Journal of Algebraic Combinatorics **16** (2002), 209–223

Ternary Code Construction of Unimodular Lattices and Self-Dual Codes over $\mathbb{Z}_6$

MASAAKI HARADA
Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan

MASAAKI KITAZUME
Department of Mathematics and Informatics, Chiba University, Chiba 263–8522, Japan

MICHIO OZEKI
Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan

Received September 7, 2001; Revised April 22, 2002

Abstract. We revisit the construction method of even unimodular lattices using ternary self-dual codes given by the third author (M. Ozeki, in *Théorie des nombres*, J.-M. De Koninck and C. Levesque (Eds.) (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 772–784), in order to apply the method to odd unimodular lattices and give some extremal (even and odd) unimodular lattices explicitly. In passing we correct an error on the condition for the minimum norm of the lattices of dimension a multiple of 12. As the results of our present research, extremal odd unimodular lattices in dimensions 44, 60 and 68 are constructed for the first time. It is shown that the unimodular lattices obtained by the method can be constructed from some self-dual $\mathbb{Z}_6$-codes. Then extremal self-dual $\mathbb{Z}_6$-codes of lengths 44, 48, 56, 60, 64 and 68 are constructed.

Keywords: ternary self-dual code, extremal self-dual $\mathbb{Z}_6$-code, extremal unimodular lattice

1. Introduction

There are many known relationships between codes and lattices [4]. In particular, self-dual codes with large minimum weights are often used to construct dense unimodular lattices. A construction method of even unimodular lattices using ternary self-dual codes was given by the third author [11]. A condition for the minimum weights of ternary self-dual codes, so that the obtained even unimodular lattices become extremal, was also provided (Theorem 2 in [11]). It was mentioned in [11] that extremal even unimodular lattices in dimensions 48, 56 and 64 are constructed from some known ternary self-dual codes whose minimum weights are greater than or equal to 15 without giving explicit generator matrices of the lattices.

In this paper, we revisit the construction method given in [11]. Our main purpose is to apply the method to odd unimodular lattices, and give explicit generator matrices of some extremal (even and odd) unimodular lattices. In [11], the construction method was considered under the assumption that a self-dual code of length n contains a codeword of maximum weight $\geq n-2$. Moreover unfortunately there was an error in [11] on the condition to determine the minimum norm of the lattices in the case when the dimension is a multiple of 12. In Section 3, we remove the restriction on the maximum weight, and complete the construction of extremal unimodular lattice, by adding the assumption that the code is admissible (Theorem 6). Our argument can be applied to odd lattices. Consequently extremal odd unimodular lattices in dimensions 44, 60 and 68 are constructed from some ternary self-dual codes for the first time (Theorem 7). Furthermore, in Section 4, it is shown that unimodular lattices obtained by the method can be constructed from self-dual $\mathbb{Z}_6$-codes. Hence extremal Type II $\mathbb{Z}_6$-codes of lengths 48, 56 and 64, and extremal Type I codes of lengths 44, 60 and 68 are constructed for the first time (Theorems 10 and 12). Note that the generator matrices of the corresponding extremal unimodular lattices are easily obtained from generator matrices of extremal self-dual $\mathbb{Z}_6$-codes.

All the results about the construction of extremal odd unimodular lattices stated in this paper were already announced in [14]. In particular, the construction of an extremal odd unimodular lattice in dimension 44 was announced in April, 1998.

2. Type II $\mathbb{Z}_6$-codes and construction A

In this section, we recall some basic notions on codes over $\mathbb{Z}_6$, unimodular lattices and the basic construction of lattices from codes. For undefined terms, we refer to [1, 4] and [13].

Let $\mathbb{Z}_6$ (= $\{0, 1, 2, \dots, 5\}$) be the ring of integers modulo 6. A code C of length n over $\mathbb{Z}_6$ (or a $\mathbb{Z}_6$-code of length n) is a $\mathbb{Z}_6$-submodule of $\mathbb{Z}_6^n$. An element of C is called a codeword. We define the inner product on $\mathbb{Z}_6^n$ by $x \cdot y = x_1y_1 + \cdots + x_ny_n$, where $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{Z}_6^n \mid x \cdot y = 0$ for all $y \in C\}$. A code C is *self-dual* if $C = C^\perp$. The Hamming weight of a codeword is the number of non-zero components in the codeword. The Euclidean weight of a codeword x is $\sum_{i=1}^n \min\{x_i^2, (6-x_i)^2\}$. The minimum Euclidean weight d_E of C is the smallest Euclidean weight among all nonzero codewords of C. Two codes over $\mathbb{Z}_6$ are said to be *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates [1]. A *Type II* code over $\mathbb{Z}_6$ is a self-dual code with all codewords having Euclidean weight divisible by 12. It is known in [1] that there is a Type II code of length n if and only if $n \equiv 0 \pmod 8$. A self-dual code which is not Type II is called *Type I*.

A (Euclidean) lattice L is *integral* if $L \subseteq L^*$ where L^* is the dual lattice under the standard inner product (x, y). An integral lattice with $L = L^*$ is called *unimodular*. A lattice with even norms is said to be *even*. A lattice containing a vector of odd norm is called *odd*. An n-dimensional even unimodular lattice exists if and only if $n \equiv 0 \pmod 8$ while an odd unimodular lattice exists for every dimension. The minimum norm $\min(L)$ of L is the smallest norm among all nonzero vectors of L. The minimum norm μ of an n-dimensional unimodular lattice is bounded by

$$\mu \le 2\left[\frac{n}{24}\right] + 2, \tag{1}$$

unless $n = 23$ when $\mu \le 3$ [12]. An n-dimensional unimodular lattice meeting the bound is called *extremal*.

