Bull. Korean Math. Soc. **60** (2023), No. 3, pp. 829–844
https://doi.org/10.4134/BKMS.b220378
pISSN: 1015-8634 / eISSN: 2234-3016

AN ALTERED GROUP RING CONSTRUCTION OF THE [24, 12, 8] AND [48, 24, 12] TYPE II LINEAR BLOCK CODE

Shefali Gupta and Dinesh Udar

Abstract. In this paper, we present a new construction for self-dual codes that uses the concept of double bordered construction, group rings, and reverse circulant matrices. Using groups of orders $2, 3, 4$, and 5, and by applying the construction over the binary field and the ring $F_2 + uF_2$, we obtain extremal binary self-dual codes of various lengths: $12, 16, 20, 24, 32, 40$, and 48. In particular, we show the significance of this new construction by constructing the unique Extended Binary Golay Code $[24, 12, 8]$ and the unique Extended Quadratic Residue $[48, 24, 12]$ Type II linear block code. Moreover, we strengthen the existing relationship between units and non-units with the self-dual codes presented in [10] by limiting the conditions given in the corollary. Additionally, we establish a relationship between idempotent and self-dual codes, which is done for the first time in the literature.

1. Introduction

Many researchers are interested in constructing extremal binary self-dual codes over Frobenius rings since these codes are linked to other mathematical structures and have numerous applications. There is a substantial body of literature devoted to the construction of the extended binary Golay code and the extended quadratic residue code.

Type II codes are self-dual codes that are doubly-even [8, p. 339]. Each nonzero codeword in a doubly-even code has a weight that is a multiple of four. There is only one Type II code with a 48 length, a 24 dimension, and a 12 minimum distance up to equivalency, this was validated in 2003 by Houghten [7]. Type II codes are known as extremal self-dual codes as they attain the greatest distance for their length. Extremal Type II codes have got the most attention in the literature because of their strong relation to sphere packings. These codes fulfill the formula $[n, \frac{n}{2}, 4\lfloor\frac{n}{24}\rfloor + 4]$, $n = 8m$ (where m is a natural number) for [length, dimension, and distance] [8, p. 346]. The first putative code in the Type II series of codes when n equals twenty-four is the extended binary

Received June 2, 2022; Revised August 12, 2022; Accepted September 5, 2022.
2020 *Mathematics Subject Classification.* Primary 94B05, 16S34.
Key words and phrases. Extremal binary self-dual codes, group rings, reverse circulant matrices, bordered constructions.

Golay code. The second putative code in this series is the extended quadratic residue code. In this paper, using a new construction, we have constructed both codes.

Extremal self-dual codes of Type II with lengths divisible by 24 are of great relevance because the codewords of weight w form a 5-design for every non-zero weight w [1]. From these codes, the Extended Golay code is the $[24, 12, 8]$ code, while the Extended Quadratic Residue Code, or Extended QR, is the $[48, 24, 12]$ code.

In 1990, the code $[24, 12, 8]$ was constructed using ideals in the group algebra F_2S_4; see [2] for details. In 2008, the $[24, 12, 8]$ code was constructed from F_2D_{24}; see [13] for details. The most common approach to constructing extended binary Golay and extended quadratic residue codes is to extend the binary Golay code of length 23 by an even parity bit and the quadratic residue code of length 47 by an even parity bit. In this paper, we have defined a new way of constructing the extended binary Golay code and the extended quadratic residue code. We construct the code here by blending the concept of double bordered constructions of self-dual codes from group rings over Frobenius rings [11] with constructing self-dual codes from group rings and reverse circulant matrices [10].

The following is an outline of the work in this paper: In Section 2, we discuss the preliminaries, which are necessary for comprehending the findings of this research. In Section 3, we present the new constructions and the theoretical results. Section 4 presents numerical results for the extended binary Golay code, extended quadratic residue code, and extremal binary self-dual codes of varying lengths obtained by directly applying our construction over a field F_2 and ring $F_2 + uF_2$ with SAGE [16]. The paper wraps up with the conclusion of our work and recommendations for future research.

2. Preliminaries

Throughout the paper, we will assume all rings are finite, commutative, and Frobenius rings with a multiplicative identity.

2.1. Group rings and ring of matrices

We will use group rings in our construction, so essential group ring descriptions are discussed. In group rings, the cardinality of ring and group can be infinite, but in our construction of codes, we will consider both the ring and the group of finite cardinality. Let G be a group of order n. Then the elements of the group rings are of the form $\sum_{i=1}^{n} \alpha_i g_i$, $\alpha_i \in R$, $g_i \in G$.

The addition of the two elements of the group rings is defined coordinate wise, i.e.,

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

The product of the two elements of the group rings is defined by

$$(\sum_{i=1}^{n}\alpha_i g_i)(\sum_{j=1}^{n}\beta_i g_i) = \sum_{i,j}\alpha_i\beta_j g_i g_j.$$

T. Hurley was the first to introduce the relationship between group rings and ring of matrices in [9]. Let R be a finite commutative Frobenius ring of characteristic 2. Let $G = \{g_1, g_2, \dots, g_n\}$ denote a finite group of order n, and $\vartheta = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n$ be an element of the group ring RG. Then the matrix representation $\sigma(\vartheta)$ of ϑ is given by

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

Let σ denote a bijective ring homomorphism between group rings RG and rings of matrix $M(RG, \vartheta)$. We will now represent $\sigma(\vartheta)$ of an element $\vartheta \in RG$, where $G = C_n$. Let $G = C_n = \{z \mid z^n = 1\}$, and $\vartheta = \alpha_0 + \alpha_1 z + \alpha_2 z^2 + \cdots + \alpha_{n-1}z^{n-1} \in RC_n$. Then $\sigma(\vartheta) = circ\begin{bmatrix}\alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1}\end{bmatrix}$.

For more details on the group ring, see [14].

