Classification of Extremal Type II $\mathbb{Z}_4$-codes of Length 24

Rowena Alma L. Betty[1] and Akihiro Munemasa[2]

[1] Institute of Mathematics, University of the Philippines-Diliman,
Quezon City 1101, Philippines
rabetty@math.upd.edu.ph
[2] Graduate School of Information Sciences, Tohoku University,
Sendai 980–8579, Japan
munemasa@math.is.tohoku.ac.jp

Abstract. In this paper, we give a classification of extremal Type II $\mathbb{Z}_4$-codes of length 24. This is equivalent to a classification of 4-frames of the Leech lattice up to the action of the automorphism group.

Keywords: self-dual code · Type II code · free code · extremal code · classification

1 Introduction

The study of self-dual codes has gained much attention because of their rich mathematical theory. One particular problem is to construct self-dual codes with largest minimum weight among self-dual codes of a given length and classify them. Type II codes are a special class of self-dual codes. In [13], it was found that there are 13 inequivalent extremal Type II codes over $\mathbb{Z}_4$ of length 24 whose reductions modulo 2, is the binary extended Golay code. All extremal Type II codes over $\mathbb{Z}_4$ of length 24 with an automorphism of prime order $p \geq 5$ are classified in [12]. In [5], extremal Type II codes over $\mathbb{Z}_4$ of length 32 and 40 were constructed using a doubling method and a generalization of the method by Harada in [8].

In [13], Rains studied self-dual codes over $\mathbb{Z}_4$, via their residue codes. This method reduces the problem of finding optimal codes over $\mathbb{Z}_4$ to a problem of enumerating lifts of a given residue code, which in this case, is a doubly-even binary code. A precise description of Rains' algorithm for classifying self-dual codes over $\mathbb{Z}_4$ with a given residue code was given in [2]. We will apply this for Type II codes over $\mathbb{Z}_4$ and give a classification of extremal Type II codes of length 24. By [10, Lemma 2], this is equivalent to a classification of 4-frames in the Leech lattice up to the action of the automorphism group. Since every 4-frame of the Leech lattice gives rise to a Virasoro frame of the moonshine vertex operator algebra $V^\natural$ (see [7]), our result has implications in the structure of $V^\natural$ as a framed vertex operator algebra. In fact, according to [9], those Virasoro frames obtained from a 4-frame of the Leech lattice are precisely the ones whose structure codes are extended doublings of the residue codes.

2 Preliminaries

Let $\mathbb{Z}_m$ denote the ring of integers modulo m. A (linear) $\mathbb{Z}_m$-code of length n is a $\mathbb{Z}_m$-submodule of $\mathbb{Z}_m^n$. Two codes $\mathcal{C}$ and $\mathcal{C}'$ over $\mathbb{Z}_m$ are equivalent if there exists a monomial $(\pm 1, 0)$-matrix P such that $\mathcal{C}' = \mathcal{C} \cdot P = \{c \cdot P \mid c \in \mathcal{C}\}$. The automorphism group $\mathrm{Aut}(\mathcal{C})$ is the group of monomials that preserves $\mathcal{C}$. We denote by $\mathbb{Z}_m^k G$ the $\mathbb{Z}_m$-code with generator matrix G.

The Hamming weight of $x \in \mathbb{Z}_m^n$ denoted by $\mathrm{wt}(x)$ is the number of its nonzero components. The Euclidean weight $\mathrm{wt}_E(x)$ of an element $x \in \mathbb{Z}_4$ is defined by $\mathrm{wt}_E(0) = 0$, $\mathrm{wt}_E(1) = \mathrm{wt}_E(3) = 1$ and $\mathrm{wt}_E(2) = 4$. The Euclidean weight of a vector in $\mathbb{Z}_4^n$ is the integral sum of the Euclidean weights of its components. The minimum Hamming and Euclidean weight of a code $\mathcal{C}$ are the smallest Hamming and Euclidean weights among all nonzero codewords of $\mathcal{C}$, respectively.

We equip $\mathbb{Z}_4^n$ with the standard inner product $x \cdot y = \sum_{i=1}^n x_i y_i$, for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{Z}_4^n$. The dual of a $\mathbb{Z}_4$-code $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{v \in \mathbb{Z}_4^n \mid u \cdot v = 0 \text{ for all } u \in \mathcal{C}\}$. We say that a code $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and self-dual if $\mathcal{C} = \mathcal{C}^\perp$. An even code is a subclass of the class of self-orthogonal codes over $\mathbb{Z}_4$, all of whose codewords have Euclidean weights divisible by 8. When an even code over $\mathbb{Z}_4$ is self-dual, then it is called Type II. The minimum Euclidean weight d_E of a Type II code of length n satisfies

$$d_E \leq 8 \left\lfloor \frac{n}{24} \right\rfloor + 8$$

by [1]. A Type II code meeting this bound with equality is said to be an extremal code.

