Bull. Korean Math. Soc. **49** (2012), No. 1, pp. 135–143
http://dx.doi.org/10.4134/BKMS.2012.49.1.135

CONSTRUCTION OF SELF-DUAL CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2$

Sunghyu Han, Heisook Lee, and Yoonjin Lee

Abstract. We present two kinds of construction methods for self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Specially, the second construction (respectively, the first one) preserves the types of codes, that is, the constructed codes from Type II (respectively, Type IV) is also Type II (respectively, Type IV). Every Type II (respectively, Type IV) code over $\mathbb{F}_2 + u\mathbb{F}_2$ of free rank larger than three (respectively, one) can be obtained via the second construction (respectively, the first one). Using these constructions, we update the information on self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$ of length 9 and 10, in terms of the highest minimum (Hamming, Lee, or Euclidean) weight and the number of inequivalent codes with the highest minimum weight.

1. Introduction

Codes over $\mathbb{Z}_4$ have had great attention since the monumental paper [5], and self-dual codes over $\mathbb{F}_2+u\mathbb{F}_2$ have also received some attention lately [1, 3] due to their importance. In fact, codes over $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ are related to lattices, and they have Gray maps [3]. Even though they are similar to each other, there are still some significant differences between them; one of the differences is that $x^2 + 1 = 0$ has a solution in $\mathbb{F}_2 + u\mathbb{F}_2$, but not in $\mathbb{Z}_4$. With this motivation we study the construction methods for producing self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Type II codes are also known to be a remarkable class of self-dual codes, therefore we are interested in finding construction methods preserving the type of codes.

In the present article, we present two kinds of construction methods for self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. In particular, the second construction (respectively, the first one) preserves the types of codes, that is, the constructed codes from Type II (respectively, Type IV) is also Type II (respectively, Type IV). In fact,

Received September 5, 2010; Revised September 10, 2011.
2010 *Mathematics Subject Classification.* Primary 94B60.
Key words and phrases. self-dual code, building-up construction, codes over ring, $\mathbb{F}_2+u\mathbb{F}_2$.
The first author was supported by the 2011 Education and Research Promotion Program of Korea University of Technology and Education.
The second author was supported by Institute of Mathematical Sciences at Ewha Womans University (2010).
The third author was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2011-0003516).

every self-dual code of free rank larger than one can be found via the first construction. Furthermore, every Type II (respectively, Type IV) code over $\mathbb{F}_2 + u\mathbb{F}_2$ of free rank larger than three (respectively, one) can be obtained via the second construction (respectively, the first one). Using these constructions, we update the information on self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length 9 and 10, in terms of the highest minimum (Hamming, Lee, or Euclidean) weight and the number of inequivalent codes with the highest minimum (Hamming, Lee, or Euclidean) weight. Our computational results are denoted in the bold face in Table 1.

Table 1 shows the current status of the classification of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length n, $1 \le n \le 16$ including our results. Basically, the data in Table 1 come from [7, Table 11] and [3, Table X]. The numbers of inequivalent Type I, II, IV-I, and IV-II codes are listed under "#I", "#II", "#IV-I", and "#IV-II", respectively. The highest value for the minimum Hamming weight followed by the number of self-dual codes with that Hamming weight is listed under "$d_H/\#$", and corresponding values are also given for the Lee and Euclidean weights under "$d_L/\#$" and "$d_E/\#$". Blanks are placed in the table when no possible codes of that type exist. Question marks indicate that the data is currently unknown.

TABLE 1. Self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $1 \le n \le 16$

n	#I	#II	#IV-I	#IV-II	$d_H/\#$	$d_L/\#$	$d_E/\#$
1	1				1/1	2/1	4/1
2	2		1		2/1	2/2	4/1
3	2				1/2	2/2	4/1
4	3	2	1	1	2/3	4/2	4/3
5	5				1/5	2/5	4/3
6	13		4		2/8	4/5	6/2
7	14				3/1	4/1	4/9
8	34	10	6	4	4/2	4/21	8/2
9	$\ge$ **46**				**2/** $\ge$ **3**	4/$\ge$ **2**	**4/** $\ge$ **32**
10	$\ge$ **157**		$\ge$ **24**		**2/** $\ge$ **111**	4/$\ge$ **82**	8/$\ge$ **4**
11	?				$\le$ 4/?	6/ $\ge$ 1	?
12	?	82	$\ge$ 1	14	$\le$ 5/?	8/1	?
13	?				$\le$ 5/?	6/ $\ge$ 1	?
14	?		$\ge$ 1		$\le$ 6/?	6/8	?
15	?				$\le$ 5/?	6/ $\ge$ 1	?
16	?	1894	?	157	$\le$ 7/?	8/ $\ge$ 21	?

