SELF-DUAL CODES USING BISYMMETRIC MATRICES AND GROUP RINGS

J. GILDEA, A. KAYA, A. KORBAN AND A. TYLYSHCHAK

Abstract. In this work, we describe a construction in which we combine together the idea of a bisymmetric matrix and group rings. Applying this construction over the ring $\mathbb{F}_4 + u\mathbb{F}_4$ together with the well known extension and neighbour methods, we construct new self-dual codes of length 68. In particular, we find 41 new codes of length 68 that were not known in the literature before.

1. Introduction

A very well known and probably the most common technique for producing extremal binary self-dual codes over rings is to consider generator matrices of the form $G = (I_n|A)$ where A is a circulant or reverse circulant matrix satisfying $AA^T = -I_n$. This technique has recently been extended so that the matrix A was replaced with $\sigma(v)$, i.e., $G = (I_n|\sigma(v))$ where $\sigma(v)$ is the image of a unitary unit in a group ring under a map that sends group ring elements to matrices. Examples of this approach where groups of different orders are used can be found in [7], [8], [9] and [13]. The motivation of the extended technique was to obtain codes whose automorphism groups are distinct from the automorphism groups that are usually obtained from the generator matrices of the form $G = (I_n|A)$.

Another natural extension of the above technique is to consider the bordered construction where A in the generator matrix G is an $(n-1)\times(n-1)$ circulant or reverse circulant matrix with a row on top of the form $(\gamma, \alpha_1, \alpha_2, \ldots, \alpha_{n-1})$, and a column on the left of the form $(\gamma, (\alpha_1, \alpha_2, \ldots, \alpha_{n-1})^T)$, where $\gamma, \alpha_i \in R$ and where R is a ring. Please see [14], [16] and [19] for some related work. Recently, the bordered construction has been extended further so that matrices that are derived from $\sigma(v)$ are employed in the construction. Again, the motivation was to obtain codes whose automorphism groups differ from the standard bordered construction. Please see [5], [6] and [7] for example.

In this work, we amend the generator matrix $G = (I_n|A)$ so that A is replaced with a 4×4 bisymmetric block matrix and each block is replaced with a construction that comes from $\sigma(v)$. This allows us to consider a variety of generator matrices when applying different groups in the group ring. Additionally, we amend the identity matrix I_n so that it is also replaced with a block matrix but here, the blocks have a fixed structure. The motivation of this approach is that the construction will produce codes whose automorphism groups differ from the ones that are produced by the standard techniques, consequently leading to finding new extremal self-dual codes that were not known in the literature before. We apply the new construction over $\mathbb{F}_4 + u\mathbb{F}_4$ to search for extremal binary images of codes with parameters $[64, 32, 12]$ to which we apply the Gray map $(\mathbb{F}_4 + u\mathbb{F}_4)^n \to \mathbb{F}_2^{4n}$ that produces a binary self-dual code of length $4n$. We then take the binary self-dual codes produced from this map and apply a well known extension method over $\mathbb{F}_2 + u\mathbb{F}_2$ to find new self-dual codes of length 68 of which we consider possible neighbours. Together with the extension and neighbours methods, we find 41 new codes of length 68 that were not known in the literature before.

The rest of the work is organised as follows. In Section 2, we give preliminary definitions and results on group rings, self-dual codes and the alphabet which we use. In Section 3, we give the main construction and conditions needed for the construction to produce a self-dual code. In Section 4, we apply the main construction over $\mathbb{F}_4 + u\mathbb{F}_4$ to search for self-dual codes whose binary images have parameters $[64, 32, 12]$. We next apply the Gray map $(\mathbb{F}_4 + u\mathbb{F}_4)^n \to \mathbb{F}_2^{4n}$ to produce binary self-dual codes of length $4n$. Finally, we use a building-up method over $\mathbb{F}_2 + u\mathbb{F}_2$ and the neighbours method to obtain new extremal binary self-dual codes of length 68. We also tabulate the results in this section.

Key words and phrases. Bisymmetric matrix, Group Rings, Self-Dual Codes.

2. Preliminaries

2.1. **Self-Dual Codes, the Field $\mathbb{F}_4$ and the Ring $\mathbb{F}_4 + u\mathbb{F}_4$.** We first recall the standard definitions from coding theory. A code C of length n over a Frobenius ring R is a subset of R^n. The following are equivalent

(1) R is a Frobenius ring;
(2) As a left module, $\widehat{R} \cong {}_R R$;
(3) As a right module $\widehat{R} \cong R_R$.

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 [3]. 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:

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

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 $C = C^\perp$.

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 $\mathbb{F}_4 + u\mathsf{F}_4 = \mathbb{F}_4[u]/\langle u^2 \rangle$ 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 [4] and [12]:

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

In [17], 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 [17]. Let $C \subseteq (\mathbb{F}_4 + u\mathbb{F}_4)^n$, then the binary codes $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$ are equivalent to each other, please see [12] and [17] 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 are 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 [17].

Proposition 2.1. *([17]) Let C be a code over $\mathbb{F}_4 + u\mathbb{F}_4$. If C is self-orthogonal, then so are $\psi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$. The code C is a Type I (resp. Type II) code over $\mathbb{F}_4 + u\mathbb{F}_4$ if and only if $\varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$ is a Type I (resp. Type II) $\mathbb{F}_4$-code, if and only if $\psi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$ is a Type I (resp. Type II) $\mathbb{F}_2 + u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of C is the same as the minimum Lee weight of $\psi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$.*

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

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

An upper bound on the minimum Hamming distance of a binary self-dual code was given in [18]. 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. **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 $A = \text{circ}(\alpha_1, \alpha_2 \ldots, \alpha_n)$, 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 $\text{CIRC}(A_1, A_2, \ldots A_n)$, where A_i are $k \times k$ 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, i.e., $A^T_{ij} = A_{ji}$.

