이학박사 학위논문

Minimal S-universality criterion sets

(최소 S-보편성 판정 집합)

2020년 2월

서울대학교 대학원

수리과학부

이 정 원

Minimal S-universality criterion sets

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
to the faculty of the Graduate School of
Seoul National University

by

Jeongwon Lee

Dissertation Director : Professor Byeong-Kweon Oh

Department of Mathematical Sciences
Seoul National University

February 2020

Abstract

For any set S of positive definite and integral quadratic forms with bounded rank, there is a finite subset S_0 of S such that any S_0-universal quadratic form is also S-universal. Such a set S_0 is called an S-universality criterion set.

In this thesis, we introduce various properties on minimal S-universality criterion sets. When S is a subset of positive integers, we show that a minimal S-universality criterion set is unique. For higher rank cases, we prove that a minimal S-universality criterion set is not unique when S is the set of all quadratic forms of rank n with $n \geq 9$.

We say a quadratic form f is recoverable if there is a minimal S_f-universality criterion set other than $\{f\}$, where S_f is the set of all subforms of f with same rank. We provide some necessary conditions, and some sufficient conditions for quadratic forms to be recoverable.

Key words: Representations of quadratic forms, minimal S-universality criterion sets
Student Number: 2013-20241

Contents

Chapter 1

Introduction

A positive definite (classic) integral quadratic form is a homogeneous quadratic polynomial

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \ (a_{ij} = a_{ji} \in \mathbb{Z})$$

such that $f(x_1, x_2, \ldots, x_n) > 0$ for any nonzero vector $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$. We say a quadratic form f *represents* an integer N if the diophantine equation $f(x_1, x_2, \ldots, x_n) = N$ has an integer solution. We also say a quadratic form f is *universal* if it represents all positive integers.

The famous Legendre's four square theorem says that every integer n is a sum of four squares of integers, that is, the quaternary quadratic form $x^2 + y^2 + z^2 + t^2$ is universal. In 1916, Ramanujan [21] found all positive definite integral diagonal quaternary universal quadratic forms. Later, Dickson [6] confirmed Ramanujan's results except for $x^2 + 2y^2 + 5z^2 + 5t^2$. In the exceptional case, it is known that $x^2 + 2y^2 + 5z^2 + 5t^2$ represents all integers except for 15.

In 1997, Conway and Schneeberger provided a very interesting criterion, so-called, the '15-Theorem', which states that any positive definite integral quadratic form representing

$$1, 2, 3, 5, 6, 7, 10, 14, \text{ and } 15.$$

is, in fact, universal.

Let S be a set of positive definite integral quadratic forms with bounded rank. A quadratic form f is called *S-universal* if it represents all quadratic forms in S. A subset S_0 of S is called *an S-universality criterion set* if any quadratic form representing all quadratic forms in S_0 is S-universal. For an arbitrary set S of quadratic forms with bounded rank, the existence of a finite S-universality criterion set was proved in [11].

An S-universality criterion set S_0 is called *minimal* if any proper subset of S_0 is not an S-universality criterion set. In [11], Kim, Kim, and Oh proposed the following questions: Let $\Gamma(S)$ be the set of all S-universality criterion sets.

(i) For which S is there a unique minimal $S_0 \in \Gamma(S)$?

(ii) Is there a constant $\gamma(S)$ such that $|S_0| = \gamma(S)$ for every minimal $S_0 \in \Gamma(S)$? If not, when?

Let Φ_n be the set of all (positive definite and integral) quadratic forms of rank n. For the question (i), the uniqueness of minimal Φ_n-universality criterion sets was proved by Bhargava [1] for rank 1 case, and by Kominers [16], [17] for rank 2 and 8 cases, respectively(see also [12], [10], and [18]). Recently, Elkies, Kane, and Kominers [8] answered the question (ii) in the negative for some special set S of quadratic forms.

In this thesis, we discuss some problems related to the above two questions. Some results in this thesis were done by joint work with B.-K. Oh.

In Chapter 2, we introduce several terminologies and results on quadratic spaces and lattices.

In Chapter 3, we consider the case when S is a subset of positive integers. In Section 1, we prove the uniqueness of minimal S-universality criterion sets. Moreover, we show that the sizes of minimal S-universality criterion sets can be arbitrarily large. We also discuss the size of a minimal S-universality criterion set for some special set S, so called, '2-full set'. In Section 2, we show that minimal S-universality criterion sets are not unique, in general. In fact, we prove there are infinitely many minimal Φ_n-universality criterion sets for any integer n greater than 8.

In Chapter 4, we give an answer for the question (ii) in the case when S is the set of all subforms of a quadratic form. Note that if S is the set of all subforms of f, then the one element set $\{f\}$ is a minimal S-universality criterion set. We say f is *recoverable by* S_0 if there is a finite set S_0 of subforms of f other than $\{f\}$ such that any quadratic form representing all quadratic forms in S_0 represents f itself. In other words, a quadratic form f is not recoverable if and only if f has the unique minimal S-universality criterion set $\{f\}$. In this chapter, we prove some necessary conditions, and some sufficient conditions for quadratic forms to be recoverable. In Section 1, we provide some properties of recoverable quadratic forms, and we prove that every indecomposable binary or ternary quadratic form is not recoverable. In Section 2 and Section 3, we concentrate on recoverable binary quadratic forms. We find infinite examples of recoverable binary quadratic forms, and also infinite examples of non-recoverable binary quadratic forms.

Chapter 2

Preliminaries

In this chapter, we introduce some terminologies and results which will be used throughout the thesis.

2.1 Quadratic spaces and lattices

Let $\mathbb{Q}$ be the rational number field. For a prime p, we denote the field of p-adic completion of $\mathbb{Q}$ by $\mathbb{Q}_p$. When $p = \infty$, we denote $\mathbb{Q}_\infty$ by the field of real numbers $\mathbb{R}$. Let F be a field $\mathbb{Q}$ or $\mathbb{Q}_p$ for some prime p.

Let V be a finite dimensional vector space over F. Let B be a symmetric bilinear map defined on V, that is, $B : V \times V \to F$ satisfies the following properties:

$$B(x, y) = B(y, x), \quad B(\alpha x + \beta y, z) = \alpha B(x, z) + \beta B(y, z),$$

for any $x, y, z \in V$ and $\alpha, \beta \in F$. Then the *quadratic map* Q associated with B is defined by

$$Q(x) = B(x, x),$$

for any $x \in V$. We define (V, B) a *quadratic space* over F. We say that a quadratic space V is *unary, binary, ternary, quaternary,. . . , n-ary*, if the dimension of V is $1, 2, 3, 4, \dots, n, respectively$.

