Constructing Self-Dual Codes from Group Rings and Reverse Circulant Matrices

Joe Gildea, Adrian Korban*
University of Chester
Department of Mathematical and Physical Sciences
Chester, UK
Abidin Kaya
Department of Mathematics Education
Sampoerna University, 12780, Jakarta, Indonesia
Bahattin Yildiz
Department of Mathematics & Statistics
Northern Arizona University
Flagstaff, AZ 86001, USA

January 15, 2020

Abstract

In this work, we describe a construction for self-dual codes in which we employ group rings and reverse circulant matrices. By applying the construction directly over different alphabets, and by employing the well known extension and neighbor methods we were able to obtain extremal binary self-dual codes of different lengths of which some have parameters that were not known in the literature before. In particular, we constructed three new codes of length 64, twenty-two new codes of length 68, twelve new codes of length 80 and four new codes of length 92.

Key Words: Group rings; extremal binary self-dual codes; codes over rings; reverse circulant matrices

*Corresponding author

1 Introduction

A search for constructing extremal binary self-dual codes over different alphabets has gained the attention of many researchers since these codes link with other mathematical structures and have many applications. There is an extensive literature with the focus on constructing the extremal binary self-dual codes whose weight enumerators have new parameters that were not known to exist before. One well known technique for constructing extremal binary self-dual codes over rings is to consider the four circulant construction which was first introduced in [1]. Recently, in [16], the authors generalized this four circulant construction with the motivation of producing codes whose automorphism groups are distinct from the automorphism groups that are obtained by the four circulant construction.

Another known technique for producing extremal binary self-dual codes is to consider generator matrices of the form $G = (I_n|\sigma(v))$ where $\sigma(v)$ is the image of a unitary unit in a group ring under a map that sends group ring elements to matrices. The advantage of this technique is that the map $\sigma(v)$ produces different matrices over the ring R when considering different groups. For example, in [14], the authors derived the mentioned above, four circulant construction by considering the generator matrix $G = (I_n|\sigma(v))$ where $v \in RD_{2n}$.

In this work, we generalize further the four circulant construction by employing the map $\sigma(v)$. The four circulant construction and its generalization which can be found in [16], both consist of circulant matrices and the latter one, additionally consists of reverse-circulant matrices. In our construction, we replace the circulant matrices with matrices that come from $\sigma(v)$ where $v \in RG$. We show that the generalized construction from [16] can be obtained directly using our construction with $v \in RC_n$, where C_n is the cyclic group of order n. We also show why our construction is different than the generalization of the four circulant construction in [16]. Using our construction together with the well known extension and neighbor methods, we are able to find extremal binary self-dual codes of lengths 64, 68 and 80 with parameters that were not known to exist before.

Additionally in this paper, we consider our construction with a restriction on the reverse circulant matrix. We do this based on the observation we make when searching for extremal binary self dual codes of length 80. By adding the restriction, we reduce the search field and we are able to construct extremal binary self-dual codes of lengths 68 and 92 directly from our construction in a reasonable time. By considering the neighbors of the codes of length 68, we find ones with parameters that were not known in the literature before. Also, the extremal binary self-dual codes of length 92 we construct, have parameters that are new in the literature.

The rest of the paper is organized as follows. In Section 2, we give preliminary definitions and results on group rings, self-dual codes, the alphabets to be used, special types of matrices and the well known four circulant construction and its generalization from [16]. In Section

3, we introduce the new construction and give theoretical results. In Section 4, we present numerical results of known and new extremal binary self-dual codes of lengths 64, 68 and 80 that we obtain by a direct application of our construction over different alphabets and by the neighbor and extension methods. In Section 5, we amend our main construction by adding in a restriction on the reverse circulant matrix and apply it over $\mathbb{F}_2$ to search for extremal binary self-dual codes of lengths 68 and 92 directly. The codes of length 92 and the neighbors of codes of length 68 we construct, have parameters that were not known in the literature before. We finish with concluding remarks and directions for possible future research.

2 Preliminaries

2.1 Self-Dual Codes, the Alphabets and the Well Known Extension and Neighbor Methods

We begin by recalling the standard definitions from coding theory. In this paper, all rings are assumed to be commutative, finite, Frobenius rings with a multiplicative identity. If the code is a submodule of R^n then we say that the code is linear. For a full description of Frobenius rings and codes over Frobenius rings, see [6]. Elements of the code $\mathcal{C}$ are called codewords of $\mathcal{C}$. 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:

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

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

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

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

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

Note that $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2 + u\mathbb{F}_2$ and so we can describe any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $\omega a + \overline{\omega} b$ uniquely, where $\overline{\omega} = \omega^2$, since $\omega \in \mathbb{F}_4$ and $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$. Let us recall the following Gray maps from [13] and [7]:

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

In [23], these maps were generalized to the following Gray maps:

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

Note that these Gray maps preserve orthogonality in their respective alphabets, for details we refer to [23]. Let $\mathcal{C} \subseteq (\mathbb{F}_4+u\mathbb{F}_4)^n$, then the binary codes $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ are equivalent to each other, please see [13] and [23] for more details. The Lee weight of an element in $\mathbb{F}_4+u\mathbb{F}_4$ is defined to be the Hamming weight of its binary image under any of the previously mentioned compositions of maps. A self-dual code in R^n where R is equipped with a Gray map to the binary Hamming space is said to be of Type II if the Lee weights of all codewords ar multiples of 4, otherwise it is said to be of Type I. Of course, it is then trivial to note that the image of a Type II code is a binary Type II code and the image of a Type I code is a binary Type I code in the traditional definition. We explain this completely in the following proposition from [23].