A standard generator matrix of a self-dual code has the form of $(I|A)$, where A is a matrix in which the rows are fully determined by the first row, for example circulant and reverse circulant matrices. We want to take a different approach to this and we want to replace A of the standard generator matrix with a matrix in which the rows do not only depend on the previous row, equivalently, the first row. A perfect fit for this is to consider a bisymmetric matrix. We now give a formal definition.

Definition. *A bisymmetric matrix is a square matrix that is symmetric about both of its main diagonals.*

We now give an example of a bisymmetric matrix.

Example. *The matrix:*

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_2 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_4 \\ \alpha_3 & \alpha_7 & \alpha_9 & \alpha_7 & \alpha_3 \\ \alpha_4 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_2 \\ \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 \end{pmatrix},$$

is a 5×5 bisymmetric matrix. As we can see, the rows of this matrix are not determined by the elements in first row.

We talk about the advantages of applying the bisymmetric matrix to search for self-dual codes in the next section where we introduce the main construction. In this 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 [15]. It was extended to Frobenius rings in [11]. 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 $v = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$. 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 $G = C_2$. Let $G = \langle x \mid x^2 = 1 \rangle \cong C_2$. If $v = \sum_{i=0}^{1} \alpha_{i+1} x^i \in RC_2$, then $\sigma(v) = \mathrm{circ}(\alpha_1, \alpha_2)$ where $\alpha_1, \alpha_2 \in R$.

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:

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

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

3. The Main Construction

In this section, we present the main construction of this work. As mentioned previously, we combine together the idea of a bisymmetric matrix and matrices that come from group rings.

Let $v_i \in RG$, where $1 \leq i \leq 6$, R is a finite commutative Frobenius ring of characteristic 2 and G is a finite group of order n. Additionally, let $B_1 = \mathrm{circ}(\alpha_1, \underbrace{\alpha_2, \ldots, \alpha_2}_{n-1})$ and $B_2 = \mathrm{circ}(\underbrace{\alpha_3, \ldots, \alpha_3}_{n})$ where $\alpha_i \in R$. Define the following matrix:

$$M_\sigma = \left[\begin{array}{cc:cc|c} B_1 & B_2 & & & \sigma(v_1)\ \sigma(v_2)\ \sigma(v_3)\ \sigma(v_4) \\ & & I_{2n} & & \\ B_2 & B_1 & & & \sigma(v_2)\ \sigma(v_5)\ \sigma(v_6)\ \sigma(v_3) \\ \hdashline & & B_1 & B_2 & \sigma(v_3)\ \sigma(v_6)\ \sigma(v_5)\ \sigma(v_2) \\ & I_{2n} & & & \\ & & B_2 & B_1 & \sigma(v_4)\ \sigma(v_3)\ \sigma(v_2)\ \sigma(v_1) \end{array}\right]$$

Let C_σ be the code that is generated by the matrix M_σ. Then, the code C_σ has length $8n$. We now state the following result.

Theorem 3.1. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite group of order n. Then C_σ is a self-dual code of length $8n$ iff*

1. $1 + \alpha_1^2 = 0$,
2. $n\alpha_2^2 + n\alpha_3^2 = 0$,
3. $v_1 v_1^* + v_2 v_2^* + v_3 v_3^* + v_4 v_4^* = 0$,
4. $v_1 v_2^* + v_2 v_5^* + v_3 v_6^* + v_4 v_3^* = 0$,

(5) $v_1v_3^* + v_2v_6^* + v_3v_5^* + v_4v_2^* = 0$,
(6) $v_1v_4^* + v_2v_3^* + v_3v_2^* + v_4v_1^* = 0$,
(7) $v_2v_2^* + v_5v_5^* + v_6v_6^* + v_3v_3^* = 0$,
(8) $v_2v_3^* + v_5v_6^* + v_6v_5^* + v_3v_2^* = 0$

and

$$rank\begin{pmatrix}\sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10})\\ \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14})\end{pmatrix} = 2n,$$

where

$$\begin{array}{llll} v_7 = & v_3+\alpha_1v_1+w(\alpha_2v_1+\alpha_3v_2), & v_8 = & v_6+\alpha_1v_2+w(\alpha_2v_2+\alpha_3v_5),\\ v_9 = & v_5+\alpha_1v_3+w(\alpha_2v_3+\alpha_3v_6), & v_{10} = & v_2+\alpha_1v_4+w(\alpha_2v_4+\alpha_3v_3),\\ v_{11} = & v_4+\alpha_1v_2+w(\alpha_3v_1+\alpha_2v_2), & v_{12} = & v_3+\alpha_1v_5+w(\alpha_3v_2+\alpha_2v_5),\\ v_{13} = & v_2+\alpha_1v_6+w(\alpha_3v_3+\alpha_2v_6), & v_{14} = & v_1+\alpha_1v_3+w(\alpha_3v_4+\alpha_2v_3)\end{array}$$

and $w = \sum_{g\in G} g \in RG$.

