NEW SELF-DUAL AND FORMALLY SELF-DUAL CODES FROM GROUP RING CONSTRUCTIONS

STEVEN T. DOUGHERTY
Department of Mathematics
University of Scranton
Scranton, PA 18510, USA

JOE GILDEA
Department of Mathematics
University of Chester
Chester, UK

ABIDIN KAYA
Department of Mathematics Education
Sampoerna University
12780, Jakarta, Indonesia

BAHATTIN YILDIRIZ*
Department of Mathematics & Statistics
Northern Arizona University
Flagstaff, AZ 86011, USA

(Communicated by Sihem Mesnager)

Abstract. In this work, we study construction methods for self-dual and formally self-dual codes from group rings, arising from the cyclic group, the dihedral group, the dicyclic group and the semi-dihedral group. Using these constructions over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$, we obtain 9 new extremal binary self-dual codes of length 68 and 25 even formally self-dual codes with parameters $[72, 36, 14]$.

1. Introduction

Self-dual and formally self-dual codes over fields and rings are important classes of codes. They have attracted a great deal of interest in terms of their relationship with designs, lattices, invariant theory and groups. Various constructions for self-dual and formally self-dual codes have been given in the literature, including the use of special types of matrices such as double circulant, bordered double circulant and four circulant matrices and constructions over different types of rings.

In [14], it was revealed that many of the well-known constructions arise from a special construction in group rings and that different groups lead to different constructions for self-dual codes.

In this paper, as a follow up on what was done in [14], we shall consider different groups to construct generator matrices that give formally self-dual and self-dual...
codes. The constructions are different than ones that have been used before in the literature. This novel approach allows us to find self-dual and formally self-dual codes that are new and whose automorphism group is different than those of the previously constructed codes.

Using modified group labelings for groups such as the cyclic group, the dihedral group, the dicyclic group and the semi-dihedral group, we come up with modified constructions for self-dual and formally self-dual codes. Using these constructions over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$, we find self-dual and formally self-dual codes of different lengths, some of which are new additions to the literature of known ones. Using the new constructions also provide us with codes that have new automorphism groups.

The rest of the paper is organized as follows. In Section 2, we give the main background on codes, self-dual and formally self-dual codes, group rings and the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$. In Section 3, we describe the constructions for self-dual and formally self-dual codes arising from the groups mentioned above. In Section 4, we give the computational results about the self-dual and formally self-dual codes found by using our methods. We tabulate the results and in particular, using $\mathbb{F}_2 + u\mathbb{F}_2$-extensions, we are able to find nine new extremal binary self-dual codes of length 68 and twenty five formally self-dual codes of parameters $[72, 36, 14]$, which are all better than the best known self-dual code of length 72. We finish the paper with some comments and possible directions for future research.

2. Definitions and notations

2.1. Codes. The alphabet we use for codes in this paper is the alphabet of finite commutative Frobenius rings. A commutative ring $R$ is Frobenius if $R$ is isomorphic as a module over itself to its character module $\hat{R}$. It is equivalent that this character module is generated by a single character.

Let $R$ be a finite Frobenius ring. A code $C$ of length $n$ over the ring $R$ is a subset of $R^n$. When the code is a submodule, then we say that the code is linear. To the ambient space we attach the usual inner-product, namely $[v, w] = \sum v_i w_i$. We denote by $C^\perp$ the dual code defined by $C^\perp = \{v \mid [v, w] = 0, \forall w \in C\}$. If a ring is Frobenius, then the MacWilliams relations apply and for all linear codes $C$ we have that $|C||C^\perp| = |R|^n$. See [18] for a complete description of these fact and for a description of codes over finite commutative Frobenius rings.

If $C \subseteq C^\perp$ we say that $C$ is a self-orthogonal code and, if $C = C^\perp$ then we say that $C$ is a self-dual code. If $C$ is equivalent to $C^\perp$, i.e., if $C$ can be obtained from $C^\perp$ by a permutation of coordinates, then $C$ is said to be isodual.

The Hamming weight enumerator of a code $C$ is defined as

$$W_C(x, y) = \sum_{c \in C} x^{n - \text{wt}_H(c)} y^{\text{wt}_H(c)}$$

where $\text{wt}_H(c)$ is the Hamming weight (number of non-zero entries) of the codeword $c$. If $W_C(x, y) = W_{C^\perp}(x, y)$ then $C$ is said to be a formally self-dual code. It follows immediately that self-dual and isodual codes are formally self-dual, but the converse is not true in general.

We will be considering two special Frobenius rings in constructing our examples, i.e., the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$. 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 $\mathbb{F}_4 + u\mathbb{F}_4$ defined via $u^2 = 0$ is a commutative binary ring of size 16. 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 $\langle u \rangle = \{0, u, u\omega, u + u\omega \}$. Note that $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2 + u\mathbb{F}_2$ and so we can describe any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $\omega a + \bar{u}b$ uniquely, where $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$.

The maps $\phi_1 : \mathbb{F}_2 + u\mathbb{F}_2 \rightarrow \mathbb{F}_2^2$, given by $\phi_1(a + ub) = (b, a + b)$ and $\varphi_{\mathbb{F}_4 + u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow (\mathbb{F}_2 + u\mathbb{F}_2)^{2n}$, $\alpha \omega + b\bar{\omega} \mapsto (a, b)$, $a, b \in (\mathbb{F}_2 + u\mathbb{F}_2)^n$ are orthogonality and distance preserving maps used in [16], and will be used here to construct binary self-dual codes.