Proposition 2.1. *([23]) Let $\mathcal{C}$ be a code over $\mathbb{F}_4+u\mathbb{F}_4$. If $\mathcal{C}$ is self-orthogonal, then so are $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$. The code $\mathcal{C}$ is a Type I (resp. Type II) code over $\mathbb{F}_4+u\mathbb{F}_4$ if and only if $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a Type I (resp. Type II) $\mathbb{F}_4$-code, if and only if $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a Type I (resp. Type II) $\mathbb{F}_2+u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of $\mathcal{C}$ is the same as the minimum Lee weight of $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$.*

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

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

An upper bound on the minimum Hamming distance of a binary self-dual code was given in [24]. 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.

In subsequent sections we will be writing tables in which vectors with elements from the rings $\mathbb{F}_2+u\mathbb{F}_2$ and $\mathbb{F}_4+u\mathbb{F}_4$ will appear. To fit the results, we will use the following notation for the above two rings:

For the elements of $\mathbb{F}_2 + u\mathbb{F}_2$ we will use $0 \to 0, 1 \to 1, u \to u$ and $1 + u \to 3$. For the elements of $\mathbb{F}_4 + u\mathbb{F}_4$ we will use the ordered basis $\{u\omega, \omega, u, 1\}$ to express the elements of $\mathbb{F}_4 + u\mathbb{F}_4$ as binary strings of length 4.

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

Theorem 2.3. *([12]) 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 to search for new extremal binary self-dual codes from codes obtained directly from our constructions or from the described above, extension method. Two self-dual binary codes of length $2n$ are said to be neighbors of each other if their intersection has dimension $n-1$. Let $x \in \mathbb{F}_2^{2n} \backslash \mathcal{C}$ then $\mathcal{D} = \left\langle \langle x\rangle^{\perp} \cap \mathcal{C}, x \right\rangle$ is a neighbour of $\mathcal{C}$.

2.2 Special Matrices and Group Rings

We start this section by recalling 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 the ring elements. A reverse circulant matrix is one where each row is shifted one element to the left relative to the preceding row. We label the reverse circulant matrix as $A = rcirc(\alpha_1, \alpha_2, \ldots, \alpha_n)$. 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

$\mathrm{CIRC}(A_1, A_2, \ldots A_n)$, where A_i are the $k \times k$ matrices over the ring R. A symmetric matrix is a square matrix that is equal to its transpose. The transpose of a matrix A, denoted by A^T, is a matrix whose rows are the columns of A.

In our main construction we also apply matrices which come from group ring elements, we therefore finish this section by giving the necessary definitions for group rings.

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

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

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_k in the product is $\sum_{g_i g_j = g_k} \alpha_i \beta_j$.

The following construction of a matrix was first given for codes over fields by Hurley in [21]. It was extended to Frobenius rings in [10]. Let R be a finite commutative Frobenius ring 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 $i, j \in \{1, 2, \cdots, n\}$. We note that the elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are the elements of the group G in some given order. We will now describe $\sigma(v)$ for the following group rings RG where $G \in \{C_n, C_{m,n}\}$.

(i) Let $C_n = \langle x \mid x^n = 1 \rangle$ and set our listing of C_n to be $\{1, x, x^2, \ldots, x^{n-1}\}$. 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

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

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

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

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

(iii) Let $G = \langle x \mid x^{mn} = 1 \rangle$. If $v = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{1+i+mj} x^{ni+j} \in RC_{m,n}$, then

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

where $A_{j+1} = circ(a_{1+mj}, a_{2+mj}, \dots, a_{m+mj})$, $A'_{j+1} = circ(a_{m+mj}, a_{1+mj}, \dots, a_{(m-1)+mj})$, $a_i \in R$ and $m, n \geq 2$. We note that $C_{m,n}$ is the same as the cyclic group C_{mn}, however we give a different labelling to the elements, which makes $\sigma(v)$ to be different than the matrix that we obtain from the standard labelling of cyclic groups.

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:

$$\sigma(v^*) = \sigma(v)^T. \tag{3}$$

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

2.3 The Four Circulant Construction and Its Generalization

In this section, we define the well known four circulant construction first introduced in [1], and its generalization from [16].

Theorem 2.4. *([1]) Let A and B be $n \times n$ circulant matrices over $\mathbb{F}_q$ such that $AA^T + BB^T = -I_n$ then the matrix*

$$G = \left(\begin{array}{c|cc} I_{2n} & \begin{matrix} A & B \\ -B^T & A^T \end{matrix} \end{array} \right), \tag{4}$$

generates a self-dual code over $\mathbb{F}_q$.

Recently, the above construction has been generalized and used to search for extremal binary self-dual codes that could not be obtained from the four circulant construction. Below is the generalized four circulant construction from [16].

Theorem 2.5. *([16]) Let $\mathcal{R}$ be a commutative Frobenius ring of characteristic 2, A and B be circulant matrices and C be a reverse circulant matrix. Then the code generated by*

$$G = \left(\begin{array}{c|cc} I_{2n} & \begin{matrix} A & B+C \\ B^T + C & A^T \end{matrix} \end{array} \right) \tag{5}$$

is self-dual when $AA^T + BB^T + C^2 = I_n$ *and* $AC = CA$.

It is well known that circulant and reverse circulant matrices are fully determined by their first rows. Therefore, assuming that the entries in the first rows of matrices A, B and C in the above theorems are independent of each other, the search field in the generator matrix (4) is significantly smaller then the search field in the generator matrix (5). For instance if we search for extremal self-dual codes of length $2n$ over $\mathbb{F}_2$, then the search field in the four circulant construction is 2^{2n} while the search field in the generalized construction is 2^{3n}. In the next section, we generalize the construction in Theorem 2.5 even further.

