New Self-Dual Codes of Length 68 from a 2×2 Block Matrix Construction and Group Rings

M. Bortos[†], J. Gildea[⋆], A. Kaya[‡], A. Korban[⋆], and A. Tylyshchak[†]

[†]Department of Algebra, Uzhgorod National University, Uzhgorod, Ukraine
[⋆]Department of Mathematical and Physical Sciences, University of Chester, UK
[‡]Harmony School of Technology, Houston, TX 77038, USA

August 6, 2020

Abstract

Many generator matrices for constructing extremal binary self-dual codes of different lengths have the form $G = (I_n \mid A)$, where I_n is the $n \times n$ identity matrix and A is the $n \times n$ matrix fully determined by the first row. In this work, we define a generator matrix in which A is a block matrix, where the blocks come from group rings and also, A is not fully determined by the elements appearing in the first row. By applying our construction over $\mathbb{F}_2 + u\mathbb{F}_2$ and by employing the extension method for codes, we were able to construct new extremal binary self-dual codes of length 68. Additionally, by employing a generalised neighbour method to the codes obtained, we were able to construct many new binary self-dual $[68, 34, 12]$-codes with the rare parameters $\gamma = 7, 8$ and 9 in $W_{68,2}$. In particular, we find 92 new binary self-dual $[68, 34, 12]$-codes.

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

1 Introduction

There has been a great interest and focus on constructing binary self-dual codes of different lengths with new weight enumerators. Researchers have employed different methods and tools to search for these codes and as a result, many new codes have been discovered. For example, a classical approach is to use a generator matrix of the form $G = (I_n \mid A)$, where I_n is the $n \times n$ identity matrix and A is a special matrix, for example, a circulant matrix.

Please see [6, 13, 18] for example. Another well known method is to search for self-dual codes over rings, and then to consider their binary images to produce extremal binary self-dual codes with new weight enumerators. Please see [4, 9, 10, 16] for examples. The well known extension and neighbour methods [10] can also be used to search for new extremal binary self-dual codes. Recently, the neighbour method has been generalised in [12] so that the k^{th} range of neighbours can be constructed leading to finding new self-dual codes. This generalised method turned out to be a very powerful tool as many new codes can be obtained by considering the family of neighbours of just one code. Please see [12] for details.

In this work, we present a generator matrix of the form $M_\sigma = (I_n \mid A)$, where A is a block matrix obtained from group rings. Similar generator matrices can be found in [6, 13]. Our construction differs from the generator matrices known in the literature, since we make sure that the block matrix A is not fully determined by the blocks appearing in the first row- this has been the case in the generator matrices known in the literature [6, 13]. By defining the block matrix A in this way, we force the search field to be greater than in the standard generator matrices which leads us to finding self-dual codes that are not attainable from other techniques. By applying our construction over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, by considering the binary images and by employing the well known extension method, the neighbour technique and its generalisation, we find new extremal binary self-dual codes of length 68. In particular, we find such codes with new weight enumerators for the rare parameters $\gamma = 7, 8$ and 9.

The rest of the paper is organised as follows. In Section 2, we give preliminary definitions and results on self-dual codes, the alphabets to be used, group rings, the well known extension method, the neighbour technique and its generalization from [12]. In Section 3, we introduce the new construction and give theoretical results. We show when our construction produces self-dual codes. In Section 4, we apply our main construction over the alphabet $\mathbb{F}_2 + u\mathbb{F}_2$ and consider their binary images to find extremal binary self-dual codes of length 64. We next apply the extension method to search for binary self-dual codes with parameters $[68, 34, 12]$. Lastly, we employ the neighbour technique and its generalisation to find extremal binary self-dual codes of length 68 with weight enumerators that were not known in the literature before. In particular, we find codes with new weight enumerator with the rare parameters $\gamma = 7, 8$ and 9. Altogether, we find 98 new extremal binary self-dual codes of length 68. We also tabulate all the numerical results in this section. We finish with concluding remarks and directions for possible future research.

2 Preliminaries

2.1 Self-Dual Codes, the Ring $\mathbb{F}_2+u\mathbb{F}_2$, Group Rings and the Well Known Extension and Neighbor Methods

We begin by recalling the standard definitions from coding theory. A code C of length n over a Frobenius ring R is a subset of R^n. If the code is a submodule of R^n then we say that the code is linear. Elements of the code C are called codewords of C. Let $\mathbf{x}=(x_1,x_2,\ldots,x_n)$ and $\mathbf{y}=(y_1,y_2,\ldots,y_n)$ be two elements of R^n. The duality is understood in terms of the Euclidean inner product, namely:

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

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

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

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

An upper bound on the minimum Hamming distance of a binary self-dual code was given in [19]. Specifically, let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a Type I and Type II binary code of length n, respectively. Then

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

and

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

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

2.2 The ring $\mathbb{F}_2+u\mathbb{F}_2$

In this section, we recall some theory on self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$. We refer to [4] where Type II, Type IV, self-dual codes and cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ have been studied.

The ring $\mathbb{F}_2+u\mathbb{F}_2$ is a ring of characteristic 2 with 4 elements with the restriction $u^2=0$. It is defined as

$$\mathbb{F}_2+u\mathbb{F}_2=\{a+bu \mid a,b\in\mathbb{F}_2, u^2=0\},$$

and it is easily seen that $\mathbb{F}_2+u\mathbb{F}_2\cong\mathbb{F}_2[x]/(x^2)$. A linear code C of length n over the ring $\mathbb{F}_2+u\mathbb{F}_2$ is an $\mathbb{F}_2+u\mathbb{F}_2$-submodule of $(\mathbb{F}_2+u\mathbb{F}_2)^n$. The elements of $\mathbb{F}_2+u\mathbb{F}_2$ are $0,1,u,1+u$

and their Lee weights are defined as $0, 1, 2, 1$ respectively. The Hamming (d_H) and Lee (d_L) distance between n tuples is then defined as the sum of the Hamming and Lee weights of the difference of the components of these tuples respectively. The smallest positive Hamming and Lee distance of a code C is denoted by $d_H(C)$ and $d_L(C)$ respectively.

A Gray map ϕ is defined as

$$\phi : (\mathbb{F}_2 + u\mathbb{F}_2) \to \mathbb{F}_2^{2n},$$

$$\phi(\mathbf{a} + \mathbf{b}u) = (\mathbf{b}, \mathbf{a} + \mathbf{b}),$$

where $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$. The map is a distance preserving isometry from $((\mathbb{F}_2 + u\mathbb{F}_2)^n, d_L)$ to $(\mathbb{F}_2^{2n}, d_H)$, where d_L and d_H denote the Lee and Hamming distance in $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ and $\mathbb{F}_2^{2n}$ respectively. This means that if C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ with parameters $[n, 2^k, d]$ (2^k is the number of the codewords), then $\phi(C)$ is a binary linear code of parameters $[2n, k, d]$. The following theorem is a natural result of the Gray map.

Theorem 2.1. *([16]) If C is a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length n, then $\phi(C)$ is a self-dual binary code of length $2n$.*

We can also define a natural projection from $\mathbb{F}_2 + u\mathbb{F}_2$ to $\mathbb{F}_2$ as follows:

$$\mu : \mathbb{F}_2 + u\mathbb{F}_2 \to \mathbb{F}_2,$$

$$\mu(a + bu) = a.$$

If $D = \mu(C)$ for some linear code C over $\mathbb{F}_2 + u\mathbb{F}_2$, we say that D is a projection of C into $\mathbb{F}_2$, and that C is a lift of D into $\mathbb{F}_2 + u\mathbb{F}_2$. It is clear that the projection of a self-orthogonal code is self-orthogonal, but the projection of a self-dual code need not be self-dual. We now state two well known results which we apply later in our work when searching for self-dual codes.

