Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Ichiro SHIMADA

A note on Quebbemann's extremal lattices of rank 64

Tome 34, nº 3 (2022), p. 813-826.

https://doi.org/10.5802/jtnb.1229

CENTRE MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **34** (2022), 813–826

A note on Quebbemann's extremal lattices of rank 64

par Ichiro SHIMADA

Résumé. En construisant des exemples explicites, nous montrons que la méthode de Quebbemann permet d'obtenir de nombreuses classes d'isomorphisme de réseaux extrémaux de dimension 64. Beaucoup de ces exemples n'ont pas d'automorphismes non triviaux.

Abstract. By constructing explicit examples, we show that the method of Quebbemann yields many isomorphism classes of extremal lattices of rank 64. Many of these examples have no non-trivial automorphisms.

1. Introduction

By a *lattice*, we mean an integral positive-definite lattice. Let L be an even unimodular lattice with the bilinear form $\langle\,\cdot\,,\cdot\,\rangle_L\colon L\times L\to\mathbb{Z}$. We put

$$\min(L) := \min\{\langle x,x\rangle_L \mid x\in L,\ x\neq 0\}.$$

It is well-known that the rank n of L is divisible by 8, and that $\min(L)$ satisfies

$$\min(L)\le 2+2\left\lfloor\frac{n}{24}\right\rfloor. \tag{1.1}$$

We say that an even unimodular lattice L of rank n is *extremal* if the equality holds in (1.1). Extremal lattices are an important research subject, because they give rise to sphere packings of high density.

Not so many *explicit* examples of extremal lattices are known. Moreover, since the construction of these examples involves very special algebraic objects, each of the known examples has a large automorphism group. For example, the automorphism group $\mathrm{O}(\Lambda)$ of the Leech lattice Λ is of order $2^{22}\cdot 3^9\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 23$.

On the other hand, it was shown in [8] that the number of isomorphism classes of extremal lattices of rank 40 is $> 8.45\times 10^{51}$. Since this bound was proved by means of a mass formula, we do not obtain explicit examples of extremal lattices of rank 40 from this result.

Manuscrit reçu le 9 juin 2021, accepté le 9 juillet 2021.
2010 *Mathematics Subject Classification.* 11H31, 11H56.
Mots-clefs. extremal lattice.
This work was supported by JSPS KAKENHI Grant Number 20H01798 and 20K20879.

We consider extremal lattices of rank 64. Quebbemann [10] gave a method to construct extremal lattices Q of rank 64 from certain ternary codes B. We call an extremal lattice of rank 64 a *Quebbemann lattice* if it is obtained by (a generalization of) this method. See Section 2 for the precise definition. A remarkable property of Quebbemann's construction is that the condition on the ternary code B required in order for the lattice Q to be extremal is an *open* condition. Therefore we expect that, by generating sufficiently general ternary codes B, we obtain many extremal lattices of rank 64. Another nice feature of this construction is that we can calculate the set $\mathrm{Min}(Q)$ of non-zero minimal-norm vectors of a Quebbemann lattice Q (that is, the set of vectors v with $\langle v, v\rangle_Q = 6$). It turns out that, by means of $\mathrm{Min}(Q)$, it is possible to compute the automorphism group of Q, and to compare the isomorphism class of Q with isomorphism classes of other Quebbemann lattices.

The purpose of this note is to generalize Quebbemann's construction slightly, and to show that this method indeed yields many mutually non-isomorphic extremal lattices of rank 64, by choosing the ternary code B (pseudo-)randomly, and that their automorphism groups are often very small. Our main result below is proved by producing Quebbemann lattices Q explicitly.

Theorem 1.1. *Quebbemann's method yields*

(1) *at least* 300 *isomorphism classes of extremal lattices Q of rank* 64 *such that* $\mathrm{O}(Q) = \{\pm 1\}$, *and*
(2) *at least* 100 *isomorphism classes of extremal lattices Q of rank* 64 *such that* $\mathrm{O}(Q) \cong \{\pm 1\} \times \mathbb{Z}/8\mathbb{Z}$.

See Section 2 for the method to produce Quebbemann lattices, Section 3.1 for a method to enumerate minimal-norm vectors, Section 3.2 for a method to distinguish isomorphism classes, and Section 3.3 for the computation of the automorphism groups. We exhibit a few examples in detail in Section 4. The computation data of a part of the lattices in Theorem 1.1 is available from the author's web-page [12]. (The whole data is too large to be put on a website.) These data are written in the `Record` format of `GAP` [3].

In Chapter 8.3(d) of [2], Conway and Sloane constructed a Quebbemann lattice that is different from the one given in Quebbemann's original paper [10], and suggested that there exist several isomorphism classes of Quebbemann lattices. In [9], Quebbemann showed by means of a mass formula that there exist at least two isomorphism classes. The ease with which we can make non-isomorphic Quebbemann lattices suggests that the number of isomorphism classes is very huge.

Unimodular lattices with no non-trivial automorphisms have been studied by many authors since the work of Bannai [1]. In [6], an even unimodular

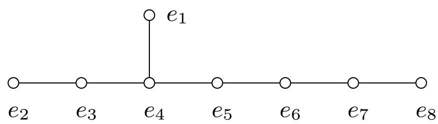

FIGURE 2.1. Dynkin diagram of type E_8

lattice of rank 64 without non-trivial automorphisms is constructed. This lattice is, however, not extremal.

In [7], Nebe constructed an extremal lattice of rank 64 by a different method. The order of the automorphism group is at least 587520. In [4] and [5], the existence of extremal Type II $\mathbb{Z}_{2k}$-codes of length 64 was shown. The isomorphism classes and the automorphism groups of the associated extremal lattices are, however, not clear. In [11], another extremal lattice of rank 64 was constructed by means of a generalized quadratic residue code. Its automorphism group is of order 119040.

Acknowledgments. Thanks are due to Professor Masaaki Harada and the anonymous referees for their comments on the first version of this paper.

