JOURNAL OF SCIENCE
SAKARYA UNIVERSITY

Sakarya University Journal of Science

ISSN 1301-4048 | e-ISSN 2147-835X | Period Bimonthly | Founded: 1997 | Publisher Sakarya University | http://www.saujs.sakarya.edu.tr/

Title: Some results on free Euclidean self-dual codes over F2+vF2

Authors: Refia Aksoy, Fatma Çalışkan
Recieved: 2019-02-11 16:12:09

Accepted: 2019-07-12 09:41:46

Article Type: Research Article
Volume: 23
Issue: 6
Month: December
Year: 2019
Pages: 1131-1136

How to cite
Refia Aksoy, Fatma Çalışkan ; (2019), Some results on free Euclidean self-dual codes over F2+vF2. Sakarya University Journal of Science, 23(6), 1131-1136, DOI: 10.16984/saufenbilder.525606
Access link
http://www.saujs.sakarya.edu.tr/issue/44246/525606

Sakarya University Journal of Science 23(6), 1131-1136, 2019

Some results on free Euclidean self-dual codes over $\mathbb{F}_2 + \upsilon\mathbb{F}_2$

Refia Aksoy [1], Fatma Çalışkan [*2]

Abstract

In this paper, free Euclidean self-dual codes over the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ with $\upsilon^2 = \upsilon$ of order 4 are considered. A necessary and sufficient condition for the form of the generator matrix of a free Euclidean self-dual code is given. By using the distance preserving Gray map from $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ to $\mathbb{F}_2 \times \mathbb{F}_2$, the generator matrix of the binary code which corresponds the code over the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ is obtained. The codes of lengths up to 100 over the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ are found.

Keywords: Euclidean self-dual codes, codes over rings, Chinese remainder theorem

1. INTRODUCTION

Let A be a finite set that is called the alphabet. A code over A is a subset of A^n ($n \in \mathbb{N}$). If A is a field of two elements, then we say that the code is a binary code. Binary codes are used for the computer applications and the digital communications. An electronic information is transmitted through channels as a sequences of zeros and ones. Hence in theory, the binary field has been used as an alphabet. However, mathematicians generalized the alphabet from the binary field to finite fields. Moreover, researchers have studied about codes over finite rings. Codes over finite rings correspond to binary codes via a Gray map.

Linear codes are an important subclass of codes, which are linear subspaces of A^n if A is a field and linear submodules of A^n if A is a ring. If $C = C^{\perp}$, then the linear code C is self-dual. There exist important properties of self-dual codes, because many of the good codes are self-dual such as extended Golay code and they have a powerful algebraic structure. There are a large number of studies about self-dual codes over different finite rings ([5], [7], [12], [16]).

A code has important parameters such as length, dimension and minimum distance. These parameters help us to measure code efficiency and error-correcting capability. The main problem of algebraic coding theory is to find one of these parameters for given values of the other two ([13]). Researchers have investigated bounds which are limits on the parameters of a code ([4], [6], [10]). There are plenty of researches related to obtaining both the minimum distance of a linear

[1] İstanbul University, Institute of Graduate Studies in Sciences, İstanbul, Turkey. ORCID: 0000-0003-3093-0586
[*] Corresponding Author: fatmac@istanbul.edu.tr
[2] İstanbul University, Department of Mathematics, İstanbul, Turkey. ORCID: 0000-0001-7869-870X

code and the linear codes that attain the bounds ([15], [17]).

Constructing new self-dual codes and classifying self-dual codes have been an interesting research subject. Researchers have used different techniques to construct self-dual codes ([9], [11], [14]). In the present paper, we deal with self-dual codes over the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ with $\upsilon^2 = \upsilon$ of order 4. We use several known construction methods to establish free Euclidean self-dual codes. We then obtain self-dual codes over the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ with the highest minimum weights of lengths up to 100.

The rest of the paper is organized as follows. In Section 2, we give some properties of codes over the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$. In Section 3, we study free Euclidean self-dual codes over the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$ using the Chinese remainder theorem. In Section 4, we find the highest possible minimum weights using the construction methods given in [14].

2. PRELIMINARIES

Let R be the ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$. A linear code C over R of length n is defined to be an *R-submodule* of R^n. An element of C is called a *codeword* of C. For codes over R, three different weights are considered. These are the *Hamming*, *Lee* and *Bachoc weights*, which are defined in [1] and [7], given in Table 1.

