2^n Bordered Constructions of Self-Dual codes from Group Rings

Steven T. Dougherty*
Department of Mathematics University of Scranton
Scranton, PA 18510
USA
Joe Gildea†,
University of Chester
Department of Mathematics
Chester, UK
Abidin Kaya‡
Sampoerna Academy, L'Avenue Campus
12780, Jakarta, Indonesia

November 7, 2019

Abstract

Self-dual codes, which are codes that are equal to their orthogonal, are a widely studied family of codes. Various techniques involving circulant matrices and matrices from group rings have been used to construct such codes. Moreover, families of rings have been used, together with a Gray map, to construct binary self-dual codes. In this paper, we introduce a new bordered construction over group rings for self-dual codes by combining many of the previously used techniques. The purpose of this is to construct self-dual codes that were missed using classical construction techniques by constructing self-dual codes with different automorphism groups. We apply the technique to codes over finite commutative Frobenius rings of characteristic 2 and several group rings and use these to construct interesting binary self-dual codes. In

*prof.steven.dougherty@gmail.com
†j.gildea@chester.ac.uk
‡abidin.kaya@sampoernaacademy.sch.id

particular, we construct some extremal self-dual codes length 64 and 68, constructing 30 new extremal self-dual codes of length 68.

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

1 Introduction

Self-dual codes are a well known and broadly studied class of codes. They are very interesting due, in part, to their connections to lattices and designs and applications in cryptography, invariant theory, and design theory. Much attention has been paid to the existence of extremal self-dual codes (codes that meet a certain bound) and to the many techniques used to construct these codes. In this paper, we shall introduce a new construction which is used to produce numerous self-dual codes. In particular, this construction seeks to construct codes that would be missed by other constructions.

A large number of techniques to produce self-dual codes involve circulant matrices, reverse circulant matrices and block circulant matrices. Recall that a circulant matrix is an $n \times n$ matrix obtained by considering the vector $(a_1, a_2, \ldots, a_n)$ and all its cyclic shifts (to the right) as rows. A reverse circulant matrix is an $n \times n$ matrix obtained by considering the vector $(a_1, a_2, \ldots, a_n)$ and all its cyclic shifts (to the left) as rows. A circulant block matrix is an $nl \times nt$ matrix by considering $(A_1, A_2, \ldots, A_n)$ and all its cyclic shifts (to the right) as rows where each A_i is a $l \times t$ matrix.

The double circulant construction is one of the most extensively applied constructions that is used to produce self-dual codes. It uses matrices of the form $(I|A)$ where A is a circulant matrix and A satisfies $AA^T = -I_n$. This technique was first introduced in the 1960s (see [4, 25]). It has been implemented significantly since its inception (see [17–21]).

In [26], Kaya et. al. modified the pure circulant construction where the matrix 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 [14], this construction was modified further to take the form:

$$\left(\begin{array}{cc} A & B \\ B^T & C \end{array}\right)$$

where A is a circulant matrix, B is a block circulant matrix (four blocks) and C is a matrix that arises from a group ring construction. In this work, we generalize this construction by letting A be a 2^n-circulant matrix, B be a block circulant matrix (2^n-blocks), and C be a matrix that arises from a group ring construction.

The motivation for these generalizations is to construct self-dual codes which are not previously known. In [12], it shown that using simpler forms can cause the automorphism group of the code to contain certain groups. We wish to alter the form so that codes with different automorphism groups can be found which leads to new codes, namely codes that do not contain certain groups in their automorphism groups.

It is well known that group rings can be very useful when constructing codes and in particular self-dual codes. In [1], the binary extended Golay code was constructed from an ideal of the group algebra $\mathbb{F}_2 S_4$ where $\mathbb{F}_2$ is the Galois field of two elements and S_4 is the symmetric group on four elements. An isomorphism between a group ring and a certain subring of the $n \times n$ matrices over the ring was introduced in [23]. It is shown in [24, 28] that this isomorphism can prove to be very useful in constructing self-dual codes. The $[48, 24, 12]$ Pless code was constructed using the group algebra $\mathbb{F}_2 D_{48}$ in [29] where D_{48} is the dihedral group of order 48. In [11, 12], 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. A connection between certain group ring elements and self-dual codes was established in [16].

