NEW EXTREMAL BINARY SELF-DUAL CODES FROM BLOCK CIRCULANT MATRICES AND BLOCK QUADRATIC RESIDUE CIRCULANT MATRICES

J GILDEA, A KAYA, R TAYLOR, A TYLYSHCHAK, B YILDIZ

Abstract. In this paper, we construct self-dual codes from a construction that involves both block circulant matrices and block quadratic residue circulant matrices. We provide conditions when this construction can yield self-dual codes. We construct self-dual codes of various lengths over $\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2$. Using extensions, neighbours and sequences of neighbours, we construct many new self-dual codes. In particular, we construct one new self-dual code of length 66 and 51 new self-dual codes of length 68.

1. Introduction

Self-dual codes are a class of linear block codes that have been extensively studied in recent history. One of the most famous and extensively used constructions, used to construct self-dual codes, is the double circulant construction. It involves considering a generator matrix of the form $(I|A)$ where A is a circulant matrix. In 2002, Gaborit ([6]) introduced the notion of a quadratic residue circulant matrix. 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:

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

In [6], Gaborit considered constructing self-dual codes from generator matrices of the form $(I|Q_p(a, b, c))$ and

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

In [7], these techniques were extended to constructing self-dual codes from generator matrices of the form $(Q_p(a, b, c)|A)$ and

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

where A is a $p \times p$ circulant matrix. In this article we consider constructing self-dual codes from generator matrices of the form

$$\left(\begin{array}{ccc|ccc} Q_0 & Q_1 & Q_2 & A_0 & A_1 & A_2 \\ Q_2 & Q_0 & Q_1 & A_2 & A_0 & A_1 \\ Q_1 & Q_2 & Q_0 & A_1 & A_2 & A_0 \end{array}\right)$$

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

Key words and phrases. self-dual codes, codes over rings, quadratic double circulant codes.

where Q_i are quadratic residue circulant matrices and A_i are $p \times p$ circulant matrices.

Section 2 of this article contains a brief introduction to self-dual codes. We discuss some important properties of quadratic residue circulant matrices in section 3. In section 4, we describe the construction itself. We provide theoretical results that establish certain conditions when this construction yields self-dual codes. In section 5, we apply the construction to find many known and unknown self-dual codes that had not been previously constructed. We conclude with listing the newly constructed codes and a suggestion for future work.

2. Preliminaries

Throughout this paper, R will denote 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 $x = (x_1, x_2, \ldots, x_n) \in R^n$ and $y = (y_1, y_2, \ldots, y_n) \in R^n$. Define the Euclidean inner product between x and y as $\langle x, y \rangle_E = \sum x_i y_i$. The dual $C^\perp$ of the code C is defined as

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

If $C = C^\perp$, we say that C is self-dual. For binary codes, a self-dual code where all weights are congruent to 0 (mod 4) is said to be Type II and a self-dual binary code is said to be Type I otherwise. The bounds on the minimum distances for self-dual codes are given in [15] and are as follows:

Theorem 2.1. ([15]) *Let $d_I(n)$ and $d_{II}(n)$ be the minimum distances 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 that meet these bounds are called *extremal*.

Although, the theoretical result in this article is based around commutative Frobenius rings of characteristic 2, all the computational results are based on the rings $\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2$. Now, $\mathbb{F}_2 + u\mathbb{F}_2 := \mathbb{F}_2[X]/(X^2)$, where u satisfies $u^2 = 0$. Thus, the elements of the ring are $0, 1, u$ and $1 + u$, where 1 and $1 + u$ are the units of $\mathbb{F}_2 + u\mathbb{F}_2$. We also define the Gray map ϕ from $\mathbb{F}_2 + u\mathbb{F}_2$ to $\mathbb{F}_2^2$ given by $\phi(a + bu) = (b, a + b)$ where $a, b \in \mathbb{F}_2$.

The next result, introduced in [14], will be implemented throughout this article.

Theorem 2.2. *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, $1 \leq i \leq n$. 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 $1 \leq i \leq n$. 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 $2n + 2$.

Two self-dual binary codes of dimension k are said to be neighbours if their intersection has dimension $k - 1$. Let C be a self-dual code. Let $x \in \mathbb{F}_2^n - C$ then $D = \left\langle \langle x \rangle^\perp \cap C, x \right\rangle$ is a neighbour of C. Let $x_0 \in \mathbb{F}_2^{2n} - \mathcal{N}_{(0)}$. In [8], the following formula for constructing the k-range neighbour codes was provided:

$$\mathcal{N}_{(i+1)} = \left\langle \langle x_i \rangle^{\perp} \cap \mathcal{N}_{(i)}, x_i \right\rangle$$

where $\mathcal{N}_{(i+1)}$ is the neighbour of $\mathcal{N}_{(i)}$ and $x_i \in \mathbb{F}_2^{2n} - \mathcal{N}_{(i)}$.