3 The Main Construction

Here we present our main construction. As mentioned before, we generalize the construction from [16]. The motivation is to produce new extremal binary self-dual codes via our construction that could not be obtained by the construction in [16] or the four circulant construction first introduced in [1].

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

$$M_\sigma = \left[\begin{array}{cc|cc} I & 0 & \sigma(v_1) & \sigma(v_2)+C \\ 0 & I & \sigma(v_2)^T + C & \sigma(v_1)^T \end{array}\right]$$

where C is an $n \times n$ reverse circulant matrix over R. Let $\mathcal{C}_\sigma$ be a code that is generated by the matrix $M(\sigma)$. Then, the code $\mathcal{C}_\sigma$ has length $4n$. We now state the main theorem of this paper.

Theorem 3.1. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite group of order n. If*

- $\sigma(v_1v_1^* + v_2v_2^*) + \sigma(v_2)C + C\sigma(v_2)^T + C^2 + I = 0$,
- $\sigma(v_1v_2 + v_2v_1) + \sigma(v_1)C + C\sigma(v_1) = 0$ *and*
- $\sigma(v_1^*v_1 + v_2^*v_2) + \sigma(v_2)^TC + C\sigma(v_2) + C^2 + I = 0$

then C_σ is a self-dual code of length $4n$.

Proof. Clearly, $\mathcal{C}_\sigma$ has free rank $2n$ as the left hand side of the generator matrix is the $2n \times 2n$ identity matrix. Now,

$$M_\sigma M_\sigma^T = I + \begin{pmatrix} \sigma(v_1v_1^* + v_2v_2^*) + \sigma(v_2)C + C\sigma(v_2)^T + C^2 & \sigma(v_1v_2 + v_2v_1) + \sigma(v_1)C + C\sigma(v_1) \\ (\sigma(v_1v_2 + v_2v_1) + \sigma(v_1)C + C\sigma(v_1))^T & \sigma(v_1^*v_1 + v_2^*v_2) + \sigma(v_2)^TC + C\sigma(v_2) + C^2 \end{pmatrix}$$

$$= 0.$$

Therefore $\mathcal{C}$ is a self-orthogonal code of rank half its length, thus $\mathcal{C}$ is self-dual. □

In direct comparison of our main construction with the generator matrix of theorem 2.5, we can clearly see that the circulant matrices A and B are replaced with matrices that come from $\sigma(v)$. It is known that $\sigma(v)$ produces a circulant matrix over the ring R if $v \in RC_n$, where C_n is the cyclic group of order n. Please see [21] for details. Thus, the generalization of the four circulant construction in [16] can be obtained using M_σ with $\sigma(v) \in RC_n$. The immediate advantage of our construction over the generator matrix (5) is that our construction can take different forms since $\sigma(v)$ enables us to produce matrices that are different to the circulant matrices, i.e., this is by considering different groups in the group ring element v.

We finish this section with some immediate results that come directly from Theorem 3.1.

Corollary 3.2. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order n. Let $\mathcal{C}_\sigma$ be self-dual. If*

- *$C\sigma(v_2)^T$ and $C\sigma(v_2)$ are symmetric,*
- *C commutes with $\sigma(v_1)$,*
- *v_1 commutes with v_2 and*
- *$C^2 = 0$,*

then $v_1v_1^* + v_2v_2^*$ and $v_1^*v_1 + v_2^*v_2$ are units in RG.

Proof. If C commutes with $\sigma(v_1)$ and v_1 commutes with v_2, then $\sigma(v_1v_2 + v_2v_1) = 0$ and $\sigma(v_1)C + C\sigma(v_1) = 0$. If $C\sigma(v_2)^T$ and $C\sigma(v_2)$ are symmetric and $C^2 = 0$, then $\sigma(v_1v_1^* + v_2v_2^*) = \sigma(v_1^*v_1 + v_2^*v_2) = I$. Therefore $v_1v_1^* + v_2v_2^*$ and $v_1^*v_1 + v_2^*v_2$ are units since $det(\sigma(v_1v_1^* + v_2v_2^*)) = det(\sigma(v_1^*v_1 + v_2^*v_2)) = 1$. □

Corollary 3.3. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order n. Let $\mathcal{C}_\sigma$ be self-dual. If*

- *$C\sigma(v_2)^T$ and $C\sigma(v_2)$ are symmetric,*
- *C commutes with $\sigma(v_1)$,*
- *v_1 commutes with v_2 and*
- *$C^2 = I$,*

then $v_1v_1^* + v_2v_2^*$ and $v_1^*v_1 + v_2^*v_2$ are units in RG.

Proof. If C commutes with $\sigma(v_1)$ and v_1 commutes with v_2, then $\sigma(v_1v_2 + v_2v_1) = 0$ and $\sigma(v_1)C + C\sigma(v_1) = 0$. If $C\sigma(v_2)^T$ and $C\sigma(v_2)$ are symmetric and $C^2 = I$, then $\sigma(v_1v_1^* + v_2v_2^*) = \sigma(v_1^*v_1 + v_2^*v_2) = 0$. Therefore $v_1v_1^* + v_2v_2^*$ and $v_1^*v_1 + v_2^*v_2$ are non-units. □

Corollary 3.4. *Let R be a finite commutative Frobenius ring of characteristic 2, and let G be a finite group of order n. Let $\mathcal{C}_\sigma$ be self-dual. If*

- *$C\sigma(v_2)^T$ and $C\sigma(v_2)$ are symmetric,*
- *C commutes with $\sigma(v_1)$,*
- *v_1 commutes with v_2 and*
- *$C^2 = I$,*
- *v_1 is unitary in RG,*

then v_2 is unitary in RG.

