New Extremal Binary codes of length 66 as extensions of Bordered-Double-Circulant codes over R_2

Assist. Prof. Suat Karadeniz

June 2012

OUTLINE

1. INTRODUCTION; SELF-DUAL CODES
2. THE STRUCTURE OF THE RING R_2
3. BORDERED DOUBLE-CIRCULANT CONSTRUCTION
4. NEW EXTREMAL CODES OF LENTH 66 OBTAINED AS EXTENSIONS

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.

Recently, in [Dougherty et. al, 2010] worked out the theoretical background of self-dual codes over commutative Frobenius rings.

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.

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. THE STRUCTURE OF THE RING R_2

In this work, R_2 denotes the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ which is defined as a characteristic 2 ring subject to the restrictions $u^2 = v^2 = 0$ and $uv = vu$. Similarly, the isomorphism

$$R_2 \cong \mathbb{F}_2 [X, Y] \Big/ \left\langle X^2, Y^2, XY = YX \right\rangle$$

is clear to see. The ring can also be described in terms of $R_1 := \mathbb{F}_2 + u\mathbb{F}_2$ as

$$R_2 \cong R_1 [v] \Big/ \left\langle v^2 = 0, uv = vu \right\rangle = R_1 + vR_1.$$

Another definition for the ring can be given as

$$R_2 = \left\{ a + bu + cv + duv | a, b, c, d \in \mathbb{F}_2,\ u^2 = v^2 = 0 \text{ and } uv = vu \right\}.$$

We refer to [Yildiz, Karadeniz, 1 and 2] for details on linear and self-dual codes over R_2.

We can list the elements of the ring to be the following:

$$R_2 = \{0, u, v, u+v, uv, u+uv, v+uv, u+v+uv,$$
$$1, 1+u, 1+v, 1+u+v, 1+uv,$$
$$1+u+uv, 1+v+uv, 1+u+v+uv\}.$$

Note that the units of $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ can easily be found to be :

$$(\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^* = \{1, 1+u, 1+v, 1+u+v, 1+u+uv,$$
$$1+v+uv, 1+uv, 1+u+v+uv\}.$$

The following proposition will be used,

Proposition

For any $a \in R_2$, $a^2 = \begin{cases} 1, & \text{if } a \text{ is a unit} \\ 0, & \text{otherwise.} \end{cases}$

The Ideal Structure of R_2

$$R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$$

$$\uparrow$$

$$I_{u,v} = \{0, u, v, uv, u+v, u+uv, v+uv, u+v+uv\}$$

$$\uparrow$$

$$I_u = \{0, u, u+uv, uv\} \qquad I_v = \{0, v, v+uv, uv\} \qquad I_{u+v} = \{0, u+v, u+v+uv, uv\}$$

$$\uparrow$$

$$I_{uv} = \{0, uv\}$$

$$\uparrow$$

$$I_0 = \{0\}$$

R_2 is a local ring with the unique maximal ideal $I_{u,v}$. R_2 is neither a chain ring nor a Principal Ideal Ring.

Theorem

The ring R_2 is a Frobenius ring.

Linear codes over R_2 of length n are defined as always to be R_2-submodules of R_2^n.
By extending the notion of the Lee weight and the Gray map from [Dougherty et.al], we define

Definition

$\phi : R_2^n \to F_2^{4n}$, which is given by

$$\phi(\bar{a} + u\bar{b} + v\bar{c} + uv\bar{d}) = (\bar{a} + \bar{b} + \bar{c} + \bar{d}, \bar{c} + \bar{d}, \bar{b} + \bar{d}, \bar{d}),$$

is defined to be the Gray map from R_2^n to F_2^{4n}, where $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in F_2^n$.

Definition

For any element $a + ub + vc + uvd \in R$, we define $w_L(a + ub + vc + uvd) = w_H(a + b + c + d, c + d, b + d, d)$, where w_H denotes the ordinary Hamming weight for binary vectors, to be the Lee weight of $a + ub + vc + uvd$.

