# MODIFIED QUADRATIC RESIDUE CONSTRUCTIONS AND NEW EXTREMAL BINARY SELF-DUAL CODES OF LENGTHS 64, 66 AND 68

JOE GILDEA, HOLLY HAMILTON, ABIDIN KAYA AND BAHATTIN YILDIZ

ABSTRACT. In this work we consider modified versions of quadratic double circulant and quadratic bordered double circulant constructions over the binary field and the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ for different prime values of $p$. Using these constructions with extensions and neighbors we are able to construct a number of extremal binary self-dual codes of different lengths with new parameters in their weight enumerators. In particular we construct 2 new codes of length 64, 4 new codes of length 66 and 14 new codes of length 68. The binary generator matrices of the new codes are available online at [8].

## 1. INTRODUCTION

Self-dual codes are a special class of codes that have algebraic and combinatorial properties, which connect them to many different structures such as lattices, invariant theory, designs, cryptography and recently with quantum codes ([11]). There are many different approaches of constructing self-dual codes in the literature. One particular construction makes use of quadratic residues modulo a prime $p$.

Let $R$ be a finite commutative Frobenius ring of characteristic 2 and $p$ be prime. Let $\gamma_i \in R$, $A$ be a $p \times p$ circulant matrix, $Q_r(a, b, c)$ be the $p \times p$ circulant matrix with three free variables, obtained through the quadratic residues and non-residues modulo $p$. Thus, the first row of $\overline{r} = (r_0, r_1, \ldots, r_{p-1})$ of $Q_p(a, b, c)$ is determined by the following rule:

$$r_i = \begin{cases} a & \text{if } i = 0 \\ b & \text{if } i \text{ is a quadratic residue modulo } p \\ c & \text{if } i \text{ is a quadratic non-residue modulo } p. \end{cases}$$

This type of quadratic circulant matrix and a bordered version were first introduced by Gaborit in [7] to construct self-dual codes over fields and later were extended over rings in [13] and [16] to construct self-dual codes over different alphabets. The main construction used in the works mentioned was to take a matrix of the form $[I_p|A]$ where $A$ is either $Q_p(a, b, c)$ or its bordered version. Note that the quadratic circulant matrix is a special case of a double circulant matrix which produces self-dual quasi-cyclic codes ([20]).

In this work, we modify this construction by replacing $I_p$ with an arbitrary circulant matrix in the double circulant case, and we do a similar replacement in the bordered case. More precisely, we consider the following type of matrices:

$$M = (Q_p(a, b, c)|A)\,,$$

where $A$ is a $p \times p$ circulant matrix and

$$M = \left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \gamma_2 & \cdots & \gamma_2 & \gamma_3 & \gamma_4 & \cdots & \gamma_4 \\ \hline \gamma_2 & & & & \gamma_4 & & & \\ \vdots & & Q_p(a,b,c) & & \vdots & & A & \\ \gamma_2 & & & & \gamma_4 & & & \end{array}\right),$$

where $A$ is a $p \times p$ circulant matrix.

---

1991 *Mathematics Subject Classification.* 94B05, 15B33.

*Key words and phrases.* combinatorial problems; extremal self-dual codes; codes over rings; quadratic residues; quadratic circulant matrices.

We consider these constructions for different prime values $p$ and over the binary field as well as the ring extensions $\mathbb{F}_2+u\mathbb{F}_2$ and $\mathbb{F}_4+u\mathbb{F}_4$. This is a novel construction method for self-dual codes, that combines several approaches in the literature. The strength and novelty of the constructions are demonstrated by the numerous new extremal self-dual codes that we are able to obtain using these methods. In particular, we are able to construct 14 new extremal binary self-dual codes of length 68, 4 new extremal binary self-dual codes of length 66 and 2 new extremal binary self-dual codes of length 64. The new beta values and the weight enumerator classes of the codes are given in section 4.

The rest of the work is organized as follows. In section 2, we give some background on self-dual codes, and the different alphabets that we use. In section 3 we give the constructions. In section 4, we give the numerical results obtained from the constructions. We finish by recapitulating the results and pointing out possible directions for future research.

