Filomat 28:5 (2014), 937–945
DOI 10.2298/FIL1405937K

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Extremal Binary Self-Dual Codes of Lengths 64 and 66 from Four-Circulant Constructions over $\mathbb{F}_2 + u\mathbb{F}_2$

Suat Karadeniz[a], Bahattin Yildiz[a], Nuh Aydin[b]

[a]*Fatih University, Istanbul-TURKEY*
[b]*Kenyon College, Gambier, OH, USA*

Abstract. A classification of all four-circulant extremal codes of length 32 over $\mathbb{F}_2 + u\mathbb{F}_2$ is done by using four-circulant binary self-dual codes of length 32 of minimum weights 6 and 8. As Gray images of these codes, a substantial number of extremal binary self-dual codes of length 64 are obtained. In particular a new code with $\beta = 80$ in $W_{64,2}$ is found. Then applying an extension method from the literature to extremal self-dual codes of length 64, we have found many extremal binary self-dual codes of length 66. Among those, five of them are new codes in the sense that codes with these weight enumerators are constructed for the first time. These codes have the values $\beta = 1, 30, 34, 84, 94$ in $W_{66,1}$.

1. Introduction

Self-dual codes make up an important research field for coding theorists. They are related to many different areas such as designs, lattice theory, invariant theory and cryptography. Parallel to the growing interest in codes over rings, self-dual codes over rings have also been a topic of interest recently. Especially self-dual codes over the rings of order 4, finite chain rings and Frobenius rings have been studied quite extensively. For some of these works we refer to [6], [5], [23], [13], [15].

Rains, in [19] updated the upper bound for the minimum distance d of an $[n, n/2]$ binary self-dual code. Self-dual codes meeting this bound are called extremal. A great interest for researchers has been in constructing and classifying extremal binary self-dual codes of certain lengths. Conway and Sloane have listed the possible weight enumerators of extremal binary self-dual codes of lengths up to 64 and 72 in [3]. But for many of the possible weight enumerators, the existence of binary self-dual codes is still an open problem. Finding extremal binary self-dual codes with new weight enumerator has been an interesting problem that has generated a lot of interest among researchers.

Different techniques have been used in constructing extremal binary self-dual codes of certain lengths, many of which involve a computer search. Among the techniques used are double-circulant and bordered-double-circulant constructions, using neighboring codes and automorphism groups. For the works in this direction we can refer to [2], [7], [9], [10], [18], [21] among others.

Recently, the authors have found extremal binary codes of new weight enumerators by using self-dual codes over a family of rings of characteristic 2. ([13], [15]).

2010 *Mathematics Subject Classification*. Primary 94B05; Secondary 94B60
Keywords. (Lee weight, Gray maps, extremal self-dual codes, projections, lifts, four-circulant codes)
Received: 03 October 2013; Accepted: 30 January 2014
Communicated by Eberhard Malkowsky
Email addresses: skaradeniz@fatih.edu.tr (Suat Karadeniz), byildiz@fatih.edu.tr (Bahattin Yildiz), aydinn@kenyon.edu (Nuh Aydin)

In this paper, inspired by the four-circulant construction explained in [1] and [9], we first classify all four-circulant extremal self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length 32, using the lifts of four-circulant binary codes of length 32 that have minimum weights 6 and 8. The Gray images of these self-dual codes turn out to be extremal binary self-dual codes of length 64. In particular, we find an extremal binary code of length 64 with $\beta = 80$ in $W_{64,2}$, the existence of which was not known before. Next, we consider extensions of binary images of these extremal self-dual codes to search for new extremal self-dual codes of length 66. Using the extension algorithm given in [16], we have found many such codes. They contain five codes which were not known to exist before. We also obtained four additional codes which were discovered only recently in [14] using a different method.

In section 2, we give some of the preliminaries on the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. In section 3, we classify all four-circulant binary self-dual codes of length 32 of minimum weight 6 and 8. We then lift each of these codes over $\mathbb{F}_2 + u\mathbb{F}_2$ to find extremal self-dual binary codes of length 64. We performed an exhaustive search over all such possible codes and present our results in the form of tables. In section 4, we present the new extremal self-dual binary codes of length 66 obtained by the extension algorithm mentioned above.