Theorem 2.2. *([16]) Suppose that C is a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $2n$, generated by the matrix $[I_n|A]$, where I_n is the $n \times n$ identity matrix. Then $\mu(C)$ is a self-dual binary code of length $2n$.*

Theorem 2.3. *([16]) Suppose C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ and that $C' = \mu(C)$, is its projection to $\mathbb{F}_2$. With d and d' representing the minimum Lee and Hamming distances of C and C' respectively, we have that $d \leq 2d'$.*

For the computational results in later sections, we are going to use the following extension method to obtain codes of length $n + 2$.

Theorem 2.4. *([10]) Let $\mathcal{C}$ be a self-dual code of length n over a commutative Frobenius ring with identity R and $G = (r_i)$ be a $k \times n$ 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 such that $c^2 = -1$ and X be a vector in S^n with $\langle X, X\rangle = -1$. Let $y_i = \langle r_i, X\rangle$ for $1 \leq i \leq k$. The following matrix*

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

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

We will also apply the neighbor method and its generalization to search for new extremal binary self-dual codes from codes obtained directly from our main construction or from the described above, extension method. Two self-dual binary codes of length $2n$ are said to be neighbours of each other if their intersection has dimension $n-1$. Let $x \in \mathbb{F}_2^{2n} \setminus \mathcal{C}$ then $\mathcal{D} = \left\langle \langle x\rangle^{\perp} \cap \mathcal{C}, x \right\rangle$ is a neighbour of $\mathcal{C}$.

Recently in [12], the neighbor method has been extended and the following formula for constructing the k^{th}-range neighbour codes was provided:

$$\mathcal{N}_{(i+1)} = \left\langle \langle x_i\rangle^{\perp} \cap \mathcal{N}_{(i)}, x_i \right\rangle,$$

where $\mathcal{N}_{(i+1)}$ is the neighbour of $\mathcal{N}_{(i)}$ and $x_i \in \mathbb{F}_2^{2n} - \mathcal{N}_{(i)}$.

2.3 Group Rings

We first give the definitions of some special matrices which we use later in our work. A circulant matrix is one where each row is shifted one element to the right relative to the preceding row. We label the circulant matrix as $A = circ(\alpha_1, \alpha_2 \ldots, \alpha_n)$, where α_i are ring elements. A block-circulant matrix is one where each row contains blocks which are square matrices. The rows of the block matrix are defined by shifting one block to the right relative to the preceding row. We label the block-circulant matrix as $CIRC(A_1, A_2, \ldots A_n)$, where A_i are $k \times k$ matrices over the ring R. The transpose of a matrix A, denoted by A^T, is a matrix whose rows are the columns of A, i.e., $A^T_{ij} = A_{ji}$. We finish this section by giving the necessary definitions for group rings and by recalling the map that sends a group ring element $v \in RG$ to a $n \times n$ matrix over R.

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

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

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

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

$$\left(\sum_{i=1}^{n}\alpha_i g_i\right)\left(\sum_{j=1}^{n}\beta_j g_j\right)=\sum_{i,j}\alpha_i\beta_j g_i g_j. \tag{2}$$

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

The following construction of a matrix was first given for codes over fields by Hurley in [15]. It was extended to Frobenius rings in [8]. Let R be a finite commutative Frobenius ring and let $G=\{g_1,g_2,\dots,g_n\}$ be a group of order n. Let $v=\sum_{i=1}^{n}\alpha_{g_i}\in RG$. Define the matrix $\sigma(v)\in M_n(R)$ to be $\sigma(v)=(\alpha_{g_i^{-1}g_j})$ where $i,j\in\{1,2,\cdots,n\}$.

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

(i) Let $C_n=\langle x\mid x^n=1\rangle$ and set our listing of C_n to be $\{1,x,x^2,\dots,x^{n-1}\}$. Let $v=\sum_{i=0}^{n-1}\alpha_i x^i\in RC_n$ where $\alpha_i\in R$, where R is a ring, then

$$\sigma(v)=circ(\alpha_0,\alpha_1,\dots,\alpha_{n-1}). \tag{3}$$

(ii) Let $G=\langle x,y\mid x^4=y^2=1,x^y=x^{-1}\rangle\cong D_8$. If $v=\sum_{i=0}^{3}\alpha_{i+1}x^i+\alpha_{i+5}x^iy\in RD_8$, then

$$\sigma(v)=\begin{pmatrix}A & B\\ B^T & A^T\end{pmatrix} \tag{4}$$

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

We also recall the canonical involution $*:RG\to RG$ on a group ring RG is given by $v^*=\sum_g\alpha_g g^{-1}$, for $v=\sum_g\alpha_g g\in RG$. An important connection between v^* and v appears when we take their images under the σ map:

$$\sigma(v^*)=\sigma(v)^T. \tag{5}$$

If v satisfies $vv^*=1$, then we say that v is a unitary unit in RG.

3 Main Construction

In this section, we present the main construction in this work. Let $v_i\in RG$ where R is a finite commutative Frobenius ring of characteristics 2 with $1\le i\le 3$ and G be a finite group of order n. Define the following matrix:

$$M_\sigma=\left[\begin{array}{c|cc} I_{2n} & \sigma(v_1) & \sigma(v_2)\\ & \sigma(v_2) & \sigma(v_3)\end{array}\right]. \tag{6}$$

Let C_σ be a code that is generated by the matrix M_σ. Then, the code C_σ has length $4n$. We now state the main result of this work.

Theorem 3.1. *Let R be a finite commutative Frobenius ring of characteristics 2 and let G be a finite group of order n. Then C_σ is a self-dual code of length $4n$ if and only if*

$$v_1v_1^* + v_2v_2^* = 1, \tag{7}$$

$$v_1v_2^* + v_2v_3^* = 0, \tag{8}$$

$$v_2v_1^* + v_3v_2^* = 0, \tag{9}$$

$$v_2v_2^* + v_3v_3^* = 1. \tag{10}$$

Proof. The code generated will be self-dual if and only if $M_\sigma M_\sigma^T$ is the zero matrix over R. Since M_σ is of the form $(I \mid A)$, where

$$A = \begin{pmatrix} \sigma(v_1) & \sigma(v_2) \\ \sigma(v_2) & \sigma(v_3) \end{pmatrix},$$

it is enough to show that $AA^T = I_{2n}$. Now,

$$AA^T = \begin{pmatrix} \sigma(v_1) & \sigma(v_2) \\ \sigma(v_2) & \sigma(v_3) \end{pmatrix} \begin{pmatrix} \sigma(v_1^*) & \sigma(v_2^*) \\ \sigma(v_2^*) & \sigma(v_3^*) \end{pmatrix} = \begin{pmatrix} \sigma(v_1v_1^* + v_2v_2^*) & \sigma(v_1v_2^* + v_2v_3^*) \\ \sigma(v_2v_1^* + v_3v_2^*) & \sigma(v_2v_2^* + v_3v_3^*) \end{pmatrix}.$$

