MATHEMATICAL COMMUNICATIONS
Math. Commun. **22**(2017), 123–133

New extremal binary self-dual codes of length 68 via the short Kharaghani array over $\mathbb{F}_2 + u\mathbb{F}_2$

Abidin Kaya*

Department of Computer Engineering, Bursa Orhangazi University, Yildirim Yerleşkesi Mimar Sinan Mah., Mimar Sinan Bulvari E-207, No. 177 TR-16 310 Yildirim/Bursa, Turkey

Received January 29, 2016; accepted September 13, 2016

Abstract. In this paper, new construction methods for self-dual codes are given. The methods use the short Kharaghani array and its variation. They are applicable to any commutative Frobenius ring. We apply the constructions over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and self-dual Type I $[64, 32, 12]_2$-codes with various weight enumerators obtained as Gray images. By using an extension theorem for self-dual codes we were able to construct 27 new extremal binary self-dual codes of length 68. The existence of extremal binary self-dual codes with these weight enumerators was previously unknown.

AMS subject classifications: 94B05, 94B99

Key words: extremal self-dual codes, codes over rings, Gray maps, Kharaghani array, extension theorems

1. Introduction

Self-dual codes constitute an interesting class of codes, especially the ones over the binary field. In [4], an upper bound on the minimum distance of a binary self-dual code is given. This type of codes is related to various topics such as design theory, graph theory and lattice theory. Recently, self-dual codes over rings have been used to construct new codes. For some of the works done in this direction we refer the reader to [6, 9, 12, 13].

The upper bound on the minimum distance of a binary self-dual code is finalized in [16]. Possible weight enumerators of self-dual codes of lengths up to 64 and 72 are listed in [4]. Since then researchers have used different techniques to construct self-dual codes. In [11], Huffman gave a survey on classification of self-dual codes over various alphabets. Construction of new self-dual codes and the classification of self-dual codes have been a dynamic research area. Among those constructions, the ones using circulant matrices are celebrated most. In [5], binary self-dual codes of length 72 are constructed by Hadamard designs, using automorphism groups is another way to build up self-dual codes. For more information we refer to [1, 3, 7, 8, 13].

In this paper, inspired by a four-block circulant construction in [1] that uses the Goethals-Seidel array, we propose a new construction via the short Kharaghani array. A variation of the method is also given. By using the methods for the ring

*Corresponding author. *Email address:* abidinkaya@mail.com (A. Kaya)

$\mathbb{F}_2+u\mathbb{F}_2$ we construct self-dual codes of length 32. As binary images of the extensions of these codes we were able to construct 27 new extremal binary self-dual codes of length 68. Self-dual codes for these weight enumerators have been obtained for the first time in the literature.

The rest of the paper is organized as follows. In Section 2, the preliminaries about the structure of the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and the construction from [1] we were inspired by are given. Section 3 is devoted to the methods we introduce which use the short Kharaghani array. The computer algebra system MAGMA [2] has been used for computation and results regarding the constructions are given in Section 4. A substantial number of self-dual Type I $[64, 32, 12]_2$-codes and 27 new extremal binary self-dual codes of length 68 are constructed. Section 5 concludes the paper with some possible lines of research.

2. Preliminaries

Throughout the text, let $\mathcal{R}$ be a commutative Frobenius ring. A linear code $\mathcal{C}$ of length n over $\mathcal{R}$ is an $\mathcal{R}$-submodule of $\mathcal{R}^n$. Elements of $\mathcal{C}$ are called codewords. Codes over $\mathbb{F}_2$ and $\mathbb{F}_3$ are called binary and ternary, respectively. Consider two arbitrary elements $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ of $\mathcal{R}^n$. The Euclidean inner product is defined as $\langle x, y\rangle_E = \sum x_i y_i$ and in this paper the duality is understood in terms of the Euclidean inner product. In other words, the dual of a code $\mathcal{C}$ of length n is denoted as $\mathcal{C}^\perp$ and defined to be

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

A code $\mathcal{C}$ is said to be *self-orthogonal* when $\mathcal{C} \subset \mathcal{C}^\perp$ and *self-dual* when $\mathcal{C} = \mathcal{C}^\perp$. An even self-dual code is said to be Type II if all codewords have weights divisible by 4; otherwise it is said to be Type I. For more information on self-dual codes over commutative Frobenius rings we refer to [7].