2.2. Self-dual codes

To begin, we'll go over the basic definitions of coding theory. We say the code is linear if it is a submodule of R^n. The codewords of the code C are the elements of C. The Euclidean inner product between two elements, says $\mathbf{l} = \{l_1, l_2, \dots, l_n\}$ and $\mathbf{m} = \{m_1, m_2, \dots, m_n\}$ of R^n, is given by $\langle \mathbf{l}, \mathbf{m}\rangle_E = \sum l_i m_i$. The dual $C^\perp$ of code C is defined as

$$C^\perp = \{\mathbf{l} \in R^n \mid \langle \mathbf{l}, \mathbf{m}\rangle_E = 0 \ \forall \mathbf{m} \in C\}.$$

If $C \subseteq C^\perp$, then the code C is said to be self orthogonal, and if $C = C^\perp$, then the code C is said to be self-dual. Throughout the paper, two types of binary self-dual codes are built: one of Type I and another of Type II. The binary self-dual code C is said to be of Type I if the weight of all its codewords is divisible by two, and of Type II if the weight of all its codewords is divisible by four.

Theorem 2.1 ([15])**.** *Let $d_I(n)$ and $d_{II}(n)$ represent the minimum distance of Type I and Type II codes of length n, respectively. Then,*

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

and

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

Self-dual codes that attain these bounds are known as extremal self-dual codes. For a full description of self-dual codes over the Frobenius ring, see [3,4].

2.3. Ring $\boldsymbol{F_2 + uF_2}$

The commutative Frobenius ring with characteristic 2 is denoted by R_k. For $k \geq 1$, the ring R_k is defined as

$$F_2[u_1, u_2, \dots, u_k]/\langle u_1^2, u_2^2, \dots, u_k^2\rangle$$

such that $u_i u_j = u_j u_i,\ 1 \leq i \neq j \leq k$. The ring R_k can be recursively expressed as

$$R_k = R_{k-1} + u_k R_{k-1}.$$

In this paper, we will do all the repetitions for generating self-dual codes over the ring $F_2 + uF_2$. The ring $F_2 + uF_2$ or R_1 is defined as a commutative Frobenius ring of characterestic 2 with the 4 elements $0, 1, u, 1+u$ and the condition that $u^2 = 0$. The ring $F_2 + uF_2$ is isomorphic to $F_2[X]/\langle X^2\rangle$ and is represented as

$$F_2 + uF_2 = \{a + bu \,|\, a, b \in F_2, u^2 = 0\}.$$

The Lee weights of the elements $0, 1, u, 1+u$ of the ring $F_2 + uF_2$ are $0, 1, 2, 1$, respectively.

The Gray map ϕ is a map defined from $(F_2 + uF_2)^n$ to F_2^{2n} in such a way that $\phi(a + bu) = (b, a + b)$, where $a, b \in F_2$. This is a distance-preserving mapping, which means that the Lee distance d_L of a code $C(n, 2^k, d_L)$ over $(F_2 + uF_2)^n$ equals the Hamming distance d_H of a code $\phi(C)(2n, k, d_H)$.

Theorem 2.2. *The Gray image of a linear self-dual code C of length n over $F_2 + uF_2$ is a binary linear self-dual code $\phi(C)$ of length $2n$.*

The natural projection Ω from $F_2 + uF_2$ to F_2 is defined as follows:

$$\Omega : F_2 + F_2 \to F_2, \quad \Omega(a + bu) = a.$$

Let C be a linear code over $F_2 + uF_2$ and $B = \Omega(C)$. Then B is a projection of C into F_2 and C is a lift of B into $F_2 + uF_2$. The projection of a self-orthogonal code is always a self-orthogonal, but the projection of a self-dual code need not be self-dual. For more details on R_k, see [5].

3. Main matrix construction

Here we present our main construction. As mentioned before, we define a double border around the matrix given in [10]. The motivation is to produce extremal binary self-dual codes of various lengths, and the most important codes are the extended Golay code, i.e., $[24, 12, 8]$ and the Extended Quadratic Residue Code, which we shall call Extended QR, the only known $[48, 24, 12]$ code, via our construction, that could not be obtained in [10] and [11]. Let

$\vartheta_1, \vartheta_2 \in RG$, where R is a Frobenius ring of characteristic 2, and G is a group of order n. The matrix is defined as follows:

$$M(\sigma) = \left[\begin{array}{cc|ccc|ccc|cc|ccc|ccc}
\beta_1 & \beta_2 & \beta_3 & \cdots & \beta_3 & \beta_4 & \cdots & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \cdots & \beta_7 & \beta_8 & \cdots & \beta_8 \\
\beta_2 & \beta_1 & \beta_4 & \cdots & \beta_4 & \beta_3 & \cdots & \beta_3 & \beta_6 & \beta_5 & \beta_8 & \cdots & \beta_8 & \beta_7 & \cdots & \beta_7 \\ \hline
\beta_3 & \beta_4 & & & & & & & \beta_7 & \beta_8 & & & & & & \\
\vdots & \vdots & & I_n & & & 0 & & \vdots & \vdots & & \sigma(\vartheta_1) & & & \sigma(\vartheta_2)+C & \\
\beta_3 & \beta_4 & & & & & & & \beta_7 & \beta_8 & & & & & & \\ \hline
\beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & & \\
\vdots & \vdots & & 0 & & & I_n & & \vdots & \vdots & & \sigma(\vartheta_2)^T+C & & & \sigma(\vartheta_1)^T & \\
\beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & &
\end{array}\right]. \tag{3.1}$$

Let $C(\sigma)$ be a code generated through the matrix $M(\sigma)$. Then, code $C(\sigma)$ has length $4n+4$.