In the following sections, we will provide important concepts required for later sections. Next, we will introduce our new construction and provide some important results relating to this construction. We will conclude with the implementation of this construction using MAGMA (see [2] 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. Next, we will introduce a family of rings called R_k. Additionally, we will introduce the ring $\mathbb{F}_4 + u\mathbb{F}_4$. We will finish 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

In this paper, all rings are assumed to be commutative, finite, Frobenius rings with a multiplicative identity. Denote the character module of R by $\widehat{R}$. Frobenius rings can be characterized as follows. For a finite ring R the following are equivalent:

- R is a Frobenius ring.
- As a left module, $\widehat{R} \cong {}_R R$.

- As a right module, $\widehat{R} \cong R_R$.

A code over a finite commutative ring R is said to be any subset C 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, specifically the inner-product is given by $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$. The orthogonal with respect to this inner-product is defined as $C^\perp = \{\mathbf{w} \mid \mathbf{w} \in R^n,\ [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{v} \in C\}$. The orthogonal is always a linear code. Since the ring is Frobenius, we have that for all linear codes over R, $|C||C^\perp| = |R|^n$. The proof of this theorem and a complete description of codes over finite commutative rings can be found in [11].

If a code satisfies the condition that $C = C^\perp$, then the code C is said to be a self-dual code. If the code satisfies the condition that $C \subseteq C^\perp$, then the code is said to be a self-orthogonal code. For binary codes, a self-dual code where all weights are congruent to 0 (mod 4) is said to be Type II and a self-dual binary code is said to be Type I otherwise. The bounds on the minimum distances for self-dual codes are given in [30] and are as follows.

Theorem 2.1. ([30]) *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 that meet these bounds are called *extremal*.

2.2 The family of rings R_k

In this subsection, we shall define a very important family of rings with characteristic 2, which we shall use extensively in our constructions.

We denote the family by R_k, these were first defined in [6] and [10]. For $k \geq 1$, define

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

Alternatively, we can define them recursively as:

$$R_k = R_{k-1}[u_k]/\langle u_k^2 = 0, u_k u_j = u_j u_k \rangle = R_{k-1} + u_k R_{k-1}. \tag{2}$$

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 $u_\emptyset = 1$. It follows that any element of R_k can be represented as

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

From this we can easily observe that

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

It follows that

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

It is shown in [10], that each R_k is a commutative, Frobenius ring with $|R_k| = 2^{(2^k)}$.

The following lemma can be found in [14].

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

We shall now define a Gray map from R_k to $\mathbb{F}_2^{2^k}$. This first appeared in [10]. 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 [6].

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

The next result, which was introduced in [9], 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 $\mathbb{F}_4[u]/\langle u^2 \rangle$. We 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 $\{u\omega, \omega, u, 1\}$.

In [15] and [8] the following Gray maps were introduced:

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

Those were generalized to the following maps in [27]:

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

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 [27].

Proposition 2.5. ([27]) *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

We shall now introduce group rings and a special isomorphism between the group ring and a certain subring of $n \times n$ matrices over a ring.

Throughout this article, let $\mathrm{circ}(a_1, a_2, \ldots, a_n)$ denote the $n \times n$ circulant matrix and let $\mathrm{CIRC}(A_1, A_2, \ldots, A_n)$ denote the circulant block $nl \times nt$ matrix where A_i is a $l \times t$ matrix. 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

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

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 restrict ourselves to finite groups since we are only concerned with using finite groups to construct codes by group rings. Throughout this paper, 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 [23], where it was done where the ring was a finite field. It was generalized to Frobenius rings in [12]. 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 $v = \sum_{i=1}^{n} \alpha_{g_i} \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be $\sigma(v) = (\alpha_{g_i^{-1} g_j})$ where $i, j \in \{1, \ldots, n\}$. 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. In this paper, we will be using group rings where the group has order 8 and the ring is a Frobenius, commutative and has characteristic 2. We will now describe $\sigma(v)$ for the following group rings RG where $G \in \{C_n, D_{2n}, C_m \times C_n, C_{mn}\}$.

- Let $G = \langle x \,|\, x^n = 1 \rangle \cong C_n$. If $v = \sum_{i=0}^{n-1} \alpha_{i+1} x^i \in RC_n$, then $\sigma(v) = \mathrm{circ}(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ where $\alpha_i \in R$.

