EMBEDDING THEORY OF LATTICES AND ITS APPLICATION TO 2-INTEGRABLE LATTICES

Qianqian Yang[1]
Department of Mathematics, Shanghai University, Shanghai, PR China
qqyang@shu.edu.cn

Kiyoto Yoshino[2]
Graduate School of Information Sciences, Tohoku University, Sendai, Miyagi, Japan
kiyoto.yosino.r2@dc.tohoku.ac.jp

Received: 12/6/21, Accepted: 6/2/22,, Published: 6/21/22

Abstract

For a positive integer s, a lattice L is said to be s-integrable if $\sqrt{s} \cdot L$ is isometric to a sublattice of $\mathbb{Z}^n$ for some integer n. Conway and Sloane found two minimal non-2-integrable lattices of rank 12 and determinant 7 in 1989. In this paper, we use a method of embedding a given lattice into a unimodular lattice and see that 15 is the next smallest candidate for the determinant of a non-2-integrable lattice of rank 12. We also find two more minimal non-2-integrable lattices of rank 12 and determinant 15.

1. Introduction

In this paper, by a lattice we mean a positive definite integral $\mathbb{Z}$-lattice, and a unimodular lattice is a positive definite unimodular $\mathbb{Z}$-lattice, unless otherwise specified. Let s be a positive integer. A lattice L is said to be *s-integrable* if $\sqrt{s} \cdot L$ is isometric to a sublattice of $\mathbb{Z}^n$ for some integer n. Let $\phi(s)$ be the smallest rank in which there is a non-s-integrable lattice. In 1937, Ko [8] and Mordell [12] showed $\phi(1) = 6$. Also, the values $\phi(2) = 12$ and $\phi(3) = 14$ were shown in [4, Theorem 1], and the value $\phi(s)$ is not determined if s is at least 4.

There are infinitely many non-1-integrable lattices of rank at least 6. In fact, we can construct infinitely many non-1-integrable lattices of rank 6 as sublattices of $\mathsf{E}_6 \perp \mathbb{Z}$. In addition, it is known that every non-1-integrable lattice of rank 6 is a

[1]Yang is partially supported by the National Natural Science Foundation of China (No. 12071454).
[2]Yoshino is supported by JSPS KAKENHI (No. JP21J14427) and a scholarship from Tohoku University, Division for Interdisciplinary Advanced Research and Education.

sublattice of $\mathsf{E}_6 \perp \mathbb{Z}^m$ (see [13, Theorem 3]). These facts lead us to pay attention to the"minimal" non-1-integrable lattices. Formally, we have the following definition. A lattice L is said to be *non-s-minimal*, if there exist a lattice M and a positive integer m such that $\sqrt{s} \cdot L$ is isometric to a sublattice of $\sqrt{s} \cdot M \perp \mathbb{Z}^m$ which is not contained in $\sqrt{s} \cdot M$. Otherwise it is said to be *s-minimal*. Notice that a non-zero s-integrable lattice is always non-s-minimal. For brevity's sake, if a non-s-integrable lattice is s-minimal, we say it is a *minimal non-s-integrable lattice*. In the case of $s = 1$, Ko [9, 10, 11] proved that the lattices E_6, E_7 and E_8 are the only minimal non-1-integrable lattices of rank 6, 7 and 8 respectively, and Plesken [13] gave a short proof by embedding lattices into unimodular lattices. Conway and Sloane [4] gave non-2-integrable lattices as shown in Theorem 1, and suspected that these lattices are the only minimal non-2-integrable lattices of rank 12.

Definition 1. For each positive integer n, let $\mathsf{A}_n := \{\mathbf{x} \in \mathbb{Z}^{n+1} \mid (\mathbf{x}, \mathbf{e}) = 0\}$ be a lattice, where $\mathbf{e}$ denotes the all one vector in $\mathbb{Z}^{n+1}$. Let A_{15}^+ denote the unimodular overlattice of A_{15}, that is, the lattice generated by A_{15} and the vector

$$[4] := (4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, -12, -12, -12, -12)/16 \in \mathbb{R}^{16}.$$

Theorem 1 ([4, Theorem 14])**.** *The sublattices in A_{15}^+ that are orthogonal to a sublattice in A_{15}^+ with Gram matrix*

$$\begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix} \tag{1.1}$$

are non-2-integrable lattices of rank 12 and determinant 7.

Furthermore, Conway and Sloane remarked that Theorem 1 gives precisely two minimal non-2-integrable lattices up to isometry. Our motivation comes from verifying the claim that Conway and Sloane suspected and determining the minimal non-2-integrable lattices of rank 12.

In order to find more candidates for non-2-integrable lattices and prove their minimality, in Theorem 2 we introduce a method of embedding lattices into unimodular lattices as follows, which can also be used to study the s-integrability of lattices with higher rank. For undefined notation, we refer to the next section.

Theorem 2. *Let m and n be positive integers. Let L be a lattice on the n-dimensional quadratic $\mathbb{Q}$-space V. Then L is a sublattice of a unimodular lattice of rank m if and only if one of the following holds:*

(1) $m = n$, and for each prime number p, $\det(V_p) = 1$ and $S_p(V) = 1$.

(2) $m = n + 1$, and for each prime number p, $S_p(V)(\det(V), \det(V))_p = 1$.

(3) $m = n+2$, *and for each prime number* p,

$$S_p(V) = \begin{cases} 1 & \textit{if } p > 2 \textit{ and } \det(V_p) = -1, \\ -1 & \textit{if } p = 2 \textit{ and } \det(V_2) = -1. \end{cases}$$

(4) $m \geq n+3$.

Conway and Sloane [4, Theorem 7] proved that (4) is a sufficient condition for Theorem 2. Following their argument, we prove this theorem in more detail, and give applications. For instance, we present a theorem to embed lattices into an odd unimodular lattice (see Theorem 10). In addition, we show that if a lattice of rank 12 is non-2-integrable and its determinant is at most 27, then its determinant is 7, 15, 18, 23 or 25 (see Corollary 2), and we give two more minimal non-2-integrable lattices.

Theorem 3. *There are precisely two lattices with Gram matrix*

$$\begin{pmatrix} 3 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \tag{1.2}$$

up to $\mathrm{Aut}(\mathsf{A}_{15}^+)$ *in* A_{15}^+, *and they are given by* $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$ *and* $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}' \rangle$, *where*

$$\begin{aligned}
\mathbf{a} &:= (-3,-3,-3,-3,1,1,1,1,1,1,1,1,1,1,1,1)/4 \in \mathsf{A}_{15}^+, \\
\mathbf{b} &:= (-3,-3,-3,1,-3,1,1,1,1,1,1,1,1,1,1,1)/4 \in \mathsf{A}_{15}^+, \\
\mathbf{c} &:= (-3,1,1,1,1,-3,-3,-3,1,1,1,1,1,1,1,1)/4 \in \mathsf{A}_{15}^+, \\
\mathbf{c}' &:= (1,1,1,-3,-3,-3,-3,1,1,1,1,1,1,1,1,1)/4 \in \mathsf{A}_{15}^+.
\end{aligned}$$

The non-isometric sublattices $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle^\perp$ *and* $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}' \rangle^\perp$ *are minimal non-2-integrable lattices of rank* 12 *and determinant* 15.

Although it is possible to provide a proof of the non-2-integrability in this theorem without a computer, it goes along the lines of Conway and Sloane's proof (see [4, Proof of Theorem 14]) and is long. Hence we will explain that a lattice is s-integrable if and only if a corresponding system of linear equations has a non-negative integer solution (see Lemma 12), and show the non-2-integrability with the aid of a computer. We remark that Plesken [14] provided an algorithm which enumerates sublattices of $\mathbb{Z}^n$ (for some n) all of which are isometric to a given 1-integrable lattice. Enumerating them corresponds to enumerating all the non-negative integer solutions of some system of linear equations. Since we want to show that such a system has no non-negative integer solution in order to show the non-2-integrability of some lattice L, or equivalently, the non-1-integrability of $\sqrt{2}L$, his algorithm is not effective for our purpose.