Lemma 3.1. *Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group of order n and R be a finite commutative Frobenius ring, so that*

$$N(\sigma) = \begin{pmatrix} \sigma(\vartheta_1) & \sigma(\vartheta_2)+C \\ \sigma(\vartheta_2)^T + C & \sigma(\vartheta_1)^T \end{pmatrix},$$

where ϑ_1 and ϑ_2 are the elements of RG, $\sigma(\vartheta_1)$ and $\sigma(\vartheta_2)$ are group-ring matrices of $n \times n$ order and C is a reverse circulant matrix of $n \times n$ order over R. Then,

$$\sigma(\vartheta_k)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \sigma(\vartheta_k)^T\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}\mu_k\\ \vdots \\ \mu_k\end{pmatrix} (k=1,2),$$

where $\mu_1 = \sum_{g\in G}\alpha_g$, $\mu_2 = \sum_{g\in G}\beta_g$.

Let η denote the sum of all elements of the first row of matrix C. Then,

$$(\sigma(\vartheta_2)+C)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = (\sigma(\vartheta_2)^T + C)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}\mu_2+\eta\\ \vdots \\ \mu_2+\eta\end{pmatrix}.$$

Proof. Clearly, $\sigma(\vartheta_1) = (\alpha_{g_i^{-1}g_j})_{i,j=1,\ldots,n}$, $\sigma(\vartheta_2) = (\beta_{g_i^{-1}g_j})_{i,j=1,\ldots,n}$, and $C = (\gamma_{ij})_{i,j=1,\ldots,n}$.

Now, the i-th element of column $\sigma(\vartheta_1)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n}\alpha_{g_i^{-1}g_j} = \sum_{g\in G}\alpha_{g_i^{-1}g} = \sum_{g\in G}\alpha_g = \mu_1,\ g_i \in G,\ g_i^{-1} \in G,$$

and the i-th element of column $\sigma(\vartheta_1)^T\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n}\alpha_{g_j^{-1}g_i} = \sum_{g\in G}\alpha_{g^{-1}g_i} = \sum_{g\in G}\alpha_{gg_i} = \sum_{g\in G}\alpha_g = \mu_1,\ g_i \in G.$$

Thus,

$$\sigma(\vartheta_1)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \sigma(\vartheta_1)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_1\\ \vdots\\ \mu_1\end{pmatrix}.$$

Similarly, the i-th element of column $\sigma(\vartheta_2)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n}\beta_{g_i^{-1}g_j} = \sum_{g\in G}\beta_{g_i^{-1}g} = \sum_{g\in G}\beta_g = \mu_2,\ g_i\in G,\ g_i^{-1}\in G,$$

and the i-th element of column $\sigma(\vartheta_2)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n}\beta_{g_j^{-1}g_i} = \sum_{g\in G}\beta_{g^{-1}g_i} = \sum_{g\in G}\beta_{gg_i} = \sum_{g\in G}\beta_g = \mu_2,\ g_i\in G.$$

Thus,

$$\sigma(\vartheta_2)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \sigma(\vartheta_2)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_2\\ \vdots\\ \mu_2\end{pmatrix}.$$

Furthermore, the i-th element of column $C\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n}\gamma_{ij} = \gamma_{i1}+\gamma_{i2}+\cdots+\gamma_{in} = \eta.$$

Thus,

$$C\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\eta\\ \vdots\\ \eta\end{pmatrix}.$$

Hence,

$$(\sigma(\vartheta_2)+C)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = (\sigma(\vartheta_2)^T+C)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_2+\eta\\ \vdots\\ \mu_2+\eta\end{pmatrix}.$$

□

In 2020, [10, Theorem 2.5], Gildea, Kaya, and Yildiz introduced a matrix and had shown that, under certain conditions, we can generate self-dual codes of order $4n$ by a group of order n. In Theorem 3.2, we extend this result by introducing double border around their matrix and demonstrating that, under certain conditions, we can generate self-dual codes of order $4n+4$ by a group of order n. The concept of double bordered was introduced by Gildea in [11].

Their main matrix construction does not involve the concept of reverse circulant matrix. In our main matrix construction we have used reverse circulant matrix. Moreover, their main theorem, i.e., [11, Theorem 3.2], was restricted for the group of order $2p$ (p is odd prime) only but, by Theorem 3.2, we have extended it to any group of order n ($n \in \mathbb{N}$). As a result we are able to construct those extremal self-dual codes which can not be attained by the technique used in [11], i.e., extremal self-dual codes of length 12, 20, 40 are constructed as shown in Table 1, Table 5 and Table 6, respectively. By blending both the concepts of [10] and in [11] Theorem 3.2, we are able to construct those extremal self-dual codes which have not been obtained in [10] and [11]. In particular, we are able to construct the well-known Extended Binary Golay Code, as shown in (Table 7, Code E_2), the Extended QR code, as shown in (Table 8, Code L_2), and various other extremal self-dual codes which are listed in Section 4.

Theorem 3.2. *Let R be a finite commutative Frobenius ring with characteristic 2, G be a finite group of order n, and C_σ be a code generated by the matrix M_σ such that $|C(\sigma)| = |R|^{\frac{n}{2}}$. Then $C(\sigma)$ is a self-dual code of length $4n+4$ if the following conditions are satisfied*

Case I: *n is odd*

(1) $\sum_{i=0}^{8} \beta_i = 0$,

(2) $\sigma(\vartheta_1\vartheta_2 + \vartheta_2\vartheta_1) + \sigma(\vartheta_1)C + C\sigma(\vartheta_1) = 0$,

(3) $$\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) + \sigma(\vartheta_2)C + C\sigma(\vartheta_2)^T + C^2 = I_n + (\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2)\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n},$$

(4) $\sigma(\vartheta_1^*\vartheta_2^* + \vartheta_2^*\vartheta_1^*) + C\sigma(\vartheta_1)^T + \sigma(\vartheta_1)^T C = 0$,

(5) $$\sigma(\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2) + \sigma(\vartheta_2)^T C + C\sigma(\vartheta_2) + C^2 = I_n + (\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2)\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n},$$

(6) $\beta_3(\beta_1+1) + \beta_4\beta_2 + \beta_7(\beta_5+\mu_1) + \beta_6\beta_8 + (\mu_2+\eta)\beta_8 = 0$, *and*

(7) $\beta_4(\beta_1+1) + \beta_3\beta_2 + \beta_8(\beta_5+\mu_1) + \beta_6\beta_7 + (\mu_2+\eta)\beta_7 = 0$.