- Let $G = \langle x, y \,|\, x^n = y^2 = 1,\ x^y = x^{-1} \rangle \cong D_{2n}$. If $v = \sum_{i=0}^{n-1} \sum_{j=0}^{1} \alpha_{i+nj+1} x^i y^j$, then

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

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

- Let $G = \langle x, y \,|\, x^n = y^m = 1,\ xy = yx \rangle \cong C_m \times C_n$ If $v = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha_{1+i+mj} x^i y^j \in R(C_m \times C_n)$, then

$$\sigma(v) = CIRC(A_1, \ldots, A_n)$$

  where $A_{j+1} = circ(\alpha_{1+mj}, \alpha_{2+mj}, \ldots, \alpha_{m+mj})$, $\alpha_i \in R$ and $m, n \geq 2$.

- Let $G = C_{m,n} = \langle x \,|\, x^{mn} = 1 \rangle$. If $v = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha_{1+i+mj} x^{ni+j} \in R\mathcal{C}_{m,n}$, then

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & \cdots & A_{n-1} & A_n \\ A'_n & A_1 & A_2 & A_3 & \cdots & A_{n-2} & A_{n-1} \\ A'_{n-1} & A'_n & A_1 & A_2 & \cdots & A_{n-3} & A_{n-2} \\ A'_{n-2} & A'_{n-1} & A'_n & A_1 & \cdots & A_{n-4} & A_{n-4} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ A'_3 & A'_4 & A'_5 & A'_6 & \cdots & A_1 & A_2 \\ A'_2 & A'_3 & A'_4 & A'_5 & \cdots & A'_n & A_1 \end{pmatrix}$$

where $A_{j+1} = circ(\alpha_{1+mj}, \alpha_{2+mj}, \ldots, \alpha_{m+mj})$, $A'_{j+1} = circ(\alpha_{m+mj}, \alpha_{1+mj}, \ldots, \alpha_{(m-1)+mj})$, $\alpha_i \in R$ and $m, n \geq 2$.

Before we proceed to the next section, we need to provide an important result regarding the determinant of a matrix of the form $\mathrm{CIRC}(A_1, A_2, \ldots, A_{p^m})$ where each A_i is a $p \times p$ circulant matrix over a finite commutative Frobenius ring of characteristic p, p is a prime and m is a positive integer.

We begin with some preliminary results.

In a slight departure from the previous notation, we shall consider a circulant matrix to be of the form:

$$\begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{pmatrix}. \tag{8}$$

This form enables us to index the matrix with $0, 1, \ldots, n-1$ and say that the entry $M_{i,j} = a_{i-j}$ where $i - j$ is done in the ring $\mathbb{Z}_n$. For any matrix M define the determinant of M by $|M|$. We shall take the Leibniz formula for the determinant of an n by n matrix which is

$$|M| = \sum_{\sigma \in \mathcal{S}_n} (sgn(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i}), \tag{9}$$

where $\mathcal{S}_n$ is the symmetric group on n letters. Recall that a transversal of the n by n grid is n coordinates where no two coordinates share a row or column. We note that there are $n!$ such transversals and that $|\mathcal{S}_n| = n!$. The determinant is then the sum of the product along all transversals where the sign in front of each product is given by the sign of the permutation σ. Note also that we are not assuming any algebraic structure among the elements of the matrix, that is we are proceeding strictly combinatorially.

Lemma 2.7. *Let M be the circulant matrix given in Equation (8). Then if the product $\prod_{k \in J} a_k$ appears in $|M|$ where $|J| > 1$ then the product $\prod_{k \in J} a_k$ appears n times.*

Proof. If the product appears in the transversal

$$a_{i_1,j_1}, a_{i_2,j_2}, \ldots, a_{i_n,j_n}$$

then it appears in the transversal

$$a_{i_1+1,j_1+1}, a_{i_2+1,j_2+1}, \ldots, a_{i_n+1,j_n+1}$$

since $i_k + 1 - (j_k + 1) = i_k - j_k$ and so the same n terms occur in the product as long as the two sets are not the same. The sets where they are the same occur at transversals $\{(i, j)\}$ where $i - j$ is a constant in the set. These correspond to the products a_i^n.