The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is a characteristic 2 ring of size 4. The ring is defined as $\mathbb{F}_2 + u\mathbb{F}_2 = \left\{a + bu | a, b \in \mathbb{F}_2, u^2 = 0\right\}$, which is isomorphic to the quotient $\mathbb{F}_2[x] / \left(x^2\right)$. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been studied in [6]. Some construction methods for self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are given in [9]. Karadeniz et al. classified self-dual four-circulant codes of length 32 over $\mathbb{F}_2 + u\mathbb{F}_2$ in [12]. For codes over $\mathbb{F}_2 + u\mathbb{F}_2$ a duality preserving a linear Gray map is given in [6] as follows:

$$\varphi : (\mathbb{F}_2 + u\mathbb{F}_2)^n \to \mathbb{F}_2^{2n},\ \varphi(a + bu) = (b, a + b), a, b \in \mathbb{F}_2^n.$$

In [4], Conway and Sloane gave an upper bound on the minimum Hamming distance of a binary self-dual code which was finalized by Rains as follows:

Theorem 1 (see [16]). *Let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a Type I and Type II binary code of length n, respectively. Then*

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

and

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

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

For the rest of the paper we let $R = (r_{ij})$ be the back diagonal $(0,1)$-matrix of order n satisfying $r_{i,n-i+1} = 1$, $r_{ij} = 0$ if $j \neq n-i+1$. We are inspried by a construction of self-dual codes given in [1] as follows:

Theorem 2 (see [1]). *Let A, B, C, D be four n by n circulant matrices satisfying $AA^T + BB^T + CC^T + DD^T = -I_n$. Then the code generated by the matrix*

$$G = \left(I_{4n} \left| \begin{array}{cccc} A & BR & CR & DR \\ -BR & A & D^TR & -C^TR \\ -CR & -D^TR & A & B^TR \\ -DR & C^TR & -B^TR & A \end{array} \right. \right)$$

is a self-dual code.

λ-circulant matrices share most of the properties of circulant matrices. For instance, they commute with each other for the same λ. Thus, the construction in Theorem 2 can easily be extended to λ-circulant matrices. The construction uses the Goethals-Seidel array and we propose four-block-circulant constructions in Section 3.

3. Self-dual codes via the short Kharaghani array

In this section, two constructions for self-dual codes over commutative Frobenius rings are given. In [15], Kharaghani gave some arrays for orthogonal designs. The first construction uses the short Kharaghani array and the second uses a variation of the array. Although the conditions of duality appear to be strict, we obtained good examples of self-dual codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and the binary field $\mathbb{F}_2$. The given methods can be used for any commutative Frobenius ring. In what follows, ternary self-dual codes are given as examples in order to demonstrate that the methods work for non-binary alphabets. A ternary self-dual code of length n is said to be *extremal* if d meets the upper bound $d \leq 3\lfloor \frac{n}{12} \rfloor + 3$.

We need the following lemma from [13];

Lemma 1 (see [13]). *Let A and C be λ-circulant matrices. Then $C' = CR$ is a λ-reverse-circulant matrix and it is symmetric. Moreover, $AC' - C'A^T = 0$. Equivalently, $ARC^T - CRA^T = 0$.*

Theorem 3 (Construction I). *Let $\mathcal{C}$ be a linear code over $\mathcal{R}$ of length $8n$ generated by the matrix in the following form:*

$$G := \left(I_{4n} \left| \begin{array}{cccc} A & B & CR & DR \\ -B & A & DR & -CR \\ -CR & -DR & A & B \\ -DR & CR & -B & A \end{array} \right. \right), \tag{1}$$

where A, B, C and D are λ-circulant matrices over the ring $\mathcal{R}$ satisfying the conditions

$$AA^T + BB^T + CC^T + DD^T = -I_n$$

and

$$AB^T - BA^T - CD^T + DC^T = 0.$$

Then $\mathcal{C}$ is self-dual.