The set of vectors $f_1, \dots, f_n$ in an n-dimensional lattice L with $(f_i, f_j) = k\delta_{ij}$ is called a *k-frame* of L where δ_{ij} is the Kronecker delta. The lattice L has a k-frame if and only if L is obtained as

$$A_k(C) = \left\{ \frac{1}{k}\sum_{i=1}^{n} x_i e_i \;\middle|\; x_i \in \mathbb{Z},\ (x_i \pmod k) \in C \right\},$$

from some $\mathbb{Z}_k$-code C by Construction A. If C is a self-dual code over $\mathbb{Z}_k$ then $A_k(C)$ is unimodular. Moreover if C is a Type I (resp. Type II) $\mathbb{Z}_6$-code with minimum Euclidean weight d_E then $A_6(C)$ is an odd (resp. even) unimodular lattice with minimum norm $\min\{d_E/6, 6\}$ (cf. [1]).

By (1), the minimum Euclidean weight d_E of a self-dual $\mathbb{Z}_6$-code of length n is bounded by

$$d_E \leq 12\left[\frac{n}{24}\right] + 12, \tag{2}$$

for length $n < 48$ (cf. [1]). We say that a self-dual $\mathbb{Z}_6$-code of length n (<48) with $d_E = 12[n/24]+12$ is *extremal*. Examples of extremal Type II codes of lengths $n \leq 40$ are known (cf. [1, 6, 7]).

3. Ternary code construction and extremal unimodular lattices

In this section, we revisit the construction method in [11] correcting the condition of minimum weights when dimensions are divisible by 12 and removing the restriction on the maximum weights. The method is also reconsidered from the viewpoint of the theory of shadow lattices in [3] and applied to odd unimodular lattices.

3.1. Ternary code construction

First we recall some results concerning shadow lattices of odd unimodular lattices from [3]. Let L be an n-dimensional odd unimodular lattice and let L_0 denote its subset of vectors of even norm. The set L_0 is a sublattice of L of index 2. Let L_2 be that unique nontrivial coset of L_0 into L. Then L_0^* can be written as a union of cosets of L_0: $L_0^* = L_0 \cup L_2 \cup L_1 \cup L_3$. The *shadow lattice* of L is defined to be $S = L_1 \cup L_3$. In the case that n is even, there are three unimodular lattices $L_0 \cup L_2$, $L_0 \cup L_1$, $L_0 \cup L_3$ containing L_0 noting that L_0^*/L_0 is the Klein 4-group. The norms of vectors of the shadow lattice are congruent to $n/4 \pmod 2$. In this section, we consider the lattices $L_0 \cup L_1$, $L_0 \cup L_3$ for the case $L = A_3(C)$.

Let C be a ternary self-dual code of length n with minimum weight d. Then n must be a multiple of 4. The lattices $A_3(C)$ and $B_3(C)$ by Constructions A and B are defined as:

$$A_3(C) = \left\{ \frac{1}{3}\sum_{i=1}^{n} x_i e_i \;\middle|\; x_i \in \mathbb{Z},\ (x_i \pmod 3) \in C \right\},$$
$$B_3(C) = \{ v \in A_3(C) \mid (v, v) \in 2\mathbb{Z} \},$$

respectively, where $e_1, \ldots, e_n$ satisfy $(e_i, e_j) = 3\delta_{ij}$, that is, $\{e_1, \ldots, e_n\}$ is a 3-frame. Then $A_3(C)$ is an odd unimodular lattice with minimum norm $\min\{3, d/3\}$, and $B_3(C)$ is the unique even sublattice of $A_3(C)$ of index 2, that is, $B_3(C) = (A_3(C))_0$.

Lemma 1

$$\min(B_3(C)) = \min\left\{6, 2\left[\frac{d+3}{6}\right]\right\}.$$

Proof: Let $u = \frac{1}{3}\sum_{i=1}^n x_i e_i\ (\neq 0) \in B_3(C)$. If $(x_i \pmod 3) = (0, \ldots, 0)$ then (u, u) is clearly a multiple of 3, and thus $(u, u) \geq 6$. Note that $B_3(C)$ contains a vector $e_1 + e_2$ of norm 6. If $(x_i \pmod 3) \neq (0, \ldots, 0)$ then $(u, u) = (1/3)\sum_{i=1}^n x_i^2 \geq (1/3)\ \mathrm{wt}((x_i \pmod 3))$ where $\mathrm{wt}(c)$ denotes the weight of a vector c. Noting that (u, u) is an even integer and d is a multiple of 3, then $(u, u) \geq (d+3)/3$ if d is odd and $(u, u) \geq d/3$ if d is even (and also a multiple of 6). In both cases $(u, u) \geq 2[(d+3)/6]$ holds, then the result follows. □

Lemma 2 *The shadow lattice of $A_3(C)$ is given by*

$$B_3(C)^* \setminus A_3(C) = \left\{ v = \frac{1}{6}\sum_{i=1}^n x_i e_i \;\middle|\; x_i \in \mathbb{Z},\ v^{(3)} \in C, v^{(2)} = (1, \ldots, 1) \right\},$$

where $v^{(p)} = (x_i \pmod p) \in \mathbb{Z}_p^n$ for $p = 2, 3$.