2. The Ring $\mathbb{F}_2 + u\mathbb{F}_2$

The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is defined as the ring of characteristic 2 with 4 elements with the restriction $u^2 = 0$. Type II, type IV, self-dual codes and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been studied extensively in [6].

$$\mathbb{F}_2 + u\mathbb{F}_2 = \left\{a + bu \mid a,\ b \in \mathbb{F}_2,\ u^2 = 0\right\},$$

and it is easily seen that $\mathbb{F}_2 + u\mathbb{F}_2 \simeq \mathbb{F}_2[x] / \left(x^2\right)$. We recall that a linear code C of length n over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is an $\mathbb{F}_2 + u\mathbb{F}_2$-submodule of $(\mathbb{F}_2 + u\mathbb{F}_2)^n$. Any linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ is permutation equivalent to a code C with generator matrix

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{bmatrix}$$

where $A,\ B_1,\ B_2$ and D are binary matrices.

We recall that the elements of $\mathbb{F}_2 + u\mathbb{F}_2$ are $0, 1, u, 1 + u$ and their Lee weights are defined as $0, 1, 2, 1$ respectively. The Hamming (d_H) and Lee (d_L) distance between n tuples is then defined as the sum of the Hamming and Lee weights of the difference of the components of these tuples respectively. The smallest positive Hamming and Lee distance of a code C is denoted by $d_H(C)$ and $d_L(C)$ respectively.

A Gray map ϕ is defined as $\phi : (\mathbb{F}_2 + u\mathbb{F}_2)^n \longrightarrow \mathbb{F}_2^{2n}$

$$\phi\left(\overline{a} + \overline{b}u\right) = \left(\overline{b}, \overline{a} + \overline{b}\right) \tag{1}$$

where $\overline{a}, \overline{b}$ in $\mathbb{F}_2^n$. ϕ is a distance preserving isometry from $((\mathbb{F}_2 + u\mathbb{F}_2)^n, d_L)$ to $\left(\mathbb{F}_2^{2n}, d_H\right)$, where d_L and d_H denote the Lee and Hamming distance in $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ and $\mathbb{F}_2^{2n}$ respectively. This means if C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ with parameters $\left[n, 2^k, d\right]$, (here 2^k means the number of the codewords) then $\phi(C)$ is a binary linear code of parameters $[2n, k, d]$.

The dual of the linear code C is denoted by $C^\perp$;

$$C^\perp = \{v \in (\mathbb{F}_2 + u\mathbb{F}_2)^n : \langle \overline{c}, v\rangle = 0, \forall \overline{c} \in C\}.$$

where $\langle , \rangle$ denotes the standard Euclidean inner product in $(\mathbb{F}_2 + u\mathbb{F}_2)^n$.

The following theorem is a natural result of the Gray map:

Theorem 2.1. *If C is a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length n, then $\phi(C)$ is a self-dual binary code of length $2n$.*

We can also define a natural projection from $\mathbb{F}_2 + u\mathbb{F}_2$ to $\mathbb{F}_2$ a follows

$$\mu : \mathbb{F}_2 + u\mathbb{F}_2 \to \mathbb{F}_2, \quad \mu(a + bu) = a. \tag{2}$$

If $D = \mu(C)$ for some linear code C over $\mathbb{F}_2 + u\mathbb{F}_2$, we say D is a *projection* of C into $\mathbb{F}_2$, and that C is a *lift* of D into $\mathbb{F}_2 + u\mathbb{F}_2$.

It is clear that the projection of a self-orthogonal code is self-orthogonal, but the projection of a self-dual code need not be self-dual. For example the code of length 1 generated by u is self-dual over $\mathbb{F}_2 + u\mathbb{F}_2$ but its projection is the zero code. However, when C has a special type of generator matrix, the assertion is true:

Theorem 2.2. *Suppose that C is a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $2n$, generated by the matrix $[I_n|A]$, where I_n is the $n \times n$ identity matrix. Then $\mu(C)$ is a self-dual binary code of length $2n$.*

We finish this section with the following useful theorem that will have an impact on our search:

Theorem 2.3. *Suppose C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ and that $C' = \mu(C)$ is its projection to $\mathbb{F}_2$. With d and d' representing the minimum Lee and Hamming distances of C and C' respectively, we have $d \le 2d'$.*

Proof. Suppose $\overline{x} \in C'$ with $w_H(\overline{x}) = d'$. Now since $C' = \mu(C)$, there exists $\overline{y} \in C$ such that $\overline{x} + u\overline{y} \in C$. However, C is linear over $\mathbb{F}_2 + u\mathbb{F}_2$, which means $u(\overline{x} + u\overline{y}) = u\overline{x} \in C$. Then we have $w_L(u\overline{x}) = w_H(\overline{x}, \overline{x}) = 2d'$. This completes the proof. □