If σ is the permutation sending i_k to j_k, let σ' be the permutation sending i_k+1 to j_k+1, then σ and σ' are related by

$$\sigma' = (0, 1, 2, \ldots, n-1)\sigma(n-1, n-2, \ldots, 0).$$

Therefore, $sgn(\sigma) = sgn(\sigma')$ since $(0, 1, 2, \ldots, n-1)$ and $(n-1, n-2, \ldots, 0)$ have the same sign. □

Lemma 2.8. *Let M be the circulant matrix given in Equation (8), where the a_i come from a ring with characteristic p, a prime with $p = n$. Then*

$$|M| = a_0^n + a_1^n + \ldots a_{n-1}^n.$$

Proof. By Lemma 2.7 The coefficient of each term other than a_i^n is n and p divides n so each of those terms disappear.

Then the coefficient of a_i is $sgn(\sigma)$ where $\sigma(j) = j + i$. If p is 2, then $-1 = 1$ and if p is odd, then the sign of σ is 1. This gives the result. □

Since we have proceeded combinatorially, the next result follows easily.

Theorem 2.9. *Let $A = CIRC(A_1, A_2, \ldots, A_{p^m})$ where each A_i is a $p \times p$ circulant matrix over a finite commutative Frobenius ring of characteristic p, p is a prime and m is a positive integer. Then*

$$|A| = \sum_{i=1}^{p^m} |A_i|^{p^m}.$$

Proof. The proof is identical to the proof of Lemma 2.8, replacing a_i with $|A_i|$. □

3 Construction

At this point, we are now in a position to describe our construction.

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

$$M(\sigma) = \left(\begin{array}{c|cc} I_{2^n(p+1)} & A & B \\ & B^T & \sigma(v) \end{array} \right)$$

where $A = \text{circ}(a_1, \ldots, a_{2^n})$ and $B = \text{CIRC}(\mathbf{a_{2^n+1}}, \ldots, \mathbf{a_{2^{n+1}}})$. Let C_σ be a code that is generated by the matrix $M(\sigma)$. Then, the code C_σ has length $2^{n+1}(p+1)$. Now,

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

Note that

$$AA^T = \text{circ}\left(\sum_{i=1}^{2^n} a_i^2, \gamma_1, \gamma_2, \ldots, \gamma_{2^n-1}, 0, \gamma_{2^n-1}, \ldots, \gamma_2, \gamma_1 \right)$$

and

$$B^TB = \text{CIRC}(\mathbf{A_1}, \delta_\mathbf{1}, \delta_\mathbf{2}, \ldots, \delta_{\mathbf{2^n-1}}, \mathbf{0}, \delta_{\mathbf{2^n-1}}, \ldots, \delta_\mathbf{2}, \delta_\mathbf{1})$$

where γ_i are linear combinations of a_ia_j, $\delta_\mathbf{i}$ are linear combinations of $\mathbf{a_i a_j}$ and $\mathbf{A_1} = \sum_{i=2^n+1}^{2^{n+1}} \mathbf{a_i^T a_i}$.

Theorem 3.1. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite group of order 2^np where p is odd. Let*

$$M(\sigma) = \left(\begin{array}{c|cc} I_{2^n(p+1)} & A & B \\ & B^T & \sigma(v) \end{array} \right)$$

If $AA^T + BB^T + I = 0$, $AB + B\sigma(v^*) = 0$ and $B^TB + \sigma(vv^*) + I = 0$ then $C_\sigma = \langle M(\sigma) \rangle$ is a self-dual code of length $2^{n+1}(p+1)$.

Proof. Clearly, C_σ has free rank $2^n(p+1)$ as the left hand side of the generator matrix is the $2^n(p+1)$ by $2^n(p+1)$ identity matrix. If $AA^T + BB^T + I = 0$, $AB + B\sigma(v^*) = 0$ and $B^TB + \sigma(vv^*) + I = 0$ then C_σ is self-orthogonal and C_σ is self-dual. □

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

Theorem 3.2. *Let $M(\sigma)$ be a matrix satisfying the conditions in Theorem 3.1 over R_k.*

- *The matrix $M(\sigma)$ generates a self-dual C code over R_s for all $s \geq k$.*
- *Then $\phi_s(C_s)$ is a binary self-dual code of length $2^{n+s+1}(p+1)$.*

Proof. For the first item, the ring R_k is a subring of the ring R_s, whenever $k \leq s$. Therefore, the matrix M has free rank $2^n(p+1)$ over any ring where it is defined. If $\mathbf{v}$ and $\mathbf{w}$ are orthogonal over R_k then they are also 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 $2^{n+1}(p+1)$.

