

Ternary Code Construction of Extremal Unimodular Lattices

山形大・理学部 原田 昌晃 (Masaaki Harada)
Department of Mathematical Sciences
Yamagata University

Abstract

In this manuscript, we briefly report the results of a recent preprint [4] which is joint work with Masaaki Kitazume and Michio Ozeki without proofs. We also give a short observation on construction of extremal even unimodular lattices in dimension 48.

1 Introduction

There are many known relationships between codes and lattices [3]. 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 Ozeki [7].

In my talk, I present results based on a recent preprint [4] which is joint work with Masaaki Kitazume and Michio Ozeki. So in this manuscript, we briefly report the results of [4] without proofs (Sections 3 and 4). We also give a short observation on construction of extremal even unimodular lattices in dimension 48 (Section 5). This observation is not contained in [4].

The purposes of [4] are as follows. We revisit the construction method given in [7]. One purpose is to apply the method to odd unimodular lattices, and give explicit generator matrices of some extremal (even and odd) unimodular lattices. In [7], 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 [7] on the condition to determine the minimum norm of the lattices in the case when the dimension is a multiple of 12. 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. 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.

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], [3] and [9].

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 $x \cdot y = x_1y_1 + \dots + x_ny_n$, where $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$. The dual code C^\perp of C is defined as $C^\perp = \{x \in \mathbb{Z}_6^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. 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. 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

$$(1) \quad \mu \leq 2 \left\lfloor \frac{n}{24} \right\rfloor + 2,$$

unless $n = 23$ when $\mu \leq 3$ [8]. 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

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

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

$$(2) \quad d_E \leq 12 \left\lfloor \frac{n}{24} \right\rfloor + 12,$$

for length $n < 48$ (cf. [1]). We say that a self-dual \mathbb{Z}_6 -code of length $n (< 48)$ with $d_E = 12\lfloor n/24 \rfloor + 12$ is *extremal*.

3 Ternary Code Construction and Extremal Unimodular Lattices

In this section, we revisit the construction method in [7] 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 [2] and applied to odd unimodular lattices.

3.1 Ternary Code Construction

First we recall some results concerning shadow lattices of odd unimodular lattices from [2]. 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:

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

respectively, where e_1, \dots, e_n satisfy $(e_i, e_j) = 3\delta_{ij}$, that is, $\{e_1, \dots, e_n\}$ 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, $B_3(C) = (A_3(C))_0$.

We denote by m the maximum weight of C . For simplicity, we may assume that C contains a codeword of the form $(1, \dots, 1, 0, \dots, 0)$ (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:

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

Note that the three unimodular lattices containing $B_3(C)$ are $L_S(C)$, $L_T(C)$ and $A_3(C) = \langle e_n, B_3(C) \rangle$ and $L_S(C)$, $L_T(C)$ are even if and only if n is divisible by eight.

The following definition is due to Koch [5], 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.

The following theorem is one of the main results in [4] and the proof is given in [4].

Theorem 1. 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

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

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

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

otherwise.

Remark. The proof in [7] 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. [3, p. 148]).

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 [9, 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. [3]). The minimum norms of lattices by the method are at most 6. Hence we deal with dimensions $32 \leq n \leq 68$ ($n \equiv 0 \pmod{4}$). 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 2. *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.

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	[3, 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	–	$(\leq 12, \leq 51)$	≤ 4	≤ 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

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 [3, 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. [6]). 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 [3]. It is shown in [5] 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. [3]). 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 [3, 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 it is known that the matrix (I , H_{32}) generates a ternary extremal self-dual code T_{64} of length 64.
- $n = 68$: 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

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

$$(3) \quad \{e_1 + e_2, e_1 - e_2, e_3 + e_4, \dots, e_{n-1} - e_n\}.$$

Hence, we have the following:

Proposition 3. *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 $\{e_i \pm e_j, e_k \pm e_l, \dots\}$. 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.

We say that a Type II code with minimum Euclidean weight 36 is *extremal* for lengths 48, 56 and 64 since the largest possible minimum Euclidean weights of Type II \mathbb{Z}_6 -codes of lengths 48, 56 and 64 are 36 [4]. 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 3 shows that there is an extremal Type II \mathbb{Z}_6 -code for lengths 48, 56 and 64.

The largest possible minimum Euclidean weights of Type I \mathbb{Z}_6 -codes of lengths 60 and 68 are 36 and Type I codes with minimum Euclidean weight 36 are called extremal. In Section 3, an extremal odd unimodular lattice is constructed for dimensions 44, 60 and 68. By Proposition 3, we have that 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.

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

$$M_{60} = 531355115551551131513341511353, 252004202402422004240532042042, \\ 041420202004242442444554402404, 422124240000442002420532420240, \\ 242212402004224404240354422044, 022043420204204202204154424002, \\ 422404302000444200404134022002, 024202432220424024440154444204, \\ 422040041000004404224514000022, 244220420100440402024314420220, \\ 040204200454220202444512020042, 242002244443244020420554202000, \\ 440424004020124440400332020042, 420044204022212442424550042404, \\ 424202240200221440424152204044, 151111153353113355135455333355,$$

200202420444242540404552440422, 424220244042004432222350442000,
 424420022220040441220332024404, 422204004240404024304114444002,
 000242202402024422030130200242, 000204204424424424245312204224,
 022224442202202022200352102040, 404044004200240224204112032242,
 040024242224402442222154241424, 244402422204044244422534000124,
 242224244220040000224514424012, 044044440444004024442350024443,
 202220420444422000042155020204, 304042000044240202404312022022.