There are two binary codes $\mathrm{res}(\mathcal{C})$ and $\mathrm{tor}(\mathcal{C})$ associated with a $\mathbb{Z}_4$-code $\mathcal{C}$:

$$\mathrm{res}(\mathcal{C}) = \{c \bmod 2 \mid c \in \mathcal{C}\} \text{ and } \mathrm{tor}(\mathcal{C}) = \{c \bmod 2 \mid c \in \mathbb{Z}_4^n,\ 2c \in \mathcal{C}\}.$$

The codes $\mathrm{res}(\mathcal{C})$ and $\mathrm{tor}(\mathcal{C})$ are called the residue and torsion codes of $\mathcal{C}$, respectively. A $\mathbb{Z}_4$-code $\mathcal{C}$ is said to be free if $\mathrm{res}(\mathcal{C}) = \mathrm{tor}(\mathcal{C})$. In this case, the code $\mathcal{C}$ is called a lift of $\mathrm{res}(\mathcal{C})$. If $\mathcal{C}$ is self-dual, then $\mathrm{res}(\mathcal{C})$ is a binary doubly-even code with $\mathrm{tor}(\mathcal{C}) = \mathrm{res}(\mathcal{C})^\perp$ (see [6]). Moreover, if $\mathcal{C}$ is Type II, then $\mathrm{res}(\mathcal{C})$ contains the all-ones vector $\mathbf{1}$ by [11, Lemma 2.2].

Let K be a field of characteristic 2, and let n a positive integer. We denote by $\mathrm{Sym}_n(K)$ (and $\mathrm{Alt}_n(K)$) by the set of symmetric (resp. alternating) matrices of order n with entries in K. For a square matrix A, we denote by $\mathrm{Diag}(A)$ the diagonal matrix whose diagonal entries are those of A. Then

$$\mathrm{Alt}_n(K) = \{A \in \mathrm{Sym}_n(K) \mid \mathrm{Diag}(A) = 0\}.$$

We state here the following lemma used to prove Lemma 3.

Lemma 1 ([3, Lemma 3.2]). *Let* $\mathrm{char}\, K = 2$, $\mathrm{rank}\, A = m$ *for* $A \in M_{m \times n}(K)$ *and the vector* $\mathbf{1}_n$ *does not belong to the row space of* A. *Then the map*

$$\begin{aligned} \overline{\Phi}_A \colon\ M_{m\times n}(K) &\to \mathrm{Sym}_m(K) \oplus K^m \\ N &\mapsto (AN^\top + NA^\top + \mathrm{Diag}(AN^\top), \mathbf{1}N^\top) \end{aligned}$$

is surjective.

3 The Set of $\mathbb{Z}_4$-Codes with Given Residue

In this section, given a binary doubly even code C, we investigate how $\mathrm{Aut}(C)$ acts on the set of Type II $\mathbb{Z}_4$-codes having the residue code C.

Let k and n be positive integers with $2k \leq n$, and set $\mathcal{M} = M_{k\times n}(\mathbb{Z}_2)$. Let C be a k-dimensional doubly-even binary code of length n containing $\mathbf{1}_n$, with generator matrix $A \in \mathcal{M}$. Moreover, let

$$\begin{bmatrix} A \\ B \end{bmatrix}$$

be a generator matrix of $C^\perp$, where $B \in M_{(n-2k)\times n}(\mathbb{Z}_2)$. Thus,

$$AA^\top = 0, \tag{1}$$
$$BA^\top = 0, \tag{2}$$
$$\mathbf{1}B^\top = 0. \tag{3}$$

Define

$$V_0 = \{M \in \mathcal{M} \mid MA^\top + AM^\top = 0\}, \tag{4}$$
$$W_0 = \langle \{M \in \mathcal{M} \mid MA^\top = 0\}, \{AE_{ii} \mid 1 \leq i \leq n\}\rangle, \tag{5}$$
$$U_0 = \{M \in V_0 \mid \mathrm{Diag}((A+J)M^\top) = 0\}, \tag{6}$$
$$W = W_0 \oplus \{0\} \subseteq W_0 \oplus \mathbb{Z}_2, \tag{7}$$
$$U = U_0 \oplus \mathbb{Z}_2, \tag{8}$$

where E_{ij} is the matrix which has 1 in the (i,j)-entry and zeros in all other entries. Define matrices F_{ij} over $\mathbb{Z}_4$ by $F_{ij} = I + 2E_{ij}$.