3. Extremal Self-Dual Codes of Length 64 from Lifts of Binary Four-Circulant Codes

Inspired by orthogonal designs, Betsumiya et al. introduced the following construction for self-dual codes over a prime field in [1]: Let M be a matrix over $\mathbb{F}_p$ of the form

$$M = \left[I_{2n} \;\middle|\; \begin{matrix} A & B \\ -B^T & -A^T \end{matrix} \right] \tag{3}$$

where A and B are $n \times n$ circulant matrices that satisfy $AA^T + BB^T = aI_n$ for some $a \in \mathbb{F}_p$. They proved that if $1 + a = 0$, then the matrix M generates a self-dual code over $\mathbb{F}_p$. This construction, which was called the two-block circulant construction in [8], was also called the four-circulant construction in [9]. When applied in the binary field, the matrix simply becomes

$$M = \left[I_{2n} \;\middle|\; \begin{matrix} A & B \\ B^T & A^T \end{matrix} \right] \tag{4}$$

with A, B being $n \times n$ binary circulant matrices that satisfy $AA^T + BB^T = I_n$.

The four-circulant construction can easily be extended to the ring $\mathbb{F}_2 + u\mathbb{F}_2$:

Theorem 3.1. *Let C be the linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $4n$ generated by the four-circulant matrix*

$$G := \left[I_{2n} \;\middle|\; \begin{matrix} A & B \\ B^T & A^T \end{matrix} \right]$$

where A and B are circulant $n \times n$ matrices over $\mathbb{F}_2 + u\mathbb{F}_2$ satisfying $AA^T + BB^T = I_n$. Then C is self-dual.

Proof. Since $|C| = |C^T|$, we just need to prove self-orthogonality. For that it is enough to show that every row of G is orthogonal to every other row of G.

Now suppose $1 \le i, j \le n$. Then $\langle G_i, G_j \rangle = \delta_{ij} + \langle A_i, A_j \rangle + \langle B_i, B_j \rangle$, where δ_{ij} is the Kroenecker delta function. Now, $\langle A_i, A_j \rangle$ is the (i, j)-entry of AA^T, and similarly for the second part. Thus, $\langle A_i, A_j \rangle + \langle B_i, B_j \rangle$ is the (i, j)-entry of $AA^T + BB^T = I_n$ which is again δ_{ij}. Since the characteristic of the ring is 2, we get $\langle G_i, G_j \rangle = \delta_{ij} + \delta_{ij} = 0$.

In exactly the same way it can be proved that $\langle G_i, G_j \rangle = 0$ when $n + 1 \le i, j \le 2n$.

We are left with the case when $1 \le i \le n$ and $n + 1 \le j \le 2n$. In that case $\langle G_i, G_j \rangle = \langle A_i, B_j^T \rangle + \langle B_i, A_j^T \rangle$. But $\langle A_i, B_j^T \rangle + \langle B_i, A_j^T \rangle$ is the (i, j)-entry of $AB + BA = AB + AB = 0$ in $\mathbb{F}_2 + u\mathbb{F}_2$, because it is well known that circulant matrices commute. □

Our first goal is to find all four-circulant extremal self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length 32. Note that the projection of such a code will be a four-circulant binary linear code of length 32. We will then take the Gray images of the codes over $\mathbb{F}_2 + u\mathbb{F}_2$ to obtain extremal self-dual binary codes of length 64. But recall that an extremal self-dual binary code of length 64 has minimum distance 12. Thus, in light of Theorem 2.3, and the observation above, we need to lift four-circulant binary codes of parameters $[32, 16, 8]$ or $[32, 16, 6]$. An exhaustive search over all possible four-circulant binary codes of length 32 result in the four non-equivalent codes given in the table below. We label these codes by C_1, C_2, C_3, C_4 with their respective generator matrices M_1, M_2, M_3, M_4. Since M_i are of the form (4), where A_i and B_i are the 8×8 circulant parts, we just need the first rows of A_i and B_i to determine the matrix M_i.