Clearly, $AA^T = I_{2n}$ iff $\sigma(v_1v_1^* + v_2v_2^*) = I_n$, $\sigma(v_1v_2^* + v_2v_3^*) = 0$, $\sigma(v_2v_1^* + v_3v_2^*) = 0$ and $\sigma(v_2v_2^* + v_3v_3^*) = I_n$. But there $I_n = \sigma(1)$ and $0 = \sigma(0)$. Moreover for any $u, v \in RG$ we have $\sigma(u) = \sigma(v)$ iff the first rows of $\sigma(u)$ and $\sigma(v)$ are the same. It implies that $\sigma(u) = \sigma(v)$ iff $u = v$. So $AA^T = I_{2n}$ iff (7–10). □

We have immediately that the code has free rank $2n$ by construction. It is also obvious from the construction that the search field of M_σ when searching for self-dual codes over R is $|R|^{3n}$. We note that the blocks $\sigma(v_1)$, $\sigma(v_2)$ and $\sigma(v_3)$ are independent of each other which makes our construction different than the usual constructions. A typical generator matrix of a self-dual code has the form $(I|A)$ where A is a special matrix in which the rows are simply permutations of the first row, for example, a circulant or reverse-circulant matrices. In our construction, the block $\sigma(v_3)$ makes the difference, namely, the rows in the matrix M_σ are no longer permutations of the elements of the first row because of $\sigma(v_3)$. If $v_1 = v_3$ then the matrix M_σ consists of rows which are permutations of the elements in the first row, but because v_3 is independent of v_1 and v_2 this is not the case in general.

Theorem 3.2. *Let R be a finite commutative Frobenius ring of characteristics 2 and let G be a finite group of order n. Then C_σ is a self-dual code of length $4n$ if and only if*

$$v_1v_1^* + v_2v_2^* = 1, \tag{11}$$

$$v_1v_2^* + v_2v_3^* = 0, \tag{12}$$

$$v_1v_1^* + v_3v_3^* = 0. \tag{13}$$

Proof. Let $v_i \in RG$ and $v_i^* \in RG$ $(i = 1, 2, 3)$ satisfy the conditions of (7)–(10). Considering any $v, u \in RG$ for which $(v+u)^* = v^*+u^*$, $(vu)^* = u^*v^*$ and $(v^*)^* = v$, we get $(v_1v_2^*+v_2v_3^*)^* = v_2v_1^* + v_3v_2^*$. It follows from (8) that $v_2v_1^* + v_3v_2^* = 0^* = 0$ and (9) also holds. Adding (7) to (10) we obtain $v_1v_1^* + v_3v_3^* = 0$. This concludes the proof. □

Let $v = \sum_{g\in G} \alpha_g g$ be an element in RG $(\alpha_g \in R)$. Then, $\sum_{g\in G} \alpha_g \in R$ is the augmentation (denoted by $\varepsilon(v)$) of v. It is obvious that ε is a ring homomorphism and that $\varepsilon(v^*) = \varepsilon(v)$.

Lemma 3.3. *Let $R = \mathbb{F}_2$ be the field of two elements and let G be a finite group of order n. If C_σ is a self-dual code of length $4n$ then $(\varepsilon(v_1), \varepsilon(v_2), \varepsilon(v_3)) \in \{(0, 1, 0),\ (1, 0, 1)\}$.*

Proof. We apply the ring homomorphism ε to equations (11)–(13). We obtain:

$$\varepsilon(v_1)^2 + \varepsilon(v_2)^2 = 1,$$

$$\varepsilon(v_1)\varepsilon(v_2) + \varepsilon(v_2)\varepsilon(v_3) = 0,$$

$$\varepsilon(v_1)^2 + \varepsilon(v_3)^2 = 0.$$

From the third equation we have that $(\varepsilon(v_1) + \varepsilon(v_3))^2 = 0$ or $\varepsilon(v_1) = \varepsilon(v_3)$. Now considering the first condition $(\varepsilon(v_1) + \varepsilon(v_2) + 1)^2 = 0$, we have $\varepsilon(v_1) + 1 = \varepsilon(v_2)$. Therefore we obtain that

$$(\varepsilon(v_1), \varepsilon(v_2), \varepsilon(v_3)) = (\varepsilon(v_1), \varepsilon(v_1) + 1, \varepsilon(v_1)).$$

So $(\varepsilon(v_1), \varepsilon(v_2), \varepsilon(v_3)) \in \{(0, 1, 0),\ (1, 0, 1)\}$. □

Lemma 3.4. *Let $R = \mathbb{F}_2+u\mathbb{F}_2$ and let G be a finite group of order n. If C_σ is a self-dual code of length $4n$ then $(\varepsilon(v_1), \varepsilon(v_2), \varepsilon(v_3)) \in \{(0, 1, 0),\ (0, 1 + u, 0),\ (1, 0, 1),\ (1, 0, 1 + u),\ (1, u, 1),\ (1, u, 1+u),\ (u, 1, u),\ (u, 1+u, u),\ (1+u, 0, 1),\ (1+u, 0, 1+u),\ (1+u, u, 1),\ (1+u, u, 1+u)\}$.*

Proof. We apply the ring homomorphism ε to equations (11)–(13). We obtain:

$$\varepsilon(v_1)^2 + \varepsilon(v_2)^2 = 1,$$

$$\varepsilon(v_1)\varepsilon(v_2) + \varepsilon(v_2)\varepsilon(v_3) = 0,$$

$$\varepsilon(v_1)^2 + \varepsilon(v_3)^2 = 0.$$

From the third equation we have that $(\varepsilon(v_1) + \varepsilon(v_3))^2 = 0$. Then $\varepsilon(v_1) = \varepsilon(v_3)$ or $\varepsilon(v_1) + u = \varepsilon(v_3)$. From the second equation: $\varepsilon(v_2)(\varepsilon(v_1) + \varepsilon(v_3)) = 0$. If $\varepsilon(v_1) = \varepsilon(v_3)$ then

$\varepsilon(v_2)\cdot 0 = 0$. If $\varepsilon(v_1)+u=\varepsilon(v_3)$ then $\varepsilon(v_2)\cdot u = 0$, so in this case either $\varepsilon(v_2)=0$ or $\varepsilon(v_2)=u$. Therefore we obtain

$$(\varepsilon(v_1),\varepsilon(v_2),\varepsilon(v_3)) = (\varepsilon(v_1),\varepsilon(v_2),\varepsilon(v_1))$$

if $\varepsilon(v_1)=\varepsilon(v_3)$ and

$$(\varepsilon(v_1),\varepsilon(v_2),\varepsilon(v_3)) \in \{(\varepsilon(v_1),0,u+\varepsilon(v_1)),\ (\varepsilon(v_1),u,u+\varepsilon(v_1))$$

in the other case. Now considering the first condition $(\varepsilon(v_1)+\varepsilon(v_2)+1)^2=0$. We have $\varepsilon(v_1)+1=\varepsilon(v_2)$ or $\varepsilon(v_1)+1+u=\varepsilon(v_2)$. Therefore we obtain that $(\varepsilon(v_1),\ \varepsilon(v_2),\ \varepsilon(v_3)) \in \{(0,1,0),\ (0,1+u,0),\ (1,0,1),\ \ (1,0,1+u),\ (1,u,1),\ (1,u,1+u),\ (u,1,u),\ (u,1+u,u),$ $(1+u,0,1),\ (1+u,0,1+u),(1+u,u,1),\ (1+u,u,1+u)\}$. □

The group C_8 and D_8 contain subgroups of order 4. Let G be a finite group of order $2n$, H be a subgroup of order n, $v=\sum_{g\in G}\alpha_g g$ be an element in RG ($\alpha_g\in R$). Let $\sum_{g\in H}\alpha_g \in RG$ and $\sum_{g\in G\backslash H}\alpha_g \in RG$ be the partial augmentation (denoted by $\varepsilon_H(v)$, $\varepsilon_{G\backslash H}(v)$) of v. Since $g\in H$ iff $g^{-1}\in H$ we have that $\varepsilon_H(v^*)=\varepsilon_H(v)$, $\varepsilon_{G\backslash H}(v^*)=\varepsilon_{G\backslash H}(v)$.

