J. Algebra Comb. Discrete Appl.
1(1) • 29-39
Received: 9 July 2014; Accepted: 19 August 2014
DOI 10.13069/jacodesmath.79879

Journal of Algebra Combinatorics Discrete Structures and Applications

New extremal binary self-dual codes of length 68

Research Article

Abidin Kaya[1]*, Bahattin Yildiz[1]**

1. Department of Mathematics, Fatih University, 34500, İstanbul, Turkey

Abstract: In this correspondence, we consider quadratic double and bordered double circulant construction methods over the ring $R := \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, where $u^3 = 1$. Among other examples, extremal binary self-dual codes of length 66 are obtained by these constructions. These are extended by using extension theorems for self-dual codes and as a result 8 new extremal binary self-dual codes of length 68 are obtained. More precisely, codes with β=117, 120, 133 in $W_{68,1}$ and with $\gamma = 1$, β=49, 57, 59 and codes with γ=2, β=69, 81 in $W_{68,2}$ are constructed for the first time in the literature. The binary generators of these codes are available online at [7]. In addition to these, some known codes are reconstructed via this extension. The results are tabulated.

2010 MSC: 94B05, 94B60, 94B65

Keywords: Extremal codes, Codes over rings, Gray maps, Quadratic double-circulant codes

1. Introduction

The theory of self-dual codes, especially the so called extremal ones, has attracted a lot of research in the coding theory community. The connection of self-dual codes with many different fields of study such as designs, lattices and cryptography has made them of interest to many researchers. The theoretical background for extremal binary self-dual codes has been established in [1, 2, 9] and the references therein. In the aforementioned works, among other things, it was established that extremal binary self-dual codes can only have certain weight enumerators. Much of the research in the study of self-dual codes has been towards finding extremal self-dual codes with new weight enumerators.

Starting with [3], the use of quadratic residues has been part of the armory for constructing binary self-dual codes. The method, which combines quadratic residues with the well-known methods of double circulant and bordered double circulant constructions has successfully been used to obtain many new extremal binary self-dual codes in [6] and [8]. In doing so, rings other than the binary field, which are endowed with duality and distance preserving Gray maps were used.

In this work we consider the construction method described above for the ring $R := \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, where $u^3 = 1$. This is a non-chain extension of the binary field. We describe a Lee weight and a related

* *E-mail: akaya@fatih.edu.tr*
** *E-mail: byildiz@fatih.edu.tr*

distance-preserving Gray map for the ring. Unlike many of the rings studied before, the Gray map is not duality-preserving. However we establish the conditions for the Gray image to be self-dual. Using quadratic double and bordered double circulant constructions over the ring R, we find extremal binary self-dual codes of length 66. Applying extensions to these codes we find eight new binary extremal self-dual codes of length 68. More precisely, codes with β=117, 120, 133 in $W_{68,1}$ and with $\gamma = 1$, β=49, 57, 59 and codes with γ=2, β=69, 81 in $W_{68,2}$ are constructed for the first time in the literature.

The rest of the work is organized as follows. Section 2 includes a general overview on the ring R and self-dual codes. In Section 3, we consider projections, lifts and duality conditions. Section 4 contains the quadratic double and bordered double circulant constructions over the ring R and some extremal self-dual examples including codes of length 66. In Section 5, codes of length 66 are extended, using extension theorems, to obtain new extremal binary self-dual codes of length 68. The paper ends with some concluding remarks and comments.

2. Preliminaries

2.1. The structure of the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ with $u^3 = 1$

The ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ defined by the relation $u^3 = 1$ is isomorphic to $\mathbb{F}_2[x]/\langle x^3-1\rangle$. Throughout the text the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ is denoted by R and it is easily observed that $R \cong \mathbb{F}_2 \times \mathbb{F}_4$. The ring R is not a local ring because its ideal structure is given by $I_0 \subset I_{u+u^2}, I_{1+u+u^2} \subset R$ where;

$$\begin{aligned} I_{1+u+u^2} &= \left(1+u+u^2\right) = \left\{0, 1+u+u^2\right\}, \\ I_{u+u^2} &= (1+u) = \left\{0, u+u^2, 1+u, 1+u^2\right\}. \end{aligned}$$

However, it is a Frobenius ring as can easily be seen by the isomorphism $R \cong \mathbb{F}_2 \times \mathbb{F}_4$. The units in the ring R are given by $\left\{1, u, u^2\right\}$ and the non-units are

$$\left\{u+u^2, 1+u, 1+u^2, 1+u+u^2\right\}.$$

The ring R has two primitive idempotent elements $\left\{u+u^2, 1+u+u^2\right\}$. Every element of the ring R can be written in a unique way as $a+bu+cu^2 = \left(1+u+u^2\right)(a+b+c) + \left(u+u^2\right)(a+c+(b+c)\,u)$.