## 2. Preliminaries

Let $R$ be a commutative Frobenius ring of characteristic 2. A code $C$ of length $n$ over $R$ is an $R$-submodule of $R^n$. Elements of the code $C$ are called codewords of $C$. Let $x=(x_1,x_2,\ldots,x_n)$ and $y=(y_1,y_2,\ldots,y_n)$ be two elements of $R^n$. The duality is understood in terms of the Euclidean inner product; $\langle x,y\rangle_E=\sum x_iy_i$. The dual $C^\perp$ of the code $C$ is defined as

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

We say that $C$ is self-dual if $C=C^\perp$. Two self-dual binary codes of dimension $k$ are said to be *neighbors* if their intersection has dimension $k-1$. A binary self-dual code is called Type II (or doubly even) if the weights of all codewords are divisible by 4, otherwise it is called Type I (or singly even). The best upper bound on the minimum Hamming distance of a binary self-dual code was proved in [19].

**Theorem 2.1.** ([19]) *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*

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

Self-dual codes meeting these bounds are called *extremal*.

2.1. **The ambient rings.** While all of the theoretical results we obtain throughout the paper are valid for all Frobenius rings of characteristic 2, we will be focusing mainly on the binary field $\mathbb{F}_2$ and the rings $\mathbb{F}_2+u\mathbb{F}_2$, $\mathbb{F}_4+u\mathbb{F}_4$ for computational purposes. Similar rings have been considered in coding theory in many different works, e.g. [21] and [22].

Let $\mathbb{F}_4=\mathbb{F}_2(\omega)$ be the quadratic field extension of the binary field $\mathbb{F}_2=\{0,1\}$, 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 $\omega a+\bar{\omega}b$ uniquely, where $a,b\in\mathbb{F}_2+u\mathbb{F}_2$.

$$\begin{array}{ccc}(\mathbb{F}_4+u\mathbb{F}_4)^n & \xrightarrow{\psi_{\mathbb{F}_4+u\mathbb{F}_4}} & (\mathbb{F}_2+u\mathbb{F}_2)^{2n}\\ \downarrow\varphi_{\mathbb{F}_4+u\mathbb{F}_4} & & \downarrow\varphi_{\mathbb{F}_2+u\mathbb{F}_2}\\ \mathbb{F}_4^{2n} & \xrightarrow{\psi_{\mathbb{F}_4}} & \mathbb{F}_2^{4n}\end{array}$$

Let us recall the following Gray Maps from [7,18] and [6];

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

Note that these Gray maps preserve orthogonality in the respective alphabets, for the details we refer to [18]. 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. 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 the maps. A self-dual code 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.

**Proposition 2.2.** ([18]) *Let $C$ be a code over $\mathbb{F}_4 + u\mathbb{F}_4$. If $C$ is self-orthogonal, so are $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$. $C$ 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 $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

**Corollary 2.3.** *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, $C$ and $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ have the same weight enumerator. If $C$ is Type I (Type II), then so is $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

In subsequent sections we will be writing tables in which vectors with elements from the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ will appear. In order to avoid writing long vectors with elements that can be confused with other elements, we will be describing the elements of this ring in a short-hand way, which will make the tables more compact. For the elements of $\mathbb{F}_2 + u\mathbb{F}_2$ we will use $0 \to 0, 1 \to 1, u \to u$ and $1 + u \to 3$.

For the elements of $\mathbb{F}_4 + u\mathbb{F}_4$, we use the ordered basis $\{u\omega, \omega, u, 1\}$ to express the elements of $\mathbb{F}_4 + u\mathbb{F}_4$ as binary strings of length 4. Then we will use the hexadecimal number system to describe each element:

$0 \leftrightarrow 0000$, $1 \leftrightarrow 0001$, $2 \leftrightarrow 0010$, $3 \leftrightarrow 0011$, $4 \leftrightarrow 0100$, $5 \leftrightarrow 0101$, $6 \leftrightarrow 0110$, $7 \leftrightarrow 0111$, $8 \leftrightarrow 1000$, $9 \leftrightarrow 1001$, $A \leftrightarrow 1010$, $B \leftrightarrow 1011$, $C \leftrightarrow 1100$, $D \leftrightarrow 1101$, $E \leftrightarrow 1110$, $F \leftrightarrow 1111$.

For example $1 + u\omega$ corresponds to 1001, which is represented by the hexadecimal 9, while $\omega + u\omega$ corresponds to 1100, which is represented by $C$.

## 3. The Constructions

We will discuss the constructions in two classes. The first will be the pure double circulant and the second will be the bordered one.