Table 1: The four-circulant codes of length 32

i	First row of A_i	First row of B_i	Parameters of C_i	$\lvert Aut(C)\rvert$
1	$(0,0,0,0,0,1,0,1)$	$(0,0,0,1,1,1,1,1)$	$[32,16,8]$	$2^{15} \cdot 3^2 \cdot 5 \cdot 7$
2	$(0,0,0,0,0,1,1,1)$	$(0,1,0,1,1,1,1,1)$	$[32,16,8]$	$2^{15} \cdot 3^2$
3	$(0,0,0,0,1,1,1,1)$	$(0,0,0,1,0,0,1,1)$	$[32,16,8]$	$2^5 \cdot 3 \cdot 5 \cdot 31$
4	$(0,0,0,0,1,1,1,1)$	$(0,0,1,1,0,1,1,1)$	$[32,16,6]$	2^5

We then lift these binary codes to $\mathbb{F}_2 + u\mathbb{F}_2$ by lifting the 0's in the first row of A_i and B_i to a non-unit in $\mathbb{F}_2 + u\mathbb{F}_2$ (0 or u) and the 1's to a unit in $\mathbb{F}_2 + u\mathbb{F}_2$ (1 or $1 + u$). We preserve the circulant structure and the identity matrix, thus a typical generating matrix for the lift is of the form

$$G = \left[I_{16} \;\middle|\; \begin{matrix} A & B \\ B^T & A^T \end{matrix} \right]$$

where A and B are 8×8 circulant matrices over $\mathbb{F}_2 + u\mathbb{F}_2$. Since we have a total of $2^8 \times 2^8 = 2^{16}$ possible such lifts for each of the matrices M_i given in the table above, we can conduct an exhaustive search to obtain extremal self-dual codes of length 64. Let us recall that there are two weight types for Type I extremal self-dual codes of length 64 as was described in [3]:

$$W_{64,1} = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \cdots, \quad 14 \le \beta \le 284 \tag{5}$$

and

$$W_{64,2} = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \cdots, \quad 0 \le \beta \le 277, \tag{6}$$

where β is a perameter. The existence of such codes is now known for β = 14, 18, 32, 36, 44, 64 in $W_{64,1}$ and for β = 0, 2, 4, 6, 8, 9, 10, 12, 14, 16, 18, 20, 22, 23, 24, 28, 30, 32, 36, 37, 40, 44, 48, 56, 64, 72, 88, 96, 104, 108, 112, 114, 118, 120, 184 in $W_{64,2}$. In [13], codes with $\beta = 22$ and $\beta = 46$ in $W_{64,1}$ and a code with $\beta = 38$ in $W_{64,2}$ were obtained by using bordered-double-circulant construction and a variation of bordered-double-circulant construction over R_2. In [15], by lifting the extended Hamming code over the ring R_3, we were able to obtain extremal self-dual codes of length 64 with new β values in $W_{64,2}$, namely codes with β = 1, 5, 13, 17, 21, 25, 29, 33, 41, 52.

3.1. *Lifting M_1:*

By exhausting all possible lifts of M_1 to $\mathbb{F}_2 + u\mathbb{F}_2$ we obtain a total of 37 inequivalent extremal self-dual binary codes of length 64. 27 of these codes are Type II codes with partial weight distribution $1 + 2976z^{12} + \cdots$. The remaining ten codes are Type I and we give the first rows of the circulant parts as well as their β values in $W_{64,2}$ and the orders of the automorphism groups in the following table:

Table 2: Extremal self-dual codes of length 64 obtained from lifts of M_1

First row of A_1	First row of B_1	β value in $W_{64,2}$	$\lvert Aut(C)\rvert$
$(0,0,0,0,0,1,u,1+u)$	$(u,u,0,1,1,1,1+u,1+u)$	16	2^7
$(0,u,0,u,0,1,u,1+u)$	$(u,u,0,1,1,1,1+u,1+u)$	16	2^6
$(u,0,0,0,0,1,u,1+u)$	$(0,u,0,1,1,1,1,1+u)$	16	2^5
$(u,u,0,u,0,1,u,1+u)$	$(u,u,u,1,1,1,1,1+u)$	16	2^5
$(u,u,u,u,u,1,0,1+u)$	$(u,u,0,1,1,1,1+u,1+u)$	16	2^6
$(u,u,0,0,u,1,u,1)$	$(u,0,0,1,1,1,1+u,1+u)$	32	2^5
$(u,0,0,u,0,1,u,1)$	$(u,0,u,1,1,1,1,1+u)$	32	2^5
$(u,0,0,0,0,1,u,1+u)$	$(u,u,u,1,1,1,1,1+u)$	32	2^5
$(0,u,0,0,0,1,u,1)$	$(u,0,0,1,1,1+u,1+u,1+u)$	48	2^5
$(u,0,0,0,u,1,u,1+u)$	$(u,u,0,1,1,1+u,1+u,1+u)$	80(New)	2^7