Proof. Let $M_\sigma = (M_1 \quad M_2)$ where $M_1 = \begin{pmatrix}B_1 & B_2 & I_n & 0\\ B_2 & B_1 & 0 & I_n\\ I_n & 0 & B_1 & B_2\\ 0 & I_n & B_2 & B_1\end{pmatrix}$ and $M_2 = \begin{pmatrix}\sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4)\\ \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3)\\ \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2)\\ \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1)\end{pmatrix}$, $B_1 = \alpha_1 I_n + \sigma(\alpha_2 w)$, $B_2 = \sigma(\alpha_3 w)$ and $w = \sum_{g\in G} g \in RG$. Clearly, $M_\sigma M_\sigma^T = M_1M_1^T + M_2M_2^T$. It is well known that w is contained in the center of the group ring RG. Clearly for any square matrices A and B of same size over the ring R, $(A+B)^2 = A^2 + B^2$ iff $AB = BA$. We have

$$\begin{aligned} M_1M_1^T &= \begin{pmatrix}\alpha_1I_n+\sigma(\alpha_2w) & \sigma(\alpha_3w) & I_n & 0\\ \sigma(\alpha_3w) & \alpha_1I_n+\sigma(\alpha_2w) & 0 & I_n\\ I_n & 0 & \alpha_1I_n+\sigma(\alpha_2w) & \sigma(\alpha_3w)\\ 0 & I_n & \sigma(\alpha_3w) & \alpha_1I_n+\sigma(\alpha_2w)\end{pmatrix}^2\\ &= \left(\alpha_1I_{4n} + \begin{pmatrix}\sigma(\alpha_2w) & \sigma(\alpha_3w) & I_n & 0\\ \sigma(\alpha_3w) & \sigma(\alpha_2w) & 0 & I_n\\ I_n & 0 & \sigma(\alpha_2w) & \sigma(\alpha_3w)\\ 0 & I_n & \sigma(\alpha_3w) & \sigma(\alpha_2w)\end{pmatrix}\right)^2\\ &= \alpha_1^2I_{4n} + \begin{pmatrix}\sigma(\alpha_2w) & \sigma(\alpha_3w) & I_n & 0\\ \sigma(\alpha_3w) & \sigma(\alpha_2w) & 0 & I_n\\ I_n & 0 & \sigma(\alpha_2w) & \sigma(\alpha_3w)\\ 0 & I_n & \sigma(\alpha_3w) & \sigma(\alpha_2w)\end{pmatrix}^2 \end{aligned}$$

because I_{4n} commutes with any $4n\times 4n$-matrix. Moreover

$$M_1M_1^T = \alpha_1^2I_{4n} + I_{4n} + \begin{pmatrix}\sigma(\alpha_2w) & \sigma(\alpha_3w) & 0 & 0\\ \sigma(\alpha_3w) & \sigma(\alpha_2w) & 0 & 0\\ 0 & 0 & \sigma(\alpha_2w) & \sigma(\alpha_3w)\\ 0 & 0 & \sigma(\alpha_3w) & \sigma(\alpha_2w)\end{pmatrix}^2$$

because $\left(\begin{smallmatrix}0 & I_{2n}\\ I_{2n} & 0\end{smallmatrix}\right)^2 = I_{4n}$ and $\left(\begin{smallmatrix}0 & I_{2n}\\ I_{2n} & 0\end{smallmatrix}\right)$ commutes with any $4n\times 4n$-matrix matrix of form $\left(\begin{smallmatrix}B & 0\\ 0 & B\end{smallmatrix}\right)$. Clearly $\sigma(w)^2 = n\sigma(w)$. So

$$\begin{aligned} M_1M_1^T &= (1+\alpha_1^2)I_{4n} + \mathrm{CIRC}\left(\begin{pmatrix}\sigma(n(\alpha_2^2+\alpha_3^2)w) & \sigma(2n\alpha_2\alpha_3w)\\ \sigma(2n\alpha_2\alpha_3w) & \sigma(n(\alpha_2^2+\alpha_3^2)w)\end{pmatrix}, 0\right)\\ &= (1+\alpha_1^2)I_{4n} + \mathrm{CIRC}(\sigma(n(\alpha_2^2+\alpha_3^2)w), 0, 0, 0). \end{aligned}$$

Additionally,

$$M_2M_2^T = \begin{pmatrix} \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix} \begin{pmatrix} \sigma(v_1^*) & \sigma(v_2^*) & \sigma(v_3^*) & \sigma(v_4^*) \\ \sigma(v_2^*) & \sigma(v_5^*) & \sigma(v_6^*) & \sigma(v_3^*) \\ \sigma(v_3^*) & \sigma(v_6^*) & \sigma(v_5^*) & \sigma(v_2^*) \\ \sigma(v_4^*) & \sigma(v_3^*) & \sigma(v_2^*) & \sigma(v_1^*) \end{pmatrix}$$
$$= \begin{pmatrix} \sigma(v_1v_1^*+v_2v_2^*+v_3v_3^*+v_4v_4^*) & \sigma(v_1v_2^*+v_2v_5^*+v_3v_6^*+v_4v_3^*) & \sigma(v_1v_3^*+v_2v_6^*+v_3v_5^*+v_4v_2^*) & \sigma(v_1v_4^*+v_2v_3^*+v_3v_2^*+v_4v_1^*) \\ \sigma(v_2v_1^*+v_5v_2^*+v_6v_3^*+v_3v_4^*) & \sigma(v_2v_2^*+v_5v_5^*+v_6v_6^*+v_3v_3^*) & \sigma(v_2v_3^*+v_5v_6^*+v_6v_5^*+v_3v_2^*) & \sigma(v_2v_4^*+v_5v_3^*+v_6v_2^*+v_3v_1^*) \\ \sigma(v_3v_1^*+v_6v_2^*+v_5v_3^*+v_2v_4^*) & \sigma(v_3v_2^*+v_6v_5^*+v_5v_6^*+v_2v_3^*) & \sigma(v_3v_3^*+v_6v_6^*+v_5v_5^*+v_2v_2^*) & \sigma(v_3v_4^*+v_6v_3^*+v_5v_2^*+v_2v_1^*) \\ \sigma(v_4v_1^*+v_3v_2^*+v_2v_3^*+v_1v_4^*) & \sigma(v_4v_2^*+v_3v_5^*+v_2v_6^*+v_1v_3^*) & \sigma(v_4v_3^*+v_3v_6^*+v_2v_5^*+v_1v_2^*) & \sigma(v_4v_4^*+v_3v_3^*+v_2v_2^*+v_1v_1^*) \end{pmatrix}.$$