Also, we point out that every non-2-integrable lattice of rank 12 is a sublattice of A_{15}^{+} (see Lemma 9). Let L be a sublattice in A_{15}^{+} which is orthogonal to a lattice generated by 3 linearly independent elements of norm at most 4. If L is non-2-integrable, then it is isometric to one of the lattices of rank 12 in Theorem 1 and Theorem 3 (see Corollary 3 and Remark 1). It is natural to wonder if there exist more minimal non-2-integrable lattices of rank 12, and this problem is still open.

This paper is organized as follows: We introduce notation in Section 2, and well-known results for quadratic spaces in Section 3. In Section 4, for every prime number p, we introduce properties of the maximal $\mathbb{Z}_p$-lattices. In Section 5, we show a method of embedding a lattice into another by applying the results in the previous two sections. In Section 6, we give necessary and sufficient conditions for a lattice to be s-integrable. In Section 7, we study the lattice A_{15}^{+}, and prove the first statement of Theorem 3. In Section 8, we discuss the minimality of non-2-integrable lattices and complete the proof of Theorem 3.

2. Notation

We will follow the book [7] and give the basic notation as follows. Throughout this paper, let R denote a principal ideal domain with quotient field $F \supsetneq R$. Let R^* denote the set of units of R, and F^* denote the set of the non-zero elements of F.

Let (V, B, q) be a *quadratic F-space*, where B is a symmetric bilinear form on V, and q is the quadratic form associated with B. For simplicity we usually just write V. We write $V \simeq W$ if two quadratic F-spaces V and W are isometric. The quadratic spaces mentioned in this paper are always *regular*, that is, they have no non-zero vector $\mathbf{v}$ such that $B(\mathbf{v}, \mathbf{u}) = 0$ holds for all its vectors $\mathbf{u}$. Let $\det(V)$ denote the *determinant* of V, which is the coset in $F^*/(F^*)^2$ represented by the determinant of the Gram matrix with respect to a basis of V.

An R-module $L \subseteq V$ is called an *R-lattice* in V if $L = 0$ or if there exist linearly independent elements $\mathbf{v}_1, \ldots, \mathbf{v}_r$ of V such that $L = R\mathbf{v}_1 \oplus \cdots \oplus R\mathbf{v}_r$. We call $\mathbf{v}_1, \ldots, \mathbf{v}_r$ a basis of L and r the *rank* of L (and $\operatorname{rank} 0 = 0$). We say L is *on* V if $\dim(V) = r$. We write $L \simeq M$ or $L \simeq_R M$ if two R-lattices L and M are isometric. Let $\det(L)$ denote the *determinant* of an R-lattice L, which is the coset in $F^*/(R^*)^2$ represented by the Gram matrix with respect to a basis of L. For $a \in F$, let aL denote the R-lattice $\{a\mathbf{u} \mid \mathbf{u} \in L\}$.

Let L' be a sublattice of L. The *orthogonal complement* of L' in L is the R-module $\{\mathbf{u} \in L \mid B(\mathbf{u}, \mathbf{v}) = 0 \text{ for all } \mathbf{v} \in L'\}$, which is also a sublattice of L and is denoted by $(L')^{\perp}$.

For every positive integer n, a matrix in $\mathrm{M}_n(R)$ is said to be *unimodular* if its determinant is in R^*. The set of unimodular matrices in $\mathrm{M}_n(R)$ is denoted by $GL_n(R)$. For two matrices M_1 and M_2 in $\mathrm{M}_n(R)$, we say that they are *R-congruent*, denoted by $M_1 \sim_R M_2$, if there exists a unimodular matrix $P \in GL_n(R)$ such that $P^\top M_1 P = M_2$. Given a symmetric matrix M and an R-lattice L (respectively quadratic F-space V), we write $L \cong M$ (respectively $V \cong M$) if the Gram matrix of L (respectively V) with respect to some basis is M. Furthermore, an R-lattice L of rank n is said to be *unimodular* if $L \cong M$ for some symmetric matrix $M \in GL_n(R)$.

In the whole paper, let S be the set of prime numbers. For each $p \in S$, let $\mathbb{Z}_p$ denote the ring of p-adic integers, $\mathbb{Q}_p$ the field of p-adic numbers, $\nu_p(a)$ the p-adic order of each $a \in \mathbb{Q}_p$, and $|\cdot|_p$ the p-adic valuation. The set $\mathbb{R}$ of real numbers is denoted by $\mathbb{Q}_\infty$. Furthermore, the *Hilbert symbol* $(\cdot,\cdot)_p$ over $\mathbb{Q}_p$ for $p \in S \cup \{\infty\}$ is defined as

$$(a,b)_p := \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a non-trivial solution } (x,y,z) \text{ in } \mathbb{Q}_p^3, \\ -1 & \text{otherwise} \end{cases}$$

for $a, b \in \mathbb{Q}_p^*$. For each odd prime number p, let δ_p denote one of non-square elements of $\mathbb{Z}_p^*$. Note that $\{1, \delta_p\}$ is a complete system of representatives of $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$ (see [7, Theorem 3.48]).

Let L be a $\mathbb{Z}$-lattice on the n-dimensional $\mathbb{Q}$-quadratic space V; say $L := \bigoplus_{i=1}^n \mathbb{Z}\mathbf{v}_i$. For each $p \in S \cup \{\infty\}$, we define the *localization* V_p of V at p to be the quadratic $\mathbb{Q}_p$-space $V \otimes \mathbb{Q}_p$. Moreover, we define the *localization* L_p of L at p to be the $\mathbb{Z}_p$-lattice on V_p generated by L, that is,

$$L_p = \bigoplus_{i=1}^n \mathbb{Z}_p \mathbf{v}_i.$$

In addition, for an orthogonal basis $(\mathbf{u}_1, \ldots, \mathbf{u}_n)$ of $V = (V, B, q)$, the *Hasse symbol* of V and that of L at p are defined to be

$$S_p(V) = S_p(L) := \prod_{1 \le i < j \le n} (q(\mathbf{u}_i), q(\mathbf{u}_j))_p \in \{-1, 1\}.$$

The *signature* of L (respectively V), denoted by $\operatorname{sign}(L)$ (respectively $\operatorname{sign}(V)$), is defined by $r-s$, where r and s are non-negative integers such that $L \otimes \mathbb{R} \cong I_r \oplus (-I_s)$ (respectively $V \otimes \mathbb{R} \cong I_r \oplus (-I_s)$). In addition, L (respectively V) is said to be *positive definite* if $\operatorname{sign}(L) = n$ (respectively $\operatorname{sign}(V) = n$).

Let L be an R-lattice on quadratic F-space. Then the R-module $sL := \{B(\mathbf{v}, \mathbf{u}) \mid \mathbf{v}, \mathbf{u} \in L\}$ is called the *scalar ideal* of L, and the R-modular nL generated by $\{q(\mathbf{v}) \mid \mathbf{v} \in L\}$ is called the *norm ideal* of L. Note that $2(sL) \subseteq nL \subseteq sL$ and $nL = sL$ if $2 \in R^*$.

A $\mathbb{Z}$-lattice L is said to be *integral* if $sL \subseteq \mathbb{Z}$. Moreover, an integral $\mathbb{Z}$-lattice L is said to be *even* if $nL \subseteq 2\mathbb{Z}$, and otherwise it is *odd*. Note that every positive definite integral $\mathbb{Z}$-lattice is isometric to a positive definite integral $\mathbb{Z}$-lattice in $\mathbb{R}^n$ equipped with the canonical bilinear form for some positive integer n. For simplicity, we call a positive definite integral $\mathbb{Z}$-lattice equipped with the canonical bilinear form *lattice*.

3. Quadratic Spaces

In this section we introduce fundamental results for quadratic $\mathbb{Q}$-spaces and quadratic $\mathbb{Q}_p$-spaces.