Proof: Suppose that $v = \frac{1}{6}\sum_{i=1}^n x_i e_i$ satisfies the conditions $v^{(3)} \in C$, $v^{(2)} = (1, \ldots, 1)$. Let $b = \frac{1}{3}\sum_{i=1}^n y_i e_i \in B_3(C)$. Then $v \notin A_3(C)$, because $(e_1, v) \notin \mathbb{Z}$. Since $v^{(3)} \in C$, we have

$$((x_i), (y_i)) \equiv 0 \pmod 3.$$

Moreover since $v^{(2)} = (1, \ldots, 1)$, we have

$$((x_i), (y_i)) \equiv \sum_i y_i \equiv \sum_i y_i^2 \equiv 0 \pmod 2,$$

by $(b, b) \in 2\mathbb{Z}$. Hence $((x_i), (y_i)) \in 6\mathbb{Z}$ and thus $(v, b) \in \mathbb{Z}$, that is, $v \in B_3(C)^*$.

We will show the converse. The existence of such a vector v is easily proved by the Chinese remainder theorem. (We will give an explicit definition after this lemma.) Then since $[B_3(C)^* : A_3(C)] = 2$ and $v \notin A_3(C)$, we have $B_3(C)^* = \langle v, A_3(C)\rangle$ where $\langle v, A_3(C)\rangle$ denotes the lattice generated by v and $A_3(C)$. Let $u \in B_3(C)^* \setminus A_3(C)$. Then u is written as $v + a$ with $a = \frac{1}{3}\sum_{i=1}^n z_i e_i \in A_3(C)$. Then by definition $a^{(p)} = (2z_i \pmod p)$ and thus we have $a^{(3)} \in C$ and $a^{(2)} = (0, \ldots, 0)$. Hence we have $u^{(3)} = v^{(3)} + a^{(3)} \in C$ and $u^{(2)} = v^{(2)} + a^{(2)} = (1, \ldots, 1)$. □

We denote by m the maximum weight of C. For simplicity, we may assume that C contains a codeword of the form $(1, \ldots, 1, 0, \ldots, 0)$ (possibly, the all-one vector) with maximum weight m. We set

$$v_0 = \frac{1}{6}\left(\sum_{i=1}^{m} e_i + \sum_{i=m+1}^{n} 3e_i\right).$$

Then clearly $v_0 \in B_3(C)^* \setminus A_3(C)$. We define the following two lattices:

$$L_S(C) = \langle v_0, B_3(C)\rangle, \text{ and } L_T(C) = \langle v_0 - e_n, B_3(C)\rangle.$$

By definition, we have directly the following:

Lemma 3
(1) *The three unimodular lattices containing $B_3(C)$ are $L_S(C)$, $L_T(C)$ and $A_3(C) = \langle e_n, B_3(C)\rangle$.*
(2) *$L_S(C)$, $L_T(C)$ are even if and only if n is divisible by eight.*

Proof: Follows from the basic fact of shadow lattices given in the beginning of this section. □

Remark After the publication of [11], Montague introduced these construction methods (when n is divisible by eight, and $m = n$ holds), which were called straight and twisted, respectively. It was shown that all the Niemeier lattices can be constructed from some ternary self-dual codes by these methods.

Lemma 4 *Suppose $m < n$. Then*

$$\min(v_0 + B_3(C)) = \min((v_0 - e_n) + B_3(C)) = \frac{1}{12}(9n - 8m).$$

Proof: Let v be one of v_0, $v_0 - e_n$, and $u = \frac{1}{6}\sum_{i=1}^{n} z_i e_i \in v + B_3(C)$. By Lemma 2, u satisfies that $u^{(3)} \in C$ and $u^{(2)} = (1, \ldots, 1)$. Hence it is easily verified that its norm is minimum when u satisfies $z_i \in \{\pm 1, \pm 3\}$ and the weight of $u^{(3)}$, which is equal to the number of i with $z_i = \pm 1$, is maximum. Since $m < n$, both of v_0, $v_0 - e_n$ satisfy these conditions, and hence we have $\min(v + B_3(C)) = (v, v) = \frac{1}{12}(m + 9(n - m))$, as required. □

Now we consider the case $m = n$. The following definition is due to Koch [8], but it is slightly modified and applied to all lengths as well as length 48.

Definition Let C be a ternary self-dual code of length n, and suppose that C contains the all-one vector (hence $n \in 12\mathbb{Z}$). The code C is said to be *admissible* if and only if C satisfies one of the following (equivalent) conditions:

(A1) For every codeword $c \in C$ of weight n, the number of 1's in the components of c is even.
(A2) If all the components of c ($\in C$) are 0 or 1, then its weight is even.

Lemma 5 *If $m = n$ (hence $n \in 12\mathbb{Z}$) then*
(1) $\min(v_0 + B_3(C)) = \frac{n}{12}$.
(2) $\min((v_0 - e_n) + B_3(C)) = \begin{cases} \frac{n}{12} + 2 & \text{if } C \text{ is admissible}, \\ \frac{n}{12} & \text{otherwise.} \end{cases}$

Proof: Let v be one of $v_0, v_0 - e_n$ and let $u \in v + B_3(C)$. Set $t = \mathrm{wt}(u^{(3)})$. If $t < m$, then $t \leq m - 3$ and $(u, u) \geq n/12 + 2$ by the proof of Lemma 4.