3.1. **Generalized quadratic double circulant.** Define the matrix $M = (Q_p(a, b, c) \mid A)$ where $A$ is a $p \times p$ circulant matrix. Let $C$ be the linear code of length $2p$, generated by the matrix $M$. Then

$$MM^T = Q_p(a, b, c)Q_p(a, b, c)^T + AA^T. \tag{1}$$

Note that $Q_p(a, b, c)Q_p(a, b, c)^T$ has previously been calculated in [7] where $Q_p(a, b, c)$ is a $p \times p$ circulant over a finite field. When $Q_p(a, b, c)$ is a $p \times p$ circulant over a ring of characterisitc 2, we can see that

(2)

$$Q_p(a, b, c)Q_p(a, b, c)^T = \begin{cases} Q_p(a^2, b^2 + k(b + c)^2, c^2 + k(b + c)^2) & \text{if } p = 4k + 1 \\ Q_p(a^2 + b^2 + c^2, ab + ac + k(b^2 + c^2) + bc, ab + ac + k(b^2 + c^2) + bc) & \text{if } p = 4k + 3 \end{cases}$$

Combining this with (1), and considering the characteristic we get the following main result:

**Theorem 3.1.** *If $C$ is a linear code generated by $M$ over a ring of characteristic 2, then $C$ is a self-orthogonal code if and only if:*

$$AA^T = \begin{cases} Q_p(a^2, b^2 + k(b + c)^2, c^2 + k(b + c)^2) & \text{if } p = 4k + 1 \\ Q_p(a^2 + b^2 + c^2, ab + ac + k(b^2 + c^2) + bc, ab + ac + k(b^2 + c^2) + bc) & \text{if } p = 4k + 3 \end{cases}.$$

3.2. **Generalized bordered quadratic residue construction.** We will now define a bordered version of the construction. Define the following matrix:

$$M = \left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \gamma_2 & \cdots & \gamma_2 & \gamma_3 & \gamma_4 & \cdots & \gamma_4 \\ \hline \gamma_2 & & & & \gamma_4 & & & \\ \vdots & & Q_p(a,b,c) & & \vdots & & A & \\ \gamma_2 & & & & \gamma_4 & & & \end{array}\right),$$

where $\gamma_i$ are some elements from the ambient ring $R$, which we assume to be a ring of characteristic 2 (including the binary field).

Let $C$ be a code that is generated by the matrix $M$ over $R$. Then, the code $C$ has length $2p+2$.

To make the computations easier, we let $M = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 \\ B_2^T & Q & B_4^T & A \end{pmatrix}$ where $B_1 = (\gamma_1)$, $B_2 = (\gamma_2, \ldots, \gamma_2)$, $B_3 = (\gamma_3)$, $B_4 = (\gamma_4, \ldots, \gamma_4)$ and $Q = Q_p(a,b,c)$. Then,

$$MM^T = \begin{pmatrix} B_1B_1^T + B_2B_2^T + B_3B_3^T + B_4B_4^T & B_1B_2 + B_2Q^T + B_3B_4 + B_4A^T \\ B_2^TB_1^T + QB_2^T + B_4^TB_3^T + AB_4^T & B_2^TB_2 + QQ^T + B_4^TB_4 + AA^T \end{pmatrix}$$

where

- $$\begin{aligned} B_1B_1^T + B_2B_2^T + B_3B_3^T + B_4B_4^T &= \gamma_1^2 + (\gamma_2, \ldots, \gamma_2)(\gamma_2, \ldots, \gamma_2)^T + \gamma_3^2 + (\gamma_4, \ldots, \gamma_4)(\gamma_4, \ldots, \gamma_4)^T \\ &= \gamma_1^2 + p\gamma_2^2 + \gamma_3^2 + p\gamma_4^2 \\ &= \left(\sum_{i=1}^{4} \gamma_i\right)^2. \end{aligned}$$

- $$\begin{aligned} B_1B_2 + B_2Q^T + B_3B_4 + B_4A^T &= \gamma_1(\gamma_2, \ldots, \gamma_2) + (\gamma_2, \ldots, \gamma_2)Q^T + \gamma_3(\gamma_4, \ldots, \gamma_4) + (\gamma_4, \ldots, \gamma_4)A^T \\ &= (\gamma_1\gamma_2, \ldots, \gamma_1\gamma_2) + (\gamma_2(a + b\lambda_p + c\lambda_p), \ldots, \gamma_2(a + b\lambda_p + c\lambda_p)) \\ &+ (\gamma_3\gamma_4, \ldots, \gamma_3\gamma_4) + (\gamma_4\mu, \ldots, \gamma_4\mu) \\ &= (\gamma_1\gamma_2 + \gamma_2(a + b\lambda_p + c\lambda_p) + \gamma_3\gamma_4 + \gamma_4\mu, \ldots, \\ &\gamma_1\gamma_2 + \gamma_2(a + b\lambda_p + c\lambda_p) + \gamma_3\gamma_4 + \gamma_4\mu) \end{aligned}$$

  where $\mu$ is the sum of the elements in the first row of $A$ and $\lambda_p = \frac{p-1}{2}$.