Clearly, C_σ is self-orthogonal iff $1+\alpha_1^2=0$, $n\alpha_2^2+n\alpha_3^2=0$, $v_1v_1^*+v_2v_2^*+v_3v_3^*+v_4v_4^*=0$, $v_1v_2^*+v_2v_5^*+v_3v_6^*+v_4v_3^*=0$, $v_1v_3^*+v_2v_6^*+v_3v_5^*+v_4v_2^*=0$, $v_1v_4^*+v_2v_3^*+v_3v_2^*+v_4v_1^*=0$, $v_2v_2^*+v_5v_5^*+v_6v_6^*+v_3v_3^*=0$, $v_2v_3^*+v_5v_6^*+v_6v_5^*+v_3v_2^*=0$, $v_2v_4^*+v_5v_3^*+v_6v_2^*+v_3v_1^*=0$ and $v_3v_4^*+v_6v_3^*+v_5v_2^*+v_2v_1^*=0$. We note here that the last two conditions are the result of the fifth and fourth conditions respectively. Namely, $v_1v_3^*+v_2v_6^*+v_3v_5^*+v_4v_2^*=0 \implies v_2v_4^*+v_5v_3^*+v_6v_2^*+v_3v_1^*=0$, that is $0=0^*=(v_1v_3^*+v_2v_6^*+v_3v_5^*+v_4v_2^*)^*=v_3v_1^*+v_6v_2^*+v_5v_3^*+v_2v_4^*=v_2v_4^*+v_5v_3^*+v_6v_2^*+v_3v_1^*$ and similarly $v_1v_2^*+v_2v_5^*+v_3v_6^*+v_4v_3^*=0 \implies v_3v_4^*+v_6v_3^*+v_5v_2^*+v_2v_1^*=0$, that is $0=0^*=(v_1v_2^*+v_2v_5^*+v_3v_6^*+v_4v_3^*)^*=v_2v_1^*+v_5v_2^*+v_6v_3^*+v_3v_4^*=v_3v_4^*+v_6v_3^*+v_5v_2^*+v_2v_1^*$. Now,

$$\begin{aligned} B_1^2+B_2^2+I_n &= (\alpha_1I_n+\sigma(\alpha_2w))^2+(\sigma(\alpha_3w))^2+I_n \\ &= \alpha_1^2I_n+\sigma((\alpha_2w)^2)+\sigma((\alpha_3w)^2)+I_n \\ &= \alpha_1^2I_n+\sigma(\alpha_2^2w^2+\alpha_3^2w^2)+I_n \\ &= \alpha_1^2I_n+\sigma(\alpha_2^2(nw)+\alpha_3^2(nw))+I_n \\ &= \alpha_1^2I_n+\sigma((n\alpha_2^2+n\alpha_3^2)w)+I_n \\ &= (1)I_n+\sigma((0)w)+I_n \\ &= 2I_n+\sigma(0) \\ &= 0. \end{aligned}$$

Consequently,

$$\begin{aligned} M_1\begin{pmatrix} I_n & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 \\ B_1 & B_2 & I_n & 0 \\ B_2 & B_1 & 0 & I_n \end{pmatrix} &= \begin{pmatrix} B_1 & B_2 & I_n & 0 \\ B_2 & B_1 & 0 & I_n \\ I_n & 0 & B_1 & B_2 \\ 0 & I_n & B_2 & B_1 \end{pmatrix}\begin{pmatrix} I_n & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 \\ B_1 & B_2 & I_n & 0 \\ B_2 & B_1 & 0 & I_n \end{pmatrix} \\ &= \begin{pmatrix} 2B_1 & 2B_2 & I_n & 0 \\ 2B_2 & 2B_1 & 0 & I_n \\ B_1^2+B_2^2+I_n & 2B_1B_2 & B_1 & B_2 \\ 2B_1B_2 & B_2^2+B_1^2+I_n & B_2 & B_1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & I_n & 0 \\ 0 & 0 & 0 & I_n \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & B_2 & B_1 \end{pmatrix} \end{aligned}$$

and

$$\mathrm{rank}M_\sigma = \mathrm{rank}\begin{pmatrix} I_n & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & I_n & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ B_1 & B_2 & \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ B_2 & B_1 & \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix}.$$