Suppose $t = m$. Then clearly $(u, u) \geq n/12$ and the equality holds if and only if all the components of u are ± 1. The vector v_0 satisfies this condition. Hence we have proved the assertion (1).

We will prove that the following condition

(#) $(v_0 - e_n) + B_3(C)$ contains a vector $u = \frac{1}{6}\sum_{i=1}^{n} z_i e_i$ with $z_i = \pm 1$,

holds if and only if C is *not* admissible.

Suppose (#) holds. Let X be the set of i with $z_i = 1$. Then $u + v_0 - e_n = (\frac{1}{3}\sum_{i\in X} e_i) - e_n$, and its norm is equal to $\frac{1}{3}|X| + 1$ (resp. $\frac{1}{3}|X| + 3$) if $n \in X$ (resp. $n \notin X$). Since this norm is even, $|X|$ is odd and this means that C is not admissible. Conversely if C is not admissible, then C does not satisfy the condition (A2), and thus C contains an odd weight codeword whose components are 0 or 1. Hence $B_3(C)$ contains a vector $w = (\frac{1}{3}\sum_{i\in X} e_i) - e_n$ for some set X with $|X| = $ odd. Then $u = w - (v_0 - e_n)$ satisfies the condition (#).

If (#) does not occur, then the minimum norm is greater than $n/12$. Since all the vectors in $(v_0 - e_n) + B_3(C)$ have the same parity, $\min((v_0 - e_n) + B_3(C)) = n/12 + 2 = (v_0 - e_n, v_0 - e_n)$. □

Remark The proof in [11] of the result corresponding to the above lemma was incorrect. More precisely, the additional assumption that C is admissible if $\min((v_0 - e_n) + B_3(C)) = \frac{n}{12} + 2$ is necessary. However, it seems that Conway and Sloane already became aware that the additional assumption is necessary because they point out that the unimodular lattices constructed from the Pless symmetry codes of lengths 36 and 60 are not extremal (cf. [4, p. 148]).

All the discussions in this section establish the following:

Theorem 6 *Let C be a ternary self-dual $[n, n/2, d]$ code with maximum weight m. Let $L = L_S(C)$ or $L_T(C)$. Then*

$$\min(L) = \min\left\{6, 2\left[\frac{d+3}{6}\right], \frac{n}{12} + 2\right\},$$

if $m = n$ (hence n is divisible by 12), $L = L_T(C)$ and C is admissible, and

$$\min(L) = \min\left\{6, 2\left[\frac{d+3}{6}\right], \frac{1}{12}(9n - 8m)\right\},$$

otherwise.

Table 1. Known unimodular lattices.

n	Codes C	(d, m)	$\min(L_T(C))$	$\min(L_S(C))$	Comments
32	Extremal	(9, 30)	4*	4*	See remark
36	P_{36}	(12, 36)	3	3	[4, p. 148]
40	Extremal	(12, 39)	4*	4*	See remark
44	T_{44}	(12, 42)	4*	4*	New
48	Q_{48}, P_{48}	(15, 48)	6*	4	P_{48p}, P_{48q}
52	–	($\le$12, $\le$51)	$\le$4	$\le$4	
56	T_{56}	(15, 54)	6*	6*	
60	Q_{60}	(18, 60)	6*	5	New
64	T_{64}	(18, 63)	6*	6*	
68	T_{68}	(18, 66)	6*	6*	New

The extremal cases are indicated by $*$.

3.2. *Extremal unimodular lattices*

In Table 1, we collect known examples of (extremal) unimodular lattices constructed by our method from known ternary self-dual codes (see [13, Table XII] for the current information on the existence of extremal ternary self-dual codes). The unimodular lattices in dimensions up to 24 and 28-dimensional odd unimodular lattices with minimum norm 3 are classified and it is known that there is no 28-dimensional odd unimodular lattice with minimum norm 4 (cf. [4]). The minimum norms of lattices by the method are at most 6. Hence we deal with dimensions $32 \le n \le 68$ ($n \equiv 0 \pmod 4$). The first column indicates the dimensions of the lattices. The second column gives the ternary self-dual codes C which we consider and the minimum and maximum weights (d, m) are listed in the third column. In the following remark, we list the examples of ternary self-dual codes given in the table. The fourth and fifth columns list the minimum norms of $L_T(C)$ and $L_S(C)$, respectively. The extremal cases are indicated by $*$. From the table, we have the following:

Theorem 7 *There is an extremal odd unimodular lattice in dimensions* 44, 60 *and* 68.

Note that an extremal odd unimodular lattice is previously unknown for each of these dimensions.

Remark We give some comments on the existence of ternary self-dual codes described in the above table. Here we denote by P_n and Q_n the Pless symmetry code and the extended quadratic residue code of length n, respectively.

- $n = 32, 40$: Many extremal ternary self-dual codes are known, and many examples of extremal even unimodular lattices can be constructed from known codes. Thus we skip these dimensions, but it is a worthwhile project to determine if the lattices constructed are isometric.