3. Quadratic Residue Circulant Matrices

Let $Q_p(a_i, b_i, c_i)$ be the i^{th}-$p \times p$ quadratic circulant matrix, where $a_i, b_i, c_i \in R$ and p is a prime number and $0 \leq i \leq 2$. For the purposes of this article, we need to evaluate $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$. From [6], we can clearly see that $Q_p(a_i, b_i, c_i)Q_p(a_i, b_i, c_i)^T$

$$= \begin{cases} Q_p(a_i^2, b_i^2 + k(b_i^2 + c_i^2), c_i^2 + k(b_i^2 + c_i^2)) & \text{if } p = 4k+1 \\ Q_p(a_i^2 + b_i^2 + c_i^2, a_ib_i + a_ic_i + b_ic_i + (b_i^2 + c_i^2)k, a_ib_i + a_ic_i + b_ic_i + (b_i^2 + c_i^2)k) & \text{if } p = 4k+3 \end{cases}.$$

We shall now calculate $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$. First we will consider the case when $p = 4k+1$ and then the case when $p = 4k+3$.

Theorem 3.1. *If $p = 4k+1$ then $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$*

$$= Q_p(a_ia_j, a_ib_j + b_ia_j + (k+1)b_ib_j + k(b_ic_j + c_ib_j) + kc_ic_j, a_ic_j + c_ia_j + kb_ib_j + k(b_ic_j + c_ib_j) + (k+1)c_ic_j).$$

Proof. Assume that $p = 4k+1$. Let $Q = Q_p(0,1,0)$ and $N = Q_p(0,0,1)$, then

$$\begin{aligned} Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T &= (a_iI + b_iQ + c_iN)(a_jI + b_jQ + c_jN)^T \\ &= (a_iI + b_iQ + c_iN)(a_jI + b_jQ^T + c_jN^T) \\ &= a_ia_jI + a_ib_jQ^T + a_ic_jN^T + b_ia_jQ + b_ib_jQQ^T \\ &\quad + b_ic_jQN^T + c_ia_jN + c_ib_jNQ^T + c_ic_jNN^T. \end{aligned}$$

Recall ([6]) that $Q = Q^T$, $N = N^T$, $QQ^T = (k+1)Q + kN$, $QN^T = NQ^T = k(Q+N)$ and $NN^T = kQ + (k+1)N$. Therefore,

$$\begin{aligned} Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T =& a_ia_jI + (a_ib_j + b_ia_j)Q + (a_ic_j + c_ia_j)N + b_ib_j((k+1)Q + kN) \\ &+ (b_ic_i + c_ib_j)(k(Q+N)) + c_ic_j(kQ + (k+1)N) \\ =& a_ia_jI + (a_ib_j + b_ia_j)Q + (a_ic_j + c_ia_j)N + b_ib_j(k+1)Q + b_ib_jkN \\ &+ (b_ic_i + c_ib_j)kQ + (b_ic_i + c_ib_j)kN + c_ic_jkQ + c_ic_j(k+1)N \\ =& I[a_ia_j] + Q[a_ib_j + b_ia_j + (k+1)b_ib_j + k(b_ic_j + c_ib_j) + kc_ic_j] \\ &+ N[a_ic_j + c_ia_j + kb_ib_j + k(b_ic_j + c_ib_j) + (k+1)c_ic_j] \end{aligned}$$

$= Q_p(a_ia_j, a_ib_j + b_ia_j + (k+1)b_ib_j + k(b_ic_j + c_ib_j) + kc_ic_j, a_ic_j + c_ia_j + kb_ib_j + k(b_ic_j + c_ib_j) + (k+1)c_ic_j)$. □

Theorem 3.2. *If $p = 4k+3$ then $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$*

$$\begin{aligned} = Q_p(&a_ia_j + b_ib_j + c_ic_j, (a_ic_j + b_ia_j) + k(b_ib_j + c_ic_j) + kb_ic_j + (k+1)c_ib_j, \\ &(a_ib_j + c_ia_j) + k(b_ib_j + c_ic_j) + (k+1)b_ic_j + kc_ib_j) \end{aligned}.$$

Proof. Assume that $p = 4k+3$. Then

$$\begin{aligned} Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T &= a_ia_jI + a_ib_jQ^T + a_ic_jN^T + b_ia_jQ + b_ib_jQQ^T \\ &\quad + b_ic_jQN^T + c_ia_jN + c_ib_jNQ^T + c_ic_jNN^T. \end{aligned}$$

Recall ([6]) that $Q = N^T$, $QQ^T = NN^T = I + kQ + kN$, $QN^T = kQ + (k+1)N$ and $NQ^T = (k+1)Q + kN$. Therefore,

$$\begin{aligned}
Q_p(a_i,b_i,c_i)Q_p(a_j,b_j,c_j)^T =& a_ia_jI+(a_ic_j+b_ia_j)Q+(a_ib_j+c_ia_j)N+(b_ib_j+c_ic_j)QQ^T+b_ic_jQN^T+c_ib_jNQ^T\\
=& a_ia_jI+(a_ic_j+b_ia_j)Q+(a_ib_j+c_ia_j)N+(b_ib_j+c_ic_j)(I+kQ+kN)\\
&+b_ic_j(kQ+(k+1)N)+c_ib_j((k+1)Q+kN)\\
&=a_ia_jI+(a_ic_j+b_ia_j)Q+(a_ib_j+c_ia_j)N+(b_ib_j+c_ic_j)I+k(b_ib_j+c_ic_j)Q\\
&+k(b_ib_j+c_ic_j)N+kb_ic_jQ+(k+1)b_ic_jN+(k+1)c_ib_jQ+kc_ib_jN\\
&=I[a_ia_j+b_ib_j+c_ic_j]+Q[(a_ic_j+b_ia_j)+k(b_ib_j+c_ic_j)+kb_ic_j\\
&+(k+1)c_ib_j]+N[(a_ib_j+c_ia_j)+k(b_ib_j+c_ic_j)+(k+1)b_ic_j+kc_ib_j]\\
&=Q_p(a_ia_j+b_ib_j+c_ic_j,(a_ic_j+b_ia_j)+k(b_ib_j+c_ic_j)+kb_ic_j+(k+1)c_ib_j,\\
&(a_ib_j+c_ia_j)+k(b_ib_j+c_ic_j)+(k+1)b_ic_j+kc_ib_j)
\end{aligned}$$