Let (V, B) be a quadratic space over F and let $\mathfrak{B} = \{x_1, x_2, \dots, x_n\}$ be a basis for V. The symmetric matrix defined by

$$(B(x_i, x_j))_{1 \le i,j \le n}$$

is called the *Gram matrix* of V in $\mathfrak{B}$, and we write

$$V = (B(x_i, x_j))_{1 \le i,j \le n} \ \text{ in } \mathfrak{B}.$$

If the symmetric matrix $(B(x_i, x_j))_{1 \le i,j \le n}$ is a diagonal matrix, then we simply write

$$V = \langle Q(x_1), Q(x_2), \dots, Q(x_n) \rangle \ \text{ in } \mathfrak{B}.$$

Given a symmetric matrix A and a quadratic space V, the expression $V \simeq A$ means that there is a basis $\mathfrak{C}$ for V such that $V = A$ in $\mathfrak{C}$. We say that a quadratic space V defined over $\mathbb{Q}$ is *positive definite* if the matrix $(B(x_i, x_j))$ is positive definite. The canonical image of the determinant of the symmetric matrix $(B(x_i, x_j))$ in $(F^\times/(F^\times)^2) \cup \{0\}$ is called the *discriminant* of V, and is denoted by dV. We say V is a *regular* quadratic space if $dV \neq 0$.

Let V and W be quadratic spaces over F and let Q be the quadratic map defined on each of them. A linear map σ from V into W satisfying

$$Q(\sigma(x)) = Q(x) \quad \text{for any } x \in V$$

is called a *representation* of V into W. We also say that W *represents* V. A bijective representation σ is called an *isometry* from V onto W. In this case, we say that V and W are *isometric*, and write $V \simeq W$.

Let R be the ring of integers $\mathbb{Z}$, or the ring of p-adic integers $\mathbb{Z}_p$ for a prime p, and let F be its quotient field. Let V be a quadratic space over F. An R-module L in V is called a *lattice* in V if L is finitely generated. We denote the set $\{\alpha x \mid \alpha \in F, x \in L\}$ as FL. We define the *rank* of L the dimension of FL and we say L is an R-lattice *on* V if $FL = V$.

Note that every finitely generated torsion-free R-module is free when $R = \mathbb{Z}$ or $\mathbb{Z}_p$ for some prime p. Let $\mathfrak{B} = \{x_1, x_2, \dots, x_n\}$ be a basis for L. The symmetric matrix defined by $(B(x_i, x_j))_{1 \le i,j \le n}$ is called the *Gram matrix* of L in $\mathfrak{B}$, and we write

$$L = (B(x_i, x_j))_{1\le i,j\le n} \ \text{ in } \mathfrak{B}.$$

If the symmetric matrix $(B(x_i, x_j))_{1\le i,j\le n}$ is a diagonal matrix, then we simply write

$$L = \langle Q(x_1), Q(x_2), \ldots, Q(x_n)\rangle \ \text{ in } \mathfrak{B}.$$

We sometimes omit 'in $\mathfrak{B}$' in the above expression if there is no confusion. Given a symmetric matrix A and an R-lattice L, the expression $L \simeq A$ means that there is a basis $\mathfrak{C}$ for L such that $L = A$ in $\mathfrak{C}$. The canonical image of the determinant of the symmetric matrix $(B(x_i, x_j))$ in $(F^\times/(R^\times)^2) \cup \{0\}$ is called the *discriminant* of L, and we denote it by dL. We say L is a *regular* R-lattice if $dL \ne 0$. If there exists a nonzero vector v in L satisfying $Q(v) = 0$, then we call L *isotropic*. Otherwise, we call L *anisotropic*. The *scale* of L is defined by the ideal of R generated by $B(x, y)$ for any x and y in L, and the *norm* of L is defined by the ideal of R generated by $Q(x)$ for any x in L. We use L^α with $\alpha \in \mathbb{Z}$ to denote the lattice L with a new bilinear form $B^\alpha(x, y) = \alpha B(x, y)$ and the quadratic map $Q^\alpha(x) = \alpha Q(x)$ for any $x, y \in L$.

The corresponding quadratic form of L is defined by

$$f_L = f_L(y_1, y_2, \ldots, y_n) = \sum_{1\le i,j\le n} B(x_i, x_j) y_i y_j.$$

Throughout this thesis, we identify a lattice with its Gram matrix or the corresponding quadratic form. We always assume that all quadratic spaces and lattices are regular. We also assume that all $\mathbb{Q}$-spaces are positive definite and all $\mathbb{Z}$-lattices are integral, that is, their scales are contained in $\mathbb{Z}$.

Let L and M be R-lattices on the quadratic spaces V and W, respectively. We say that M *represents* L if there is a representation $\sigma : FL \to FM$ satisfying $\sigma(L) \subseteq M$, and in this case, we simply write $L \to M$. Moreover, we say that L and M are *isometric* if there is a representation $\sigma : FL \to FM$ satisfying $\sigma(L) = M$ and we write $L \simeq M$.

Let $\mathbb{Z}_p$ be the p-adic integer ring for a prime p. We define $L_p = \mathbb{Z}_p \otimes L$, which is a $\mathbb{Z}_p$-lattice. We say that L is *anisotropic at a prime* p if L_p is anisotropic. For $\mathbb{Z}$-lattices L and M, if L_p is isometric to M_p for all primes p, then we say that L is *locally isometric* to M. The set of all $\mathbb{Z}$-lattices isometric to L is defined by the *class of* L, and denoted by $\text{cls}(L)$. The set of all $\mathbb{Z}$-lattices that are locally isometric to L is defined by the *genus of* L, and denoted by $\text{gen}(L)$. The *class number* $h(L)$ of L is defined by the number of classes in the genus of L.

For $\mathbb{Z}$-lattices L and M, although L locally represents M for every prime p, L does not represent M, in general. More precisely, the following theorem holds.

Theorem 2.1.1. *For $\mathbb{Z}$-lattices L and M, if M is locally represented by L, then there exist a $\mathbb{Z}$-lattice $L' \in gen(L)$ which represents M.*

Proof. See 102:5 Example in [19]. □

Theorem 2.1.2. *For $3 \leq n \leq 5$, every quadratic form of rank n is represented by a sum of $n+3$ integral linear squares.*

Proof. See [15]. One may easily verify this by using the above theorem and the local representation theory. □

When the rank of L is greater than or equal to 4, the following theorems are also known.

Theorem 2.1.3. *For a $\mathbb{Z}$-lattice L of rank $r \geq 5$, there is a constant $c(L)$ satisfying the following property: if an integer n is locally represented by L and $n \geq c(L)$, then n is represented by L.*

Proof. See [22]. □

Theorem 2.1.4. *For a $\mathbb{Z}$-lattice L of rank 4, there is a constant $c(L)$ satisfying the following property: if an integer n satisfies*

(i) *n is locally represented by L,*

(ii) *n is primitively represented by L at the anisotropic primes,*

(iii) *$n \geq c(L)$,*

then n is represented by L.

Proof. See [14]. □

Suppose that $L_1, L_2, \ldots, L_r$ are sublattices of an R-lattice L and

$$L = L_1 \oplus L_2 \oplus \cdots \oplus L_r.$$

Suppose further that

$$B(x, y) = 0 \text{ for any } x \in L_i, y \in L_j \text{ with } 1 \leq i < j \leq r.$$

Then we say that L is the *orthogonal sum of* $L_1, \ldots, L_r$, and in this case, we write

$$L = L_1 \perp L_2 \perp \cdots \perp L_r.$$

The *dual lattice* $L^{\#}$ of a $\mathbb{Z}$-lattice L is defined by

$$L^{\#} = \{x \in \mathbb{Q}L \mid B(x, L) \subseteq \mathbb{Z}\}.$$

One may easily show that $L \subseteq L^{\#}$ and $|L^{\#}/L| = |dL|$. A $\mathbb{Z}$-lattice L is called *unimodular* if $dL = \pm 1$. If L is unimodular, then we have $L^{\#} = L$.