2.2. Group rings. We give the standard definition of a group ring. Let $R$ be a ring and $G$ be a finite group. It is possible to use infinite groups but we shall only consider finite groups in this paper since we are using them to construct self-dual codes where the length is twice the size of the group. Let $G = \{g_1, g_2, \ldots, g_n\}$. An element of $RG$ is of the form $\sum_{i=1}^{n} a_i g_i$, $a_i \in R$, $g_i \in G$. Addition is given by coordinate addition, namely $\sum_{i=1}^{n} a_i g_i + \sum_{i=1}^{n} b_i g_i = \sum_{i=1}^{n} (a_i + b_i) g_i$ and the product is given by $(\sum_{i=1}^{n} a_i g_i)(\sum_{j=1}^{n} b_j g_j) = \sum_{i,j} a_i b_j g_i g_j$. This implies that the coefficient of $g_k$ in this product is $\sum_{g,j=g_k}^n a_i b_j$. Throughout the paper, we use $e_G$ to denote the identity element of the group. As is standard, we use $x^y$ to denote $yxy^{-1}$, where $x$ and $y$ are elements of the group $G$.

2.3. Circulant matrices. Circulant matrices and their variations will come up in many of the constructions that we will consider.

Recall that a circulant matrix over a ring $R$ is a matrix of the form

$$
circ(a_1, a_2, \ldots, a_n) = \begin{pmatrix}
    a_1 & a_2 & a_3 & \cdots & a_n \\
    a_n & a_1 & a_2 & \cdots & a_{n-1} \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    a_2 & a_3 & a_4 & \cdots & a_1 \\
\end{pmatrix} \in M_n(R) \quad (a_i \in R),
$$

while a reverse circulant matrix over a ring $R$ is a matrix of the form

$$
rcirc(a_1, a_2, \ldots, a_n) = \begin{pmatrix}
    a_1 & a_2 & a_3 & \cdots & a_n \\
    a_2 & a_3 & a_4 & \cdots & a_1 \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    a_n & a_1 & a_2 & \cdots & a_{n-1} \\
\end{pmatrix} \in M_n(R) \quad (a_i \in R).
$$

We note that a reverse circulant matrix is symmetric.

A generalization of circulant matrices can also be defined in the form of $g$-circulant matrices as follows: Let $0 \leq g \leq n$. A $g$-circulant matrix $B$ of order $n$ is a matrix of the form

$$
B = g - circ(a_1, a_2, \ldots, a_n) = \begin{pmatrix}
    a_1 & a_2 & \cdots & a_n \\
    a_{n-g+1} & a_{n-g+2} & \cdots & a_{n-g} \\
    a_{n-2g+1} & a_{n-2g+2} & \cdots & a_{n-2g} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{g+1} & a_{g+2} & \cdots & a_g \\
\end{pmatrix}
$$

where each subscript are calculated $\mod n$. Note that, each row of $B$ is the previous row moved $g$ places to the right.
3. Code constructions

The following construction was given in [9] for codes over rings, which is a straightforward generalization of a construction given by Hurley in [15].

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 $v \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be

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

(1)

We note that the elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are the elements of the group $G$ in some order. For $v \in RG$, the code $C(v)$ is defined as follows:

$$C(v) = \langle \sigma(v) \rangle.$$

Namely, the code $C(v)$ is formed by taking the row space of the matrix $\sigma(v)$. We note that matrix $\sigma(v)$ is not necessarily a linearly independent set of generators.

These codes are canonically ideals in the group ring.

3.1. Self-Dual codes. In this paper, we shall take a new construction coming from variations of the construction of the matrix $\sigma(v)$. Here the codes are not canonically ideals in the group ring, since we shall construct codes from matrices of the from $(I_k | A)$. We have immediately that any code of this form is a free code of rank $k$. Moreover, we have that $C^\perp$ is generated by the matrix $(-A^T | I_{n-k})$.

For a given matrix $A$ we define, $C(A)$ as the code generated by the matrix $(I_k | A)$.

**Theorem 3.1.** Let $R$ be a finite Frobenius ring of characteristic 2. Let $v = (v_i) \in R^k$. Let $\tau_1, \tau_2, \ldots, \tau_k$ be elements of the symmetric group $S_k$ such that $\tau_i$ is the identity and $\tau_j(a) \neq \tau_k(a)$ if $j \neq i$. Let the $j$-th row of $A$ be $\tau_j(v)$. If $[v, v] = 1$ and $[\tau_j(v), \tau_j'(v)] = 0$ when $j \neq j'$ then $C(A)$ is a self-dual code of length $n = 2k$.

**Proof.** We have that the code has free rank $k$ by construction. Since each row is a permutation of the first row and $[v, v] = 1$ then each row of $(I_k | A)$ is self-orthogonal. Since $[\tau_j(v), \tau_j'(v)] = 0$ when $j \neq j'$, then any two distinct rows of $(I_k | A)$ are orthogonal. This gives that $C(A)$ is a self-dual code. 

Essentially, the permutations $\tau$ are forming a Latin square on the positions $1, 2, \ldots, k$. However, the matrix $A$ is not necessarily a Latin square since the elements of $v$ may not be distinct. The theorem is saying that we want the matrix $A$ to satisfy $AA^T = I_k$ as usual. However we are not choosing $A$ arbitrarily, but rather we are going to produce the matrix $A$ via a series of permutations which is why we state the theorem in this manner. In general, we shall use the group ring in a variety ways to accomplish this theorem. Namely, the permutations $\tau_i$ are generally given using group actions as in the following corollary.