Table 1. The weights of the elements of R

The elements	Hamming Weights	Lee Weights	Bachoc Weights
$\mathbf{0}$	0	0	0
$\mathbf{1}$	1	2	1
$\boldsymbol{\upsilon}$	1	1	2
$\mathbf{1}+\boldsymbol{\upsilon}$	1	1	2

The *minimum Hamming, Lee* and *Bachoc distances*, denoted by d_H, d_L and d_B, of C are the smallest Hamming, Lee and Bachoc weights among all non-zero codewords of C, respectively.

The ring R has two maximal ideals $I_1 = \langle\upsilon\rangle$ and $I_2 = \langle 1+\upsilon\rangle$. Therefore the Gray map $\Phi : R \to R/I_1 \times R/I_2$ is a ring isomorphism via the Chinese remainder theorem, where $\Phi(a+\upsilon b) = (a, a+b)$. Also, $\Phi_i : R \to R/I_i$ is a canonical homomorphism and $R/I_i \cong \mathbb{F}_2$ for $i = 1,2$. The Gray map is extended to R^n such that

$$\begin{aligned} \phi: R^n &\to \mathbb{F}_2^n \times \mathbb{F}_2^n \\ \mathbf{x} &\mapsto \phi(\mathbf{x}) = (\mathbf{r}, \mathbf{r}+\mathbf{q}), \end{aligned}$$

where $\mathbf{x} = \mathbf{r} + \upsilon\mathbf{q}$ and $\mathbf{r}, \mathbf{q} \in \mathbb{F}_2^n$. The map ϕ is a weight-preserving map from R^n (Lee weight) to $\mathbb{F}_2^{2n}$ (Hamming weight), which is, $w_L(\mathbf{x}) = w_H(\phi(\mathbf{x}))$ for $\mathbf{x} \in R^n$. The map ϕ is $\mathbb{F}_2$-linear and every element $\mathbf{x}$ of R^n can be written uniquely as $\mathbf{x} = \mathbf{r} + \upsilon\mathbf{q}$ for $\mathbf{r}, \mathbf{q} \in \mathbb{F}_2^n$. Let $C = \phi^{-1}(C_1, C_2)$ be a code over R. In this case, we denote C as $CRT(C_1, C_2)$, where C_1 and C_2 are uniquely determined for each C.

The *Euclidean inner product* on R^n is given by $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i y_i$ and the *Hermitian inner product* on R^n is $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$ where $\mathbf{x}, \mathbf{y} \in R^n$, with $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n)$, and $\overline{0} = 0$, $\overline{1} = 1$, $\overline{\upsilon} = 1+\upsilon$, $\overline{1+\upsilon} = \upsilon$.

The *Euclidean dual* of an $[n,k]$-code C is the $[n, n-k]$-code

$$C^{\perp} = \{\mathbf{x} \in R^n | (\mathbf{x}, \mathbf{c}) = 0 \text{ for all } \mathbf{c} \in C\}$$

and the *Hermitian dual* is the code

$$C^{*} = \{\mathbf{x} \in R^n | \langle \mathbf{x}, \mathbf{c} \rangle = 0 \text{ for all } \mathbf{c} \in C\}.$$

C is *Euclidean self-orthogonal* if $C \subseteq C^{\perp}$ and *Hermitian self-orthogonal* if $C \subseteq C^{*}$. C is *Euclidean self-dual* if $C = C^{\perp}$ and *Hermitian self-dual* $C = C^{*}$.

Two codes are *equivalent* if one can be obtained from the other by permuting the coordinates. A code C is called *isodual* if it is equivalent to its dual. A code C is called *formally self-dual* if C and the dual code of C have the same weight enumerators. Both self-dual codes and isodual codes are formally self-dual codes.

A Euclidean self-dual code is *Type IV* if the Hamming weights of all codewords are even. A Euclidean self-dual code is called *Type I* if it has at least one codeword of odd weight.

Proposition 2.1. ([8]) A code $C = CRT(C_1, C_2)$ is Euclidean self-dual if and only if C_1 and C_2 are both binary self-dual codes.

Remark 2.2. Binary self-dual codes of length n exist if and only if n is even. Moreover, binary self-dual codes have even weights.

Corollary 2.3. ([7]) A Euclidean self-dual code of length n exists if and only if n is even.

Proposition 2.4. ([7]) A code $C = CRT(C_1, C_2)$ is Euclidean Type IV self-dual if and only if $C_1 = C_2$.