Lemma 3.5. *Let R be a commutative Frobenius ring of characteristics 2, G be a finite group of order $2n$, H be a subgroup of order n and $C_2=\{1,x\}$ be a group of order 2. Let $\varphi:\ v\to\varepsilon_H(v)+x\varepsilon_{G\backslash H}(v)$ be a ring homomorphism $\varphi:\ RG\to RC_2$. Here, $\varphi(v^*)=\varphi(v)$ for any $v\in RG$.*

Proof. It is obvious that H is a subgroup of G of index $[G:H]=2$. Thus

$$g\to\begin{cases}1 & \text{if}\quad g\in H,\\ x & \text{if}\quad g\in G\backslash H\end{cases}$$

is a group homomorphism from G to C_2. Then for any $\alpha_g\in R$ we have the following ring homomorphism $\varphi:\ RG\to RC_2$:

$$v=\sum_{g\in G}\alpha_g g=\sum_{g\in H}\alpha_g g+\sum_{g\in G\backslash H}\alpha_g g\to\sum_{g\in H}\alpha_g+\sum_{g\in G\backslash H}\alpha_g x=\varepsilon_H(v)+\varepsilon_{G\backslash H}(v)x.$$

Moreover, for any $v\in RG$, we get

$$\varphi(v^*)=\varepsilon_H(v^*)+\varepsilon_{G\backslash H}(v^*)x=\varepsilon_H(v)+\varepsilon_{G\backslash H}(v)x=\varphi(v).$$

□

Theorem 3.6. *Let R be a finite commutative Frobenius ring of characteristics 2, G be a finite group of order $2n$, and H be a subgroup of order n. If C_σ is a self-dual code of length $4n$ then*

$$(\varphi(v_1)+\varphi(v_2))^2=1,\ \varphi(v_2)(\varphi(v_1)+\varphi(v_3))=0,\ (\varphi(v_1)+\varphi(v_3))^2=0. \tag{14}$$

Proof. Applying the ring homomorphism $\varphi:\ u \to \varepsilon_H(u) + x\varepsilon_{G\setminus H}(u)$ to equations (11)–(13), we get

$$\varphi(v_1)^2 + \varphi(v_2)^2 = 1,\ \varphi(v_1)\varphi(v_2) + \varphi(v_2)\varphi(v_3) = 0,\ \varphi(v_1)^2 + \varphi(v_3)^2 = 0.$$

This concludes the proof. □

Lemma 3.7. *Let $R = \mathbb{F}_2$ be the field of two elements and G be a finite group of order $2n$, H be a subgroup of order n. If C_σ is a self-dual code of length $4n$ then* $(\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_2), \varepsilon_{G\setminus H}(v_2), \varepsilon_H(v_3), \varepsilon_{G\setminus H}(v_3)) \in \{(0,0,1,0,0,0),\ (0,1,1,1,0,1),\ (1,0,0,0,1,0),\ (1,1,0,1,1,1),\ (0,0,0,1,0,0),\ (0,1,0,0,0,1),\ (1,0,1,1,1,0),\ (1,1,1,0,1,1),\ (0,1,1,1,1,0),\ (0,1,0,0,1,0),\ (1,0,0,0,0,1),\ (1,0,1,1,0,1)\}$.

Proof. From the equations in (14), we have that if $\mathbb{F}_2C_2 = \{0, 1, x, 1+x\}$ ($x^2 = 1$) then $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) \in \{1, x\}$, $\varphi(v_1 + v_3) = \varphi(v_1) + \varphi(v_3) \in \{0, 1+x\}$.

Now, let $\varphi(v_1 + v_3) = 0$. Then we have $\varphi(v_1) = \varphi(v_3) = 0$ and $\varepsilon_H(v_1) = \varepsilon_H(v_3)$, $\varepsilon_{G\setminus H}(v_1) = \varepsilon_{G\setminus H}(v_3)$. If $\varphi(v_1) + 1 = \varphi(v_2)$ then $\varepsilon_H(v_1) + 1 = \varepsilon_H(v_2)$, $\varepsilon_{G\setminus H}(v_1) = \varepsilon_{G\setminus H}(v_2)$. If $\varphi(v_1) + x = \varphi(v_2)$ then $\varepsilon_H(v_1) = \varepsilon_H(v_2)$, $\varepsilon_{G\setminus H}(v_1) + 1 = \varepsilon_{G\setminus H}(v_2)$. Thus

$$u = (\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_2), \varepsilon_{G\setminus H}(v_2), \varepsilon_H(v_3), \varepsilon_{G\setminus H}(v_3))$$

is either

$$(\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_1) + 1, \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1))$$

or

$$(\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1) + 1, \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1)).$$

Therefore, $u \in \{(0,0,1,0,0,0),\ (0,1,1,1,0,1),\ (1,0,0,0,1,0),\ (1,1,0,1,1,1),\ (0,0,0,1,0,0),\ (0,1,0,0,0,1),\ (1,0,1,1,1,0),\ (1,1,1,0,1,1)\}$.

Next, let $\varphi(v_1 + v_3) = 1 + x$. Then we have $\varphi(v_1) + 1 + x = \varphi(v_3)$ and $\varepsilon_H(v_1) + 1 = \varepsilon_H(v_3)$, $\varepsilon_{G\setminus H}(v_1) + 1 = \varepsilon_{G\setminus H}(v_3)$. Moreover, $\varphi(v_2)(1+x) = 0$ and $\varphi(v_2) \in \{0, 1+x\}$. So $(\varepsilon_H(v_2), \varepsilon_{G\setminus H}(v_2)) \in \{(0,0),(1,1)\}$. If $\varphi(v_1) + 1 = \varphi(v_2)$ then $\varepsilon_H(v_1) + 1 = \varepsilon_H(v_2)$, $\varepsilon_{G\setminus H}(v_1) = \varepsilon_{G\setminus H}(v_2)$. If $\varphi(v_1) + x = \varphi(v_2)$ then $\varepsilon_H(v_1) = \varepsilon_H(v_2)$, $\varepsilon_{G\setminus H}(v_1) + 1 = \varepsilon_{G\setminus H}(v_2)$. Moreover, $(\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1)) \in \{(0,1),(1,0)\}$.

