.4 and we replace $u + 1$ with 3 to save space.

Self dual binary codes C and D of length n are said to be neighbors if $\dim(C \cap D) = n/2 - 1$. In order to consider some neighbors of a code C we pick a vector $x \in \mathbb{F}_2^n - C$ and

Table 3: Extremal self-dual codes of length 68 from C_4 over $\mathbb{F}_4 + u\mathbb{F}_4$.

$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β	$|Aut(\mathrm{C}_{68,i})|$
1	2	1	$(uu333033031110uu3u13u001u0133313)$	**1**	**44**	2
2	2	1	$(131103u0uuu1011033uu033u0u0u3013)$	**1**	**48**	2
3	2	1	$(3uu010u30uuu00013uu0u3131u0u1313)$	**2**	**58**	2
4	2	1	$(3u0uu11313u0u01130130303u1uu00u3)$	**3**	**86**	2
5	2	1	$(3u13u0u01uu013u10u13010131011uu0)$	**4**	**100**	2
6	2	$u+1$	$(0101u3u1uuu03u3u01301100u0101u30)$	**4**	**114**	2
7	3	1	$(1u0133000010u313011133u01u331u33)$	**3**	**87**	2
8	3	1	$(3100u303u331003u033u013u301u13u1)$	**3**	**89**	2
9	4	1	$(313u030313u11u133130u1101u0u3uu1)$	**3**	**99**	2
10	8	1	$(030uuu30010u0033131u1333uuu03u11)$	**3**	**92**	2
11	9	1	$(00300u001001u00u330u33u3330111uu)$	**3**	**82**	2
12	10	1	$(1u01000u1310u1u011u0111u1u103100)$	**3**	**111**	2
13	21	$u+1$	$(u3u11u113u1333u1u031333u1100131u)$	**4**	**139**	2
14	26	$u+1$	$(uu0uu10uu11u3u0u03u3u0uuuu1u3331)$	**4**	**143**	2
15	30	1	$(13u031u03330uu0uuu3313u330110310)$	**4**	**149**	2
16	37	1	$(1000uu11u100uu0001uuu310u0103u00)$	**2**	**141**	2
17	40	1	$(3300u30103010u111u311303u01303u0)$	**4**	**158**	2
18	40	$u+1$	$(u01101310u030110111110uu33u11uuu)$	**4**	**162**	2
19	40	$u+1$	$(10031u301u01010uuuuuu311uu10u011)$	**4**	**170**	2

let $D = \left\langle \langle x \rangle^{\perp} \cap C, x \right\rangle$. We use the standard form of the generator matrix of C, which lets us to fix first $n/2$ entries of x without loss of generality. We set the first 34 entries of x to be 0. We consider the neighbors of the binary images of the codes in Table 3 and obtain five new codes of length 68 which are listed in Table 4.

4.2 Constructions coming from groups of order 12

Here we present the results for the above construction using $G \in \{C_{12}, D_{12}, A_4\}$. We construct self-dual codes of length 32 and 64 by considering this construction over $\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2$. Again, we construct new extremal self-dual codes of length 68 by extending certain extremal self-dual codes of length 64.

4.2.1 New Codes of length 68 from R_1A_4

We now consider extensions of the previously constructed codes of length 64 (codes from A_4 over $\mathbb{F}_2 + u\mathbb{F}_2$). The following table records newly constructed extremal self-dual codes of length 68. Again, we note the original code of length 64 from the previous table, the unit

Table 4: New codes of length 68 with $\gamma = 4$ as neighbors of codes in Table 3

$\mathcal{N}_{68,i}$	$\mathcal{C}_{68,j}$	$(x_{35}, x_{36}, ..., x_{68})$	β	$|Aut(\mathcal{N}_{68,i})|$
$\mathcal{N}_{68,1}$	$\mathcal{C}_{68,19}$	(00100010011001110111111101110111001)	**166**	2
$\mathcal{N}_{68,2}$	$\mathcal{C}_{68,17}$	(01111001000101010011010111111011011)	**167**	2
$\mathcal{N}_{68,3}$	$\mathcal{C}_{68,17}$	(11100111011110101000110011001100110110)	**168**	2
$\mathcal{N}_{68,4}$	$\mathcal{C}_{68,18}$	(11111010101101001101101100101001100)	**169**	2
$\mathcal{N}_{68,5}$	$\mathcal{C}_{68,19}$	(00111011011101001101111100011000000)	**171**	2

Table 5: Type II Extremal Self-dual code of length 64 from D_{12} over R_1.

