Extremal even unimodular lattices of rank 32 and related codes

Helmut Koch and Gabriele Nebe

Helmut Koch
Max-Planck-Arbeitsgruppe
für Algebraische Geometrie und
Zahlentheorie
Mohrenstr. 39
O-1086 Berlin
Germany

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

Germany

Gabriele Nebe
Lehrstuhl/B für Mathematik
Templergraben 64
W-5100 Aachen
Germany

MPI/92-35

Introduction

In the following we consider even unimodular lattices Λ in the euclidean space $\mathbf{R}^{32}$ without vectors of squared length 2. Such lattices are called extremal. They were studied in [5], [1]. One associates an invariant $\nu(\Lambda)$ to Λ, the neighbor defect ([1], p. 156):

$$\nu(\Lambda) := 32 - \max\{E(\Lambda)_v | v \in \Lambda, (v,v) = 8\}$$

where Λ_v is the modification of Λ by means of v and $E(\Lambda_v)$ is the rank of the root lattice of Λ_v.

There are five lattices Λ with $\nu(\Lambda) = 0$ ([1], Satz 10) corresponding to the five doubly-even, self-dual, linear codes in $\mathbf{F}_2^{32}$ with minimal weight 8. If $\nu(\Lambda) > 0$, then $\nu(\Lambda) \geq 8$ ([1], Satz 4). In [3] it was shown that there are at least ten extremal lattices Λ with $\nu(\Lambda) = 8$. They are uniquely determined by linear codes C in $\mathbf{F}_2^{24}$ with weight enumerator

$$f_C(x) = 1 + 39x^8 + 176x^{12} + 39x^{16} + x^{24}. \tag{1}$$

In [3] these codes are denoted by $S_3, C_1, \ldots, C_5, G_1, \ldots G_4$. There are two further linear codes S_1, S_2 with weight enumerator (1), which lead to lattices Λ with $\nu(\Lambda) = 0$ ([1], Satz 14).

In the sections 1., 2. and 3. we prove the following

Theorem 1. *Any linear code C with weight enumerator* (1) *is equivalent to one of the twelve codes $S_1, S_2, S_3, C_1, \ldots, C_5, G_1, \ldots, G_4$.*

Table 1 presents the twelve codes by means of basis words corresponding to the proof of Theorem 1.

For a given extremal lattice Λ we denote the set of adjacent lattices Λ_v with $E(\Lambda_v) = 24$ by L_Λ. In [3] it was shown that the lattices Λ corresponding to the twelf codes in Theorem 1 are pairwise not isometric. Hence up to isometry there are precisely ten extremal lattices with neighbor defect 8.

Furthermore this implies that for a given lattice Λ the codes associated to the adjacent lattices Λ_v with $E(\Lambda_v) = 24$ are equivalent. From this and from the considerations in [1], 1.8, it follows that the automorphism group $\mathbf{Aut}\,\Lambda$ of Λ acts transitively on L_Λ. Hence

$$|\mathbf{Aut}\,\Lambda| = |L_\Lambda| \cdot 2^9 \cdot |\mathbf{Aut}\,C|$$

where C denotes the code corresponding to Λ.

The computation of the function g_Λ in [2] and [3] shows that $g_\Lambda(17) = 0$ for all lattices Λ with $\nu(\Lambda) \leq 8$. In section 4. we construct extremal lattices Λ with $g_\Lambda(17) \neq 0$. In section 5. we study the transition from adjacent lattices L to Λ in the case that the defect lattice V of L has the property $V^* = \frac{1}{2}V$ where V^* denotes the dual lattice of V. We show that this transition is uniquely determined up to isometry (Theorem 2).

The first author is grateful to B. B. Venkov for many discussions about the subject of this paper. This research was carried out during the visit of the first author at the Max-Planck-Institut für Mathematik in Bonn in 1991. He thanks the Institut for its hospitality. Furthermore, we want to thank Ms Catto for her excellent typing of our manuscript.

1.