We say that L is *decomposable* if L is isometric to the orthogonal sum of two nonzero sublattices of L. Otherwise, we say that L is *indecomposable.*

Let L be a $\mathbb{Z}$-lattice. Suppose that for any representation σ from L into the orthogonal sum of two nonzero $\mathbb{Z}$-lattices M_1 and M_2, $\sigma(L) \subseteq M_1$ or $\sigma(L) \subseteq M_2$ holds. Then, we say that L is *additively indecomposable.* It is well known that every indecomposable unimodular lattice is also additively indecomposable. For more properties on additively indecomposable lattices, see [20].

2.2 Minkowski-reduced forms

Let V be a quadratic space over $\mathbb{Q}$ and let L be a $\mathbb{Z}$-lattice in V. We say $\mathfrak{B} = \{x_1, x_2, \ldots, x_n\}$ is a *Mikowski-reduced basis* for L if for each i with $1 \leq i \leq n$,

$$Q(x_i) \leq Q(y),$$

for any vector $y \in L$ such that the set $\{x_1, x_2, \ldots, x_{i-1}, y\}$ can be extended to a basis for L. Here, if $i = 1$, the above inequality holds for all primitive vectors y in L.

Theorem 2.2.1. *Every positive definite $\mathbb{Z}$-lattice has at least one Minkowski-reduced basis.*

Proof. See Theorem 1.1 of Chapter 12 in [2]. □

If rank of L is less than or equal to 4, then the following holds.

Theorem 2.2.2. *Let $n \leq 4$. For a $\mathbb{Z}$-lattice L, $\{x_1, x_2, \ldots, x_n\}$ is a Mikowski-reduced basis for L if and only if the following holds:*

(i) $0 < Q(x_1) \leq Q(x_2) \leq \cdots \leq Q(x_n)$*;*

(ii) $Q(x_j) \leq Q(y)$ *for any* j *with* $1 \leq j \leq 4$ *and for any*

$$y = \sum_{i=1}^{n} a_i x_i \text{ with } a_i = \begin{cases} 0 \text{ or } \pm 1 & \text{if } i < j, \\ 1 & \text{if } i = j, \\ 0 & \text{if } i > j. \end{cases}$$

Proof. See Lemma 1.2 of Chapter 12 in [2]. □

Note that for $n = 2$, the conditions (i) and (ii) are equivalent to

$$0 < Q(x_1) \leq Q(x_2), \text{ and } 2|B(x_1, x_2)| \leq Q(x_1).$$

For $n = 3$, the conditions (i) and (ii) implies that

$$0 < Q(x_1) \leq Q(x_2) \leq Q(x_3),$$
$$2|B(x_1, x_2)| \leq Q(x_1), \quad 2|B(x_1, x_3)| \leq Q(x_1), \quad 2|B(x_2, x_3)| \leq Q(x_2).$$

On the other hand, for a $\mathbb{Z}$-lattice L of rank n, the *i-th minimum* $\mu_i(= \mu_i(L))$ of L is defined by the positive integer such that

(i) the dimension of the subspace of $\mathbb{Q}L$ which spanned by $x \in L$ with $Q(x) \leq \mu_i$ is greater than or equal to i;

(ii) the dimension of the subspace of $\mathbb{Q}L$ which spanned by $x \in L$ with $Q(x) < \mu_i$ is less than i.

Note that

$$\mu_1(L) = \min(L) = \min_{x \in L - \{0\}} Q(L).$$

The integers $\mu_1, \mu_2, \ldots, \mu_n$ are called the *successive minima* of L. One may easily show that $\mu_1, \mu_2, \ldots, \mu_n$ are well defined and, in fact,

$$\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n.$$

Theorem 2.2.3. *Let L be a $\mathbb{Z}$-lattice of rank n and let i be an integer with $2 \leq i \leq n$. Suppose that there exist linearly independent vectors $x_1, x_2, \ldots, x_{i-1}$ in L such that $Q(x_j) = \mu_j$ for all j with $1 \leq j \leq i-1$. If $y \in L$ satisfies $Q(y) < \mu_i$, then y is linearly independent of $x_1, x_2, \ldots, x_{i-1}$.*

Proof. See Lemma 2.1 of Chapter 12 in [2]. □

Theorem 2.2.4. *Let L be a $\mathbb{Z}$-lattice of rank n with successive minima $\mu_1, \mu_2, \ldots, \mu_n$. Then there exists a constant C depending only on n such that*

$$dL \leq \mu_1 \cdot \mu_2 \cdots \mu_n \leq C \cdot dL.$$

Proof. See Proposition 2.3 in [7]. □

Theorem 2.2.5. *Let d and n be positive integers. Then there exist only finitely many $\mathbb{Z}$-lattices of discriminant d of rank n up to isometry.*

Proof. See Corollary 2.1.1 in [13]. □

The above two theorems imply that there exist only finitely many $\mathbb{Z}$-lattices of given rank n such that their n-th successive minima are bounded.

2.3 Gluing theory

Let $\{e_1, e_2, \cdots, e_n\}$ be a standard orthonormal basis for $\mathbb{R}^n$. Then we define some $\mathbb{Z}$-lattices as follows.

$$\begin{aligned}
I_n &= \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n && \text{(for } n \geq 1\text{)}\\
A_n &= \left\{ \sum_{i=1}^{n+1} a_i e_i \in I_{n+1} \ : \ \sum_{i=1}^{n+1} a_i = 0 \right\} && \text{(for } n \geq 1\text{)}\\
&= \mathbb{Z}(e_1 - e_2) + \mathbb{Z}(e_2 - e_3) + \cdots + \mathbb{Z}(e_n - e_{n+1})\\
D_n &= \left\{ \sum_{i=1}^{n} a_i e_i \in I_n \ : \ \sum_{i=1}^{n} a_i \in 2\mathbb{Z} \right\} && \text{(for } n \geq 4\text{)}\\
&= \mathbb{Z}(e_1 - e_2) + \mathbb{Z}(e_2 - e_3) + \cdots + \mathbb{Z}(e_{n-1} - e_n) + \mathbb{Z}(e_{n-1} + e_n)\\
E_8 &= \left\{ \sum_{i=1}^{8} a_i e_i \ : \ 2a_i \in \mathbb{Z}, a_i - a_j \in \mathbb{Z}, \sum_{i=1}^{8} a_i \in 2\mathbb{Z} \right\}\\
E_7 &= \left\{ \sum_{i=1}^{8} a_i e_i \in E_8 \ : \ \sum_{i=1}^{8} a_i = 0 \right\}\\
E_6 &= \left\{ \sum_{i=1}^{8} a_i e_i \in E_8 \ : \ \sum_{i=2}^{7} a_i = a_1 + a_8 = 0 \right\}
\end{aligned}$$

We call these lattices *root lattices*. Witt's Theorem states that for any $\mathbb{Z}$-lattice L, the sublattice generated by vectors of norm 1 and 2 is a direct sum of root lattices.