Proof. Let M be the right half of the matrix G in (1). Then it is enough to show that $MM^T = -I_{4n}$.

$$\begin{aligned} MM^T &= \begin{pmatrix} A & B & CR & DR \\ -B & A & DR & -CR \\ -CR & -DR & A & B \\ -DR & CR & -B & A \end{pmatrix} \begin{pmatrix} A^T & -B^T & -RC^T & -RD^T \\ B^T & A^T & -RD^T & RC^T \\ RC^T & RD^T & A^T & -B^T \\ RD^T & -RC^T & B^T & A^T \end{pmatrix} \\ &= \begin{pmatrix} X & Y & Z & T \\ -Y & X & -T & -Z \\ -Z & -T & X & Y \\ -T & Z & -Y & X \end{pmatrix}, \end{aligned}$$

where

$$\begin{aligned} X &= AA^T + BB^T + CC^T + DD^T \\ Y &= -AB^T + BA^T + CD^T - DC^T \\ Z &= -ACR - BDR + CRA^T + DRB^T \\ T &= -ADR + BCR - CRB^T + DRA^T. \end{aligned}$$

We have $Z = T = 0$ by Lemma 1 and $Y = 0$, $X = -I_n$ by the assumption. Hence $MM^T = -I_{4n}$, which implies $GG^T = 0$. Therefore, the code $\mathcal{C}$ is self-orthogonal and self-dual due to its size. □

In the following example we obtain an extremal ternary self-dual code of length 56 by Theorem 3.

Example 1. *Let $\mathcal{C}_{56}$ be the code over $\mathbb{F}_3$ obtained by Construction I for $n = 7, \lambda = 1$, $r_A = (2200120), r_B = (0020102), r_C = (0010020)$ and $r_D = (2111001)$. Then $\mathcal{C}_{56}$ is a self-dual $[56, 28, 15]_3$-code. In other words, it is an extremal ternary self-dual code of length 56 with 68544 words of weight 15 and an automorphism group of order $2^3 \times 7$.*

Now we give a variation of the construction in Theorem 3 as follows:

Theorem 4 (Construction II)**.** *Let λ be an element of the ring $\mathcal{R}$ with $\lambda^2 = 1$ and $\mathcal{C}$ a linear code over $\mathcal{R}$ of length $8n$ generated by the matrix:*

$$G := \left(\begin{array}{c|cccc} & A & B & CR & DR \\ I_{4n} & -B^T & A^T & DR & -CR \\ & -CR & -DR & A & B \\ & -DR & CR & -B^T & A^T \end{array} \right), \tag{2}$$

where A, B, C and D are λ-circulant matrices over $\mathcal{R}$ satisfying the conditions

$$\begin{aligned} AA^T + BB^T + CC^T + DD^T &= -I_n \\ CD^T - DC^T &= 0 \end{aligned}$$

and

$$-ADR + BCR - CRB + DRA = 0.$$

Then the code $\mathcal{C}$ is a self-dual code over $\mathcal{R}$.

Proof. Let M be the right half of the matrix G in (2). Then

$$MM^T = \begin{pmatrix} X & Y & Z & T \\ -Y^T & X & -T^T & -U \\ -Z & -T & X & Y \\ -T^T & U & -Y^T & X \end{pmatrix},$$

where

$$\begin{aligned} X &= AA^T + BB^T + CC^T + DD^T \\ Y &= -AB + BA + CD^T - DC^T \\ Z &= -ACR - BDR + CRA^T + DRB^T \\ T &= -ADR + BCR - CRB + DRA \\ U &= B^T DR + A^T CR - DRB - CRA. \end{aligned}$$

By Lemma 1, $Z = 0$. Matrices A^T and B^T are λ^{-1}-circulant, they are λ-circulant since $\lambda = \lambda^{-1}$. Hence by Lemma 1, $U = 0$.

$$Y = -AB + BA + CD^T - DC^T = CD^T - DC^T,$$

since λ-circulant matrices commute. By the assumption, $Y = 0 = T$ and $X = -I_n$. It follows that $MM^T = -I_{4n}$, which implies $\mathcal{C}$ is self-orthogonal. The code $\mathcal{C}$ is self-dual due to its size. □

There are only two extremal self-dual ternary codes of length 24. Those are the extended quadratic residue code and the Pless symmetry code. In the following example we obtain both by Theorem 4.