□

4. The Construction

We shall now describe the main construction itself and provide conditions when this construction produces self-dual codes. Let $Q_l=Q_p(a_l,b_l,c_l)$. Define the matrix

$$M=\left(\begin{array}{ccc|ccc} Q_0 & Q_1 & Q_2 & A_0 & A_1 & A_2\\ Q_2 & Q_0 & Q_1 & A_2 & A_0 & A_1\\ Q_1 & Q_2 & Q_0 & A_1 & A_2 & A_0\end{array}\right)$$

and let $\mathcal{C}$ be the linear code of length $6p$ generated by the matrix M, where A_i are $p\times p$ circulant matrices over R. Let $CIRC(A_1,\dots,A_n)$ be the block circulant matrix where the first row of block matrices are $A_1,\dots,A_n$ and $a_{[l]_3}=a_{(l \mod 3)}$, then

$$MM^T=CIRC\left(\sum_{i=0}^{2}(Q_iQ_i^T+A_iA_i^T),\sum_{i=0}^{2}Q_iQ_{[(i+2)]_3}^T+A_iA_{[(i+2)]_3}^T,\left(\sum_{i=0}^{2}Q_iQ_{[(i+2)]_3}^T+A_iA_{[(i+2)]_3}^T\right)^T\right).$$

Clearly, C is self-orthogonal if and only $\sum_{i=0}^{2}A_iA_i^T=\sum_{i=0}^{2}Q_iQ_i^T$ and $\sum_{i=1}^{3}A_iA_{[(i+2)]_3}^T=\sum_{i=1}^{3}Q_iQ_{[(i+2)]_3}^T$.

Using Theorem 3.1, we can see that $\sum_{i=0}^{2}Q_iQ_i^T=$

$$\begin{cases} Q_p\left(\sum_{i=0}^{2}a_i^2,\sum_{i=0}^{2}(b_i^2+k(b_i^2+c_i^2)),\sum_{i=0}^{2}(c_i^2+k(b_i^2+c_i^2))\right) & \text{if } p=4k+1\\ Q_p\left(\sum_{i=0}^{2}(a_i^2+b_i^2+c_i^2),\sum_{i=0}^{2}(a_ib_i+a_ic_i+b_ic_i+k(b_i^2+c_i^2),\sum_{i=0}^{2}(a_ib_i+a_ic_i+b_ic_i+k(b_i^2+c_i^2)\right) & \text{if } p=4k+3\end{cases}.$$

Additionally (by Theorem 3.2), if $p=4k+1$ then

$$\begin{aligned}\sum_{i=1}^{3}Q_iQ_{[(i+2)]_3}^T=Q_p\Bigg(&\sum_{i=0}^{2}a_ia_{[(i+2)]_3},\sum_{i=0}^{2}(a_ib_{[(i+2)]_3}+b_ia_{[(i+2)]_3}+(k+1)b_ib_{[(i+2)]_3}+k(b_ic_{[(i+2)]_3}+c_ib_{[(i+2)]_3}\\
&+kc_ic_{[(i+2)]_3}),\sum_{i=0}^{2}(a_ic_{[(i+2)]_3}+c_ia_{[(i+2)]_3}+kb_ib_{[(i+2)]_3}+k(b_ic_{[(i+2)]_3}+c_ib_{[(i+2)]_3}+(k+1)c_ic_{[(i+2)]_3})\Bigg)\end{aligned}$$

and if $p = 4k+3$ then

$$\sum_{i=1}^{3} Q_i Q_{[(i+2)]_3}^T = Q_p \Bigg(\sum_{i=0}^{2} (a_i a_{[(i+2)]_3} + b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}, \sum_{i=0}^{2} [(a_i c_{[(i+2)]_3} + b_i a_{[(i+2)]_3}) + k(b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}) + k b_i c_{[(i+2)]_3} + (k+1) c_i b_{[(i+2)]_3}], \sum_{i=0}^{2} [(a_i b_{[(i+2)]_3} + c_i a_{[(i+2)]_3}) + k(b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}) + (k+1) b_i c_{[(i+2)]_3} + k c_i b_{[(i+2)]_3})] \Bigg)$$

Combining these results, we reach the following:

Theorem 4.1. *Assume that $p = 4k+1$. Then, C is a self-orthogonal code if and only if the following conditions hold:*

(1) $$\sum_{i=0}^{2} A_i A_i^T = Q_p \left(\sum_{i=0}^{2} a_i^2, \sum_{i=0}^{2} (b_i^2 + k(b_i^2 + c_i^2)), \sum_{i=0}^{2} (c_i^2 + k(b_i^2 + c_i^2)) \right),$$