Gluing theory is a way to describe a $\mathbb{Z}$-lattice of rank n that has a sublattice of full rank which is the orthogonal sum

$$L_1 \perp L_2 \perp \cdots \perp L_k$$

of given $\mathbb{Z}$-lattices $L_1, L_2, \ldots, L_k$. We can write every vector x in L as $x_1 + x_2 + \cdots + x_k$ with $x_i \in L_i^{\#}$ for all $1 \leq i \leq k$. Since any x_i can be replaced by adding a vector of L_i, we may assume that x_i is one of representatives of a standard system for the cosets of L_i in $L_i^{\#}$. These representatives are called *glue vectors* for L_i and the quotient group $L_i^{\#}/L_i$ is called the *glue group* for

L_i. Note that the order of the glue group for L_i equals to the determinant of L_i. We list glue vectors and the glue group for each root lattices. We usually choose glue vectors to be of minimal norm in their cosets for the computational convenience.

(i) A_n for $n \geq 1$:

The glue group of A_n is the cyclic group of order $n+1$, that is,

$$A_n^{\#}/A_n \simeq \mathbb{Z}/(n+1)\mathbb{Z}.$$

The typical glue vector of A_n is given by

$$[i] = \Big(\underbrace{\frac{i}{n+1}, \ldots, \frac{i}{n+1}}_{j\text{–components}}, \underbrace{\frac{-j}{n+1}, \ldots, \frac{-j}{n+1}}_{i\text{–components}} \Big),$$

where $i + j = n + 1$ and $0 \leq i \leq n$. For i, j and k with $0 \leq i, j, k \leq n$, the norm of $[i]$ is $\frac{ij}{n+1}$ and $[j] + [k] = [j + k]$ holds in glue group.

(ii) D_n for $n \geq 4$:

The glue group of D_n is

$$D_n^{\#}/D_n \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } n \equiv 1 \pmod 2, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } n \equiv 0 \pmod 2. \end{cases}$$

The typical glue vectors of D_n are given by

$$\begin{aligned} &[0] = (0, 0, \ldots, 0) && \text{of norm } 0, \\ &[1] = \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right) && \text{of norm } \frac{n}{4}, \\ &[2] = (0, 0, \ldots, 0, 1) && \text{of norm } 1, \\ &[3] = \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2}\right) && \text{of norm } \frac{n}{4}. \end{aligned}$$

Note that if n is even, then $[i] + [i] = 0$ holds for any i with $0 \leq i \leq 3$ and if n is odd, then $[1] + [2] = [3]$ holds.

(iii) E_n for $n = 6, 7, 8$:

The glue group of E_n is the cyclic group of order $9 - n$, that is,

$$E_n^{\#}/E_n \simeq \mathbb{Z}/(9-n)\mathbb{Z}.$$

Since $E_8^{\#} = E_8$, the only glue vector for E_8 is

$$[0] = (\underbrace{0, 0, \ldots, 0}_{8\text{–components}}).$$

The typical glue vectors of E_7 are given by

$$\begin{aligned} &[0] = (0,0,0,0,0,0,0,0) && \text{of norm } 0, \\ &[1] = \left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{3}{4}, -\frac{3}{4}\right) && \text{of norm } \frac{3}{2}. \end{aligned}$$

The typical glue vectors of E_6 are given by

$$\begin{aligned} &[0] = (0,0,0,0,0,0,0,0) && \text{of norm } 0, \\ &[1] = \left(0, -\frac{2}{3}, -\frac{2}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, 0\right) && \text{of norm } \frac{4}{3}, \\ &[2] = -[1] && \text{of norm } \frac{4}{3}. \end{aligned}$$

2.4 S-universality criterion sets

Definition 2.4.1. Let S be any set of $\mathbb{Z}$-lattices. A $\mathbb{Z}$-lattice L is called S-*universal* if L represents all $\mathbb{Z}$-lattices in S. For a subset S_0 of S, if every S_0-universal lattice is also S-universal, then we say that S_0 is an S-*universality criterion set*.

When S is a subset of positive integers, the existence of a finite S-universality criterion set was proved by Bhargava. He also found a finite S-universality criterion set for some interesting set S such as the set of all primes, and the set of all positive odd integers:

Theorem 2.4.2. *An integral quadratic form represents all prime numbers if and only if it represents*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 67, \text{ and } 73.$$

Theorem 2.4.3. *An integral quadratic form represents all odd integers if and only if it represents*

$$1, 3, 5, 7, 11, 15, \text{ and } 33.$$

Bhargava's result was fully generalized by Kim, Kim, and Oh [11]. In fact, they proved the following:

Theorem 2.4.4. *Let S be a set of $\mathbb{Z}$-lattices with bounded rank. Then there exists a finite subset S_0 of S such that every S_0-universal $\mathbb{Z}$-lattice is S-universal.*

Proof. See [11]. □

Corollary 2.4.5. *Let S be any set of $\mathbb{Z}$-lattices with bounded rank. There always exists an S-universal $\mathbb{Z}$-lattice.*

Proof. By Theorem 2.4.4, there exists a finite subset S_0 of S such that every S_0-universal $\mathbb{Z}$-lattice is S-universal. Put $S_0 = \{L_1, L_2, \dots, L_t\}$. Then $L_1 \perp L_2 \perp \cdots \perp L_t$ is S_0-universal, and so it is S-universal. □

Definition 2.4.6. Let S be any set of $\mathbb{Z}$-lattices. For a subset S_0 of S, we say that S_0 is a *minimal* S-universality criterion set if S_0 itself is an S-universality criterion set and any proper subset of S_0 is not an S-universality criterion set.

Let Φ_n be the set of all quadratic $\mathbb{Z}$-lattices of rank n. It is well known that there is a unique minimal Φ_n-universality criterion set for $n = 1, 2$ or 8.

Theorem 2.4.7. *The set*

$$S_0 = \{1, 2, 3, 5, 6, 7, 10, 14, 15\}$$

is the unique minimal Φ_1-universality criterion set.

Proof. See [1]. □

Theorem 2.4.8. *The set*

$$\mathcal{T}_0 = \left\{ \langle 1,1\rangle, \langle 2,3\rangle, \langle 3,3\rangle, \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix} \right\}$$

is the unique minimal Φ_2-universality criterion set.

Proof. See [10]. □

Theorem 2.4.9. *The set*

$$\mathcal{U}_0 = \{I_8, E_8\}$$

is the unique minimal Φ_8-universality criterion set.

Proof. See [18]. □

However, in general, minimal S-universality criterion sets are not unique, and furthermore, the sizes of minimal S-universality criterion sets may vary. The following example was given by Elkies and his collaborators.

Theorem 2.4.10. *Let S be the set of all sublattices of a $\mathbb{Z}$-lattice $\langle 1,1,2\rangle$. Then the sets*

$$\{\langle 1,1,2\rangle\} \text{ and } \{\langle 1,1,16\rangle, \langle 2,2,2\rangle\}$$

are minimal S-universality criterion sets.

Proof. See [8]. □

Chapter 3

Uniqueness of minimal S-universality criterion sets

In this chapter, we focus on answering of the question:

> for which S is there a unique minimal S-universality criterion set?

We prove that there is a unique minimal S-universality criterion set when S is a subset of integers. Moreover, we prove that there is a subset S of positive integers such that the cardinality of its minimal universality criterion set is arbitrarily large.