Example 2. *Let $\mathcal{C}_{24}$ be the code over $\mathbb{F}_3$ obtained by Construction II for $n = 3, \lambda = 2$, $r_A = (221), r_B = (201), r_C = (212)$ and $r_D = (221)$. Let $\mathcal{D}_{24}$ be the code over $\mathbb{F}_3$ obtained by Construction II for $n = 3, \lambda = 2$, $r_A = (200), r_B = (112), r_C = (102)$ and $r_D = (110)$. Then $\mathcal{C}_{24}$ and $\mathcal{D}_{24}$ are self-dual $[24, 12, 9]_3$-codes. The code $\mathcal{C}_{24}$ is the Pless symmetry code and the code $\mathcal{D}_{24}$ is the extended quadratic residue code over $\mathbb{F}_3$ for $p = 23$.*

Remark 1. *The two extremal self-dual $[24, 12, 9]_3$-codes in Example 2 are also easily obtained by Theorem 3. On the other hand, only the Pless symmetry code of parameters $[24, 12, 9]_3$ could be constructed by Theorem 2. That exhibits that the constructions proposed in this section might be advantageous compared to Theorem 2 even if the conditions are restrictive.*

4. Computational results

The constructions given in Section 3 can be applied to any commutative Frobenius ring. We focus on binary self-dual codes obtained by the methods. The constructions applied to the binary field $\mathbb{F}_2$ and the ring $\mathbb{F}_2 + u\mathbb{F}_2$. The results are tabulated. Twenty seven new extremal binary self-dual codes of length 68 are obtained as an application of Theorem 3 and Theorem 4.

In [4], possible weight enumerators for a self-dual Type I $[64, 32, 12]_2$-code were characterized as:

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

Recently, codes with β =29, 59 and 74 in $W_{64,1}$ [13], a code with β =80 in $W_{64,2}$ were constructed in [12]. Together with these, the existence of codes is known for β =14, 18, 22, 25, 29, 32, 36, 39, 44, 46, 53, 59, 60, 64 and 74 in $W_{64,1}$ and for β =0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, 17, 18, 20, 21, 22, 23, 24, 25, 28, 19, 30, 32, 33, 36, 37, 38, 40, 41, 44, 48, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120 and 184 in $W_{64,2}$.

4.1. Computational results for Construction I

Results for Construction I for $n = 8$ over $\mathbb{F}_2$ and for $n = 4$over $\mathbb{F}_2 + u\mathbb{F}_2$ are given. Self-dual Type I $[64, 32, 12]_2$-codes are constructed and tabulated.

$\mathcal{C}_i$	r_A	r_B	r_C	r_D	$\lvert Aut(\mathcal{C}_i)\rvert$	β in $W_{64,2}$
$\mathcal{C}_1$	(10001101)	(00010000)	(01000110)	(01111010)	2^5	0
$\mathcal{C}_2$	(10111001)	(01111101)	(01100001)	(01111111)	2^5	16
$\mathcal{C}_3$	(10110011)	(01101001)	(11101101)	(01101111)	2^6	16
$\mathcal{C}_4$	(00100011)	(11010010)	(11110011)	(01010011)	2^5	32
$\mathcal{C}_5$	(11011000)	(00001110)	(11010100)	(11000000)	2^5	48
$\mathcal{C}_6$	(11011000)	(11110001)	(01000111)	(01011100)	2^7	80

Table 1: *Construction I over* $\mathbb{F}_2$ *for* $n = 8$

For $n = 8$, Theorem 3 gives self-dual codes over the binary field $\mathbb{F}_2$ listed in Table 1.

$\mathcal{D}_i$	λ	r_A	r_B	r_C	r_D	$\lvert Aut(\mathcal{D}_i)\rvert$	β in $W_{64,2}$
$\mathcal{D}_1$	3	$(3, 3, 1, u)$	$(u, 0, 0, 1)$	$(0, 0, 3, 0)$	$(3, u, 1, 0)$	2^5	0
$\mathcal{D}_2$	3	$(1, 1, 1, u)$	$(u, 1, 0, 1)$	$(u, 3, 3, 0)$	$(0, u, 1, 1)$	2^5	16
$\mathcal{D}_3$	3	$(3, 1, 3, u)$	$(0, 1, u, 1)$	$(u, 3, 3, u)$	$(u, u, 1, 1)$	2^6	16
$\mathcal{D}_4$	3	$(3, 1, 3, 0)$	$(0, 1, u, 1)$	$(u, 1, 3, u)$	$(u, 0, 1, 1)$	2^5	32
$\mathcal{D}_5$	3	$(1, 3, 1, 0)$	$(u, 1, 0, 1)$	$(0, 3, 3, u)$	$(0, 0, 3, 1)$	2^5	48
$\mathcal{D}_6$	3	$(3, 1, 3, u)$	$(u, 3, 0, 3)$	$(u, 3, 1, 0)$	$(u, 0, 1, 3)$	2^7	80

Table 2: *Construction I over* $\mathbb{F}_2 + u\mathbb{F}_2$ *for* $n = 4$

In Table 2, Construction II is applied to the ring $\mathbb{F}_2 + u\mathbb{F}_2$ in order to construct self-dual codes of length 32.