For the second item, it follows from this theorem and Theorem 2.3. □

Theorem 3.3. *Let $M(\sigma)$ be a matrix satisfying the conditions in Theorem 3.1 over R_1.*

- *The matrix $M(\sigma)$ generates a self-dual code C 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 $2^{n+3}(p+1)$.*

Proof. For the first item, 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 3.2.

The second item follows immediately from Corollary 2.6. □

Corollary 3.4. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order $2^n p$ where p is odd. Let C_σ be self-dual. If $B^T B = 0$, then $v \in RG$ is unitary.*

Proof. Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order $2^n p$ where p is odd. Let C_σ be self-dual. If $B^T B = 0$, then $\sigma(vv^*) + I = 0$ and $vv^* = 1$. Therefore v is unitary. □

Corollary 3.5. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order $2^n p$ where p is odd. Let C_σ be self-dual. If $\sum_{i=1}^{2^n} a_{i+2^n} = 1$, then $v \in RG$ is a non-unit.*

Proof. Assume that C_σ is self-dual and $\sum_{i=1}^{2^n} a_{i+2^n} = 1$. Now, $B^T B + I$ takes the form

$$B^T B = \mathrm{CIRC}(\mathbf{A_1}, \delta_\mathbf{1}, \delta_\mathbf{2}, \ldots, \delta_{\mathbf{2^n-1}}, \mathbf{0}, \delta_{\mathbf{2^n-1}}, \ldots, \delta_\mathbf{2}, \delta_\mathbf{1})$$

where $A_1 = circ(0, \underbrace{1, \ldots, 1}_{(p-1)-\text{times}})$. Using Theorem 2.9, we can see that

$$\begin{aligned} |B^T B + I| &= |\mathbf{A_1}|^{2^n} + |\delta_\mathbf{1}|^{2^n} + |\delta_\mathbf{2}|^{2^n} + \cdots + |\delta_{\mathbf{2^n-1}}|^{2^n} + |\delta_{\mathbf{2^n-1}}|^{2^n} + \cdots + |\delta_\mathbf{2}|^{2^n} + |\delta_\mathbf{1}|^{2^n} \\ &= |\mathbf{A_1}|^{2^n} + 2|\delta_\mathbf{1}|^{2^n} + 2|\delta_\mathbf{2}|^{2^n} + \cdots + 2|\delta_{\mathbf{2^n-1}}|^{2^n} \\ &= |\mathbf{A_1}|^{2^n}. \end{aligned}$$

Now,

$$|\mathbf{A_1}| = \begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix} = \begin{vmatrix} p-1 & p-1 & p-1 & \cdots & p-1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix} = (p-1) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = 0$$

since p is odd. Recall that $B^TB + \sigma(vv^*) + I = 0$ if C_σ is self-dual. Clearly $|\sigma(vv^*)| = 0$ since $|B^TB + I| = 0$. Therefore, vv^* is a non-unit by Corollary 3 in [23] and $v \in RG$ is a non-unit. □

4 Results

In this section, we will present the results obtained using this construction to construct self-dual codes when $n = 1$ and $p = 3$ and when $n = 3$ and $p = 1$. Self-dual codes when $n = 2$ and $p \in \{1, 3\}$ were constructed in [14].

4.1 Construction when $n = 1$ and $p = 3$

Here, we present the results for the above construction using $G = D_6$. We construct self-dual codes of length 64 by considering this construction over $\mathbb{F}_4 + u\mathbb{F}_4$.

We recall that the possible weight enumerators for a self-dual Type I $[64, 32, 12]$-code is given in [5, 7] 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 $W_{64,2}$.

Table 1: Extremal self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$ of length 64 from D_6.