3.1 Rank 1 case

Let $\mathbb{N}$ be the set of positive integers. For a positive integer m and a nonnegative integer α, we define the set of arithmetic progressions

$$A_{m,\alpha} = \{mn + \alpha : n = 0, 1, 2, \dots\}.$$

If a quadratic form f represents all elements in $A_{m,\alpha}$, we simply write $A_{m,\alpha} \to f$.

Proposition 3.1.1. *Let $S = \{s_0, s_1, s_2, \dots\}$ be a subset of $\mathbb{N}$, where $s_i \leq s_{i+1}$ for any nonnegative integer i, and let k be a positive integer. If there is a* *quadratic form* $f(x_1, x_2, \ldots, x_u)$ *such that*

$$s_0, s_1, \ldots, s_{k-1} \in Q(f) \quad \textit{and} \quad s_k \notin Q(f),$$

then there is a quadratic form F *such that* $Q(F) \cap S = S - \{s_k\}$.

Proof. First, we define

$$\mathfrak{C} = \{0 \le u \le s_{k+1} - 1 : A_{s_{k+1},u} \cap \{s_{k+1}, s_{k+2}, \ldots\} \ne \emptyset\} = \{c_1, c_2, \ldots, c_v\},$$

and for each $c \in \mathfrak{C}$, $s(c) = \min(A_{s_{k+1},c} \cap \{s_{k+1}, s_{k+2}, \ldots\})$. Now, define

$$\begin{aligned} &F(x_1, \ldots, x_u, y_1, \ldots, y_4, z_1, \ldots, z_v) \\ &= f(x_1, \ldots, x_u) + s_{k+1}(y_1^2 + \cdots + y_4^2) + \sum_{j=1}^{v} s(c_j) z_j^2. \end{aligned}$$

Since $s_{k+1}, s(c_j) > s_k$ and $s_k \notin Q(f)$, s_k is not represented by F. Furthermore, for any integer $a \in \{s_{k+1}, s_{k+2}, \ldots\}$, there is a nonnegative integer M and an integer i $(1 \le i \le v)$ such that $a = s_{k+1}M + s(c_i)$. Since M is represented by a sum of four squares, the integer a is represented by F. The proposition follows directly from this. □

Theorem 3.1.2. *For any set* $S = \{s_0, s_1, s_2, \ldots\} \subseteq \mathbb{N}$*, a minimal* S*-universality criterion set is unique.*

Proof. Without loss of generality, we may assume that $s_i \le s_{i+1}$ for any nonnegative integer i. An integer $s_i \in S$ is called a truant of S if there is a quadratic form f such that f represents all integers in $\{s_0, s_1, \ldots, s_{i-1}\}$, whereas f does not represent s_i. Clearly, s_0 is a truant of S. Let $T(S)$ be the set of truants of S. Then, by Proposition 3.1.1, any S-universality criterion set should contain $T(S)$. Hence it suffices to show that $T(S)$ itself is an S-universality criterion set. Let f be a quadratic form that represents all integers in $T(S)$. Suppose that f is not S-universal. Let m be the smallest integer such that s_m is not represented by f. Then, clearly, s_m is a truant of S, and hence $s_m \in T(S)$. This is a contradiction. Therefore $T(S)$ is the unique minimal S-universality criterion set. □

From the proof of Theorem 3.1.2, one may also show that if S_0 is the unique minimal S-universality criterion set, then for any $N \in S_0$, there is a $\mathbb{Z}$-lattice L_N that represents all integers in S except for N.

Proposition 3.1.3. *For any positive integer k greater than 3, the diagonal $\mathbb{Z}$-lattice $\langle k, k+1, \dots, 2k\rangle$ represents all integers greater than or equal to k.*

Proof. Note that every positive integer n greater than or equal to k is of the form $km + a$ for some integers m and a with $m \geq 0$ and $k \leq a \leq 2k-1$.

Firstly, assume that k is greater than or equal to 7. Let a be any integer with $k \leq a \leq 2k-1$. One may choose two integers k_1 and k_2 with $0 < k_1 < k_2 \leq \lfloor \frac{k-1}{2} \rfloor$ such that both of k_1 and k_2 are not equal to $a-k$ and $2k-a$. Note that $\langle 1,2,3,3\rangle$ is universal. Since $\langle k, 2k, 3k, 3k\rangle$ is a sublattice of the diagonal $\mathbb{Z}$-lattice

$$L = \langle k, 2k, k+k_1, 2k-k_1, k+k_2, 2k-k_2\rangle,$$

L represents all nonnegative integers which are multiple of k. Then

$$A_{k,a} \longrightarrow \langle k, 2k, k+k_1, 2k-k_1, k+k_2, 2k-k_2, a\rangle,$$

which implies that $A_{k,a} \to \langle k, k+1, \dots, 2k\rangle$.

Secondly, suppose that $k = 6$. Since $\langle 6, 12, 18, 36\rangle$ is a sublattice of $\langle 6, 6+k', 9, 12-k', 12\rangle$ for $k' = 1, 2$, it is clear that

$$A_{6,a} \longrightarrow \langle 6,7,8,9,10,11,12\rangle \text{ with } a = 7,8,10,11.$$

On the other hand, we know that $A_{6,0} \to \langle 6,12,18,18\rangle$ and $\langle 6,12,18,18\rangle$ is a sublattice of $\langle 6,7,8,10,11,12\rangle$. Therefore,

$$A_{6,6} \to \langle 6,7,8,9,10,11,12\rangle \text{ and } A_{6,9} \to \langle 6,7,8,9,10,11,12\rangle.$$

Thirdly, assume that $k = 5$. It is well known that $\langle 1,2,3\rangle$ represents all nonnegative integers except for integers of the form $4^m(16u+10)$ for some nonnegative integers m and u. Note that $\langle 5,10,15\rangle$ is a sublattice of $\langle 5,6,9,10\rangle$ and $\langle 5,7,8,10\rangle$.

(Case 1) For an integer n with $n \geq 11$, note that

$$5n+5 = 5(n-2)+15 = 5(n-11)+15\cdot 2^2$$

and either $n-2$ or $n-11$ is not of the form $4^m(16u+10)$. Then either

$$5(n-2) \longrightarrow \langle 5,10,15\rangle \quad \text{or} \quad 5(n-11) \longrightarrow \langle 5,10,15\rangle$$

holds, and the same thing is also true for $\langle 5,6,9,10\rangle$. Thus, every integer of the form $5n+5$ with $n \geq 3$ is represented by $\langle 5,6,7,8,9,10\rangle$. One may easily check that $\langle 5,6,7,8,9,10\rangle$ also represents all integers of the form $5n+8$ for $0 \leq n < 11$.

(Case 2) For an integer n with $n \geq 15$, note that

$$5n+6 = 5(n-15)+9\cdot 3^2$$

and either n or $n-15$ is not of the form $4^m(16u+10)$. Then either

$$5n \longrightarrow \langle 5,10,15\rangle \quad \text{or} \quad 5(n-15) \longrightarrow \langle 5,10,15\rangle$$

holds, and the same thing is also true for $\langle 5,7,8,10\rangle$. Thus, every integer of the form $5n+6$ with $n \geq 15$ is represented by $\langle 5,6,7,8,9,10\rangle$. One may easily check that $\langle 5,6,7,8,9,10\rangle$ also represents all integers of the form $5n+6$ for $0 \leq n < 15$.