Case II: *n is even*

(1) $\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2 = 0$,

(2) *Conditions* 2 *to* 9 *for this case is same as for the case 'n is odd'.*

Proof. Let

$$M(\sigma) = \begin{bmatrix} M_1 & M_2 & M_3 & M_4 \\ M_2^T & I_{2n} & M_4^T & N(\sigma) \end{bmatrix},$$

where $M_1 = circ(\beta_1, \beta_2)$, $M_2 = CIRC(A_1, A_2)$, $M_3 = circ(\beta_5, \beta_6)$, $M_4 = CIRC(A_3, A_4)$, $A_1 = (\beta_3, \ldots, \beta_3) \in R^n$, $A_2 = (\beta_4, \ldots, \beta_4) \in R^n$, $A_3 = (\beta_7, \ldots, \beta_7) \in R^n$, $A_4 = (\beta_8, \ldots, \beta_8) \in R^n$, and $N(\sigma) = \begin{bmatrix} \sigma(\vartheta_1) & \sigma(\vartheta_2)+C \\ \sigma(\vartheta_2)^T+C & \sigma(\vartheta_1)^T \end{bmatrix}$.

Then

$$M(\sigma)M(\sigma)^T$$
$$= \begin{bmatrix} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T & M_1M_2 + M_2 + M_3M_4 + M_4N(\sigma)^T \\ M_2^TM_1^T + M_2^T + M_4^TM_3^T + N(\sigma)M_4^T & M_2^TM_2 + I_{2n} + M_4^TM_4 + N(\sigma)N(\sigma)^T \end{bmatrix}.$$

Now,

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + n\beta_{i+2}^2 + \beta_{i+4}^2 + n\beta_{i+6}^2), 0).$$

Case I: n is odd

$$\begin{aligned} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T &= circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+2}^2 + \beta_{i+4}^2 + \beta_{i+6}^2), 0) \\ &= circ(\sum_{i=1}^{8}\beta_i^2, 0). \end{aligned}$$

Case II: n is even

$$\begin{aligned} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T &= circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+4}^2), 0) \\ &= circ(\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2, 0) \end{aligned}$$

and

$$\begin{aligned} & M_2^TM_2 + I_{2n} + M_4^TM_4 + N(\sigma)N(\sigma)^T \\ = & \sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2 CIRC(\mathbf{A}, \mathbf{0}) + I_{2n} + N(\sigma)N(\sigma)^T, \end{aligned}$$

where $\mathbf{A} = circ(\underbrace{1, \ldots, 1}_{n\text{-times}})$, $\mathbf{0} = circ(\underbrace{0, \ldots, 0}_{n\text{-times}})$ and

$$N(\sigma)N(\sigma)^T$$
$$= \begin{bmatrix} \sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) + \sigma(\vartheta_2)C + C\sigma(\vartheta_2)^T + C^2 & \sigma(\vartheta_1\vartheta_2) + \sigma(\vartheta_1)C + \sigma(\vartheta_2\vartheta_1) + C\sigma(\vartheta_1) \\ \sigma(\vartheta_1^*\vartheta_2^*) + C\sigma(\vartheta_1)^T + \sigma(\vartheta_2^*\vartheta_1^*) + \sigma(\vartheta_1)^TC & \sigma(\vartheta_2^*\vartheta_2) + \sigma(\vartheta_2)^TC + C\sigma(\vartheta_2) + C^2 + \sigma(\vartheta_1^*\vartheta_1) \end{bmatrix}.$$

It follows from Lemma 3.1 that

$$N(\sigma)M_4^T = \begin{bmatrix} \mu_1\beta_7 + \mu_2\beta_8 + \eta\beta_8 & \mu_1\beta_8 + \mu_2\beta_7 + \eta\beta_7 \\ \vdots & \vdots \\ \mu_1\beta_7 + \mu_2\beta_8 + \eta\beta_8 & \mu_1\beta_8 + \mu_2\beta_7 + \eta\beta_7 \\ \mu_2\beta_7 + \eta\beta_7 + \mu_1\beta_8 & \mu_2\beta_8 + \eta\beta_8 + \mu_1\beta_7 \\ \vdots & \vdots \\ \mu_2\beta_7 + \eta\beta_7 + \mu_1\beta_8 & \mu_2\beta_8 + \eta\beta_8 + \mu_1\beta_7 \end{bmatrix}.$$

Additionally,

$$M_2^TM_1^T + M_2^T + M_4^TM_3^T + N(\sigma)M_4^T$$

$$= \begin{bmatrix} \beta_3\beta_1+\beta_4\beta_2+\beta_3+\beta_7\beta_5+\beta_6\beta_8+\mu_1\beta_7+\mu_2\beta_8+\eta\beta_8 & \beta_4\beta_1+\beta_3\beta_2+\beta_4+\beta_8\beta_5+\beta_6\beta_7+\mu_1\beta_8+\mu_2\beta_7+\eta\beta_7 \\ \vdots & \vdots \\ \beta_3\beta_1+\beta_4\beta_2+\beta_3+\beta_7\beta_5+\beta_6\beta_8+\mu_1\beta_7+\mu_2\beta_8+\eta\beta_8 & \beta_4\beta_1+\beta_3\beta_2+\beta_4+\beta_8\beta_5+\beta_6\beta_7+\mu_1\beta_8+\mu_2\beta_7+\eta\beta_7 \\ \beta_4\beta_1+\beta_3\beta_2+\beta_4+\beta_8\beta_5+\beta_6\beta_7+\mu_2\beta_7+\eta\beta_7+\mu_1\beta_8 & \beta_4\beta_2+\beta_3\beta_1+\beta_3+\beta_5\beta_7+\beta_6\beta_8+\mu_2\beta_8+\eta\beta_8+\mu_1\beta_7 \\ \vdots & \vdots \\ \beta_4\beta_1+\beta_3\beta_2+\beta_4+\beta_8\beta_5+\beta_6\beta_7+\mu_2\beta_7+\eta\beta_7+\mu_1\beta_8 & \beta_4\beta_2+\beta_3\beta_1+\beta_3+\beta_5\beta_7+\beta_6\beta_8+\mu_2\beta_8+\eta\beta_8+\mu_1\beta_7 \end{bmatrix}.$$