- $$\begin{aligned} B_2^TB_1^T + QB_2^T + B_4^TB_3^T + AB_4^T &= \begin{pmatrix} \gamma_2 \\ \vdots \\ \gamma_2 \end{pmatrix}\gamma_1 + Q\begin{pmatrix} \gamma_2 \\ \vdots \\ \gamma_2 \end{pmatrix} + \begin{pmatrix} \gamma_4 \\ \vdots \\ \gamma_4 \end{pmatrix}\gamma_3 + A\begin{pmatrix} \gamma_4 \\ \vdots \\ \gamma_4 \end{pmatrix} \\ &= \begin{pmatrix} \gamma_1\gamma_2 \\ \vdots \\ \gamma_1\gamma_2 \end{pmatrix} + \begin{pmatrix} \gamma_2(a + b\lambda_p + c\lambda_p) \\ \vdots \\ \gamma_2(a + b\lambda_p + c\lambda_p) \end{pmatrix} + \begin{pmatrix} \gamma_3\gamma_4 \\ \vdots \\ \gamma_3\gamma_4 \end{pmatrix} + \begin{pmatrix} \mu\gamma_4 \\ \vdots \\ \mu\gamma_4 \end{pmatrix} \\ &= \begin{pmatrix} \gamma_1\gamma_2 + \gamma_2(a + b\lambda_p + c\lambda_p) + \gamma_3\gamma_4 + \mu\gamma_4 \\ \vdots \\ \gamma_1\gamma_2 + \gamma_2(a + b\lambda_p + c\lambda_p) + \gamma_3\gamma_4 + \mu\gamma_4 \end{pmatrix}. \end{aligned}$$

$$\bullet\ B_2^TB_2+QQ^T+B_4^TB_4+AA^T=\begin{pmatrix}\gamma_2\\ \vdots\\ \gamma_2\end{pmatrix}(\gamma_2,\dots,\gamma_2)+QQ^T+\begin{pmatrix}\gamma_4\\ \vdots\\ \gamma_4\end{pmatrix}(\gamma_4,\dots,\gamma_4)+AA^T$$
$$=(\gamma_2+\gamma_4)^2\begin{pmatrix}1&\cdots&1\\ \vdots&\ddots&\vdots\\ 1&\cdots&1\end{pmatrix}+QQ^T+AA^T.$$

Using (2) for $QQ^T$, we see that

$$B_2^TB_2+QQ^T+B_4^TB_4+AA^T=\begin{cases}Q_p((\gamma_2+\gamma_4)^2+a^2,(\gamma_2+\gamma_4)^2+b^2+k(b+c)^2,(\gamma_2+\gamma_4)^2\\ +c^2+k(b+c)^2)+AA^T & \text{if } p=4k+1\\ Q_p((\gamma_2+\gamma_4)^2+a^2+b^2+c^2,(\gamma_2+\gamma_4)^2+ab+ac\\ +k(b^2+c^2)+bc,(\gamma_2+\gamma_4)^2+ab+ac+k(b^2+c^2)+bc)+AA^T & \text{if } p=4k+3\end{cases}$$

Combining all these results and factoring in the characteristic of the ambient ring, we arrive at the following results:

**Theorem 3.2.** *Assume that $p=4k+1$. Then, $C$ is a self-orthogonal code if and only if the following conditions hold:*

(1) $\sum_{i=1}^{4}\gamma_i=0$,
(2) $\gamma_1\gamma_2+\gamma_2a+\gamma_3\gamma_4+\gamma_4\mu=0$,
(3) $AA^T=Q_p((\gamma_2+\gamma_4)^2+a^2,(\gamma_2+\gamma_4)^2+b^2+k(b+c)^2,(\gamma_2+\gamma_4)^2+c^2+k(b+c)^2)$.

**Theorem 3.3.** *Assume that $p=4k+3$. Then, $C$ is a self-orthogonal code if and only if the following conditions hold:*

(1) $\sum_{i=1}^{4}\gamma_i=0$,
(2) $\gamma_1\gamma_2+\gamma_2(a+b+c)+\gamma_3\gamma_4+\mu\gamma_4=0$,
(3) $AA^T=Q_p((\gamma_2+\gamma_4)^2+a^2+b^2+c^2,(\gamma_2+\gamma_4)^2+ab+ac+k(b^2+c^2)+bc,(\gamma_2+\gamma_4)^2+ab+ac+k(b^2+c^2)+bc)$.

