Extremal Type II $\mathbb{Z}_4$-Codes of Lengths 56 and 64

Masaaki Harada*

July 12, 2009

Abstract

Type II $\mathbb{Z}_4$-codes are a remarkable class of self-dual $\mathbb{Z}_4$-codes. A Type II $\mathbb{Z}_4$-code of length n exists if and only if n is divisible by eight. For lengths up to 48, extremal Type II $\mathbb{Z}_4$-codes are known. In this note, extremal Type II $\mathbb{Z}_4$-codes of lengths 56 and 64 are constructed for the first time.

1 Introduction

Let $\mathbb{Z}_4$ $(= \{0, 1, 2, 3\})$ denote the ring of integers modulo 4. A $\mathbb{Z}_4$-code C of length n is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$. Two codes are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{Z}_4^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ where $x \cdot y = x_1y_1 + \cdots + x_ny_n$ for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. A code C is *self-dual* if $C = C^\perp$. The Euclidean weight of a codeword x is $\sum_{i=1}^n \min\{x_i^2, (4 - x_i)^2\}$. The minimum Euclidean weight $d_E(C)$ of C is the smallest Euclidean weight among all nonzero codewords of C.

The notion of Type II $\mathbb{Z}_4$-codes was first defined in [1] as self-dual codes containing a (± 1)-vector and with the property that all Euclidean weights are divisible by eight. Then it was shown in [5] that, more generally, the

*Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan and PRESTO, Japan Science and Technology Agency, Kawaguchi, Saitama 332–0012, Japan. email: mharada@sci.kj.yamagata-u.ac.jp

condition of containing a (± 1)-vector is redundant. Therefore *Type II codes* are self-dual codes which have the property that all Euclidean weights are divisible by eight. This is a remarkable class of self-dual $\mathbb{Z}_4$-codes, one reason being that any Type II code gives an even unimodular lattice. A Type II $\mathbb{Z}_4$-code of length n exists if and only if $n \equiv 0 \pmod 8$ [1].

The concept of extremality for the Euclidean weights was introduced in [1]. It was shown in [1] that the minimum Euclidean weight $d_E(C)$ of a Type II code C of length n is bounded by

$$d_E(C) \leq 8\left\lfloor \frac{n}{24} \right\rfloor + 8.$$

A Type II code meeting this bound with equality is called *extremal*. At lengths 8 and 16, all Type II codes are extremal. At lengths $24, 32$ and 40, a large number of extremal Type II codes are known (cf. [7]). At length 48, only two inequivalent extremal Type II codes are known [6]. For lengths $n \geq 56$, no extremal Type II code is known.

The aim of this note is to establish the following theorem.

Theorem 1. *There is an extremal Type II $\mathbb{Z}_4$-code for lengths* 56 *and* 64.

Thus the existence of extremal Type II $\mathbb{Z}_4$-codes is known for lengths up to 64. It is a question to determine whether an extremal Type II $\mathbb{Z}_4$-code exists for length 72. We remark that the existence of a binary extremal Type II (doubly even self-dual) code of length 72 and a 72-dimensional extremal Type II (even unimodular) lattice is a long-standing open question.

2 Construction

Every $\mathbb{Z}_4$-code C of length n has two binary codes $C^{(1)}$ and $C^{(2)}$ associated with C:

$$C^{(1)} = \{c \pmod 2 \mid c \in C\} \text{ and } C^{(2)} = \{c \in \mathbb{F}_2^n \mid 2c \in C\}.$$

The binary codes $C^{(1)}$ and $C^{(2)}$ are called the residue and torsion codes of C, respectively. If C is a self-dual $\mathbb{Z}_4$-code then $C^{(1)}$ is a binary doubly even code with $C^{(2)} = {C^{(1)}}^{\perp}$ [4]. Moreover, if C is Type II then $C^{(1)}$ contains the all-ones vector, or equivalently, $C^{(2)}$ is even.