3.2. Lifting M_2:

By searching over all possible lifts of M_2 to $\mathbb{F}_2 + u\mathbb{F}_2$ that are self-dual, we obtain as Gray images, a total of 29 inequivalent extremal self-dual codes of length 64. 24 of these codes are Type II codes with partial weight distribution $1 + 2976z^{12} + \cdots$. The remaining five codes are Type I and we give the first rows of the circulant parts as well as their β values in $W_{64,2}$ and the orders of the automorphism groups in the following table:

Table 3: Extremal self-dual codes of length 64 obtained from lifts of M_2

First row of A_2	First row of B_2	β value in $W_{64,2}$	$\lvert Aut(C)\rvert$
$(u,u,u,u,0,1,1,1)$	$(u,1,u,1,1+u,1+u,1,1+u)$	16	2^5
$(u,0,u,u,0,1,1,1+u)$	$(u,1,0,1+u,1,1+u,1,1+u)$	16	2^5
$(u,0,u,0,0,1,1,1)$	$(0,1,0,1,1+u,1+u,1,1+u)$	16	2^5
$(u,u,u,u,0,1,1,1)$	$(0,1,0,1,1,1+u,1+u,1+u)$	32	2^5
$(u,u,0,u,0,1,1,1)$	$(u,1,0,1+u,1+u,1+u,1+u,1)$	32	2^5

3.3. Lifting M_3:

By searching over all possible lifts of M_3 to $\mathbb{F}_2 + u\mathbb{F}_2$ that are self-dual, we obtain as Gray images, a total of 86 inequivalent extremal self-dual codes of length 64. 68 of these codes are Type II codes with partial weight distribution $1 + 2976z^{12} + \cdots$. The remaining eighteen codes are Type I and we give the first rows of the circulant parts as well as their β values in $W_{64,2}$ and the orders of the automorphism groups in the following table:

Table 4: Extremal self-dual codes of length 64 obtained from lifts of M_3

First row of A_3	First row of B_3	β value in $W_{64,2}$	$\lvert Aut(C)\rvert$
$(u,0,0,0,1,1,1,1)$	$(0,u,0,1,u,0,1+u,1+u)$	0	2^5
$(u,u,u,u,1,1,1,1+u)$	$(u,0,u,1,0,u,1+u,1+u)$	0	2^5
$(u,u,u,0,1,1,1,1)$	$(0,u,0,1,u,0,1+u,1+u)$	0	2^5
$(u,u,0,0,1,1,1,1+u)$	$(0,0,0,1,u,0,1+u,1$	0	2^5
$(u,u,u,0,1,1,1,1)$	$(u,0,u,1,0,0,1+u,1)$	16	2^5
$(u,u,0,u,1,1,1,1)$	$(u,u,u,1,0,u,1+u,1)$	16	2^5
$(u,u,0,0,1,1,1,1+u)$	$(u,0,u,1,0,u,1,1+u)$	16	2^5
$(u,0,u,0,1,1,1+u,1)$	$(u,0,u,1,0,u,1+u,1+u)$	16	2^5
$(u,0,0,u,1,1,1,1+u)$	$(0,0,0,1,u,0,1,1)$	16	2^5
$(u,0,0,0,1,1,1,1)$	$(0,0,u,1,u,0,1+u,1)$	16	2^5
$(0,u,u,0,1,1,1,1+u)$	$(u,u,u,1,0,0,1,1+u)$	16	2^5
$(0,u,0,0,1,1,1,1)$	$(0,u,u,1,u,u,1+u,1)$	16	2^5
$(0,u,0,0,1,1,1+u,1+u)$	$(u,u,u,1,0,u,1,1)$	16	2^5
$(0,0,0,0,1,1,1,1+u)$	$(0,0,u,1,u,u,1+u,1+u)$	16	2^5
$(u,0,0,u,1,1,1,1+u)$	$(u,u,0,1,0,u,1+u,1)$	32	2^5
$(u,0,0,0,1,1,1+u,1+u)$	$(u,u,u,1,0,u,1+u,1)$	32	2^5
$(0,u,u,0,1,1,1,1+u)$	$(0,0,u,1,u,u,1+u,1+u)$	48	2^5