In the follwoing we identify a word w in $\mathbf{F}_2^{24}$ with the set of places of w with coordinate 1. The places will be denoted by $1, \ldots, 24$. We put $\mathbf{1} := \{1, 2, \ldots, 24\}$. Furthermore $(a_1; a_2; \ldots; a_s)$ denotes the set of words $\{a_i + a_j | i, j \in \{\mathbf{1}, \ldots, s\}\}$.

The basis for the classification of the linear codes with weight enumerator (1) is the following

Proposition 2. *Any linear code C with weight enumerator* (1) *contains a subcode C_1 which is equivalent to the code generated by*

$$(\{1, \ldots, 6\}; \{7, \ldots, 12\}; \{13, \ldots, 18\}; \{19, \ldots, 24\})$$

and

$$\{1, 2, 3, 7, 8, 9, 13, 14, 15, 19, 20, 21\}.$$

Proof. a) Let y_1 be an element of C of weight 12. Without loss of generality we can assume

$$y_1 = \{1, \ldots, 12\}.$$

The type (a, b) of $\bar{x} \in C/(y_1, \mathbf{1})$ is defined by

$$a = |x \cap y_1|, \; b = |x \cap (\mathbf{1} + y_1)|$$

for x of minimal weight in its class in $C/(y_1, \mathbf{1})$. The possible types are $(0,0)$, $(2,6) = (6,2)$, $(4,4)$, $(6,6)$. A class of type $(2,6)$, $(4,4)$, $(6,6)$ contains $2, 1, 0$ words of weight 8. Let $\alpha_1, \alpha_2, \alpha_3$ be the number of classes of type $(2,6)$, $(4,4)$, $(6,6)$ respectively. Then

$$\alpha_1 + \alpha_2 + \alpha_3 = 63, \; 2\alpha_1 + \alpha_2 = 39.$$

It follows $-\alpha_1 + \alpha_3 = 24$, hence $\alpha_3 > 0$. Let y_2 be a word of type $(6,6)$. Without loss of generality we can assume

$$y_2 = \{7, \ldots, 18\}.$$

b) Now we consier in the same way the classes of $C/(y_1, y_2, \mathbf{1})$. There are six types

$$(0,0,0,0), \; (2,2,2,2), \; (2,2,4,0), \; (1,1,1,5), \; (1,1,3,3), \; (3,3,3,3).$$

They contain $0, 1, 3, 4, 2, 0$ words of weight 8 respectively. The even classes form a subgroup of index 1 or 2.

If the index is 2, we have with similar notation as in a)

$$\alpha_1 + \alpha_2 = 15, \; \alpha_3 + \alpha_4 + \alpha_5 = 16, \; \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4 = 39$$

hence $\alpha_5 = 4 + \alpha_2 + \alpha_3 > 0$. This implies Proposition 2.

c) Now we consider the case that there are only even classes. Then $\alpha_1 = 27$, $\alpha_2 = 4$. We change our notation and write the words of C as four dimensional vectors with coordinates which are subsets of $\{1, \ldots, 6\}$. Since there are 15 pairs in $\{1, \ldots, 6\}$ and 27 words of type $(2,2,2,2)$, C contains words $x_1 = (\phi, a_2, a_3, a_4)$, $x_2 = (b_1, \phi, b_3, b_4)$, $x_3 =$

(c_1, c_2, ϕ, c_4), $x_4 = (d_1, d_2, d_3, \phi)$. They deliver us the four classes $\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4$ of type $(2,2,4,0)$ in $C/(y_1, y_2, \mathbf{1})$. Without loss of generality we can assume

$$x_1 = (\phi, \{1,\ldots,4\}, \{1,\ldots,4\}, \{1,\ldots,4\}).$$

We have up to equivalence the following possibilities for x_2 :

$$\begin{aligned} x_2 &= (\{1,\ldots,4\},\ \phi,\ \{2,\ldots,5\},\ \{2,\ldots,5\}), \\ x_2' &= (\{1,\ldots,4\},\ \phi,\ \{3,\ldots,6\},\ \{3,\ldots,6\}), \\ x_2'' &= (\{1,\ldots,4\},\ \phi,\ \{1,\ldots,4\},\ \{3,\ldots,6\}). \end{aligned}$$