A linear code $\mathcal{C}$ of length n over the ring R is an R-submodule of R^n and has a generating matrix that is permutation equivalent to

$$G = \begin{pmatrix} I_{k_1} & A & B & C \\ 0 & \left(u+u^2\right) I_{k_2} & 0 & \left(u+u^2\right) D \\ 0 & 0 & \left(1+u+u^2\right) I_{k_3} & \left(1+u+u^2\right) E \end{pmatrix}.$$

We define a Gray map as follows;

$$\begin{aligned} \varphi &: R^n \to \mathbb{F}_2^{3n} \\ \overline{a}+\overline{b}u+\overline{c}u^2 &\mapsto \left(\overline{a}, \overline{b}, \overline{c}\right). \end{aligned}$$

Definition 2.1. *The Lee weight of an element $x = a+bu+cu^2 \in R$ is the Hamming weight of its Gray image, i.e. $wt_L\left(a+bu+cu^2\right) = wt_H(a) + wt_H(b) + wt_H(c)$. An element is called even if its Lee weight is even and odd otherwise.*

So, the elements in ideal I_{u+u^2} are even and $1, u, u^2, 1+u+u^2$ are the odd elements. The Lee weight of a codeword is defined to be the sum of the Lee weights of its components. The minimum Lee weight of a code $\mathcal{C}$ is denoted by $wt_L(\mathcal{C})$ and defined as $wt_L(\mathcal{C}) = \min\{wt_L(c) \,|\, c \in \mathcal{C}\}$.

Definition 2.2. *A code $\mathcal{C}$ over R is called an even code if all the codewords have even Lee weight.*

The duality is understood in terms of the Euclidean inner product; $\overline{a} \circ \overline{b} = \sum a_i b_i$. The dual of $\mathcal{C}$ is defined as $\mathcal{C}^{\perp} = \{\overline{y} \in R^n \mid \overline{y} \circ \overline{x} = 0 \text{ for all } \overline{x} \in \mathcal{C}\}$. A code $\mathcal{C}$ is said to be self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ and self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$. A self-dual binary code is said to be Type II if all codewords have weight divisible by 4 and Type I otherwise.

The minimum distance d of a binary self-dual code of length n is bounded above as $d \leq 4\,[n/24] + 6$ if $n \equiv 22 \pmod{24}$ and $d \leq 4\,[n/24] + 4$, otherwise ([1, 9]). A self-dual code is called extremal if it meets the bound.

2.2. Quadratic double circulant codes

Quadratic double circulant (QDC) codes are a generalization of quadratic residue codes and have been introduced in [3]. Let p be an odd prime and $Q_p\,(a,b,c)$ be the circulant matrix with first row r based on quadratic residues modulo p defined as $r\,[1] = a$, $r\,[i+1] = b$ if i is a quadratic residue and $r\,[i+1] = c$ if i is a quadratic non-residue modulo p. We state the special case of the main theorem from [3] where p is an odd prime;

Theorem 2.3. *([3]) Let p be an odd prime and let $Q_p\,(a,b,c)$ be the circulant matrix with a, b and c as the elements of the ring R. If $p = 4k+1$ then*

$$\begin{aligned} & Q_p\,(a,b,c)\,Q_p\,(a,b,c)^T \\ = \; & Q_p\left(a^2 + 2k\left(b^2+c^2\right), 2ab - b^2 + k\,(b+c)^2, 2ac - c^2 + k\,(b+c)^2\right) \end{aligned}$$

If $p = 4k+3$ then

$$\begin{aligned} & Q_p\,(a,b,c)\,Q_p\,(a,b,c)^T \\ = \; & Q_p(a^2 + (2k+1)\left(b^2+c^2\right), ab + ac + k\left(b^2+c^2\right) + (2k+1)\,bc, \\ & ab + ac + k\left(b^2+c^2\right) + (2k+1)\,bc). \end{aligned}$$

Definition 2.4. *([3]) The code generated by $P_p\,(a,b,c) = \left(\, I_p \,|\, Q_p\,(a,b,c) \,\right)$ over the ring R is called a quadratic pure double circulant code and is denoted by $\mathcal{P}_p\,(a,b,c)$. In a similar way, the code generated by*

$$B_p\,(a,b,c \mid \lambda,\beta,\gamma) = \left(\begin{array}{c|cc} I_{p+1} & \lambda & \beta \times \mathbf{1} \\ & \gamma \times \mathbf{1}^T & Q_p\,(a,b,c) \end{array} \right),$$

where $\mathbf{1}$ is the all 1 vector of length p, is called a bordered quadratic double circulant code and is denoted by $\mathcal{B}_p\,(a,b,c \mid \lambda,\beta,\gamma)$.

3. Projections, lifts and duality conditions

Since the Gray map introduced in Section 2 does not preserve orthogonality, we start with determining the conditions when the binary image of a code over the ring R is self-orthogonal. Then, a projection and related lift will be defined. The extended quadratic residue codes of parameters $[24, 12, 8]_2$ and $[48, 24, 12]_2$ which are unique up to equivalence are constructed as lifts of self-dual double circulant binary codes.

The following example indicates that the Gray image of a self-orthogonal code over the ring R is not necessarily a self-orthogonal binary code.