From Table 1, we obtain the following theorem. More detailed description is given in Section 4.

Theorem 1.1. *For self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, the highest minimum Hamming weights and the highest minimum Euclidean weights are determined for the lengths* 9 *and* 10.

This paper is organized as follows. Section 2 gives basic definitions and known results about self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. In Section 3, we present two kinds of construction methods for self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. In Section 4, we provide our computational results for self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ obtained by using the constructions given in Section 3.

All the computations are made using Magma [2]. All the generator matrices and the symmetrized weight enumerators in this paper can be found in [6].

2. Preliminaries

Let R be the commutative ring $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}$ with $u^2 = 0$. We note that 1 and $1 + u$ are the only units of R.

A *linear code* C of length n over R is defined to be an R-submodule of R^n, and an element of C is called a *codeword*. Throughout this paper, we assume that C is a linear code over R unless specified. We define the inner product of x and y in R^n by $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. Then, the *dual code* $C^\perp$ of a code C is defined as follows: $C^\perp = \{y \in R^n \mid \langle x, y\rangle = 0 \text{ for all } x \in C\}$. A code C is called *self-dual* if $C = C^\perp$. Two codes over R are called *equivalent* if one can be obtained from the other by a permutation of coordinates followed by a possible multiplication of coordinates by $1 + u$. The *Lee composition* of a vector $x = (x_1, \ldots, x_n) \in R^n$ is defined as $(n_0(x), n_1(x), n_2(x))$ where $n_0(x)$ is the number of $x_i = 0$, $n_2(x)$ is the number of $x_i = u$, and $n_1(x) = n - n_0(x) - n_2(x)$. For $x \in R^n$, there are three kinds of weights. Namely, *Hamming weight*, *Lee weight*, and *Euclidean weight*. The Hamming weight $wt_H(x)$ of x is $wt_H(x) = n_1(x) + n_2(x)$, the Lee weight $wt_L(x)$ of x is $wt_L(x) = n_1(x) + 2n_2(x)$, and the Euclidean weight $wt_E(x)$ of x is $wt_E(x) = n_1(x) + 4n_2(x)$. For $x, y \in R^n$, the *Hamming distance* between x and y is $wt_H(x - y)$. The *minimum Hamming weight* d_H of C is the minimum nonzero Hamming weight of any codeword in C. The *minimum Lee weight* d_L and *minimum Euclidean weight* d_E of C are defined similarly.

A self-dual code over R is said to be *Type II* if the Lee weight of every codeword is a multiple of 4 and *Type I* otherwise. A self-dual code over R is said to be *Type IV* if the Hamming weight of every codeword is even. A Type IV code that is also Type I (respectively, Type II) is called a *Type IV-I* (respectively, *Type IV-II*) code.

Let C be a code over R. The *symmetrized weight enumerator* is defined as

$$swe_C(a, b, c) = \sum_{x \in C} a^{n_0(x)} b^{n_1(x)} c^{n_2(x)}.$$

The *Hamming weight enumerator* is defined as

$$W_C(x, y) = swe_C(x, y, y).$$

A code C over R is permutation equivalent to a code with generator matrix:

$$G = \begin{pmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{pmatrix},$$

where A, B_1, B_2, and D are matrices over $\mathbb{F}_2$. If C is self-dual, then we have more information about the generator matrix form as in the following proposition given in [3, Proposition 4.1].

Proposition 2.1. *The set of self-dual codes over R is equal to the set of codes over R which are permutation-equivalent to a code C with a generator matrix of the form*:

$$\begin{pmatrix} I_{k_1} + uB & A \\ 0 & uD \end{pmatrix}, \tag{1}$$

where A, B and D are matrices over $\mathbb{F}_2$ satisfying

(1) *B is symmetric,*
(2) *A and D are such that $C_{(1)} = C_{(2)}^{\perp}$ and $C_{(1)}$ is even, where $C_{(1)} = \{x \in \mathbb{F}_2^n \mid x + uy \in C \text{ for some } y \in \mathbb{F}_2^n\}$, $C_{(2)} = \{x \in \mathbb{F}_2^n \mid ux \in C\}$, $C_{(1)}$ has a generator matrix $\begin{pmatrix} I_{k_1} & A & B_1 \end{pmatrix}$, and $C_{(2)}$ has a generator matrix $\begin{pmatrix} I_{k_1} & A & B_1 \\ 0 & I_{k_1} & D \end{pmatrix}$.*

3. Construction methods

In this section we discuss two kinds of construction methods for self-dual codes over $R = \mathbb{F}_2 + u\mathbb{F}_2$. The following theorem is the first one, constructing self-dual codes of length increased by two.