$(a_1, \ldots, a_4)$	$(\alpha_1, \ldots, \alpha_6)$	$\lvert Aut(C)\rvert$	$W_{64,2}$	$(a_1, \ldots, a_4)$	$(\alpha_1, \ldots, \alpha_6)$	$\lvert Aut(C)\rvert$	$W_{64,2}$
$(1, 6, 8, 6)$	$(2, A, 9, 0, 9, F)$	$2^2 \cdot 3$	$\beta = 13$	$(1, 4, 8, 4)$	$(8, 8, 1, A, 3, D)$	$2^3 \cdot 3$	$\beta = 13$
$(2, 0, 6, 7)$	$(2, 9, 9, B, 6, D)$	$2^4 \cdot 3$	$\beta = 16$	$(0, 6, A, 5)$	$(1, 6, 7, 4, D, F)$	$2^2 \cdot 3$	$\beta = 19$
$(1, 4, 8, 4)$	$(B, 4, E, 0, 2, 6)$	$2^2 \cdot 3$	$\beta = 22$	$(9, 6, 2, 6)$	$(2, A, 1, 8, 3, D)$	$2^2 \cdot 3$	$\beta = 25$
$(4, 1, 4, 8)$	$(1, A, A, 7, 8, B)$	$2^3 \cdot 3$	$\beta = 25$	$(1, 4, 8, 4)$	$(A, 6, D, E, 5, F)$	$2^2 \cdot 3$	$\beta = 37$
$(2, 4, 9, 6)$	$(6, 3, 7, 4, F, F)$	$2^3 \cdot 3$	$\beta = 37$	$(0, 2, 6, 7)$	$(0, 9, 9, 9, 4, F)$	$2^4 \cdot 3^2$	$\beta = 40$
$(0, 2, 6, 7)$	$(0, 9, 9, 1, E, D)$	$2^4 \cdot 3$	$\beta = 64$				

4.2 Construction when $n = 3$ and $p = 1$

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 R_1.

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

$\mathcal{C}_i$	$(a_1, \ldots, a_{16})$	$(\alpha_1, \ldots, \alpha_8)$	$\lvert Aut(C)\rvert$	$W_{64,2}$
1	$(u,u,u,0,0,1,1,3,u,u,0,0,u,1,0,1)$	$(3,1,u,3,1,u,1,0)$	2^4	$\beta = 0$
2	$(u,u,0,0,0,1,1,3,u,0,u,0,u,1,u,3)$	$(1,1,0,3,3,u,1,0)$	2^6	$\beta = 0$
3	$(u,u,u,0,0,1,1,3,u,u,0,0,u,1,u,1)$	$(3,0,0,u,1,3,3,1)$	2^4	$\beta = 20$
4	$(u,u,0,0,0,1,1,3,u,u,u,u,u,1,0,3)$	$(1,u,u,0,3,1,3,3)$	2^5	$\beta = 20$
5	$(u,0,0,0,u,1,u,3,u,u,0,1,1,3,3,3)$	$(u,3,u,1,u,0,0,0)$	2^7	$\beta = 80$

4.3 New Self-Dual Codes of Length 68

The possible weight enumerator of a self-dual $[68, 34, 12]_2$-code is in one of the following forms by [3, 22]:

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

where $0 \leq \gamma \leq 9$. Recently, Yankov et al. constructed the first examples of codes with a weight enumerator for $\gamma = 7$ in [31]. In [13], [14] and [16], more unknown $W_{68,2}$ codes were constructed. Together with these, the existence of the codes in $W_{68,2}$ is known for;

$$\begin{aligned} \gamma &= 0,\ \beta \in \{2m \,|m = 0, 7, 11, 14, 17, 21 \ldots 99, 102, 105, 110, 119, 136, 165\}\ ;\ \text{or} \\ \beta &\in \{2m + 1 \,|m = 3, 5, 8, 10, 15, 16, 17, 20, \ldots, 82, 87, 93, 94, 101, 104, 110, 115\}\ ; \\ \gamma &= 1,\ \beta \in \{2m|m = 22, 24, \ldots, 99\}\ ;\ \text{or}\ \beta \in \{2m + 1|m = 24, \ldots, 85\}\ ; \\ \gamma &= 2,\ \beta \in \{2m \,|m = 29, \ldots, 100, 103, 104\}\ \text{or}\ \beta \in \{2m + 1 \,|m = 32, 34, \ldots, 79\}\ ; \\ \gamma &= 3,\ \beta \in \{2m \,|m = 40, \ldots, 92, 94, 95, 97, 98, 101, 102\}\ ;\ \text{or} \\ \beta &\in \{2m + 1|m = 43, \ldots, 77, 79, 80, 83, 96\}\ ; \\ \gamma &= 4,\ \beta \in \{2m \,|m = 43, 48, \ldots, 58, 60, \ldots, 92, 97, 98\}\ ;\ \text{or} \\ \beta &\in \{2m + 1 \,|m = 48, \ldots, 55, 58, 60, 61, 62, 64, 68, 69, 70, 71, 72, 74, 78, 80, 83, 84, 85\}\ ; \\ \gamma &= 5 \text{ with } \beta \in \{m|m = 113, 116, \ldots 153, 158, \ldots, 169\} \\ \gamma &= 6 \text{ with } \beta \in \{2m|m = 69, 77, 78, 79, 81, 88\} \\ \gamma &= 7 \text{ with } \beta \in \{7m|m = 14, \ldots, 39, 42\}\,. \end{aligned}$$