(2)

$$\sum_{i=1}^{3} A_i A_{[(i+2)]_3}^T = Q_p \Bigg(\sum_{i=0}^{2} a_i a_{[(i+2)]_3}, \sum_{i=0}^{2} (a_i b_{[(i+2)]_3} + b_i a_{[(i+2)]_3} + (k+1) b_i b_{[(i+2)]_3} + k(b_i c_{[(i+2)]_3} + c_i b_{[(i+2)]_3} + k c_i c_{[(i+2)]_3}), \sum_{i=0}^{2} (a_i c_{[(i+2)]_3} + c_i a_{[(i+2)]_3} + k b_i b_{[(i+2)]_3} + k(b_i c_{[(i+2)]_3} + c_i b_{[(i+2)]_3} + (k+1) c_i c_{[(i+2)]_3}) \Bigg).$$

Theorem 4.2. *Assume that $p = 4k+3$. Then, C is a self-orthogonal code if and only if the following conditions hold:*

(1) $$\sum_{i=0}^{2} A_i A_i^T = Q_p \left(\sum_{i=0}^{2} (a_i^2 + b_i^2 + c_i^2), \sum_{i=0}^{2} (a_i b_i + a_i c_i + b_i c_i + k(b_i^2 + c_i^2), \sum_{i=0}^{2} (a_i b_i + a_i c_i + b_i c_i + k(b_i^2 + c_i^2) \right),$$

(2)

$$\sum_{i=1}^{3} A_i A_{[(i+2)]_3}^T = Q_p \Bigg(\sum_{i=0}^{2} (a_i a_{[(i+2)]_3} + b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}, \sum_{i=0}^{2} [(a_i c_{[(i+2)]_3} + b_i a_{[(i+2)]_3}) + k b_i b_{[(i+2)]_3} + k c_i c_{[(i+2)]_3} + k b_i c_{[(i+2)]_3} + (k+1) c_i b_{[(i+2)]_3}], \sum_{i=0}^{2} [(a_i b_{[(i+2)]_3} + c_i a_{[(i+2)]_3}) + k b_i b_{[(i+2)]_3} + k c_i c_{[(i+2)]_3} + (k+1) b_i c_{[(i+2)]_3} + k c_i b_{[(i+2)]_3})] \Bigg).$$

Theorem 4.3. *The matrix M has full rank iff the following conditions hold:*

(1) $\sum_{i=0}^{2} (A_i C_i + A_i D_i) = I_p$,

(2) $\sum_{i=0}^{2} (A_i C_{[i+2]_3} + A_i D_{[i+2]_3}) = 0_p$ *and*

(3) $\sum_{i=0}^{2} (A_i C_{[i+1]_3} + A_i D_{[i+1]_3}) = 0_p$

for some $p \times p$ circulant matrices C_k and D_l over R.

Proof. Clearly,

$$M = \left(\; CIRC(Q_0, Q_1, Q_2) \mid CIRC(A_0, A_1, A_2) \; \right)$$

has full rank iff $MN = I_{3p}$ for some $6p \times 3p$ matrix N over R. Let $N' = (n_1, \ldots, n_{6p})^T$ be the first column of N, clearly $M(circ(n_1, \ldots, n_p)^T, \ldots, circ(n_{5p+1}, \ldots, n_{6p})^T)^T = (I_p, 0_p, 0_p, 0_p, 0_p, 0_p)^T$. If $N'' = (C_0, C_1, C_2, D_0, D_1, D_2)^T$ is the matrix that satisfies $MN'' = (I_p, 0_p, 0_p, 0_p, 0_p, 0_p)^T$, then N can take the form

$$N = \begin{pmatrix} CIRC(C_0, C_2, C_1) \\ CIRC(D_0, D_2, D_1) \end{pmatrix}$$

where C_k and D_l are $p \times p$ circulant matrices over R. Now,

$$MN = CIRC\left(\sum_{i=0}^{2}(A_iC_i + A_iD_i), \sum_{i=0}^{2}(A_iC_{[i+2]_3} + A_iD_{[i+2]_3}), \sum_{i=0}^{2}(A_iC_{[i+1]_3} + A_iD_{[i+1]_3})\right)$$

and M has full rank iff:

(1) $\displaystyle\sum_{i=0}^{2}(A_iC_i + A_iD_i) = I_p$,

(2) $\displaystyle\sum_{i=0}^{2}(A_iC_{[i+2]_3} + A_iD_{[i+2]_3}) = 0_p$ and

(3) $\displaystyle\sum_{i=0}^{2}(A_iC_{[i+1]_3} + A_iD_{[i+1]_3}) = 0_p$

□

Theorem 4.4. *Let $\mathcal{C}$ be self-dual. Then,*

$$\left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right)^T B' = I_p$$

for some $p \times p$ matrices B and B' over R.

Proof. By the previous result,

(1) $\displaystyle\sum_{i=0}^{2}(A_iC_i + A_iD_i) = I_p$,

(2) $\displaystyle\sum_{i=0}^{2}(A_iC_{[i+2]_3} + A_iD_{[i+2]_3}) = 0_p$ and

(3) $\displaystyle\sum_{i=0}^{2}(A_iC_{[i+1]_3} + A_iD_{[i+1]_3}) = 0_p$.