Theorem 3.1. *Let $R = \mathbb{F}_2 + u\mathbb{F}_2$. Let C_0 be a self-dual code over R of length n and $G_0 = (\mathbf{r}_i)$ be a $k \times n$ generator matrix for C_0, where $\mathbf{r}_i$ is the i-th row of G_0, $1 \le i \le k$. Let c be in R such that $c^2 = 1$ in R. Let $\mathbf{x}$ be a vector in R^n with $\langle \mathbf{x}, \mathbf{x} \rangle = 1$. Suppose that $y_i = \langle \mathbf{r}_i, \mathbf{x} \rangle$ for $1 \le i \le k$. Then the following matrix*

$$G = \left[\begin{array}{cc|c} 1 & 0 & \mathbf{x} \\ \hline y_1 & cy_1 & \mathbf{r}_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & \mathbf{r}_k \end{array}\right]$$

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

Proof. The proof is very similar to that of [8, Proposition 2.1]. □

What follows shows that all self-dual codes over R of free rank larger than one can be obtained by the first construction given in Theorem 3.1.

Theorem 3.2. *Let C be a self-dual code over R of length $n + 2$ with free rank $k_1 \ge 2$ in (1). Then C is obtained from some self-dual code over R of length n by the construction method in Theorem 3.1 (up to equivalence).*

Proof. Using Proposition 2.1, the result can be proved in a similar way as given in [8, Proposition 2.2]. □

Lemma 3.3 ([4, Corollary 5.6])**.** *Let G be a generator matrix of a self-dual code C over R. Then C is Type IV if and only if the Hamming weight of every row in G is even.*

The following Corollary 3.4 shows that the first construction preserves the types of codes, that is to say, the constructed codes from Type IV is also Type IV, and every Type IV code over R of free rank larger than one can be found by the construction given in Theorem 3.5.

Corollary 3.4. *Let $R = \mathbb{F}_2 + u\mathbb{F}_2$, and $\mathbf{x}$ be a vector in R^n with $\langle \mathbf{x}, \mathbf{x} \rangle = 1$ and $w_H(\mathbf{x}) \equiv 1 \pmod 2$. Under the same notations as Theorem 3.1, if C_0 is of Type* **IV***, so is the code generated by the following matrix G :*

$$G = \left[\begin{array}{cc|c} 1 & 0 & \mathbf{x} \\ \hline y_1 & cy_1 & \mathbf{r}_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & \mathbf{r}_k \end{array}\right]$$

Conversely, if C is a Type IV code over R of length $n+2$ with free rank $k_1 \geq 2$ in (1)*, then C is obtained from some Type IV code over R of length n by the construction given as above* (*up to equivalence*)*.*

Proof. This follows from Theorem 3.1, Theorem 3.2 and Lemma 3.3. □

The second kind of construction is given as follows, a construction of self-dual codes of length increased by four. The second construction preserves the types of codes, that is, the constructed codes from Type II is also Type II.

Theorem 3.5. *Let $R = \mathbb{F}_2 + u\mathbb{F}_2$. Let C_0 be a Type II code over R of length $2n$ with n even, and $G_0 = (\mathbf{r}_i)$ be a $k \times 2n$ generator matrix for C_0, where $\mathbf{r}_i$ is the i-th row of G_0, $1 \leq i \leq k$. Let $\mathbf{x}_1$ and $\mathbf{x}_2$ be vectors in $R^{2\ell}$ such that $\langle \mathbf{x}_1, \mathbf{x}_2 \rangle = 0$ in R and $\langle \mathbf{x}_i, \mathbf{x}_i \rangle = 1$ in R and $w_L(\mathbf{x}_i) \equiv 3 \pmod 4$ for each $i = 1, 2$. For each $i, 1 \leq i \leq k$, let $s_i = \langle \mathbf{x}_1, \mathbf{r}_i \rangle$, $t_i = \langle \mathbf{x}_2, \mathbf{r}_i \rangle$, and $\mathbf{y}_i = (s_i, t_i, s_i + ut_i, us_i + t_i)$ be a vector of length 4. Then the following matrix*

$$G = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{x}_1 \\ 0 & 1 & 0 & 0 & \mathbf{x}_2 \\ \hline & \mathbf{y}_1 & & & \mathbf{r}_1 \\ & \vdots & & & \vdots \\ & \mathbf{y}_k & & & \mathbf{r}_k \end{array}\right]$$

generates a Type II code C over R of length $2n + 4$.