Example 3.1. *Let us consider the code $\mathcal{C}$ over the ring R of length 3 generated by*

$$\left(1+u, 1+u^2, u+u^2\right).$$

We may easily observe that the code is self-orthogonal since

$$(1+u)^2+\left(1+u^2\right)^2+\left(u+u^2\right)^2=1+u^2+1+u+u+u^2=0.$$

On the other hand, its binary image is the code generated by

$$G=\begin{pmatrix}1&1&0&1&0&1&0&1&1\\0&1&1&1&1&0&1&0&1\\1&0&1&0&1&1&1&1&0\end{pmatrix}$$

and it is not self-orthogonal since distinct rows of G are not orthogonal to each other.

Definition 3.2. *A vector $\overline{x}=\overline{a}+\overline{b}u+\overline{c}u^2$ over the ring R can be expressed as*

$$\overline{x}=\left(1+u+u^2\right)\left(\overline{a}+\overline{b}+\overline{c}\right)+\left(u+u^2\right)\left(\overline{a}+\overline{c}+\left(\overline{b}+\overline{c}\right)u\right).$$

$\overline{a}+\overline{b}+\overline{c}$ and $\overline{a}+\overline{c}+\left(\overline{b}+\overline{c}\right)u$ are called $\mathbb{F}_2$ and $\mathbb{F}_4$-components of $\overline{x}$, respectively.

Definition 3.3. *A matrix over the ring R is said to be free of u if all its entries are of the form $a+bu^2$ with $a,\ b\in\mathbb{F}_2$.*

Lemma 3.4. *The Gray images of two vectors $\overline{x}=\overline{a}+\overline{b}u+\overline{c}u^2$ and $\overline{y}=\overline{d}+\overline{e}u+\overline{f}u^2$ in R^n are orthogonal to each other if their $\mathbb{F}_2$-components are orthogonal and the product of their $\mathbb{F}_4$-components is free of u.*

Proof. If the $\mathbb{F}_2$-components of the vectors $\overline{x}$ and $\overline{y}$ are orthogonal we have

$$\left(\overline{a}+\overline{b}+\overline{c}\right)\circ\left(\overline{d}+\overline{e}+\overline{f}\right)=\overline{a}\circ\overline{d}+\overline{a}\circ\overline{e}+\overline{a}\circ\overline{f}+\overline{b}\circ\overline{d}+\overline{b}\circ\overline{e}+\overline{b}\circ\overline{f}+\overline{c}\circ\overline{d}+\overline{c}\circ\overline{e}+\overline{c}\circ\overline{f}=0 \qquad (1)$$

and if the inner product of their $\mathbb{F}_4$-components $\left(\overline{a}+\overline{c}+\left(\overline{b}+\overline{c}\right)u\right)\circ\left(\overline{d}+\overline{f}+\left(\overline{e}+\overline{f}\right)u\right)$ is free of u we have $\overline{a}\circ\overline{e}+\overline{a}\circ\overline{f}+\overline{b}\circ\overline{d}+\overline{b}\circ\overline{f}+\overline{c}\circ\overline{d}+\overline{c}\circ\overline{e}=0$, which implies $\overline{a}\circ\overline{d}+\overline{b}\circ\overline{e}+\overline{c}\circ\overline{f}=0$ by (1). Hence $\varphi\left(\overline{x}\right)\circ\varphi\left(\overline{y}\right)=0$. □

We would like to determine when the Gray image of a code is self-dual. Much like ring elements and vectors, a matrix G over R can also be expressed as

$$\begin{aligned}G&=G_1+uG_2+u^2G_3\\&=\left(1+u+u^2\right)\left(G_1+G_2+G_3\right)+\left(u+u^2\right)\left(G_1+G_3+\left(G_2+G_3\right)u\right)\end{aligned}$$

where $G_1,\ G_2$ and G_3 are binary matrices. $G_1+G_2+G_3$ is called $\mathbb{F}_2$-component of G and denoted by $G_{\mathbb{F}_2}$ and $G_1+G_3+\left(G_2+G_3\right)u$ is called $\mathbb{F}_4$-component of G and denoted by $G_{\mathbb{F}_4}$.

The following theorem characterizes codes over the ring R with self-orthogonal binary images:

Theorem 3.5. *Let $\mathcal{C}$ be the code generated by G over the ring R. Then $\varphi\left(\mathcal{C}\right)$ is a self-orthogonal binary code if $G_{\mathbb{F}_2}G_{\mathbb{F}_2}^T=0$ and $G_{\mathbb{F}_4}G_{\mathbb{F}_4}^T$ and $G_{\mathbb{F}_4}\left(uG\right)_{\mathbb{F}_4}^T$ are matrices over the ring R which are free of u.*