Assume $x_2 \in C$. Then x_1, x_2 give the $(6,6,6,6)-$ division

$$((\phi, \phi, \{2,3,4\}, \{2,3,4\}); (\phi,\ \{1,2,3,4\}, \{1\}, \{1\}); (\{1,2,3,4\}, \phi, \{5\}, \{5\});$$
$$(\{5,6\}, \{5,6\}, \{6\}, \{6\})),$$

for which $(\phi, \{1,\ldots,6\}\{1,\ldots,6\}, \phi)$ is odd. Hence we come back to b).

d) Now assume that corresponding coordinates of $x_1, \ldots, x_4$ have even intersection. Then the classes $\bar{x}_1, \ldots, \bar{x}_4$ in $C/(y_1, y_2, \mathbf{1})$ can not be linearly independent.

If $\bar{x}_1 + \bar{x}_2 + \bar{x}_3 = 0$, then we have without loss of generality

$$x_1 = (\phi,\ \{1,\ldots,4\},\ \{1,\ldots,4\}),\ x_2 = (\{1,\ldots,4\},\ \phi,\ \{1,\ldots,4\},\ \{3,\ldots,6\}),$$
$$x_3 = (\{1,\ldots,4\},\ \{1,\ldots,4\},\ \phi,\ \{1,2,5,6\}),\ x_4 = (\{3,\ldots,6\},\ \{3,\ldots,6\},\ \{3,\ldots,6\},\ \phi).$$

Let x_5 be a further basis element. x_5 has type $(2,2,2,2)$. Its coordinates are pairs distinct from $\{1,2\}$, $\{3,4\}$, $\{5,6\}$. Choosing suitable words of weight 12 in x_5 and $(y_1, y_2, \mathbf{1})$ one finds a $(6,6,6,6)-$ division for which x_1 is odd. The case $\bar{x}_1 + \bar{x}_2 + \bar{x}_3 + \bar{x}_4 = 0$ can be handled analogously. This finishes the proof of proposition 2.

2.

By Proposition 2 we can assume that C contains the words

$$\begin{aligned} \mathbf{1} &= \{1,\ldots,24\}, \\ y_1 &= \{1,\ldots,12\}, \\ y_2 &= \{7,\ldots,18\}, \\ y_3 &= \{1,2,3,7,8,9,13,14,15,19,20,21\}. \end{aligned}$$

We denote by C_1 the code generated by these words. C_1 gives a division of $\{1,\ldots,24\}$ in 8 parts $\{1,2,3\},\ldots,\{22,23,24\}$. The classes in C/C_1 are type

$$\begin{aligned} A_0 &= (0,0,0,0,0,0,0,0), \\ A_1 &= (1,1,1,1,1,1,1,1), \\ A_2 &= (1,1,1,1,2,2,0,0), \\ A_3 &= (2,2,2,0,2,0,0,0). \end{aligned}$$

The components of the types can not be arbitrarily permuted. The admissible permutations are the permutations of the $(8,4)-$ Hamming code H generated by $\{1,\ldots,8\}$, $\{1,\ldots,4\}$, $\{3,\ldots,6\}$, $\{1,2,5,7\}$ according to the structure of C_1. This means that one can prescribe the images of four places which do not form a set in H, such that the set of images is not in H, too. This determines an automorphism of H.

Let α_i be the number of classes of type A_i. Then

$$\alpha_1 + \alpha_2 + \alpha_3 = 15, \alpha_1 + 3\alpha_2 + 5\alpha_3 = 39$$

and therefore $\alpha_1 - \alpha_3 = 3$.