Proposition 2.5. ([2]) Let d_H and d_L be the minimum Hamming distance and the minimum Lee distance of a code $C = CRT(C_1, C_2)$, respectively. Then

$$d_H(C) = d_L(C) = min\{d(C_1), d(C_2)\},$$

where $d(C_1)$ and $d(C_2)$ denote the minimum distances of the binary codes C_1 and C_2, respectively.

3. FREE EUCLIDEAN SELF-DUAL CODES

In our study, we consider free Euclidean self-dual codes over R. In this section, we present a general information about the structure of the generator matrix of a free Euclidean self-dual code over R and then we give a necessary and sufficient condition for the form of the generator matrix of a free Euclidean self-dual code.

The generator matrix G of a code C is a matrix whose rows generate C. We say that a code that is generated as a free R-module is called a *free code* over R. The row operations and the properties of R imply that any free code over R can be brought to an equivalent form which is generated by the rows of the matrix $[I_k, A + vB]$, where A and B are $k \times k$ binary matrices and I_k is the $k \times k$ identity matrix.

In general, a non-zero linear code C over R is permutation equivalent to a code with generator matrix of the form

$$G = \begin{bmatrix} I_{k_1} & A_1 & B_1 & D_1 + vD_2 \\ 0 & vI_{k_2} & 0 & vC_1 \\ 0 & 0 & (1+v)I_{k_3} & (1+v)E_1 \end{bmatrix},$$

where A_1, B_1, C_1, D_1, D_2 and E_1 are binary matrices and $|C| = 4^{k_1}2^{k_2}2^{k_3}$ [18].

Proposition 3.1. Let C be the free code given by $CRT(C_1, C_2)$. If $G = [I_k, A + vB]$ generates C, then the corresponding binary codes C_1 and C_2 have generator matrices $G_1 = [I_k, A]$ and $G_2 = [I_k, A + B]$, respectively, and vice versa.

Proof: From Corollary 3.2 in [18], we obtain that the Gray image of C is generated by

$$G' = \begin{bmatrix} \phi(G) \\ \phi(vG) \end{bmatrix} = \begin{bmatrix} I_k & A & 0 & 0 \\ 0 & 0 & I_k & A + B \end{bmatrix}.$$

Theorem 3.2. The matrix $G = [I_k, A + vB]$ generates a Euclidean self-dual code over R of length $2k$ if and only if A is an orthogonal matrix and $AB^T + BA^T + BB^T = 0$, where A and B are $k \times k$ binary matrices.

Proof: Let G be the generator matrix of a Euclidean self-dual code. Then

$$G \cdot G^T = 0.$$

Since

$$G \cdot G^T = [I_k, A + vB] \cdot \begin{bmatrix} I_k \\ A^T + vB^T \end{bmatrix},$$

we find

$$(I_k + AA^T) + v(AB^T + BA^T + BB^T) = 0.$$

Hence

$$AA^T = I_k$$

and

$$AB^T + BA^T + BB^T = 0.$$

Conversely, assume that $AA^T = I_k$ and $AB^T + BA^T + BB^T = 0$. Then $G \cdot G^T = 0$ which implies G generates a Euclidean self-dual code.

Remark 3.3. Let C be a free Euclidean self-dual code with the generator matrix $G = [I_k, A + \upsilon B]$, where A and B are $k \times k$ binary matrices. According to Theorem 3.2, B cannot be equal to A. Otherwise we would obtain $I_k = 0$ which is a contradiction.

Corollary 3.4. A Euclidean self-dual code which is generated by the matrix $G = [I_k, A + \upsilon B]$ is of Type IV if and only if the matrix B is a zero matrix.

4. THE CONSTRUCTION METHODS

In this section, we state three construction methods given in the following. By using these construction methods, we obtain Euclidean self-dual codes satisfying the conditions given in Theorem 3.2. All the computations were done with MAGMA Package [3].

Theorem 4.1. ([14]) Let A be a binary matrix and let I_k be the $k \times k$ identity matrix, then the following assertions hold:

a) A code with a double-circulant construction, i.e., a code with generating matrix $[I_k, A]$, where A is a circulant matrix, is isodual.
b) A code with a bordered double-circulant construction, i.e., a code with generating matrix

$$G = \left[\begin{array}{c|ccc} & \alpha & \beta & \cdots & \beta \\ I_k & \gamma & & & \\ & \vdots & & A & \\ & \gamma & & & \end{array}\right],$$

where A is a $(k-1) \times (k-1)$ circulant matrix, is isodual provided that $\beta = \gamma = 0$ or both β and γ are non-zero.

c) A code with a symmetric construction, i.e., a code with generating matrix $[I_k, A]$, where A is a symmetric matrix, is isodual.