In this section we extend certain codes of length 64 (from Table 4.2) using Theorem 2.4 to construct new codes of length 68.

Table 3: Type I Extremal Self-dual code of length 68 from C_8 over R_1.

$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β	$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β
1	1	$u+1$	(13u30131100u111u000030u11u3u1uu0)	**4**	**88**	2	1	$u+1$	(0010u13330u1303uu3u101103101013u)	**4**	**118**
3	2	1	(0u0uu01u3uu0u0103uu133u3uu11u311)	**0**	**37**	4	2	$u+1$	(11100u3u30333303330u030331uu1110)	**3**	**83**
5	3	$u+1$	(10130u11u33uu3u103uuu01030u1u13u)	**4**	**127**	6	3	$u+1$	(11u3u33uuu11u31u3311u303013uuu0u)	**4**	**131**
7	3	1	(33u0u13101u00u30110311011uu0u030)	**4**	**133**	8	3	$u+1$	(1u0u1103310u13130301001031331333)	**4**	**135**
9	3	1	(00u13u100110uu133u0uu0u33u11u113)	**4**	**147**	10	3	$u+1$	(uuu13uu13001310001u130u311001010)	**4**	**151**
11	3	$u+1$	(113010330u000u13130u1033330011u0)	**4**	**153**	12	3	1	(u3111313011u30uu0003uuu33u003111)	**4**	**155**
13	4	$u+1$	(030u1u100u110uuu1111103011013u00)	**5**	**155**	14	4	1	(301u11u11u1131u311113311uu103u00)	**5**	**157**
15	4	1	(0001uuu11u0u10331303111113311u10)	**5**	**175**	16	4	1	(3110u13333110101000011111333003)	**5**	**177**
17	5	$u+1$	(11u0000u30u310003u33313u30101u10)	**1**	**204**	18	5	1	(0303u1u30300u30000u0003313u0uu10)	**3**	**186**
19	5	$u+1$	(3013303131113uu3010u30001130u33u)	**3**	**192**						

4.4 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 be a self-dual code of length 68. In order to reduce the search field, 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. As neighbors of codes in Table 3, we obtain eleven new codes, which are listed in Table 4. The first 34 entries of x are set to be 0, the rest of the vectors are listed in Table 4. All the codes have an automorphism group of order 2.

Table 4: New codes of length 68 as neighbors of codes in Table 3

$\mathcal{N}_{68,i}$	$\mathcal{C}_{68,i}$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
$\mathcal{N}_{68,1}$	$\mathcal{C}_{68,17}$	(01010011110100011111011110011111000)	**1**	**175**
$\mathcal{N}_{68,2}$	$\mathcal{C}_{68,16}$	(10001100011001001011010100100100)	**5**	**154**
$\mathcal{N}_{68,3}$	$\mathcal{C}_{68,15}$	(10110110111111100000100100000110011)	**5**	**156**
$\mathcal{N}_{68,4}$	$\mathcal{C}_{68,16}$	(11010010001001111101011110111101010)	**5**	**170**
$\mathcal{N}_{68,5}$	$\mathcal{C}_{68,15}$	(01010111110000011010001000101110001)	**5**	**171**
$\mathcal{N}_{68,6}$	$\mathcal{C}_{68,16}$	(00101000000001010001000111011011111)	**5**	**172**
$\mathcal{N}_{68,7}$	$\mathcal{C}_{68,16}$	(01010011010111011010100101000011111)	**5**	**176**
$\mathcal{N}_{68,8}$	$\mathcal{C}_{68,16}$	(11110011011100011011011001101101000)	**5**	**178**
$\mathcal{N}_{68,9}$	$\mathcal{C}_{68,15}$	(11000010011011111011110001010111)	**5**	**179**
$\mathcal{N}_{68,10}$	$\mathcal{C}_{68,16}$	(01000011111001111100101010011100010)	**5**	**180**
$\mathcal{N}_{68,11}$	$\mathcal{C}_{68,15}$	(01000110100101110100011111111001100)	**5**	**181**