In this note, we employ the following method of construction of Type II $\mathbb{Z}_4$-codes, which was given in [8]. Suppose that n is divisible by eight. Let

C_1 be a binary doubly even $[n,k]$ code containing the all-ones vector. Without loss of generality, we may assume that C_1 has generator matrix of the following form:

$$G_1 = \begin{pmatrix} A & \tilde{I_k} \end{pmatrix}, \tag{1}$$

where A is a $k \times (n-k)$ matrix which has the property that the first row is the all-ones vector, $\tilde{I_k} = \begin{pmatrix} 1 & \cdots & 1 \\ 0 & & \\ \vdots & I_{k-1} & \\ 0 & & \end{pmatrix}$, and I_{k-1} denotes the identity matrix of order $(k-1)$. This means that the first row of G_1 is the all-ones vector. Since C_1 is self-orthogonal, the matrix G_1 can be extended to a generator matrix of $C_1^{\perp}$ as follows:

$$\begin{pmatrix} G_1 \\ D \end{pmatrix}.$$

Then there are $2^{1+k(k-1)/2}$ $k \times k$ $(1,0)$-matrices B such that the following matrices

$$\begin{pmatrix} A & \tilde{I_k} + 2B \\ & 2D \end{pmatrix} \tag{2}$$

are generator matrices of Type II $\mathbb{Z}_4$-codes C, where we regard the matrices as matrices over $\mathbb{Z}_4$ [8]. In this case, of course, C_1 is the residue code of C. For each Type II code C, there is a Type II code containing the all-ones vector, which is equivalent to C. Hence, without loss of generality, we may assume that the first row of B is the zero vector.

We investigate the residue and torsion codes of extremal Type II $\mathbb{Z}_4$-codes.

Lemma 2. *Let C be an extremal Type II $\mathbb{Z}_4$-code of length n. Then the torsion code $C^{(2)}$ has minimum weight $d \geq 2[n/24] + 2$.*

Proof. Any codeword x of $C^{(2)}$ corresponds to a codeword $2x$ of C. Hence the torsion code $C^{(2)}$ has minimum weight $d \geq d_E(C)/4$. □

Lemma 3. *Let C be an extremal Type II $\mathbb{Z}_4$-code of length* 56 *(resp.* 64*). Then the dimension of the residue code $C^{(1)}$ is at least* 12 *(resp.* 13*).*

Proof. By the above lemma, the torsion codes of extremal Type II $\mathbb{Z}_4$-codes of lengths 56 and 64 have minimum weight $d \geq 6$. If a binary $[56, k, 6]$ code exists then $k \leq 44$ and if a binary $[64, k, 6]$ code exists then $k \leq 51$ (cf. [3]). Hence the dimensions of the torsion codes $C^{(2)}$ $(= C^{(1)^\perp})$ of extremal Type II $\mathbb{Z}_4$-codes of lengths 56 and 64 must be at most 44 and 51, respectively. □

We describe how extremal Type II $\mathbb{Z}_4$-codes of lengths $n = 56$ and 64 were constructed. We first constructed a binary doubly even $[n, n/4, 20]$ code B_n which has the property that B_n contains the all-ones vector and $B_n^\perp$ has minimum weight at least 6. The latter condition is necessary by Lemma 2. These codes B_{56} and B_{64} were constructed by considering quasi-cyclic codes. The codes B_n $(n = 56, 64)$ have generator matrices of the following form:

$$(3) \qquad \begin{pmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 & & \\ & R_1 & & & R_2 & & & R_3 & & \tilde{I_{n/4}} \end{pmatrix},$$

where R_i are $(\frac{n}{4} - 1) \times \frac{n}{4}$ circulant matrices $(i = 1, 2, 3)$. For the codes B_{56} and B_{64}, the first rows r_i of R_i $(i = 1, 2, 3)$ in (3) are as follows:

$r_1 = (00100110001100), r_2 = (10010010001100), r_3 = (10101110011110),$
$r_1 = (1011110000101011), r_2 = (0011010010110001), r_3 = (0101011011111110),$

respectively. These codes B_{56} and B_{64} have weight enumerators

$$1 + 756y^{20} + 4095y^{24} + 6680y^{28} + \cdots + y^{56} \text{ and}$$
$$1 + 240y^{20} + 3600y^{24} + 16144y^{28} + 25566y^{32} + \cdots + y^{64},$$

respectively.

As described above, starting from generator matrices (3) of the binary doubly even codes B_{56} and B_{64}, there are $2^{1+k(k-1)/2}$ $(k = 14$ and 16) Type II $\mathbb{Z}_4$-codes with generator matrices of the form (2), respectively. These codes can be constructed by choosing suitable matrices B in (2). By a random search, we have found matrices B such that the matrices (2) generate extremal Type II $\mathbb{Z}_4$-codes C_{56} and C_{64} of lengths 56 and 64. A generator matrix of C_{56} (resp. C_{64}) is listed in Figure 1 (resp. Figure 2) where we only list the 14×56 (resp. 16×64) matrix $(A \;\; \tilde{I_k} + 2B)$ in (2) since the lower part in (2) can be obtained from the matrix.