Proof. If C commutes with $\sigma(v_1)$ and v_1 commutes with v_2, then $\sigma(v_1v_2 + v_2v_1) = 0$ and $\sigma(v_1)C + C\sigma(v_1) = 0$. If $C\sigma(v_2)^T$ and $C\sigma(v_2)$ are symmetric, $C^2 = I$ and v_1 is unitary in RG, then $\sigma(1 + v_2v_2^*) = \sigma(1 + v_2^*v_2) = 0$. Therefore $v_2v_2^* = 1$, $v_2^*v_2 = 1$ and v_2 is unitary. □

4 Computational Results

In this section we apply our main construction over $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ to search for extremal binary self-dual codes of lengths 64 and 80. We consider groups of orders 4, 5 and 8, in particular $C_{2,2}, C_5$ and $C_{4,2}$. We also employ the well known extension and neighbor methods to find new extremal binary self-dual codes of lengths 64 and 68. Since the focus in this section is to construct extremal self-dual codes of lengths 64, 68 and 80 with parameters that were not known in the literature before, we start by recalling their weight enumerators with parameters that are known.

There are two possibilities for the weight enumerators of extremal singly-even $[64, 32, 12]_2$ codes ([4]):

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

Recently, many new codes are constructed for both weight enumerators in [22] and [28]. 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, 59, 60, 64 and 74 in

$W_{64,1}$ and for $\beta = 0, \ldots, 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 62, 64, 69, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120$ 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 [3, 19]:

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

where β and γ are parameters and $0 \leq \gamma \leq 9$. The first examples of codes with a $\gamma = 7$ in $W_{68,2}$ are constructed in [27]. Together with these the existence of the codes in $W_{68,2}$ is known for the following parameters (see [14, 8, 9, 26, 27]):

$\gamma = 0,\ \beta \in \{2m | m = 0, 7, 11, 14, 17, 21, \ldots, 99, 102, 105, 110, 119, 136, 165\}$; or
$\beta \in \{2m + 1 | m = 3, 5, 8, 10, 15, 16, 17, 20, \ldots, 82, 87, 93, 94, 101, 104, 110, 115\}$;
$\gamma = 1,\ \beta \in \{2m | m = 19, 22, \ldots, 99\}$; or $\beta \in \{2m + 1 | m = 24, \ldots, 85\}$;
$\gamma = 2,\ \beta \in \{2m | m = 29, \ldots, 100, 103, 104\}$; 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
$\beta \in \{2m + 1 | m = 38, 40, 43, \ldots, 77, 79, 80, 81, 83, 87, 88, 89, 96\}$;
$\gamma = 4,\ \beta \in \{2m | m = 43, 46, \ldots, 58, 60, \ldots, 93, 97, 98, 100\}$; or
$\beta \in \{2m + 1 | m = 48, \ldots, 55, 57, 58, 60, 61, 62, 64, 68, \ldots, 72, 74, 78, 79, 80, 83, 84, 85, 89, 95\}$;
$\gamma = 5\ \beta \in \{m | m = 113, 116, \ldots, 153, 158, \ldots, 169, 182, 187, 189, 191, 193\}$;
$\gamma = 6$ with $\beta \in \{2m | m = 69, 77, 78, 79, 81, 88\}$;
$\gamma = 7$ with $\beta \in \{7m | m = 14, \ldots, 39, 42\}$.

The possible weight enumerators for a self-dual Type I $[80, 40, 14]$ code is given by [25] as:

$$W_{80,2} = 1 + (3200 + 4\alpha)y^{14} + (4765 - 8\alpha + 256\beta)y^{16} + \ldots,$$

where α and β are integers. A $[80, 40, 14]$ code was constructed in [5] (its weight enumerator was not stated) and a $[80, 40, 4]$ code was constructed in [18] with $\alpha = -280, \beta = 10$. In [25], codes with parameters $[80, 40, 14]$ were constructed for $\beta = 0$ and $\alpha = -17k$ where $k \in \{2, \ldots, 25, 27\}$. In [15], codes with parameters $[80, 40, 14]$ were constructed for $\beta = 1, \alpha = -96, -150, -168, -186, -204, -222, -240, -258, -312$ and for $\beta = 10, \alpha = -204, -276, -294, -330, -348, -366$.

The rest of this section is split into three subsections. In all three, we apply our main construction with groups of orders 4,5 and 8; in the first subsection we employ the group of order 4, namely $C_{2,2}$, in the second subsection we employ the group of order 8, namely $C_{4,2}$ and in the third subsection we use the group of order 5, namely C_5. In each subsection we tabulate our computational results. These were obtained using MAGMA ([2]). Additionally, in each table, we only state the elements of the first row of $\sigma(v_1)$ and $\sigma(v_2)$ since these matrices are fully determined by their first rows when the groups $C_{2,2}$, $C_{4,2}$ and C_5 are used in the group ring element v (we saw this in Section 2). We label the first rows of $\sigma(v_1)$ and

$\sigma(v_2)$ as $r_{\sigma(v_1)}$ and $r_{\sigma(v_2)}$ respectively in the upcoming tables. Similarly, the reverse circulant matrix C is also fully determined by the first row, we therefore only state the elements of that row in the upcoming tables. We label the first row of a reverse circulant matrix as r_C.

4.1 The group $G = C_{2,2}$

Here we search for extremal self-dual codes using the main construction with $G = C_{2,2}$. We construct self-dual codes of length 32 by considering our construction over $\mathbb{F}_4 + u\mathbb{F}_4$. These codes have binary Gray images of extremal binary self dual codes of length 64. We only list these codes of length 64 that extend to give new extremal binary self-dual codes of length 68.