Adding these equations, we obtain that

$$\left(\sum_{i=0}^{2} Q_i\right)\left(\sum_{i=0}^{2} C_i\right) + \left(\sum_{i=0}^{2} A_i\right)\left(\sum_{i=0}^{2} D_i\right) = I_p.$$

Let $Q_3 = \displaystyle\sum_{i=0}^{2}Q_i$, $A_3 = \displaystyle\sum_{i=0}^{2}A_i$, $C_3 = \displaystyle\sum_{i=0}^{2}C_i$ and $D_3 = \displaystyle\sum_{i=0}^{2}D_i$. Thus,

$$Q_3C_3 + A_3D_3 = I_p$$

and

$$(Q_3C_3 + A_3D_3)^T = C_3^TQ_3^T + D_3^TA_3^T = Q_3^TC_3^T + A_3^TD_3^T = I_p$$

since circulant matrices commute. Therfore,

$$\begin{aligned} Q_3C_3 + A_3D_3 &= Q_3C_3 + A_3(Q_3^TC_3^T + A_3^TD_3^T)D_3 \\ &= Q_3C_3 + A_3Q_3^TC_3^TD_3 + A_3A_3^TD_3^TD_3 \\ &= I_p. \end{aligned}$$

If $\mathcal{C}$ is self-dual, then $MM^T = 0_{3p}$ and

$$\begin{pmatrix} I_p & I_p & I_p \end{pmatrix} MM^T \begin{pmatrix} I_p & I_p & I_p \end{pmatrix}^T = 0_p.$$

Consequently,

$$\begin{pmatrix} Q_3 & Q_3 & Q_3 & A_3 & A_3 & A_3 \end{pmatrix}\begin{pmatrix} Q_3 & Q_3 & Q_3 & A_3 & A_3 & A_3 \end{pmatrix}^T = 0_p \text{ and } Q_3Q_3^T = A_3A_3^T.$$

Finally,

$$\begin{aligned} I_p &= Q_3C_3 + A_3Q_3^TC_3^TD_3 + A_3A_3^TD_3^TD_3 \\ &= Q_3C_3 + A_3Q_3^TC_3^TD_3 + Q_3Q_3^TD_3^TD_3 \\ &= Q_3C_3 + Q_3Q_3^TD_3^TD_3 + A_3Q_3^TC_3^TD_3 \\ &= Q_3(C_3 + Q_3^TD_3^TD_3) + Q_3^T(A_3C_3^TD_3) \\ &= Q_3B + Q_3^TB' \end{aligned}$$

where $B = C_3 + Q_3^TD_3^TD_3$ and $B' = A_3C_3^TD_3$. □

Theorem 4.5. *Assume that $p = 4k+1$. Let $\mathcal{C}$ be self-dual. Then, $\sum_{i=0}^{2} Q_i$ is invertible.*

Proof. By the previous result,

$$\left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right)^T B' = I_p$$

for some $p \times p$ matrices B and B' over R. Clearly, $Q_i = a_iI_p + b_iQ + c_iN$ where $Q = Q_p(0,1,0)$, $N = Q_p(0,0,1)$. Now,

$$\begin{aligned} Q_i^T &= (a_iI_p + b_iQ + c_iN)^T \\ &= a_iI_p + b_iQ^T + c_iN^T \\ &= a_iI_p + b_iQ + c_iN \\ &= Q_i \end{aligned}$$

since $Q = Q^T$, $N = N^T$. Therefore,

$$\left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right)^T B' = \left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right) B' = \left(\sum_{i=0}^{2} Q_i\right)(B + B') = I_p$$

and $\sum_{i=0}^{2} Q_i$ is invertible. □

In the next result, we consider a specific example of a commutative Frobenius ring of characteristic 2. For the purpose of the next result, we assume that R is a local ring with a residue class field that contains 2 elements.

Theorem 4.6. *Assume that $p = 4k+3$, R be a local ring with a residue class field that contains* 2 *elements and assume that k is even. Let $\mathcal{C}$ be a self-dual code over R. Then, $\sum_{i=0}^{2} Q_i$ is invertible.*

Proof. Let $Q_3 = \sum_{i=0}^{2} Q_i$, $a_3 = \sum_{i=0}^{2} a_i$, $b_3 = \sum_{i=0}^{2} b_i$ and $c_3 = \sum_{i=0}^{2} c_i$. Clearly, $Q_3 = a_3 I_p + b_3 Q + c_3 N$ (where $Q = Q_p(0,1,0)$, $N = Q_p(0,0,1)$) and $Q_3 B + Q_3^T B' = I_p$ for some matrices B and B'. Let J be the unique maximal ideal in R. It remains to show that $Q_3 \pmod J$ is invertible. If $b_3 \equiv c_3 \pmod J$ then

$$Q_3^T \equiv (a_3 I_p + b_3 Q + b_3 N)^T \equiv a_3 I_p + b_3 Q^T + b_3 N^T \equiv a_3 I_p + b_3 N + b_3 Q \equiv Q_3 \pmod J$$

since $Q = N^T$. Therefore,

$$Q_3(B + B') \equiv Q_3 B + Q_3^T B' \equiv I_p \pmod J.$$

and $Q_3 \pmod J$ is invertible.