3.4. Lifting M_4:

By searching over all possible lifts of M_4 to $\mathbb{F}_2+u\mathbb{F}_2$ that are self-dual, we obtain as Gray images, a total of 86 inequivalent extremal self-dual codes of length 64. 68 of these codes are Type II codes with partial weight distribution $1+2976z^{12}+\cdots$. The remaining eighteen codes are Type I and we give the first rows of the circulant parts as well as their β values in $W_{64,2}$ and the orders of the automorphism groups in the following table:

Table 5: Extremal self-dual codes of length 64 obtained from lifts of M_4

First row of A_3	First row of B_3	β value in $W_{64,2}$	$\lvert Aut(C)\rvert$
$(u,u,u,u,1,1,1,1+u)$	$(u,u,1,1+u,0,1,1+u,1)$	0	2^5
$(u,0,0,u,1,1,1,1+u)$	$(0,0,1,1,0,1,1+u,1)$	0	2^5
$(u,0,0,0,1,1,1,1)$	$(0,0,1,1+u,u,1,1+u,1)$	0	2^5
$(0,0,0,0,1,1,1,1+u)$	$(u,u,1,1+u,0,1,1+u,1)$	0	2^5
$(u,u,u,0,1,1,1,1)$	$(0,0,1,1+u,u,1,1+u,1)$	0	2^5
$(0,0,0,0,1,1,1,1+u)$	$(u,u,1,1,0,1,1+u,1+u$	16	2^5
$(0,u,0,0,1,1,1,1)$	$(u,u,1,1,u,1+u,1,1+u)$	16	2^5
$(u,0,0,0,1,1,1+u,1+u)$	$(u,u,1,1+u,u,1+u,1,1)$	16	2^5
$(u,0,0,0,1,1,1,1)$	$(0,u,1,1,0,1+u,1,1+u)$	16	2^5
$(u,0,0,u,1,1,1,1+u)$	$(u,u,1,1+u,0,1,1+u,1)$	16	2^5
$(u,0,u,0,1,1,1+u,1)$	$(u,u,1,1+u,0,1,1+u,1)$	16	2^5
$(u,u,0,0,1,1,1+u,1)$	$(0,u,1,1,u,1+u,1+u,1+u)$	16	2^5
$(u,u,0,0,1,1,1,1+u)$	$(0,0,1,1+u,0,1+u,1,1)$	16	2^5
$(u,u,0,u,1,1,1,1)$	$(u,u,1,1+u,u,1+u,1,1)$	16	2^5
$(u,u,u,0,1,1,1,1)$	$(0,0,1,1+u,u,1,1+u,1)$	16	2^5
$(u,u,0,0,1,1,1,1+u)$	$(u,0,1,1+u,u,1,1,1)$	32	2^5
$(0,u,0,0,1,1,1+u,1+u)$	$(u,u,1,1,u,1,1,1+u)$	32	2^5
$(u,u,0,0,1,1,1+u,1)$	$(u,u,1,1,0,1,1+u,1+u)$	48	2^5

4. New Extremal Binary Self-Dual Codes of Length 66

We combined the lifting method of the previous section with the extension algorithm from [16] to search for new extremal binary self-dual codes of length 66. We have been able to construct 5 such codes. Additionally, we found 4 codes that have been recently obtained in [14] from the ring R_3. It is well-known that there are three possibilities for the weight enumerators of extremal self-dual codes of length 66 [4].

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

In [11] and [22] codes were obtained with weight enumerator $W_{66,2}$. A substantial number of codes with weight enumerator $W_{66,1}$ are obtained in [3],[11],[12] and [20]. Codes with weight enumerator $W_{66,3}$ are found by Tsai et al. in [21] for $\beta = 28, 33$ and 34. Most recently, codes with β = 29, 30, 31, 32, 49, 50, 54, 55, 56, 57, 58, 59, 62, 63 and 66 in $W_{66,3}$ and codes with β = 21, 25, 28, 37, 39, 48, 49, 64 and 67 in $W_{66,1}$ are discovered in [14]. In this work, we obtain new extremal binary self-dual codes with β = 1, 30, 34, 84, 94, 25, 28, 39, 48 in $W_{66,1}$. Note that, the last four β values are obtained in [14], whereas the codes with the first five β values, to the best of our knowledge, are obtained for the first time.