**Corollary 1.** Let $R$ be a finite Frobenius ring of characteristic 2, $G$ a finite group of size $k$. Denote the elements of the group by $g_1, \ldots, g_k$ and use these to index the rows and columns of $A$ and let $v = \sum g_i \alpha_i \in RG$. Let $A_{g_j, g_i} = \alpha_{g_j, g_i}$. If $\sum_{i=1}^k \alpha_{g_i} g_i = 0$ for all $g_j \neq e_G \in G$ and $\sum_{i=1}^k \alpha_{g_i} g_i = 1$ when $g_j = e_G$, then $C(A)$ is a self-dual code of length $n = 2k$. 


Proof. It is easy to see that the group action here gives $k$ permutations $\tau_j$ satisfying the conditions of Theorem 3.1. The fact that $\sum_{i=1}^k \alpha_i g_i g_j = 1$ and the fact $\sum_{i=1}^k \alpha_i g_i g_j = 0$ for all $g_j \neq e_G \in G$ gives that $[\tau_j(v), \tau_j'(v)] = 0$. Therefore, Theorem 3.1 gives that the code $C(A)$ is a self-dual code.

The most usual technique of constructing self-dual codes is a specific case of Corollary 1. Namely, the group $G$ is the cyclic group of order $k$. In that case, $A$ is a circulant matrix.

We will often generalize the construction in Corollary 1 to get different codes. For example, we have the following technique.

Consider the cyclic group of order $mn$, $C_{mn} = \langle x \mid x^{mn} = 1 \rangle$. We shall modify the usual circulant construction to obtain a new construction that is not simply a rearrangement of the columns.

Let
\begin{equation}
\alpha = \sum_{i=0}^{m-1} \left[a_i + x^n a_{i+1} + x^{2n} a_{i+2} + \cdots + x^{n(m-1)} a_{i+m-1}\right]
\end{equation}
be in $RC_{mn}$, where $a_i \in R$ and $m, n \geq 2$. Then, let
\begin{equation}
\rho(\alpha) = \begin{pmatrix}
A_1 & A_2 & A_3 & A_4 & \cdots & A_{n-1} & A_n \\
A'_n & A_1 & A_2 & A_3 & \cdots & A_{n-2} & A_{n-1} \\
A'_{n-1} & A'_n & A_1 & A_2 & \cdots & A_{n-3} & A_{n-2} \\
& & & & \vdots & \vdots \\
A''_3 & A'_4 & A'_5 & A'_6 & \cdots & A_1 & A_2 \\
A'_2 & A'_3 & A'_4 & A'_5 & \cdots & A'_n & A_1
\end{pmatrix}
\end{equation}
where $A_{j+1} = circ(a_1 + x^{mj}, a_2 + x^{mj}, \ldots, a_{m+ mj})$ and $A'_{j+1} = circ(a_{m+j}, a_{1+j}, \ldots, a_{(m-1)+nj})$. Then using $\rho(\alpha)$ as $A$ we consider codes that are generated by the following matrix:
\begin{equation}
I_{mn} = \begin{pmatrix}
A_1 & A_2 & A_3 & A_4 & \cdots & A_{n-1} & A_n \\
A'_n & A_1 & A_2 & A_3 & \cdots & A_{n-2} & A_{n-1} \\
A'_{n-1} & A'_n & A_1 & A_2 & \cdots & A_{n-3} & A_{n-2} \\
& & & & \vdots & \vdots \\
A''_3 & A'_4 & A'_5 & A'_6 & \cdots & A_1 & A_2 \\
A'_2 & A'_3 & A'_4 & A'_5 & \cdots & A'_n & A_1
\end{pmatrix}
\end{equation}
In this case, we shall call the constructed code $P(\alpha)$.

Note that except for trivial cases, this matrix is not equivalent to the circulant constructed matrix. We construct codes like this so that we can get codes which we do not get from the usual circulant construction.

3.2. Formally self-dual codes. We shall give constructions for producing isodual codes which are then formally self-dual codes.

**Theorem 3.2.** Let $R$ be a finite Frobenius ring of characteristic 2. Let $v = (v_i) \in R^k$. Let $\tau_1, \tau_2, \ldots, \tau_k$ be elements of the symmetric group $S_k$ such that $\tau_1$ is the identity and $\tau_j(a) \neq \tau_k(a)$ if $j \neq 1$. Let the $j$-th row of $A$ be $\tau_j(v)$. If $\tau_j(v_i) = \tau_i(v_j)$ then $C(A)$ is an isodual code of length $n = 2k$. 

**Proof.** It is easy to see that the group action here gives $k$ permutations $\tau_j$ satisfying the conditions of Theorem 3.1. The fact that $\sum_{i=1}^k \alpha_i g_i g_j = 1$ and the fact $\sum_{i=1}^k \alpha_i g_i g_j = 0$ for all $g_j \neq e_G \in G$ gives that $[\tau_j(v), \tau_j'(v)] = 0$. Therefore, Theorem 3.1 gives that the code $C(A)$ is a self-dual code.
Proof. We have that the code has free rank $k$ by construction. Since $\tau_j(v_i) = \tau_i(v_j)$ we have that $A = A^T$. Since the dual code of $C(A)$ is generated by the matrix $(A^T \mid I_k)$ we have that the code $C(A)$ is isodual. \hfill \Box

Here we are looking for matrices $A$ that satisfy $A = A^T$, but like in the self-dual case, we are constructing codes using the algebra of the group ring so we state the result in this manner for use in our construction.

**Corollary 2.** Let $R$ be a finite Frobenius ring of characteristic 2, $G$ a finite commutative group of size $k$. Denote the elements of the group by $g_1, \ldots, g_k$ and use these to index the rows and columns of $A$ and let $v = \sum \alpha_i g_i \in RG$. Let $A_{g_i,g_j} = \alpha_{g_i} g_j$. Then $C(A)$ is an isodual and therefore a formally self-dual code of length $n = 2k$.