(Case 3) For an integer n with $n \geq 5$, note that

$$5n+7 = 5(n-5)+8\cdot 2^2$$

and either n or $n-5$ is not of the form $4^m(16u+10)$. Then either

$$5n \longrightarrow \langle 5,10,15\rangle \quad \text{or} \quad 5(n-5) \longrightarrow \langle 5,10,15\rangle$$

holds, and the same thing is also true for $\langle 5,6,9,10\rangle$. Thus, every integer of the form $5n+7$ with $n \geq 5$ is represented by $\langle 5,6,7,8,9,10\rangle$. One may easily check that $\langle 5,6,7,8,9,10\rangle$ also represents all integers of the form $5n+7$ for $0 \leq n < 5$.

(Case 4) For an integer n with $n \geq 11$, note that

$$5n+8 = 5(n-11) + 7 \cdot 3^2$$

and either n or $n-11$ is not of the form $4^m(16u+10)$. Then either

$$5n \longrightarrow \langle 5, 10, 15 \rangle \quad \text{or} \quad 5(n-11) \longrightarrow \langle 5, 10, 15 \rangle$$

holds and the same thing is also true for $\langle 5, 6, 9, 10 \rangle$. Thus, every integer of the form $5n+7$ with $n \geq 5$ is represented by $\langle 5, 6, 7, 8, 9, 10 \rangle$. One may easily check that $\langle 5, 6, 7, 8, 9, 10 \rangle$ also represents all integers of the form $5n+8$ for $0 \leq n < 11$.

(Case 5) For an integer n with $n \geq 3$, it is true that

$$5n+9 = 5(n-3) + 6 \cdot 2^2$$

and either n or $n-3$ is not of the form $4^m(16u+10)$. Then either

$$5n \longrightarrow \langle 5, 10, 15 \rangle \quad \text{or} \quad 5(n-3) \longrightarrow \langle 5, 10, 15 \rangle$$

holds and the same thing is also true for $\langle 5, 7, 8, 10 \rangle$. Thus, every integer of the form $5n+9$ with $n \geq 3$ is represented by $\langle 5, 6, 7, 8, 9, 10 \rangle$. One may easily check that $\langle 5, 6, 7, 8, 9, 10 \rangle$ also represents all integers of the form $5n+5$ for $0 \leq n < 3$.

Finally, suppose that $k = 4$. Note that $\langle 1, 2, 5, 6 \rangle$ and $\langle 1, 2, 5, 7 \rangle$ are universal. Since $\langle 4, 8, 20, 24 \rangle$ is a sublattice of $\langle 4, 5, 6, 8 \rangle$ and $\langle 4, 8, 20, 28 \rangle$ is a sublattice of $\langle 4, 5, 7, 8 \rangle$, we have

$$\begin{aligned}
A_{4,4} &\to \langle 4, 8, 20, 24 \rangle \to \langle 4, 5, 6, 8 \rangle \to \langle 4, 5, 6, 7, 8 \rangle, \\
A_{4,6} &\to \langle 4, 8, 20, 28 \rangle \to \langle 4, 5, 7, 8 \rangle \to \langle 4, 5, 6, 7, 8 \rangle, \\
A_{4,7} &\to \langle 4, 8, 20, 24 \rangle \to \langle 4, 5, 6, 8 \rangle \to \langle 4, 5, 6, 7, 8 \rangle.
\end{aligned}$$

On the other hand, One may easily check that $\langle 1, 2, 6 \rangle$ represents all non-negative integers except for integers of the form $4^m(8u+5)$ for some non-negative integers m and u. For an integer n with $n \geq 10$, it is true that

$4n+5 = 4(n-10)+5\cdot 3^2$, and either n or $n-10$ is not of the form $4^m(8u+5)$. Thus, every integer of the form $4n+5$ is represented by $\langle 4,5,6,7,8\rangle$ for $n \geq 10$ and one may easily check that $\langle 4,5,6,7,8\rangle$ also represents all integers of the form $4n+5$ for $0 \leq n \leq 10$. □

Remark 3.1.4. Note that $\langle 3,4,5,6\rangle$ and $\langle 2,3,4\rangle$ do not represent 35 and 10, respectively.

Theorem 3.1.5. *The diagonal $\mathbb{Z}$-lattice $\langle 3,4,5,6,7\rangle$ represents all integers greater than or equal to* 3 *and the diagonal $\mathbb{Z}$-lattice $\langle 2,3,4,5\rangle$ represents all integers greater than or equal to* 2*.*

Proof. First, we will show that $\langle 3,4,5,6,7\rangle$ represents all integers greater than or equal to 3. It is well known that $\langle 2,3,6\rangle$ represents all nonnegative integers except for integers of the form $4^m(8u+7)$ or $3v+1$ with nonnegative integers m, u and v. Note that $\langle 4,6,12\rangle$ is a sublattice of $\langle 3,4,6\rangle$. We observe that

$$\begin{aligned} 2n+1 &= 2(n-2)+5 = 2(n-3)+7 = 2(n-13)+5\cdot 2^2+7,\\ 2n &= 2(n-6)+5+7 = 2(n-10)+5\cdot 2^2 = 2(n-40)+5\cdot 4^2. \end{aligned}$$

For the convenience of discussion, we assume that $n \geq 40$.
(Case 1-1) Suppose that

$$n \not\equiv 1 \pmod 3 \quad \text{and} \quad n \neq 4^m(8u+7).$$

If n is not of the form $4^m(8u+7)+3$, then $n-3 \not\equiv 1 \pmod 3$ and $n-3$ is not of the form $4^m(8u+7)$. Then $\langle 4,6,12\rangle$ represents $2(n-3)$ and so does $\langle 3,4,6\rangle$. Thus, $2n+1$ is represented by $\langle 3,4,5,6,7\rangle$. Assume that n is of the form $4^m(8u+7)+3$. Then either $n-2$ or $n-13$ is not congruent to 1 modulo 3 and is not of the form $4^m(8u+7)$. Hence, either

$$2(n-2) \longrightarrow \langle 4,6,12\rangle \quad \text{or} \quad 2(n-13) \longrightarrow \langle 4,6,12\rangle$$

holds and the same thing is also true for $\langle 3,4,6\rangle$. Thus, every integer of the form $2n+1$ is represented by $\langle 3,4,5,6,7\rangle$ if $n \not\equiv 1 \pmod 3$ and n is not of the form $4^m(8u+7)$.

(Case 1-2) Suppose that

$$n \not\equiv 1 \pmod 3 \quad \text{and} \quad n = 4^{m_0}(8u_0 + 7)$$

for some nonnegative integers m_0 and u_0. If $m_0 > 0$, then $n - 3 \not\equiv 1 \pmod 3$ and $n - 3$ is not of the form $4^m(8u + 7)$. Then $\langle 4, 6, 12\rangle$ represents $2(n - 3)$ and so does $\langle 3, 4, 6\rangle$. Thus, $2n + 1$ is represented by $\langle 3, 4, 5, 6, 7\rangle$. Assume that $m_0 = 0$, that is, $n = 8u_0 + 7$. Then, either $n - 2$ or $n - 13$ is not congruent to 1 modulo 3 and is not of the form $4^m(8u + 7)$. Hence, either

$$2(n - 2) \longrightarrow \langle 4, 6, 12\rangle \quad \text{or} \quad 2(n - 13) \longrightarrow \langle 4, 6, 12\rangle$$

holds and the same thing is also true for $\langle 3, 4, 6\rangle$. Thus, every integer of the form $2n + 1$ is represented by $\langle 3, 4, 5, 6, 7\rangle$ if $n \not\equiv 1 \pmod 3$ and n is not of the form $4^m(8u + 7)$.