Lemma 2. *We have $W_0 \subseteq U_0$ and $W \subseteq U$.*

As in [2], we denote by $\iota : \mathbb{Z}_2 \to \mathbb{Z}_4$ the mapping defined by $\iota(0) = 0$ and $\iota(1) = 1$. We also define the mapping $\alpha : \mathbb{Z}_4 \to \mathbb{Z}_8$ by $\alpha(x) = x$ for $x \in \{0,1,2,3\}$. We use the same symbol ι and α to denote its elementwise application to matrices. Observe that for $x \in \mathbb{Z}_4$, $\alpha(x)^2 = \mathrm{wt}_E(x) \bmod 8$. The following lemma shows that a doubly even binary code containing $\mathbf{1}$ can be lifted to a free even code over $\mathbb{Z}_4$.

Lemma 3. *Let C be a doubly even binary code of length n containing $\mathbf{1}_n$, where $n \equiv 0 \pmod 8$. Let $x \in C \setminus \{0\}$, and let $a \in \mathbb{Z}_4^n$ be such that $a \bmod 2 = x$ and $\mathrm{wt}_E(a) \equiv 0 \pmod 8$. Then there exists a free even $\mathbb{Z}_4$-code $\mathcal{C}$ such that $a \in \mathcal{C}$ and $\mathrm{res}(\mathcal{C}) = C$.*

By Lemma 3, the code C can be lifted to a free even $\mathbb{Z}_4$-code. This means that there exists $\tilde{A} \in M_{k\times n}(\mathbb{Z}_4)$ such that

$$\begin{aligned} \tilde{A}\tilde{A}^\top &= 0, \\ 2\tilde{A} &= 2\iota(A), \\ \mathrm{Diag}(\alpha(\tilde{A})\alpha(\tilde{A}^\top)) &= 0. \end{aligned}$$

Then the $\mathbb{Z}_4$-code generated by

$$\begin{bmatrix} \tilde{A} \\ 2\iota(B) \end{bmatrix}$$

is a Type II code by (2) and (3).

Lemma 4. *For $M \in \mathcal{M}$, the code $\mathbb{Z}_4^k \left[\tilde{A} + 2\iota(M)\right]$ is even if and only if $M \in U_0$. In particular, the code*

$$C_M = \mathbb{Z}_4^{n-k} \begin{bmatrix} \tilde{A} + 2\iota(M) \\ 2\iota(B) \end{bmatrix} \tag{9}$$

is Type II if and only if $M \in U_0$.

Suppose $P \in \mathrm{Aut}(C)$. Since A has full row rank, there exists a unique matrix $E_1(P) \in \mathrm{GL}(k, \mathbb{Z}_2)$ such that

$$AP = E_1(P)A.$$

Also, there exists a unique matrix $E_2(P) \in \mathcal{M}$ such that

$$2\iota(E_2(P)) = \iota(E_1(P)^{-1})\tilde{A}\iota(P) - \tilde{A}.$$

It was shown in [2] that the group $\mathrm{Aut}(C)$ acts on V/W linearly by

$$((M, a) + W)^P = (E_1(P)^{-1}MP + aE_2(P), a) + W, \tag{10}$$

where $V = V_0 \oplus \mathbb{Z}_2$. We have the following lemma from [2].

Lemma 5. *For $M \in \mathcal{M}$, $P \in \mathrm{Aut}(C)$ and $\Lambda \subseteq \{1, 2, \ldots, n\}$, we have*

$$\begin{aligned} &\mathbb{Z}_4^{n-k} \begin{bmatrix} \tilde{A} + 2\iota(M) \\ 2\iota(B) \end{bmatrix} \left(\prod_{i \in \Lambda} F_{ii} \right) \iota(P) \\ &= \mathbb{Z}_4^{n-k} \begin{bmatrix} \tilde{A} + 2\iota(E_1(P)^{-1}MP + E_2(P) + A\sum_{i \in \Lambda^P} E_{ii}) \\ 2\iota(B) \end{bmatrix}. \end{aligned}$$

Now, the next theorem is an analogue of [2, Theorem 1] for Type II $\mathbb{Z}_4$-codes.