Conventions. Elements of a vector space or a lattice are written as *row* vectors. For a lattice L or a quadratic space L, we denote by $\langle \cdot, \cdot \rangle_L$ the symmetric bilinear form on L. The automorphism group $\mathrm{O}(L)$ of $(L, \langle \cdot, \cdot \rangle_L)$ acts on L from the *right*.

2. Quebbemann lattice

2.1. Quebbemann's construction. We recall Quebbemann's construction [10] of extremal lattices of rank 64. See also Chapter 8.3 (d) of [2]. In fact, our construction below is slightly more general than Quebbemann's original.

Let E be the root lattice of type E_8, that is, E is the lattice of rank 8 generated by vectors $e_1, \dots, e_8$ with $\langle e_i, e_i \rangle_E = 2$ that form the dual graph in Figure 2.1. It is well-known that E is unimodular.

We consider the $\mathbb{F}_3$-quadratic space $U := E/3E$. A subspace V of U is said to be *maximal isotropic* if $\dim V = 4$ and $\langle v, v \rangle_U = 0$ holds for all $v \in V$. There exists a direct sum decomposition

$$U = V \oplus W, \quad \text{where } V \text{ and } W \text{ are maximal isotropic subspaces.} \tag{2.1}$$

Let $\mathcal{D}$ be the set of ordered pairs (V, W) of maximal isotropic subspaces of U satisfying $V \cap W = 0$. Since $\langle \cdot, \cdot \rangle_U$ is non-degenerate, we have a natural isomorphism

$$W \cong \mathrm{Hom}(V, \mathbb{F}_3) \quad \text{for each } (V, W) \in \mathcal{D}. \tag{2.2}$$

Let S denote the orthogonal direct sum E^8 of eight copies of E. Then S is unimodular of rank 64. For $i=1,\dots 8$, we denote by U_i the i^{th}-factor of $S/3S=U^8$. We choose and fix an element

$$\Delta := (\,(V_1,W_1),\dots,(V_8,W_8)\,)$$

of $\mathcal{D}^8$. We put $T:=\{1,\dots,8\}$, and for a subset J of T, we put

$$U_J := \bigoplus_{j\in J} U_j,\quad V_J := \bigoplus_{j\in J} V_j,\quad W_J := \bigoplus_{j\in J} W_j.$$

Then we have

$$S/3S \;=\; U_T \;=\; V_T\oplus W_T.$$

We consider U_T, V_T and W_T as $\mathbb{F}_3$-vector spaces. Let B be a linear subspace of V_T with $\dim B=8$. Note that W_T can be regarded as the dual space of V_T by (2.2). We put

$$B^\perp := \{\bar z\in W_T \mid \langle \bar z,\bar y\rangle_{U_T}=0 \text{ for all } \bar y\in B\}.$$

Then we have $\dim B^\perp = 24$. Let $\pi\colon S\to S/3S=U_T$ denote the natural projection. For any elements $\bar x,\bar x'$ of $B\oplus B^\perp\subset U_T$, we have $\langle \bar x,\bar x'\rangle_{U_T}=0$, and hence, for any elements x,x' of the pre-image $\pi^{-1}(B\oplus B^\perp)$, we have $\langle x,x'\rangle_S\equiv 0 \bmod 3$. We denote by $Q(\Delta,B)$ the lattice whose underlying $\mathbb{Z}$-module is $\pi^{-1}(B\oplus B^\perp)$ and whose bilinear form $\langle\,\cdot\,,\cdot\,\rangle_Q$ is given by

$$\langle\,\cdot\,,\cdot\,\rangle_Q := \frac{1}{3}\,\langle\,\cdot\,,\cdot\,\rangle_S.$$

Then $Q:=Q(\Delta,B)$ is an even lattice, and we have

$$\det Q = \left(\frac{1}{3}\right)^{64}\det S\cdot[S:Q]^2 = \left(\frac{1}{3}\right)^{64}\left(\frac{|U_T|}{|B\oplus B^\perp|}\right)^2 = 1.$$

Definition 2.1. For $J=\{i,j\}\subset T$ with $|J|=2$, we denote by $p_J\colon B\to V_J$ the projection to the J-factor. We say that B satisfies p_2-*condition* if p_J is an isomorphism for all $J\subset T$ with $|J|=2$.

Remark 2.2. If the projection $p_J\colon B\to V_J$ is an isomorphism, then the projection $p_{T\setminus J}\colon B^\perp\to W_{T\setminus J}$ to the $(T\setminus J)$-factor is also an isomorphism. Hence, if B satisfies p_2-condition, then $B^\perp$ satisfies the following p_6-*condition*: for all $J'\subset T$ with $|J'|=6$, the projection $p_{J'}\colon B^\perp\to W_{J'}$ to the J'-factor is an isomorphism.

It is obvious that p_2-condition imposes an open condition on the Grassmannian variety of 8-dimensional subspaces B of V_T.

Proposition 2.3 (Quebbemann [10])**.** *Let $U_T=V_T\oplus W_T$ be the decomposition of $U_T=S/3S$ associated with an element Δ of $\mathcal{D}^8$, and let B be an 8-dimensional subspace of V_T. Suppose that B satisfies* p_2*-condition. Then $\min(Q(\Delta,B))=6$ holds, that is, $Q(\Delta,B)$ is an extremal lattice of rank* 64.