(Case 1-3) Suppose that

$$n \equiv 1 \pmod 3.$$

Then $n - 2 \equiv 2 \pmod 3$ and $n - 13 \equiv 0 \pmod 3$. Moreover, either $n - 2$ or $n - 13$ is not of the form $4^m(8u + 7)$. Then, either

$$2(n - 2) \longrightarrow \langle 4, 6, 12\rangle \quad \text{or} \quad 2(n - 13) \longrightarrow \langle 4, 6, 12\rangle$$

holds and the same thing is also true for $\langle 3, 4, 6\rangle$. Thus, every integer of the form $2n + 1$ with $n \equiv 1 \pmod 3$ is represented by $\langle 3, 4, 5, 6, 7\rangle$.

(Case 2-1) Suppose that

$$n \not\equiv 1 \pmod 3 \quad \text{and} \quad n \neq 4^m(8u + 7).$$

Then we have

$$2n \longrightarrow \langle 4, 6, 12\rangle$$

and so $2n$ is represented by $\langle 3, 4, 6\rangle$. Thus, every integer of the form $2n$ is represented by $\langle 3, 4, 5, 6, 7\rangle$ if $n \not\equiv 1 \pmod 3$ and n is not of the form $4^m(8u + 7)$.

(Case 2-2) Suppose that

$$n \not\equiv 1 \pmod 3 \quad \text{and} \quad n = 4^{m_0}(8u_0+7)$$

for some nonnegative integers m_0 and u_0. It is true that $n-6 \not\equiv 1 \pmod 3$ and $n-6$ is not of the form $4^m(8u+7)$. Then we have

$$2(n-6) \longrightarrow \langle 4, 6, 12\rangle$$

and so $2(n-6)$ is represented by $\langle 3,4,6\rangle$. Thus, every integer of the form $2n$ with $n \not\equiv 1 \pmod 3$ is represented by $\langle 3,4,5,6,7\rangle$.
(Case 2-3) Suppose that

$$n \equiv 1 \pmod 3.$$

Then $n-10 \equiv n-40 \equiv 0 \pmod 3$. Moreover, either $n-10$ or $n-40$ is not of the form $4^m(8u+7)$. Then, either

$$2(n-10) \longrightarrow \langle 4,6,12\rangle \quad \text{or} \quad 2(n-40) \longrightarrow \langle 4,6,12\rangle$$

holds and the same thing is also true for $\langle 3,4,6\rangle$. Thus, every integer of the form $2n$ with $n \equiv 1 \pmod 3$ is represented by $\langle 3,4,5,6,7\rangle$.

One may easily check that $\langle 3,4,5,6,7\rangle$ also represents all integers n with $3 \le n < 80$ and therefore, $\langle 3,4,5,6,7\rangle$ represents all integers greater than or equal to 3.

Now, we will show that $\langle 2,3,4,5\rangle$ represents all integers greater than or equal to 2. It is well known that $\langle 1,2,6\rangle$ represents all nonnegative integers except for integers of the form $4^m(8u+5)$ with nonnegative integers m and u. We observe that

$$\begin{aligned} 2n+1 &= 2(n-2)+5 = 2(n-22)+5\cdot 3^2 = 2(n-62)+5\cdot 5^2, \\ 2n &= 2(n-10)+5\cdot 2^2. \end{aligned}$$

(Case 1) It is obvious that $\langle 2,3,4,5\rangle$ represents 3, so we assume that $n \ge 2$. If $n-2$ is not of the form $4^m(8u+5)$, then

$$2(n-2) \longrightarrow \langle 2,4,12\rangle \longrightarrow \langle 2,3,4\rangle$$

and so $2n+1$ is represented by $\langle 2,3,4,5\rangle$.

Suppose that $n-2$ is of the form $4^m(8u+5)$ and $n \geq 62$. Either $n-22$ or $n-62$ is not of the form $4^m(8u+5)$. Then, either

$$2(n-22) \longrightarrow \langle 2,4,12\rangle \quad \text{or} \quad 2(n-62) \longrightarrow \langle 2,4,12\rangle$$

holds and the same thing is also true for $\langle 2,3,4\rangle$. Thus, $2n+1$ is represented by $\langle 2,3,4,5\rangle$ if $n \geq 62$. One may easily check that $\langle 2,3,4,5\rangle$ also represents all odd integers n with $1 < n < 125$.

(Case 2) Suppose that $n \geq 10$. Either n or $n-10$ is not of the form $4^m(8u+5)$. Then, either

$$2n \longrightarrow \langle 2,4,12\rangle \quad \text{or} \quad 2(n-10) \longrightarrow \langle 2,4,12\rangle$$

holds and the same thing is also true for $\langle 2,3,4\rangle$. Thus, $2n$ is represented by $\langle 2,3,4,5\rangle$. One may easily check that $\langle 2,3,4,5\rangle$ also represents all even positive integers less than 20. This completes the proof. □

Theorem 3.1.6. *For any positive integer k, there is a subset S of positive integers such that the cardinality of its minimal universality criterion set is exactly k.*

Proof. Let L be a $\mathbb{Z}$-lattice such that there exist vectors $x_1, \ldots, x_k$ in L satisfying $Q(x_i) = k+i$ for any i with $1 \leq i \leq k$. Consider the sublattice ℓ of L defined by

$$\ell = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_k.$$

Let m be the rank of ℓ and $\mu_1, \mu_2, \ldots, \mu_m$ be successive minima of ℓ. Then we have $m \leq k$ and $\mu_m \leq 2k$. It follows from $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_m$ that

$$d\ell \leq \mu_1\mu_2\cdots\mu_m \leq (2k)^k.$$

Then there are only finitely many candidates for ℓ since the discriminant and the rank of ℓ are bounded. Let $\{\ell_1, \ell_2, \ldots, \ell_t\}$ be the set of all candidates for ℓ and put

$$S = \cup_{i=1}^{t} Q(\ell_i).$$

Then by the definition of S, it is obvious that $\{k+1, k+2, \ldots, 2k\}$ is an S-universality criterion set.

Put $M_1 = \langle k+2 \rangle$. Since $k+1$ is not represented by M_1, by Proposition 3.1.1, there is a $\mathbb{Z}$-lattice N_1 such that $Q(N_1) \cap S = S - \{k+1\}$. Now, put

$$M_i = \langle k+1, \ldots, k+i-1 \rangle$$

for $i = 2, 3, \ldots, k$. One may easily show that $k + j \to M_i$ for any j with $j = 0, 1, \ldots, i-1$ and $k+i$ is not represented by M_i. Then, by Proposition 3.1.1 again, there is a $\mathbb{Z}$-lattice N_i such that $Q(N_i) \cap S = S - \{k+i\}$. This implies that $\{k+1, k+2, \ldots, 2k\}$ is the minimal S-universality criterion set. □

From the above theorem, we directly obtain the following corollary.