## 4. Numerical results

We will apply the construction methods described in section 3 to obtain extremal binary self-dual codes of various lengths. We need to point out that the theorems in section 3 provide us with necessary and sufficient conditions for when the codes generated are self-orthogonal. This is one of the points of distinction that our constructions have from those introduced in [7]. Using a random circulant matrix $A$ instead of $I_n$ means that the rank of the codes might not always be that of a self-dual code. However, we believe using a random circulant matrix brings more variety and helps us find more self-dual codes as has been demonstrated by our computations. All the computations are run on Magma ([2]).

4.1. **New Codes of lengths 64.** The possible weight enumerators for a self-dual Type I $[64,32,12]$-code is given in [4,5] as:

$$W_{64,1} = 1+(1312+16\beta)\,y^{12}+(22016-64\beta)\,y^{14}+\cdots,14\le\beta\le284,$$
$$W_{64,2} = 1+(1312+16\beta)\,y^{12}+(23040-64\beta)\,y^{14}+\cdots,0\le\beta\le277.$$

With the most updated information, [1], extremal singly even self-dual codes with weight enumerator $W_{64,1}$ are known

$$\beta\in\left\{\begin{array}{l}14,16,18,20,22,24,25,26,28,29,30,32,\\ 34,35,36,38,39,44,46,53,59,60,64,74\end{array}\right\}$$

and extremal singly even self-dual codes with weight enumerator $W_{64,2}$ are known for

$$\beta \in \left\{ \begin{array}{l} 0,1,...,42,44,45,48,50,51,52,56,58,64,65, \\ 72,80,88,96,104,108,112,114,118,120,184 \end{array} \right\} \setminus \{31,39\}.$$

In this section, we obtain the codes with weight enumerators for $\beta = 48$ and 50 in $W_{64,1}$. We apply Theorem 3.3 for $p = 7$ over $\mathbb{F}_4 + u\mathbb{F}_4$ and obtain Type I codes of length 64 as binary images.

TABLE 1. Self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$ when $p = 7$

| $C_i$ | $(\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ | $(a, b, c)$ | $r_A$ | $\lvert Aut(C_i)\rvert$ | $W_{64,1}$ |
|---|---|---|---|---|---|
| 1 | $(0, 1, B, A)$ | $(B, 4, F)$ | $(A, 4, 6, 5, E, 7, F)$ | $2^2 \cdot 7$ | $\beta = 18$ |
| 2 | $(0, 1, B, A)$ | $(1, 6, 7)$ | $(A, 4, 6, F, E, 5, 7)$ | $2^2 \cdot 7$ | $\beta = 32$ |
| 3 | $(0, 1, B, A)$ | $(1, 6, 7)$ | $(A, 4, 6, 7, E, F, 5)$ | $2^2 \cdot 7$ | $\beta = 46$ |
| 4 | $(0, 1, B, A)$ | $(1, 6, 7)$ | $(A, 4, 6, 5, E, 7, F)$ | $2^2 \cdot 7$ | $\beta = 60$ |

Self dual binary codes $C$ and $D$ of length $n$ are said to be neighbors if $\dim(C \cap D) = n/2 - 1$. In order to consider some neighbors of a code $C$ we pick a vector $x \in \mathbb{F}_2^n - C$ and let $D = \left\langle \langle x \rangle^{\perp} \cap C, x \right\rangle$. We use the standard form of the generator matrix of $C$, which lets us to fix first $n/2$ entries of $x$ without loss of generality. We set the first 32 entries of $x$ to be 0. We consider the neighbours of the binary images of the codes in Table 1 and obtain new codes of length 64 which are listed in Table 2.