Theorem 4 ([7, Theorem 4.29]). *Let p be a prime number. Two quadratic $\mathbb{Q}_p$-spaces V and W are isometric if and only if*

$$\dim(V) = \dim(W),\ \ \det(V) = \det(W) \textit{ and } S_p(V) = S_p(W).$$

Theorem 5 ([7, Theorem 4.32]). *Let p be a prime number. Then there exists a quadratic $\mathbb{Q}_p$-space V with dimension n, determinant $d = \det(V)$ and Hasse symbol $s = S_p(V)$ if and only if*

$$(d, s) \neq (1, -1) \textit{ or } (n, d, s) \neq (2, -1, -1). \tag{3.1}$$

For every $a, b \in \mathbb{Q}^*$, $(a, b)_p = 1$ for almost all p, that is, there is a finite set S' such that $(a, b)_p = 1$ for every $p \in S \setminus S'$. Moreover,

$$\prod_{p \in S \cup \{\infty\}} (a, b)_p = 1 \tag{3.2}$$

holds (see [7, Theorem 5.2]). This immediately implies the following lemma.

Lemma 1 ([7, Corollary 5.3]). *We have $\prod_{p \in S \cup \{\infty\}} S_p(V_p) = 1$ for every non-zero quadratic $\mathbb{Q}$-space V.*

Theorem 6 ([7, Corollary 5.9]). *Let V and W be two quadratic $\mathbb{Q}$-spaces. Then $V \simeq W$ if and only if $V_\infty \simeq W_\infty$ and $V_p \simeq W_p$ for each prime number p.*

Theorem 7 ([2, Chapter 6, Theorem 1.3]). *Let $n \geq 2$ and $d \in \mathbb{Q}^*$. For each $p \in S \cup \{\infty\}$, let $V_{(p)}$ be an n-dimensional quadratic $\mathbb{Q}_p$-space and suppose that*

(1) $\det(V_{(p)}) \in d\mathbb{Q}_p^{*2}$,

(2) $\prod_{p \in S \cup \{\infty\}} S_p(V_{(p)}) = 1$, *and* $S_p(V_{(p)}) = 1$ *for almost all p.*

Then there exists a quadratic $\mathbb{Q}$-space V with $\det(V) = d$, $\operatorname{sign}(V) = \operatorname{sign}(V_{(\infty)})$ *and $V_p \simeq V_{(p)}$ for each $p \in S$.*

4. Maximality and Existence of $\mathbb{Z}_p$-Lattices

Let A be a fractional R-ideal, that is, $A \subseteq F$ is an R-module, and $aA \subseteq R$ for some $a \in R$. An R-lattice L on a quadratic F-space V is $A^{(n)}$*-maximal* (respectively $A^{(s)}$-*maximal*) if $nL \subseteq A$ (respectively $sL \subseteq A$) and for any R-lattice M on V containing

L, $nM \subseteq A$ (respectively $sM \subseteq A$) implies $M = L$. Note that for every odd prime number p, a $\mathbb{Z}_p$-lattice is $A^{(n)}$-maximal if and only if it is $A^{(s)}$-maximal. The following lemma shows that $\mathbb{Z}^{(s)}$-maximal $\mathbb{Z}$-lattices and $\mathbb{Z}_p^{(s)}$-maximal $\mathbb{Z}_p$-lattices are closely related.

Lemma 2 ([7, Lemma 9.8])**.** *Let L be a $\mathbb{Z}$-lattice on a quadratic $\mathbb{Q}$-space V, and let A be a fractional $\mathbb{Z}$-ideal. Then L is $A^{(s)}$-maximal (respectively $A^{(n)}$-maximal) if and only if L_p is $A_p^{(s)}$-maximal (respectively $A_p^{(n)}$-maximal) for each prime number p.*

4.1. The Isometry Classes of $\mathbb{Z}_p^{(s)}$-Maximal $\mathbb{Z}_p$-Lattices for an Odd Prime Number p

The following theorem immediately gives the $\mathbb{Z}_p^{(s)}$-maximal $\mathbb{Z}_p$-lattices up to isometry.

Theorem 8 ([7, Theorem 8.8])**.** *Let F be a field with a complete discrete valuation $|\cdot|$, and let R be the associated valuation ring. Suppose V is a (regular) quadratic F-space and A is a fractional R-ideal. Then there is only one isometry class of $A^{(n)}$-maximal R-lattices on V.*

We set $F := \mathbb{Q}_p$, $R := \mathbb{Z}_p$ and $|\cdot| := |\cdot|_p$ for each odd prime number p, and then apply this theorem to $\mathbb{Z}_p$-lattices. Since the existence of quadratic $\mathbb{Q}_p$-spaces is asserted in Theorem 5, we derive the following proposition.

Proposition 1 ([4, Theorem 4 for odd prime numbers])**.** *Given an odd prime number p, there exists a unique $\mathbb{Z}_p^{(s)}$-maximal $\mathbb{Z}_p$-lattice on a quadratic $\mathbb{Q}_p$-space V if and only if condition* (3.1) *is satisfied.*

Example 1. Let p be an odd prime number and n a positive integer. As asserted in Proposition 1, we may find a $\mathbb{Z}_p^{(s)}$-maximal $\mathbb{Z}_p$-lattice on a quadratic $\mathbb{Q}_p$-space V if condition (3.1) is satisfied. Actually, a complete system of representatives of isometry classes of $\mathbb{Z}_p^{(s)}$-maximal $\mathbb{Z}_p$-lattices are enumerated by $\mathbb{Z}_p$-lattices $H^p_{n,d,\varepsilon}$ of rank n, determinant d and Hasse symbol ε defined as follows:

$$
\begin{aligned}
&H^p_{n,1,1} \cong I_n, && H^p_{n,\delta_p,1} \cong I_{n-1} \oplus (\delta_p),\\
&H^p_{n,p,1} \cong I_{n-1} \oplus (p), && H^p_{n,p\delta_p,1} \cong I_{n-1} \oplus (p\delta_p),\\
&H^p_{n,p\delta_p,-1} \cong I_{n-2} \oplus (\delta_p) \oplus (p)\ (n \geq 2), && H^p_{n,p,-1} \cong I_{n-2} \oplus (\delta_p) \oplus (p\delta_p)\ (n \geq 2),
\end{aligned}
$$

$$
H^p_{n,-\delta_p,-1} \cong \begin{cases} I_{n-2} \oplus (p) \oplus (p\delta_p) & \text{if } p \equiv 1 \pmod 4, \\ I_{n-2} \oplus (p) \oplus (p) & \text{if } p \equiv 3 \pmod 4, \end{cases} \quad (n \geq 2),
$$

$$
H^p_{n,-1,-1} \cong \begin{cases} I_{n-3} \oplus (\delta_p) \oplus (p) \oplus (p\delta_p) & \text{if } p \equiv 1 \pmod 4, \\ I_{n-3} \oplus (\delta_p) \oplus (p) \oplus (p) & \text{if } p \equiv 3 \pmod 4, \end{cases} \quad (n \geq 3).
$$

4.2. Maximality and Existence of $\mathbb{Z}_2$-Lattices

In this subsection we introduce fundamental results for $\mathbb{Z}_2$-lattices. First, adopting a similar method as in the proof of [3, Proposition 2], we obtain the following result.

Proposition 2 (cf. [3, Proposition 2])**.** *If a $\mathbb{Z}_2$-lattice L is $\mathbb{Z}_2^{(s)}$-maximal, then $\nu_2(\det(L)) = 0$ or 1.*

Proposition 3. *There exists a $\mathbb{Z}_2$-lattice whose norm ideal is $\mathbb{Z}_2$ on a quadratic $\mathbb{Q}_p$-space V if and only if condition (3.1) is satisfied and $(\dim(V), \det(V), S_2(V)) \neq (2, 3, -1)$.*

Proof. We show the necessity by enumerating $\mathbb{Z}_2$-lattices $H_{n,d,\varepsilon}$ of rank n, determinant d and Hasse symbol ε as follows:

$$
\begin{aligned}
&H_{n,1,1} \cong I_n, && H_{n,-1,1} \cong I_{n-1} \oplus (-1),\\
&H_{n,3,1} \cong I_{n-1} \oplus (3), && H_{n,-3,1} \cong I_{n-1} \oplus (-3),\\
&H_{n,1,-1} \cong I_{n-2} \oplus (-I_2)\ (n \geq 2), && H_{n,-1,-1} \cong I_{n-3} \oplus (-I_3)\ (n \geq 3),\\
&H_{n,3,-1} \cong I_{n-3} \oplus (3I_3)\ (n \geq 3), && H_{n,-3,-1} \cong I_{n-2} \oplus (-1) \oplus (3)\ (n \geq 2),\\
&H_{n,2,1} \cong I_{n-1} \oplus (2), && H_{n,-2,1} \cong I_{n-1} \oplus (-2),\\
&H_{n,6,1} \cong I_{n-1} \oplus (6), && H_{n,-6,1} \cong I_{n-1} \oplus (-6),\\
&H_{n,2,-1} \cong I_{n-2} \oplus (-3) \oplus (-6)\ (n \geq 2), && H_{n,-2,-1} \cong I_{n-2} \oplus (-3) \oplus (6)\ (n \geq 2),\\
&H_{n,6,-1} \cong I_{n-2} \oplus (-3) \oplus (-2)\ (n \geq 2), && H_{n,-6,-1} \cong I_{n-2} \oplus (-3) \oplus (2)\ (n \geq 2).
\end{aligned}
$$

(In fact, they give a complete system of representatives of isometry classes of $\mathbb{Z}_2^{(s)}$-maximal $\mathbb{Z}_2$-lattices with $nL = \mathbb{Z}_2$.)