- $n = 36$: Only known extremal ternary self-dual [36, 18, 12] code is P_{36}. The code has maximum weight $m = 36$ and is not admissible [4, p. 148]. If there exists a self-dual [36, 18, 9] code with $m = 33$ or an admissible extremal code, then it is possible to construct an extremal unimodular lattice. We do not know such examples.
- $n = 44$: Some extremal ternary self-dual codes of length 44 are obtained from an extremal self-dual code of length 48 by subtracting. Two such codes are known, namely P_{48} and Q_{48} (cf. [9]). As an example, we consider the extremal self-dual code T_{44} of length 44 subtracting the first four coordinates from Q_{48}. Hence an extremal odd unimodular lattice is constructed from such a code.
- $n = 48$: It is well known that the two codes P_{48} and Q_{48} are admissible and the extremal even unimodular lattices P_{48p} and P_{48q} are obtained from P_{48} and Q_{48}, respectively [4]. It is shown in [8] that any admissible code of length 48 has the same complete weight enumerator as P_{48} and Q_{48} containing the all-one vector. In addition, such a code is constructed from some Hadamard matrix of order 48.
- $n = 56$: Some extremal ternary self-dual [56, 28, 15] codes are constructed by subtracting from Q_{60} and P_{60} which are known extremal self-dual [60, 30, 18] codes (cf. [4]). Here we consider the extremal self-dual [56, 28, 15] code T_{56} subtracting the first four coordinates from Q_{60}.
- $n = 60$: Only Q_{60} and P_{60} are known extremal ternary self-dual codes of length 60. It is already mentioned in [4, p. 148] that P_{60} is not admissible. However, we have verified that Q_{60} is admissible. Hence an extremal odd unimodular lattice is constructed.
- $n = 64$: Let H_{32} be the Paley Hadamard matrix of order 32. Then the matrix (I, H_{32}) generates a ternary extremal self-dual code T_{64} of length 64 [5].
- $n = 68$: It is not known if there is a ternary extremal self-dual [68, 34, 18] code. However, a ternary self-dual [68, 34, 15] code makes an extremal odd unimodular lattice. Such a code is obtained from Q_{72} which is a ternary self-dual [72, 36, 18] code by subtracting. Here we consider the self-dual [68, 34, 15] code T_{68} subtracting the first four coordinates from Q_{72}.

We note that all examples of codes satisfy $n - m < 2$. It seems that no examples with minimum weight >3 and maximum weight $<n - 3$ are known. It follows from the Gleason theorem that an extremal self-dual code of length $n \leq 68$ satisfies the condition that $n - m < 2$.

4. Extremal self-dual $\mathbb{Z}_6$-codes

First we demonstrate that the lattices constructed from ternary self-dual codes can be constructed from some self-dual $\mathbb{Z}_6$-codes by Construction A. Then we construct self-dual $\mathbb{Z}_6$-codes which determine the lattices described in Table 1 for dimensions 44, 48, 56, 60, 64 and 68 showing that these codes are extremal. The generator matrices of the corresponding extremal unimodular lattices are easily obtained from the generator matrices of the above extremal self-dual $\mathbb{Z}_6$-codes.

4.1. 6-Frames and self-dual $\mathbb{Z}_6$-codes

Let C be a ternary self-dual code of length n. Clearly the lattice $B_3(C)$ contains the sublattice generated by $e_i \pm e_j$ $(1 \leq i, j \leq n)$, which is isometric to $\sqrt{3}R(D_n)$ where $R(D_n)$ is the root lattice of type D_n. Thus the two lattices $L_S(C)$ and $L_T(C)$ contain a 6-frame

$$\{e_1 + e_2, e_1 - e_2, e_3 + e_4, \ldots, e_{n-1} - e_n\}. \tag{3}$$

Hence, we have the following:

Proposition 8 *The lattices $L_S(C)$ and $L_T(C)$ are constructed from some self-dual $\mathbb{Z}_6$-codes by Construction A.*

By permuting the vectors e_i's, it is easy to get other 6-frames $\{e_i \pm e_j, e_k \pm e_l, \ldots\}$. In this section, we specify a 6-frame given in (3) so as to construct self-dual $\mathbb{Z}_6$-codes. In general, it is possible to construct distinct self-dual $\mathbb{Z}_6$-codes which generate the same lattice.

4.2. Extremal type II $\mathbb{Z}_6$-codes

Proposition 9 *The largest possible minimum Euclidean weights of Type II $\mathbb{Z}_6$-codes of lengths* 48, 56 *and* 64 *are* 36.

Proof: Proofs of three lengths are similar, so we give only the proof for length 48. Suppose that C is a Type II code with minimum Euclidean weight >36. Then its minimum Euclidean weight is greater than or equal to 48, since C is of Type II. Consider the even unimodular lattice $A_6(C)$. By the assumption, the vectors of norm 6 in $A_6(C)$ are only $\pm f_1, \ldots, \pm f_{48}$ where $\{f_1, \ldots, f_{48}\}$ is the 6-frame in $A_6(C)$. However, the theta series of an extremal even unimodular lattice is uniquely determined for each dimension and such a lattice contains 52416000 vectors of norm 6 for dimension 48 (cf. [4, p. 195]). □

Remark A similar argument can be applied to larger lengths in order to determine the largest possible minimum Euclidean weights.

We say that a Type II code with minimum Euclidean weight 36 is *extremal* for lengths 48, 56 and 64. This definition coincides with the one derived from (2) in Section 2 for lengths up to 40. In Section 3, an extremal even unimodular lattice is constructed for dimensions 48, 56 and 64. Since an extremal lattice is constructed from an extremal code, Proposition 8 shows the following:

Theorem 10 *There is an extremal Type II $\mathbb{Z}_6$-code for lengths* 48, 56 *and* 64.

Now we give explicit generator matrices of the extremal Type II $\mathbb{Z}_6$-codes. We give generator matrices (I, M) in standard form after suitable permutations and changing the signs of certain coordinates, that is, generator matrices of equivalent codes. In addition, throughout this section, only right halves M are given using the form $m_1, m_2, \ldots, m_{n/2}$

where m_j is the j-th row in order to save space.