Theorem 1. *Let C be a binary doubly-even code containing $\mathbf{1}$ with generator matrix A. Define V_0, W_0, U_0, W, U by (4)–(8). Then the action of $\mathrm{Aut}(C)$ given by (10) leaves the subset*

$$\Omega' = \{(M, 1) + W \mid M \in U_0\}$$

invariant, and the orbits of $\mathrm{Aut}(C)$ on Ω' are in one-to-one correspondence with the equivalence classes of Type II codes over $\mathbb{Z}_4$ with residue code C.

4 Extremal Type II $\mathbb{Z}_4$-Codes

We continue to use the notation fixed in the beginning of Section 3, that is, (1)–(8). From the previous section, we know that every Type II $\mathbb{Z}_4$-codes whose residue code is a doubly-even code $C = \mathbb{Z}_2^k A$ can be found as an element of U/W, up to column negation, in the sense (9) above.

For a subset $T \subseteq \{1, \ldots, n\}$ of coordinates and a vector $v \in \mathbb{Z}_2^n$, denote by $v|_T$ the restriction $(v_i)_{i \in T}$ to T. The punctured code $C|_T \subseteq \mathbb{Z}_2^{|T|}$ is defined as

$$C|_T = \{v|_T \mid v \in C\}.$$

For $x \in \mathbb{Z}_2^k$, define

$$S(x) = \{1, \ldots, n\} \setminus \mathrm{supp}(xA),$$

where $\mathrm{supp}(xA)$ denote the support of xA.

Lemma 6. *If $0 \neq x \in \mathbb{Z}_2^k$, then*

$$\{(xM)|_{S(x)} \mid M \in W_0\} = C^\perp|_{S(x)}.$$

For $x \in \mathbb{Z}_2^k$, define an affine subspace $H(x)$ of $\mathbb{Z}_2^{|S(x)|}$ by

$$H(x) = \left(\frac{(\iota(x)\tilde{A})_i}{2} \bmod 2 \right)_{i \in S(x)} + C^\perp|_{S(x)},$$

where $\tilde{A} \bmod 2 = A$.

Lemma 7. *If $0 \neq x \in \mathbb{Z}_2^k$ with $\mathrm{wt}(xA) \equiv 0 \pmod 8$, then there exists an element $M_x \in U_0$ such that $(xM_x)|_{S(x)} \in H(x)$.*

For each $x \in \mathbb{Z}_2^k$, define

$$K_0(x) = \{M \in U_0 \mid (xM)|_{S(x)} \in C^\perp|_{S(x)}\}, \tag{11}$$

$$K(x) = \langle K_0(x) \oplus \{0\}, (M_x, 1) \rangle. \tag{12}$$

Then by Lemma 6, we have $W \subseteq K(x)$, and obviously $K(x) \subseteq U$.

Lemma 8. *For $0 \neq x \in \mathbb{Z}_2^k$ with $\mathrm{wt}(xA) \equiv 0 \pmod 8$ and $M \in U_0$, the following are equivalent:*

(i) $(M, 1) + W \in K(x)/W$,
(ii) $(xM)|_{S(x)} \in H(x)$.

Lemma 9. *Let $M \in U_0$. Then the code C_M defined in (9) has a codeword of Euclidean weight 8 reducing modulo 2 to a codeword of Hamming weight 8 if and only if*

$$(M, 1) + W \in \bigcup_{\substack{x \in \mathbb{Z}_2^k \\ \mathrm{wt}(xA)=8}} K(x)/W.$$

By definition, a Type II $\mathbb{Z}_4$-code of length 24 is called extremal if its minimum Euclidean weight is 16. Since Euclidean weights are divisible by 8 for codewords in Type II codes, a Type II $\mathbb{Z}_4$-code of length 24 is extremal if and only if it has no codeword of Euclidean weight 8. Lemma 9 allows us to discard those non-extremal codes which contain a codeword of Euclidean weight 8 reducing modulo 2 to a codeword of Hamming weight 8. Note that we need to assume that the dual $C^\perp$ of C has minimum Hamming weight at least 4, since otherwise the torsion code of a Type II $\mathbb{Z}_4$-code $\mathcal{C}$ with $\mathrm{res}(\mathcal{C}) = C$ will have a codeword of Hamming weight 2, and hence $\mathcal{C}$ contains a codeword of composition $2^2 0^{22}$. Note also that a Type II $\mathbb{Z}_4$-code of length 24 may contain a codeword of composition $(\pm 1)^4 2^1 0^{19}$, of Euclidean weight 8. Such a code needs to be eliminated during the classification of extremal Type II $\mathbb{Z}_4$-codes of length 24. As a result of computer enumeration, we obtain the following classification theorem.