Proof. Let $G=G_1+uG_2+u^2G_3$ then $G_{\mathbb{F}_2}G_{\mathbb{F}_2}^T=0$ implies

$$\left(G_1+G_2+G_3\right)\left(G_1^T+G_2^T+G_3^T\right)=0. \qquad (2)$$

The matrix $G_{\mathbb{F}_4}G_{\mathbb{F}_4}^T=\left(G_1+G_3+\left(G_2+G_3\right)u\right)\left(G_1^T+G_3^T+\left(G_2^T+G_3^T\right)u\right)$ is free of u implies

$$G_1G_2^T+G_1G_3^T+G_3G_2^T+G_2G_1^T+G_2G_3^T+G_3G_1^T=0$$

then this together with equation (2) implies

$$G_1G_1^T+G_2G_2^T+G_3G_3^T=0. \qquad (3)$$

Similarly, if $G_{\mathbb{F}_4}(uG)_{\mathbb{F}_4}^T = (G_1+G_3+(G_2+G_3)u)\left(G_3^T+G_2^T+\left(G_1^T+G_2^T\right)u\right)$ is free of u then we have $G_1G_1^T+G_1G_2^T+G_3G_1^T+G_2G_3^T+G_2G_2^T+G_3G_3^T=0$ then this together with equation (3) gives

$$G_1G_2^T+G_3G_1^T+G_2G_3^T=0. \tag{4}$$

Now consider the Gray image $\varphi(\mathcal{C})$ of $\mathcal{C}$ which is generated by

$$G^*=\begin{pmatrix}\varphi(G)\\ \varphi(uG)\\ \varphi\left(u^2G\right)\end{pmatrix}=\begin{pmatrix}G_1 & G_2 & G_3\\ G_3 & G_1 & G_2\\ G_2 & G_3 & G_1\end{pmatrix}.$$

By equations (3) and (4) we have $G^*\left(G^*\right)^T=0$ which implies $\varphi(\mathcal{C})$ is a self-orthogonal binary code. □

Example 3.6. *The code generated by the matrix*

$$G=\begin{pmatrix}1 & 0 & 1+u & u\\ 0 & 1 & u & 1+u\end{pmatrix}$$

is a free self-dual code over the ring R but its Gray image is not self-dual. We may easily observe that $G_{\mathbb{F}_2}=\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}$ and it generates a binary self-dual code. On the other hand, $G_{\mathbb{F}_4}=G$ and $(uG)_{\mathbb{F}_4}=\begin{pmatrix}u&0&1&1+u\\0&u&1+u&1\end{pmatrix}$. The matrix $G_{\mathbb{F}_4}(uG)_{\mathbb{F}_4}^T=\begin{pmatrix}1+u+u^2&1+u+u^2\\1+u+u^2&1+u+u^2\end{pmatrix}$ is not free of u.

If $\mathcal{C}$ is self-orthogonal over the ring R then some of the conditions of Theorem 3.5 may be relaxed.

Lemma 3.7. *Let $\mathcal{C}$ be a self-orthogonal code over the ring R and G be a generator matrix of $\mathcal{C}$. Then $\varphi(\mathcal{C})$ is a binary self-orthogonal code if $G_{\mathbb{F}_4}G_{\mathbb{F}_4}^T$ and $G_{\mathbb{F}_4}(uG)_{\mathbb{F}_4}^T$ are free of u.*

Proof. Let $G=\left(1+u+u^2\right)G_{\mathbb{F}_2}+\left(u+u^2\right)G_{\mathbb{F}_4}$ be a generator matrix for a self-orthogonal code over R. Then $GG^T=0$ which implies $G_{\mathbb{F}_2}G_{\mathbb{F}_2}^T=0$. The result follows by Theorem 3.5. □

An immediate consequence of Lemma 3.7 is;

Lemma 3.8. *Let G be a generator matrix of a self-dual code $\mathcal{C}$ over the ring R. Then $\varphi(\mathcal{C})$ is a binary self-dual code if $G_{\mathbb{F}_4}G_{\mathbb{F}_4}^T$ and $G_{\mathbb{F}_4}(uG)_{\mathbb{F}_4}^T$ are free of u.*

Lemma 3.9. *A self-orthogonal code $\mathcal{C}$ over the ring R is an even code.*

Proof. Let $\mathcal{C}$ be a self-orthogonal code of length n over the ring R and $\overline{x}$ be an arbitrary codeword in $\mathcal{C}$. Let $\overline{x}=\overline{a}+\overline{b}u+\overline{c}u^2$ where $\overline{a},\overline{b}$ and $\overline{c}\in\mathbb{F}_2^n$ then $\overline{x}\circ\overline{x}=\overline{a}\circ\overline{a}+(\overline{c}\circ\overline{c})u+\left(\overline{b}\circ\overline{b}\right)u^2=0$ implies $\overline{a}\circ\overline{a}=0=\overline{b}\circ\overline{b}=\overline{c}\circ\overline{c}$. Then, $wt_H(\overline{a})$, $wt_H\left(\overline{b}\right)$ and $wt_H(\overline{c})$ are even since a self-orthogonal binary vector has even weight. Hence, $wt_L(\overline{x})=wt_H(\overline{a})+wt_H\left(\overline{b}\right)+wt_H(\overline{c})$ is even. □

We define a projection $\pi:R\to\mathbb{F}_2$ as;

$$\pi(r)=\begin{cases}1 & \text{if } r \text{ is odd}\\ 0 & \text{if } r \text{ is even.}\end{cases}$$

The projection π is extended componentwise and denoted by Π. For a matrix G over the ring R the projection of the matrix is its $\mathbb{F}_2$-component; $\Pi(G)=G_{\mathbb{F}_2}$.

