Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 176–181*

New extremal binary codes of length 66 as extensions of bordered-double-circulant codes over R_2

Suat Karadeniz skaradeniz@fatih.edu.tr
Department of Mathematics, Fatih University,Istanbul, Turkey
Bahattin Yildiz byildiz@fatih.edu.tr
Department of Mathematics, Fatih University, Istanbul, Turkey

Abstract. In this work, we extend two extremal codes of length 64 which were obtained by the authors as bordered-double-circulant codes over R_2. Using the extension, we have constructed seven new extremal binary codes of length 66 which were not previously known to exist.

1 Introduction

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 lattice theory. Contrary to the early periods, there has been a burst of activity in codes over rings recently. Self-dual codes over rings also have received a considerable attention since they have applications to unimodular lattices and non-linear binary codes. For some of these works we refer to [3] and [13].

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 72 in [2]. 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.

In this work, we use the ring $R_2 = \mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, which is a non-chain ring of size 16 and characteristic 2 to construct self-dual codes. A natural linear Gray map from R_2 to $\mathbb{F}_2^4$ maps self-dual codes over R_2 of length n to binary self-dual codes of length $4n$. Thus, in searching for extremal binary self-dual codes we make our search on R_2 instead. Since we are considering special generating matrices and because the self-duality condition imposes some constraints on these matrices, the number of independent variables in the search is reduced considerably. We find seven new extremal binary self-dual codes of length 66 as extensions of codes constructed in [7].

In section 2, we give a short background on the ring R_2, linear and self-dual codes over R_2, referring mainly to [12].

In section 3, we refer to [7] for the bordered-double-circulant construction for self-dual codes over R_2 and two previously unknown extremal binary self-dual codes of length 64 with $\beta = 46$ in $W_{64,1}$ of different automorphism groups. The extension method given in [8] is used for these two new codes. We were able to obtain seven new extremal self-dual binary codes of length 66 which were not previously known to exist.

2 Basics

Most of what follows can be found in [12]. The ring $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ is defined as a characteristic 2 ring subject to the restrictions $u^2 = v^2 = 0$ and $uv = vu$. Note that R_2 is not a chain ring, but its ideals can easily be described as

$$\{0\} \subseteq I_{uv} = uv(R_2) = \{0, uv\} \subseteq I_u, I_v, I_{u+v} \subseteq I_{u,v} \subseteq I_1 = R_2 \tag{1}$$

$I_{u,v}$ is the maximal ideal of R_2 that contains all the zero divisors with everything outside $I_{u,v}$ being a unit.

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 [3], we define

Definition 1. *$\phi : R_2^n \to \mathbb{F}_2^{4n}$, which is given by*

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

is defined to be the Gray map from R_2^n to $\mathbb{F}_2^{4n}$, where $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{F}_2^n$.

Definition 2. *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 $a + ub + vc + uvd$.*

We observe that the units $1, 1 + u, 1 + v$ and $1 + u + v + uv$ each have Lee weights 1 while the other units, $1 + uv$, $1 + u + uv$, $1 + v + uv$, $1 + u + v$ have weights 3.

The non-zero non-units all have Lee weight 2 except uv, which has Lee weight 4.

From the definitions it can be deduced that ϕ is a linear distance-preserving map, thus we obtain the following lemma, which will later be useful:

Lemma 1. *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

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= x_1y_1 + x_2y_2 + \cdots + x_ny_n \tag{2}$$

where the operations are performed in the ring R_2.

Definition 3. *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 1. *([12]) 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 1. *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 $[4n, k, d]$.*

3 The bordered-double-circulant construction

In [7], we consider a bordered-double-circulant matrix with a special structure over R_2 and use this to construct self-dual codes.

Theorem 2. *Let C be a linear code of length $4m$ over R_2, generated by a bordered double-circulant matrix of the form*

$$G = \left[\begin{array}{c|c|c} & x & y \; y \; . \; . \; . \; y \\ \hline & z & \\ & z & \\ I_{2m} & . & D \\ & . & \\ & . & \\ & z & \end{array}\right],$$

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.

3.1 Two new extremal Type I codes of length 64

In [7] by using the bordered-double-circulant construction given above, we were able to obtain a substantial amount of length 64 extremal self-dual codes some of which were known ones, but we managed to obtain two new ones.

Now, in order to clarify the generating matrix, observe that from the construction of Theorem 2, we only need to specify x, y, z and the first three entries of D_1, because $D_1 = \{d_1, d_2, d_3, d_3, d_2, d_1, xyz\}$.

Table 1: 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	$\lvert Aut(C)\rvert$
C_1	$(uv, uv+1, v+1)$	$(v+1, uv+1, uv+u+v+1)$	46(in $W_{64,1}$)	$2^3 \times 7$
C_2	$(uv, u+v+1, u+1)$	$(uv+u+1, u+v+1, uv+v+1)$	46(in $W_{64,1}$)	$2^3 \times 3 \times 7$

3.2 Seven new extremal codes of length 66

As given in [2], there are three possibilities for the weight enumerators of extremal self-dual codes of length 66

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

In [5] and [11] codes were obtained with weight enumerator $W_{66,2}$. A substantial number of codes with weight enumerator $W_{66,1}$ are obtained in [2], [5], [6] and [9]. Recently, the codes with weight enumerator $W_{66,3}$ first found by Tsai et al. in [10] 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.

Theorem 3. *[8] 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:*

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

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

1. The extension in Theorem 3 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 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 0 1 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0)} gives a code with $\beta = \mathbf{59}$ 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 $\beta = \mathbf{57}$ 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 1 0 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 $\beta = \mathbf{56}$ 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 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 $\beta = \mathbf{66}$ in $W_{66,3}$.

2. The extension in Theorem 3 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 $\beta = \mathbf{58}$ 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 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 $\beta = \mathbf{62}$ 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 $\beta = \mathbf{54}$ in $W_{66,3}$.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

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

[7] S. Karadeniz and B. Yildiz, *Double Circulant and bordered double circulant constructions for self-dual codes over R_2*, to appear in Advances in Mathematics of Communication.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.