If $b_3 \not\equiv c_3 \pmod J$ then $b_3 + c_3 \equiv 1 \pmod J$ and

$$(\underbrace{1,\dots,1}_{p}) Q_3^T = (\underbrace{1,\dots,1}_{p}) Q_3 \equiv (\underbrace{a_3 + b_3 + c_3, \dots, a_3 + b_3 + c_3}_{p}) \equiv (a_3 + 1)(\underbrace{1,\dots,1}_{p}) \pmod J.$$

Thus

$$(\underbrace{1,\dots,1}_{p}) Q_3 B + (\underbrace{1,\dots,1}_{p}) Q_3^T B' = (\underbrace{1,\dots,1}_{p}) I_p,$$

$$(a_3+1)(\underbrace{1,\dots,1}_{p})(B + B') \equiv (a_3+1)(\underbrace{1,\dots,1}_{p}) B + (a_3+1)(\underbrace{1,\dots,1}_{p}) B' \equiv (\underbrace{1,\dots,1}_{p}) \pmod J$$

and

$$(a_3+1)(\underbrace{1,\dots,1}_{p})(B + B')(\underbrace{1,\dots,1}_{p})^T \equiv (\underbrace{1,\dots,1}_{p})(\underbrace{1,\dots,1}_{p})^T \equiv 1 \pmod J.$$

So $a_3 + 1$ is invertible by modulo ideal J and $a_3 \equiv 0 \pmod J$. Thus $Q_3 \equiv Q \pmod J$ or $Q_3 \equiv N \pmod J$ and $Q^2 = N^2 = I_p$ since k is even and $Q^2 = N^2 = I_p + kQ + kN$. Thus $Q_3 \pmod J$ is invertible. □

5. Numerical results

In this section, we construct new self-dual codes of length 66 and 68 via certain extensions, neighbours and sequences of neighbours. Initially, we consider the above construction when $p = 5$ over $\mathbb{F}_2 + u\mathbb{F}_2$. We construct an extremal self-dual code (type I) of length 60 (described in Table 1). From this code, we construct an extremal self-dual code (type I) of length 64 via an $\mathbb{F}_2 + u\mathbb{F}_2$ extension (Table 2). Next, we find a new self-dual code of length 66 by an $\mathbb{F}_2$ extension of the previously constructed self-dual code of length 64 (Table 3). Finally, we find new self-dual codes of length 68 via an $\mathbb{F}_2 + u\mathbb{F}_2$ extension of the previously constructed self-dual code of length 64 and sequences of neighbours of this code (Tables 4, 5, 6, 7 and 8). Magma ([2]) was used to construct all of the codes throughout this section.

The possible weight enumerators for a self-dual Type I $[60, 30, 12]$-code is given in [4, 5] as:

$$\begin{aligned} W_{60,1} &= 1 + 3451y^{12} + 24128y^{14} + 336081y^{16} + \cdots, \\ W_{60,2} &= 1 + (2555 + 64\beta)\, y^{12} + (33600 - 384\beta)\, y^{14} + \cdots, 0 \le \beta \le 10. \end{aligned}$$

Extremal singly even self-dual codes with weight enumerator $W_{60,1}$ and $W_{60,2}$ are known ([10]) for $\beta \in \{0, 1, \dots, 8, 10\}$.

To begin with, we construct the following code:

The possible weight enumerators for a self-dual Type I $[64, 32, 12]$-code are given in [4, 5] as:

$$\begin{aligned} W_{64,1} &= 1 + (1312 + 16\beta)\, y^{12} + (22016 - 64\beta)\, y^{14} + \cdots, 14 \le \beta \le 284, \\ W_{64,2} &= 1 + (1312 + 16\beta)\, y^{12} + (23040 - 64\beta)\, y^{14} + \cdots, 0 \le \beta \le 277. \end{aligned}$$

TABLE 1. Self-dual codes of length 60 (codes over $\mathbb{F}_2+u\mathbb{F}_2$ when $p=5$)

$\mathcal{C}_i$	(a_1,b_1,c_1)	(a_2,b_2,c_2)	(a_3,b_3,c_3)	v_1	v_2	v_3	$Aut(\mathcal{C}_i)$	β
1	(u,u,u)	$(u,u,1)$	$(1,u,0)$	$(u,u,u,u,0)$	$(u,0,0,u,1)$	$(u,u+1,u+1,u,0)$	$2^3\cdot 3\cdot 5$	0

Extremal singly even self-dual codes with weight enumerators $W_{64,1}$ are known ([1,9,16])

$$\beta \in \left\{ \begin{array}{c} 14,16,18,19,20,22,24,25,26,28,29,30,32,34, \\ 35,36,38,39,44,46,49,53,54,58,59,60,64,74 \end{array} \right\}$$

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

$$\beta \in \left\{ \begin{array}{c} 0,...,40,41,42,44,45,46,47,48,49,50,51,52,54,55,56,57, \\ 58,60,62,64,69,72,80,88,96,104,108,112,114,118,120,184 \end{array} \right\} \setminus \{31,39\}.$$

The weight enumerators of an extremal self-dual code of length 66 is given in [5] as follows:

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

Together with the codes recently obtained in [1] and the ones from [12], [13] and [7], 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

$$\beta \in \{22,23,\ldots,92\}\setminus\{89,91\}.$$

The known weight enumerators of a self-dual $[68,34,12]_I$-code are as follows ([3,11]):