Remark 2. *The first extremal self-dual binary code of length* 64 *with a weight enumerator* $\beta = 80$ *in* $W_{64,2}$ *is constructed in [12] by using four circulant construction over* $\mathbb{F}_2 + u\mathbb{F}_2$. *In Tables 1 and 2, we give an alternative construction for the code by the short Kharaghani array.*

4.2. Computational results for Construction II

In this section, we give computational results for Construction II.

$\mathcal{E}_i$	r_A	r_B	r_C	r_D	$\lvert Aut(\mathcal{E}_i)\rvert$	β in $W_{64,2}$
$\mathcal{E}_1$	(00000010)	(01101100)	(01100111)	(10110000)	2^4	0
$\mathcal{E}_2$	(11101100)	(10101110)	(10111110)	(01111010)	2^5	0
$\mathcal{E}_3$	(01110110)	(10101000)	(11110010)	(11001001)	2^6	0
$\mathcal{E}_4$	(10010011)	(01110101)	(01000110)	(10011110)	2^4	8
$\mathcal{E}_5$	(01111000)	(01110101)	(10000001)	(00100100)	2^5	8
$\mathcal{E}_6$	(00110100)	(01011010)	(00010011)	(01000011)	2^4	16
$\mathcal{E}_7$	(00110001)	(01011010)	(01101011)	(11100011)	2^5	16
$\mathcal{E}_8$	(01000110)	(11000000)	(10110100)	(10101001)	2^4	24
$\mathcal{E}_9$	(10100011)	(11111101)	(11111001)	(01011010)	2^5	24
$\mathcal{E}_{10}$	(01000110)	(11001101)	(10111110)	(00011100)	2^5	32
$\mathcal{E}_{11}$	(01100100)	(10100101)	(10011111)	(10101100)	2^4	40
$\mathcal{E}_{12}$	(11110000)	(00010011)	(11110001)	(10110101)	2^5	48

Table 3: *Construction II over* $\mathbb{F}_2$ *for* $n = 8$

In Table 3, extremal self-dual Type I codes of length 64 are constructed.

$\mathcal{F}_i$	λ	r_A	r_B	r_C	r_D	$\lvert Aut(\mathcal{F}_i)\rvert$	β in $W_{64,2}$
$\mathcal{F}_1$	3	$(0,0,1,0)$	$(3,0,3,u)$	$(u,u,0,1)$	$(1,0,1,3)$	2^4	0
$\mathcal{F}_2$	3	$(1,0,1,u)$	$(u,3,1,1)$	$(1,1,u,0)$	$(0,u,1,3)$	2^4	8
$\mathcal{F}_3$	3	$(1,0,3,u)$	$(u,1,3,3)$	$(1,3,u,u)$	$(0,0,1,1)$	2^5	8
$\mathcal{F}_4$	1	$(1,0,0,u)$	$(0,0,1,1)$	$(3,1,1,3)$	$(0,u,1,1)$	2^4	16
$\mathcal{F}_5$	3	$(0,u,u,1)$	$(u,1,3,3)$	$(0,3,0,0)$	$(1,u,1,u)$	2^5	16
$\mathcal{F}_6$	3	$(u,0,1,u)$	$(1,1,3,1)$	$(3,3,1,u)$	$(3,1,1,u)$	2^4	24
$\mathcal{F}_7$	3	$(3,u,1,0)$	$(u,1,1,3)$	$(1,3,0,0)$	$(u,u,3,3)$	2^5	24
$\mathcal{F}_8$	1	$(3,0,0,u)$	$(u,0,1,3)$	$(3,1,1,3)$	$(u,u,1,3)$	2^5	32
$\mathcal{F}_9$	3	$(0,0,1,u)$	$(1,1,1,1)$	$(1,3,1,u)$	$(3,3,3,u)$	2^5	48

Table 4: *Construction II over* $\mathbb{F}_2 + u\mathbb{F}_2$ *for* $n = 4$

Now we apply the construction in Theorem 4 to the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and give the results in Table 4.