We first give the statement of the extension theorem from [16] for the convenience of the reader. We then give the details of the new codes in two tables. Note that to denote the vector x used in the extension theorem stated below, we use an abbreviation in Table 6 and Table 7 for binary strings when a bit appears more than once in consecutive positions. Thus for example, the vector 11010000 is denoted by 1^2010^4.

Theorem 4.1. *[16] Let S be a subset of the set $\{1, 2, \ldots, 2n\}$ of coordinate indices such that $|S|$ is odd. Let $G_0 = [L|R] = [l_i|r_i]$ be a generator matrix (may not be in standard form) of a self-dual code C_0 of length $2n$, where l_i and r_i are rows of L and R, respectively, for $1 \le i \le n$. Let $x = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$ be the characteristic vector of S, i.e., $x_j := 1$ if $j \in S$ and $x_j := 0$ if $j \notin S$ for $1 \le j \le 2n$. Suppose that $y_i := (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) \cdot (l_i|r_i)$ for $1 \le i \le n$. Here $\cdot$ denotes the (scalar) inner product. Then the following matrix:*

$$\left[\begin{array}{cc|cccccc} 1 & 0 & x_1 & \ldots & x_n & x_{n+1} & \ldots & x_{2n} \\ \hline y_1 & y_1 & & & & & & \\ \vdots & \vdots & & L & & & R & \\ y_n & y_n & & & & & & \end{array}\right]$$

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

Table 6: New extremal binary self-dual codes of length 66

Src	First row of A	First row of B	Vector x in 4.1	β in $W_{66,1}$
M_1	$u, u, 0, u, 0, 1, u, 1+u$	$u, u, u, 1, 1, 1, 1, 1+u$	$101^20^81^20^210^810^6$	
			$0^310^41010^510^210^81^30$	30
M_1	$u, 0, 0, 0, u, 1, u, 1+u$	$u, u, 0, 1, 1, 1+u, 1+u, 1+u$	$10^41010^310^21^30^5101^20^310^2$	
			$10^21010^21010^{13}10^4101$	84
M_1	$u, 0, 0, 0, u, 1, u, 1+u$	$u, u, 0, 1, 1, 1+u, 1+u, 1+u$	$0^21^40^31^30^610^210^31^2010^21$	
			$01^201^601^20^710^2101^30^210$	94
M_3	$u, u, u, 0, 1, 1, 1, 1$	$u, 0, u, 1, 0, 0, 1+u, 1$	$1^20^310^4101^201^20^41^{11}$	
			$101^201^201^20101^30^21^20^3101^3010^2$	34
M_4	$u, u, u, u, 1, 1, 1, 1+u$	$u, u, 1, 1+u, 0, 1, 1+u, 1$	$1^70^21^501^20^21^301^201^6$	
			$1^201010^31^80^31^{12}$	1

Table 7: New extremal binary self-dual codes of length 66 recently found by another method

Src	First row of A	First row of B	Vector x in 4.1	β in $W_{66,1}$
M_1	$u, u, 0, u, 0, 1, u, 1+u$	$u, u, u, 1, 1, 1, 1, 1+u$	$0^2 1^2 0 1^2 0 1^2 0101010 10^4 1^2 01010^4$	
			$1^2 0^4 1^3 0^4 1010101 0^3 1^2 0 1^2 0 1^3 0^2 1$	28
M_3	$u, u, u, 0, 1, 1, 1, 1$	$u, 0, u, 1, 0, 0, 1+u, 1$	$1^4 0 1^6 01010 1^3 0 1^2 010 1^3 0 1^3$	
			$1^{17} 0 1^4 010 1^4 0^2 1$	39
M_1	$u, u, u, 0, 1, 1, 1, 1$	$0, u, 0, 1, u, 0, 1+u, 1+u$	$010^4 1010^{14} 10^8$	
			$0^3 10^2 10^3 10^2 1^2 010^4 10^{10}$	25
M_1	$u, u, 0, 0, u, 1, u, 1$	$u, 0, 0, 1, 1, 1, 1+u, 1+u$	$01^2 01^2 01^2 0^2 10^3 1^3 0^2 1^4 0^2 1^4 0^2$	
			$1^4 0^2 1^3 0^3 1^2 0^3 1^2 0^2 1^5 01$	48

5. Conclusion

We first note that what is done for length 32 here can be done for other lengths as well. A four-circulant binary code has length of the form $4k$, thus over $\mathbb{F}_2 + u\mathbb{F}_2$ it will also have length $4k$, meaning that using this idea, we can only obtain binary self-dual codes of lengths divisible by 8. (However, it is possible to obtain codes of lengths of the form $8m \pm 2$ using extension or shortening algorithms on known codes.) Theorem 2.3 gives an important idea about which binary four-circulant codes to lift, thus narrowing the search space considerably.