Thus u is either

$$(\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_1) + 1, \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_1) + 1, \varepsilon_{G\setminus H}(v_1) + 1)$$

or

$$(\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1) + 1, \varepsilon_H(v_1) + 1, \varepsilon_{G\setminus H}(v_1) + 1).$$

Therefore, $u \in \{(0,1,1,1,1,0),\ (0,1,0,0,1,0),\ (1,0,0,0,0,1),\ (1,0,1,1,0,1)\}$. □

Lemma 3.8. *Let $R = \mathbb{F}_2 + u\mathbb{F}_2$ and G be a finite group of order $2n$, H be a subgroup of order n, and $C_2 = \{1, x\}$ be a group of order 2. If C_σ is a self-dual code of length $4n$ then $(\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_1), \varepsilon_H(v_2), \varepsilon_{G\setminus H}(v_2), \varepsilon_H(v_3), \varepsilon_{G\setminus H}(v_3)) = (\varepsilon_H(v_2) + b_1, \varepsilon_{G\setminus H}(v_2) + b_2, \varepsilon_H(v_2), \varepsilon_{G\setminus H}(v_2), \varepsilon_H(v_2) + b_1 + c_1, \varepsilon_{G\setminus H}(v_2) + b_2 + c_2)$ where*

$$(b_1, b_2) \in \{(1,0), (0,1), (1+u, 0), (u, 1), (1, u), (0, 1+u), (1+u, u), (u, 1+u)\},$$

$$(c_1, c_2) \in \{(0,0), (1,1), (u, 0), (1+u, 1), (0, u), (1, 1+u), (u, u), (1+u, 1+u)\}.$$

If $(c_1, c_2) = (1, 1)$ or $(c_1, c_2) = (1+u, 1+u)$ then $\varepsilon_H(v_1) = \varepsilon_{G\setminus H}(v_2)$,
if $(c_1, c_2) = (1, 1)$ or $(c_1, c_2) = (u, 0)$ then $\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2) \in \{0, u\}$,
if $(c_1, c_2) = (1+u, 1)$ or $(c_1, c_2) = (1, 1+u)$ then $(1+u)\varepsilon_H(v_1) = \varepsilon_{G\setminus H}(v_2)$,
if $(c_1, c_2) = (u, u)$ then $\varepsilon_H(v_1) + \varepsilon_{G\setminus H}(v_2) \in \{0, u\}$,
if $(c_1, c_2) = (0, 0)$ then $\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2) \in \mathbb{F}_2 + u\mathbb{F}_2$.
For $(c_1, c_2, \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2))$ we have 48 possibilities and for $(b_1, b_2, c_1, c_2, \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2))$ we have 384 possibilities.

Proof. Let $b = v_1 + v_2$, $c = v_1 + v_3$. From the equations in (14) we have that if $(\mathbb{F}_2 + u\mathbb{F}_2)C_2 = \{(\mathbb{F}_2 + u\mathbb{F}_2) + (\mathbb{F}_2 + u\mathbb{F}_2)x\}$ $(u^2 = 0,\ x^2 = 1)$ then $\varphi(b)^2 = 1$, $\varphi(v_2)\varphi(c) = 0$, $\varphi(c)^2 = 0$. It is obvious that the square of any element of $(\mathbb{F}_2 + u\mathbb{F}_2)C_2$ is either zero or one and $\varphi(b) \in \{1, x, 1+u, x+u, 1+xu, x+xu, 1+u+xu, x+u+xu\}$, $\varphi(v_2) \in \operatorname{Ann}\varphi(c)$, and $\varphi(c) \in \{0, 1+x, u, 1+x+u, xu, 1+x+xu, u+xu, 1+x+u+xu\}$.

$\varphi(c)$	$\operatorname{Ann}\varphi(c)$	$\lvert\operatorname{Ann}\varphi(c)\rvert$
0	$(\mathbb{F}_2 + u\mathbb{F}_2)C_2$	16
$1+x$	$\{0, 1+x, u+xu, 1+x+u+xu\}$	4
u	$\{0, u, xu, u+xu\}$	4
$1+x+u$	$\{0, 1+x+u, 1+x+xu, u+xu\}$	4
xu	$\{0, u, xu, u+xu\}$	4
$1+x+xu$	$\{0, 1+x+u, 1+x+xu, u+xu\}$	4
$u+xu$	$\{0, 1+x, u, 1+x+u, xu, 1+x+xu, u+xu, 1+x+u+xu\}$	8
$1+x+u+xu$	$\{0, 1+x, u+xu, 1+x+u+xu\}$	4

Now let $\varepsilon_H(b) = b_1$, $\varepsilon_{G\setminus H}(b) = b_2$, $\varepsilon_H(c) = c_1$, $\varepsilon_{G\setminus H}(c) = c_2$. It implies that $\varphi(b) = b_1 + b_2x$, $\varphi(c) = c_1 + c_2x$ and

$$(b_1, b_2) \in \{(1,0), (0,1), (1+u, 0), (u, 1), (1, u), (0, 1+u), (1+u, u), (u, 1+u)\},$$

$$(c_1, c_2) \in \{(0,0), (1,1), (u, 0), (1+u, 1), (0, u), (1, 1+u), (u, u), (1+u, 1+u)\}.$$

Moreover from the above table we have
if $(c_1, c_2) = (1, 1)$ or $(c_1, c_2) = (1+u, 1+u)$ then $\varepsilon_H(v_1) = \varepsilon_{G\setminus H}(v_2)$ (4 possibilities),

if $(c_1, c_2) = (1, 1)$ or $(c_1, c_2) = (u, 0)$ then $\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2) \in \{0, u\}$ (4 possibilities),
if $(c_1, c_2) = (1 + u, 1)$ or $(c_1, c_2) = (1, 1 + u)$ then $(1 + u)\varepsilon_H(v_1) = \varepsilon_{G\setminus H}(v_2)$ (4 possibilities),
if $(c_1, c_2) = (u, u)$ then $\varepsilon_H(v_1) + \varepsilon_{G\setminus H}(v_2) \in \{0, u\}$ (8 possibilities),
if $(c_1, c_2) = (0, 0)$ then $\varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2) \in \mathbb{F}_2 + u\mathbb{F}_2$ (16 possibilities). So we have $2 \cdot 4 \cdot 3 + 8 + 16 = 48$ possibilities for $(c_1, c_2, \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2))$ and any of these cases have 8 possibilities for (b_1, b_2). We also have $8 \cdot 48 = 384$ possibilities for $(b_1, b_2, c_1, c_2, \varepsilon_H(v_1), \varepsilon_{G\setminus H}(v_2))$. □

4 Computational Results

In this section, we employ our main construction, the extension method, the neighbor technique and its generalization to search for extremal self-dual binary codes of length 68. Namely, we apply the main construction over the field $\mathbb{F}_2$ to search for self-dual codes of length 32. We then lift these to codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ whose binary images are the extremal self-dual binary codes of length 64. Next we consider the extensions of the codes of length 64 to obtain extremal self-dual binary codes with parameters $[68, 34, 12]$. Finally, we apply the neighbor technique and its generalization to the codes of length 68 to find many codes of that length with weight enumerators not known in the literature before. In particular we find many new codes with the rare parameters $\gamma = 7, 8$ and 9. Before we tabulate the results, we recall the weight enumerators of extremal self-dual binary codes with parameters $[64, 32, 12]$ and $[68, 34, 12]$.

There are two possibilities for the weight enumerators of extremal singly-even $[64, 32, 12]_2$ codes ([3]):

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

Recently, many new codes are constructed for both weight enumerators in [11], [17] and [22]. With the most updated information, the existence of codes is known for β =14, 16, 18, 19, 20, 22, 24, 25, 26, 28, 29, 30, 32, 34, 35, 36, 38, 39, 44, 46, 49, 53, 54, 58, 59, 60, 64 and 74 in $W_{64,1}$ and for $\beta = 0, \dots,$40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 62, 64, 69, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120 and 184 in $W_{64,2}$.