- $n = 48$: Here we give generator matrices $(I, M_{48,P})$ and $(I, M_{48,Q})$ of the extremal Type II codes $C_{48,P}$ and $C_{48,Q}$ corresponding to P_{48_P} and P_{48_Q}, respectively.

$$\begin{aligned} M_{48,P} = {} & 320422043242002002022250, 502222044142204204002234,\\ & 340022002232020220240412, 100022004423244004042434,\\ & 342000024042324400022254, 342402440440432040004052,\\ & 320044404002443004002032, 542422222200444500020410,\\ & 300440244002244050442430, 142024404024424005422230,\\ & 500420000402222240144010, 522024444240240242432030,\\ & 140222244242242242023250, 540400500200440440020050,\\ & 540454204002402404244054, 324540242442202224402412,\\ & 542201400000020020240230, 350020204420242442424054,\\ & 435353135533315315355153, 543444240242222442040214,\\ & 124040420000040040040011, 353355353515535535133341,\\ & 304420410420220220020054, 100420220242002002200154, \end{aligned}$$

$$\begin{aligned} M_{48,Q} = {} & 020120400244424042222231, 153515135131331115153101,\\ & 351311531151133311311330, 000452022240000400220053,\\ & 242201022242004224202053, 020040520222400004002233,\\ & 044222012220202022042431, 402220005402002204020033,\\ & 200404202322240240244455, 244040022212444240440031,\\ & 240022044005042420004015, 424042002442300042442451,\\ & 204422022222032244422211, 000020042004425042442453,\\ & 200242022042240120402251, 420000200420044250424435,\\ & 442440204224404403042453, 440400424200002044100411,\\ & 402440024000224004450235, 424444402000402404205451,\\ & 240444004420042442020511, 432444442022222044242213,\\ & 003422240224220002202233, 500240024442404222224053. \end{aligned}$$

Note that the generator matrices given in this section can be also obtained electronically from "`http://www-sci.yamagata-u.ac.jp/~ozeki`". We say that $C \pmod{p} = \{x \pmod{p} | x \in C\}$ is the binary part (resp. the ternary part) of C if $p = 2$ (resp. $p = 3$). The binary and ternary parts of a Type II (resp. Type I) $\mathbb{Z}_6$-code is a binary Type II (resp. Type I) code and a ternary self-dual code, respectively [6]. We have verified by MAGMA that the binary parts of the two codes are equivalent and they have the following weight enumerator $1 + 276y^4 + 10626y^8 + 134596y^{12} + \cdots$. The ternary parts of the codes are self-dual [48, 24, 9] codes with weight enumerators $1 + 8y^9 + 3560y^{12} + 373920y^{15} + \cdots$ and $1 + 2y^9 + 2918y^{12} + 380472y^{15} + \cdots$, respectively.

We have found one more extremal Type II code C_{48}. The code C_{48} is the extended cyclic code over $\mathbb{Z}_6$ by appending 1's to the generators where the generator polynomial g_{48} is defined as

$$\begin{aligned} g_{48} = {} & x^{23} + 4x^{22} + 4x^{21} + 3x^{19} + x^{18} + 4x^{17} + 4x^{16} + x^{14} + 5x^{13} + 3x^{12}\\ & + 2x^{11} + 3x^{10} + 3x^9 + 4x^8 + 3x^7 + 5x^6 + x^5 + 5x^3 + 3x^2 + 3x + 5. \end{aligned}$$

Note that $g_{48} \pmod 2$ (resp. $g_{48} \pmod 3$) is a generator polynomial of the binary (resp. ternary) extended quadratic residue code of length 48. By Construction A, an extremal even unimodular lattice $A_6(C_{48})$ is constructed from the above extremal Type II code C_{48}. Robin Chapman has shown in private communication [2] that the extremal even unimodular lattice $A_6(C_{48})$ from C_{48} by Construction A is isometric to P_{48q}. We thank him for his useful comment.

Therefore there are at least three inequivalent extremal Type II $\mathbb{Z}_6$-codes of length 48.

- $n = 56, 64$: We give a generator matrix (I, M_n) of the extremal Type II code C_n corresponding to the extremal lattice $L_T(T_n)$ obtained from T_n which is given in Section 3.

$$
\begin{aligned}
M_{56} = {} & 3355315513153333515531511305, 1513353155331535111533155415,\\
& 0522000222244242000200402312, 2012404422422000224020440154,\\
& 4445420024240422040000002312, 4220540422422202420002404051 2,\\
& 4044410224222024440242404552, 4440243200202420220002044354,\\
& 0040222100404240200240024114, 0044224414000240204000404152,\\
& 0424022025242220220044202354, 0202224420120220440000020114,\\
& 4200222444214044404202424554, 2402044044043440402444000534,\\
& 2224440424040520240020240552, 0020040240044010444004002132,\\
& 0202422002440405200442440530, 0040420004444040120044204112,\\
& 4024440442224000230222220552, 4444240222002024405000020314,\\
& 4040422004004402040344002130, 4440224440400420424054020554,\\
& 4200002042420424222203240332, 0022244424020224224444522312,\\
& 0442202440420202224440230512, 4444242004024240024222421554,\\
& 2040222200024004002042242135, 1242004204002022400422004134.
\end{aligned}
$$