5 Conclusion

In this work, we generalise a previous construction that was described in [14]. We establish conditions when this construction produces self-dual codes and we provide a connection between certain group ring elements and self-dual codes. We highlight the significance of this construction by constructing many new extremal self-dual codes. In particular, we construct the following unknown $W_{68,2}$ codes:

$(\gamma = 0, \quad \beta = \{37\})$,
$(\gamma = 1, \quad \beta = \{175, 204\})$,
$(\gamma = 3, \quad \beta = \{83, 186, 192\})$,
$(\gamma = 4, \quad \beta = \{88, 106, 118, 127, 131, 133, 135, 147, 151, 153, 155\})$ and
$(\gamma = 5, \quad \beta = \{154, 155, 156, 157, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181\})$.

Due to computational limitations, we were restricted to small values of n and p. Investigating larger values of n and p would yield more results with higher computational power. One could also consider 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 **55** (1990), no. 2, 235–246.

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).

[3] S. Buyuklieva and I. Boukliev, *Extremal self-dual codes with an automorphism of order* 2, IEEE Trans. Inform. Theory **44** (1998), no. 1, 323–328.

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

[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 **36** (1990), no. 6, 1319–1333.

[6] S. T. Dougherty, B. Yıldız, and S. Karadeniz, *Self-dual codes over R_k and binary self-dual codes*, Eur. J. Pure Appl. Math. **6** (2013), no. 1, 89–106.

[7] S. T. Dougherty, T. A. Gulliver, and M. Harada, *Extremal binary self-dual codes*, IEEE Trans. Inform. Theory **43** (1997), no. 6, 2036–2047.

[8] S. T. Dougherty, P. Gaborit, M. Harada, and P. Solé, *Type II codes over $\mathbf{F}_2 + u\mathbf{F}_2$*, IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45.

[9] S. T. Dougherty, J. L. Kim, H. Kulosman, and H. Liu, *Self-dual codes over commutative Frobenius rings*, Finite Fields Appl. **16** (2010), no. 1, 14–26.

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

[11] S. T. Dougherty, *Algebraic coding theory over finite commutative rings*, SpringerBriefs in Mathematics, Springer, Cham, 2017.

[12] 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 Cryptogr. **86** (2018), no. 9, 2115–2138.

[13] S. T. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylyshchak, and Bahattin Yildiz, *Bordered constructions of self-dual codes from group rings and new extremal binary self-dual codes*, Finite Fields Appl. **57** (2019), 108–127.

[14] S. T. Dougherty, J. Gildea, and A. Kaya, *Quadruple Bordered Constructions of Self-Dual codes from Group Rings over Frobenius Rings*, Cryptogr. Commun. **https://doi.org/10.1007/s12095-019-00380-8** (2019).

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

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

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

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

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

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

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

[22] M. Harada and A. Munemasa, *Some restrictions on weight enumerators of singly even self-dual codes*, IEEE Trans. Inform. Theory **52** (2006), no. 3, 1266–1269.

[23] T. Hurley, *Group rings and rings of matrices*, Int. J. Pure Appl. Math. **31** (2006), no. 3, 319–335.

[24] T. Hurley, *Self-dual, dual-containing and related quantum codes from group rings*, Int. J. Pure Appl. Math. **arXiv:0711.3983** (2007).

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

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

[27] S. Ling and P. Solé, *Type II codes over* $\mathbf{F}_4 + u\mathbf{F}_4$, European J. Combin. **22** (2001), no. 7, 983–997.

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

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

[30] E. M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 134–139.

[31] N. Yankov, M. Ivanova, and Moon Ho Lee, *Self-dual codes with an automorphism of order 7 and s-extremal codes of length 68*, Finite Fields Appl. **51** (2018), 17–30.