Moreover, π is a ring homomorphism. So, the following result follows;

Lemma 3.10. *Let $\mathcal{C}$ be a linear code over the ring R generated by matrix G then $\mathcal{C}$ is an even code if the rows of G are even.*

Definition 3.11. *Let $\mathcal{C}$ be a code of length n over the ring R. The code $\mathcal{C}$ is said to be a lift of the binary code $\mathcal{D}$ if $\Pi(\mathcal{C}) = \mathcal{D}$. The code $\mathcal{D}$ is called the projection of $\mathcal{C}$.*

Note that the projection of a self-dual code is a binary self-orthogonal code. On the other hand a lift of a self-dual code may not be self-dual. In the following example we construct the extended binary Golay code as a lift of the $[8,4,4]_2$ extended Hamming code.

Example 3.12. *Take the following generator matrix of the $[8,4,4]_2$ extended Hamming code*

$$G = \left(\begin{array}{c|cccc} I_4 & \begin{matrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{matrix} \end{array}\right).$$

We lift G to a matrix G^* over the ring R by keeping I_4 as it is and lifting 0 to an even element and 1 to an odd element. Let $\mathcal{C}^*$ be the code generated by

$$G^* = \left(\begin{array}{c|cccc} I_4 & \begin{matrix}u+u^2 & 1+u+u^2 & 1 & 1\\ 1 & u+u^2 & 1+u+u^2 & 1\\ 1 & 1 & u+u^2 & 1+u+u^2\\ 1+u+u^2 & 1 & 1 & u+u^2\end{matrix} \end{array}\right).$$

$G^*_{\mathbb{F}_2} = G$ and

$$G^*_{\mathbb{F}_4} = \left(\begin{array}{c|cccc} I_4 & \begin{matrix}1&0&1&1\\1&1&0&1\\1&1&1&0\\0&1&1&1\end{matrix} \end{array}\right), \quad (uG)^*_{\mathbb{F}_4} = \left(\begin{array}{c|cccc} uI_4 & \begin{matrix}1+u&0&u&u\\u&1+u&0&u\\u&u&1+u&0\\0&u&u&1+u\end{matrix} \end{array}\right)$$

$GG^T = 0$ and $G^*_{\mathbb{F}_4}\left(uG^*_{\mathbb{F}_4}\right)^T$ is 4×4 circulant matrix with first row $(1,0,1,1)$ and hence is free of u. Thus by Theorem 3.5 $\varphi(\mathcal{C}^*)$ is self-dual, which turns out to be the $[24,12,8]_2$ extended binary Golay code.

Example 3.13. *The binary code generated by $G = (I_8 \mid A)$ where A is the circulant matrix with first row $r_A = (0,1,0,0,0,1,0,1)$ is a self-dual $[16,8,4]_2$-code. Consider a lift*

$$r_{A'} = \left(1+u, u^2, u+u^2, 1+u, 0, 1+u+u^2, u+u^2, 1+u+u^2\right)$$

of r_A. Then the code generated by $G' = (I_8 \mid A')$ where A' is the circulant matrix with first row $r_{A'}$ has a self-dual binary image that is the unique self-dual $[48,24,12]_2$-code.

Example 3.14. *The double circulant binary code generated by $G = (I_{11} \mid A)$ where A is the 11×11 circulant matrix with first row $r_A = (1,1,1,0,0,0,1,0,0,1,0)$ is a self-dual $[22,11,6]_2$-code. Let*

$$r_{A'} = \left(1,1,1,1+u^2,1+u^2,1+u^2,1,1+u^2,u+u^2,1,1+u^2\right)$$

be a lift of r_A and $\mathcal{C}$ be the code over the ring R generated by $G' = (I_{11} \mid A')$ where A' is the circulant matrix with first row $r_{A'}$. The binary image $\varphi(\mathcal{C})$ of $\mathcal{C}$ which we denote by $\mathcal{C}_{66,0}$ is an extremal self-dual binary code of lengh 66.

4. Quadratic Double Circulant codes over R

In this section, we consider QDC codes over the ring R and obtain families of codes which satisfy duality conditions given in Theorem 3.5. Therefore we obtain self-dual binary codes as Gray images of codes over the ring R. In particular, some extremal self-dual $[66,33,12]_2$-codes are reconstructed.

Theorem 4.1. *Let $p \equiv 3 \pmod 8$ be an odd prime. Then $\mathcal{P}_p\left(0, 1+u^2, 1+u+u^2\right)$ and $\mathcal{P}_p\left(1+u^2, u, 1+u\right)$ are codes over the ring R with self-dual binary images.*

Proof. A generator matrix of $\mathcal{P}_p\left(0, 1+u^2, 1+u+u^2\right)$ is given by

$$G = \left(I_p \,|\, Q_p\left(0, 1+u^2, 1+u+u^2\right) \right).$$

Then $G_{\mathbb{F}_2} = \left(I_p \,|\, Q_p\left(0,0,1\right) \right)$ and by Theorem 2.3 we have

$$Q_p\left(0,0,1\right) Q_p\left(0,0,1\right)^T = Q_p\left(1,0,0\right) = I_p.$$

So $G_{\mathbb{F}_2}\left(G_{\mathbb{F}_2}\right)^T = 0$. Analogously, $G_{\mathbb{F}_4} = \left(I_p \,|\, Q_p\left(0,u,0\right) \right)$ by Theorem 2.3 we have

$$Q_p\left(0,u,0\right) Q_p\left(0,u,0\right)^T = Q_p\left(u^2,0,0\right) = u^2 I_p.$$