**Proof.** It is easy to see that the group action here gives $k$ permutations $\tau_j$ satisfying the conditions of Theorem 3.2. Then $A_{g_i,g_j} = \alpha_{g_i} g_j = A_{g_i,g_j}$ which gives that $A = A^T$. Then, Theorem 3.2 gives that the code $C(A)$ is an isodual code. \hfill \Box

**Theorem 3.3.** Let $R$ be a finite Frobenius ring of characteristic 2, $C_{mn}$ the cyclic group of order $mn$ and $\alpha$ be an element of $RC_{mn}$. Then the matrix $(I_{mn} \mid \rho(\alpha))$ generates an isodual code over $R$.

**Proof.** Let $C$ be the code generated by $(I_{mn} \mid \rho(\alpha))$. Then its dual $C^\perp$ is generated by $(\rho(\alpha)^T \mid I_{mn})$. It is enough to show that $\rho(\alpha)$ and its transpose are permutationally equivalent. We get $\rho(\alpha)^T$ when we apply the reversing permutation

$$
\pi = \left( \begin{array}{ccccccc}
1 & 2 & 3 & \cdots & n-2 & n-1 & n \\
 n & n-1 & n-2 & \cdots & 3 & 2 & 1
\end{array} \right)
$$

blockwise to $\rho(\alpha)$ on its rows and columns. Hence $C$ and $C^\perp$ are permutationally equivalent. In other words, the code $C$ is isodual. \hfill \Box

We will now provide $\sigma(\alpha)$ for $\alpha \in RG$, where $G \in \{RD_{2t}, Dic_{4t}, SD_{2t}\}$. Here $D_{2t}$ is the dihedral group of order $2t$, $Dic_{4t}$ is the dihedral group of order $4t$ and $SD_{2t}$ is the semidihedral group of order $2t$.

Let $D_{2t} = \langle x,y \mid x^t = y^2 = 1, x^y = x^{-1} \rangle$, $t \geq 3$ and $\alpha = \sum_{i=1}^t (\alpha_i x^{i-1} + \alpha_{i+n} y x^{t-1}) \in RD_{2t}$. Then,

$$
(6) \quad \sigma(\alpha) = \begin{pmatrix} A & B \\ B & A \end{pmatrix}
$$

where $A = circ(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $B = rcirc(\alpha_{1+n}, \alpha_{2+n}, \ldots, \alpha_{2t})$ and $\alpha_j \in R$.

Let $Dic_{4t} = \langle x,y \mid x^{2t} = 1, y^2 = x^t, x^y = x^{-1} \rangle$, $t \geq 2$ and $\alpha = \sum_{i=1}^{2t} (\alpha_i x^{i-1} + \alpha_{i+2n} y x^{t-1}) \in Dic_{4t}$. Then

$$
\sigma(\alpha) = \begin{pmatrix} A & B \\ C & A \end{pmatrix}
$$

where $\alpha_j \in R$, $A = circ(\alpha_1, \alpha_2, \ldots, \alpha_{2t})$, $B = rcirc(\alpha_{1+2t}, \alpha_{2+2t}, \ldots, \alpha_{4t})$ and

$C = rcirc(\alpha_{1+3t}, \alpha_{2+3t}, \ldots, \alpha_{4t}, \alpha_{1+2t}, \alpha_{2+2t}, \ldots, \alpha_{3t})$.

Let $SD_{2t} = \langle x,y \mid x^{2t-1} = y^2 = 1, x^y = x^{2t-2}, t \geq 3$ and $\alpha = \sum_{i=1}^{2t-1} (\alpha_i x^{i-1} + \alpha_{i+2t-1} y x^{t-1}) \in SD_{2t}$. Then,

$$
\sigma(\alpha) = \begin{pmatrix} A & B \\ B & A \end{pmatrix}
$$

where $A = circ(\alpha_1, \alpha_2, \ldots, \alpha_{2t-1})$, $B = (2^{t-2} + 1) - circ(\alpha_{1+2t-1}, \alpha_{2+2t-1}, \ldots, \alpha_{2t})$ and $\alpha_j \in R$. 
Corollary 3. Let $R$ be a finite Frobenius ring of characteristic 2.

- If $G$ is the dihedral group of order $k = 2t$ and $v = \sum \alpha_{a^i,b^j}a^ib^j$ where $\alpha_{a^i,b^j} = \alpha_{a^i,b^{j-1}}$, where $\sigma(v)$ is given as in Equation 6, then $C(A)$ is an isodual code and therefore a formally self-dual code of length $n = 2k$.
- If $G$ is the cyclic group of order $k = 4t$, and $v = \sum \alpha_{a^i,b^j}a^ib^j$, where $\alpha_j = \alpha_{2i-j+2}$ for $j = 1, \ldots, 2t$ and $\alpha_{2i+i} = \alpha_{3i+i}$ for $i = 1, \ldots, t-1$, then $C(A)$ is an isodual code and therefore a formally self-dual code of length $n = 2k$.
- If $G$ is the semidihedral group of order $k = 2^t$, and $v = \sum \alpha_{a^i,b^j}a^ib^j$, where $\alpha_j = \alpha_{2i-j+2}$ for $j = 1, \ldots, 2^t$. Then $C(A)$ is an isodual code and therefore a formally self-dual code of length $n = 2k$.