Furthermore let C_2 be the linear code in $\mathbb{F}_2^{24}$ generated by $\{1,2,3\}, \{4,5,6\}, \dots, \{22,23,24\}$. Then $C \cap C_2 = C_1$. Each class in $CC_2/C_2 \cong C/C_1$ has a unique representative with components of cardinality 0 or 1. In the following we write $0,1,2,3$ for these components. For instance the class of the word $\{1,2,4,5,7,8,13,14\}$ will be written $(3,3,3,0,3,0,0,0)$. Hence we consider now the group K^8 with $K = \mathbb{F}_4^+$. We call an element of K^8 admissable if the corresponding class in C/C_1 is of type A_0, A_1, A_2 or A_3. A subgroup U in K^8 of order 16 corresponds to a code C if and only if all its elements are admissible and the equation $\alpha_1 + 3\alpha_2 + 5\alpha_3 = 39$ is satisfied.

Since $\alpha_1 \geq 3$, we can choose our next basis element in the form

$$x = (1,1,1,1,1,1,1,1).$$

Every further basis element of type A_1 in U contains $0,2$ or 4 coordinates 1. Hence we have up to equivalence three possibilities:

$$a)\ y = (2,2,2,2,2,2,2,2),$$
$$b)\ y = (1,1,2,2,2,2,2,2),$$
$$c)\ y = (1,1,1,2,1,2,2,2).$$

a) If U contains an element with four coordinates 0, then up to equivalence the next basis element can be chosen in the form

$$aa)\ z = (0,0,0,1,0,1,1,1)$$

or

$$ab)\ z = (0,0,0,1,0,1,2,2).$$

If U contains no vector with four coordinates 0, then all further vectors of U are of type A_2 and consists of two components $0,1,2,3$ respectively. Up to equivalence there are three possibilities:

$$ac)\ z = (0,0,1,1,2,2,3,3),$$
$$ad)\ z = (0,0,1,1,2,3,2,3),$$
$$ac)\ z = (0,0,1,2,1,3,2,3).$$

b) There is a further vector of type A_1 in U. It contains $2,1$ or 0 coordinates 1 at the first two components. Let $z = (z_1, z_2, \dots, z_8)$. $ba)$ $z_1 = z_2 = 1$. We can assume that there are exactly two further coordinates 1. Otherwise one permutes 1 and 2 in all components beside the first two.

$$baa)\ z = (1,1,1,2,1,2,3,3),$$
$$bab)\ z = (1,1,1,2,1,3,2,3),$$
$$bac)\ z = (1,1,1,3,1,3,3,3).$$

$bb)$ $z_1 = 1,\ z_2 = 2.$

$$bba)\ z = (1,2,1,1,1,2,2,2),$$
$$bbb)\ z = (1,2,1,1,1,2,3,3),$$
$$bbc)\ z = (1,2,1,1,1,3,2,3),$$
$$bbd)\ z = (1,2,1,2,1,3,3,1),$$
$$bbe)\ z = (1,2,1,3,1,3,2,1),$$
$$bbf)\ z = (1,2,1,3,2,3,3,3).$$

$bc)$ $z_1 = z_2 = 2.$

$$bca)\ z = (2,2,1,1,1,2,1,2),$$
$$bcb)\ z = (2,2,1,1,2,2,3,3),$$
$$bcc)\ z = (2,2,1,1,2,3,2,3),$$
$$bcd)\ z = (2,2,1,2,1,2,3,3),$$
$$bce)\ z = (2,2,1,2,1,3,2,3).$$

c) Up to equivalence and cases which appear already in a) or b) we have only two possibilities

$$ca)\ z = (1,1,1,3,1,3,3,3),$$
$$cb)\ z = (1,1,2,1,2,2,1,2).$$

3.

We have seen in 2. that every code with weight enumerator (1) is of the form $\tilde{S} = (S, v)$ for one of the 21 codes S of dimension 7 and some $v \in S^{\perp}$. It suffices to look at some representative v for each of the 2^{10} classes in $S^{\perp}/S$.