It is interesting to note that $B_1=\alpha_1I_n+\sigma(\alpha_2w)=\sigma(\alpha_1e+\alpha_2w)$ as $I_n=\sigma(e)$, where e be identity element of group G. Additionally,

$$\mathrm{rank}M_\sigma = \mathrm{rank}\begin{pmatrix} \sigma(e) & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & \sigma(e) & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ \sigma(\alpha_1e+\alpha_2w) & \sigma(\alpha_3w) & \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ \sigma(\alpha_3w) & \sigma(\alpha_1e+\alpha_2w) & \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix} =$$

$$\operatorname{rank}\left[\begin{pmatrix} I_n & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 \\ \sigma(\alpha_1 e+\alpha_2 w) & \sigma(\alpha_3 w) & I_n & 0 \\ \sigma(\alpha_3 w) & \sigma(\alpha_1 e+\alpha_2 w) & 0 & I_n \end{pmatrix} \times \begin{pmatrix} \sigma(e) & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & \sigma(e) & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ \sigma(\alpha_1 e+\alpha_2 w) & \sigma(\alpha_3 w) & \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ \sigma(\alpha_3 w) & \sigma(\alpha_1 e+\alpha_2 w) & \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix}\right] =$$

$$\operatorname{rank}\begin{pmatrix} \sigma(e) & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & \sigma(e) & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ 0 & 0 & \sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10}) \\ 0 & 0 & \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14}) \end{pmatrix},$$

where

$$\begin{array}{llll} v_7 = & v_3+\alpha_1 v_1+w(\alpha_2 v_1+\alpha_3 v_2), & v_8 = & v_6+\alpha_1 v_2+w(\alpha_2 v_2+\alpha_3 v_5), \\ v_9 = & v_5+\alpha_1 v_3+w(\alpha_2 v_3+\alpha_3 v_6), & v_{10} = & v_2+\alpha_1 v_4+w(\alpha_2 v_4+\alpha_3 v_3), \\ v_{11} = & v_4+\alpha_1 v_2+w(\alpha_3 v_1+\alpha_2 v_2), & v_{12} = & v_3+\alpha_1 v_5+w(\alpha_3 v_2+\alpha_2 v_5), \\ v_{13} = & v_2+\alpha_1 v_6+w(\alpha_3 v_3+\alpha_2 v_6), & v_{14} = & v_1+\alpha_1 v_3+w(\alpha_3 v_4+\alpha_2 v_3). \end{array}$$

Hence,

$$\operatorname{rank} M_\sigma = 2n+\operatorname{rank}\begin{pmatrix} \sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10}) \\ \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14}) \end{pmatrix}.$$

Finally, the self-orthogonal code C_σ is self-dual iff

$$\operatorname{rank}\begin{pmatrix} \sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10}) \\ \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14}) \end{pmatrix} = 2n.$$

□

If we assume that the group G is Abelian, we get the following result.

Corollary 3.2. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be an Abelian finite group of order n. Then C_σ is a self-dual code of length $8n$ if*

(1) $1+\alpha_1^2 = 0$,
(2) $n\alpha_2^2 + n\alpha_3^2 = 0$,
(3) $v_1^2+v_2^2+v_3^2+v_4^2 = 0$,
(4) $v_1v_3+v_2v_4+v_3v_5+v_2v_6 = 0$,
(5) $(v_2+v_3)(v_1+v_4+v_5+v_6) = 0$,
(6) $(v_1+v_4+v_5+v_6)^2 = 0$.

Proof. From Theorem 3.1 we have the first two conditions. Since G is Abelian then $v^* = v$ for any $v \in RG$. The equations $(3)-(8)$ in Theorem 3.1 are equivalent to

$$\begin{gathered} v_1^2+v_2^2+v_3^2+v_4^2 = 0, \\ v_1v_2+v_2v_5+v_3v_6+v_3v_4 = 0, \\ v_1v_3+v_2v_4+v_2v_6+v_3v_5 = 0, \\ v_1v_4+v_1v_4+v_2v_3+v_2v_3 = 0, \\ v_2^2+v_5^2+v_6^2+v_3^2 = 0, \\ v_2v_3+v_2v_3+v_5v_6+v_5v_6 = 0, \end{gathered}$$

or

$$\begin{gathered} v_1^2+v_2^2+v_3^2+v_4^2 = 0, \\ v_1v_2+v_2v_5+v_3v_6+v_3v_4 = 0, \\ v_1v_3+v_2v_4+v_2v_6+v_3v_5 = 0, \\ 0 = 0, \\ v_2^2+v_5^2+v_6^2+v_3^2 = 0, \\ 0 = 0. \end{gathered}$$

Adding the 5th equation to the 1st one, the 2nd equation to the third one (omitting the tautology) we obtain the required equations:

$$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0,$$
$$v_1v_2 + v_2v_5 + v_3v_6 + v_3v_4 = 0,$$
$$(v_2 + v_3)(v_1 + v_4 + v_5 + v_6) = 0,$$
$$v_1^2 + v_4^2 + v_5^2 + v_6^2 = 0.$$

□

We can clearly see that the search field is greater in our construction than in the standard generator matrix of the form $(I_n|A)$, where I_n is the identity matrix and A is a matrix that is fully defined by the elements in the first row. Also, $\sigma(v_i)$ represent matrices that come from group rings. This means that we can create many different M_σ matrices by considering different groups in the group rings- this is another advantage of our construction. We next apply the above matrix to search for extremal self-dual codes.