Table 1: Self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$ of length 64 from $C_{2,2}$.

$\mathcal{C}_i$	$r_{\sigma(v_1)}$	$r_{\sigma(v_2)}$	r_C	$\lvert Aut(\mathcal{C}_i)\rvert$	β
1	$(0, 9, 2, 1)$	$(0, 0, A, 4)$	$(3, C, 3, 3)$	2^4	0
2	$(0, 9, 4, F)$	$(0, 0, 0, 6)$	$(2, 5, 2, 2)$	2^5	0

The codes in Table 1 are over $\mathbb{F}_4 + u\mathbb{F}_4$, so in order to apply Theorem 2.3, we first need to use the Gray map $\psi_{\mathbb{F}_4+u\mathbb{F}_4}$ to convert them to a code over $\mathbb{F}_2 + u\mathbb{F}_2$. The following table details the new extremal self-dual codes of length 68. For each new code constructed we note the original code of length 64 from the previous table, the unit $c \in \mathbb{F}_2 + u\mathbb{F}_2$ and the vector X required to apply Theorem 2.3.

Table 2: Extremal Self-dual codes of length 68 from Theorem 2.3.

$\mathcal{M}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β	$\lvert Aut(\mathcal{M}_{68,i})\rvert$
1	1	1	$(3u0u01u103103030u01u0u0301u10013)$	**0**	**40**	2
2	2	$u+1$	$(33313311u3uu13110u1030u1u31u31u3)$	**3**	**77**	2

4.2 The group $G = C_{4,2}$

This time, we search for extremal self-dual codes over the $\mathbb{F}_2 + u\mathbb{F}_2$ ring. The $\sigma(v_1)$ and $\sigma(v_2)$ matrices both come from the group ring element $v_1, v_2 \in RC_{4,2}$. The codes obtained have binary Gray images of extremal binary self-dual codes of length 64. As previously, we only list these codes that extend to give new extremal binary self-dual codes of length 68.

Table 3: Self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length 64 from $C_{4,2}$.

$\mathcal{E}_i$	$r_{\sigma(v_1)}$	$r_{\sigma(v_2)}$	r_C	$\lvert Aut(\mathcal{E}_i)\rvert$	β
1	$(u,0,1,1,u,u,u,u)$	$(u,u,1,1,0,u,u,3)$	$(0,1,0,1,0,1,0,1)$	2^5	0
2	$(u,u,1,3,u,u,u,u)$	$(u,u,1,1,u,u,0,3)$	$(u,3,u,3,u,3,u,3)$	2^6	0
3	$(u,0,u,u,0,0,1,3)$	$(u,u,0,1,u,0,3,1)$	$(3,3,3,3,3,3,3,3)$	2^7	80

By considering the possible neighbors of the codes in Table 3, we were able to construct the following extremal binary self-dual codes of length 64 with parameters that were not known in the literature before. We list these in Table 4.

Table 4: New codes of length 64 as neighbors

$\mathcal{L}_{64,i}$	$\mathcal{E}_i$	$(x_{33},...,x_{64})$	$W_{64,i}$	β	$\lvert Aut(\mathcal{L}_{64,i})\rvert$
1	3	(01110001001001101000011001011111)	1	**58**	2^2
2	3	(11011001001101110110010110011010)	2	**54**	2^3
3	3	(11111100101011111001111001010010)	2	**62**	2

Remark 1. *The first codes with weight enumerators for $\beta = 54$ and 62 in $W_{64,2}$ are constructed in [28]. The codes constructed in Table 8 are not equivalent to the ones constructed earlier. Also, the method is different.*

Also, by applying Theorem 2.3 to the codes listed in Table 3, we were able to construct three new extremal binary self-dual codes of length 68. These codes and their parameters are listed in Table 5.

Table 5: Extremal Self-dual codes of length 68 from Theorem 2.3.

$\mathcal{N}_{68,i}$	$\mathcal{E}_i$	c	X	γ	β	$\lvert Aut(\mathcal{N}_{68,i})\rvert$
1	1	3	$(01330u3131uuu3330uuuu000333u1u1u)$	**0**	**39**	2
2	2	1	$(0013u1111uu1u0uuuu101u1333330130)$	**3**	**79**	2
3	2	1	$(u30u1u03u10uu113uuu01131u111u030)$	**3**	**85**	2

4.3 The group $G = C_5$

Here we search for extremal self-dual codes of length 40 over $\mathbb{F}_4 + u\mathbb{F}_4$ using our main construction with $G = C_5$. These codes have Gray images of extremal binary self-dual codes

of length 80. We only list such codes with parameters that were not known in the literature before.

Table 6: $[80, 40, 14]$ Self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$ from C_5.