$$
\begin{aligned}
M_{64} = {} & 13515331131333535513114335153111, 35331135353333135135543553511533,\\
& 32242440240002402444413002424422, 43004244400024404444031424022002,\\
& 24302240442404204444215204242424, 02210424204222444222435422022402,\\
& 44203402400442024240415020004404, 42424322004224440224415420044444,\\
& 20404054400204402404013040004022, 22042405240044202440213404224420,\\
& 02024244304244442200433202022200, 00402442454024200004253402002422,\\
& 20224004225020004044011240002244, 22224024402322024200455200222044,\\
& 40220004224254204202413020040044, 44040202242221242000255020400400,\\
& 22204000040044344000451200224004, 22022400440402003440053420040440,\\
& 42024020224020244244431240420232, 00024404022420022440235200440300,\\
& 20040222202202402200015022410022, 00444002404244424422011442302220,\\
& 04200400022220220002235021004404, 40224402224424204022253344000242,\\
& 24440204420042240225013400444444, 24400004000404422342015200202040,\\
& 04020422442244234200051424204420, 20244400020042004454251444402442,\\
& 42222240244204440240553442024222, 42420042244242002044211014020404,\\
& 40240402042244004402253020205022, 44040000200224204024251004244205.
\end{aligned}
$$

The binary and ternary parts of the code C_{56} have the following weight enumerators $1 + 378y^4 + 20475y^8 + 376740y^{12} + \cdots$ and $1 + 346y^{12} + 69928y^{15} + \cdots$, respectively. The binary and ternary parts of the code C_{64} have the weight enumerators $1 + 496y^4 + 35960y^8 + \cdots$ and $1 + 64y^{12} + 9088y^{15} + \cdots$, respectively.

4.3. *Extremal type I $\mathbb{Z}_6$-codes*

Proposition 11 *The largest possible minimum Euclidean weights of Type I $\mathbb{Z}_6$-codes of lengths* 60 *and* 68 *are* 36.

Proof: Conway and Sloane [3] show that if the theta series of an odd unimodular lattice L is written as

$$\theta_L(q) = \sum_{j=0}^{\lfloor n/8 \rfloor} a_j \theta_3(q)^{n-8j} \Delta_8(q)^j,$$

then the theta series of the shadow lattice S is written as

$$\theta_S(q) = \sum_{j=0}^{\lfloor n/8 \rfloor} \frac{(-1)^j}{16^j} a_j \theta_2(q)^{n-8j} \theta_4(q^2)^{8j},$$

where $\Delta_8(q) = q \prod_{m=1}^{\infty}(1 - q^{2m-1})^8 (1 - q^{4m})^8$ and $\theta_2(q)$, $\theta_3(q)$ and $\theta_4(q)$ are the Jacobi theta series [4]. For dimension 60, the theta series of an extremal odd unimodular lattice and its shadow lattice are

$$\theta_L(q) = 1 + (3416640 + a_6)q^6 + \cdots,$$
$$\theta_S(q) = -\frac{a_7}{2^{24}} q + \left(\frac{27a_7}{2^{22}} + \frac{a_6}{2^{12}}\right) q^3 + \cdots,$$

respectively. Hence a_6 must be divisible by 2^{12}. Then $3416640 + a_6$ cannot be 120. Therefore a similar argument to the proof of Proposition 9 shows the assertion.

Similarly, the theta series of a 68-dimensional extremal odd unimodular lattice and its shadow lattice are written as using parameters a_6, a_7, a_8:

$$\theta_L(q) = 1 + (388416 + a_6)q^6 + \cdots,$$
$$\theta_S(q) = \frac{a_8}{2^{28}} q - \left(\frac{a_7}{2^{16}} + \frac{31a_8}{2^{26}}\right) q^3 + \frac{a_6}{2^4} q^5 + \cdots,$$

respectively. Hence a_6 must be divisible by 2^4 then $388416 + a_6$ cannot be 136. So the result follows. □

Remark A similar argument can be applied to other lengths in order to determine the largest possible minimum Euclidean weights.

In Section 3, an extremal odd unimodular lattice is constructed for dimensions 44, 60 and 68. By Proposition 8, we have the following:

Theorem 12 *For lengths* 44, 60 *and* 68, *there is an extremal Type I $\mathbb{Z}_6$-code.*

For $n = 44$, 60 and 68, we give a generator matrix (I, M_n) of the extremal Type I code C_n corresponding to the extremal lattice $L_T(T)$ obtained from $T = T_{44}$, Q_{60} and T_{68}, respectively.

M_{44} = 4211504004224442402024, 2031052022240000400220,
0033205204404420222224, 0231204100242200420244,
4453224030404420042220, 0033402043040002044400,
2415002204144044024242, 4051402440050202220404,
2011002044005402442024, 0035004200442504244242,
2253002020020250040022, 0431220220202241042040,
4253224042422420322420, 0233244022420402452200,
4015202044220222445220, 4031042402400444402104,
0213200204400422202454, 3253042422204244442402,
0315224022422000220220, 3345131551531115531551,
3354135113351353315155, 4455002024222442042025.