Clearly, $M(\sigma)M(\sigma)^T$ is a symmetric matrix and C_σ is self orthogonal if for $\sum_{i=0}^{8}\beta_i = 0$,

$$\begin{aligned} &\sigma(\vartheta_1\vartheta_2+\vartheta_2\vartheta_1)+\sigma(\vartheta_1)C+C\sigma(\vartheta_1)=0,\\ &\sigma(\vartheta_1\vartheta_1^*+\vartheta_2\vartheta_2^*)+\sigma(\vartheta_2)C+C\sigma(\vartheta_2)^T+C^2\\ &=I_n+(\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2)\begin{bmatrix} 1 & \cdots & 1\\ \vdots & \ddots & \vdots\\ 1 & \cdots & 1\end{bmatrix}_{n\times n},\\ &\sigma(\vartheta_1^*\vartheta_2^*+\vartheta_2^*\vartheta_1^*)+C\sigma(\vartheta_1)^T+\sigma(\vartheta_1)^TC=0,\\ &\sigma(\vartheta_1^*\vartheta_1+\vartheta_2^*\vartheta_2)+\sigma(\vartheta_2)^TC+C\sigma(\vartheta_2)+C^2\\ &=I_n+(\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2)\begin{bmatrix} 1 & \cdots & 1\\ \vdots & \ddots & \vdots\\ 1 & \cdots & 1\end{bmatrix}_{n\times n},\\ &\beta_3(\beta_1+1)+\beta_4\beta_2+\beta_7(\beta_5+\mu_1)+\beta_6\beta_8+(\mu_2+\eta)\beta_8=0,\\ &\beta_4(\beta_1+1)+\beta_3\beta_2+\beta_8(\beta_5+\mu_1)+\beta_6\beta_7+(\mu_2+\eta)\beta_7=0. \end{aligned}$$

Because $|C(\sigma)| = |R|^{\frac{n}{2}}$ and $C(\sigma)$ is self-orthogonal under the conditions established above, we can conclude that the code $C(\sigma)$ is a self-dual code if all of the preceding conditions are met. □

In 2020, [10, Corollary 3.2, Corollary 3.3 and Corollary 3.4], Gildea, Kaya, and Korban under certain conditions defined a relationship of units, non-units, and unitary units with self-dual codes, respectively. In Corollaries 3.3, 3.4, 3.5 and 3.6 we have relaxed both the restrictions, i.e., C commutes with $\sigma(\vartheta_1)$ and ϑ_1 commutes with ϑ_2. In addition, we have replaced the condition that both $C\sigma(\vartheta_2)^T$ and $C\sigma(\vartheta_2)$ must be symmetric with the simple condition that $\sigma(\vartheta_2)$ is symmetric, which strenghtens the relationship between units, non-units and unitary units with the self-dual codes.

Corollary 3.3. *Let $C(\sigma)$ be a self-dual code, G be a finite group of order n, and R be a finite commutative Frobenius ring of characteristic 2. Then the elements $\vartheta_1\vartheta_1^*+\vartheta_2\vartheta_2^*$, $\vartheta_1^*\vartheta_1+\vartheta_2^*\vartheta_2 \in RG$ are units if the following conditions are satisfied:*

(1) $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2=0$,
(2) $\sigma(\vartheta_2)$ *is symmetric, and*
(3) $C^2=0$.

Proof. If $\sigma(\vartheta_2)$ is symmetric, then $\sigma(\vartheta_2)C + C\sigma(\vartheta_2)^T = 0$. If $C^2 = 0$, and $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0$, then $\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) = \sigma(\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2) = I_n$. Then, $\det(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) = \det(\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2) = 1$. Hence, $\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*$ and $\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2$ are unitary units. □

Corollary 3.4. *Let $C(\sigma)$ be a self-dual code, G be a finite group of order n (odd), and R be a finite commutative Frobenius ring of characteristic 2. Then the elements $\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*$, $\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2 \in RG$ are non units if the following conditions are satisfied:*

(1) $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1$,
(2) $\sigma(\vartheta_2)$*is symmetric, and*
(3) $C^2 = 0$.

Proof. If $\sigma(\vartheta_2)$ is symmetric, then $\sigma(\vartheta_2)C + C\sigma(\vartheta_2)^T = 0$. If $C^2 = 0$, and $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1$, then

$$\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) = I_n + \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}_{n\times n} = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}_{n\times n}.$$

Then,

$$\begin{aligned} \det(\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*)) &= \det \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}_{n\times n} \\ &= (n-1)\det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n\times n} \\ &= 0 \text{ (if } n \text{ is odd).} \end{aligned}$$

Hence, $\det(\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*)) = 0$ and $\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*$ is a non-unit by Corollary 3 of [9]. Similarly, $\det(\sigma(\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2)) = 0$ and $\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2$ is a non-unit. □

Corollary 3.5. *Let $C(\sigma)$ be a self-dual code, G be a finite group of order n (odd), and R be a finite commutative Frobenius ring of characteristic 2. Then the elements $\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*$, $\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2 \in RG$ are non units if the following conditions are satisfied:*

(1) $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0$,
(2) $\sigma(\vartheta_2)$ *is symmetric, and*
(3) $C^2 = I$.