$\mathcal{D}_i$	$r_{\sigma(v_1)}$	$r_{\sigma(v_2)}$	r_C	$\lvert Aut(\mathcal{D}_i)\rvert$	(β, α)	$\mathcal{D}_i$	$r_{\sigma(v_1)}$	$r_{\sigma(v_2)}$	r_C	$\lvert Aut(\mathcal{D}_i)\rvert$	(β, α)
1	$(A, A, A, 1, 3)$	$(0, 2, 1, 3, E)$	$(7, 7, 7, 7, 7)$	$2^3 \cdot 5$	$(0, -120)$	2	$(0, A, 2, 6, F)$	$(2, 1, E, 2, 1)$	$(6, 6, 6, 6, 6)$	$2^2 \cdot 5$	$(0, -125)$
3	$(A, A, 0, 4, F)$	$(2, A, 6, 2, F)$	$(1, 1, 1, 1, 1)$	$2^2 \cdot 5$	$(0, -150)$	4	$(0, A, A, 4, 5)$	$(0, 3, 6, A, B)$	(E, E, E, E, E)	$2^2 \cdot 5$	$(0, -155)$
5	$(2, 0, A, 4, 5)$	$(2, A, 4, 0, 5)$	(B, B, B, B, B)	$2^2 \cdot 5$	$(0, -180)$	6	$(0, A, B, B, E)$	$(0, 2, 1, 3, 1)$	$(6, 6, 6, 6, 6)$	$2^2 \cdot 5$	$(0, -190)$
7	$(0, A, 2, 6, F)$	$(2, 2, 6, 2, 7)$	(B, B, B, B, B)	$2^2 \cdot 5$	$(0, -200)$	8	$(0, 0, A, 6, F)$	$(2, 1, E, 0, 3)$	$(6, 6, 6, 6, 6)$	$2^2 \cdot 5$	$(0, -215)$
9	$(A, 0, 1, 4, 7)$	$(0, 3, E, 2, 7)$	(B, B, B, B, B)	$2^2 \cdot 5$	$(0, -230)$	10	$(A, 2, A, 1, 4)$	$(0, 0, 7, 1, F)$	$(7, 7, 7, 7, 7)$	$2^2 \cdot 5$	$(0, -250)$
11	$(A, A, 3, B, 4)$	$(0, A, 4, 0, 7)$	$(4, 4, 4, 4, 4)$	$2^2 \cdot 5$	$(0, -275)$	12	$(0, 2, B, 1, E)$	$(0, 0, 1, 1, 3)$	$(4, 4, 4, 4, 4)$	$2^2 \cdot 5$	$(10, -370)$

The results in Table 6 are interesting, especially the elements of the reverse circulant matrix C. For each code that we found, the reverse circulant matrix consists of the same elements, which means that C is equivalent to a constant matrix. This is interesting because we can use that fact when searching for extremal self-dual binary codes of higher lengths using our construction directly over $\mathbb{F}_2$, i.e., we can force the reverse circulant matrix to be a constant matrix. This will reduce the search field significantly and will allow us to search for self-dual codes of higher lengths in a reasonable time. We present some examples in the next section.

5 The Main Construction with a restriction

In this section, we consider our main construction restricted to the case where the reverse circulant matrix C is now a constant matrix over R, i.e., $C = rcirc(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1 = \alpha_2 = \cdots = \alpha_n$ and $\alpha_i \in R$, where R is a finite commutative Frobenius ring of characteristic 2. In fact, we let the C to be a constant matrix with 1's only. We also force n to be an odd prime. We employ the cyclic group C_n of order n so that for $v \in RC_n$, $\sigma(v)$ is a circulant matrix of order n (we saw this in Section 2). Note that in this case, when C is a constant matrix over R and when $v \in RC_n$, our construction is equivalent to the usual four circulant construction. However, we want to draw a connection between certain group ring elements and self-dual codes in this case. Also, by doing this we were able to construct extremal binary self-dual codes of lengths 68 and 92 over $\mathbb{F}_2$ directly from our construction in a reasonable time. The codes of length 92 we found, have new parameters and the neighbors of codes of length 68 have also parameters that were not known to exist before. All the results are tabulated later in this section. We first state the following result.

Theorem 5.1. *Let R be a finite commutative Frobenius ring of characteristic 2, C be a $p \times p$ constant reverse circulant matrix over R and let G be a finite group of order p where p is an odd prime. Let $\mathcal{C}_\sigma$ be self-dual. Then,*

- v_1 *commutes with* v_2,
- $v_1v_1^* + v_2v_2^*$ *and* $v_1^*v_1 + v_2^*v_2$ *are units in* RG

Proof. If C is a $p \times p$ matrix of ones over R, then $\sigma(v_2)C = C\sigma(v_2)^T$, $\sigma(v_1)C = C\sigma(v_1)$ and $\sigma(v_2)^T C = C\sigma(v_2)$. Consequently, $v_1v_2 = v_2v_1$. Additionally, $\sigma(v_1v_1^*+v_2v_2^*) = C^2+I = C+I$. Now, $det(C + I) = 0$ since $det(\sigma(v_1v_1^* + v_2v_2^*)) = 0$. Therefore $v_1v_1^* + v_2v_2^*$ is non unit. □

We next look at the computational results. As mentioned above, the main objective of using our main construction with a restriction was to find new extremal binary self-dual codes of lengths 68 and 92. We therefore state the weight enumerators for the codes of length 92 with their known parameters. We know the weight enumerators of codes of length 68 from the previous section.

The possible weight enumerators $W_{92,i}$ of extremal singly even self dual $[92, 46, 16]$ codes are as follows ([11]):

$$W_{92,1} = 1 + (4692 + 4\beta)y^{16} + (174800 - 8\beta + 256\alpha)y^{18} + (-2048\alpha + 2425488 - 52\beta)y^{20} + \ldots,$$

$$W_{92,2} = 1 + (4692 + 4\beta)y^{16} + (174800 - 8\beta + 256\alpha)y^{18} + (-2048\alpha + 2441872 - 52\beta)y^{20} + \ldots,$$

$$W_{92,3} = 1 + (4692 + 4\beta)y^{16} + (121296 - 8\beta)y^{18} + (3213968 - 52\beta)y^{20} + \ldots,$$

where α and β are integers. In [20], codes with parameters $[92, 46, 16]$ were constructed for $\alpha = -69, \beta = 2024$, $\alpha = -46, \beta = 1426, 1518, 1656, 1679, 1702, 1725, 1748, 1794, 1840, 1863$, $\alpha = -23, \beta = 1081, 1150, 1196, 1242, 1265, 1288, 1334, 1357, 1380, 1403, 1426, 1449, 1472, 1495, 1518, 1564$, $\alpha = 0, \beta = 782, 805, 828, 851, 897, 920, 943, 966, 989, 1035, 1058, 1081, 1104, 1127, 1150, 1173, 1196, 1219, 1242, 1334, 1380, 1403, 1426$ in $W_{92,1}$.