Proof. We write $x \in Q(\Delta, B)$ as $x = (x_1, \dots, x_8)$, where $x_i \in E$ is the i^{th} component by the embedding $Q(\Delta, B) \hookrightarrow S = E^8$. We put

$$\bar{x} := \pi(x) = (\bar{x}_1, \dots, \bar{x}_8) \;\in\; B \oplus B^\perp \;\subset\; U_T,$$

where $\bar{x}_i \in U_i$ is $x_i \bmod 3E$. Decomposing each $\bar{x}_i$ as $\bar{y}_i + \bar{z}_i$ with $\bar{y}_i \in V_i$ and $\bar{z}_i \in W_i$, we obtain $\bar{x} = \bar{y} + \bar{z}$, where

$$\bar{y} := (\bar{y}_1, \dots, \bar{y}_8) \in B, \quad \bar{z} := (\bar{z}_1, \dots, \bar{z}_8) \in B^\perp.$$

Suppose that $\langle x, x\rangle_Q \le 4$. We show that $x = 0$. Since

$$\langle x, x\rangle_S = \sum \langle x_i, x_i\rangle_E \le 12, \tag{2.3}$$

we see that at least two of the components x_i are zero. Since at least two of $\bar{y}_i$ are zero, the assumption that B satisfy p_2-condition implies $\bar{y} = 0$. Therefore we have $\bar{x} = \bar{z}$. In particular, each $\bar{x}_i$ belongs to W_i. Since W_i is isotropic in $U = E/3E$, we have $\langle x_i, x_i\rangle_E \equiv 0 \bmod 3$ and hence $\langle x_i, x_i\rangle_E \equiv 0 \bmod 6$. Combining this with (2.3), we see that at most two of x_i are non-zero. Since $B^\perp$ satisfies p_6-condition by Remark 2.2, we see that $\bar{z} = 0$. Therefore $\bar{x} = 0$, and hence $x \in 3S$. If x were non-zero, we would have $\langle x, x\rangle_S \ge 18$, which is a contradiction. □

Definition 2.4. An extremal lattice of rank 64 of the form $Q(\Delta, B)$, where Δ is an element of $\mathcal{D}^8$ and B is an 8-dimensional subspace of V_T satisfying p_2-condition, is called a *Quebbemann lattice*.

2.2. Maximal isotropic subspaces of U. Recall that the lattice E is equipped with a basis $e_1, \dots, e_8$ in Figure 2.1. We write elements of E or of $U = E/3E$ as row vectors with respect to $e_1, \dots, e_8$. The automorphism group $\mathrm{O}(E)$ of E is generated by the reflections

$$x \;\mapsto\; x \;-\; \langle x, e_i\rangle_E \, e_i$$

with respect to the vectors e_i $(i = 1, \dots, 8)$ of norm 2, and the order of $\mathrm{O}(E)$ is $2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$. The natural homomorphism $\mathrm{O}(E) \to \mathrm{O}(U)$ to the automorphism group of the $\mathbb{F}_3$-quadratic space U is injective. Let $\mathcal{V}$ be the set of maximal isotropic subspaces V of U. We can prove the following by the standard orbit stabilizer algorithm using `GAP` [3].

Proposition 2.5. *The size of $\mathcal{V}$ is* 2240*, and* $\mathrm{O}(E)$ *acts transitively on the set $\mathcal{V}$.*

Let $V_0 \in \mathcal{V}$ be the maximal isotropic subspace with basis $v_1, \dots, v_4$ in Table 2.1. The stabilizer subgroup $\mathrm{Stab}(V_0)$ of V_0 in $\mathrm{O}(E)$ is of order $2^8 \cdot 3^5 \cdot 5$. Let $\mathcal{W}(V_0)$ be the set of all $W \in \mathcal{V}$ such that $V_0 \cap W = 0$. We have $|\mathcal{W}(V_0)| = 729$.

TABLE 2.1. Bases of maximal isotropic subspaces $V_0, W^{\mathrm{I}}, W^{\mathrm{II}}$

$$v_1 = (0,0,0,0,0,0,1,2), \qquad v_2 = (0,0,0,1,2,0,0,0),$$
$$v_3 = (0,1,0,0,1,0,0,1), \qquad v_4 = (1,0,2,0,0,0,0,1).$$

$$v_1^{*\mathrm{I}} = (1,2,1,0,2,2,0,2), \qquad v_2^{*\mathrm{I}} = (0,1,2,0,0,0,0,0),$$
$$v_3^{*\mathrm{I}} = (2,2,1,0,1,0,2,2), \qquad v_4^{*\mathrm{I}} = (1,0,2,0,1,0,2,1).$$

$$v_1^{*\mathrm{II}} = (1,2,1,0,2,2,0,2), \qquad v_2^{*\mathrm{II}} = (1,1,1,0,0,0,0,1),$$
$$v_3^{*\mathrm{II}} = (0,2,0,0,1,0,2,0), \qquad v_4^{*\mathrm{II}} = (1,2,2,2,1,0,2,0).$$

Proposition 2.6. *The action of* $\mathrm{Stab}(V_0)$ *decomposes* $\mathcal{W}(V_0)$ *into two orbits of size* 648 *and* 81*. The orbit of size* 648 *contains* W^{I} *with basis* $v_1^{*\mathrm{I}}, \dots, v_4^{*\mathrm{I}}$ *in Table 2.1, and the orbit of size* 81 *contains* W^{II} *with basis* $v_1^{*\mathrm{II}}, \dots, v_4^{*\mathrm{II}}$ *in Table 2.1.* □

Remark 2.7. The basis $v_1^*, \dots, v_4^*$ of W above is dual to the basis $v_1, \dots, v_4$ of V_0 by the canonical pairing (2.2).

Corollary 2.8. *The action of* $\mathrm{O}(E)$ *decomposes* $\mathcal{D}$ *into two orbits. One orbit contains* (V_0, W^{I}) *with the stabilizer subgroup* G^{I} *of order* 480*, and the other orbit contains* (V_0, W^{II}) *with the stabilizer subgroup* G^{II} *of order* 3840*.*

2.3. Construction of $Q(\Delta, B)$ with an automorphism of order 8. We fix a pair $(V, W) \in \mathcal{D}$, and consider the 8-tuple

$$\Delta_0 := ((V,W), \dots, (V,W)) \in \mathcal{D}^8.$$

Let G be the stabilizer subgroup of (V, W) in $\mathrm{O}(E)$, and let γ be an element of order 8 in G. (The stabilizer subgroup G^{I} (resp. G^{II}) in Corollary 2.8 contains 120 elements (resp. 1360 elements) of order 8.) We define an automorphism $\tilde{\gamma}$ of $S = E^8$ by

$$x = (x_1, \dots, x_8) \mapsto x^{\tilde{\gamma}} = (x_2^{\gamma}, \dots, x_8^{\gamma}, x_1^{\gamma}).$$