Proof. If $\sigma(\vartheta_2)$ is symmetric, then $\sigma(\vartheta_2)C + C\sigma(\vartheta_2)^T = 0$. If $C^2 = I$, and $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0$, then $\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) = \sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) = 0$ Hence, $\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*$ and $\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2$ are non-units. □

Corollary 3.6. *Let $C(\sigma)$ be a self-dual code, G be a finite group of order n (odd), and R be a finite commutative Frobenius ring of characteristic 2. Then the element $\vartheta_2 \in RG$ is unitary unit if following conditions are satisfied:*

(1) *$\sigma(\vartheta_2)$ is symmetric,*
(2) $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0$,
(3) $C^2 = I$, *and*
(4) *ϑ_1 is unitary in RG.*

Proof. If $\sigma(\vartheta_2)$ is symmetric, then $\sigma(\vartheta_2)C + C\sigma(\vartheta_2)^T = 0$. If $C^2 = I$, $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0$, and ϑ_1 is unitary in RG, then $\sigma(1 + \vartheta_2\vartheta_2^*) = \sigma(1 + \vartheta_2^*\vartheta_2) = 0$ Thus, $\vartheta_2\vartheta_2^* = \vartheta_2^*\vartheta_2 = 1$, and ϑ_2 is unitary unit. □

By Corollary 3.7, we have established a relationship between idempotents and self-dual codes, which have been established for the first time in the literature.

Corollary 3.7. *Let $C(\sigma)$ be a self-dual code, G be a finite group of order n (odd), and R be a finite commutative Frobenius ring of characteristic 2. Then the elements $\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*$, $\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2 \in RG$ are idempotents if following conditions are satisfied:*

(1) $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1$,
(2) *$\sigma(\vartheta_2)$ is symmetric, and*
(3) $C^2 = 0$.

Proof. If $\sigma(\vartheta_2)$ is symmetric, then $\sigma(\vartheta_2)C + C\sigma(\vartheta_2)^T = 0$.

If n is odd, then

$$\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}^2 = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}.$$

That is, $\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$ is an idempotent matrix.

If $C^2 = 0$, and $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1$, then

$$\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*) = I_n + \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n} = I_n - \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}.$$

If E is an idempotent matrix, then $I - E$ is also an idempotent matrix. Thus, $\sigma(\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*)$ is an idempotent matrix and $\vartheta_1\vartheta_1^* + \vartheta_2\vartheta_2^*$ is an idempotent element of RG. Similarly, we can say that $\vartheta_1^*\vartheta_1 + \vartheta_2^*\vartheta_2$ is an idempotent element of RG. □

4. Computational results

In this section, we apply our main construction over the field F_2 and the ring F_2+uF_2 to search for extremal binary self-dual codes of lengths of $12, 16, 20, 24, 32, 40, 48$. We consider groups of orders $2, 3, 4$ and 5, in particular C_2, C_3, C_4 and C_5. We also employ the Gray map to construct the famous Extended QR code. For all our computational calculation, we have used the SAGE software [16].

Algorithm:
INPUT: Field F_2.
OUTPUT: Extemal Self-dual Codes.

1. Generate matrices $\sigma(\vartheta)$ of order $n \times n$ by a group of order n, over the field F_2. The structure of the matrix $\sigma(\vartheta)$ is described in Section 2.1.
2. Generate reverse circulant matrices C of order $n \times n$ over the field F_2.
3. Generate boundary matrices M_1, M_2, M_3 and M_4 over the Field F_2, where $M_1 = circ(\beta_1, \beta_2)$, $M_2 = CIRC(A_1, A_2)$, $M_3 = circ(\beta_5, \beta_6)$, $M_4 = CIRC(A_3, A_4)$, $A_1 = (\beta_3, \dots, \beta_3) \in R^n$, $A_2 = (\beta_4, \dots, \beta_4) \in R^n$, $A_3 = (\beta_7, \dots, \beta_7) \in R^n$, $A_4 = (\beta_8, \dots, \beta_8) \in R^n$.
4. Construct the set of generator matrices $M(\sigma)$ of order $(2n+2)\times(4n+4)$ having the structure mentioned in Equation (3.1) using all the possible combinations of matrices obtained in Step 1, Step 2 and Step 3.
5. From the given set of generator matrices, collect matrices that satisfy the condition $M(\sigma)M(\sigma)^T = 0$ and have rank $2n+2$. These matrices generate self-dual codes $C(\sigma)$ with parameters $(4n+4, 2n+2, d_{\min})$, where $d_{\min}$ is the minimum distance of the code.
6. Evaluate $d_{\min} = \min\{d(a,b) \mid a \neq b\}$ for the self-dual codes that are generated from matrices collected in Step 5. Here, $d(a,b) = |\{i \mid 1 \leq i \leq 4n+4, a_i \neq b_i\}|$, where $a, b \in F_2^{4n+4}$ are the codewords of length $4n+4$ for the code $C(\sigma)$.
7. Shortlist matrices from Step 5, whose $d_{\min}$ of its corresponding self-dual code matches the minimum distance of extremal self-dual codes of length $4n+4$. Refer to Theorem 2.1 for the minimum distance of extremal self-dual codes. In this step, we obtain matrices which can generate the extremal self-dual codes $C(\sigma)$ of length $4n+4$.
8. Classify self-dual codes constructed from the matrices obtained in Step 7 are of Type I or Type II. The binary self-dual code $C(\sigma)$ is said to be of Type I and Type II if the weight of all of its codewords is divisible by two and four respectively. The weight of a codeword a is defined as $w(a) = d(a, 0)$, where $0 = (0, 0, \dots, 0)$ is the zero vector.
9. Lift the obtained self-dual codes in Step 8, to the ring $F_2 + uF_2$, as discussed in Section 2.3. Generate a set of all possible lifted matrices

by mapping an element 0 of F_2 to two elements 0 and u of the ring F_2+uF_2 and element 1 of F_2 is mapped to elements 1 and $1+u$ of the ring F_2+uF_2.