Proof. In each case, the matrix $\sigma(v)$ is symmetric and then invoking Theorem 3.2 we have the result. \qed

4. Computational results

We apply the constructions for self-dual codes over the alphabets $\mathbb{F}_4 + u\mathbb{F}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ in Section 4.1. We obtain self-dual codes of length 32 over $\mathbb{F}_2 + u\mathbb{F}_2$. In Section 4.2, we get new extremal binary self-dual codes of length 68 by considering $\mathbb{F}_2 + u\mathbb{F}_2$-extensions. Moreover, some constructions are used to construct new even formally self-dual codes of parameters $[72, 36, 14]_2$ in Section 4.3.

For codes over $\mathbb{F}_4 + u\mathbb{F}_4$ we use the following Gray map, which is duality preserving and linear.

\[ \varphi_{\mathbb{F}_4 + u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow (\mathbb{F}_2 + u\mathbb{F}_2)^{2n} \]

\[ a\omega + b\overline{\omega} \mapsto (a, b), \quad a, b \in (\mathbb{F}_2 + u\mathbb{F}_2)^n \]

Let $C$ be a self-dual code of length $n$ over $\mathbb{F}_4 + u\mathbb{F}_4$, then $\varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$ is a self-dual code of length $2n$ over $\mathbb{F}_2 + u\mathbb{F}_2$. By the binary image of $C$ we mean $\varphi_1 \circ \varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(C)$, which is a binary self-dual code of length $4n$.

4.1. Self-dual Type I $[64, 32, 12]_2$ codes by the constructions. The possible weight enumerators for a self-dual Type I $[64, 32, 12]_2$-code were characterized in [6]

as:

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

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

Recently, six new codes are constructed in [1]. Together with these 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 $\beta = 0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, \ldots, 25, 28, 19, 30, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120$ and $184$ in $W_{64,2}$.

We obtain self-dual Type I $[64, 32, 12]_2$ codes by applying the constructions emerging from groups of order 8 and 16 to $\mathbb{F}_4 + u\mathbb{F}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$, respectively. We need a brief notation for the elements of $\mathbb{F}_4 + u\mathbb{F}_4$, for this reason we match hexadecimals to binary quadruples as follows:

\[
\begin{align*}
0 & \leftrightarrow 0000, \quad 1 \leftrightarrow 0001, \quad 2 \leftrightarrow 0010, \quad 3 \leftrightarrow 0011, \\
4 & \leftrightarrow 0100, \quad 5 \leftrightarrow 0101, \quad 6 \leftrightarrow 0110, \quad 7 \leftrightarrow 0111, \\
8 & \leftrightarrow 1000, \quad 9 \leftrightarrow 1001, \quad A \leftrightarrow 1010, \quad B \leftrightarrow 1011, \\
C & \leftrightarrow 1100, \quad D \leftrightarrow 1101, \quad E \leftrightarrow 1110, \quad F \leftrightarrow 1111.
\end{align*}
\]
The ordered basis \( \{uw, \omega, u, 1\} \) is used to express the elements of \( F_4 + uF_4 \). For instance, \( 1 + u + u \omega \) corresponds to 1011, which is represented by the hexadecimal \( B \). In order to simplify the notation, the element \( 1 + u \) of \( F_2 + uF_2 \) is denoted by 3 in the upcoming tables. The \( C_{mn} \) construction is used over \( F_4 + uF_4 \) for two cases in Tables 1 and 2.

**Table 1.** \([64, 32, 12]_2\) codes via \( C_{mn} \) with \( m = 4, n = 2 \) over \( F_4 + uF_4 \)

| \( C_{64,i} \) | \( r_{A_1} \) | \( r_{A_2} \) | \( |Aut(C_i)| \) | \( \beta \) in \( W_{64,2} \) |
|-------------|-------------|-------------|----------------|----------------|
| \( C_{64,1} \) | \((B, 4, 6, 2)\) | \((E, 9, 7, 0)\) | \(2^6\) | 0 |
| \( C_{64,2} \) | \((B, 6, 6, 0)\) | \((E, 3, 5, 8)\) | \(2^4\) | 4 |
| \( C_{64,3} \) | \((9, E, E, 0)\) | \((6, 9, 3, A)\) | \(2^2\) | 12 |
| \( C_{64,4} \) | \((B, 4, C, A)\) | \((6, B, D, 0)\) | \(2^2\) | 16 |
| \( C_{64,5} \) | \((3, 6, E, 0)\) | \((E, B, F, A)\) | \(2^2\) | 20 |
| \( C_{64,6} \) | \((1, E, 6, 0)\) | \((C, 9, D, 8)\) | \(2^2\) | 36 |
| \( C_{64,7} \) | \((9, C, E, 2)\) | \((C, 9, D, 8)\) | \(2^2\) | 48 |
| \( C_{64,8} \) | \((3, 6, 4, 8)\) | \((E, B, F, A)\) | \(2^2\) | 52 |