Theorem 2. *There are 4,744 inequivalent extremal Type II $\mathbb{Z}_4$-codes of length 24.*

In Table 1, we list the number of inequivalent extremal Type II $\mathbb{Z}_4$-codes $\mathcal{C}$ of length 24. It is known that a residue code C of an extremal Type II $\mathbb{Z}_4$-code of length 24 must be a binary doubly-even code containing $\mathbf{1}$ whose dual $C^\perp$ has minimum Hamming weight at least 4 and $\dim C \geq 6$, and there is a unique Type II $\mathbb{Z}_4$-code of length 24 whose residue code has dimension 6 (see [9]).

We have also examined which of the codes we classified have an automorphism of order p for $p = 23, 11, 7, 5$. Such codes have been classified by Huffman [12], and the numbers agree with ours, except for $p = 5$. In [12, Theorem 3.5], it is claimed that there are 28 extremal Type II $\mathbb{Z}_4$-codes of length 24 with an automorphism of order 5. Our result shows, however, that there are only 22 such codes. In the notation of [12], the codes $\mathcal{C}_{24}, \mathcal{C}_{25}, \mathcal{C}_{28}$ are equivalent to $\mathcal{C}_{23}$, and the codes $\mathcal{C}_{39}, \mathcal{C}_{40}, \mathcal{C}_{44}$ are equivalent to $\mathcal{C}_{38}$.

All computer calculations in this paper were done with the help of MAGMA [4].

Table 1. Number of inequivalent extremal Type II $\mathbb{Z}_4$-codes of length 24

$\dim \mathrm{res}(\mathcal{C})$	6	7	8	9	10	11	12
$\#(\mathrm{res}(\mathcal{C}))$	1	7	32	60	49	21	9
$\#\mathcal{C}$	1	5	29	171	755	1880	1903

References

1. C. Bachoc, A. Bonnecaze, B. Mourrain and P. Solé, Type II codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory, 43, 969–976 (1997).

2. R.A.L. Betty and A. Munemasa, Classification of self-dual codes of length 20 over $\mathbb{Z}_4$ and length at most 18 over $\mathbb{F}_2 + u\mathbb{F}_2$, Lecture Notes in Computer Science, 11929, 64–77 (2019).
3. R.A.L. Betty and A. Munemasa, Mass formula for self-orthogonal codes over $\mathbb{Z}_{p^2}$, Journal of Combinatorics, Information and System Sciences, 34, 51–66 (2009).
4. W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput., 24, 235–265 (1997).
5. K.H. Chan, Three new methods for construction of extremal Type II $\mathbb{Z}_4$-codes. Ph.D. Thesis, University of Illinois at Chicago, Illinois, U.S.A. (2012)
6. J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, J. Combin. Theory, Ser. A, 62, 30–45 (1993).
7. C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the moonshine module, Proc. Symp. Pure. Math. 56 II , 295–316 (1994).
8. M. Harada. On the residue codes of extremal Type II $\mathbb{Z}_4$-codes of lengths 32 and 40, Discrete Mathematics, 311, 2148–2157, (2011).
9. M. Harada, C.H. Lam and A. Munemasa, Residue codes of extremal Type II $\mathbb{Z}_4$-codes and the moonshine vertex operator algebra, Mathematische Zeitschrift, 274, 685–700, (2013).
10. M. Harada, A. Munemasa and B. Venkov, Classification of ternary extremal self-dual codes of length 28, Math. Comp. 78, 1787–1796 (2009).
11. M. Harada, P. Solé and P.Gaborit, Self-dual codes over $\mathbf{Z}_4$ and unimodular lattices: a survey, Algebras and combinatorics (Hong Kong, 1997), 255–275, Springer, Singapore (1999).
12. W.C. Huffman, Decompositions and extremal Type II codes over $\mathbb{Z}_4$ IEEE Trans. Inform. Theory, 44, 800–809 (1998).
13. E.M. Rains, Optimal self-dual codes over $\mathbb{Z}_4$, Discrete Mathematics, 203, 215–228 (1999).