TABLE 2. New codes of length 64 ($W_{64,1}$) as neighbours of codes in Table 1

| $\mathcal{D}_{64,i}$ | $C_j$ | $(x_{33}, x_{34}, ..., x_{64})$ | $\beta$ | $\lvert Aut(\mathcal{D}_{64,i})\rvert$ |
|---|---|---|---|---|
| 1 | 4 | (00001100111100110111000000001110) | **48** | 2 |
| 2 | 4 | (01110111100100101111100100110111) | **50** | 2 |

4.2. **New extremal self-dual codes of lengths 66.** The weight enumerator of an extremal self-dual code of length 66 is given in [5] as follows:

$$\begin{aligned} W_{66,1} &= 1 + (858 + 8\beta)y^{12} + (18678 - 24\beta)y^{14} + \cdots \quad \text{where } 0 \le \beta \le 778, \\ W_{66,2} &= 1 + 1690y^{12} + 7990y^{14} + \cdots \quad \text{and} \\ W_{66,3} &= 1 + (858 + 8\beta)y^{12} + (18166 - 24\beta)y^{14} + \cdots \quad \text{where } 14 \le \beta \le 756. \end{aligned}$$

Together with the codes recently obtained in [1] and the ones from [12], [14], [15] and [16], extremal singly even self-dual codes with weight enumerator $W_{66,1}$ are known for

$$\beta \in \{0, 1, 2, 3, 5, 6, \ldots, 94, 100, 101, 115\}$$

and extremal singly even self-dual codes with weight enumerator $W_{66,3}$ are known for

$$\beta \in \{22, 23, \ldots, 92\} \setminus \{65, 68, 69, 72, 89, 91\}.$$

In this section, we construct the codes with weigth enumerators for $\beta$=65, 68, 69 and 72 in $W_{66,3}$ as extensions of codes in Section 4.1.

We recall the following extension theorem that helps us construct self-dual codes of length $2n+2$ from self-dual codes of length $2n$:

**Theorem 4.1.** ([17]) *Let $C$ be a binary self-dual code of length $2n$, $G = (r_i)$ be an $n \times 2n$ generator matrix for $C$, where $r_i$ is the $i$-th row of $G$, $1 \le i \le n$. Let $X$ be a vector in $\mathbb{F}_2^{2n}$ with $\langle X, X \rangle = 1$. Let $y_i = \langle r_i, X \rangle$ for $1 \le i \le n$. Then the following matrix*

$$\left[\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & y_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_n & y_n & r_n \end{array}\right],$$

*generates a binary self-dual code of length* $2n+2$.

We apply Theorem 4.1 to the codes of length 64 tabulated in Table 1 and 2 to find extremal self-dual codes of length 66, with $X = (0_{32}|x)$, where $0_{32}$ denotes that the first 32 bits of $X$ are 0's. The new codes of length 66 that we obtain are tabulated in the following table:

TABLE 3. Extremal Self-dual code of length 66 from binary extensions of codes of length 64

| $\mathcal{N}_{66,i}$ | Code | $x$ | $W_{66,3}$ | $\lvert Aut(\mathcal{N}_{66,i})\rvert$ |
|---|---|---|---|---|
| 1 | $C_3$ | (10101101111000010010011001101101) | $\beta = \mathbf{65}$ | 1 |
| 2 | $\mathcal{D}_{64,2}$ | (11010111011111000001101111100100) | $\beta = \mathbf{68}$ | 1 |
| 3 | $C_3$ | (00011111011010110011100110110000) | $\beta = \mathbf{69}$ | 1 |
| 4 | $C_4$ | (00001111111011001101011110101001) | $\beta = \mathbf{72}$ | 1 |

4.3. **New extremal self-dual codes of length 68.** The possible weight enumerator of an extremal binary self-dual code of length 68 (of parameters $[68, 34, 12]$) is in one of the following forms by [3,10]:

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

where $0 \le \gamma \le 9$. Recently, Yankov et al. constructed the first examples of codes with a weight enumerator for $\gamma = 7$ in $W_{68,2}$. The new codes we have constructeed all have $\gamma = 0, 1$ or 2 in $W_{68,2}$. So, in order to save space we only give the list of known values for $\gamma = 0$, $\gamma = 1$ and $\gamma = 2$ in $W_{68,2}$. For a full list of known codes we refer to [9].

$$\begin{aligned} \gamma &= 0,\ \beta = 0,\ 7,\ 11,\ 14,\ 17,\ 21,\ 22,\ 28,\ 33,\ 35,\ 42,\ 44, \ldots, 158, 159,\ 161,\ 163,\ 165, \\ &\quad 175,\ 187,\ 189,\ 203,\ 209,\ 221,\ 231,\ 255,\ 303 \text{ or} \\ \beta &\in \{2m \mid m = 17,\ 20,\ 102,\ 110,\ 119,\ 136,\ 165 \text{ or } 80 \le m \le 99\}; \\ \gamma &= 1,\ \beta = 49, 51, 53, 55,\ 57,\ 59, \ldots, 160, 161, 163, 165, 167, 169, 171 \text{ or} \\ \beta &\in \{2m \mid m = 22, 24, \ldots,\ 29,\ 81, \ldots,\ 90, 92, \ldots,\ 96\}; \\ \gamma &= 2,\ \beta = 58, 65, 69, 71, 73, 75, 77, 79, 81, 157, 159,\ 206,\ 208 \text{ or } \beta \in \{2m \mid 30 \le m \le 100\} \text{ or} \\ \beta &\in \{2m+1 \mid 41 \le m \le 77\} \end{aligned}$$

In the following table, we list self-dual codes of length 68 as Gray images of codes over $\mathbb{F}_2 + u\mathbb{F}_2$ via Theorem 3.1 for $p = 17$.