**Table 2.** \([64, 32, 12]_2\) codes via \( C_{mn} \) with \( m = 2, n = 4 \) over \( F_4 + uF_4 \)

| \( C_{64,i} \) | \( r_{A_1} \) | \( r_{A_2} \) | \( r_{A_3} \) | \( r_{A_4} \) | \( |Aut(C_{64,i})| \) | \( \beta \) in \( W_{64,2} \) |
|-------------|-------------|-------------|-------------|-------------|----------------|----------------|
| \( C_{64,9} \) | \((D, 6)\) | \((8, F)\) | \((B, 0)\) | \((4, A)\) | \(2^6\) | 0 |
| \( C_{64,10} \) | \((D, 6)\) | \((8, F)\) | \((B, 0)\) | \((6, 8)\) | \(2^6\) | 4 |
| \( C_{64,11} \) | \((7, 4)\) | \((E, 0)\) | \((8, B)\) | \((1, 6)\) | \(2^6\) | 12 |
| \( C_{64,12} \) | \((4, A)\) | \((0, B)\) | \((C, B)\) | \((6, D)\) | \(2^6\) | 16 |
| \( C_{64,13} \) | \((D, C)\) | \((4, 2)\) | \((8, 9)\) | \((1, C)\) | \(2^6\) | 20 |
| \( C_{64,14} \) | \((D, 4)\) | \((6, 8)\) | \((A, 3)\) | \((3, 4)\) | \(2^6\) | 28 |
| \( C_{64,15} \) | \((F, 4)\) | \((8, 5)\) | \((9, 2)\) | \((C, A)\) | \(2^6\) | 32 |
| \( C_{64,16} \) | \((5, 6)\) | \((C, 2)\) | \((A, 9)\) | \((3, 4)\) | \(2^6\) | 36 |
| \( C_{64,17} \) | \((5, E)\) | \((C, A)\) | \((8, 3)\) | \((3, E)\) | \(2^6\) | 44 |
| \( C_{64,18} \) | \((8, 9)\) | \((D, A)\) | \((C, D)\) | \((D, 3)\) | \(2^6\) | 48 |
| \( C_{64,19} \) | \((D, C)\) | \((E, 0)\) | \((8, 9)\) | \((9, E)\) | \(2^6\) | 52 |

The dihedral group \( D_8 \) is considered over \( F_4 + uF_4 \) and binary self-dual Type I \([64, 32, 12]_2\) codes are constructed. The results are given in Table 3.

Binary self-dual Type I \([64, 32, 12]_2\) codes obtained via \( D_{16} \) construction over \( F_2 + uF_2 \) are listed in Table 4.

4.2. New extremal self-dual binary codes of length 68. In [5] the possible weight enumerators of a self-dual \([68, 34, 12]_2\)-code were characterized as follows:

\[
W_{68,1} = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \cdots, \quad 104 \leq \beta \leq 1358,
\]

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

where \( 0 \leq \gamma \leq 9 \). The existence of codes is known for \( \gamma = 0, 1, 2, 3, 5 \) and 6. First codes for \( \gamma = 3 \) in \( W_{68,2} \) are obtained in [16] and codes exist for \( \gamma = 3 \) in \( W_{68,2} \).
In this section, we obtain 9 new codes with weight enumerators for $\gamma, \beta = 3$ such that $C_{64,4}$, $X = 3, \gamma = 4$, $C_{64,2}$.

| $C_{64,4}$ | $r_A$ | $r_B$ | $|Aut(C_{64,4})|$ | $\beta$ in $W_{64,2}$ |
|-----------|-------|-------|------------------|-------------------|
| $C_{64,20}$ | $(6, D, 7, E)$ | $(2, 2, 4, 5)$ | $2^6$ | 0 |
| $C_{64,21}$ | $(C, 5, F, 4)$ | $(2, 0, C, D)$ | $2^2$ | 4 |
| $C_{64,22}$ | $(0, C, 8, 8)$ | $(9, A, B, D)$ | $2^2$ | 8 |
| $C_{64,23}$ | $(4, B, A, 4)$ | $(E, D, 5, C)$ | $2^2$ | 12 |
| $C_{64,24}$ | $(F, 8, 5, E)$ | $(A, 1, D, 9)$ | $2^2$ | 16 |
| $C_{64,25}$ | $(6, 4, 9, 2)$ | $(7, C, C, F)$ | $2^2$ | 20 |
| $C_{64,26}$ | $(E, 3, B, 1)$ | $(0, 7, 8, 1)$ | $2^2$ | 24 |
| $C_{64,27}$ | $(9, 9, 8, 0)$ | $(6, 6, 1, 2)$ | $2^2$ | 28 |
| $C_{64,28}$ | $(7, 0, A, 8)$ | $(F, 8, 5, C)$ | $2^6$ | 32 |
| $C_{64,29}$ | $(6, 7, 7, 6)$ | $(A, 2, 4, 5)$ | $2^2$ | 36 |
| $C_{64,30}$ | $(0, 6, 8, 2)$ | $(6, 3, 1, 1)$ | $2^2$ | 40 |
| $C_{64,31}$ | $(5, F, E, E)$ | $(4, 1, 0, C)$ | $2^4 \times 3$ | 44 |
| $C_{64,32}$ | $(F, F, 6, 6)$ | $(4, 3, A, 4)$ | $2^2$ | 48 |
| $C_{64,33}$ | $(D, D, 4, 4)$ | $(6, B, 0, 6)$ | $2^2$ | 52 |

| $C_{64,4}$ | $r_A$ | $r_B$ | $|Aut(C_{64,4})|$ | $\beta$ in $W_{64,2}$ |
|-----------|-------|-------|------------------|-------------------|
| $C_{64,34}$ | $(0331u00)$ | $(0003u013)$ | $2^2$ | 0 |
| $C_{64,35}$ | $(3033u110)$ | $(u3010u0u)$ | $2^2$ | 16 |
| $C_{64,36}$ | $(3031u130)$ | $(u01001u1)$ | $2^2$ | 32 |
| $C_{64,37}$ | $(11013u03)$ | $(u003111u)$ | $2^2$ | 48 |
| $C_{64,38}$ | $(3u13u130)$ | $(0u301u0u)$ | $2^2$ | 80 |

When $\gamma = 3$, $\beta = 101, 103, 105, 107, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 137, 141, 145, 147, 149, 153, 159, 193$ or $2m \in \{44, 45, 47, \ldots, 72, 74, 75, 77, \ldots, 84, 86, 87, 88, 89, 90, 91, 92, 94, 95, 97, 98\}$.