The weight enumerator of a self-dual $[68, 34, 12]_2$ code is in one of the following forms by [2, 14]:

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

where β and γ are parameters and $0 \le \gamma \le 9$. The first examples of codes with a $\gamma = 7$ in $W_{68,2}$ are constructed in [21]. The first examples of codes with $\gamma = 8, 9$ in $W_{68,2}$ are constructed in [12]. Together with these the existence of the codes in $W_{68,2}$ is known for the following parameters (see [6, 5, 7, 20, 21, 11]):

$\gamma = 0$, $\beta \in \{2m|m = 0, 7, 11, 14, 17, 20, 21, \ldots, 99, 100, 102, 105, 110, 119, 136, 165\}$; or $\beta \in \{2m+1|m = 3, 5, 8, 10, 15, 16, 17, 19, 20, \ldots, 82, 87, 91, \ldots, 99, 101, 104, 110, 115\}$;

$\gamma = 1$, $\beta \in \{2m|m = 19, 22, \ldots, 99, 108\}$; or $\beta \in \{2m+1|m = 24, \ldots, 85, 94, 100, 101, 106, 108, 116\}$;

$\gamma = 2$, $\beta \in \{2m|m = 29, \ldots, 100, 103, 104\}$; or $\beta \in \{2m+1|m = 32, \ldots, 81, 84, 85, 86\}$;

$\gamma = 3$, $\beta \in \{2m|m = 39, \ldots, 92, 94, 95, 97, 98, 101, 102\}$; or $\beta \in \{2m+1|m = 38, 39, 40, 42, 43, \ldots, 77, 79, 80, 81, 83, 87, 88, 89, 96\}$;

$\gamma = 4$, $\beta \in \{2m|m = 43, 46, \ldots, 58, 60, \ldots, 93, 97, 98, 100\}$; or $\beta \in \{2m+1|m = 48, \ldots, 55, 57, 58, 60, 61, 62, 64, 68, \ldots, 72, 74, 78, 79, 80, 83, 84, 85, 89, 95\}$;

$\gamma = 5$ $\beta \in \{m|m = 113, 116, \ldots, 153, 158, \ldots, 169, 182, 187, 189, 191, 193, 195, 198, 200, 202, 211\}$;

$\gamma = 6$ with $\beta \in \{2m|m = 69, 77, 78, 79, 81, 88, 91, 93, 94, 95, 97, \ldots, 103\}$; or $\beta \in \{2m+1|m = 87, \ldots, 100, 103\}$;

$\gamma = 7$ with $\beta \in \{2m|m = 49, 56, 63, 70, 77, 83, \ldots, 99, 105, 106, 112, 119, 126, 133, 147\}$; or $\beta \in \{2m+1|m = 52, 59, 66, 73, 80, 81, 84, \ldots, 99, 101, 108, 115, 122, 129, 136\}$;

$\gamma = 8$ with $\beta \in \{2m|m = 90, \ldots, 110\}$; or $\beta \in \{2m+1|m = 90, \ldots, 110\}$;

$\gamma = 9$ with $\beta \in \{2m|m = 93, \ldots, 105, 107, \ldots, 115\}$; or $\beta \in \{2m+1|m = 93, 94, 96, 97, 99, \ldots, 112\}$;

All the upcoming computational results were obtained by performing the searches using MAGMA ([1]).

4.1 The group C_8

We first consider the main construction with the cyclic group C_8 to search for binary self-dual codes with parameters $[32, 16, 6 \text{ or } 8]$. We only list these codes which then lead to us finding new extremal binary self-dual codes of length 68.

Table 1: Codes of length 32 via Theorem 3.1 with the cyclic group C_8

Code	v_1	v_2	v_3	$\lvert Aut(C)\rvert$	Type
C_1	$(0,0,0,0,0,1,1,1)$	$(0,0,0,0,0,1,0,1)$	$(0,1,0,1,0,0,1,0)$	$2^9 3^2 5$	$[32,16,6]_I$
C_2	$(0,0,0,0,1,1,1,1)$	$(0,0,1,1,0,1,1,1)$	$(0,0,0,1,1,1,1,0)$	2^5	$[32,16,6]_I$

We now consider the R_1 lifts of the codes from Table 1. The codes obtained have binary images of extremal binary self-dual codes with parameters $64, 32, 12$. As before, we only list these codes that we later use to obtain new extremal binary self-dual codes of length 68.

Table 2: Codes of length 64 from R_1 lifts of C_1 and C_2

Code		v_1	v_2	v_3	$\|Aut(C)\|$	$W_{64,2}$
I_1	C_2	$(u,0,0,u,1,1,u+1,1)$	$(0,0,1,u+1,0,u+1,1,1)$	$(0,u,u,u+1,u+1,u+1,1,0)$	2^5	$\beta=0$
I_2	C_1	$(0,u,0,0,0,1,1,u+1)$	$(0,u,0,u,u,1,0,1)$	$(0,1,0,u+1,0,0,1,u)$	2^7	$\beta=80$

4.2 The group D_8

Now we consider the main construction and the dihedral group D_8 to search for binary self-dual codes with parameters $[32, 16, 6 \text{ or } 8]$.

Table 3: Codes of length 32 via Theorem 3.1 with the dihedral group D_8

Code	v_1	v_2	v_3	$\|Aut(C)\|$	Type
C_3	$(0,0,0,1,0,0,1,1)$	$(0,0,1,1,0,1,0,1)$	$(1,1,0,1,0,1,1,0)$	$2^3 3$	$[32,16,6]_I$

R_1 lifts:

Table 4: Codes of length 64 from R_1 lifts of C_3

Code		v_1	v_2	v_3	$\|Aut(C)\|$	$W_{64,2}$
I_3	C_3	$(0,u,u,1,0,0,1,1)$	$(0,0,1,u+1,u,1,0,1)$	$(u+1,u+1,0,u+1,0,1,u+1,0)$	$2^4 3$	$\beta=64$

4.3 Extremal Binary Self-Dual Codes of length 68 via Extensions

We now apply Theorem 2.4 to the codes obtained in Tables 2 and 4. As a result, we obtain codes whose binary images are the extremal binary self-dual codes of length 68. The order of the automorphism group of all the codes obtained in the table below is 2.

Table 5: New codes of length 68 from Theorem 2.4

$C_{68,i}$	Code	$(x_{17}, x_{18}, \ldots, x_{32})$	c	γ	β *in* $W_{64,2}$
$C_{68,1}$	I_3	$(u,u,0,1,3,u,u,u,u,3,u,1,0,0,u,3,u,1,0,1,1,3,3,3,u,0,3,u,u,1,0,0)$	1	**0**	**181**
$C_{68,2}$	I_3	$(0,3,0,1,3,1,3,1,1,1,3,1,u,0,u,0,u,0,u,3,0,0,1,1,1,1,u,u,1,3,u,u)$	3	**1**	**185**
$C_{68,3}$	I_1	$(0,1,1,u,u,3,u,1,3,3,1,0,0,3,3,u,1,3,3,u,u,3,0,u,3,u,3,u,1,3,0,0)$	3	**2**	**54**
$C_{68,4}$	I_2	$(u,3,1,3,0,0,3,u,0,3,0,u,u,u,0,u,3,1,0,3,0,3,u,1,1,1,1,u,0,3,0,1)$	1	**2**	**202**
$C_{68,5}$	I_3	$(u,u,u,3,0,0,1,u,1,u,1,3,u,0,0,3,0,1,u,3,0,1,0,3,1,1,0,3,u,3,0,1)$	1	**3**	**179**
$C_{68,6}$	I_3	$(u,0,0,1,1,0,1,0,3,3,u,0,1,0,3,3,1,0,3,0,3,3,1,u,1,u,1,u,3,0,1,u)$	3	**3**	**189**
$C_{68,7}$	I_3	$(0,3,0,1,u,3,u,3,0,1,0,3,0,3,0,0,1,u,u,1,0,u,1,0,u,0,u,1,3,0,1,u)$	3	**3**	**198**

4.4 Extremal Binary Self-Dual Codes of length 68 via Neighbours

We now apply the k^{th} range neighbour formula (mentioned earlier) to one of the codes obtained in Table 5, namely, the code $C_{68,4}$.

