Extremal binary self-dual codes of length 64 from four-circulant constructions over $\mathbb{F}_2 + u\mathbb{F}_2$

Dr Suat Karadeniz
Department of Mathematics, Fatih University, Istanbul-TURKEY

Joint work with Dr Bahattin Yildiz

July 2013

OUTLINE

1. INTRODUCTION; EXTREMAL SELF-DUAL CODES
2. THE STRUCTURE OF THE RING $\mathbb{F}_2 + u\mathbb{F}_2$
3. THE FOUR-CIRCULANT CONSTRUCTION
4. EXTREMAL CODES OF LENGTH 64 OBTAINED FROM FOUR CIRCULANT CODES

I. INTRODUCTION, SELF DUAL CODES

Self-dual codes are an important class of codes and have been studied by researchers for a long time. These codes are found to be connected with many different fields of study such as combinatorial theory, group theory and cryptography. In the early periods the focus was on self-dual codes over finite fields, especially over , and there was a lot of work towards classifying binary self-dual codes up to certain lengths.

Later, when rings became more popular in coding theory, the scope of self-dual codes extended to rings as well. Self-dual codes over rings have received attention especially with respect to their connection to unimodular lattices and invariant theory.

Bounds on Self-dual Codes, Rains' Bound

Definition

A self-dual code over an arbitrary ring with a suitably defined Lee weight is said to be *Type II* (or **doubly-even**) if the Lee weight of every codeword is a multiple of 4 and *Type I* (or **singly-even**) otherwise.

The following theorem gives an upper bound on the minimum distance of a binary self-dual code.

Theorem

([Rains, 1998]) For a Type II code of length n, its minimum weight d satisfies $d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$. For a Type I code of length n, the minimum weight d is upper bounded by $d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 6$ if $n \equiv 22 \pmod{24}$ and $d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ otherwise.

A self-dual code is called **extremal** if the minimum weight meets the bound described in the theorem.

Extremal Codes

Binary self-dual codes of Type I and Type II have bounds on their minimum distances. So a great focus in coding theory has been on classifying extremal binary self-dual codes of certain lengths. Conway and Sloane have listed the possible weight enumerators of extremal self-dual codes of lengths up to 64 and 72 in [Conway, Sloane].

But for many of the possible weight enumerators, the existence of binary self-dual codes with that weight enumerator 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.

II. Linear codes over 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 by Dougherty et al. in late nineties.

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

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 $\left(\mathbb{F}_2 + u\mathbb{F}_2\right)^n$. 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 $\phi : (\mathbb{F}_2 + u\mathbb{F}_2)^n \longrightarrow \mathbb{F}_2^{2n}$

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

where $\bar{a}, \bar{b}$ in $\mathbb{F}_2^n$. ϕ is a distance preserving isometry from $\left((\mathbb{F}_2 + u\mathbb{F}_2)^n, d_L\right)$ 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.

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

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

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

Theorem

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

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

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 $d \leq 2d'$.

III. THE FOUR CIRCULANT CONSTRUCTION

Inspired by orthogonal designs, Betsumiya et al. introduced the following construction for self-dual codes over a prime field in 2003: Let M be a matrix over $\mathbb{F}_p$ of the form

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

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 by Georgiou in 2012, was also called the four-circulant construction by Harada et al. in their 2010 work. When applied in the binary field, the matrix simply becomes

$$M = \left[\begin{array}{c|cc} I_{2n} & A & B \\ & B^T & A^T \end{array}\right] \tag{4}$$

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

The four circulant construction in $\mathbb{F}_2 + u\mathbb{F}_2$

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

Theorem

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

$$G := \left[\begin{array}{c|cc} I_{2n} & A & B \\ & B^T & A^T \end{array}\right]$$

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.

The proof, being very similar to the ones in the literature is omitted here.

IV. Extremal binary self-dual codes of length 64

Our 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 5, 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 following four non-equivalent codes:
C_i is a binary self-dual code of length 32 generated by the matrix M_i of the form 4, where A_i and B_i are the 8×8 circulant parts. To determine the matrix M_i, we just need the first rows of A_i and B_i.

Table: 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 will now 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 will preserve the circulant structure and the identity matrix, thus a typical generating matrix for the lift will be of the form

$$G = \left[\begin{array}{c|cc} I_{16} & A & B \\ & B^T & A^T \end{array}\right]$$

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 run an exhaustive search to obtain extremal self-dual codes of length 64.

Let us recall that there are two kinds of weight enumerators for Type I extremal self-dual codes of length 64 as was described by Conway:

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

and

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

The existence of such codes is now known for $\beta = 14, 18, 32, 36, 44, 64$ in $W_{64,1}$ and for $\beta = 0, 2, 4, 6, 8, 9, 10, 12, 14, 16, 18, 20, 22, 23, 24, 28, 30, 32, 36, 37, 40, 44, 48, 56, 64, 72, 88, 96, 104, 108, 112, 114, 118, 120, 184$ in $W_{64,2}$.

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 our 2012 work.

In a work that has been submitted for publication we used a lift of the extended Hamming code over the ring R_3, to obtain extremal self-dual codes of length 64 with new β values in $W_{64,2}$, namely codes with $\beta = 1$, 5, 13, 17, 21, 25, 29, 33, 41, 52.

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

First row of A_1	First row of B_1	β 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

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

1st row of A_2	1st row of B_2	β, $W_{64,2}$	$\lvert Aut(C)\rvert$
$(u,u,u,u,0,1,1,1)$	$(u,1,u,1,1+u,1+u,1,1+u)$	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

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:

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

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:

First row of A_3	First row of B_3	β 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

THANKS