$(a_1, \ldots, a_8)$	$(\alpha_1, \ldots, \alpha_{12})$	$|Aut(C)|$
$(u, 1, 0, 1, u, 0, u, 1)$	$(u, 1, 1, u, u+1, 0, u, 1, u+1, 1, u+1, u+1)$	$2^3 \cdot 3$
$(u, 1, 0, 1, u, 0, u, 1)$	$(u, 1, 1, u, u+1, 0, u, 1, u+1, u+1, u+1, 1)$	$2^3 \cdot 3$

Table 6: Type II Extremal Self-dual code of length 64 from A_4 over R_1.

$(a_1, \ldots, a_8)$	$(\alpha_1, \ldots, \alpha_{12})$	$|Aut(C)|$
$(1, u+1, u+1, u+1, u, 0, u, 1)$	$(u, u, 1, 0, u, 1, 1, u, 0, 1, u+1, 1)$	$2^4 \cdot 3$
$(u+1, 1, 1, 1, u, 0, u, 1)$	$(0, u, 1, u, u, 1, u+1, u, 0, u+1, u+1, 1)$	2^4

Table 7: Type I Extremal Self-dual code of length 64 from A_4 over R_1.

$\mathcal{D}_i$	$(a_1, \ldots, a_8)$	$(\alpha_1, \ldots, \alpha_{12})$	$|Aut(C)|$	$W_{64,2}$
1	$(u+1, 1, 1, 1, u, u, u, 1)$	$(0, u, 1, u, u, 1, u+1, u, 0, u+1, u+1, 1)$	$2^4 \cdot 3$	$\beta = 64$
2	$(1, u+1, u+1, u+1, u, u, u, 1)$	$(0, 0, 1, u, 0, 1, 1, 0, u, 1, u+1, 1)$	$2^4 \cdot 3^2$	$\beta = 40$
3	$(u, 0, 0, 0, u, 1, 1, 1)$	$(u, 1, 1, u, u, 0, 0, 1, 1, u+1, 0, u+1)$	$2^3 \cdot 3$	$\beta = 52$

$c \in \mathbb{F}_2 + u\mathbb{F}_2$, the vector X required to apply Theorem 2.4 and we replace $u + 1$ with 3 to save space

Table 8: Extremal Self-dual code of length 68 from A_4 over R_1.

$\mathcal{D}_{68,i}$	$\mathcal{D}_i$	c	X	γ	β	$|Aut(\mathrm{D}_{68,i})|$
1	1	$u+1$	$(1uuuu1u13u1uu110113u0u33u301133u)$	**0**	**159**	2
2	1	$u+1$	$(03030000uu01u111u33u13u0u1u0uu11)$	**0**	**163**	2
3	1	1	$(31u03u003u1031u030uu0uu30110011u)$	**1**	**161**	2
4	1	$u+1$	$(300133130u110013303u0u1uu1u30013)$	**1**	**163**	2
5	1	1	$(31u311331311003u0u1u0u1u331u1uu1)$	**1**	**165**	2
6	1	$u+1$	$(u333010u1u33u011u33u03u100101130)$	**1**	**167**	2
7	1	$u+1$	$(333010130uu00u10130101u30u1u1133)$	**1**	**169**	2
8	1	1	$(33000303uu1u3030100uu101333u1111)$	**1**	**171**	2
9	3	$u+1$	$(1u031u0u3310030u13uu3330301u30uu)$	**2**	**138**	2

4.3 Constructions coming from groups of order 20

Here we present the results for the above construction using $G \in \{C_{20}, D_{20}\}$. We construct self-dual codes of length 48 by considering this construction over $\mathbb{F}_2$.

Table 9: Binary self-dual code of length 48 from C_{20}.

$(a_1, \ldots, a_8)$	$(\alpha_1, \ldots, \alpha_{20})$	$|Aut(C)|$	Type
$(0,0,0,0,0,1,1,1)$	$(0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,1,0,1)$	$2^{18} \cdot 3^2 \cdot 5^2$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,0,0,0,0,0,1,1,1,1,0,1,1,1,1,0,0,0)$	$2^6 \cdot 3 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,0,0,0,1,1,1,1,1,0,1,1,1,1,1,0,1,1)$	$2^8 \cdot 3^3 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,1,1,0,0,1,0,1,1,1,1,1,0,1,1,1,0,1)$	$2^3 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,1,1,0,1,0,1,0,0,0,1,0,1,1,0,0,1,0)$	$2^6 \cdot 3^2 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,1,1,1,1,0,1,1,0,0,1,0,1,1,1,1,1,0)$	$2^7 \cdot 3 \cdot 5$	$[48,24,8]$

Table 10: Binary self-dual code of length 48 from D_{20}.