For the testing of the equivalence of codes we introduce the following notion of profile:

Let C be a code with weight enumerator (1). For $w \in C_8 := \{c \in C / |c| = 8\}$ define A_w by $A_w := \{c \in C_8 | c \cap w = \phi\}$. Since $\{1 + w, \phi\} \cup A_w$ is a linear code the cardinality of A_w is $2^i - 2$ for some $i \in N$. We put

$$z_i := |\{w \in C_8|\ |A_w| = 2^i - 2\}|.$$

The triple $Z_C := (z_1, z_2, z_3)$ is called the profile of the code C.

It is clear that equivalent codes have the same profile. The twelve known codes have the following profiles: $Z_{S_3} = (0,0,36)$, $Z_{S_2} = (0,24,12)$, $Z_{S_3} = (24,0,15)$, $Z_{C_1} = (0,32,6)$, $Z_{C_2} = (8,24,7)$, $Z_{C_3} = (16,18,5)$, $Z_{C_4} = (24,12,3)$, $Z_{C_5} = (16,21,2)$, $Z_{G_1} = (24,15,0)$, $Z_{G_2} = (18,21,0)$, $Z_{G_3} = (0,39,0)$, $Z_{G_4} = (32,6,1)$.

Hence we can distinguish them by their profiles. A computer test shows that all codes $\tilde{S}$ have one of the profiles above. It remains to show that $\tilde{S}$ is equivalent to the corresponding known code. This was done by a slight modification of an algorithm of W. Plesken and M. Pohst [4].

The following table presents the codes of Theorem 1 in the form (S, v).

C	S	c	$\|\text{Aut } C\|$
S_1	$ac)$	$(0,0,2,2,3,3,1,1)$	$2^{15} \cdot 3^2$
S_2	$ac)$	$(3,0,1,2,3,0,1,2)$	$2^{13} \cdot 3$
S_3	$ad)$	$(3,3,1,1,2,0,2,0)$	$2^7 \cdot 3^3 \cdot 5$
C_1	$ac)$	$(1,0,1,0,3,2,3,2)$	$2^5 \cdot 3$
C_2	$bcc)$	$(0,2,0,2,3,1,2,1)$	2^6
C_3	$bba)$	$(3,3,3,1,1,0,3,0)$	2^7
C_4	$bca)$	$(2,2,0,3,3,3,0,3)$	$2^6 \cdot 3$
C_5	$bcc)$	$(1,2,1,3,1,3,1,2)$	2^4
G_1	$ab)$	$(3,2,2,1,1,2,3,2)$	$2^5 \cdot 3 \cdot 5$
G_2	$ab)$	$(3,3,2,1,1,3,3,2)$	1
G_3	$ab)$	$(3,1,2,3,3,2,3,1)$	$2^6 \cdot 3^2$
G_4	$ab)$	$(3,2,2,2,1,1,3,2)$	$2^7 \cdot 3$

Table 1

4.

In the study of even unimodular extremal lattices Λ of rank 32 one finds that in the cases of neighbor defect 0 and 8 one has always $g_\Lambda(17) = 0([2],[3])$. Therefore the question arises whether this is true for all extremal lattices Λ of rank 32. In the following we construct extremal lattices Λ with $g_\Lambda(17) \neq 0$. Such a lattice has by definition a neighbor Λ_w with root system $\{\pm a_1, \dots, \pm a_{17}\}$ and by [1], Theorem 4, the defect lattice of Λ_w has the form $\sqrt{2}\left(\tilde{A}_{15}\right)$. On the other hand it is easy to see and we come to this question in 5. that for any even unimodular lattice L of rank 32 with root system $\{\pm a_1, \dots, \pm a_{17}\}$ there exists a neighbor without roots. Hence it is sufficient to consider such lattices L. By [2], Satz 1.5, the code D of L has dimension 1. Hence up to equivalence there are three possibilities:

a) $D = (\{1, \dots, 16\})$, b) $D = (\{1, \dots, 12\})$, c) $D = (\{1, \dots, 8\})$. We consider here only the first case.