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

where $0\le\gamma\le 9$. Codes have been obtained for $W_{68,2}$ when ([8])

$\gamma=2,\ \beta\in\{2m|m=29,\ldots,100,103,104\}$; or $\beta\in\{2m+1|m=32,\ldots,81,84,85,86\}$;

$\gamma=3,\ \beta\in\{2m|m=39,\ldots,92,94,95,97,98,101,102\}$; or

$\beta\in\{2m+1|m=38,40,43,\ldots,77,79,80,81,83,87,88,89,96\}$;

$\gamma=4,\ \beta\in\{2m|m=43,46,\ldots,58,60,\ldots,93,97,98,100\}$; or

$\beta\in\{2m+1|m=48,\ldots,55,57,58,60,61,62,64,68,\ldots,72,74,78,79,80,83,84,85,89,95\}$;

$\gamma=5$ with $\beta\in\{101,105,109,111,...,182,187,189,191,192,193,195,198,200,201,202,211,213\}$

$\gamma=6,\ \beta\in\{131,133,137,\ldots,202,203,206,207,210\}$;

$\gamma=7,\ \beta\in\{7m\,|m=14,\ldots 22,28,\ldots,39,42\}$ or $\beta\in\{155,\ldots,199\}$;

$\gamma=8,\ \beta\in\{180,\ldots,221\}$;

$\gamma=9,\ \beta\in\{186,\ldots,226,228,230\}$;

Applying Theorem 2.2 over $\mathbb{F}_2$ and $\mathbb{F}_2+u\mathbb{F}_2$ (to the code constructed in Table 1), we construct self-dual codes of lengths 64, 66 and 68 (Tables 2, 3 and 4). We replace 3 with $1+u$ to save space.

TABLE 2. Self-dual codes of length 64 from $\mathbb{F}_2+u\mathbb{F}_2$ extensions of codes from Table 2

$\mathcal{D}_i$	$\mathcal{C}_i$	c	X	$W_{64,i}$	β	$Aut(\mathcal{D}_i)$
1	1	3	$(uu0u3030u330301013u1u1100u1311)$	1	14	2^2

TABLE 3. Self-dual codes of length 66 from $\mathbb{F}_2$ extensions of codes from Table 3 where $x_i = 0$ for $1 \leq i \leq 33$.

$\mathcal{E}_i$	$\mathcal{D}_i$	c	X	$W_{66,i}$	β	$Aut(\mathcal{E}_i)$
1	1	1	(001111001101100110011110011101011)	3	**21**	1

TABLE 4. Self-dual codes of length 68 ($W_{68,2}$) from $\mathbb{F}_2 + u\mathbb{F}_2$ extensions of codes from Table 2

$\mathcal{F}_i$	$\mathcal{D}_i$	c	X	α	β	$Aut(\mathcal{F}_i)$
1	1	$1+u$	$(0uu01u130130000031100u1u331030u0)$	2	67	2

Let $\mathcal{N}_{(0)} = \mathcal{F}_1$. Applying the k^{th}-range neighbour formula (in section 2), we obtain:

TABLE 5. i^{th} neighbour of $\mathcal{N}_{(0)}$

i	$\mathcal{N}_{(i+1)}$	x_i	γ	β
0	$\mathcal{N}_{(1)}$	(101000100111110010101010010000001)	3	103
1	$\mathcal{N}_{(2)}$	(100101010000111100111110001111110)	4	124
2	$\mathcal{N}_{(3)}$	(111110101111110111101000011011011)	5	134
3	$\mathcal{N}_{(4)}$	(101010001110000110001100011001001)	6	149
4	$\mathcal{N}_{(5)}$	(001010100011000101101010101101011)	6	133
5	$\mathcal{N}_{(6)}$	(000000100100011110111100000001011)	**7**	**145**
6	$\mathcal{N}_{(7)}$	(110111110111111100111110101011101)	**8**	**161**
7	$\mathcal{N}_{(8)}$	(100100000110001000011110000011001)	**8**	**153**
8	$\mathcal{N}_{(9)}$	(001011101101001110000111000010111)	**9**	**177**

We shall now separately consider the neighbours of $\mathcal{N}_{(7)}$, $\mathcal{N}_{(8)}$ and $\mathcal{N}_{(9)}$.

TABLE 6. New codes of length 68 as neighbours

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
7		(1001110100001011001000010110001111)	**6**	**135**	7		(0110101110011000110111101110111101)	**7**	**142**
7		(1010101111010000011101101110100001)	**7**	**144**	7		(1010000000100110010001100111001011)	**7**	**148**
7		(1100000100000010000001111101000110)	**7**	**150**	7		(0000001101101010011100110000101010)	**7**	**152**
7		(1100001010100000101010001010000011)	**8**	**156**	7		(0111011101011111010001111101111101)	**8**	**157**
7		(1001110111011110111110110100110111)	**8**	**158**	7		(1100111101110001001101011111111010)	**8**	**159**
7		(0111111111111101111011010001001110)	**8**	**160**	7		(0000010100011010000011100000110110)	**8**	**162**
7		(1011100110110111110001111010111001)	**8**	**163**	7		(1000001100011101010001001011100111)	**8**	**164**
7		(0101101010111111100000010110011010)	**8**	**165**	7		(1100111110111111011000111101101101)	**8**	**166**
7		(0110110011000101101101010000111011)	**8**	**167**	7		(1110001001011001000010101101101111)	**8**	**168**
7		(0000110001100111100110010110000100)	**8**	**169**	7		(1101100001010100111111000110010000)	**8**	**170**
7		(0100111101011101000000001111011110)	**8**	**171**	7		(1101011100101001111000001010101101)	**8**	**172**
7		(0011011111010111110100010011001110)	**8**	**173**	7		(1000000111111110110000111001110100)	**8**	**174**
7		(1000111010001101101000001010100111)	**8**	**175**	7		(1011011001110100101000011000010011)	**8**	**176**
7		(1101110100011011100010110101010001)	**8**	**177**	7		(0000001001111010000101101011000101)	**8**	**178**
7		(1010110111110111000100101010000110)	**8**	**179**					