A rather curious observation is that the β values of all the codes of length 64 we have found are multiples of 16. This could prove to be useful in working out theoretical results for the β values. Another observation is that we get automorphism groups with different sizes only when we use the first generator. With the remaining three generators the automorphism groups all have size 2^5.

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] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada, C. Koukouvinos, On self-dual codes over some prime fields, Discrete Math, 262 (2003) 37–58.
[2] N. Chigira, M. Harada, M. Kitazume, Extremal self-dual codes of length 64 through neighbors and covering radii, Des. Codes Cryptogr., 42 (2007) 93–101.
[3] J. H. Conway, N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inf. Theory, 36 (1990) 1319–1333.
[4] S. T. Dougherty, A. Gulliver, M. Harada, Extremal binary self-dual codes, IEEE Trans. Infrom. Theory, 43 (1997) 2036–2047.
[5] S. T. Dougherty, J. L. Kim, H. Kulosman H. Liu, Self-dual codes over commutative Frobenius rings, Finite Fields Appl., 16 (2010) 14–26.
[6] S. T. Dougherty, P. Gaborit, M. Harada, P.Solé, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Infrom. Theory, 45 (1999) 32–45.
[7] P. Gaborit, A. Otmani, Experimental constructions of self-dual codes, Finite Fields Appl., 9 (2003) 372–394.
[8] S. D. Georgiou, E. Lappas, Self-dual codes from circulant matrices, Des. Codes Cryptogr., 64 (2012) 129–141.
[9] M. Harada, M. Kiermaier, A. Wasserman, R. Yorgova, New Binary Singly even self-dual codes, IEEE Trans. Inf. Theory, 56 (2010) 1612–1617.
[10] M. Harada, T. A. Gulliver, H. Kaneta, Classification of extremal double-circulant self-dual codes of length up to 62, Discrete Math., 188 (1998) 127–136.
[11] M. Harada, T. Nishimura, R. Yorgova, New extremal self-dual codes of length 66, Mathematica Balkanica., 21 (2007) 113–121.
[12] W. C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields Appl., 11 (2005) 451–490.
[13] S.Karadeniz, B.Yildiz, Double-Circulant and Double-Bordered-Circulant constructions for self-dual codes over R_2, Adv. Math. Commun., 6 (2012) 193–202.
[14] S.Karadeniz, B.Yildiz, New extremal binary self-dual codes of length 66 as extensions of self-dual code over R_k, J. Franklin Inst., 350 (2013) 1963–1973.
[15] S. Karadeniz, B. Yildiz, New extremal binary self-dual codes of length 64 as R_3-lifts of the extended binary Hamming code, **in press**, Des. Codes Cryptogr, (2013).

[16] J. L. Kim, New Extremal Self-Dual Codes of Lengths 36, 38 and 58, IEEE Trans. Inf. Theory, 47 (2001) 386–393.
[17] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997) 235-265.
[18] T. Nishimura, A new Extremal Self-dual code of length 64, IEEE Trans. Inf. Theory, 50 (2004) 2173–2174.
[19] E. M. Rains, Shadow Bounds for Self Dual Codes, IEEE Trans. Inf. Theory, 44 (1998) 134–139.
[20] R. Russeva, N. Yankov, On binary self-dual codes of length 69,62,64 and 66 having an automorphism of order 9, Des. Codes Cryptogr., 45 (2007) 335–346.
[21] H. P. Tsai, P. Y. Shih, R. Y. Wuh, W. K. Su, C. H. Chen, Construction of Self-dual codes, IEEE Trans. Inf. Theory, 54 (2008) 3826–3831.
[22] H. P. Tsai, Extremal self-dual codes of length 66 and 68, IEEE Trans. Inf. Theory, 45 (1999) 2129–2133.
[23] B.Yildiz, S.Karadeniz, Self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst., 347 (2010) 1888–1894.