Let $\mathcal{N}_{(0)}$ be $\gamma = 2$, $\beta = 202$ (Table 5 ($C_{68,4}$)), then we obtain the following codes by applying the k^{th} range formula:

Table 6: i^{th} neighbour of $\mathcal{N}_{(0)}$

i	$\mathcal{N}_{(i+1)}$	x_i	γ	β	i	$\mathcal{N}_{(i+1)}$	x_i	γ	β
0	$\mathcal{N}_{(1)}$	(1110000000100111101000100100001000 0)	3	180	1	$\mathcal{N}_{(2)}$	(0110111111100111000010000110011111)	4	177
2	$\mathcal{N}_{(3)}$	(1111110110010011100101001000101111)	5	169	3	$\mathcal{N}_{(4)}$	(0100000000110011110000010000011110)	6	191
4	$\mathcal{N}_{(5)}$	(0100000000000110111001000111000011 0)	6	199	5	$\mathcal{N}_{(6)}$	(0000100000000110001001100111000011 1)	7	199
6	$\mathcal{N}_{(7)}$	(1011111101001111000101010111111010)	**7**	**209**	7	$\mathcal{N}_{(8)}$	(1110011111110110000101111101111110)	**7**	**220**
8	$\mathcal{N}_{(9)}$	(1100101001011011001101000000111100)	8	212	9	$\mathcal{N}_{(10)}$	(1110110100111111000010011111011000)	**8**	**226**
10	$\mathcal{N}_{(11)}$	(1011101011111010111010001000101000)	**8**	**233**	11	$\mathcal{N}_{(12)}$	(1101100000000101110010111111001110)	9	213
12	$\mathcal{N}_{(13)}$	(0111110101110100100110100100000111)	9	222	13	$\mathcal{N}_{(14)}$	(1100011000000000100101010101100010)	**9**	**229**
14	$\mathcal{N}_{(15)}$	(0100111000100000110010100011000100)	**9**	**235**	15	$\mathcal{N}_{(16)}$	(0000111011111101001101111010001101)	**9**	**236**
16	$\mathcal{N}_{(17)}$	(0110010111000111101001101101101110)	**9**	**240**	17	$\mathcal{N}_{(18)}$	(0001101000010111100111111110001001)	**9**	**243**
18	$\mathcal{N}_{(19)}$	(1111010011001111000010010001010001)	**9**	**247**	19	$\mathcal{N}_{(20)}$	(0001000000100010001011101011110000)	**8**	**234**
20	$\mathcal{N}_{(21)}$	(0110110001101011101000111100110001)	**8**	**245**	21	$\mathcal{N}_{(22)}$	(1000011100010110100110011011000011)	**8**	**250**

We shall now separately consider the neighbours of $\mathcal{N}_{(7)}, \mathcal{N}_{(8)}, \mathcal{N}_{(10)}, \mathcal{N}_{(11)}, \mathcal{N}_{(12)}, \mathcal{N}_{(14)}, \mathcal{N}_{(15)}, \mathcal{N}_{(17)}, \mathcal{N}_{(18)}, \mathcal{N}_{(19)}, \mathcal{N}_{(20)}, \mathcal{N}_{(21)}$ and $\mathcal{N}_{(22)}$.

First, the neighbours of $\mathcal{N}_{(7)}$.

Table 7: Neighbours of $\mathcal{N}_{(7)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
7	1	(0001101011101000000010101100100000)	**7**	**200**	7	2	(1011110000101000000000000110110010)	**7**	**201**
7	3	(1010110010100001100100011110001110)	**7**	**202**	7	4	(0001001110011000100100000010000111)	**7**	**204**
7	5	(0110000000101001011011010010111000)	**7**	**205**	7	6	(1101010010010101110001000011001000)	**7**	**206**
7	7	(0000101100001000100101011000010101)	**7**	**207**	7	8	(1101100101111100101110100100000011)	**7**	**212**
7	9	(1111011000001111101001111011111111)	**7**	**214**					

The neighbours of $\mathcal{N}_{(8)}$.

Table 8: Neighbours of $\mathcal{N}_{(8)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
8	10	(0101101001001001100111000010001010)	**6**	**205**	8	11	(0000111000000101110110010000000101)	**6**	**211**
8	12	(1000110101001001010000000111111011)	**7**	**208**	8	13	(1100001010000110010100101000001100)	**7**	**211**
8	14	(0000011000010001001000011101100110)	**7**	**213**	8	15	(0011000110000110101101001101111011)	**7**	**215**
8	16	(0100001111110010110100000101101010)	**7**	**216**	8	17	(1111101111010101000001000100011110)	**7**	**218**

The neighbours of $\mathcal{N}_{(10)}$.

Table 9: Neighbours of $\mathcal{N}_{(10)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
10	18	(1000111101011101000010001111000100)	**8**	**222**	10	19	(1000001100101001110001001010110111)	**8**	**223**
10	20	(0000100110010101011101101001100110)	**8**	**227**	10	21	(1011001101010011010111011000101010)	**8**	**229**

The neighbours of $\mathcal{N}_{(11)}$.

Table 10: Neighbours of $\mathcal{N}_{(11)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
11	22	(1010110110000101110101111100110110)	**7**	**221**	11	23	(0000001101000001110010110101100000)	**7**	**222**
11	24	(1101010100100000111010001000010011)	**8**	**224**	11	25	(0000010011001000010100011111011111)	**8**	**225**
11	26	(1110111110110010111011101101101110)	**8**	**228**	11	27	(1001100110100111000010100000100101)	**8**	**230**
11	28	(0000110001111000001001000011101000)	**8**	**231**	11	29	(1001011111010011000001100001010000)	**8**	**232**

The neighbours of $\mathcal{N}_{(12)}$.

Table 11: Neighbours of $\mathcal{N}_{(12)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
12	30	(1000100110000001010101010100001001)	**9**	**191**	12	31	(0111010100101000000001100101011010)	**9**	**197**
12	32	(1111100000101101001011110111000010)	**9**	**212**					

The neighbours of $\mathcal{N}_{(14)}$.

Table 12: Neighbour of $\mathcal{N}_{(14)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
14	33	(1011110001101000100111010000010000)	**9**	**227**

The neighbours of $\mathcal{N}_{(15)}$.

Table 13: Neighbours of $\mathcal{N}_{(15)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
15	34	(1011000011111110011101011000000101)	**9**	**231**	15	35	(1111110111110000010110000100010011)	**9**	**232**
15	36	(0011000011010010100011010000111001)	**9**	**233**	15	37	(0000000000111100000000101100111101)	**9**	**234**

The neighbours of $\mathcal{N}_{(17)}$.

Table 14: Neighbours of $\mathcal{N}_{(17)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
17	38	(0110000100000010110010110000110100)	**9**	**237**	17	39	(0011111001100000111100111101010010)	**9**	**238**

The neighbours of $\mathcal{N}_{(18)}$.

Table 15: Neighbours of $\mathcal{N}_{(18)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
18	40	(0110010110000001001110111010011100)	**9**	**239**	18	41	(1111000010111111010100101000111101)	**9**	**241**

The neighbours of $\mathcal{N}_{(19)}$.