Therefore, $G_{\mathbb{F}_4}\left(G_{\mathbb{F}_4}\right)^T = \left(1+u^2\right) I_p$ which is free of u. Now, we need to show that $G_{\mathbb{F}_4}\left(uG\right)_{\mathbb{F}_4}^T$ is also free of u where $\left(uG\right)_{\mathbb{F}_4} = \left(uI_p \,|\, Q_p\left(0,1+u,0\right) \right)$. We have

$$\begin{aligned} Q_p\left(0,u,0\right) Q_p\left(0,1+u,0\right)^T &= uQ_p\left(0,1,0\right)\left(1+u\right) Q_p\left(0,1,0\right) \\ &= \left(u+u^2\right) I_p \text{ by Theorem 2.3,} \end{aligned}$$

which implies $G_{\mathbb{F}_4}\left(uG\right)_{\mathbb{F}_4}^T = uI_p + \left(u+u^2\right) I_p = u^2 I_p$ which is free of u. Hence, by Theorem 3.5 the binary image of $\mathcal{P}_p\left(0, 1+u^2, 1+u+u^2\right)$ is self-orthogonal. Since $\left|\mathcal{P}_p\left(0, 1+u^2, 1+u+u^2\right)\right| = 8^p$ it has a self-dual binary image. The same can be done for $\mathcal{P}_p\left(1+u^2, u, 1+u\right)$. □

Theorem 4.2. *Let p be a prime with $p \equiv 3 \pmod 8$. Then the code*

$$\mathcal{B}_p\left(1, u+u^2, 1+u+u^2 \mid 0,1,1\right)$$

is a self-dual code over the ring R and its Gray image is a binary self-dual Type II code.

Proof. Let b_i denote the i-th row of the matrix

$$G = B_p\left(1, u+u^2, 1+u+u^2 \mid 0,1,1\right) = \left(\begin{array}{c|cc} I_{p+1} & \begin{matrix} 0 \\ \mathbf{1}^T \end{matrix} & \begin{matrix} \mathbf{1} \\ Q_p\left(1, u+u^2, 1+u+u^2\right) \end{matrix} \end{array} \right).$$

Then $b_1 \circ b_1 = 0$ since p is odd. If $p = 8k+3$ then for $2 \le i \le p+1$ we have

$$b_1 \circ b_i = 1 + \frac{p-1}{2}\left(u+u^2\right) + \frac{p-1}{2}\left(1+u+u^2\right) = 1 + (4k+1) = 0.$$

So by Theorem 2.3 we have

$$\begin{aligned} & Q_p\left(1, u+u^2, 1+u+u^2\right) Q_p\left(1, u+u^2, 1+u+u^2\right)^T \\ = \; & Q_p\left(1+u+u^2+1+u+u^2, u+u^2+1+u+u^2+0, u+u^2+1+u+u^2+0\right) \\ = \; & Q_p\left(0,1,1\right), \end{aligned}$$

which implies $b_i \circ b_j = 0$ for $2 \le i \le j \le q+1$. Hence the code is self-dual. On the other hand, the binary code generated by $G_{\mathbb{F}_2} = \Pi\left(G\right) = B_p\left(1,0,1 \mid 0,1,1\right)$ generates a self-dual binary code since $Q_p\left(1,0,1\right) Q_p\left(1,0,1\right)^T = Q_p\left(0,1,1\right)$. So, $G_{\mathbb{F}_2}\left(G_{\mathbb{F}_2}\right)^T = 0$. $G_{\mathbb{F}_4} = B_p\left(1,1,0 \mid 0,1,1\right)$ is a binary matrix and moreover $G_{\mathbb{F}_4}\left(G_{\mathbb{F}_4}\right)^T = 0$ since $Q_p\left(1,1,0\right) Q_p\left(1,1,0\right)^T = Q_p\left(0,1,1\right)$.

$$\left(uG\right)_{\mathbb{F}_4} = \left(\begin{array}{c|cc} uI_{p+1} & \begin{matrix} 0 \\ u\mathbf{1}^T \end{matrix} & \begin{matrix} u\mathbf{1} \\ Q_p\left(u,u,0\right) \end{matrix} \end{array} \right) = u\left(G_{\mathbb{F}_4}\right)$$

and $G_{\mathbb{F}_4}\left(uG\right)_{\mathbb{F}_4}^T = uG_{\mathbb{F}_4}\left(G_{\mathbb{F}_4}\right)^T = u0 = 0$. Hence by Theorem 3.5 the binary image of the code is self-dual. In addition, $wt\left(b_1\right) = 8k+4$ and $wt\left(b_i\right) = 3 + (4k+1)\,2 + (4k+1)\,3 = 20k+8$ for $2 \le i \le q+1$ which implies that the Gray image is Type II. □

An extremal self-dual binary code of length 66 has a weight enumerator in one of the following forms ([2]):

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

Recently, 24 new codes in $W_{66,3}$ are constructed in [6]. For a list of known codes we refer to [6] and references therein. The code $\mathcal{C}_{66,0}$ in Example 3.14 has weight enumerator $\beta=0$ in $W_{66,1}$. We complete this section by giving some examples of QDC codes over the ring R in Table 1. The binary images of two of the codes are extremal self-dual binary codes with weight enumerators $\beta=0$ and 66 in $W_{66,1}$.