4. Results

In this section, we apply the above construction to the ring $\mathbb{F}_4 + u\mathbb{F}_4$ to obtain self-dual codes whose binary images have parameters $[64, 32, 12]$ when $G = C_2$. Next, we extend these codes to obtain new self-dual codes of length 68. We finally consider their possible neighbours and find more new self-dual codes of length 68. We implement the search of self-dual codes over the alphabets using the software *MAGMA* ([1]).

4.1. $[64, 32, 12]$ **Singly-Even Codes.** There are two possibilities for the weight enumerators of extremal singly-even $[64, 32, 12]_2$ codes ([2]):

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

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

With the most updated information, the existence of codes is known for $\beta = 14, 18, 22, 25, 29, 32, 35, 36, 39, 44, 46, 53, 59, 60, 64$ and 74 in $W_{64,1}$ and for $\beta = 0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, \ldots, 25, 28, 29, 30, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120$ and 184 in $W_{64,2}$.

Using the above method when $G = C_2$ over $\mathbb{F}_4 + u\mathbb{F}_4$, we obtain many extremal codes of length 64. To save space, we will only list two. These codes in turn are used to find new codes of length 68. Recall that the above construction involves $v_i \in RC_2$ for $i \in \{1, \ldots, 6\}$. Instead of listing each v_i separately, we list $(v_1, \ldots, v_6)$ as one vector.

Table 1. Codes of length 64 and their β values

$\mathcal{C}_i$	$(\alpha_1, \alpha_2, \alpha_3)$	$(v_1, \ldots, v_6)$	$\lvert Aut(\mathcal{C}_i)\rvert$	$W_{64,2}$	$\mathcal{C}_i$	$(\alpha_1, \alpha_2, \alpha_3)$	$(v_1, \ldots, v_6)$	$\lvert Aut(\mathcal{C}_i)\rvert$	$W_{64,2}$
1	$(0, 4, 2)$	$(A, 1, 0, 0, 4, 4, 1, 7, A, 1, 7, 1)$	2^5	$\beta = 0$	2	$(0, E, 2)$	$(A, 3, 0, 1, 4, 7, 5, 3, 4, 3, 4, 4)$	$2^4 \cdot 3$	$\beta = 64$

4.2. **New Extremal Self-Dual Binary Codes of Length 68 from $\mathbb{F}_2 + u\mathbb{F}_2$ Extensions.** The possible weight enumerator of a self-dual $[68, 34, 12]_2$-code is in one of the following forms ([18]):

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

where $0 \leq \gamma \leq 9$. Recently, in [20], Yankov et al. constructed the first examples of codes with a weight enumerator for $\gamma = 7$ in $W_{68,2}$. In [5], [7] and [13] more unknown $W_{68,2}$ codes were constructed. Together with these, the existence of the codes in $W_{68,2}$ is known for;

$\gamma = 1,\ \beta \in \{2m | m = 15, 20, 21, 22, 24, \ldots, 99, 102\}$ or $\beta \in \{2m+1 | m = 23, \ldots, 85, 87\}$;

$\gamma = 2,\ \beta \in \{2m\,| m = 29, \ldots, 100, 103, 104\}$ or $\beta \in \{2m+1\,| m = 31, 32, 34, \ldots, 79, 80, 82, 84, 85, 86\}$;

$\gamma = 3,\ \beta \in \{2m\,| m = 38, 40, \ldots, 98, 101, 102\}$ or

$\beta \in \{2m+1 | m = 41, 43, \ldots, 77, 79, 80, 81, 83, 87, 88, 96\}$;

$\gamma = 5$ with $\beta \in \{m | m = 107, 113, 115, \ldots, 182, 187, 189, 191, 193\}$;

$\gamma = 6$ with $\beta \in \{2m | m = 59, 63, \ldots, 66, 69, 77, 78, 79, 81, 88\}$ or $\beta \in \{2m+1\,| m = 62, \ldots, 65\}$.

We now describe a technique for extending self-dual codes..

Theorem 4.1. *([10]) Let 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 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 D over R of length $n+2$.

Theorem 4.1 is applied to the $\psi_{\mathbb{F}_4+u\mathbb{F}_4}$-images of the codes in Table 1. The results are tabulated in Table 2, where $1+u$ in $\mathbb{F}_2 + u\mathbb{F}_2$ is denoted as 3.