$M_{68} =$ 2002442404243522252002420420444442, 1535535131335055513351315153515311,
 2424422244205122045044422024204422, 2420220204425504422340040422400044,
 4444044442403524044454420242402020, 0024404402445520044401224022020440,
 2240220042423544422042344442422004, 0424444440405542200220452240204444,
 4044204224021122024024401242002242, 0200420224041144000224242542402040,
 0024002022021104020402040254004244, 4242400242205144004022440045042002,
 4420222000443100022244420444540022, 222242200002114244222422242034400,
 0024040244445524200242024440201200, 2404242022441504242242004220204520,
 4422222200041142000420002200200054, 2020404022245120504042444202004044,
 5513333111334555111555531531353315, 0442422042203545404202240222244440,
 2424244242223330040242244220422404, 3422444244421102024422024042200420,
 0244002000005524444220220022404023, 4100004040001122442240000422242002,
 4430022404005120402000024420442204, 0001204202041502402040224424040004,
 2444120200423342424420224244404024, 0004054404045522042400404000422404,
 2220020542423122220040202220404202, 4420025004001142042240000224020042,
 4222244450445340204002220022442422, 0444222245041122242002242444040400,
 4224024024121300042042242000000044, 2440402404211140202244222424440020.

5 Dimension 48

By Theorem 1, if C is admissible extremal self-dual code then $L_T(C)$ is an extremal even unimodular lattice. In this section, we investigate a method to construct extremal admissible codes. Let H_n be a Hadamard matrix of order n and let $C(H_n)$ be the ternary code generated by the rows of H_n . We say that $C(H_n)$ is a code constructed from H_n .

Proposition 4 (Koch [5]). *Any admissible extremal self-dual code of length 48 is constructed from some Hadamard matrix of order 48.*

Hence in order to construct a (new) extremal even unimodular lattice in dimension 48, we would like to construct Hadamard matrices H with the property that $C(H)$ is admissible extremal. We give some basic properties of codes from Hadamard matrices.

Lemma 5. *If H and H' are equivalent Hadamard matrices then $C(H)$ and $C(H')$ are equiv-*

Proof. Clear. □

From now on, let H denote a Hadamard matrix of order 48.

Lemma 6. $C(H)$ is a self-dual code.

Proof. Clearly $C(H)$ is self-orthogonal. Let d_1, d_2, \dots, d_{48} be the elementary divisors of H . Then $|\det H| = d_1 \cdot d_2 \cdots d_{48} = 48^{24} = 3^{24} 2^{96}$. Therefore there are at most 24 3's among d_i . Hence the dimension of $C(H)$ is at least 24, so $C(H)$ is self-dual. □

Lemma 7. If H has a submatrix consisting of four rows which is equivalent to the following matrix

$$(4) \quad \begin{array}{cccc} + \cdots + & + \cdots + & + \cdots + & + \cdots + \\ + \cdots + & + \cdots + & - \cdots - & - \cdots - \\ + \cdots + & - \cdots - & + \cdots + & - \cdots - \\ \underbrace{+ \cdots +}_{12 \text{ columns}} & \underbrace{- \cdots -}_{12 \text{ columns}} & \underbrace{- \cdots -}_{12 \text{ columns}} & \underbrace{+ \cdots +}_{12 \text{ columns}} \end{array}$$

where we denote 1 and -1 by $+$ and $-$ respectively. Then $C(H)$ has a codeword of weight 12.

Proof. The sum of the four rows has weight 12. □

Lemma 8. $C(H_2 \otimes H_{24})$ and $C(H_4 \otimes H_{12})$ are not extremal.

Proof. First note that $C(H_{24})$ and $C(H_{12})$ are self-dual codes. The minimum weights of $C(H_{24})$ and $C(H_{12})$ are at most 9 and 6, respectively. We denote a codeword of minimum weight by x . Then $C(H_2 \otimes H_{24})$ contains vectors (x, x) and $(x, -x)$. Hence the sum of the two vectors has weight ≤ 9 . Similarly, $C(H_4 \otimes H_{12})$ has a vector of weight ≤ 6 . □

We end this manuscript by listing the following problems.

Problem. Find a Hadamard matrix H such that H has no submatrix which is equivalent to (4) and is inequivalent to $H_2 \otimes H_{24}$ and $H_4 \otimes H_{12}$. More specially, find a Hadamard matrix H such that $C(H)$ is admissible extremal.

Problem. Characterize a Hadamard matrix H such that $C(H)$ is admissible extremal.

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] J.H. Conway and N.J.A. Sloane, A note on optimal unimodular lattices, *J. Number Theory* **72** (1998), 357–362.
- [3] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York, 1999.
- [4] M. Harada, M. Kitazume and M. Ozeki, Ternary code construction of unimodular lattices and self-dual codes over \mathbb{Z}_6 , (submitted).
- [5] H. Koch, The 48-dimensional analogues of the Leech lattice, *Proc. Steklov Inst. Math.* **208** (1995), 172–178.
- [6] C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$, *SIAM. J. Appl. Math.* **31** (1976), 649–666.
- [7] M. Ozeki, Ternary code construction of even unimodular lattices, in *Théorie des nombres*, J.-M. De Koninck and C. Levesque, eds., (Quebec, PQ, 1987), 772–784, de Gruyter, Berlin, 1989.
- [8] E. Rains and N.J.A. Sloane, The shadow theory of modular and unimodular lattices, *J. Number Theory* **73** (1998), 359–389.
- [9] 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, 177–294.