Construction II has an advantage over Construction I. Although the conditions are strict, Construction II allows us to narrow down the search area. We may fix the matrices C and D satisfying $CD^T - DC^T = 0$ and search for circulant matrices A and B which satisfy the remaining necessary conditions. We present that in the following example:

Example 3. *Let* $n = 4, \lambda = 1 + u, C$ *and* D *be* λ*-circulant matrices with first rows* $r_C = (1, 1 + u, u)$ *and* $r_D = (0, 0, 1, 1)$, *respectively. Then* $CD^T - DC^T = 0$. *So we*

may search for λ-circulant matrices A and B that satisfy

$$AA^T + BB^T + CC^T + DD^T = -I_n$$

and

$$-ADR + BCR - CRB + DRA = 0.$$

For each pair of such matrices a self-dual code of length 32 over $\mathbb{F}_2 + u\mathbb{F}_2$ will be obtained by Construction II. Let A and B be λ-circulant matrices with the following first rows

r_A	r_B	β *in* $W_{64,2}$
$(1, 0, 1+u, u)$	$(u, 1, 1+u, 1+u)$	8
$(1+u, u, 1, 0)$	$(u, 1, 1, 1+u)$	24

Then we obtain two extremal binary self-dual $[64, 32, 12]_2$-codes with automorphism groups of order 2^5 as Gray images. Note that this approach reduces the search field remarkably from $4^{16} = 4294967296$ to $4^8 = 65536$.

Remark 3. *Although constructions I and II have more strict conditions than the construction in Theorem 2, computational results indicate that they are superior to the method given in Theorem 2 since only one Type I $[64, 32, 12]_2$-code with weight enumerator $\beta = 8$ in $W_{64,2}$ is obtained by applying the construction that uses the Goethals-Seidel array to $\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2$.*

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

In [3], possible weight enumerators of a self-dual $[68, 34, 12]_2$-code are characterized as follows:

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

where $0 \le \gamma \le 9$ by [10]. So far, the existence of codes with weight enumerators for $\gamma = 0, 1, 2, 3, 4$ and 6 is known. Recently, new codes in $W_{68,2}$ have been obtained in [8, 13]. These codes exist for $W_{68,2}$ when

$$\gamma = 0, \beta = 11, 17, 22, 33, 44, \ldots, 158, 165, 187, 209, 221, 231, 255, 303$$

or

$$\beta \in \{2m | m = 17, 20, 88, 99, 102, 110, 119, 136, 165 \text{ or } 80 \le m \le 86\};$$

$$\gamma = 1, \beta = 49, 57, 59, \ldots, 160$$

or

$$\beta \in \{2m | m = 27, 28, 29, 95, 96 \text{ or } 81 \le m \le 90\};$$

$$\gamma = 2, \beta = 65, 69, 71, 77, 81, 159, 186$$

or

$$\beta \in \{2m | 30 \le m \le 68,\ 70 \le m \le 91\}$$

or

$$\beta \in \{2m + 1 | 42 \le m \le 69,\ 71 \le m \le 77\};$$

$\gamma = 3, \beta = 101, 103, 105, 107, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 137, 141, 145, 147, 149, 153, 159, 193$

or

$$\beta \in \left\{ 2m \,\middle|\, \begin{array}{l} m = 44, 45, 47, 48, 50, 51, 52, 54, \ldots, 72, 74, 75, \\ 77, \ldots, 84, 86, 87, 88, 89, 90, 91, 92, 94, 95, 97, 98 \end{array} \right\};$$

$$\gamma = 4, \beta \in \left\{ 2m \,\middle|\, \begin{array}{c} m = 43, 48, 49, 51, 52, 54, 55, 56, 58, 60, 61, 62, \\ 64, 65, 67, \ldots, 71, 75, \ldots, 78, 80, 87, 97 \end{array} \right\};$$

$\gamma = 6$ with $\beta \in \{2m | m = 69, 77, 78, 79, 81, 88\}$.

In this section, we obtain 27 new codes with weight enumerators for $\gamma = 0$ and β =174, 180, 182, 184, 186, 188, 190, 192, 194; $\gamma = 1$ and β =50, 52, 184, 186, 188; $\gamma = 2$ and β =184, 188, 190, 192, 194, 196, 198, 200, 206, 208; $\gamma = 3$ and β =98, 106; $\gamma = 4$ and β =196 in $W_{68,2}$.