Table 1. Examples of quadratic double circulant codes over the ring R

p	Code over R	Gray image	remark
3	$\mathcal{P}_3\left(1+u^2,u,1+u\right)$	$[18,9,4]_2$	
3	$\mathcal{P}_3\left(0,1+u^2,1+u+u^2\right)$	$[18,9,4]_2$	
3	$\mathcal{B}_3\left(0,u,1+u^2\mid 1+u+u^2,1+u,1+u\right)$	$[24,12,6]_2$	
11	$\mathcal{P}_{11}\left(1+u^2,u,1+u\right)$	$[66,33,12]_2$	$\beta=0$ in $W_{66,1}$
11	$\mathcal{P}_{11}\left(0,1+u^2,1+u+u^2\right)$	$[66,33,12]_2$	$\beta=66$ in $W_{66,1}$
11	$\mathcal{B}_{11}\left(1,u+u^2,1+u+u^2\mid 0,1,1\right)$	$[72,36,12]_2$	Type II
19	$\mathcal{P}_{19}\left(1+u^2,u,1+u\right)$	$[114,57,16]_2$	
19	$\mathcal{P}_{19}\left(0,1+u^2,1+u+u^2\right)$	$[114,57,16]_2$	
19	$\mathcal{B}_{19}\left(1,u+u^2,1+u+u^2\mid 0,1,1\right)$	$[120,60,16]_2$	Type II

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

An efficient method to construct self-dual binary codes of length $n+2$ is to extend a self-dual binary code of length n. Such an extension method for an arbitrary generator matrix of the code is used in [5]. Such extension methods for binary rings are introduced in [8] and a substantial number of new extremal binary self-dual codes of length 68 are obtained. In this section, extension is used for extremal self-dual binary codes of length 66 which were constructed in sections 3 and 4. As a result, we were able to obtain eight extremal self-dual binary codes of length 68 with new weight enumerators.

The weight enumerator of an extremal binary self-dual code of length 68 is characterized in [2] as follows:

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

where $0\le\gamma\le 11$ and $14\gamma\le\beta\le 1870-32\gamma$. Tsai et al. constructed new extremal self-dual binary codes of lengths 66 and 68 in [10]. Together with the codes obtained in [10] the existence of codes in $W_{68,1}$ are known for β =104, 122, 125,...,132, 134,...,168, 170,...,232, 234, 235, 236, 241, 255, 257,...,269, 302, 328,..., 336, 338, 339, 345, 347, 355, 401. We construct codes with weight enumerators β =117, 120 and 133 in $W_{68,1}$ which are listed in Table 2. Recently, new codes in $W_{68,2}$ are obtained in [6, 8] together

with these, codes exists for $W_{68,2}$ when

$$\begin{aligned}
\gamma &= 0,\ \beta = 44,\ldots,154 \text{ or } \beta \in \{2m | m = 17,\ 20,\ 88,\ 102,\ 119,\ 136 \text{ or } 78 \leq m \leq 86\};\\
\gamma &= 1,\ \beta = 60,\ldots,160 \text{ or } \beta \in \{2m | m = 27,\ 28,\ 29,\ 95,\ 96 \text{ or } 81 \leq m \leq 89\};\\
\gamma &= 2,\ \beta = 65,68,71,77,159 \text{ or } \beta \in \{2m | 37 \leq m \leq 68,\ 70 \leq m \leq 81\} \text{ or}\\
\beta &\in \{2m+1 | 42 \leq m \leq 69,\ 71 \leq m \leq 77\};\\
\gamma &= 3,\ \beta = 101,117,123,127,133,137,141,145,147,149,153,159,193 \text{ or}\\
\beta &\in \{2m | m = 44,45,48,50,51,52,54,\ldots,58,61,63,\ldots,66,68,\ldots,72,74,77,\ldots,81,88,94,98\};\\
\gamma &= 4,\ \beta \in \{2m | m = 51,\ 55,\ 58,\ 60,\ 61,\ 62,\ 64,\ 65,\ 67,\ldots,71,\ 75,\ldots,\ 78,\ 80\} \text{ and}\\
\gamma &= 6 \text{ with } \beta \in \{2m | m = 69,\ 77,\ 78,\ 79,\ 81,\ 88\}.
\end{aligned}$$

We construct codes with weight enumerators $\gamma = 1$ and β =49, 57, 59, 67, 69, 71 and codes with weight enumerators $\gamma = 2$ and β =69, 81 in $W_{68,2}$ that are given in Table 3 and Example 5.2.

The following is an extension theorem that is true for all commutative rings A of characteristic 2.