TABLE 4. Self-dual codes of length 68 via $\mathbb{F}_2 + u\mathbb{F}_2$ when $p = 17$ ($W_{68,2}$)

| $\mathcal{D}_i$ | $(a, b, c)$ | $r_A$ | $\lvert Aut(\mathcal{D}_i)\rvert$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|---|
| 1 | $(1, u, u)$ | $(0, 0, 0, u, u, 1, 3, 3, 0, u, 1, 3, u, 3, 3, 1, 3)$ | $2^2 \cdot 7$ | 0 | $\beta = 204$ |
| 2 | $(1, u, u)$ | $(u, u, u, 0, 0, 3, 3, 3, 0, u, 1, 3, 0, 3, 3, 1, 1)$ | $2^2 \cdot 7$ | 0 | $\beta = 238$ |
| 3 | $(1, u, u)$ | $(0, u, 0, 0, 0, 1, 3, 1, 0, u, 3, 3, 0, 1, 1, 3, 3)$ | $2^2 \cdot 7$ | 0 | $\beta = 272$ |

By considering the neighbours of codes in Table 4 we construct 14 new codes of length 68, which are listed in Table 5. The generator matrix of $\mathcal{D}_j$ is used in standard form. Therefore, we assume the first 34 entries to be 0 without loss of generality.

TABLE 5. New codes of length 68 ($W_{68,2}$) as neighbours of codes in Table 4

| $\mathcal{N}_{68,i}$ | $\mathcal{D}_j$ | $(x_{35}, x_{36}, ..., x_{68})$ | $\gamma$ | $\beta$ | $\lvert Aut(\mathcal{N}_{68,i})\rvert$ |
|---|---|---|---|---|---|
| 1 | 1 | (11101110110100010011010100010000 10) | 0 | **167** | 2 |
| 2 | 3 | (10101110001101000001001101011001 10) | 0 | **169** | 2 |
| 3 | 2 | (11110010100001100110011001000010 00) | 0 | **171** | 1 |
| 4 | 3 | (00100011011011000010111010011111 10) | 0 | **173** | 1 |
| 5 | 2 | (11010001101011000100010011011101 11) | 0 | **177** | 1 |
| 6 | 2 | (10010000001001100100111001100100 11) | 0 | **179** | 1 |
| 7 | 3 | (00011000011100110011010100110011 10) | 0 | **181** | 2 |
| 8 | 3 | (10011011011010011101010001001111 00) | 0 | **202** | 2 |
| 9 | 3 | (10010110001100100110100110101100 10) | 0 | **217** | 2 |
| 10 | 1 | (11101101101100011100010000000011 01) | 1 | **183** | 2 |
| 11 | 3 | (01100111001101010101101111011011 11) | 1 | **199** | 2 |
| 12 | 3 | (01000010001101110010110000011000 00) | 1 | **207** | 1 |
| 13 | 3 | (11001111011000011110111100111100 00) | 1 | **214** | 2 |
| 14 | 2 | (10111010100100001100101100001001 11) | 2 | **216** | 2 |

## 5. Conclusion

In this work, we introduced modified versions of quadratic double circulant and bordered quadratic double circulant constructions for self-dual codes. We demonstrated the relevance of this new construction by constructing many binary self-dual codes, including new extremal binary self-dual codes of length 64, 66 and 68.

- **Codes of length** 64**:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{64,1}$:
$$\beta = \{48, 50\}.$$
- **Codes of length** 66**:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{66,3}$:
$$\beta = \{65, 68, 69, 72\}.$$
- **Codes of length** 68**:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{68,2}$:
$$(\gamma = 0, \quad \beta = \{167, 169, 171, 173, 177, 179, 181, 202, 217\}).$$
$$(\gamma = 1, \quad \beta = \{183, 199, 207, 214\}).$$
$$(\gamma = 2, \quad \beta = \{216\}).$$

A possible direction for future research could be considering different primes $p$ and different alphabets that could result in self-dual codes of different lengths.