4.1. The Double-Circulant Construction

Let A be a $k \times k$ orthogonal circulant matrix. The code C_1 whose generator matrix is of the form $[I_k, A]$ is a $[2k, k, d_1]$-code. Since C_1 is binary self-dual, we find the matrix B which satisfies the condition given in Theorem 3.2. The code C_2 whose generator matrix is of the form $[I_k, A + B]$ is a $[2k, k, d_2]$-code. Since C_2 is binary self-dual, we obtain the code C over the ring R, where C is a $[2k, k, min\{d_1, d_2\}]$-code. The minimum weights of the Euclidean self-dual codes that are obtained by using this construction method are given in Table 2.

In Table 2, $d_{max}(n)$ is the highest minimum weight of a binary linear code of length n and of dimension $n/2$, $d_{DC}(n)$ is the minimum weight of a Euclidean self-dual code of length n obtained by applying the double-circulant construction.

Table 2. The Euclidean self-dual codes obtained by using the double-circulant construction

length n	$d_{max}(n)$	$d_{DC}(n)$	length n	$d_{max}(n)$	$d_{DC}(n)$
2	2	2	**52**	10-12	10
4	2	2	**54**	11-13	10
6	3	2	**56**	12-14	8
8	4	4	**58**	12-14	10
10	4	2	**60**	12-14	12
12	4	4	**62**	12-15	10
14	4	2	**64**	12-16	12
16	5	4	**66**	12-16	12
18	6	4	**68**	13-16	12
20	6	4	**70**	14-16	10
22	7	6	**72**	15-17	12
24	8	8	**74**	14-18	12
26	7	6	**76**	14-18	12
28	8	4	**78**	15-18	12
30	8	6	**80**	16-19	16
32	8	8	**82**	14-20	14
34	8	6	**84**	15-20	12
36	8	6	**86**	16-20	14
38	8-9	8	**88**	17-20	16
40	9-10	8	**90**	18-21	14
42	10	6	**92**	16-22	14
44	10	8	**94**	16-22	14
46	11	10	**96**	16-22	16
48	12	12	**98**	17-22	14
50	10-12	10	**100**	18-23	14

4.2. The Bordered Double-Circulant Construction

While applying this construction, when k is even, we take $\beta = \gamma = 1$ and $\alpha = 0$. In this case, we may obtain codes whose minimum distance is greater than 2. When k is odd, we take $\beta = \gamma = 0$

and $\alpha = 1$. Since the first row of the matrix G has the minimum weight, this row determines the minimum distance of the code, which is 2. Otherwise, the generator matrix cannot generate a self-dual code. The minimum weights of the Euclidean self-dual codes that are obtained by using this construction method can be seen in Table 3.

In Table 3, $d_{BDC}(n)$ is the minimum weight of a Euclidean self-dual code of length n obtained by applying the bordered double-circulant construction.

Table 3. The Euclidean self-dual codes obtained by using the bordered double-circulant construction

length n	$d_{max}(n)$	$d_{BDC}(n)$	length n	$d_{max}(n)$	$d_{BDC}(n)$
4	2	2	**56**	12-14	12
8	4	4	**60**	12-14	12
12	4	4	**64**	12-16	12
16	5	4	**68**	13-16	12
20	6	4	**72**	15-17	12
24	8	8	**76**	14-18	12
28	8	6	**80**	16-19	12
32	8	8	**84**	15-20	12
36	8	8	**88**	17-20	16
40	9-10	8	**92**	16-22	14
44	10	8	**96**	16-22	16
48	12	12	**100**	18-23	16
52	10-12	10			

4.3. The Symmetric Construction

In this construction, we find all orthogonal symmetric $k \times k$ matrices for $k \leq 8$. When $k \geq 9$, the search field is too big for obtaining all orthogonal symmetric $k \times k$ matrices. We use random orthogonal symmetric 9×9 matrices to obtain a Euclidean self-dual code of length 18. Since investigating a matrix which is both orthogonal and symmetric is a restrictive criterion, we do our search up to length 18.

The minimum weights of the Euclidean self-dual codes that are obtained by using this construction method are given in Table 4. In this table, $d_S(n)$ is the minimum weight of a Euclidean self-dual code of length n obtained by applying the symmetric construction.