Next we show the sufficiency. Theorem 5 asserts that every quadratic $\mathbb{Q}_2$-space satisfies condition (3.1). Thus it suffices to show that there is no $\mathbb{Z}_2$-lattice L with $nL = \mathbb{Z}_2$ and $(\dim(V), \det(V), S_2(V)) = (2, 3, -1)$, where $V = \mathbb{Q}_2 \otimes L$. By way of contradiction, we suppose that there is such a $\mathbb{Z}_2$-lattice L. Since $nL = \mathbb{Z}_2$, we have $L \cong (x) \oplus (y)$ for some $x \in \mathbb{Z}_2^*$ and $y \in \mathbb{Z}_2$. Then

$$-1 = S_2(V) = (x, y)_2 = (x, -xy)_2 = (x, -\det(V))_2 = (x, -3)_2 = 1.$$

This is a contradiction, and the desired result follows. $\square$

Note that a $\mathbb{Z}_2$-lattice L with the Gram matrix $(2) \oplus (6)$ satisfies that $\det(L) = 3$ and $S_2(L) = -1$.

5. Embedding Theory

One useful way to investigate lattices is embedding a lattice into another well-known lattice. In this section, we aim to prove Theorem 2 and Theorem 10 which give conditions for a given lattice to be embedded into a unimodular lattice and an odd unimodular lattice, respectively.

5.1. Hasse Symbols of Unimodular Lattices and Unimodular $\mathbb{Z}_p$-Lattices

In this subsection we introduce the Hasse symbols of unimodular lattices and unimodular $\mathbb{Z}_p$-lattices.

Lemma 3. *Let p be an odd prime number. Suppose that L is a unimodular $\mathbb{Z}_p$-lattice on the n-dimensional quadratic $\mathbb{Q}_p$-space V. Then $S_p(V) = 1$. In particular, if $\det(L) = 1$, then $L \cong I_n$.*

Proof. Let G be the Gram matrix of L with respect to some basis. Since p is an odd prime, G is $\mathbb{Z}_p$-congruent to a diagonal matrix D in $\mathrm{M}_n(\mathbb{Z}_p)$ (see [5, p. 369]). Then the diagonal entries of D are units in $\mathbb{Z}_p$ as $\det(G) \in \mathbb{Z}_p^*$. Note that $(a, b)_p = 1$ for any $a, b \in \mathbb{Z}_p^*$. This implies $\prod_{i<j}(D_{ii}, D_{jj})_p = 1$, and thus $S_p(L) = 1$. This is the desired result.

Next, we suppose that $\det(L) = 1$. By the previous argument, we have $S_p(L) = 1$. Since L is a $\mathbb{Z}_p^{(s)}$-maximal $\mathbb{Z}_p$-lattice, Proposition 1 forces $L \simeq H^p_{n,1,1} \cong I_n$. □

We remark that this lemma can also be proved by a classification of $\mathbb{Z}_p^{(s)}$-maximal $\mathbb{Z}_p$-lattices for each odd prime number p in Example 1.

Lemma 4. *Suppose that there exists a unimodular lattice on the n-dimensional quadratic $\mathbb{Q}$-space V. Then $\det(V_p) = 1,\ S_p(V_p) = 1$ for every prime number p.*

Proof. Let L be a unimodular lattice on V. Since $\det(L) = 1$, we find that L_p is a unimodular $\mathbb{Z}_p$-lattice on V_p with $\det(L_p) = 1$. This implies that $\det(V_p) = 1$ for each $p \in S$. From Lemma 3, we find that $S_p(V_p) = 1$ if p is odd. Note that $S_\infty(V \otimes \mathbb{Q}_\infty) = 1$ as L is positive definite. Theorem 1 shows that $S_2(V_2) = 1$. □

5.2. Embedding a Quadratic Space

In order to embed $\mathbb{Z}$-lattices, it is essential to embed quadratic $\mathbb{Q}$-spaces. In this subsection we aim to prove Proposition 4, which will be used in the next subsection.

Lemma 5. *Let p be a prime number, and m and n positive integers with $m > n$. Suppose that V is an n-dimensional quadratic $\mathbb{Q}_p$-space. Then there exists a quadratic $\mathbb{Q}_p$-space U which satisfies $V \perp U \cong I_m$, if and only if there exists a quadratic $\mathbb{Q}_p$-space U with*

$$(\dim(U), \det(U), S_p(U)) = (m - n, \det(V), S_p(V)(\det(V), \det(V))_p).$$

Proof. Let U be a quadratic $\mathbb{Q}_p$-space U. Then $V \perp U \cong I_m$ if and only if $\dim(V)+\dim(U) = m$, $\det(V)\det(U) = 1$ and $S_p(V)S_p(U)(\det(V), \det(U))_p = 1$ by Theorem 4. Since $(\det(V), \det(V))_p(\det(V), \det(U))_p = (\det(V), \det(V)\det(U))_p = (\det(V), 1)_p = 1$ holds, the desired result follows. □

Lemma 6. *Let p be a prime number, and m and n positive integers with $m \geq n$. Suppose that V is an n-dimensional quadratic $\mathbb{Q}_p$-space. Then there exists an $(m-n)$-dimensional quadratic $\mathbb{Q}_p$-space U such that $V \perp U \cong I_m$ if and only if one of the following is satisfied:*

(1) $m = n$, $\det(V) = 1$ *and* $S_p(V) = 1$.

(2) $m = n+1$, *and* $S_p(V)(\det(V), \det(V))_p = 1$.

(3) $m = n+2$, *and* $S_p(V) = \begin{cases} 1 & \text{if } p > 2 \text{ and } \det(V) = -1, \\ -1 & \text{if } p = 2 \text{ and } \det(V) = -1. \end{cases}$

(4) $m \geq n+3$.

Proof. This follows from Theorem 5 and Lemma 5 immediately. □

Lemma 7. *Let m and n be positive integers with $m \geq n$. Suppose that V is an n-dimensional quadratic $\mathbb{Q}$-space with $\operatorname{sign}(V) = n$. Then there exists an $(m-n)$-dimensional quadratic $\mathbb{Q}$-space U such that*

$$V \perp U \cong I_m \tag{5.1}$$

if and only if for each prime number p, there exists a quadratic $\mathbb{Q}_p$-space $U_{(p)}$ such that

$$V_p \perp U_{(p)} \cong I_m. \tag{5.2}$$

Proof. If $m = n$, then Theorem 6 implies the desired result. Hence we assume that $m > n$. Only the sufficiency needs to be proved. Suppose that there exists a quadratic $\mathbb{Q}_p$-space $U_{(p)}$ such that (5.2) holds for each prime number p. Then by Lemma 5, we find that $\det(U_{(p)}) = \det(V_p) \in \det(V)\mathbb{Q}_p^{*2}$ and

$$S_p(U_{(p)}) = S_p(V)(\det(V), \det(V))_p.$$

Define $U_{(\infty)} \cong I_{m-n}$. Then $\det(U_{(\infty)}) = 1 \in \det(V)\mathbb{Q}_\infty^{*2}$ as V is positive definite. Now condition (1) of Theorem 7 is satisfied. By Lemma 1 and (3.2), condition (2) of Theorem 7 is also satisfied and thus there exists a quadratic $\mathbb{Q}$-space U with $\operatorname{sign}(U) = m - n$ whose localization U_p is isometric to $U_{(p)}$ for each prime number p. This implies that

$$(V \perp U)_p = V_p \perp U_p \simeq V_p \perp U_{(p)} \cong I_m \text{ for each prime number } p.$$

Using Theorem 6, we obtain $V \perp U \cong I_m$. □

Combining Lemma 6 and Lemma 7, we have the following proposition.