In this section, we obtain 9 new codes with weight enumerators for $\gamma = 3$ and $\beta = 135, 139, 143, 146, 151, 152, 155, 161, 186, 202$ and 204. We use the following extension theorem to extend $F_2 + uF_2$ images of self-dual codes over $F_4 + uF_4$, which are listed in tables 1, 2 and 3. It is also applied to self-dual $F_2 + uF_2$-codes that are obtained by the dihedral group of order 16.

**Theorem 4.1.** ([8]) Let $C$ be a self-dual code over $R$ of length $n$ and $G = \langle r_i \rangle$ 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 $R^n$ with $\langle X, X \rangle = 1$. Let $y_i = \langle r_i, X \rangle$ for $1 \leq i \leq k$. Then the following matrix

\[
\begin{pmatrix}
1 & 0 & X \\
y_1 & cy_1 & r_1 \\
\vdots & \vdots & \vdots \\
y_k & cy_k & r_k
\end{pmatrix}
\]
generates a self-dual code $C'$ over $R$ of length $n + 2$.

Table 5. New extremal binary self-dual codes of length 68

| $C_{68, d}$ | $C$ | $c$ | $X$ | $\gamma$ | $\beta$ |
|---|---|---|---|---|---|
| $C_{68, 6}$ | $C_{64, 29}$ | $1 + u$ | $(uu0u33313u1333130u30uu3130113133)$ | 3 | 135 |
| $C_{68, 6}$ | $C_{64, 29}$ | $1 + u$ | $(00u013331u113310u30u111u331313)$ | 3 | 139 |
| $C_{68, 8}$ | $C_{64, 29}$ | $1 + u$ | $(uu0u33333u131133003u0u113u131313)$ | 3 | 143 |
| $C_{68, 8}$ | $C_{64, 29}$ | $1 + u$ | $(uu0011133u311331u1u0u31101131111)$ | 3 | 151 |
| $C_{68, 8}$ | $C_{64, 29}$ | $1 + u$ | $(000u3333103131u30u0331u331133)$ | 3 | 155 |
| $C_{68, 6}$ | $C_{64, 29}$ | $1$ | $(uu0u11131u1311110u30u03110113111)$ | 3 | 161 |
| $C_{68, 6}$ | $C_{64, 38}$ | $1 + u$ | $(33131u1011333u130100030u111u13)$ | 3 | 186 |
| $C_{68, 6}$ | $C_{64, 38}$ | $1$ | $(13131uu0u0u3033u1u30100030u11u0)$ | 3 | 202 |
| $C_{68, 9}$ | $C_{64, 38}$ | $1$ | $(133330u301331u30311003uu0130011)$ | 3 | 204 |

Remark 1. The binary generator matrices of the new codes in Table 5 is available online at [13].

Theorem 4.2. The existence of extremal binary self-dual codes for $\gamma = 3$ in $W_{68, 2}$ is known for 80 parameters.

4.3. Formally self-dual codes. The existence of a Type I self-dual code with parameters [72, 36, 14] or a Type II self-dual code with parameters [72, 36, 16] is unknown. The best known self-dual binary codes of length 72 have minimum distance 12. On the other hand, there are formally self-dual codes with a better minimum distance. Ten even f.s.d. codes of parameters [72, 36, 14] were constructed in [17].

In this section, we construct 25 even f.s.d codes of the same parameters by considering $C_{mn}$; the cyclic group of order $mn$. Theorem 3.3 is applied to $F_2$ and $F_2 + uF_2$ for various values of $m$ and $n$. The results are given in Table 6 and Table 7 respectively for $F_2$ and $F_2 + uF_2$. Partial weight distributions are given where $A_d$ denotes the number of codewords of weight $d$.

Table 6. FSD [72, 36, 14]_{m-1} codes by $C_{mn}$ construction over $F_2 + uF_2$

| $n$ | $m$ | $r_1, \ldots, r_n$ | $A_{14}$ | $A_{16}$ | $A_{18}$ |
|---|---|---|---|---|---|
| 2 | 9 | 13u10u000, 03u100011 | 8820 | 123039 | 1210564 |
| 2 | 9 | 30u0031uu, 10u1u3u3u | 8856 | 122850 | 1210492 |
| 2 | 9 | uu0031u01, 01uu3u013 | 8784 | 123417 | 1207344 |
| 2 | 9 | 3031uu10u, 30033uu30 | 8928 | 122436 | 1210776 |
| 2 | 9 | uu0003103, 300u1303u | 9288 | 120690 | 1206328 |
| 2 | 9 | 1333u1313, 11u3u31uu | 9360 | 119583 | 1216936 |
| 3 | 6 | 11010u, 30u1u0, 105u11 | 8820 | 123927 | 1207092 |
| 3 | 6 | uu30u33, 331330, 030u03 | 9180 | 121194 | 1209304 |
| 3 | 6 | 33u101, 0u0311, 13u1u3 | 9504 | 119151 | 1212760 |
| 3 | 6 | 3uu0u0u, u31uu0, 10uu13 | 9648 | 118170 | 1215172 |
Table 7. FSD $[72,36,14]^b$ codes by $C_{mn}$ over $\mathbb{F}_2$