Lemma

If C is a linear code over R_2 of length n, size 2^k and minimum Lee distance d, then $\phi(C)$ is a binary $[4n, k, d]$-linear code.

The inner product and duality can be defined next. For $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in R_2^n$, we define

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= x_1y_1 + x_2y_2 + \cdots + x_ny_n \qquad (1)$$

where the operations are performed in the ring R_2.

Definition

Let C be a linear code over R_2 of length n, then the dual of C is defined as

$$C^{\perp} := \{\overline{y} \in (R_2)^n | < \overline{y}, \overline{x} >= 0, \forall \overline{x} \in C\}.$$

C is said to be self-orthogonal if $C \subseteq C^{\perp}$, and it is self-dual if $C = C^{\perp}$. A self-dual code over R_2 is said to be of Type II if the Lee weights of all codewords are divisible by 4, otherwise it is said to be of Type I.

The following theorem is very useful in connecting self-dual codes over R_2 to binary self-dual codes:

Theorem

Suppose C is a self-dual linear code over R_2 of length n. Then $\phi(C)$ is a self-dual binary linear code of length $4n$.

Because the Gray map is distance preserving, we get the following corollary:

Corollary

If C is a Type I (respectively Type II) code over R_2 with parameters $[n, 2^k, d]$, then $\phi(C)$ is a binary Type I (respectively, Type II) code of parameters $[4n, k, d]$.

III. THE BORDERED DOUBLE CIRCULANT CONSTRUCTION

Double Circulant Construction

The self-dual code generated by $[I_n|R]$ where R is a circulant matrix is called **pure double circulant code** .

Similarly the self-dual code generated by

$$\left[\begin{array}{c|cccc} & 0 & 1 & \cdots & 1 \\ I_n & 1 & & & \\ & \vdots & & R & \\ & 1 & & & \end{array}\right]$$

where R is a circulant matrix is called **bordered double circulant code**.

The Bordered-Double-Circulant Construction

In [Karadeniz, Yildiz 2012], we consider a bordered-double-circulant matrix with a special structure over R_2 and use this to construct self-dual codes.

Theorem

Let be a linear code of length over , generated by a bordered double-circulant matrix of the form

$$G = \begin{bmatrix} & x & y & y & y & \cdots & y \\ & z & & & & & \\ I_{2m} & z & & & & & \\ & \vdots & & & D & & \\ & z & & & & & \\ & z & & & & & \end{bmatrix}$$

where x is an arbitrary non-unit in R_2; y and z are arbitrary units in R_2, and D is a circulant $(2m-1) \times (2m-1)$ matrix over R_2 with the first row given by

$$D_1 = \{d_1, d_2, \cdots, d_{m-1}, d_{m-1}, d_{m-2}, \cdots, d_1, xyz\}.$$

Then C is a self-dual code over R_2.

Two New Extremal Type I Codes of Length 64

Table Two New Type I codes of parameters $[64, 32, 12]$ obtained via bordered-double-circulant construction.

(x, y, z)	(d_1, d_2, d_3)	β	$\lvert Aut\,(C)\rvert$
$(uv, uv+1, v+1)$	$(v+1, uv+1, uv+u+v+1)$	46	$2^3 \times 7$
$(uv, u+v+1, u+1)$	$(uv+u+1, u+v+1, uv+v+1)$	46	$2^3 \times 3 \times 7$

IV. NEW EXTREMAL CODES OF LENTH 66 AS EXTENSIONS

As given in [Conway,Sloane], there are three possibilities for the weight enumerators of extremal self-dual codes of length 66

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

In [Harada et. al.] and [Tsai] codes were obtained with weight enumerator $W_{66,2}$. A substantial number of codes with weight enumerator $W_{66,1}$ are obtained in [Conway, Sloane], [Gulliver, Harada], [Harada et. al.], [Huffman] and [Russeva,Yankov]. Recently, the codes with weight enumerator $W_{66,3}$ first found by Tsai et al. in [Tsai et.al. 2008] for $\beta = 28, 33$ and 34. In the following, we obtain the codes with $\beta = 54, 56, 57, 58, 59, 62$ and 66 in $W_{66,3}$. The extension method given below is used to obtain $[66, 33, 12]$ extremal codes from $[64, 32, 12]$ self-dual codes obtained as the Gray images of bordered-double circulant codes over R_2. We managed to obtain seven new extremal binary codes of length 66.