We assume $D = (\{1,\ldots,16\})$. Then $D^\perp$ is generated by $\{17\}$ and $D' = \{d \subseteq \{1,\ldots,16\} \mid |d| \in 2\mathbf{Z}\}$. Let U be the code lattice of L, which as abelian group is generated by $a_1,\ldots,a_{17}$, $\frac{1}{2}(a_1+\ldots+a_{16})$.

We represent $\sqrt{2}(A_{15})$ in the standard form

$$\sqrt{2}(A_{15}) = \left\{ \sum_{i=1}^{16} \beta_i b_i \middle| \beta_i \in \mathbf{Z},\ \sum_{i=1}^{16} \beta_i = 0 \right\},$$

where $b_1,\ldots,b_{16}$ denotes an orthogonal basis of $\mathbf{R}^{16}$ with $(b_i,b_i) = 2$ for $i = 1,\ldots,16$. Then $\sqrt{2}\left(\tilde{A}_{15}\right)$ is generated by $\sqrt{2}(A_{15})$ and the vector $\frac{1}{4}(b_1+\ldots+b_{12}) - \frac{3}{4}(b_{13}+\ldots+b_{16})$. In the gluing process we have to combine $\frac{1}{2}a_{17}$ with a vector v whose class in $\frac{1}{\sqrt{2}}\left(\tilde{A}_{15}\right)/\sqrt{2}\left(\tilde{A}_{15}\right)$ has minimal length $\frac{7}{2}$. One can take for instance

$$v = \frac{1}{8}(b_1+\ldots+b_{14}) - \frac{7}{8}(b_{15}+b_{16}). \qquad (1)$$

To finish the gluing process, it is sufficient to combine the vector classes $\bar{x} = \frac{1}{2}\sum_{i\in d} a_i + U$ for $d \in D'$ with vector classes $\bar{w}$ in V^*/V such that the corresponding mapping $U^*/U \to V^*/V$ is an isomorphism and

$$l(\bar{w}) + l(\bar{x}) \in 2\mathbf{Z},\ l(\bar{w}) + l(\bar{x}) \neq 2,$$

where l denotes the minimal (squared) length of a vector class. Every class $\bar{w}$ in V^*/V with integral length $l(\tilde{w})$ contains a representative w in $\frac{1}{2}(A_{15})$ such that $l(\tilde{w}) = \min\{(w,w),2\}$.

We consider the linear code $C \subset \mathbf{F}_2^{32}$ which is constructed as follows: $c \in C$ if and only if

$$\frac{1}{2}\sum_{i\in c'} a_i + \frac{1}{2}\sum_{j\in c''} b_{j-16} \in L, \qquad (2)$$

where $c' = c \cap \{1,\ldots,16\}$, $c'' = c \cap \{17,\ldots,32\}$.

By construction it is clear that C is doubly even and has minimal weight 8. Furthermore, since $\dim D^\perp = 15$ and $\{17,\ldots,32\} \in C$, the dimension of C is 16 hence C is self-dual. One knows from [0] that there are precisely five inequivalent linear codes C in $\mathbf{F}_2^{32}$ which are doubly even, self-dual and of minimal weight 8. Each such code contains words h of weight 16 which contain no subword $\neq \phi$ lying in C.

On the other hand, given such a pair C, h one gets a lattice L with the desired properties by means of $(1),(2)$ with $h = 1,\ldots,16$.

5.

Now we consider the transition from L to Λ. More generally we want to prove the following Theorem.

Theorem 2. *Let L be an even unimodular lattice of rank 32 such that $L_2 = \{\pm a_1,\ldots,\pm a_s\}$ and such that the defect lattice V of L, i.e. the sublattice of L consisting of all vectors which* *are orthogonal to* $a_1, \ldots, a_s$, *has the property* $V^* = \frac{1}{2}V$. *Then a)* $s \geq 16$. *b) There is up to isometry at most one adjacent lattice of* L *without roots. c) If* $s > 16$ *then there exists an adjacent lattice of* L *without roots. d) If* $s = 16$, *then there exists an adjacent lattice of* L *if and only if* $\frac{1}{\sqrt{2}}V$ *is odd.*

Proof: We denote the code lattice of L, i.e. the sublattice of L consisting of all linear combinations of $a_1, \ldots, a_s$, by U. Furthermore

$$C = \left\{ c \in \mathbb{F}_2^s | \frac{1}{2} \sum_{i \in c} a_i \in L \right\}$$

denotes the code of L.