M_{60} = 531355115551551131513341511353, 252004202402422004240532042042,
041420202004242442444554402404, 422124240000442002420532420240,
242212402004224404240354422044, 022043420204204202204154424002,
422404302000444200404134022002, 024202432220424024440154444204,
422040041000004404224514000022, 244220420100440402024314420220,
040204200454220202444512020042, 242002244443244020420554202000,
440424004020124444040033202004 2, 420044204022212442424550042404,
424202240200221440424152204044, 151111153353113355135455333355,
200202420444242540404552440422, 424220244042004432222350442000,
424420022220040441220332024404, 422204004240404024304114444002,
000242202402024422030130200242, 000204204424424424245312204224,
022224442202202022200352102040, 404044004200240224204112032242,
040024242222440244222215424142 4, 244402422204044244422534000124,
242224244220040000224514424012, 044044440444004024442350024443,
202220420444422000042155020204, 304042000044240202404312022022.

M_{68}
= 2002442404243522252002420420444442, 1535535131335055513351315153515311,
2424422244205122045044422024204422, 2420220204425504422340040422400044,
4444044442403524044454420242402020, 0024404402445520044401224022020440,
2240220042423544422042344442422004, 0424444440405542200220452240204444,
4044204224021122024024401242002242, 0200420224041144000224242542402040,
0024002022021104020402040254004244, 4242400242205144004022440045042002,
4420222000443100022244420444540022, 2222422000021142442222422242034400,
0024040244445524200242024440201200, 2404242022441504242224200422020452 0,
4422222200041142000420002200200054, 2020404022245120504042444202004044,
5513333111334555111555531531353315, 0442422042203545404202240222244440,
2424244242223330040242244220422404, 3422444244421102024422024042200420,
0244002000005524444220220022404023, 4100004040001122442240000422242002,
4430022404005120402000024420442204, 0001204202041502402040224424040004,
2444120200423342424420224244404024, 0004054404045522042400404000422404,
2220020542423122220040202220404202, 4420025004001142042240000224020042,
4222244450445340204002220022442422, 0444222245041122242002242444040400,
4224024024121300042042242000000044, 2440402404211140202244222424440020.

Let $W_n^{(2)}$ and $W_n^{(3)}$ be the weight enumerators of the binary and ternary parts of C_n, respectively. Then

$$\begin{aligned}
W_{44}^{(2)} &= 1 + 231y^4 + 7315y^8 + 74613y^{12} + \cdots,\\
W_{44}^{(3)} &= 1 + 46y^9 + 8330y^{12} + \cdots,\\
W_{60}^{(2)} &= 1 + 435y^4 + 27405y^8 + 593775y^{12} + \cdots,\\
W_{60}^{(3)} &= 1 + 82y^{12} + 25464y^{15} + \cdots,\\
W_{68}^{(2)} &= 1 + 561y^4 + 46376y^8 + 1344904y^{12} + \cdots,\\
W_{68}^{(3)} &= 1 + 8y^{12} + 2524y^{15} + \cdots.
\end{aligned}$$

5. Concluding remarks

For dimensions 56 and 64, we have constructed an extremal even unimodular lattice from some ternary self-dual code in Section 3. Note that generator matrices of the lattices can be obtained from those of extremal Type II codes given in Section 4. It is interesting to investigate lattices constructed from other ternary self-dual codes. For these dimensions, only a few examples of extremal even unimodular lattices are known [4, p. 194]. It is also worthwhile to determine if these lattices are isometric.

The largest possible minimum norms of the lattices $L_S(C)$ and $L_T(C)$ from ternary self-dual codes C are 6. If we seek to construct unimodular lattices with larger minimum norms along with the present ideas, then we will be forced to use codes over larger fields such as $\mathbb{F}_5$, $\mathbb{F}_7$ and so on.

References

1. E. Bannai, S.T. Dougherty, M. Harada, and M. Oura, "Type II codes, even unimodular lattices and invariant rings," *IEEE Trans. Inform. Theory* **45** (1999), 257–269.
2. R. Chapman, private communication, November 4, 2000.
3. J.H. Conway and N.J.A. Sloane, "A note on optimal unimodular lattices," *J. Number Theory* **72** (1998), 357–362.
4. J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups*, 3rd edition, Springer-Verlag, New York, 1999.
5. E. Dawson, "Self-dual ternary codes and Hadamard matrices," *Ars Combin.* **19** (1985), 303–308.
6. S.T. Dougherty, M. Harada, and P. Solé, "Self-dual codes over rings and the Chinese remainder theorem," *Hokkaido Math. J.* **28** (1999), 253–283.
7. M. Harada, "On the existence of extremal Type II codes over $\mathbb{Z}_6$," *Discrete Math.* **223** (2000), 373–378.
8. H. Koch, "The 48-dimensional analogues of the Leech lattice," *Proc. Steklov Inst. Math.* **208** (1995), 172–178.
9. C.L. Mallows, V. Pless, and N.J.A. Sloane, "Self-dual codes over $GF(3)$," *SIAM. J. Appl. Math.* **31** (1976), 649–666.
10. P.S. Montague, "A new construction of lattices from codes over GF(3)," *Discrete Math.* **135** (1994), 193–223.
11. M. Ozeki, "Ternary code construction of even unimodular lattices," in *Théorie des nombres*, J.-M. De Koninck and C. Levesque (Eds.) (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 772–784.

12. E. Rains and N.J.A. Sloane, "The shadow theory of modular and unimodular lattices," *J. Number Theory* **73** (1998), 359–389.
13. E. Rains and N.J.A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman (Eds.), Elsevier, Amsterdam, 1998, pp. 177–294.
14. N.J.A. Sloane and G. Nebe, "Unimodular lattices, together with a table of the best such lattices," in *A Catalogue of Lattices*, published electronically at `http://www.research.att.com/~njas/lattices/`.