The action of $\tilde{\gamma}$ on $S/3S = U_T$ preserves the decomposition $U_T = V_T \oplus W_T$ associated with Δ_0 above. For $v \in V_T = V^8$, we denote by $B(\gamma, v)$ the linear subspace of V_T generated by the orbit of v under the action of $\langle \tilde{\gamma} \rangle \cong \mathbb{Z}/8\mathbb{Z}$. If $B(\gamma, v)$ is of dimension 8 and satisfies p_2-condition, then $Q(\Delta_0, B(\gamma, v))$ is a Quebbemann lattice invariant under the action of $\langle \tilde{\gamma} \rangle$ on S. In particular, the automorphism group $\mathrm{O}(Q)$ of $Q := Q(\Delta_0, B(\gamma, v))$ contains an element

$$\tilde{\gamma}_Q := \tilde{\gamma} | Q$$

of order 8.

Table 3.1. $N(a,E)$ and $N(a,U)$

a	$\lvert N(a,E)\rvert$	$\lvert N(a,U)\rvert$
0	1	1
2	240	240
4	2160	2160
6	6720	2240

3. Computations on Quebbemann lattices

We fix an 8-tuple $\Delta = ((V_1, W_1), \ldots, (V_8, W_8)) \in \mathcal{D}^8$. Let B be an 8-dimensional linear subspace of $V_T = V_1 \oplus \cdots \oplus V_8$ satisfying p_2-condition, and we consider the extremal lattice $Q(\Delta, B)$ of rank 64.

3.1. Enumeration of minimal-norm vectors. In this section, we explain a method to calculate the set

$$\mathrm{Min}(Q(\Delta, B)) := \{x \in Q \mid \langle x, x\rangle_Q = 6\} = \{x \in Q \mid \langle x, x\rangle_S = 18\}$$

of all minimal-norm vectors of $Q := Q(\Delta, B)$. A *norm-type* is an 8-tuple $[n_1, \ldots, n_8]$ of non-negative even integers n_i such that $\sum n_i = 18$. For $x = (x_1, \ldots, x_8) \in \mathrm{Min}(Q(\Delta, B))$, we put

$$\nu(x) := [\langle x_1, x_1\rangle_E, \ldots, \langle x_8, x_8\rangle_E],$$

and call it the *norm-type of* x. For a non-negative even integer a, we put

$$N(a, E) := \{v \in E \mid \langle v, v\rangle_E = a\},$$

and let $N(a, U) \subset U$ be the image of $N(a, E)$ by the natural projection $E \to U$. (See Table 3.1.) A minimal-norm vector $x \in \mathrm{Min}(Q(\Delta, B))$ is said to be *of divisible type* if $x \in 3S$ holds, or equivalently, if only one of $x_1, \ldots, x_8$ (say x_i) is non-zero and x_i is written as $3x'_i$ by some $x'_i \in N(2, E)$, or equivalently, if the norm-type $\nu(x)$ of x is obtained by a permutation of components from $[0, \ldots, 0, 18]$. Since $|N(2, E)| = 240$, there exist exactly 240×8 minimal-norm vectors of divisible type.

Proposition 3.1. *Let $x \in Q(\Delta, B)$ be a minimal-norm vector that is not of divisible type. Then the norm-type $\nu(x)$ of x is obtained by a permutation of components from one of the following:*

$$(3.1)\qquad \begin{array}{ll} [0,0,0,0,0,6,6,6] & (\text{of type } 0^5 6^3), \\ [0,2,2,2,2,2,4,4] & (\text{of type } 0^1 2^5 4^2), \\ [0,2,2,2,2,2,2,6] & (\text{of type } 0^1 2^6 6^1), \\ [2,2,2,2,2,2,2,4] & (\text{of type } 2^7 4^1). \end{array}$$

Proof. As in the proof of Proposition 2.3, we see that $\bar{x} := \pi(x) \in B \oplus B^{\perp}$ is decomposed uniquely as $\bar{y} + \bar{z}$, where $\bar{y} = (\bar{y}_1, \ldots, \bar{y}_8) \in B$ and $\bar{z} = (\bar{z}_1, \ldots, \bar{z}_8) \in B^{\perp}$. Suppose that $\bar{y} = 0$. Since x is not of divisible type, we

<table>
<tr><td>I_8</td><td></td><td>C_{13}</td><td>C_{14}</td><td>C_{15}</td><td>C_{16}</td><td>C_{17}</td><td>C_{18}</td></tr>
<tr><td></td><td>I_8</td><td>C_{23}</td><td>C_{24}</td><td>C_{25}</td><td>C_{26}</td><td>C_{27}</td><td>C_{28}</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td>A_3</td><td></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">C_{37}</td><td rowspan="2">C_{38}</td></tr>
<tr><td></td><td>A_4</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td>A_5</td><td></td><td rowspan="2">C_{47}</td><td rowspan="2">C_{48}</td></tr>
<tr><td></td><td>A_6</td></tr>
</table>

FIGURE 3.1. Echelon form of a generator matrix of $B \oplus B^{\perp}$

see that $\bar{x} = \bar{z}$ is not zero. Since $B^{\perp}$ satisfies p_6-condition, at most five of $\bar{z}_1, \dots, \bar{z}_8$ are zero. Since $\bar{x}_i = \bar{z}_i \in W_i$, we have $\langle x_i, x_i \rangle_E \equiv 0 \bmod 3$ and hence $\langle x_i, x_i \rangle_E \in \{0, 6, 12, 18\}$. Combining these, we see that $\nu(x)$ is of type $0^5 6^3$. Suppose that $\bar{y} \neq 0$. Since B satisfies p_2-condition, at most one of $\bar{y}_1, \dots, \bar{y}_8$ is zero. Hence at most one of $x_1, \dots, x_8$ is zero. Therefore $\nu(x)$ is either of type $0^1 2^5 4^2$ or $0^1 2^6 6^1$ or $2^7 4^1$. $\square$

For $k = 1, \dots, 8$, let $e_1^{(k)}, \dots, e_8^{(k)}$ be the copy of the basis $e_1, \dots, e_8$ of E in the k^{th} factor of $S = E^8$. We use the ordered set

$$e_1^{(1)}, \dots, e_8^{(1)}, e_1^{(2)}, \dots, e_8^{(2)}, \dots\dots\dots, e_1^{(8)}, \dots, e_8^{(8)} \tag{3.2}$$

of vectors as a basis of S and of $S/3S = U^8 = U_T$.