$V^* = \frac{1}{2}V$ implies

$$s - 2 \dim C = \dim C^\perp / C = \dim U^*/U = \dim V^*/V = 32 - s$$

hence $\dim C = s - 16$. This proves a).

Let $y \in L$ with $(L_y)_2 = \phi$. Then y can be chosen in the form

$$y = \frac{1}{2}(a_1 + \ldots + a_s) + z \tag{3}$$

or

$$y = \frac{1}{2}(-3a_1 + a_2 + \ldots + a_s) + z \tag{4}$$

with $z \in V^*$.

If $\frac{1}{\sqrt{2}}V$ is even all vectors of V have integral squared length. Therefore $\{1, \ldots, s\} \in C$ and $\frac{1}{2}(a_1 + \ldots + a_s) \in U$, $z \in V$. Then there is an $u \in U^*$ such that $u + \frac{1}{2}z \in L$ and $\left(u + \frac{1}{2}z, y\right) \in 2Z$. Hence $\frac{1}{2}y - \left(u + \frac{1}{2}z\right) \in L_y$. It follows that up to isometry y can be chosen in the form (3) or (4) with $z = 0$ if $s = 32$ or $s = 24$ and Λ does not exist if $s = 16$.

If $\frac{1}{\sqrt{2}}V$ is odd $z \notin V$. Hence there is an $x \in V$ such that $(z, x) \equiv 1$ (mod 2) and therefore in the case (4)

$$\frac{1}{2}y + a_1 + x = \frac{1}{4}(a_1 + \ldots + a_s) + \frac{1}{2}z + x \in L_y.$$

Hence it is sufficient to consider the case (3).

Now let y_1, y_2 be vectors of L such that $(L_{y_i})_2 = \phi$ and

$$y_i = \frac{1}{2}(a_1 + \ldots + a_s) + z_i,\ z_i \in V,\ i = 1,\ 2.$$

Then $z_1 - z_2 \in V$. Hence there is a $u \in U^*$ with

$$u + \frac{1}{2}(z_1 - z_2) \in L,\ \left(u + \frac{1}{2}(z_1 - z_2), w_2\right) \in 2\mathbb{Z}.$$

Therefore

$$\frac{1}{4}(a_1 + \ldots + a_s) + u + \frac{1}{2}z_1 \in L_{y_2}.$$

This shows that L_{y_2} is isometric to L_{y_3}

$$y_3 = \frac{1}{2}(a_1 + \ldots + a_{17}) + z_1$$

or

$$y_3 = \frac{1}{2}(-3a_1 + a_2 + \ldots + a_{17}) + z_1$$

But in the second case L_{y_3} is odd. Hence L_{y_2} is isometric to L_{y_1}.

References

[0] Conway J. H., Pless V., On the enumeration of self-dual codes, J. Comb Th. Ser. A, 28 (1980), 26–53.

[1] Koch H., Venkov B. B., Ganzzahlige unimodulare Gitter in euklidischen Räumen. J. reine angew. Math. 398, 144–168 (1989).

[2] Koch H., Venkov B.B., Über gerade unimodulare Gitter der Dimension 32, III, Preprint des Max-Planck-Institut für Mathematik Bonn MPI/89-85 (1989), Mathem. Nachr. 152, 191–213 (1991).

[3] Nebe G., Anhang zu [2].

[4] Plesken W., Pohst M., Constructing integral lattices with prescribed minimum. I, Math. of Comp. 45, Nr. 171, July 1985, 209–221.

[5] Venkov B.B., Even unimodular lattices of dimension 32, Zap. Nauchn. Sem. LOMI 116, 44–55 (1982) (Russian).