TABLE 2. New codes of length 68 from Theorem 4.1

$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β	$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β
$\mathcal{C}_{68,1}$	2	1	(133u330310100uu130u0313311110u03)	**1**	**173**	$\mathcal{C}_{68,2}$	2	1	(331031u1101uuu01100033311133uuu1)	**1**	**177**
$\mathcal{C}_{68,3}$	2	1	(313u31031u1000u1100u33311131u001)	**1**	**181**	$\mathcal{C}_{68,4}$	2	1	(1010u113u3u3011u1u3uuu13u33uu1u1)	**2**	**167**
$\mathcal{C}_{68,5}$	2	1	(11u033013u3uu0u0u0003110013133u0)	**2**	**175**	$\mathcal{C}_{68,6}$	2	3	(00u11333330uu00uu30130100300u311)	**2**	**177**
$\mathcal{C}_{68,7}$	2	3	(331u33uu10u000u1303uu03u0033u0u3)	**2**	**179**	$\mathcal{C}_{68,8}$	2	1	(013u331u0uu1uu3u3uu33u033101333u)	**2**	**181**
$\mathcal{C}_{68,9}$	2	3	(0003uu3u1u03013u300003013311111u0)	**2**	**183**	$\mathcal{C}_{68,10}$	2	1	(u0u3u03u3uu1011010u0010131111100)	**2**	**187**
$\mathcal{C}_{68,11}$	2	1	(31u11u133u10013011u01103u033u110)	**2**	**191**	$\mathcal{C}_{68,12}$	2	1	(0uu1uu1u3003011u10u0u301113331u0)	**2**	**197**
$\mathcal{C}_{68,13}$	1	3	(1u33u331u33330u10u130310u130u0uu)	**3**	**74**	$\mathcal{C}_{68,14}$	2	1	(uu01003u01003u30113131$uuuu$00330u)	**3**	**157**
$\mathcal{C}_{68,15}$	2	3	(11130u0u11013333u0u31uu3133$uuuuu$)	**3**	**181**	$\mathcal{C}_{68,16}$	2	3	(33u11u11303uu310110u310100110110)	**3**	**183**
$\mathcal{C}_{68,17}$	2	1	(u31u31300001uu303003100311033310)	**3**	**185**	$\mathcal{C}_{68,18}$	2	1	(13330u13u311011131u113u3u3u300u3)	**3**	**187**
$\mathcal{C}_{68,19}$	2	1	(01301130uu030u1010u31u033103331u)	**3**	**195**	$\mathcal{C}_{68,20}$	2	1	(031u3330uu01001010u3300131011330)	**3**	**197**
$\mathcal{C}_{68,21}$	2	1	(131100110111u311130313u3u1030uu3)	**3**	**199**	$\mathcal{C}_{68,22}$	2	1	(11310011013303311103 11u301010003)	**3**	**201**
$\mathcal{C}_{68,23}$	2	1	(u310313$uuuu$1003u10u31u0111011130)	**3**	**203**	$\mathcal{C}_{68,24}$	2	1	(u1303310u003uu1u30u13uu131u3311u)	**3**	**217**
$\mathcal{C}_{68,25}$	2	1	(u31u111uuu010u1u10u130u11301111u)	**5**	**205**	$\mathcal{C}_{68,26}$	2	1	(011u113uu0u3001u10u3300333u1311u)	**5**	**213**

4.3. **New Codes of length** 68 **from Neighbours.** Two self-dual binary codes of length $2n$ are said to be neighbours of each other if their intersection has dimension $n-1$. Let $x \in \mathbb{F}_2^{2n} - \mathcal{C}$ then $\mathcal{D} = \left\langle \langle x\rangle^{\perp} \cap \mathcal{C}, x \right\rangle$ is a neighbour of $\mathcal{C}$. We obtain 15 new codes of length 68 as neighbours of the codes in Table 2. The neighbours of the codes $\mathcal{C}_{15}$ and $\mathcal{C}_{16}$ have trivial automorphism. We set the first 34 entries of x to be 0, the rest of the vectors are listed in Table 3.

TABLE 3. New codes of length 68 as neighbours

$\mathcal{N}_{68,27}$	$\mathcal{C}_{68,26}$	(01011110001100010111110101111110111)	**5**	**183**	$\mathcal{N}_{68,28}$	$\mathcal{C}_{68,25}$	(01011100010001110111100110101011100)	**5**	**184**
$\mathcal{N}_{68,29}$	$\mathcal{C}_{68,25}$	(01101000111101111001000001001000000)	**5**	**185**	$\mathcal{N}_{68,30}$	$\mathcal{C}_{68,25}$	(10100110111000100010001001100111101)	**5**	**186**
$\mathcal{N}_{68,31}$	$\mathcal{C}_{68,26}$	(00000100001111100001100110001011101)	**5**	**188**	$\mathcal{N}_{68,32}$	$\mathcal{C}_{68,25}$	(11011010100101101010010010010001110)	**5**	**190**
$\mathcal{N}_{68,33}$	$\mathcal{C}_{68,25}$	(01011111101110000000110101000101101)	**5**	**192**	$\mathcal{N}_{68,34}$	$\mathcal{C}_{68,26}$	(11111111111010010010011001110000001)	**5**	**194**
$\mathcal{N}_{68,35}$	$\mathcal{C}_{68,26}$	(11110010011000011101001111000000111)	**5**	**196**	$\mathcal{N}_{68,36}$	$\mathcal{C}_{68,26}$	(10000110110001010111111111110000010)	**5**	**197**
$\mathcal{N}_{68,37}$	$\mathcal{C}_{68,26}$	(00111010000101101011101110001011001)	**5**	**199**	$\mathcal{N}_{68,38}$	$\mathcal{C}_{68,26}$	(11010010111100101000100100100010011)	**5**	**203**
$\mathcal{N}_{68,39}$	$\mathcal{C}_{68,26}$	(10101101010001101001101011111000001)	**5**	**204**	$\mathcal{N}_{68,40}$	$\mathcal{C}_{68,26}$	(00100011010000010101000101010110 11)	**6**	**192**
$\mathcal{N}_{68,41}$	$\mathcal{C}_{68,26}$	(10100110001111001010011110000001100)	**6**	**210**					