Theorem 5 (see [7]). *Let $\mathcal{C}$ be a self-dual code over $\mathcal{R}$ of length n and $G = (r_i)$ a $k \times n$ generator matrix for $\mathcal{C}$, where r_i is the i-th row of G, $1 \le i \le k$. Let c be a unit in $\mathcal{R}$ such that $c^2 = 1$ and X a vector in $\mathcal{R}^n$ with $\langle X, X \rangle = 1$. Let $y_i = \langle r_i, X \rangle$ for $1 \le i \le k$. Then the following matrix*

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

generates a self-dual code $\mathcal{C}'$ over $\mathcal{R}$ of length $n + 2$.

In Table 5, the codes are generated over $\mathbb{F}_2 + u\mathbb{F}_2$ by the matrices of the following form:

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

where G is the generating matrix of the code $\mathcal{C}$ with the specified circulant matrices. Then $\mathcal{C}_{68,i}$ is the binary image $\varphi(G')$ of the extension.

Theorem 6. *The existence of extremal self-dual binary codes is known for* 492 *parameters in $W_{68,2}$.*

Remark 4. *The binary generator matrices of the codes in Table 5 are available online at [14]. Those have automorphism groups of order* 2.

$\mathcal{C}_{68,i}$	$\mathcal{C}$	c	X	γ	β
$\mathcal{C}_{68,1}$	$\mathcal{D}_6$	1	$(13u11uu3331uu10133u330u31u010031)$	0	174
$\mathcal{C}_{68,2}$	$\mathcal{D}_6$	3	$(103u303u0001333u3u03uu1u000u3313)$	0	180
$\mathcal{C}_{68,3}$	$\mathcal{D}_6$	3	$(u1331u01333u31113101100310u1uu33)$	0	182
$\mathcal{C}_{68,4}$	$\mathcal{D}_6$	3	$(001u3010uu1u00313101100310u1uu33)$	0	184
$\mathcal{C}_{68,5}$	$\mathcal{D}_6$	3	$(1u303u1uu00311103uu1uu3000uu1313)$	0	186
$\mathcal{C}_{68,6}$	$\mathcal{D}_6$	3	$(301u1u1u00u1311u3uu30u10uu0u1333)$	0	188
$\mathcal{C}_{68,7}$	$\mathcal{D}_6$	3	$(3u13u333100u03011uu1333u1u110uu0)$	0	190
$\mathcal{C}_{68,8}$	$\mathcal{D}_6$	3	$(310110310uu1u33011331u00u3300001)$	0	192
$\mathcal{C}_{68,9}$	$\mathcal{D}_6$	3	$(101010100003111u3uu1u03u000u3331)$	0	194
$\mathcal{C}_{68,10}$	$\mathcal{F}_1$	3	$(uu00333011u1330uu0u10u0u013u1100)$	1	50
$\mathcal{C}_{68,11}$	$\mathcal{F}_1$	3	$(u0uu333013u113uu00u3uuu00330310u)$	1	52
$\mathcal{C}_{68,12}$	$\mathcal{D}_6$	1	$(31013uu3133uu30311011uu33u03uu11)$	1	184
$\mathcal{C}_{68,13}$	$\mathcal{D}_6$	3	$(330330u3113uu30311u13u013003uu11)$	1	186
$\mathcal{C}_{68,14}$	$\mathcal{D}_6$	1	$(330130u3333uu3u3310330u33uu10011)$	1	188
$\mathcal{C}_{68,15}$	$\mathcal{D}_6$	1	$(3u3u1u100uu1133u301u0u3113131uu0)$	2	184
$\mathcal{C}_{68,16}$	$\mathcal{D}_6$	3	$(3u1u3u10uuu1133u301uuu3131113uuu)$	2	188
$\mathcal{C}_{68,17}$	$\mathcal{D}_6$	3	$(011u01u3330u1001330310u13u010011)$	2	190
$\mathcal{C}_{68,18}$	$\mathcal{D}_6$	1	$(1u1u10300u01311u1u100u11333130uu)$	2	192
$\mathcal{C}_{68,19}$	$\mathcal{D}_6$	3	$(0310010111uu10u131u310u310010011)$	2	194
$\mathcal{C}_{68,20}$	$\mathcal{D}_6$	1	$(10301010000333301010u01313111u00)$	2	196
$\mathcal{C}_{68,21}$	$\mathcal{D}_6$	3	$(u310u1u3130u1uu113u130u11uu30u33)$	2	198
$\mathcal{C}_{68,22}$	$\mathcal{D}_6$	1	$(u110u10331u0100111u3100310010u33)$	2	200
$\mathcal{C}_{68,23}$	$\mathcal{D}_6$	1	$(0130u3u311uu1uu1310330013u030011)$	2	206
$\mathcal{C}_{68,24}$	$\mathcal{D}_6$	3	$(301u1u1u00u1311u3010u01333133uu0)$	2	208
$\mathcal{C}_{68,25}$	$\mathcal{D}_1$	3	$(u3330030u10uu313010001uu1030u0u3)$	3	98
$\mathcal{C}_{68,26}$	$\mathcal{D}_1$	3	$(1030uu1130u31311101u13u03030uu30)$	3	106
$\mathcal{C}_{68,27}$	$\mathcal{D}_6$	3	$(u310u30313u030u311u130u130u10033)$	4	196