Proposition 4. *Let m be a positive integer greater than n. Suppose that V is an n-dimensional quadratic $\mathbb{Q}$-space with $\mathrm{sign}(V) = n$. Then there exists an $(m-n)$-dimensional quadratic $\mathbb{Q}$-space U such that $V \perp U \cong I_m$ if and only if one of the conditions* (1)–(4) *in Theorem 2 is satisfied.*

5.3. Embedding a Positive Definite Integral $\mathbb{Z}$-Lattice

In this subsection we combine results in the previous subsections with Sections 3 and 4, and prove Theorem 2 and Theorem 10. In addition, Corollary 1 shows that a lattice can be embedded into a unimodular lattice if its determinant satisfies certain conditions.

Lemma 8. *Let $n \geq 2$ be an integer. Suppose that V is an n-dimensional positive definite quadratic $\mathbb{Q}$-space. Then the following are equivalent.*

(1) There exists a unimodular lattice on V.

(2) For each prime number p, the localization V_p of V satisfies $\det(V_p) = 1$ and $S_p(V_p) = 1$.

(3) Every $\mathbb{Z}^{(s)}$-maximal $\mathbb{Z}$-lattice on V is unimodular.

(4) $V \cong I_n$.

Proof. First we see that (1) implies (2) by Lemma 4. Next, (3) clearly implies (1). Also, (2) and (4) are equivalent by Theorem 6. We prove that (2) implies (3). Let L be a $\mathbb{Z}^{(s)}$-maximal $\mathbb{Z}$-lattice on V. If p is an odd prime number, then we have $V_p \cong I_n$ by Theorem 4. This together with Proposition 1 implies $L_p \cong I_n$. Next we consider the case of $p = 2$. By Proposition 2, $\nu_2(\det(L_2)) \in \{0, 1\}$ follows. This together with $\det(V_2) = 1$ implies that $\nu_2(\det(L_2)) = 0$. Therefore $\det(L_p) \in \mathbb{Z}_p^*$ for every prime number p, and $\det(L) \in \bigcap_{p \in S}(\det(L_p) \cap \mathbb{Z}) = \{1, -1\}$. This shows that L is unimodular. □

Theorem 2 follows from Proposition 4 and Lemma 8. As a corollary of Theorem 2, we immediately derive the following corollary.

Corollary 1. *Suppose that L is a lattice of rank n and $\det(L) = p_1^{\alpha_1} \cdots p_t^{\alpha_t} d$, where $p_1 < p_2 < \cdots < p_t$ are odd prime numbers, $\alpha_1, \ldots, \alpha_t$ are positive even numbers, and d is an integer with $\gcd(d, p_1 \cdots p_t) = 1$. Then L is a sublattice of a unimodular lattice of rank $n+2$, if the following conditions are satisfied:*

(1) For each odd prime number $p \in S - \{p_1, \ldots, p_t\} \cup \{2\}$, $\nu_p(d)$ is odd if $\nu_p(d) > 0$.

(2) For each odd prime number $p \in \{p_1, \ldots, p_t\}$, the Legendre symbol $\left(\frac{-d}{p}\right)$ equals -1.

(3) $d/2^{\nu_2(d)} \not\equiv -1 \pmod 8$ *if* $\nu_2(d)$ *is even.*

Proof. Let $V = L \otimes \mathbb{Q}$ be the n-dimensional quadratic $\mathbb{Q}$-space. Let $S' = \{p \in S \mid \nu_p(d) \text{ is odd}\}$. If $p \in S - S' \cup \{2, p_1, \ldots, p_t\}$, then L_p is unimodular, and hence $S_p(V) = 1$ by Lemma 3. Next we easily show that for each $p \in S' \cup \{2, p_1, \ldots, p_t\}$, $\det(V_p) \neq 1$. Following from condition (2) of Theorem 2, we have the result immediately. $\square$

Theorem 9 ([7, Theorem 9.4])**.** *Let L be a $\mathbb{Z}$-lattice on the n-dimensional quadratic $\mathbb{Q}$-space V. Suppose T is a finite subset of S, and suppose that for each $p \in T$, a $\mathbb{Z}_p$-lattice $M_{(p)}$ is given on V_p. Then there is a $\mathbb{Z}$-lattice L' on V such that*

$$L'_p = \begin{cases} M_{(p)} & \text{if } p \in T, \\ L_p & \text{if } p \in S - T. \end{cases}$$

Theorem 10. *Let m be a positive integer. Suppose that L is a lattice on the n-dimensional quadratic $\mathbb{Q}$-space V and one of the conditions (1)–(4) in Theorem 2 is satisfied. Then L is a sublattice of an odd unimodular lattice of rank m if one of the following holds:*

(1) *L is odd,*

(2) $m = n + 2$ and $(\det(V_2), S_2(V_2)) \neq (3, 1)$,

(3) $m \geq n + 3$.

Proof. While L is odd, the desired result holds immediately by Theorem 2. So now we may assume $m = n + 2$, the condition (3) in Theorem 2 is satisfied, and $(\det(V_2), S_2(V_2)) \neq (3, 1)$. By Proposition 4, we find that there exists a 2-dimensional quadratic $\mathbb{Q}$-space U such that

$$V \perp U \cong I_{n+2}.$$

Let N be an integral $\mathbb{Z}$-lattice on U. Since $(\det(U_2), S_2(U_2)) \neq (-1, -1)$ by Theorem 5 and

$$(\det(U_2), S_2(U_2)) = (\det(V_2), S_2(V_2)(\det(V_2), \det(V_2))_2) \neq (3, -1),$$

Proposition 3 implies that there exists a $\mathbb{Z}_2$-lattice H with $nH = \mathbb{Z}_2$ on U_2 so that $U_2 \simeq \mathbb{Q}_2 \otimes H$. Using Theorem 9, we find that there exists a $\mathbb{Z}$-lattice N' such that

$$N'_p = \begin{cases} H & \text{if } p = 2, \\ N_p & \text{if } p > 2. \end{cases}$$

Since $(sN')_p = sN'_p \subseteq \mathbb{Z}_p$ for every prime number p, we have that $sN' \subseteq \bigcap_{p \in S}(\mathbb{Z}_p \cap \mathbb{Q}) = \mathbb{Z}$, and hence N' is integral. Moreover, N' is odd as $nN'_2 = nH = \mathbb{Z}_2$. Let

$$M = L \perp N'.$$

Note that the integral $\mathbb{Z}$-lattice M is odd and the quadratic $\mathbb{Q}$-space $M \otimes \mathbb{Q}$ is isometric to I_{n+2}. A $\mathbb{Z}^{(s)}$-maximal $\mathbb{Z}$-lattice on $M \otimes \mathbb{Q}$ which contains M is a desired odd unimodular $\mathbb{Z}$-lattice by Lemma 8.

If $m \geq n+3$, then the desired result holds in a similar way. □

5.4. Applications

In this subsection, we prove Corollary 2 which gives a sufficient condition for a lattice of rank 12 to be 2-integrable and Corollary 3 which explains how to find candidates for non-2-integrable lattices of rank 12.

The unimodular lattices of rank up to 25 are completely classified (see [5, Chapter 16–18]). Conway and Sloane [4] studied the s-integrability of unimodular lattices among them. The following theorems are a part of their results.

Theorem 11 ([4, Proof of Theorem 12]). *Every unimodular lattice of rank up to* 14 *is* 2*-integrable.*

Theorem 12 ([4, Theorem 13]). *The lattice* A_{15}^{+} *is a non-*2*-integrable unimodular lattice of rank* 15.