10. From the given set of uplifted matrices, collect matrices that can generate self-dual codes of length $4n+4$, as done in Step 5.
11. Evaluate d_L for the self-dual codes which are generated from matrices collected in Step 10. Here d_L denotes the smallest positive Lee distance of a code. The Lee weight of the ring F_2+uF_2 elements $0, 1, u$ and $1+u$ are $0, 1, 2$ and 1, respectively. The Lee distance between $4n+4$ tuple is defined as the sum of Lee weights of the difference between the components of these tuples.
12. Shortlist matrices whose d_L of its corresponding self-dual code matches the minimum distance of extremal self-dual codes of length $2(4n+4)$. In this step, we obtain matrices which can generate the self-dual codes over the ring F_2+uF_2 of length $4n+4$, whose binary images are extremal self-dual codes of length $2(4n+4)$.
13. Classify self-dual codes constructed from the matrices obtained in Step 12 are of Type I or Type II.

4.1. Construction from cyclic group of order 2

Here we execute the above construction for $G = C_2$ over the field F_2 and obtain an extremal self-dual code of length 12. Now, we lift the code A_1 over the Frobenius ring F_2+uF_2 to obtain an extremal self-dual code of length 12, whose binary image is the Type II extremal self-dual code of length 24.

TABLE 1. Self-dual codes of length 12 from C_2 over F_2.

Code(A_i)	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	$\lvert Aut(A_i)\rvert$	*Type*
1	$(1,0,1,1,1,0,0,0)$	$(0,0)$	$(0,0)$	$(1,0)$	23040	$[12,6,4]_I$

TABLE 2. The extremal binary self-dual codes of length 24 obtained from F_2+uF_2 lift of A_1.

$CodeI_i$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	*Type*
1	A_1	$(1,u,1,1,1,0,0,u)$	$(0,u)$	$(0,0)$	$(1,0)$	*TypeII*

4.2. Construction from cyclic group of order 3

Here we execute the above construction for $G = C_3$ over the field F_2 and obtain an extremal self-dual code of length 16.

Now, we lift the codes B_1, B_2, and B_3 over the Frobenius ring F_2+uF_2 to

TABLE 3. Self-dual codes of length 16 from C_3 over F_2.

$Code(B_i)$	$(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	$\lvert Aut(B_i)\rvert$	$Type$
1	$(1,0,1,1,1,0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(1,0,0)$	5160960	$[16,8,4]_{II}$
2	$(1,0,0,0,0,0,0,1)$	$(0,0,0)$	$(0,0,0)$	$(1,1,0)$	3612672	$[16,8,4]_{II}$
3	$(1,0,1,1,0,0,0,1)$	$(0,0,0)$	$(0,0,0)$	$(1,1,0)$	73728	$[16,8,4]_I$

obtain an extremal self-dual code of length 16, whose binary image is the Type II extremal self-dual code of length 32.

TABLE 4. The extremal binary self-dual codes of length 32 obtained from $F_2 + uF_2$ lift of B_1, B_2 and B_3.

$CodeJ_i$		$(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	$Type$
1	B_1	$(1,u,1,1,1,0,0,u)$	$(u,0,0)$	$(0,0,0)$	$(1,0,0)$	$TypeII$
2	B_1	$(u+1,0,1,u+1,u+1,u,0,u)$	$(u,0,0)$	(u,u,u)	$(u+1,u,u)$	$TypeII$
3	B_2	$(1,0,0,0,0,0,0,1)$	$(0,u,u)$	$(0,0,0)$	$(1,1,0)$	$TypeII$
4	B_2	$(u+1,0,0,u,u,0,0,1)$	$(u,0,0)$	(u,u,u)	$(u+1,u+1,u)$	$TypeII$
5	B_3	$(1,0,1,1,0,0,u,1)$	$(0,u,u)$	$(0,0,0)$	$(1,1,0)$	$TypeII$
6	B_3	$(u+1,0,1,u+1,0,u,0,1)$	$(u,0,0)$	(u,u,u)	$(u+1,u+1,u)$	$TypeII$

4.3. Construction from cyclic group of order 4

Here we execute the above construction for $G = C_4$ over the field F_2 and obtain an extremal self-dual code of length 20.

TABLE 5. Self-dual codes of length 20 from C_4 over F_2.

$Code(D_i)$	$(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	$\lvert Aut(D_i)\rvert$	$Type$
1	$(1,0,1,1,1,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$	$(1,0,0,0)$	1857945600	$[20,10,4]_I$
2	$(1,0,1,1,1,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$	$(1,1,1,0)$	294912	$[20,10,4]_I$
3	$(1,0,1,1,1,0,0,0)$	$(1,0,0,0)$	$(1,0,0,0)$	$(1,0,0,0)$	4423680	$[20,10,4]_I$
4	$(1,0,1,1,1,0,0,0)$	$(1,0,0,0)$	$(1,0,0,0)$	$(1,1,0,1)$	122880	$[20,10,4]_I$

Now, we lift the codes D_1, D_2, D_3, and D_4 over the Frobenious ring $F_2 + uF_2$ to obtain extremal self-dual code of length 20, whose binary image is the Type II extremal self-dual code of length 40.

TABLE 6. The extremal binary self-dual codes of length 40 obtained from $F_2 + uF_2$ lift of D_1, D_2, D_3 and D_4.

$Code(K_i)$		$(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	$Type$
1	D_1	$(1,u,1,1,1,0,0,u)$	$(0,0,u,0)$	$(0,0,0,0)$	$(1,0,0,0)$	$TypeII$
2	D_1	$(1,u,1,1,u+1,0,0,u)$	$(u,u,0,u)$	(u,u,u,u)	$(1,0,u,0)$	$TypeII$
3	D_2	$(1,u,1,1,1,0,0,u)$	$(0,0,u,0)$	$(0,0,0,0)$	$(1,1,1,u)$	$TypeII$
4	D_2	$(u+1,0,u+1,u+1,u+1,u,u,0)$	$(u,u,0,u)$	(u,u,u,u)	$(u+1,u+1,u+1,0)$	$TypeII$

4.4. Construction from cyclic group of order 5

Here we execute the above construction for $G = C_5$ over the field F_2 and obtain an extremal self-dual code of length 24 of Type I and well known Extended Binary Golay Code.