We split the rest of this section into two subsections to organise the computational results. In the first subsection, we apply the group C_{17} and force C to be a constant matrix of 1's only. In the second subsection we use the group C_{23} and also force C to be a constant matrix of 1's only. As in previous tables, we only give the first rows of $\sigma(v_1)$, $\sigma(v_2)$ since these are fully determined by their first rows (we saw this in Section 2 in the case of $\sigma(v)$ where $v \in RC_n$). We label the first rows of $\sigma(v_1)$ and $\sigma(v_2)$ as $r_{\sigma(v_1)}$ and $r_{\sigma(v_2)}$ respectively. We omit giving the elements of C since we force it to be a constant matrix of 1's only. The search was implemented using MAGMA ([2]).

5.1 The Cyclic Group of Order 17

Here we apply the restricted construction over $\mathbb{F}_2$ to search for extremal binary self-dual codes of length 68. We only list two such codes. Next, by considering their possible neighbors, we were able to find new extremal binary self-dual codes of length 68.

Table 7: Self-dual codes over $\mathbb{F}_2$ of length 68 from C_{17}.

$\mathcal{C}_i$	$r_{\sigma(v_1)}$	$r_{\sigma(v_2)}$	γ	β	$\lvert Aut(\mathcal{C}_i)\rvert$
1	$(0,0,0,0,0,0,0,1,1,0,1,1,0,1,1,1,1)$	$(0,0,0,1,0,0,0,1,1,1,0,0,1,0,1,1,1)$	0	255	$2 \cdot 17$
2	$(0,0,0,0,0,0,0,0,1,1,1,0,1,0,1,1,1)$	$(0,0,0,1,0,1,1,1,1,0,1,1,0,1,1,1,1)$	0	272	$2^2 \cdot 17$

Now we list the neighbors of the codes in Table 7. The codes listed below all have parameters that were not known in the literature before.

Table 8: New codes of length 68 as neighbors

$\mathcal{N}_{68,i}$	$\mathcal{C}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{68,i}$	$\mathcal{C}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
$\mathcal{N}_{68,1}$	$\mathcal{C}_1$	(10011100101010100110000010001110 11)	**0**	**183**	$\mathcal{N}_{68,2}$	$\mathcal{C}_1$	(11010000000100011101010110101000 01)	**0**	**185**
$\mathcal{N}_{68,3}$	$\mathcal{C}_1$	(00010000100110001101011000101010 00)	**0**	**189**	$\mathcal{N}_{68,4}$	$\mathcal{C}_1$	(01000000011101101000111100111011 11)	**0**	**191**
$\mathcal{N}_{68,5}$	$\mathcal{C}_1$	(01101100010010001100101101111000 01)	**0**	**193**	$\mathcal{N}_{68,6}$	$\mathcal{C}_2$	(00000011101010001110010110000011 01)	**0**	**195**
$\mathcal{N}_{68,7}$	$\mathcal{C}_2$	(10010001110001001100100001111111 11)	**0**	**197**	$\mathcal{N}_{68,8}$	$\mathcal{C}_2$	(01101001000000010100001010011011 00)	**0**	**199**
$\mathcal{N}_{68,9}$	$\mathcal{C}_2$	(10101110011100100010101001000110 10)	**0**	**200**	$\mathcal{N}_{68,10}$	$\mathcal{C}_2$	(00000001000001111001111100001101 10)	**0**	**203**
$\mathcal{N}_{68,11}$	$\mathcal{C}_1$	(10010100000110000111011000110110 1)	**1**	**189**	$\mathcal{N}_{68,12}$	$\mathcal{C}_1$	(01101001110001100000010010011000 11)	**1**	**201**
$\mathcal{N}_{68,13}$	$\mathcal{C}_1$	(10100111111100011110011101110011 10)	**1**	**203**	$\mathcal{N}_{68,14}$	$\mathcal{C}_1$	(11110111111011011001011000000101 01)	**1**	**205**
$\mathcal{N}_{68,15}$	$\mathcal{C}_1$	(10111101111111101011011111111011 11)	**1**	**213**	$\mathcal{N}_{68,16}$	$\mathcal{C}_2$	(10100011111101000000101000111010 01)	**1**	**216**
$\mathcal{N}_{68,17}$	$\mathcal{C}_1$	(10111100111110110011011111001110 1)	**1**	**217**	$\mathcal{N}_{68,18}$	$\mathcal{C}_2$	(00000100110011001001010111011101 01)	**1**	**233**

5.2 The Cyclic Group of Order 23

Finally, we apply the restricted construction over $\mathbb{F}_2$ to search for extremal binary self-dual codes of length 92. Here the group employed is the cyclic group of order 23, namely $G = C_{23}$. We only list codes with parameters that were not known in the literature before.

Table 9: Self-dual codes over $\mathbb{F}_2$ of length 92 from C_{23}.