Proof. We can show that G generate a self-orthogonal code C and $|C| = 4^{n+2}$ in a similar way as given in [9, Proposition II.2], so C is self-dual.

We need to show that the type of a code is preserved as being Type II. In order to show that C is of Type II as well, we have to show that every codeword of C has Lee weight divisible by 4. We first note that for codewords x and y in C, if $w_L(x) \equiv w_L(y) \equiv 0 \pmod 4$, then $w_L(x+y) \equiv 0 \pmod 4$ by [3, Proposition 4.3]. It is thus sufficient to show that Lee weight of each row of the generator matrix G is divisible by four. There are 16 possible cases for $\mathbf{y}_i$. For each case, it is easy to show that $w_L(\mathbf{y}_i) \equiv 0 \pmod 4$; so, the Lee weight of each row of G is divisible by four. Let x be a row of G. We claim that $w_L(\alpha x) \equiv 0 \pmod 4$ for all $\alpha \in R$; this is obvious when α is $0, 1$, or $1+u$, and if $\alpha = u$, noting that $w_L(x) = n_1(x) + 2n_2(x) \equiv 0 \pmod 4$, we have $w_L(ux) = 2n_1(x) \equiv 0 \pmod 4$. Therefore, C is Type II, so the proof is complete. □

Remark 3.6. In Theorem 3.5, the choice $\mathbf{y}_i = (s_i, t_i, s_i + ut_i, us_i + t_i)$ is the unique choice in the following sense. According to Proposition II.2 in [9], we should find $\alpha, \beta \in R$ such that $\alpha^2 + \beta^2 + 1 = 0$ and the Lee weight $\mathbf{y}_i = (s_i, t_i, \alpha s_i + \beta t_i, \beta s_i + \alpha t_i)$ is a multiple of four for all s_i and t_i. Up to equivalence, the unique value is $\alpha = 1$ and $\beta = u$.

The following shows that every Type II code over R of free rank larger than three can be obtained by the second construction given in Theorem 3.5.

Theorem 3.7. *Let C be a Type II code over R of length $n+4$ with free rank $k_1 \geq 4$ in* (1)*. Then C is obtained from some Type II code over R of length n by the construction method in Theorem 3.5* (*up to equivalence*).

Proof. The result can be proved in a similar way as given in [9, Proposition II.3], so the proof is omitted. □

4. Computational results

In this section we first explain our computation method, and we provide computational results for self-dual codes over R of length 9 and 10 using the methods given in Section 3. We also compute their symmetrized weight enumerators. Using these constructions, we update the information on self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of length 9 and 10, in terms of the highest minimum (Hamming, Lee, or Euclidean) weight and the number of inequivalent codes with the highest minimum weight. This is summarized in Table 1.

The following lemma shows characterization for the generator matrices of self-dual codes with free rank $k_1 = 0$ or 1.

Lemma 4.1. *Let C be a self-dual code of length n over R. If $k_1 = 0$, then C has the generator matrix $G = uI_n$ up to equivalence. If $k_1 = 1$, then C has the following generator matrix* (*up to equivalence*) :

$$G = \begin{bmatrix} 1 & & \mathbf{a} \\ \mathbf{0}^T & uI_{n-2} & u\mathbf{b}^T \end{bmatrix},$$

where $\mathbf{0}$ *is a zero vector of length* $n-2$, $\mathbf{a}$ *is a binary vector of length* $n-1$, $\mathbf{b}$ *is a binary vector of length* $n-2$, I_{n-2} *is the identity matrix of order* $n-2$.

Proof. The case $k_1 = 0$ follows from Proposition 2.1, and the case $k_1 = 1$ can be shown by using Proposition 2.1 and a similar result as in [10, Lemma 3.1 (ii)]. □

Now we explain our classification method for self-dual codes. In the cases $k_1 = 0, 1$ we can use the generator matrices in an explicit form given in Lemma 4.1. For the case $k_1 \geq 2$, we first assume that we have representatives of all equivalence classes of self-dual codes of length n. Then applying the construction in Theorem 3.2 to each representative produces all self-dual codes of length $n+2$ up to equivalence.