Proposition 3.2. *The ternary code $B \oplus B^{\perp} \subset U_T$ is generated by row vectors of a 32×64 matrix of the echelon form as in Figure 3.1, where I_8 is the identity matrix of size 8, A_i are 4×8 matrices whose row vectors form a basis of $W_i \subset U$ for $i = 3, \dots, 6$, $C_{\mu\nu}$ are some 8×8 matrices, and the blank blocks are zero matrices.*

Proof. Since the projection $p_{12} \colon B \to V_1 \oplus V_2$ to the (12)-factor and the projection $p_{\overline{78}} \colon B^{\perp} \to W_1 \oplus \cdots \oplus W_6$ to the (123456)-factor are both isomorphisms, the projection

$$P_{12} \colon B \oplus B^{\perp} \to U \oplus U$$

to the (12)-factor is surjective, and its kernel $\operatorname{Ker} P_{12}$ is mapped isomorphically to $W_3 \oplus \cdots \oplus W_6$ by the projection

$$P_{3456} \colon \operatorname{Ker} P_{12} \to U \oplus U \oplus U \oplus U$$

to the (3456)-factor. $\square$

We make the symmetric group $\mathfrak{S}_8$ act on $S = E^8$ by

$$(x_1, \dots, x_8)^\sigma := (x_{\sigma(1)}, \dots, x_{\sigma(8)}) \quad \text{for } \sigma \in \mathfrak{S}_8.$$

For $\Delta = ((V_1, W_1), \dots, (V_8, W_8)) \in \mathcal{D}^8$, we put

$$\Delta^\sigma := ((V_{\sigma(1)}, W_{\sigma(1)}), \dots, (V_{\sigma(8)}, W_{\sigma(8)})).$$

Then we have $Q(\Delta, B)^\sigma = Q(\Delta^\sigma, B^\sigma)$ in S. If $x \in \mathrm{Min}(Q(\Delta, B))$ is of norm-type $[n_1, \dots, n_8]$, then $x^\sigma \in \mathrm{Min}(Q(\Delta^\sigma, B^\sigma))$ is of norm-type $[n_{\sigma(1)}, \dots, n_{\sigma(8)}]$.

Let $n = [n_1, \dots, n_8]$ be a norm-type obtained by a permutation of components from one of the norm-types in (3.1). We calculate the set $\overline{M}(n)$ of codewords $\bar{x} = \pi(x) \in B \oplus B^\perp$ corresponding $x \in \mathrm{Min}(Q(\Delta, B))$ with $\nu(x) = n$ by the following method.

First we choose a permutation $\tau \in \mathfrak{S}_8$ such that $n^\tau = [n_{\tau(1)}, \dots, n_{\tau(8)}]$ satisfies

$$n_{\tau(1)} \le n_{\tau(2)} \le \dots \le n_{\tau(8)}.$$

We then transform a generator matrix of $(B \oplus B^\perp)^\tau = B^\tau \oplus B^{\tau\perp}$ into the echelon form in Figure 3.1, and search for $\bar{x}_1, \dots, \bar{x}_8 \in U$ satisfying conditions (3.3) below by back track search; that is, if we find $(\bar{x}_1, \dots, \bar{x}_i)$ satisfying the first i conditions of (3.3), then we search for $\bar{x}_{i+1}$ satisfying the $(i+1)^{\text{st}}$ condition of (3.3). Recall that $N(n_i, U)$ is the image of $N(n_i, E)$ by the natural map $E \to U$.

$$(3.3)\quad \begin{aligned} &\bar{x}_1 \in N(n_{\tau(1)}, U), \\ &\bar{x}_2 \in N(n_{\tau(2)}, U), \\ &\bar{x}_3 := \bar{x}_1 C_{13} + \bar{x}_2 C_{23} + \bar{u}_3 A_3 \in N(n_{\tau(3)}, U), \text{ where } \bar{u}_3 \in \mathbb{F}_3^4, \\ &\bar{x}_4 := \bar{x}_1 C_{14} + \bar{x}_2 C_{24} + \bar{u}_4 A_4 \in N(n_{\tau(4)}, U), \text{ where } \bar{u}_4 \in \mathbb{F}_3^4, \\ &\bar{x}_5 := \bar{x}_1 C_{15} + \bar{x}_2 C_{25} + \bar{u}_5 A_5 \in N(n_{\tau(5)}, U), \text{ where } \bar{u}_5 \in \mathbb{F}_3^4, \\ &\bar{x}_6 := \bar{x}_1 C_{16} + \bar{x}_2 C_{26} + \bar{u}_6 A_6 \in N(n_{\tau(6)}, U), \text{ where } \bar{u}_6 \in \mathbb{F}_3^4, \\ &\bar{x}_7 := \bar{x}_1 C_{17} + \bar{x}_2 C_{27} + (\bar{u}_3, \bar{u}_4) C_{37} + (\bar{u}_5, \bar{u}_6) C_{47} \in N(n_{\tau(7)}, U), \\ &\bar{x}_8 := \bar{x}_1 C_{18} + \bar{x}_2 C_{28} + (\bar{u}_3, \bar{u}_4) C_{38} + (\bar{u}_5, \bar{u}_6) C_{48} \in N(n_{\tau(8)}, U). \end{aligned}$$

If we find $\bar{x} = (\bar{x}_1, \dots, \bar{x}_8)$ satisfying all conditions in (3.3), then $\bar{x}$ belongs to $\overline{M}(n^\tau)$ and hence

$$\bar{x}^{\tau^{-1}} = (\bar{x}_{\tau^{-1}(1)}, \dots, \bar{x}_{\tau^{-1}(8)})$$

is an element of $\overline{M}(n)$. All elements of $\overline{M}(n)$ are obtained in this way.