6. CONCLUSION

In this work, we introduced a new construction that involved both block circulant matrices and block quadratic residue circulant matrices. We demonstrated the relevance of this new construction by constructing many binary self-dual codes, including new self-dual codes of length 66 and 68.

- **Codes of length 66:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{66,3}$:

$$\beta = \{21\}.$$

Table 7. New codes of length 68 as neighbours

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \ldots, x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \ldots, x_{68})$	γ	β
8		(1011100000000100011001011001010000)	**6**	**134**	8		(0100011011001110010010110000110000)	**7**	**146**
8		(1000010001101000000110110001001100)	**8**	**154**	8		(0100010111101000010111100101011101)	**8**	**155**

Table 8. New codes of length 68 as neighbours

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \ldots, x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \ldots, x_{68})$	γ	β
9		(1011000010111001011111100101111111)	**9**	**169**	9		(0111011011011100111010101011101011)	**9**	**171**
9		(1010111001101000111110101111110011)	**9**	**173**	9		(1000100101111111111101111101000011)	**9**	**174**
9		(1001010100111110011111000101100001)	**9**	**175**	9		(1100110001000010011000011000010100)	**9**	**176**
9		(0000111100010110110000010011101110)	**9**	**178**	9		(0000111111001110111000111100010001)	**9**	**179**
9		(0010110110000001011001111001010110)	**9**	**180**	9		(1101100001101011010000110010101111)	**9**	**181**
9		(1000010010001101110110100111100100)	**9**	**182**	9		(1111010101110110001110101110011011)	**9**	**183**
9		(0101001111100011111010011011111011)	**9**	**184**	9		(1011000000001100111100001100011001)	**9**	**185**

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

$$(\gamma = 6, \quad \beta = \{134, 135\}).$$
$$(\gamma = 7, \quad \beta = \{142, 144, 145, 146, 148, 150, 152\}).$$
$$(\gamma = 8, \quad \beta = \{153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179\}).$$
$$(\gamma = 9, \quad \beta = \{169, 171, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185\}).$$

In this paper, we considered 3×3 blocks of both block circulant matrices and block quadratic residue circulant matrices. A possible direction in the future could be to consider $n \times n$ blocks of both block circulant matrices and block quadratic residue circulant matrices.

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] P. Gaborit, *Quadratic double circulant codes over fields*, J. Combin. Theory Ser. A **97** (2002), no. 1, 85–107.

[7] J. Gildea, H. Hamilton, A. Kaya, and B. Yildiz, *"Binary generator matrices for extremal binary self-dual codes of lengths* 64, 66 *and* 68*"*, to appear in Inform. Process. Lett. (https://doi.org/10.1016/j.ipl.2020.105927).

[8] J. Gildea, A. Kaya, A. Korban, and B. Yildiz, *New Extremal binary self-dual codes of length 68 from a novel approach to neighbors*, https://arxiv.org/abs/2002.10030.

[9] J. Gildea, A. Kaya, A. Korban, and B. Yildiz, *Constructing Self-Dual Codes from Group Rings and Reverse Circulant Matrices*, to appear in Adv. Math. Commun.

[10] M. Harada, *Binary extremal self-dual codes of length 60 and related codes*, Des. Codes Cryptogr. **86** (2018), no. 5, 1085–1094.

[11] 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.

[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, *New extremal binary self-dual codes of lengths 64 and 66 from R_2-lifts*, Finite Fields Appl. **46** (2017), 271–279.

[14] J. L. Kim, *New extremal self-dual codes of lengths 36, 38, and 58*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 386–393.

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

[16] N. Yankov and D. Anev, *On the self-dual codes with an automorphism of order 5*, Appl. Algebra Engrg. Comm. Comput. **https://doi.org/10.1007/s00200-019-00403-0** (2019).

Department of Mathematics, Faculty of Science and Engineering, University of Chester, England
E-mail address: j.gildea@chester.ac.uk

Department of Mathematics Education, Sampoerna University, 12780, Jakarta, Indonesia
E-mail address: nabidin@gmail.com

Department of Mathematics, Faculty of Science and Engineering, University of Chester, England
E-mail address: rhian.taylor@chester.ac.uk

Department of Algebra, Uzhgorod National University, Uzhgorod, Ukraine
E-mail address: alxtlk@bigmir.net

Department of Mathematics & Statistics, Northern Arizona University, Flagstaff, AZ 86001, USA
E-mail address: Bahattin.Yildiz@nau.edu