Table 7. Self-dual codes of length 24 from C_5 over F_2.

$Code(E_i)$	$(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	$\lvert Aut(E_i)\rvert$	$Type$
1	$(1,0,0,0,0,0,0,1)$	$(0,0,1,1,0)$	$(0,0,0,0,0)$	$(1,0,1,0,0)$	138240	$[24,12,6]_I$
2	$(1,0,1,1,0,0,0,1)$	$(0,0,1,1,0)$	$(0,0,0,0,0)$	$(1,0,1,0,0)$	244823040	$[24,12,8]_{II}$

Now, we lift the codes E_2 over the Frobenious ring $F_2 + uF_2$ to obtain extremal self-dual code of length 24, whose binary image is the well known Extended QR code.

Table 8. The extremal binary self-dual codes of length 48 obtained from $F_2 + uF_2$ lift of E_2.

$Code(L_i)$		$(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8)$	$f_{(\sigma(\vartheta_1))}$	$f_{(\sigma(\vartheta_2))}$	f_C	$Type$
1	E_2	$(1,0,1,1,0,0,0,1)$	$(0,u,1,1,u)$	$(0,0,0,u,u)$	$(1,0,1,0,0)$	$[48,24,10]_I$
2	E_2	$(u+1,0,u+1,u+1,0,u,u,u+1)$	$(u,0,u+1,u+1,0)$	(u,u,u,u,u)	$(u+1,u,u+1,0,0)$	$[48,24,12]_{II}$

5. Conclusion

We presented a new method for creating self-dual codes using group rings. By doing so, we were able to show the relevance of this new construct by constructing extremal binary self-double codes of various lengths: $12, 16, 20, 24$ (Extended binary golay code), $32, 40$, and most importantly, we have completed the exhaustive search for $[48, 24, 12]$ self-dual doubly-even codes begun in [6], [7], [12]. We established a link between unitary units/units/non-units and particularly idempotents with self-dual codes. Due to the computing limits imposed by the construction approach, we were able to consider the groups of orders $2, 3, 4$, and 5. These computational techniques can be applied to several families of rings and several groups within this framework.

Acknowledgment. The authors are greatful to the referee for his/her helpful suggestions and comments.

References

[1] E. F. Assmus, Jr., and H. F. Mattson, Jr., *New 5-designs*, J. Combinatorial Theory **6** (1969), 122–151. `https://doi.org/10.1016/S0021-9800(69)80115-8`

[2] F. Bernhardt, P. Landrock, and O. Manz, *The extended Golay codes considered as ideals*, J. Combin. Theory Ser. A **55** (1990), no. 2, 235–246. `https://doi.org/10.1016/0097-3165(90)90069-9`

[3] S. T. Dougherty, *Algebraic Coding Theory over Finite Commutative Rings*, SpringerBriefs in Mathematics, Springer, Cham, 2017. `https://doi.org/10.1007/978-3-319-59806-2`

[4] S. T. Dougherty, J. Kim, H. Kulosman, and H. Liu, *Self-dual codes over commutative Frobenius rings*, Finite Fields Appl. **16** (2010), no. 1, 14–26. https://doi.org/10.1016/j.ffa.2009.11.004

[5] S. T. Dougherty, B. Yildiz, and S. Karadeniz, *Codes over R_k, Gray maps and their binary images*, Finite Fields Appl. **17** (2011), no. 3, 205–219. https://doi.org/10.1016/j.ffa.2010.11.002

[6] S. Houghten, C. Lam, and L. Thiel, *Construction of* $(48, 24, 12)$ *doubly-even self-dual codes*, Congr. Numer. **103** (1994), 41–53.

[7] S. K. Houghten, C. W. H. Lam, L. H. Thiel, and J. A. Parker, *The extended quadratic residue code is the only* $(48, 24, 12)$ *self-dual doubly-even code*, IEEE Trans. Inform. Theory **49** (2003), no. 1, 53–59. https://doi.org/10.1109/TIT.2002.806146

[8] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003. https://doi.org/10.1017/CBO9780511807077

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

[10] J. Gildea, A. Korban, A. Kaya, and B. Yildiz, *Constructing self-dual codes from group rings and reverse circulant matrices*, Adv. Math. Commun. **15** (2021), no. 3, 471–485. https://doi.org/10.3934/amc.2020077

[11] J. Gildea, R. Taylor, A. Kaya, and A. Tylyshchak, *Double bordered constructions of self-dual codes from group rings over Frobenius rings*, Cryptogr. Commun. **12** (2020), no. 4, 769–784. https://doi.org/10.1007/s12095-019-00420-3

[12] I. McLoughlin, *A group ring construction of the* $[48, 24, 12]$ *type II linear block code*, Des. Codes Cryptogr. **63** (2012), no. 1, 29–41. https://doi.org/10.1007/s10623-011-9530-0

[13] I. McLoughlin and T. Hurley, *A group ring construction of the extended binary Golay code*, IEEE Trans. Inform. Theory **54** (2008), no. 9, 4381–4383. https://doi.org/10.1109/TIT.2008.928260

[14] C. Polcino Milies and S. K. Sehgal, *An introduction to group rings*, Algebra and Applications, 1, Kluwer Academic Publishers, Dordrecht, 2002.

[15] E. M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 134–139. https://doi.org/10.1109/18.651000

[16] The SAGE Group, *SAGE*: *Mathematical software*, version 2.10, http://www.sagemath.org/

Shefali Gupta
Department of Applied Mathematics
Delhi Technological University
Delhi 110042, India
Email address: shefali.gupta48@yahoo.com

Dinesh Udar
Department of Applied Mathematics
Delhi Technological University
Delhi 110042, India
Email address: dineshudar@yahoo.com