Using the maps $N(a, E) \to N(a, U)$, we can make from $\overline{M}(n)$ the set $M(n)$ of vectors $x \in \mathrm{Min}(Q(\Delta, B))$ with $\nu(x) = n$. Taking the union of these sets $M(n)$ together with the set of minimal-norm vectors of divisible type, we obtain the set $\mathrm{Min}(Q(\Delta, B))$ of all minimal-norm vectors of $Q(\Delta, B)$.

Remark 3.3. Thanks to the permutation τ, we have $|N(n_{\tau(i)}, U)| \le |N(n_{\tau(j)}, U)|$ for $i < j$, and hence, in the back track search above, there exist few possibilities of $\bar{x}_i$ for small indexes i. By this trick, the enumeration of $\mathrm{Min}(Q(\Delta, B))$ becomes tractable.

Remark 3.4. We know that $|\mathrm{Min}(L)| = 2611200$ for an extremal lattice L of rank 64 by the theory of theta series and modular forms. (See, for example, [2, Chapter 7.7].) Hence we can confirm easily that we left no minimal-norm vectors uncounted.

3.2. Isomorphism classes. In order to distinguish isomorphism classes of two extremal lattices L and L' of rank 64, we use the *distribution of intersection patterns of minimal-norm vectors*. Let $\mathrm{Min}(L)$ be the set of vectors $v \in L$ with $\langle v, v\rangle_L = 6$. For $v, v' \in \mathrm{Min}(L)$, we have $\langle v, v'\rangle_L \in \{0, \pm 1, \pm 2, \pm 3, \pm 6\}$. For $k = 0, 1, 2, 3, 6$, we put

$$a_k(v) := \frac{1}{2}\left|\{v' \in \mathrm{Min}(L) \mid \langle v, v'\rangle_L = k \text{ or } -k\}\right|.$$

We have $a_6(v) = 1$ and $\sum a_k(v) = 1305600$. The triple

$$a(v) := [a_1(v), a_2(v), a_3(v)]$$

is called the *intersection pattern* of v. For a triple $a = [a_1, a_2, a_3]$ of non-negative integers with $a_1 + a_2 + a_3 + 1 \le 1305600$, we put

$$\mathcal{A}_L(a) := \{v \in \mathrm{Min}(L) \mid a(v) = a\}, \quad A_L(a) := \frac{1}{2}\,|\mathcal{A}_L(a)|,$$

and call the function A_L the *distribution of intersection patterns*. It is obvious that, if $A_L \ne A_{L'}$, then L and L' are not isomorphic.

Remark 3.5. In fact, the calculation of intersection patterns $a(v)$ of all elements v of $\mathrm{Min}(Q(\Delta, B))/\{\pm 1\}$ takes most of the computation time in the proof of Theorem 1.1.

3.3. Automorphism group. Let L be an extremal lattice of rank 64, and let Γ be a subgroup of $\mathrm{O}(L)$. We will apply Proposition 3.7 below to the cases $\Gamma = \{\pm 1\}$ and $\Gamma = \{\pm 1\} \times \langle \widetilde{\gamma}_Q\rangle$, where $\widetilde{\gamma}_Q$ is the automorphism of $Q(\Delta_0, B(\gamma, v))$ introduced in Section 2.3.

Definition 3.6. An ordered list $(v_1, \dots, v_{64})$ of vectors in $\mathrm{Min}(L)$ is said to be a Γ-*rigidifying basis* if the following hold:

(a) The vectors $v_1, \dots, v_{64}$ form a basis of $L \otimes \mathbb{Q}$.
(b) The group Γ acts on the set $\mathcal{A}_L(a(v_1))$ transitively.
(c) Suppose that $i > 1$. Then the set

$$\{v' \in \mathcal{A}_L(a(v_i)) \mid \langle v', v_j\rangle_L = \langle v_i, v_j\rangle_L \text{ for all } j < i\,\}$$

consists of a single element v_i.

Proposition 3.7. *If a* Γ*-rigidifying basis exists, then* $\mathrm{O}(L)$ *is equal to* Γ.

Table 4.1. Matrix G_0'

$$\left[\begin{array}{cccc|cccc|cccc|cccc|cccc|cccc}
0&0&2&0&1&0&0&1&1&0&2&2&1&0&0&1&1&0&2&1&0&2&2&2\\
1&1&0&2&2&0&0&1&0&1&0&1&1&0&0&2&0&1&1&0&2&0&1&2\\
1&0&2&0&0&2&0&0&2&1&0&1&1&0&1&1&1&2&1&2&0&2&1&1\\
2&1&0&0&1&1&1&1&1&0&1&0&2&1&0&0&1&2&0&0&0&2&2&0\\
\hline
1&1&0&0&2&0&1&2&1&0&2&2&0&0&2&2&2&1&0&1&1&1&2&2\\
2&0&1&0&2&0&0&1&1&0&0&2&0&2&0&0&1&1&1&0&1&0&1&2\\
1&0&2&1&2&2&2&1&1&2&2&2&1&1&1&2&1&1&1&2&1&2&2&1\\
2&2&1&1&2&0&2&2&1&0&2&1&1&0&1&1&1&1&2&1&0&0&2&0
\end{array}\right]$$