Note that a lattice is said to be *irreducible* if it is not the orthogonal sum of two non-zero lattices. As A_{15}^{+} is the unique irreducible unimodular lattice of rank 15 (see [5, p. 49]), following from Theorems 11, 12 and 2, we have the following lemma.

Lemma 9. *The lattice* A_{15}^{+} *is the unique unimodular lattice of rank* 15 *which is not* 2*-integrable. In particular, every non-*2*-integrable lattice of rank* 12 *is a sublattice in* A_{15}^{+}.

We derive the following corollary from Corollary 1:

Corollary 2. *Suppose that* L *is a non-*2*-integrable lattice of rank* 12 *and determinant at most* 27*. Then the determinant of* L *is equal to one of* $7, 15, 18, 23$ *or* 25.

Proof. Let L be a lattice of rank 12. Suppose that $\det(L)$ is not equal to $7, 15, 18, 23$ or 25. Then Corollary 1 implies that L is contained in a unimodular lattice of rank 14. This together with Theorem 11 implies that L is 2-integrable. □

We will use Corollary 2 to obtain Corollary 3, which gives candidates for non-2-integrable lattices. To prepare for the proof of it, we introduce some terminology and a lemma. For a lattice L, its *dual* is the lattice $\{\mathbf{u} \in L \otimes \mathbb{Q} \mid (\mathbf{u}, \mathbf{v}) \in \mathbb{Z} \text{ for all } \mathbf{v} \in L\}$, and we denote it by L^*. Let L be a lattice, and M a sublattice of it. The lattice M is said to be *primitive* if $M = M^* \cap L$.

Lemma 10 ([6, Proposition 1.2]). *Let* L *be a unimodular lattice and* M *be its primitive sublattice. Then, the determinant of* M *is equal to that of the sublattice* $M^{\perp}$ *orthogonal to* M *in* L.

Corollary 3. *Let M be a sublattice in A_{15}^+ which is generated by 3 linearly independent elements of norm 3, and L be the sublattice orthogonal to M in A_{15}^+. If L is non-2-integrable, then it is isometric to one of the lattices of rank 12 in Theorem 1 and Theorem 3.*

Proof. We enumerate the positive definite matrices of order 3 all of whose diagonal entries are 3 and off-diagonal entries are in $\{-2,-1,0,1,2\}$. Let $\mathcal{G}$ be the set of these matrices. It is verified that G is $\mathbb{Z}$-congruent to either the matrix (1.1) or (1.2) for each $G \in \mathcal{G}$ with $\det(G) \in \{7, 15\}$. Hence it suffices to show that, if $\det(M) \neq 7, 15$, then L is 2-integrable.

Suppose that $\det(M) \neq 7, 15$. Note that the Gram matrix with respect to some basis of M is contained in $\mathcal{G}$. By calculating the determinants of all matrices in $\mathcal{G}$, we have

$$\det(M) \in \{3, 5, 8, 12, 13, 16, 20, 21, 24, 27\}.$$

Set $P := (M \otimes \mathbb{Q}) \cap \mathsf{A}_{15}^+$. Then P is primitive in A_{15}^+ since $P^* \cap \mathsf{A}_{15}^+ \subset (P \otimes \mathbb{Q}) \cap \mathsf{A}_{15}^+ = (M \otimes \mathbb{Q}) \cap \mathsf{A}_{15}^+ = P$. Lemma 10 implies $\det(L) = \det(P)$ since $L = M^\perp = P^\perp$ in A_{15}^+. In addition, we have $\det(M) = \det(P)[P : M]^2$. Hence we see that

$$\det(L) = \det(P) \in \{1, 2, 3, 4, 5, 6, 8, 12, 13, 16, 20, 21, 24, 27\}.$$

This together with Corollary 2 implies that L is 2-integrable. $\square$

Remark 1. It is a natural question to ask if we can obtain more candidates for non-2-integrable lattices of rank 12 in A_{15}^+. By using a computer, we derive a better result than Corollary 3 as follows. As will be discussed in Lemma 13, it is possible to enumerate the lattices in A_{15}^+ each of which is orthogonal to a lattice of rank 3 generated by 3 linearly independent elements of norm at most 4. Since we can judge whether a given lattice is 2-integrable by solving (with a computer) a corresponding system of linear equations, it turns out that there is no non-2-integrable lattice among them except the non-2-integrable lattices obtained in Theorem 1 and Theorem 3. Now we may not immediately verify this result without a computer.

6. The s-Integrability and Eutactic Stars of Scale s

Since it is difficult to determine whether a lattice is s-integrable from its definition, Conway and Sloane [4] gave equivalent conditions for a given lattice to be s-integrable in terms of eutactic stars. Here we introduce them. Hereafter, we let $\mathbf{e}_i$ denote the vector of which the i-th entry is 1 and the others are 0.

Definition 2. Let s be a positive integer. For positive integers $m \geq n$, let ρ be the orthogonal projection from $\mathbb{R}^m$ to an n-dimensional subspace. Then vectors $\rho(\sqrt{s} \cdot$

$\mathbf{e}_1), \ldots, \rho(\sqrt{s} \cdot \mathbf{e}_m)$ (with repetitions allowed) are said to form an *(n-dimensional) eutactic star (of scale s).*

Most proofs of non-s-integrability of a given lattice are reduced to arguments using the following theorem and lemma.

Theorem 13 ([4, Theorem 3])**.** *Let s be a positive integer. A lattice L of rank n is s-integrable if and only if its dual L^* contains an n-dimensional eutactic star of scale s.*

Lemma 11 ([4, pp. 215–216])**.** *A necessary and sufficient condition for $\mathbf{s}_1, \ldots, \mathbf{s}_m \in \mathbb{R}^n$ to be an n-dimensional eutactic star of scale s is that, for each $\mathbf{w} \in \mathbb{R}^n$,*

$$\sum_{i=1}^{m} (\mathbf{w}, \mathbf{s}_i)^2 = s(\mathbf{w}, \mathbf{w}). \tag{6.1}$$

According to the following lemma, determining whether a lattice is s-integrable is equivalent to judging the existence of a non-negative integer solution of a system of linear equations. Hence, it can be determined by computer if the number of variables is few.

Lemma 12. *Let s be a positive integer, L a lattice with a basis $\mathbf{w}_1, \ldots, \mathbf{w}_n$, and $\mathbf{u}_1, \ldots, \mathbf{u}_N$ the pairwise distinct vectors in L^* of norm at most s. Then L is s-integrable if and only if the following system of equations has a non-negative integer solution $(x_1, \ldots, x_N)$:*

$$\sum_{k=1}^{N} (\mathbf{w}_i + \mathbf{w}_j, \mathbf{u}_k)^2 x_k = s(\mathbf{w}_i + \mathbf{w}_j, \mathbf{w}_i + \mathbf{w}_j) \quad (i, j = 1, \ldots, n). \tag{6.2}$$

Proof. Theorem 13 asserts that L is s-integrable if and only if L^* contains an n-dimensional eutactic star of scale s. Thus it is sufficient to show that the two conditions, namely, that the dual lattice L^* contains an n-dimensional eutactic star of scale s and that Equation (6.2) has a non-negative integer solution, are equivalent.

Suppose that $\mathbf{s}_1, \ldots, \mathbf{s}_m$ in L^* is a eutactic star of scale s. As $(\mathbf{s}_i, \mathbf{s}_i) \leq s$ for each i, we have $\mathbf{s}_1, \ldots, \mathbf{s}_m \in \{\mathbf{u}_1, \ldots, \mathbf{u}_N\}$. Now applying Lemma 11, we find that a solution $(x_1, \ldots, x_N)$ of Equation (6.2) can be given by setting $x_j = |\{i \mid \mathbf{s}_i = \mathbf{u}_j\}|$ for $j = 1, \ldots, N$.