Extension Method [Jon-Lark Kim]

Theorem

(J.-L. Kim) 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 $1 \leq i \leq n$. 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 $1 \leq j \leq 2n$. Suppose that $y_i := (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) \cdot (l_i|r_i)$ for $1 \leq i \leq n$. Here $\cdot$ denotes the (scalar) inner product. Then the following matrix:

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

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

The extension in Theorem 11 is applied to $\phi(C_1)$ with binary vector X_j and extremal codes of length 66 with new weight enumerators are found;

$X_1 =\{(0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0$
$0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0)\}$ gives a code with $\beta = 59$ in $W_{66,3}$,

$X_2 =\{(0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1$
$0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1)\}$ gives a code with $\beta = 57$ in $W_{66,3}$,

$X_3 =\{(1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1$
$1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1)\}$ gives a code with $\beta = 56$ in $W_{66,3}$,

$X_4 =\{(1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1$
$1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1)\}$ gives a code with $\beta = 66$ in $W_{66,3}$.

The extension in Theorem 11 is applied to $\phi(C_2)$ with binary vector X_j and extremal codes of length 66 with new weight enumerators are found;

$X_5 =\{(0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0$
$1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)\}$, gives a code with $\beta = 58$ in $W_{66,3}$,

$X_6 =\{(1\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0$
$1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1)\}$, gives a code with $\beta = 62$ in $W_{66,3}$,

$X_7 =\{(0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1$
$1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)\}$, gives a code with $\beta = 54$ in $W_{66,3}$.

THANKS

[Chigira et. al] N. Chigira, M. Harada and M. Kitazume, *Extremal self-dual codes of length 64 through neighbors and covering radii*, Des. Codes Cryptogr., vol. 42, pp. 93–101, 2007.

[Conway, Sloane] J. H. Conway and N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inf. Theory, vol.36, no.6, pp.1319–1333, 1990.

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

[Gulliver, Harada] T. A. Gulliver and M. Harada, *Classification of extremal double circulant self-dual codes of lengths 64 to 72*, Des. Codes Cryptogr., vol.13, pp.257–269, 1998.

[Harada et. al] M. Harada, T. Nishimura and R. Yorgova, *New extremal self-dual codes of length 66*, Mathematica Balkanica., vol 21, pp. 113–121, 2007.

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

[Karadeniz, Yildiz, 2012] S. Karadeniz and B. Yildiz, *Double Circulant and bordered double circulant cons*tructions for self-dual codes over R_2, Advances in Mathematics of Communications, vol.6, no.2, pp.193–202, April 2012.

[Jon-Lark Kim] J. L. Kim, New Extremal Self-Dual Codes of Lengths $36, 38$ and 58, *IEEE Trans. Inf. Theory*, vol.47, no.1, pp.386–393, 2001.

[Russeva, Yankov] R. Russeva and N. Yankov, *On binary self-dual codes of length 69,62,64 and 66 having an automorphism of order 9*, Des. Codes Cryptogr., vol. 45, pp. 335–346, 2007.

[Tsai et.al.] H. P. Tsai, P. Y. Shih, R. Y. Wuh, W. K. Su and C. H. Chen, *Construction of Self-fual codes*, IEEE Trans. Inf. Theory, vol.54, no.8, pp.3826–3831, 2008.

[Tsai] H. P. Tsai, *Extremal self-dual codes of length 66 and 68*, IEEE Trans. Inf. Theory, vol.45, no.6, pp.2129–2133, 1999.

[Yildiz, Karadeniz, 1] B. Yildiz and S. Karadeniz, *Linear Codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des Codes Crypt, Vol. 54, pp.61–81, 2010.

[Yildiz, Karadeniz, 2] B. Yildiz and 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.