$\mathcal{C}_i$	$r_{\sigma(v_1)}$	$r_{\sigma(v_2)}$	γ	β	$\lvert Aut(\mathcal{C}_i)\rvert$	Type
1	$(0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,0,1,1,0,1,1,1)$	$(0,0,0,0,1,1,0,0,1,0,0,1,1,1,0,0,1,0,0,0,1,1,1)$	0	**759**	$2 \cdot 23$	$W_{92,1}$
3	$(0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,1,0,1,1)$	$(0,0,0,0,1,1,0,0,0,1,1,0,1,0,0,1,1,0,1,0,1,1,1)$	0	**1012**	$2 \cdot 23$	$W_{92,1}$
13	$(0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,0,0,0,1,1,1)$	$(0,0,0,0,1,1,0,1,1,0,1,0,1,0,1,0,1,1,0,1,1,1)$	-46	**1564**	$2^2 \cdot 23$	$W_{92,1}$
16	$(0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,1,1,0,0,0,1,1)$	$(0,0,0,0,0,0,1,0,0,0,0,1,1,0,1,0,1,1,1,0,0,0,1)$	-46	**1978**	$2 \cdot 23$	$W_{92,1}$

6 Conclusion

In this work, we generalized the construction given in [16]. We showed how our construction, together with a restriction can be used to search for extremal binary self-dual codes of lengths

68, 80 and 92 in reasonable time. We demonstrated the relevance of this new construction by constructing many new extremal binary self-dual codes of lengths 68, 80 and 92. In particular, we constructed the following codes that were not known in the literature before. The binary generating matrices of the codes are available online at [17].

- **Codes of length** 64**:** We were able to construct the following extremal binary self-dual codes with new weight enumerators:

$$\begin{aligned}(W_{64,1}, &\quad \beta = \{58\}),\\ (W_{64,2}, &\quad \beta = \{54, 62\}).\end{aligned}$$

- **Codes of length** 68**:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{68,2}$:

$$\begin{aligned}(\gamma = 0, &\quad \beta = \{39, 40, 183, 185, 189, 191, 193, 195, 197, 199, 200, 203\}),\\ (\gamma = 1, &\quad \beta = \{189, 201, 203, 213, 216, 217, 233\}),\\ (\gamma = 3, &\quad \beta = \{77, 79, 85\}).\end{aligned}$$

- **Codes of length** 80**:** We were to able to construct the following $[80, 40, 14]$ codes with new weight enumerators in $W_{80,2}$:

$$\begin{aligned}(\beta = 0, &\quad \alpha = \{-120, -125, -150, -155, -180, -190, -200, -215, -230, -250, -275\}),\\ (\beta = 10, &\quad \alpha = \{-370\}).\end{aligned}$$

- **Codes of length** 92**:** We were to able to construct the following $[92, 46, 16]$ codes with new weight enumerators in $W_{92,1}$:

$$\begin{aligned}(\alpha = 0, &\quad \beta = \{759, 1012\}),\\ (\alpha = -46, &\quad \beta = \{1564, 1978\}).\end{aligned}$$

A suggestion for future work would be to consider groups different than the cyclic group in the construction we described in this work. This would produce more interesting or complex matrix constructions that then could potentially lead to finding more extremal binary self-dual codes of different lengths. Another direction is to apply matrices different to the reverse circulant ones.

Acknowledgement. The authors would like to thank to anonymous referees for their valuable comments.

References

[1] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada and C. Koukouvinos, "On self-dual codes over some prime fields", Discrete Math, vol. 262, pp. 37–58, 2003.

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

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

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

[5] G. Dorfer and H. Maharaj, "Generalized AG codes and generalized duality", Finite Fields Appl., vol. 9, pp. 194–210, 2018.

[6] S.T. Dougherty, "Algebraic coding theory over finite commutative rings", Springer Briefs in Mathematics. Springer, 2017.

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

[8] 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`.

[9] 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, pp. 108–127, 2019.

[10] 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 Crypt., vol. 86, no 9, pp. 2115–2138, 2018.

[11] S.T. Dougherty, T.A. Gulliver and M. Harada, "Extremal binary self-dual codes", IEEE Trans. Inform. Theory, vol. 43, pp. 2036–2047, 1997.

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

[13] P. Gaborit, V. Pless, P. Sole and O. Atkin, "Type II codes over $\mathbb{F}_4$", Finite Fields Appl., vol. 8, pp. 171–183, 2002.

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

[15] J. Gildea, A. Kaya, A. Tylyshchak, B. Yildiz, "A group induced four-circulant construction for self-dual codes and new extremal binary self-dual codes", available online at `https://arxiv.org/abs/1912.11758`.

[16] J. Gildea, A. Kaya and B. Yildiz, "New binary self-dual codes via a generalization of the four circulant construction", available online at `https://arxiv.org/abs/1912.11754`.

[17] J. Gildea, A. Korban, A. Kaya and B. Yildiz, *Binary generator matrices of new self-dual binary codes of lengths 64, 68, 80 and 92*, available online at `http://abidinkaya.wix.com/math/adrian`.

[18] T.A. Gulliver and M. Harada, "Classification of extremal double circulant self-dual codes of lengths 74-88", Discr. Math., vol. 306, pp. 2064–2072, 2006.

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

[20] M. Harada, T. Nishimura, "An extremal singly even self-dual codes of length 88", Advances in Mathematics of Communications, vol. 1, no. 2, pp. 261–267, 2007.

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

[22] A. Kaya, "New extremal binary self-dual codes of lengths 64 and 66 from R_2-lifts", Finite Fields Appl., vol. 46, pp. 271-279, 2017.

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

[24] E.M. Rains, "Shadow bounds for self-dual codes", IEEE Trans. Inf. Theory, vol. 44, pp. 134–139, 1998.

[25] N. Yankov, D. Anev and M. Gurel, "Self-dual codes with an automorphism of order 13", Advances in Mathematics of Communications, vol. 11, no. 3, pp. 635–645, 2017.

[26] 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, no. 3, pp. 1188-1193, 2015.

[27] 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, pp. 17-30, 2018.

[28] 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`.