Table 4. The Euclidean self-dual codes obtained by using the symmetric construction

length n	$d_{max}(n)$	$d_{BDC}(n)$
2	2	2
4	2	2
6	3	2
8	4	4
10	4	2
12	4	4
14	4	4
16	5	4
18	6	4

5. CONCLUSION

Our aim in this work was to apply construction methods mentioned above for obtaining Euclidean self-dual codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$. Comparing our results with $d_{max}(n)$, we see that our results are slightly close to $d_{max}(n)$ when we use the double-circulant construction. Our results are mostly close to $d_{max}(n)$ except when $n \equiv 2(mod\ 4)$ in the bordered double-circulant construction. The limited results obtained in the symmetric construction are coincide with the results obtained in the double-circulant construction except when $n = 14$.

ACKNOWLEDGMENTS

We sincerely thank to all colleagues who have inspired and supported us during the preparation of the manuscript. This work was supported by İstanbul University Scientific Research Projects Coordination Unit. Project Number: 29539.

REFERENCES

[1] C. Bachoc, "Applications of coding theory to the construction of modular lattices," *J. Combin. Theory Ser. A,* vol. 78, pp. 92-119, 1997.

[2] K. Betsumiya and M. Harada, "Optimal self-dual codes over $\mathbb{F}_2 \times \mathbb{F}_2$ with respect to the Hamming weight," *IEEE Trans. Inform. Theory*, vol. 50, pp. 356-358, 2004.

[3] W. Bosma, J. Cannon and C. Playoust, "The Magma algebra system I: The user

language," *J Symbolic Comput.*, vol. 24, pp. 235-265, 1997.

[4] A. E. Brouwer, Bounds on the size of linear codes, in: V. S. Pless, W. C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, pp. 295-461, 1998.

[5] Y. Cengellenmis, A. Dertli and S. T. Dougherty, "Codes over an infinite family of rings with a Gray map," *Des. Codes Cryptogr.*, vol. 72, pp. 559-580, 2014.

[6] J. H. Conway, N. J. A. Sloane, "A New Upper Bound on Minimal Distance of Self-Dual Codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319-1333, 1990.

[7] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, "Type IV self-dual codes over rings," *IEEE Trans. Inform. Theory,* vol. 45, pp. 2345-2360, 1999.

[8] S. T. Dougherty, M. Harada and P. Solé, "Self-dual codes over rings and the Chinese remainder theorem," *Hokkaido Math. J.*, vol. 28, pp. 253-283, 1999.

[9] S. T. Dougherty, J. L. Kim, H. Liu, "Constructions of self-dual codes over finite commutative chain rings*," Int. J. Inf. Coding Theory 1*, vol. 2, pp. 171-190, 2010.

[10] J. Gao, Y. Wang, J. Li, "Bounds on covering radius of linear codes with Chinese Euclidean distance over the finite non chain ring $\mathbb{F}_2 + \upsilon\mathbb{F}_2$," *Inf. Process. Lett.*, vol. 138, pp. 22-26, 2018.

[11] J. Gildea, A. Kaya, R. Taylor, B. Yildiz, "Constructions for self-dual codes induced from group rings," *Finite Fields Appl.*, vol. 51, pp. 71—92, 2018.

[12] C. A. Castillo-Guillén, C. Rentería-Márquez, H. Tapia-Recillas, "Duals of constacyclic codes over finite local Frobenius non-chain rings of length 4," *Discrete Math.*, vol. 341, pp. 919-933, 2018.

[13] R. Hill, A First Course in Coding Theory, Oxford University Press, 1986.

[14] S. Karadeniz, S. T. Dougherty and B. Yildiz, "Constructing formally self-dual codes over R_k," *Discrete Appl. Math.*, vol. 167, pp. 188-196, 2014.

[15] B. Kim, Y. Lee, "Lee Weights of Cyclic Self-Dual Codes over Galois Rings of Characteristic p^2," *Finite Fields Appl.*, vol. 45, pp. 107-130, 2017.

[16] J. L. Kim, Y. Lee, "An Efficient Construction of Self-Dual Codes," *Bull. Korean Math. Soc.*, vol. 52, pp. 915-923, 2015.

[17] J. Li, A. Zhang, K. Feng, "Linear Codes over $\mathbb{F}_q[x]/(x^2)$ and $GR(p^2, m)$ Reaching the Griesmer Bound," *Des. Codes Cryptogr.*, vol. 86, pp. 2837-2855, 2018.

[18] S. Zhu, Y. Wang and M. Shi, "Some results on cyclic codes over $\mathbb{F}_2 + \upsilon\mathbb{F}_2$," *IEEE Trans. Inform. Theory*, vol. 56, pp. 1680-1684, 2010.