Now suppose $(x_1, \ldots, x_N)$ is a non-negative integer solution for Equation (6.2). Then the multiple set $\{\mathbf{u}_1^{(x_1)}, \ldots, \mathbf{u}_N^{(x_N)}\}$, where $\mathbf{u}_i^{(x_i)}$ denotes x_i copies of vector $\mathbf{u}_i$, is a eutactic star of scale s in L^* by using Lemma 11 again. This completes the proof. $\square$

7. The Lattice A_{15}^{+}

The lattice A_{15}^{+} is given in Definition 1. For a positive integer n, let S_n denote the symmetric group on $\{1,\ldots,n\}$. The symmetric group S_{16} acts on A_{15}^{+} such that, for $\mathbf{x} \in \mathsf{A}_{15}^{+}$, $\sigma \in S_{16}$ and $i \in \{1,\ldots,16\}$, the $\sigma(i)$-th entry of $\sigma(\mathbf{x})$ is defined by the i-th entry of $\mathbf{x}$. In fact, $\mathrm{Aut}(\mathsf{A}_{15}^{+}) = \langle S_{16}, -1\rangle$ holds (see [5, Subsection 6.1 in Chapter 4]).

In this section we discuss properties of the lattice A_{15}^{+} and its non-2-integrable sublattices. As claimed in Lemma 9, every non-2-integrable lattice of rank 12 is contained in A_{15}^{+}. Lemma 13 is the first statement of Theorem 3, which asserts our newly found lattices are $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}\rangle^{\perp}$ and $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}'\rangle^{\perp}$.

Lemma 13. *There are precisely two sublattices in A_{15}^{+} up to $\mathrm{Aut}(\mathsf{A}_{15}^{+})$ with Gram matrix defined as in (1.2). Furthermore, they are $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}\rangle$ and $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}'\rangle$ in A_{15}^{+}.*

Proof. Let T be the set of elements of norm 3 in A_{15}^{+}. For pairwise distinct integers i_1, i_2, i_3 and $i_4 \in \{1,\ldots,16\}$, we let

$$\mathbf{t}_{i_1,i_2,i_3,i_4} = \mathbf{t}_{\{i_1,i_2,i_3,i_4\}} := (1/4)\mathbf{e} - \mathbf{e}_{i_1} - \mathbf{e}_{i_2} - \mathbf{e}_{i_3} - \mathbf{e}_{i_4} \in \mathsf{A}_{15}^{+},$$

where $\mathbf{e}$ denotes the all one vector in $\mathbb{Z}^{16}$. For example the vector $[4]$ defined in Definition 1 is $\mathbf{t}_{13,14,15,16}$. First, we show that

$$T = \{\pm \mathbf{t}_I \mid I \subseteq \{1,\ldots,16\} \text{ and } |I| = 4\}. \tag{7.1}$$

As the representatives of cosets of A_{15} in A_{15}^{+} are 0, $\pm[4]$ and $2[4]$, and the norm of every element in A_{15} and $2[4] + \mathsf{A}_{15}$ is even, every element in T must belong to $\pm[4] + \mathsf{A}_{15}$. Let $\mathbf{y} = (y_1,\ldots,y_{16}) \in \mathsf{A}_{15}$, and suppose $[4] + \mathbf{y} \in T$. Then we obtain the two conditions

$$\sum_{i=1}^{12}(4y_i + 1) + \sum_{j=13}^{16}(4y_j - 3) = 0$$

and

$$\sum_{i=1}^{12}(4y_i + 1)^2 + \sum_{j=13}^{16}(4y_j - 3)^2 = 3 \cdot 4^2 = 48.$$

By the second condition, the odd integers $4y_i + 1$ and $4y_j - 3$ clearly belong to $\{-3, 1, 5\}$ for all i and j. For $h \in \{-3, 1, 5\}$, let

$$N_h := |\{i \in \{1,\ldots,12\} \mid 4y_i + 1 = h\}| + |\{j \in \{13,\ldots,16\} \mid 4y_j - 3 = h\}|.$$

Then we see that $N_5 \in \{0, 1\}$. In the case of $N_5 = 1$, the second condition implies that $N_{-3} \le 2$ and $N_1 \ge 16 - 3 = 13$. This contradicts the first condition. Namely

$N_5 = 0$ holds. Thus there exists $I \subseteq \{1, \ldots, 16\}$ with $|I| = 4$ such that $[4] + \mathbf{y} = \mathbf{t}_I$. This implies

$$\left([4] + \mathsf{A}_{15}^+\right) \cap T \subseteq \{\mathbf{t}_I \mid I \subseteq \{1, \ldots, 16\} \text{ and } |I| = 4\}.$$

As $-[4] + \mathsf{A}_{15}^+ = -([4] + \mathsf{A}_{15}^+)$, it comes with

$$\left(-[4] + \mathsf{A}_{15}^+\right) \cap T \subseteq \{-\mathbf{t}_I \mid I \subseteq \{1, \ldots, 16\} \text{ and } |I| = 4\}$$

and Equation (7.1) holds. Next, we classify three elements $\mathbf{x}, \mathbf{y}$ and $\mathbf{z}$ of norm 3 in A_{15}^+ up to $\mathrm{Aut}(\mathsf{A}_{15}^+)$ such that the Gram matrix with respect to them is defined as in (1.2). We can let $\mathbf{x} := \mathbf{t}_{1,2,3,4} = \mathbf{a}$. For subsets I and J of cardinality 4 in $\{1, \ldots, 16\}$, we have $(\mathbf{t}_I, \mathbf{t}_J) = -1 + |I \cap J|$. Hence, we let $\mathbf{y} := \mathbf{t}_{1,2,3,5} = \mathbf{b}$ to satisfy $(\mathbf{x}, \mathbf{y}) = 2$. Similarly, to satisfy $(\mathbf{x}, \mathbf{z}) = (\mathbf{y}, \mathbf{z}) = 0$, we let $\mathbf{z} := \mathbf{t}_{1,6,7,8} = \mathbf{c}$ or $\mathbf{z} := \mathbf{t}_{4,5,6,7} = \mathbf{c}'$. The desired conclusion holds. $\square$

8. Minimal Non-s-Integrable Lattices and the Proof of Theorem 3

8.1. Minimal Non-s-Integrable Lattices

In this subsection, we prove Proposition 5 which will be used to show the minimality of the sublattices $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}\rangle^\perp$ and $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}'\rangle^\perp$ in A_{15}^+. Let M be a lattice found by Conway and Sloane in Theorem 1. Although some non-2-minimal non-2-integrable lattices can be obtained as lattices contained in $M \perp \mathbb{Z}^m/\sqrt{2}$ for some positive integer m, the minimality of $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}\rangle^\perp$ and $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}'\rangle^\perp$ indicates that these two non-2-integrable lattices can not be obtained from Conway and Sloane's lattices in this way.

Plesken [13] studied minimal non-1-integrable lattices and additively indecomposable ones defined in the following. Note that he calls the bilinear form corresponding to a minimal non-1-integrable lattice a *block form*. We state his claims in terms of lattice theory.

Definition 3. A lattice L is said to be *additively decomposable* if there are two lattices M and N such that L is isometric to a sublattice of $M \perp N$ which is contained in neither N nor M. Otherwise it is said to be *additively indecomposable.*

Lemma 14 ([13, (II.5) Corollary])**.** *A lattice L is minimal non-1-integrable if and only if the minimum norm of L^* is greater than 1.*

Moreover, Plesken gave a sufficient condition for a lattice to be additively indecomposable (see [13, (III.1) Proposition]). With a slight change in his argument, the following proposition is derived.

Proposition 5. *Let L be a minimal non-1-integrable lattice. Suppose that there is an irreducible sublattice of rank at least* $\operatorname{rank} L - 5$ *which is generated by elements of norm at most* 3*. Then L is additively indecomposable.*

Proof. Suppose that there exists such a sublattice L'. By way of contradiction, we suppose that L is additively decomposable. Thus there are two lattices M and N such that $L \subseteq M \perp N$, $L \not\subseteq M$ and $L \not\subseteq N$. Let ρ_M and ρ_N denote the orthogonal projections to M and N, respectively. Namely, $\rho_M : L \to M$ and $\rho_N : L \to N$ are maps defined as $\rho_M(\mathbf{u}) := \mathbf{u}_M$ and $\rho_N(\mathbf{u}) := \mathbf{u}_N$ for $\mathbf{u} = \mathbf{u}_M + \mathbf{u}_N \in L$ with $\mathbf{u}_M \in M$ and $\mathbf{u}_N \in N$.