Proof. Note that $\mathrm{O}(L)$ preserves each subset set $\mathcal{A}_L(a)$ of $\mathrm{Min}(L)$ for any a. In particular, we have $v^g \in \mathcal{A}_L(a(v))$ for any $g \in \mathrm{O}(L)$ and any $v \in L$. Let g be an arbitrary element of $\mathrm{O}(L)$. By (b), there exists an element $g' \in \Gamma$ such that $v_1^g = v_1^{g'}$. By (c), we can prove that $v_i^g = v_i^{g'}$ holds for all $i = 1, \dots, 64$ by induction on i. Then (a) implies that $g = g'$. □

4. Examples

4.1. Examples without non-trivial automorphisms. Let V_0 be the maximal isotropic subspace of U with basis $v_1, \dots, v_4$ in Table 2.1. By this basis, an element of V_0 is expressed by a vector in $\mathbb{F}_3^4$, and hence an element of V_0^8 is expressed by a vector in $\mathbb{F}_3^{32}$. Let G_0 be the 8×32 matrix with components in $\mathbb{F}_3$ of the form $[\, I_8 \,|\, G_0' \,]$, where I_8 is the identity matrix of size 8 and G_0' is given in Table 4.1. (This matrix G_0' was produced by choosing components pseudo-randomly.) Let B_0 be the linear subspace of V_0^8 generated by the row vectors of G_0. Then B_0 satisfies p_2-condition. Recall that we have given maximal isotropic subspaces W^{I} and W^{II} in Table 2.1. Let Q^{I} (resp. Q^{II}) be the Quebbemann lattice $Q(\Delta^{\mathrm{I}}, B_0)$ (resp. $Q(\Delta^{\mathrm{II}}, B_0)$), where

$$\Delta^{\mathrm{I}} = ((V_0, W^{\mathrm{I}}), \dots, (V_0, W^{\mathrm{I}})) \in \mathcal{D}^8,\ \Delta^{\mathrm{II}} = ((V_0, W^{\mathrm{II}}), \dots, (V_0, W^{\mathrm{II}})) \in \mathcal{D}^8.$$

Then the distributions of intersection patterns of Q^{I} and Q^{II} are as in Table 4.2. (The left table is of Q^{I} and the right is of Q^{II}.) In these tables, the intersection patterns $a = [a_1, a_2, a_3]$ are sorted by the lexicographic order. We can readily see that Q^{I} and Q^{II} are not isomorphic. Both of Q^{I} and Q^{II} have $\{\pm 1\}$-rigidifying basis, and hence $\mathrm{O}(Q^{\mathrm{I}})$ and $\mathrm{O}(Q^{\mathrm{II}})$ are equal to $\{\pm 1\}$.

4.2. Examples with an automorphism of order 8. Let γ be an element of $\mathrm{O}(E)$ represented by the matrix in Table 4.3 with respect to the basis $e_1, \dots, e_8$ of E. Then γ is of order 8 and belongs to the stabilizer subgroup G^{I} of $(V_0, W^{\mathrm{I}}) \in \mathcal{D}$. Let $v = (v_1, \dots, v_8) \in V_0^8$ be

$$(\ 2210 \mid 0120 \mid 0201 \mid 1001 \mid 0201 \mid 0222 \mid 0122 \mid 0122\ ),$$

TABLE 4.2. Distributions of intersection patterns of Q^{I} and Q^{II}

no.	a_1	a_2	a_3	$A_{Q^{\mathrm{I}}}(a)$
1	568092	40191	612	1
2	568290	40155	606	1
3	568356	40143	604	3
4	568488	40119	600	2
5	568554	40107	598	2
6	568620	40095	596	3
7	568686	40083	594	2
8	568752	40071	592	6
9	568818	40059	590	6
10	568884	40047	588	9
	...			
110	579840	38055	256	5333
111	579906	38043	254	6275
112	579972	38031	252	7616
113	580038	38019	250	8752
114	580104	38007	248	10065
115	580170	37995	246	11511
116	580236	37983	244	13332
117	580302	37971	242	15370
118	580368	37959	240	17252
119	580434	37947	238	19533
120	580500	37935	236	22294
	...			
170	583800	37335	136	17
171	583866	37323	134	9
172	583932	37311	132	6
173	583998	37299	130	5
174	584130	37275	126	3
175	584196	37263	124	2
176	584262	37251	122	1
			total	1305600

no.	a_1	a_2	a_3	$A_{Q^{\mathrm{II}}}(a)$
1	568422	40131	602	1
2	568488	40119	600	2
3	568554	40107	598	1
4	568620	40095	596	3
5	568686	40083	594	7
6	568752	40071	592	5
7	568818	40059	590	8
8	568884	40047	588	8
9	568950	40035	586	11
10	569016	40023	584	11
	...			
110	580104	38007	248	9761
111	580170	37995	246	11289
112	580236	37983	244	13121
113	580302	37971	242	15330
114	580368	37959	240	17148
115	580434	37947	238	19598
116	580500	37935	236	22119
117	580566	37923	234	24532
118	580632	37911	232	27067
119	580698	37899	230	29774
120	580764	37887	228	32471
	...			
170	584064	37287	128	2
171	584130	37275	126	1
172	584196	37263	124	2
173	584262	37251	122	1
174	584328	37239	120	1
			total	1305600

TABLE 4.3. Elements of $\mathrm{O}(E)$ of order 8

$$\gamma := \begin{bmatrix} 2 & 1 & 2 & 4 & 3 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -2 & -2 & -2 & -2 & -2 & -1 \\ -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 & -1 & 0 & 0 & 0 \\ 2 & 2 & 3 & 4 & 3 & 2 & 1 & 0 \\ -3 & -2 & -4 & -6 & -5 & -4 & -2 & -1 \\ 2 & 1 & 3 & 4 & 3 & 2 & 1 & 1 \end{bmatrix}, \quad \gamma' := \begin{bmatrix} 1 & 1 & 2 & 2 & 1 & 1 & 1 & 0 \\ -2 & -1 & -2 & -4 & -3 & -2 & -2 & -1 \\ 3 & 2 & 4 & 6 & 5 & 3 & 2 & 1 \\ -2 & -2 & -4 & -5 & -4 & -3 & -2 & -1 \\ 1 & 1 & 2 & 3 & 3 & 3 & 2 & 1 \\ -1 & -1 & -1 & -2 & -2 & -2 & -1 & 0 \\ -1 & 0 & -1 & -1 & -1 & -1 & -1 & -1 \\ 2 & 1 & 2 & 3 & 2 & 2 & 1 & 1 \end{bmatrix}$$

where each component v_i is written with respect to the basis of V_0 in Table 2.1. Then the subspace $B(\gamma, v)$ of V_0^8 satisfies p_2-condition, and we obtain a Quebbemann lattice $Q := Q(\Delta^{\mathrm{I}}, B(\gamma, v))$ with an automorphism