Table 16: Neighbours of $\mathcal{N}_{(19)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
19	42	(1011110110001100110101001011001010)	**9**	**242**	19	43	(0101010111011010111100000111011110)	**9**	**244**
19	44	(1010110011000110001101001010010000)	**9**	**246**					

The neighbours of $\mathcal{N}_{(20)}$.

Table 17: Neighbours of $\mathcal{N}_{(20)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
20	45	(1111111110101111010101000110001101)	**8**	**236**	20	46	(1010000010110000100011110101111001)	**8**	**239**

The neighbours of $\mathcal{N}_{(21)}$.

Table 18: Neighbours of $\mathcal{N}_{(21)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
21	47	(0100000110001011000001000101101010)	**6**	**208**	21	48	(1101111000000001010010000110110001)	**6**	**209**
21	49	(1011101011101010010101111101000101)	**6**	**212**	21	50	(1111110111000100010010111011100000)	**6**	**214**
21	51	(1011111101010010111011101111111100)	**6**	**215**	21	52	(0000000001100001001001100111011100)	**6**	**218**
21	53	(1111011001110010100001101011011011)	**6**	**220**	21	54	(0100000001010101001001101001000011)	**7**	**219**
21	55	(1100000000000001110100001001100111)	**7**	**223**	21	56	(0000001101000100110101111100001111)	**7**	**225**
21	57	(1111011001111010111110100111110110)	**7**	**226**	21	58	(0010011000011000001000111001000101)	**7**	**227**
21	59	(1001010101101111101110000000000011)	**7**	**230**	21	60	(1111110101100000100011001110100110)	**8**	**235**
21	61	(0110000110110100100100101111100100)	**8**	**238**	21	62	(1010010010111110111001111011100010)	**8**	**240**
21	63	(1101011100111011010011111101111110)	**8**	**241**					

Finally, the neighbours of $\mathcal{N}_{(22)}$.

Table 19: Neighbours of $\mathcal{N}_{(22)}$

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
22	63	(0011111100111010011001010011100100)	**5**	**207**	22	64	(1011111100101111100110111111111101)	**6**	**213**
22	65	(1001011101001100101011001000110100)	**6**	**217**	22	66	(0100111101000110110111101101111110)	**6**	**219**
22	68	(1000010000111101010101110010010011)	**7**	**229**	22	69	(0100000001011101000011001111110011)	**8**	**237**
22	70	(1111111101001111101100000010100000)	**8**	**242**	22	71	(0010000100001001100001001110111000)	**8**	**243**
22	72	(1110110000001011011001101011011010)	**8**	**247**					

Note that $|Aut(C)| = 1$ for all the codes constructed.

5 Conclusion

In this paper, we presented a generator matrix of the form $G = (I_n \mid A)$, where A is a block matrix where the blocks come from group rings and the rows of A are not fully determined by permuting the entries of the first row. Together with our construction, extension and neighbours techniques, we were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{68,2}$:

$$\begin{aligned}
&(\gamma = 0,\ \beta = \{181\}),\\
&(\gamma = 1,\ \beta = \{185\}),\\
&(\gamma = 2,\ \beta = \{54, 202\}),\\
&(\gamma = 3,\ \beta = \{179, 189, 198\}),\\
&(\gamma = 5,\ \beta = \{207\}),\\
&(\gamma = 6,\ \beta = \{205, 208, 209, 211, 212, 213, 214, 215, 217, 218, 219, 220\}),\\
&(\gamma = 7,\ \beta = \{200, 201, 202, 204, 205, 206, 207, 208, 209, 211, 212,\\
&\qquad 213, 214, 215, 216, 218, 219, 220, 221, 222, 223, 225, 226, 227, 229, 230\}),\\
&(\gamma = 8,\ \beta = \{222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236,\\
&\qquad 237, 238, 239, 240, 241, 242, 243, 245, 247, 250\}),\\
&(\gamma = 9,\ \beta = \{191, 197, 212, 227, 229, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240,\\
&\qquad 241, 242, 243, 244, 246, 247\}).
\end{aligned}$$

A suggestion for future work would be to consider groups other than C_8 or D_8 used in our main construction when performing the searches for self-dual codes. Another direction is to consider groups of larger lengths to obtain codes of greater lengths with weight enumerators not known in the literature yet.

References

[1] W. Bosma, J. Cannon and C. Playoust, "The Magma algebra system. I. The user language", J. Symbolic Comput., vol. 24, (1997), 235–265.

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

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

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

[5] S.T. Dougherty, J. Gildea, A. Kaya, "Quadruple bordered constructions of self-dual codes from group rings over Frobenius rings", Cryptogr. Commun. (2019), `https://doi.org/10.1007/s12095-019-00380-8`.

[6] S. T. Dougherty, J. Gildea, A. Korban, A. Kaya, "Composite Constructions of Self-Dual Codes from Group Rings and New Extremal Self-Dual Binary Codes of Length 68", Advances in Mathematics of Communications, (2019), doi: 10.3934/amc.2020037.

[7] S.T. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylshchak, B. Yildiz, “Bordered constructions of self-dual codes from group rings”, Finite Fields Appl., vol. 57, (2019), 108–127.

[8] S.T. Dougherty, J. Gildea, R. Taylor and A. Tylshchak, “Group Rings, G-Codes and Constructions of Self-Dual and Formally Self-Dual Codes”, Des., Codes and Cryptog., Designs, vol. 86, no. 9, (2018), 2115–2138.

[9] S.T. Dougherty, S. Karadeniz, B. Yildiz, “Codes over R_k, Gray maps and their Binary Images”, Finite Fields Appl., vol. 17, (2011), no. 3, 205–219.

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

[11] J. Gildea, A. Kaya, A. Korban and B. Yildiz, “Constructing Self-Dual Codes from Group Rings and Reverse Circulant Matrices”, Advances in Mathematics of Communications, doi: 10.3934/amc.2020077.

[12] J. Gildea, A. Kaya, A. Korban and B. Yildiz, “New Extremal Binary Self-Dual Codes of Length 68 from Generalized Neighbours”, Finite Fields Appl., (2020), `https://doi.org/10.1016/j.ffa.2020.101727`.

[13] J. Gildea, A. Kaya, R. Taylor and B. Yildiz, “Constructions for Self-dual Codes Induced from Group Rings”, Finite Fields Appl., vol. 51, (2018), 71–92.

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

[15] T. Hurley, “Group Rings and Rings of Matrices”, Int. Jour. Pure and Appl. Math, vol. 31, (2006), no. 3, 319–335.

[16] S.Karadeniz, B. Yildiz, N. Aydin, “Extremal Binary Self-Dual Codes of Lengths 64 and 66 from Four-Circulant Constructions over $\mathbb{F}_2 + u\mathbb{F}_2$, Filomat 28:5, (2014), 937–945.

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

[18] A.Kaya and B. Yildiz, “Various Constructions for Self-Dual Codes over Rings and New Binary Self-Dual Codes”, Discrete Math., vol. 339, (2016), 460–469.

[19] E.M. Rains, “Shadow Bounds for Self-Dual Codes”, IEEE Trans. Inf. Theory, vol. 44, (1998), 134–139.

[20] N. Yankov, M. H. Lee, M. Gurel and M. Ivanova, “Self-dual codes with an automorphism of order 11”, IEEE Trans. Inform. Theory, vol. 61, (2015), no. 3, 1188–1193.

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

[22] N. Yankov and D. Anev, "On the self-dual codes with an automorphism of order 5", AAECC (2019), https://doi.org/10.1007/s00200-019-00403-0.