| n | m | $r_1, \ldots, r_n$ | $A_{14}$ | $A_{16}$ | $A_{18}$ |
|---|---|-------------------|---------|---------|---------|
| 3 | 12 | 00100000010, 11000111010, 000010101010 | 8496    | 124911  | 1209160 |
| 3 | 12 | 01111011111, 010110100010, 101110001000 | 8568    | 124362  | 1211068 |
| 3 | 12 | 11100000101, 101001011100, 111000111110 | 9072    | 121053  | 1210816 |
| 3 | 12 | 10111000011, 001000010111, 010001011011 | 9144    | 121221  | 1211328 |
| 3 | 12 | 001110100000, 000001101100, 111011001000 | 9468    | 119601  | 1209700 |
| 4 | 9  | 001011111, 0010111110, 00110010, 10100011 | 8388    | 125730  | 1206348 |
| 4 | 9  | 01011011, 10011010, 10100111, 001010111 | 8712    | 123741  | 1209160 |
| 4 | 9  | 01111011, 100100100, 010101100, 010111000 | 8820    | 120399  | 1210564 |
| 4 | 9  | 111011010, 101110101, 111000101, 110001001 | 8928    | 122328  | 1212076 |
| 4 | 9  | 000010001, 11100101, 101110110, 110011100 | 8928    | 122769  | 1206784 |
| 4 | 9  | 110001100, 101110111, 001100100, 101101100 | 9036    | 121764  | 1211868 |
| 4 | 9  | 101100101, 101110111, 010011000, 010010110 | 9036    | 121977  | 1208276 |
| 4 | 9  | 0001000, 110100, 010111, 101000, 100000, 010111 | 8388    | 125973  | 1203436 |
| 4 | 9  | 001010, 011001, 110010, 111011, 010100, 110101 | 8784    | 123570  | 1206532 |
| 6 | 6  | 000100, 110100, 010111, 101000, 100000, 010111 | 8820    | 122328  | 1212076 |
| 6 | 6  | 010101, 011001, 110101, 110110, 101000, 001100 | 9360    | 120114  | 1210564 |

5. Conclusion

Finding new construction methods for self-dual and formally self-dual codes opens up new venues of research and possibilities for researchers working on self-dual codes. Group rings have recently been shown to be of interest in finding new construction methods. The strong connection between the group used in the construction method and the automorphism group of the self-dual code thus constructed provides an exciting motivation for the study of these construction methods.

We have used different groups in finding new construction methods and we have shown the effectiveness of these constructions by producing many new self-dual and formally self-dual codes. There are a few possible directions for future research. One is to use different groups to come up with new construction methods. The second possible direction is to apply these construction methods with other rings that have been studied in the literature.

Acknowledgments

We would like to thank the anonymous referees for their helpful comments and suggestions that have improved our paper.

References

[1] D. Anev, M. Harada and N. Yankov, New extremal singly even self-dual codes of lengths 64 and 66, *J. Algebra Comb. Discrete Appl.*, 5 (2018), 143–151.
[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, 24 (1997), 235–265.
[3] A. Bovdi and C. A. Szakács, Unitary Subgroup of the group of units of a modular group algebra of a finite abelian $p$-group, *Math. Zametki*, 45 (1989), 23–29.
[4] V. Bovdi and A. L. Rosa, On the order of the unitary subgroup of a modular group algebra, *Comm. Algebra*, 28 (2000), 1897–1905.
[5] S. Buyuklieva and I. Boukliev, Extremal self-dual codes with an automorphism of order 2, *IEEE Trans. Inform. Theory*, 44 (1998), 323–328.
[6] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimum distance of self-dual codes, *IEEE Trans. Inform. Theory*, 36 (1990), 1319–1333.
[7] P. J. Davis, Circulant Matrices, A Wiley-Interscience Publication. Pure and Applied Mathematics. John Wiley & Sons, New York-Chichester-Brisbane, 1979.

[8] S. T. Dougherty, J.-L. Kim, H. Kulosman and H. W. Liu, Self-dual codes over commutative Frobenius rings, Finite Fields Appl., 16 (2010), 14–26.

[9] S. T. Dougherty, J. Gildea, R. Taylor and A. Tylyshchak, Group rings, G-codes and constructions of self-dual and formally self-dual codes, Des. Codes Crypt., 86 (2018), 2115–2138.

[10] S. T. Dougherty, B. Yildiz and S. Karadeniz, Codes over $\mathbb{R}_k$, Gray maps and their Binary Images, Finite Fields Appl., 17 (2011), 205–219.

[11] S. T. Dougherty, S. Karadeniz and B. Yildiz, Cyclic codes over $\mathbb{R}_k$, Des. Codes Crypt., 63 (2012), 113–126.

[12] S. Dougherty, B. Yildiz and S. Karadeniz, Self-dual codes over $\mathbb{R}_k$ and binary self-dual codes, Eur. J. Pure and Applied Math., 6 (2013), 89–106.

[13] Binary Generator Matrices of New Extremal Binary Self-Dual Codes of Length 68, Available from: http://www.abidinkaya.wix.com/math/research4.

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

[15] T. Hurley, Group rings and rings of matrices, Int. J. Pure Appl. Math., 31 (2006), 319–335.

[16] A. Kaya and B. Yildiz, Various constructions for self-dual codes over rings and new binary self-dual codes, Discrete Math., 339 (2016), 460–469.

[17] A. Kaya and B. Yildiz, Constructing formally self-dual codes from block $\lambda$-circulant matrices, Math. Commun., 24 (2019), 91–105.

[18] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math., 121 (1999), 555–575.

Received January 2018; revised February 2019.

E-mail address: Prof.Steven.Dougherty@gmail.com
E-mail address: J.Gildea@chester.ac.uk
E-mail address: abidin.kaya@sampoernauiversity.ac.id
E-mail address: bahattin.yildiz@nau.edu