TABLE 4.4. Distributions of intersection patterns of Q and Q'

no.	a_1	a_2	a_3	$A_Q(a)$
1	568026	40203	614	8
2	568092	40191	612	16
3	568290	40155	606	24
4	568356	40143	604	16
5	568422	40131	602	16
	...			
100	580104	38007	248	11240
101	580170	37995	246	12984
102	580236	37983	244	14840
103	580302	37971	242	16712
104	580368	37959	240	18800
105	580434	37947	238	20808
106	580500	37935	236	23184
107	580566	37923	234	25304
108	580632	37911	232	27416
109	580698	37899	230	29720
110	580764	37887	228	32472
	...			
155	583734	37347	138	40
156	583800	37335	136	24
157	583866	37323	134	16
158	583932	37311	132	8
			total	1305600

no.	a_1	a_2	a_3	$A_{Q'}(a)$
1	568092	40191	612	8
2	568224	40167	608	24
3	568290	40155	606	8
4	568488	40119	600	8
5	568686	40083	594	16
	...			
100	580104	38007	248	10688
101	580170	37995	246	12344
102	580236	37983	244	14656
103	580302	37971	242	16064
104	580368	37959	240	19240
105	580434	37947	238	20104
106	580500	37935	236	22984
107	580566	37923	234	25128
108	580632	37911	232	28064
109	580698	37899	230	29128
110	580764	37887	228	32304
	...			
155	583734	37347	138	32
156	583800	37335	136	48
157	583866	37323	134	24
158	583932	37311	132	24
159	583998	37299	130	16
160	584064	37287	128	8
161	584196	37263	124	8
			total	1305600

$\widetilde{\gamma}_Q$ of order 8, where $\Delta^{\mathrm{I}} \in \mathcal{D}^8$ is given in the previous subsection. By the method of Γ-rigidifying basis, we see that $\mathrm{O}(Q) = \{\pm 1\} \times \langle \widetilde{\gamma}_Q \rangle$. The action of $\mathrm{O}(Q)$ decomposes $\mathrm{Min}(Q)$ into $2611200/16 = 163200$ orbits. The distribution of intersection patterns is given in Table 4.4 (left).

Let γ' be an element of $\mathrm{O}(E)$ given in Table 4.3, which is of order 8 and belongs to the stabilizer subgroup G^{II} of $(V_0, W^{\mathrm{II}}) \in \mathcal{D}$. Let $v' \in V_0^8$ be

$$(\ 2220 \mid 0102 \mid 2120 \mid 2220 \mid 2202 \mid 1202 \mid 2220 \mid 2112 \ ) .$$

Then $B(\gamma', v')$ satisfies p_2-condition, and we obtain a Quebbemann lattice $Q' := Q(\Delta^{\mathrm{II}}, B(\gamma', v'))$. We see that $\mathrm{O}(Q') = \{\pm 1\} \times \langle \widetilde{\gamma}_{Q'} \rangle$, and its action decomposes $\mathrm{Min}(Q')$ into 163200 orbits. The distribution of intersection patterns is given in Table 4.4 (right).

References

[1] E. Bannai, *Positive definite unimodular lattices with trivial automorphism groups*, Memoirs of the American Mathematical Society, vol. 429, American Mathematical Society, 1990, 70 pages.

[2] J. H. Conway & N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der Mathematischen Wissenschaften, vol. 290, Springer, 1999, lxxiv+703 pages.
[3] The GAP Group, "GAP — Groups, Algorithms, and Programming, Version 4.11.0", 2020, http://www.gap-system.org.
[4] M. Harada, M. Kitazume & M. Ozeki, "Ternary code construction of unimodular lattices and self-dual codes over $\mathbb{Z}_6$", *J. Algebr. Comb.* **16** (2002), no. 2, p. 209-223.
[5] M. Harada & T. Miezaki, "On the existence of extremal Type II $\mathbb{Z}_{2k}$-codes", *Math. Comput.* **83** (2014), no. 287, p. 1427-1446.
[6] Y. Mimura, "A construction of unimodular lattices without non-trivial automorphisms (a survey)", *RIMS Kokyuroku* **1476** (2006), p. 105-110.
[7] G. Nebe, "Some cyclo-quaternionic lattices", *J. Algebra* **199** (1998), no. 2, p. 472-498.
[8] M. Peters, "Definite unimodular 48-dimensional quadratic forms", *Bull. Lond. Math. Soc.* **15** (1983), p. 18-20.
[9] H.-G. Quebbemann, "An application of Siegel's formula over quaternion orders", *Mathematika* **31** (1984), p. 12-16.
[10] ———, "A construction of integral lattices", *Mathematika* **31** (1984), p. 137-140.
[11] I. Shimada, "An even extremal lattice of rank 64", *J. Number Theory* **185** (2018), p. 1-15.
[12] ———, "A note on Quebbemann's extremal lattices of rank 64: computation data", 2021, http://www.math.sci.hiroshima-u.ac.jp/shimada/lattice.html.

Ichiro Shimada
Department of Mathematics, Graduate School of Science, Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526, Japan
E-mail: ichiro-shimada@hiroshima-u.ac.jp
URL: http://www.math.sci.hiroshima-u.ac.jp/shimada/index.html