Theorem 5.1. *([8]) Let $\mathcal{C}$ be a self-dual code over A of length n and $G = (r_i)$ be a $k \times n$ generator matrix for $\mathcal{C}$, where r_i is the i-th row of G, $1 \leq i \leq k$. Let c be a unit in A such that $c^2 = 1$ and X be a vector in A^n with $X \circ X = 1$. Let $y_i = r_i \circ X$ for $1 \leq i \leq k$. Then the following matrix*

$$G^* = \left(\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array}\right),$$

generates a self-dual code $\mathcal{C}^*$ over A of length $n+2$.

Example 5.2. *When we apply the extension in Theorem 5.1 to $\mathcal{C}_{66,0}$ in Example 3.14 with*

$$X = (000101000011111010001111011100110101001110001101101011001111111111)$$

in other words, when we consider the code generated by

$$\left(\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & y_1 & \\ \vdots & \vdots & \varphi(G') \\ y_{33} & y_{33} & \end{array}\right)$$

we obtain an extremal binary self-dual code of length 68 with an automorphism group of order 10 and weight enumerator $\gamma = 1$, $\beta = 49$ in $W_{68,2}$. Note that this is the first extremal binary self-dual code with this weight enumerator.

In a similar way, the extension is applied to the Gray image of $\mathcal{P}_{11}\left(1+u^2, u, 1+u\right)$ in Table 1 and seven new extremal self-dual binary codes of length 68 are obtained. These are listed in tables 2 and 3.

Remark 5.3. *Recently, in [6] by using a different method codes with weight enumerators $\gamma = 1$ and $\beta = 67, 69, 71$ in $W_{68,2}$ are constructed for the first time in literature. Since the method used here is different we list them in Table 3.*

6. Conclusion

In this work, we applied the quadratic double and bordered double circulant constructions over the ring $R := \mathbb{F}_2[u]/\left(u^3 - 1\right)$ to obtain extremal binary self-dual codes. Applying extension theorems to the

Table 2. **Extremal binary self-dual codes in $W_{68,1}$ as extensions of $\varphi\left(\mathcal{P}_{11}\left(1+u^2, u, 1+u\right)\right)$**

X	β
01101101101101100100111010011100010000011001000001000000011100111	117
01101100100101100001010111101110111101010101101101011010100011111011	120
01110000000101000000000111101110111100101111101010000110010111010 0	133

Table 3. **Extremal binary self-dual codes in $W_{68,2}$ as extensions of $\varphi\left(\mathcal{P}_{11}\left(1+u^2, u, 1+u\right)\right)$**

X	γ	β
10001001010100010111001101111110010110000000000101101000001001111 11	1	57
00001000100110010101111111010001100011000100101111111110110111100 01	1	59
00101011100100111111101001010010001010100000101011010101010100 1010	1	67
00110010101001111011011100100000011110111010011110010111010100 1111	1	69
11100000001010000101000010100110111010101110011011001110111000 1100	1	71
10001010110001100001100110110010010111011010111100101111100110 1001	2	69
00011100001010110110111111001000100010001101001011010110110011 0101	2	81

extremal self-dual binary codes of length 66 obtained from the ring R we were able to find eight new extremal self-dual binary codes of length 68 updating the list of all known such codes. The methods we have used have proven to be useful in many works in the literature of self-dual codes. We believe they could be applied to other rings and structures such as $\mathbb{Z}_4$.

Acknowledgements

The authors would like to thank Prof. İrfan Şiap for his suggestions and the anonymous referees for their remarks which improved the manuscript considerably.

References

[1] J. H. Conway, N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory, 36(6), 1319-1333, 1990.
[2] S. T. Dougherty, T. A. Gulliver, M., Harada, *Extremal binary self dual codes*, IEEE Trans. Inform. Theory, 43(6), 2036-2047, 1997.
[3] P. Gaborit, *Quadratic double circulant codes over fields*, Journal of Combinatorial Theory Series A, 97(1), 85-107, 2002.
[4] W.C. Huffman, V. Pless, *Fundamentals of error correcting codes*, Cambridge University press, 2003.
[5] J.-L. Kim, *New extremal self-dual codes of lengths* $36, 38$ *and* 58, IEEE Trans. Inf. Theory, 47(1), 386-393, 2001.
[6] A. Kaya, B. Yildiz, İ. Şiap, *New extremal binary self-dual codes from* $\mathbb{F}_4 + u\mathbb{F}_4$*-lifts of quadratic*

double circulant codes over $\mathbb{F}_4$, available online at http://arxiv.org/abs/1405.7147

[7] A. Kaya, B. Yildiz, *Binary generator matrices of new extremal self-dual binary codes of length 68*, available online at http://www.fatih.edu.tr/~akaya/binary/68u31.txt

[8] A. Kaya, B. Yildiz, *Extension theorems for self-dual codes over rings and new binary self-dual codes*, available online at http://arxiv.org/abs/1404.0195.

[9] E. M. Rains, *Shadow Bounds for Self Dual Codes*, IEEE Trans. Inf. Theory, 44(1), 134-139, 1998.

[10] H.-P. Tsai, P.-Y. Shih, R.-Y. Wuh, W.-K. Su, C.-H. Chen, *Construction of self-dual codes*, IEEE Trans. Inform. Theory, 54(8), 3826-3831, 2008.