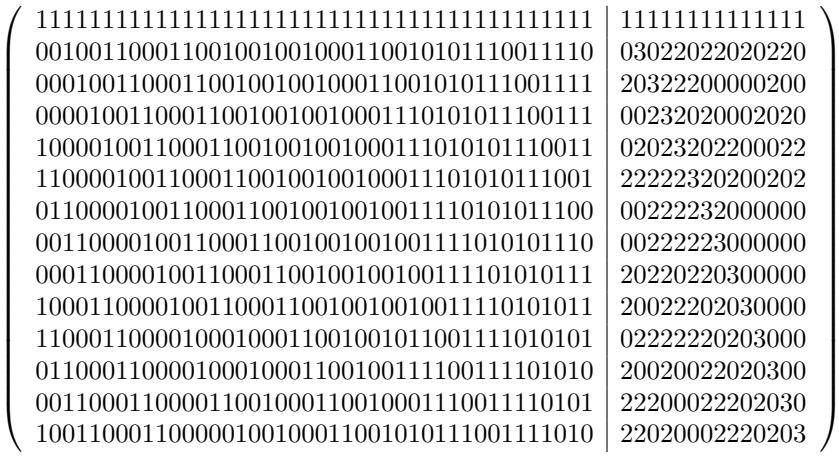

Figure 1: An extremal Type II $\mathbb{Z}_4$-code of length 56

Let C be a Type II $\mathbb{Z}_4$-code and let $A_4(C)$ be the lattice obtained from C by Construction A (cf. [1]). Then $A_4(C)$ is an even unimodular lattice. Moreover, C is an extremal Type II $\mathbb{Z}_4$-code of length 56 (resp. 64) if and only if $A_4(C)$ has minimum norm 4 and kissing number 112 (resp. 128). By checking this using MAGMA [2], the extremality of the new codes C_{56} and C_{64} was verified. We verified by MAGMA that both codes C_{56} and C_{64} have minimum Lee weight 12 (see [1] for the definition of the minimum Lee weight).

Acknowledgment. The author would like to thank Akihiro Munemasa for helpful discussions.

References

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

[2] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

$$\left(\begin{array}{l|l}
1111111111111111111111111111111111111111111111111111 & 1111111111111111 \\
1011110000101011001101001011000101010111111111110 & 2320002002202020 \\
1101111000010101100110100101100000101011011111111 & 0030200202222002 \\
1110111100001010010011010010110010010101101111111 & 2023020200020000 \\
0111011110000101001001101001011011001010111011111 & 2022302022220200 \\
1011101111000010000100110100101111100101011011111 & 0202230202200020 \\
0101110111100001100010011010010111110010101101111 & 0220223000202222 \\
1010111011110000110001001101001011111001010111011 & 2220022300000000 \\
0101011101111000011000100110100111111100101011011 & 0220000230000000 \\
0010101110111100101100010011010011111110010101101 & 2202200023000000 \\
0001010111011110010110001001101001111111001010110 & 2022020002300000 \\
0000101011101111001011000100110110111111110010101 & 0202020200230000 \\
1000010101110111100101100010011011011111111001010 & 0202020020023000 \\
1100001010111011010010110001001101101111111100101 & 0202000202002300 \\
1110000101011101101001011000100110111011111110010 & 2220202220200230 \\
1111000010101110110100101100010001011011111111001 & 0022020022020023
\end{array}\right)$$

Figure 2: An extremal Type II $\mathbb{Z}_4$-code of length 64

[3] A.E. Brouwer, "Bounds on the size of linear codes," in Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 295–461.

[4] J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A* **62** (1993), 30–45.

[5] M. Harada, P. Solé and P. Gaborit, Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey, Algebras and combinatorics (Hong Kong, 1997), 255–275, Springer, Singapore, 1999.

[6] M. Harada, M. Kitazume, A. Munemasa and B. Venkov, On some self-dual codes and unimodular lattices in dimension 48, *European J. Combin.* **26** (2005), 543–557.

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

[8] V. Pless, J. Leon and J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, *J. Combin. Theory Ser. A* **78** (1997), 32–50.