$(a_1, \ldots, a_8)$	$(\alpha_1, \ldots, \alpha_{20})$	$|Aut(C)|$	Type
$(0,0,0,0,0,1,1,1)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,0,1)$	$2^{18} \cdot 3^2 \cdot 5^2$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,0,0,0,0,0,1,1,0,0,0,1,1,1,1,1,0,0)$	$2^6 \cdot 3 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,0,0,0,1,1,1,1,0,1,1,1,1,1,1,0,1,1)$	$2^8 \cdot 3^3 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,1,1,0,0,1,0,1,0,0,0,1,1,1,1,0,0,0)$	$2^6 \cdot 3^2 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,1,1,0,0,1,0,1,0,1,1,1,1,1,1,0,1,1)$	$2^7 \cdot 3 \cdot 5$	$[48,24,8]$
$(0,0,0,0,0,1,1,1)$	$(0,0,0,1,1,0,1,0,0,1,0,0,0,1,1,0,1,1,0,0)$	$2^3 \cdot 5$	$[48,24,8]$

5 Conclusion

In this work, we introduce a new construction (quadruple border) together with certain group rings for constructing self-dual codes. Additionally, we established a link between certain elements of the group ring (units and non-units) and self-dual codes under this construction. We establish the relevance of this new construction by constructing new extremal self-dual codes of length 68. In particular, we construct the following unknown $W_{68,2}$ codes:

$$(\gamma = 0, \quad \beta = \{159, 163\}),$$
$$(\gamma = 1, \quad \beta = \{44, 48, 161, 163, 165, 167, 169, 171\}),$$
$$(\gamma = 2, \quad \beta = \{58, 138, 141\}),$$
$$(\gamma = 3, \quad \beta = \{82, 86, 87, 89, 92, 99, 111\}) \text{ and}$$
$$(\gamma = 4, \quad \beta = \{100, 114, 139, 143, 149, 158, 162, 166, 167, 168, 169, 170, 171\}).$$

We consider certain groups of order $4p$ where p is odd. A suggestion for further work would be to consider other classes of groups of order $4p$ and possibly groups of order $4p$ when p is even. Finally, one could consider groups of order larger than 20.

References

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

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

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

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

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

[6] S.T. Dougherty, Algebraic Coding Theory Over Finite Commutative Rings, Springer-Briefs in Mathematics. Springer, Cham, 2017, ISBN: 978-3-319-59805-5; 978-3-319-59806-2.

[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, **45**, 1999, 32 - 45.

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

[9] S.T. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylshchak, B. Yildiz, Bordered constructions of self-dual codes from group rings, submitted.

[10] S.T. Dougherty, M. Harada, T.A. Gulliver, Extremal binary self-dual codes, IEEE Trans. Information Theory, **43**, no. 6, 1997, 2036 - 2047.

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

[12] S.T. Dougherty, B. Yildiz, S. Karadeniz, Codes over R_k, Gray maps and their binary images, Finite Fields Appl., **17**, no. 3., 2011, 205 - 219.

[13] S.T. Dougherty, B. Yildiz, S. Karadeniz, Self-dual codes over R_k and binary self-dual codes, European Journal of Pure and Applied Mathematics, **6**, no. 1, 2013, 89 - 106.

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

[15] J. Gildea, A. Kaya, R. Taylor, B. Yildiz, Constructions for self-dual codes induced from group rings, Finite Fields Appl., **51**, 2018, 71 - 92.

[16] T.A. Gulliver, M. Harada, Weight enumerators of double circulant codes and new extremal self-dual codes, Des. Codes Cryptogr., **11**, no. 2, 2997, 141 - 150.

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

[18] T.A. Gulliver, M. Harada, H. Miyabayashi, Double circulant and quasi-twisted self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$, Adv. Math. Commun., **1**, no. 2, 2007, 223 - 238.

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

[20] T.A. Gulliver, M. Harada, On the performance of optimal double circulant even codes, Adv. Math. Commun., **11**, no. 4, 2017, 767 - 775.

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

[22] T. Hurley, Group Rings and Rings of Matrices, Int. Jour. Pure and Appl. Math, **31**, no. 3, 2006, 319 - 335.

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

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

[25] M. Karlin, New binary coding results by circulants, IEEE Trans. Information Theory **15**, 1969, 81 - 92.

[26] F.J. MacWilliams, N.J.A. Sloane, The theory of error-correcting codes. I. North-Holland Mathematical Library, **16**, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–xv and 1 - 369. ISBN: 0-444-85009-0.

[27] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.16 (2010), 5017 pages.

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

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

[30] McLoughlin, I., Hurley, T., A group ring construction of the extended binary Golay code, IEEE Trans. Inform. Theory, **54**, no. 9, 2008, 4381 - 4383.

[31] E.M. Rains, Shadow bounds for self-dual codes, IEEE Trans. Inform. Theory, **44**, 1998, 134 - 139.