Table 5: *New extremal binary self-dual codes of length 68 by Theorem 5*

5. Conclusion

Most of the constructions for self-dual codes are used to reduce the search field. In this paper, we use the short Kharaghani array and determine the necessary conditions for duality. The constructions could be used over different alphabets such as $\mathbb{Z}_4$; the integers modulo 4. One may suggest such constructions by using various arrays. By such methods we may attempt to construct codes as the extremal binary self-dual Type II codes of length 72, which is a long standing open problem.

Acknowledgement

The author would like to thank the anonymous referees and the editor for their valuable comments.

References

[1] K. Betsumiya, S. Georgiou, T. A. Gulliver, M. Harada, C. Koukouvinos, *On self-dual codes over prime fields*, Discrete Math. **262**(2003), 37–58.

[2] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**(1997), 235–265.

[3] S. Buyuklieva, I. Boukliev, *Extremal self-dual codes with an automorphism of order 2*, IEEE Trans. Inform. Theory **44**(1998), 323–328.

[4] J. H. Conway, N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory **36**(1990), 1319–1333.

[5] D. Crnković, S. Rukavina, L. Simčić, *Binary doubly-even self-dual codes of length 72 with large automorphism groups*, Math. Commun. **18**(2013), 297–308.

[6] S. T. Dougherty, P. Gaborit, M. Harada, P. Sole, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45**(1999), 32–45.

[7] S. T. Dougherty, J. -L. Kim, H. Kulosman, H. Liu, *Self-dual codes over commutative Frobenius rings*, Finite Fields Appl. **16**(2010), 14–26.

[8] M. Gürel, N. Yankov, *Self-dual codes with an automorphism group of order* 17, Math. Commun. **21**(2016), 1–11.

[9] S. Han, H. Lee, Y. Lee, *Construction of self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, Bull. Korean Math. Soc. **49**(2012), 135–143.

[10] M. Harada, A. Munemasa, *Some restrictions on weight enumerators of singly even self-dual codes*, IEEE Trans. Inform. Theory **52**(2006), 1266–1269.

[11] W. C. Huffman, *On the classification and enumeration of self-dual codes*, Finite Fields Appl. **11**(2005), 451–490.

[12] S. Karadeniz, B. Yildiz, N. Aydin, *Extremal binary self-dual codes of lengths* 64 *and* 66 *from four-circulant constructions over codes* $\mathbb{F}_2 + u\mathbb{F}_2$, Filomat **28**(2014), 937–945.

[13] A. Kaya, B. Yildiz, A. Pasa, *New extremal binary self-dual codes from a modified four circulant construction*, Discrete Math. **339**(2016), 1086–1094.

[14] A. Kaya, *Binary generator matrices of new extremal self-dual binary codes of lengths 68*, available at `http://abidinkaya.wix.com/main#!research2/mmfl6`.

[15] H. Kharaghani, *Arrays for orthogonal designs*, J. Combin. Des. **8**(2003), 166–173.

[16] E. M. Rains, *Shadow Bounds for Self Dual Codes*, IEEE Trans. Inform. Theory **44**(1998), 134–139.