Following the idea described as above, we show our computational results for the code length 9 and 10. We compute the symmetrized weight enumerators of self-dual codes over R instead of checking equivalence of codes because of their complexity.

4.1. Self-dual codes $\mathbb{F}_2 + u\mathbb{F}_2$ of length 9

In this subsection, we discuss self-dual codes over R of length 9. Our calculation shows that there are exactly 46 different symmetrized weight enumerators. It was known [3] that the highest minimum Hamming weight for self-dual codes over R of length 9 is ≤ 3. We find that the highest minimum Hamming weight for self-dual codes over R of length 9 is exactly 2, and there are exactly three different symmetrized weight enumerators for self-dual codes with the highest minimum Hamming weight 2. On the other hand, the highest minimum Lee weight for self-dual codes over R of length 9 was known to be 4, and only one code with the minimum Lee weight 4 was found in [3]. According to our computation, we find that there are exactly two different symmetrized weight enumerators for self-dual codes with the highest minimum Lee weight 4. No information has been given for the highest minimum Euclidean weight of self-dual codes of length 9, but we find that the highest minimum Euclidean weight for self-dual codes over R of length 9 is in fact 4, and there are exactly 32 different symmetrized weight enumerators for self-dual codes with the highest minimum Euclidean weight 4. All the symmetrized weight enumerators and a generator matrix corresponding to each symmetrized weight enumerator can be found in [6].

We therefore have the following theorem, and all the discussions given above are summarized in Table 1.

Theorem 4.2. *The highest minimum Hamming weight of self-dual codes over* R *of length* 9 *is* 2, *and the highest minimum Euclidean weight of self-dual codes over* R *of length* 9 *is* 4.

4.2. Self-dual codes $\mathbb{F}_2 + u\mathbb{F}_2$ of length 10

We discuss self-dual codes over R of length 10. Our computation shows that there are exactly 157 different symmetrized weight enumerators for self-dual codes over R of length 10. Previously [3], the highest minimum Hamming weight was known to be ≤ 3, but we show that the highest minimum Hamming weight is exactly 2, and there are exactly 111 different symmetrized weight enumerators for self-dual codes with the highest Hamming weight 2. The highest minimum Lee weight for self-dual codes over R of length 10 was known to be 4, and only 14 codes were found [4] for the highest minimum Lee weight 4. Our calculation shows that there are precisely 82 different symmetrized weight enumerators for self-dual codes of the highest minimum Lee weight 4. On the other hand, the highest minimum Euclidean weight for self-dual codes over R of length 10 was known to be 8, and only one code was found for the highest minimum Euclidean weight 8 [4]. From our calculation, we see that there are exactly 4 different symmetrized weight enumerators for self-dual codes with the highest minimum Euclidean weight 8. All the symmetrized weight enumerators and a generator matrix corresponding to each symmetrized weight enumerator are given in [6].

All the discussions given above are summarized in Table 1, and we have the following theorem.

Theorem 4.3. *The highest minimum Hamming weight of self-dual codes over R of length* 10 *is* 2.

References

[1] C. Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Combin. Theory Ser. A **78** (1997), no. 1, 92–119.

[2] J. Cannon and C. Playoust, *An Introduction to Magma*, University of Sydney, Sydney, Australia, 1994.

[3] S. T. Dougherty, P. Gaborit, M. Harada, and P. Solé, *Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45.

[4] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, and P. Solé, *Type IV self-dual codes over rings*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2345–2360.

[5] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

[6] S. Han, online available at http://kutacc.kut.ac.kr/~sunghyu/data/sdF2uF2.htm

[7] W. C. Huffman, *On the classification and enumeration of self-dual codes*, Finite Fields Appl. **11** (2005), no. 3, 451–490.

[8] J.-L. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A **105** (2004), no. 1, 79–95.

[9] ———, *Building-up constructions for self-dual codes*, preprint.

[10] H. Lee and Y. Lee, *Construction of self-dual codes over finite rings Z_{p^m}*, J. Combin. Theory Ser. A **115** (2008), no. 3, 407–422.

Sunghyu Han
School of Liberal Arts
Korea University of Technology and Education
Cheonan 330-708, Korea
E-mail address: sunghyu@kut.ac.kr

Heisook Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: hsllee@ewha.ac.kr

Yoonjin Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: yoonjinl@ewha.ac.kr