5. Conclusion

In this paper, we presented a construction in which we combined the idea of a bisymmetric matrix and group rings. This construction was applied over $\mathbb{F}_4 + u\mathbb{F}_4$ to search for self-dual codes whose binary images have parameters $[64, 32, 12]$. The Gray map $(\mathbb{F}_4 + u\mathbb{F}_4)^n \to \mathbb{F}_2^{4n}$ was employed next to produce a binary self-dual code of length $4n$. Next, a building up method over $\mathbb{F}_2 + u\mathbb{F}_2$ was used to find new extremal self-dual codes of length 68. Of those we considered possible neighbours which are also new self-dual codes of length 68. In particular, we construct the following unknown $W_{68,2}$ codes:

$$
\begin{aligned}
&(\gamma = 1, \quad \beta = \{173, 177, 181\}),\\
&(\gamma = 2, \quad \beta = \{167, 175, 177, 179, 181, 183, 187, 191, 197\}),\\
&(\gamma = 3, \quad \beta = \{74, 157, 181, 183, 185, 187, 195, 197, 199, 201, 203, 217\}),\\
&(\gamma = 5, \quad \beta = \{183, 184, 185, 186, 188, 190, 192, 194, 196, 197, 199, 203, 204, 205, 213\})\\
&(\gamma = 6, \quad \beta = \{192, 210\}).
\end{aligned}
$$

The main advantage of our construction over the standard generator matrices that produce self-dual codes is that the search field is greater in the matrix M_σ than in the standard one. Namely, a standard generator matrix of a self-dual code has the form $(I|A)$ where I is the identity matrix and A is a matrix that is fully defined by the elements in the first row. In our construction, A is replaced with a bisymmetric matrix in which the blocks are matrices that come from group rings. The bisymmetric design itself opens up more 'freedom' when searching for self-dual codes as the elements in the blocks that are in the middle of the two rows of M_σ are independent of the elements of blocks that are in the first row. Additionally, we replace the identity matrix with a block matrix to expand the search field even more. We note here, that this block matrix has a fixed structure while the bisymmetric matrix can lead to different designs if different groups are considered. It therefore follows, that a suggestion for further work would be to consider groups different from the group C_2 that we used in this work. Also, groups of higher orders could be considered, but this would increase the search field significantly. Another possible direction is to determine if our main construction can be applied to search for the MDS (Maximal Distance Separable) codes.

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] 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, 6, 1319-1333, 1990.

[3] S.T. Dougherty, "Algebraic Coding Theory over Finite Commutative Rings", Springer Briefs in Mathematics. Springer, 2017.

[4] 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, 32-45, 1999.

[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. Kaya, "2^n Bordered Constructions of Self-Dual codes from Group Rings", **submitted**.

[7] S.T. Dougherty, J. Gildea, A. Kaya, A. Korban, A. Tylyshchak and B. Yildiz, "Bordered Constructions of Self-Dual Codes from Group Rings and New Extremal Binary Self-Dual Codes", Finite Fields Appl., vol. 57, 108-127, 2019.

[8] S. T. Dougherty, J. Gildea, A. Kaya, A. Korban, "Composite Constructions of Self-Dual Codes from Group Rings and New Extremal Self-Dual Binary Codes of Length 68", Advances in Mathematics of Communications, doi: 10.3934/amc.2020037.
[9] S.T. Dougherty, J. Gildea, A. Kaya, A. Korban, (**in press**) "New Extremal Self-Dual Binary Codes of Length 68 via Composite Construction, $\mathbb{F}_2 + u\mathbb{F}_2$ Lifts, Extensions and Neighbors", International Journal of Information and Coding Theory.
[10] S.T. Dougherty, J. L. Kim, H. Kulosman and H. Liu, "Self-Dual Codes over Commutative Frobenius rings", Finite FIelds and Applications, vol. 16, no. 1, pp. 14-26, 2010.
[11] 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., vol. 86, no. 9, 2115-2138, 2018.
[12] P. Gaborit, V. Pless, P. Sole and O. Atkin, "Type II codes over $\mathbb{F}_4$", Finite Fields Appl., vol. 8, 171-183, 2002.
[13] J. Gildea, A .Kaya, R. Taylor and B. Yildiz, "Constructions for Self-dual Codes Induced from Group Rings", Finite Fields Appl., vol. 51, 71-92, 2018.
[14] T.A. Gulliver and M. Harada, "Classification of Extremal double circulant self-dual codes of lengths 74-88", Discrete Mathematics, vol. 306, no. 17, pp. 2064-2072, 2006.
[15] T. Hurley, "Group Rings and Rings of Matrices", Int. Jour. Pure and Appl. Math, vol. 31, no. 3, pp. 319-335, 2006.
[16] S. Karadeniz and B. Yildiz, "Double-circulant and bordered-double-circulant constructions for self-dual codes over R_2", Advances in Mathematics of Communications, vol. 6, no. 2, pp. 193-202, 2012.
[17] S. Ling, P. Sole, "Type II Codes Over $\mathbb{F}_4 + u\mathbb{F}_4$", Europ. J. Combinatorics, vol. 22, 983-997, 2001.
[18] E.M. Rains,"Shadow Bounds for Self-Dual Codes", IEEE Trans. Inf. Theory, vol. 44, 134-139, 1998.
[19] M. Ventou and C. Rigoni, "Self-dual doubly circulant codes", Discrete Mathematics, vol. 56, no. 2-3, pp. 291-298, 1985.
[20] 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.

Department of Mathematical and Physical Sciences, Thornton Science Park, University of Chester, England
Email address: j.gildea@chester.ac.uk

Department of Mathematics Education, Sampoerna University, 12780, Jakarta, Indonesia
Email address: abidin.kaya@sampoernauniversity.ac.id

Department of Mathematical and Physical Sciences, Thornton Science Park, University of Chester, England
Email address: adrian3@windowslive.com

Department of Algebra, Uzhgorod National University, Uzhgorod, Ukraine
Email address: alxtlk@bigmir.net