**Acknowledgment:** The authors would like to thank the anonymous referees and the editor for their valuable remarks that improved the presentation of this 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 Struct. Appl. **5** (2018), no. 3, 143–151.
[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).
[3] S. Buyuklieva and I. Boukliev, *Extremal self-dual codes with an automorphism of order* 2, IEEE Trans. Inform. Theory **44** (1998), no. 1, 323–328.
[4] J. H. Conway and Sloane N.J.A, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory **36** (1990), no. 6, 1319–1333.
[5] S.T. Dougherty, T.A. Gulliver, and M. Harada, *Extremal binary self-dual codes*, IEEE Trans. Inform. Theory **43** (1997), no. 6, 2036–2047.

[6] S.T. Dougherty, P. Gaborit, M. Harada, and Patrick Solé, *Type II codes over* $\mathbf{F}_2 + u\mathbf{F}_2$, IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45.
[7] P. Gaborit, *Quadratic double circulant codes over fields*, J. Combin. Theory Ser. A **97** (2002), no. 1, 85–107.
[8] J. Gildea, H. Hamilton, A. Kaya, and B. Yildiz, *"Binary generator matrices for extremal binary self-dual codes of lengths* $64, 66$ *and* $68$*"*, available at `http://abidinkaya.wixsite.com/math/gildeaqr`.
[9] J. Gildea, A. Kaya, and B. Yildiz, *An altered four circulant construction for self-dual codes from group rings and new extremal binary self-dual codes I*, Discrete Math. **342** (2019), no. 12, 111620, 8.
[10] M. Harada and A. Munemasa, *Some restrictions on weight enumerators of singly even self-dual codes*, IEEE Trans. Inform. Theory **52** (2006), no. 3, 1266–1269.
[11] M. Harada, *New quantum codes constructed from some self-dual additive* $F_4$*-codes*, Inform. Prcoess. Letters **138** (2018), 35–38.
[12] S. Karadeniz and B. Yildiz, *New extremal binary self-dual codes of length 66 as extensions of self-dual codes over* $R_k$, J. Franklin Inst. **350** (2013), no. 8, 1963–1973.
[13] A. Kaya, B. Yildiz, and I. Siap, *Quadratic residue codes over* $\mathbb{F}_p + v\mathbb{F}_p$ *and their Gray images*, J. Pure Appl. Algebra **218** (2014), no. 11, 1999–2011.
[14] A. Kaya, *New extremal binary self-dual codes of lengths 64 and 66 from* $R_2$*-lifts*, Finite Fields Appl. **46** (2017), 271–279.
[15] A. Kaya, B. Yildiz, and A. Pasa, *New extremal binary self-dual codes from a modified four circulant construction*, Discrete Math. **339** (2016), no. 3, 1086–1094.
[16] A. Kaya, B. Yildiz, and I. Siap, *New extremal binary self-dual codes from* $\mathbb{F}_4 + u\mathbb{F}_4$*-lifts of quadratic circulant codes over* $\mathbb{F}_4$, Finite Fields Appl. **35** (2015), 318–329.
[17] J. L. Kim, *New extremal self-dual codes of lengths 36, 38, and 58*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 386–393.
[18] S. Ling and P. Solé, *Type II codes over* $\mathbf{F}_4 + u\mathbf{F}_4$, European J. Combin. **22** (2001), no. 7, 983–997.
[19] E.M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 134–139.
[20] M.Shi, L. Qian, Y. Liu, and P. Solé, *Good self-dual generalized quasi-cylic codes exist*, Inform. Process. Letters **118** (2017), 21–24.
[21] M.Shi, L. Qian, L. Sok, and P. Solé, *On constacyclic codes over* $\mathbb{Z}_4[u]/ < u^2 - 1 >$ *and their Gray images*, Finite Fields Appl. **45** (2017), 86–95.
[22] M.Shi, Y. Guan, and P. Solé, *Two new families of two-weight codes*, IEEE Trans. Inform. Theory **63** (2017), no. 10, 6240–6246.

Department of Mathematics, Faculty of Science and Engineering, University of Chester, England
*Email address*: `j.gildea@chester.ac.uk`

Department of Mathematics, Faculty of Science and Engineering, University of Chester, England
*Email address*: `holham30@gmail.com`

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

Department of Mathematics & Statistics, Northern Arizona University, Flagstaff, AZ 86001, USA
*Email address*: `bahattin.yildiz@nau.edu`