First we show that either $L' \subseteq M$ or $L' \subseteq N$. It suffices to show that there is no element $\mathbf{u} \in L'$ of norm at most 3 such that $\rho_M(\mathbf{u}) \neq 0$ and $\rho_N(\mathbf{u}) \neq 0$. Suppose that there exists such an element $\mathbf{u}$. Since

$$\{1, 2, 3\} \ni (\mathbf{u}, \mathbf{u}) = (\rho_M(\mathbf{u}), \rho_M(\mathbf{u})) + (\rho_N(\mathbf{u}), \rho_N(\mathbf{u})),$$

$\rho_M(\mathbf{u}) \neq 0$ and $\rho_N(\mathbf{u}) \neq 0$, one of the norms of $\rho_M(\mathbf{u})$ and $\rho_N(\mathbf{u})$ equals 1. Hence, without loss of generality we may assume the norm of $\rho_N(\mathbf{u})$ is equal to 1. Then $N = N' \perp \langle \rho_N(\mathbf{u}) \rangle$ for a sublattice N' of N. Therefore

$$L \subseteq M \perp N \subseteq (M \perp N') \perp \langle \rho_N(\mathbf{u}) \rangle \simeq (M \perp N') \perp \mathbb{Z}.$$

Also $0 \neq \rho_N(\mathbf{u}) \notin M \perp N'$ implies $L \not\subseteq M \perp N'$. Thus L is non-1-minimal, which contradicts the assumption that L is a minimal non-1-integrable lattice.

Now we may assume that $L' \subseteq M$. Set $P := (L' \otimes \mathbb{Q}) \cap L$. Then P is a primitive sublattice of L and $L = P \oplus Q$ for some sublattice Q of L. Since $P \subseteq M \otimes \mathbb{Q}$, we have

$$L \subseteq M \perp \rho_N(L) = M \perp \rho_N(Q).$$

As

$$\operatorname{rank} \rho_N(Q) \leq \operatorname{rank} Q = \operatorname{rank} L - \operatorname{rank} P = \operatorname{rank} L - \operatorname{rank} L' \leq 5,$$

this together with Theorem 10 implies that $\rho_N(Q)$ is a sublattice of an odd unimodular lattice of rank at most 8. It is well-known that every odd unimodular lattice of rank $k \leq 8$ is isometric to a standard lattice $\mathbb{Z}^k$ (see [5, Table 16.7]). Thus $\rho_N(Q) \subseteq \mathbb{Z}^8$. Furthermore, $L \subseteq M \perp \mathbb{Z}^8$ and $L \not\subseteq M$. This means that L is non-1-minimal, which leads to a contradiction. Thus, the desired conclusion holds. $\square$

8.2. Proof of Theorem 3

In this subsection, we complete the proof of Theorem 3.

Proof of Theorem 3. Set $N := \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle^{\perp}$ and $N' := \langle \mathbf{a}, \mathbf{b}, \mathbf{c}' \rangle^{\perp}$. As asserted in Lemma 13, there are precisely two sublattices N and N' in A_{15}^{+} up to $\operatorname{Aut}(\mathsf{A}_{15}^{+})$

with Gram matrix defined as in (1.2). Hence it suffices to show that they are non-isometric and minimal non-2-integrable.

First we show that N and N' are non-isometric by calculating the kissing numbers. Let R be the set of elements in A_{15}^{+} of norm 2. Note that $\mathsf{R} \subset \mathsf{A}_{15}$ holds. We have

$$N \cap \mathsf{R} = \{\mathbf{e}_i - \mathbf{e}_j \mid i \neq j \text{ and } i, j \in Y \text{ for some } Y \in \tau\}, \tag{8.1}$$

where $\tau := \{\{1\}, \{2,3\}, \{4\}, \{5\}, \{6,7,8\}, \{9,\ldots,16\}\}$. Since the minimum norm of N is 2, the kissing number of N is $|N \cap \mathsf{R}|$. Hence the kissing number of N is $2 \cdot 1 + 3 \cdot 2 + 8 \cdot 7 = 64$. Similarly,

$$N' \cap \mathsf{R} = \{\mathbf{e}_i - \mathbf{e}_j \mid i \neq j \text{ and } i, j \in Y \text{ for some } Y \in \tau'\}, \tag{8.2}$$

where $\tau' := \{\{1,2,3\}, \{4\}, \{5\}, \{6,7\}, \{8,\ldots,16\}\}$, and the kissing number of N' is $3 \cdot 2 + 2 \cdot 1 + 9 \cdot 8 = 80$. Hence N and N' are non-isometric.

Next we verify that N and N' are non-2-integrable by using a computer together with Lemma 12. We used Magma [1]. Indeed, we construct the lattice N in Magma, enumerate vectors of norm at most 2 in N^*, and check that (6.2) has no non-negative integer solutions. This together with Lemma 12 implies that N is non-2-integrable. By the same method, we may confirm that N' is non-2-integrable.

Finally we prove the minimality of N and N'. By using Magma again, we find that the minimum norms of N^* and $(N')^*$ are greater than 1. Thus, by Lemma 14, they are minimal non-1-integrable lattices. By applying Proposition 5 with $L := N$ and $L := N'$, we prove that N and N' are additively indecomposable. In particular, they are minimal non-2-integrable. Namely, it suffices to show that each of N and N' contains an irreducible sublattice of rank at least $7 = 12 - 5$ generated by elements of norm at most 3. By (8.1) and (8.2), both N and N' contain

$$\langle \mathbf{e}_9 - \mathbf{e}_{10}, \ldots, \mathbf{e}_{15} - \mathbf{e}_{16} \rangle$$

as a sublattice of rank 7. Therefore the desired conclusion follows. □

We remark that Plesken [13] has proved that $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}' \rangle^{\perp}$ is additively indecomposable (see [13, (III.3) Example]), where $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}' \rangle^{\perp}$ is written as $1^8, 2^3; 6$. Although $1^8, 2^3; 6$ was defined in a different way from $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}' \rangle^{\perp}$, we can verify by using a computer that $\langle \mathbf{a}, \mathbf{b}, \mathbf{c}' \rangle^{\perp}$ and $1^8, 2^3; 6$ are isometric.

Acknowledgements. We are grateful to Professor Munemasa, the editor and the anonymous referee for their valuable comments and suggestions that improve the quality of the paper.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[2] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, London, New York, 1978.

[3] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices I: Quadratic forms of small determinant, *Proc. Roy. Soc. London Ser. A* **418** (1988) 17–41.

[4] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices V: Integral coordinates for integral lattices. *Proc. Roy. Soc. London Ser. A* **426** (1989), no. 1871, 211–232.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups: 3rd Edition*, Springer-Verlag, New York, 1999.

[6] W. Ebeling, *Lattices and Codes: A Course Partially Based on Lectures by F. Hirzebruch, 3rd Edition*, Springer Spektrum, Berlin, 2013.

[7] L. J. Gerstein, *Basic Quadratic Forms*, Amer. Math. Soc., Providence, 2008.

[8] C. Ko, On the representation of a quadratic form as a sum of squares of linear forms, *Q. J. Math.* **8** (1937), 81–98.

[9] C. Ko, On the decomposition of quadratic forms in six variables, *Acta Arith.* **3** (1939), 64–78.

[10] C. Ko, On the decomposition of quadratic forms in seven variables, *Acad. Sinica Sci. Rec.* **1** (1942), 30–33.

[11] C. Ko, On the decomposition of quadratic forms in eight variables, *Acad. Sinica Sci. Rec.* **1** (1942), 33–36.

[12] L. J. Mordell, The representation of a definite quadratic form as a sum of two others, *Ann. of Math. (2)* **38** (1937), 751–757.

[13] W. Plesken, Additively indecomposable positive integral quadratic forms, *J. Number Theory* **47** (1994), 273–283.

[14] W. Plesken, Solving $XX^{\mathrm{tr}} = A$ over the integers, *Linear Algebra Appl.* **226-228** (1995), 331–344.