Corollary 3.1.7. *For any positive integer N, there is a subset S of positive integers such that the cardinality of a minimal S-universality criterion set is greater that N.*

It seems to be very difficult to determine a minimal S-universality criterion set for an arbitrary subset S of positive integers. In the following, we give some information on the cardinality of a minimal S-universality criterion set for some subset S of positive integers satisfying some special property.

Definition 3.1.8. Let S be a subset of positive integers and let

$$\pi : \mathbb{N} \longrightarrow \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$$

be a natural projection. We say that the set S is 2-*full* if the restriction of π to S is surjective. For example, the set $\{1, 2, 3, 5, 6, 7, 10, 14\}$ is 2-full.

Proposition 3.1.9. *Let S be a 2-full set. Then the cardinality of the minimal criterion set is greater than or equal to 7. Moreover, there exists a 2-full set whose minimal universality criterion set consists of exactly 7 elements.*

Proof. At first, we list $\mathbb{Z}$-lattices that represents all positive integers except for positive integers that are in only one coset of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ in the following table. Therefore, if S is a 2-full set, then the minimal S-universality cri-

$\mathbb{Z}$-lattices	exceptions
$\begin{bmatrix}2&1&0\\1&2&1\\0&1&3\end{bmatrix}$	$2^{2s}(8k+1)$
$\langle 1\rangle \perp \begin{bmatrix}3&1\\1&5\end{bmatrix}$	$2^{2s+1}(8k+1)$
$\langle 1,1,5\rangle$	$2^{2s}(8k+3)$
$\langle 1\rangle \perp \begin{bmatrix}2&1\\1&2\end{bmatrix}$	$2^{2s}(8k+5)$
$\langle 1,2,3\rangle$	$2^{2s+1}(8k+5)$
$\langle 1,1,1\rangle$	$2^{2s}(8k+7)$
$\langle 1,1,2\rangle$	$2^{2s+1}(8k+7)$

Table 3.1: Ternary $\mathbb{Z}$-lattices and their exceptions

terion set must contain positive integers whose projection to $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ are $1, 2, 3, 5, 7, 10, 14$.

Now, we prove that there exists a 2-full set whose minimal criterion set consists of exactly 7 elements. To prove this, we will construct a 2-full set whose minimal criterion set is

$$\{1, 2, 3, 5, 7, 10, 14\}.$$

Let L be a $\mathbb{Z}$-lattice that represents $1, 2, 3, 5, 7, 10$ and 14. Since L represents 1, we have $L \simeq \langle 1\rangle \perp L_0$. Since L represents 2, either $L \simeq \langle 1, 1\rangle \perp L_1$ or $2 \to L_0$ holds. First, consider the case when $L \simeq \langle 1, 1\rangle \perp L_1$. Since 3 is not represented by $\langle 1, 1\rangle$, we have $\min(L_1) \le 3$. Then L represents at least one of the following $\mathbb{Z}$-lattices:

$$L(0) = \langle 1, 1, 3\rangle, \qquad L(1) = \langle 1, 1, 1\rangle, \qquad L(2) = \langle 1, 1, 2\rangle.$$

Next, consider the case when $2 \to L_0$. Since 5 is not represented by $\langle 1,2\rangle$, we have $\mu_2(L_0) \le 5$. Then L represent at least one of the following $\mathbb{Z}$-lattices:

$$\begin{aligned}
&L(3) = \langle 1,2,2\rangle, && L(4) = \langle 1,2,3\rangle,\\
&L(5) = \langle 1,2,4\rangle, && L(6) = \langle 1,2,5\rangle,\\
&L(7) = \langle 1\rangle \perp \begin{bmatrix} 2 & 1\\ 1 & 2\end{bmatrix}, && L(8) = \langle 1\rangle \perp \begin{bmatrix} 2 & 1\\ 1 & 3\end{bmatrix},\\
&L(9) = \langle 1\rangle \perp \begin{bmatrix} 2 & 1\\ 1 & 4\end{bmatrix}, && L(10) = \langle 1\rangle \perp \begin{bmatrix} 2 & 1\\ 1 & 5\end{bmatrix}.
\end{aligned}$$

We define the truant of a $\mathbb{Z}$-lattice ℓ to be the smallest positive integer not represented by ℓ, and denote it by $t(L)$. Then, the truant of $L(i)$ for each i with $0 \le i \le 10$ is as follows:

$$\begin{aligned}
&t(L(0)) = 6 && t(L(1)) = 7, && t(L(2)) = 14, && t(L(3)) = 7\\
&t(L(4)) = 10, && t(L(5)) = 14, && t(L(6)) = 10, && t(L(7)) = 5,\\
&t(L(8)) = 5, && t(L(9)) = 7, && t(L(10)) = 7.
\end{aligned}$$

Suppose that $L(1) = \langle 1,1,1\rangle \to L$. To represent all elements of 1,2,3,5,7, 10 and 14, we have $\mu_4(L) \le t(L(1)) = 7$. Then one can find the set $\mathscr{C}(1)$ of quaternary $\mathbb{Z}$-lattices consisting of $\mathbb{Z}$-lattices that represent $L(1)$, and whose 4-th minimum is less than or equal to 7. By the same argument, for each i with $2 \le i \le 10$, one can also find the set $\mathscr{C}(i)$ of quaternary $\mathbb{Z}$-lattices consisting of $\mathbb{Z}$-lattices that represent $L(i)$ and whose 4-th minimum is less than or equal to $t(L(i))$. Finally, one may also find the set $\mathscr{C}(0)$ of quaternary $\mathbb{Z}$-lattices consisting of $\mathbb{Z}$-lattices that represent $L(0)$, and whose 4th minimum is less than or equal to 7.

Put $\mathscr{C} = \cup_{0\le i\le 10}\mathscr{C}(i)$ and let D be the product of all odd primes that divide the discriminant of a $\mathbb{Z}$-lattice in $\mathscr{C}$. Then by the Dirichlet's theorem on arithmetic progression, one can find a prime p such that

$$p \equiv 3 \pmod 8, \quad \text{and} \quad 2p \equiv 1 \pmod D.$$

Note that any positive integer which is not represented by $L(0)$ is of the form $3^{2k+1}(3s+2)$ for some nonnegative integers k and s. For any prime q with $q|D$, we have $2p \equiv 1 \pmod q$, and so $2p$ is primitively represented by ℓ_q

for any $\ell \in \mathscr{C}$. For any prime q with $q \nmid 2D$, every $\ell \in \mathscr{C}$ is a unimodular quaternary $\mathbb{Z}$-lattice over $\mathbb{Z}_q$, and so $2p$ is represented by ℓ_q. If $q = 2$, one may easily check that 6 is primitively represented by $L(i)$ for any i with $1 \le i \le 10$ and 22 is primitively represented by $L(0)$. Thus, $2p$ is primitively represented by ℓ_2 for any $\ell \in \mathscr{C}$. Thus, $2p_0$ is locally represented by ℓ and is primitively represented by ℓ at the anisotropic primes for any $\ell \in \mathscr{C}$. Hence there exists an integer $2p_0$ such that

$$p_0 \equiv 3 \pmod 8, \text{ and } 2p_0 \equiv 1 \pmod D,$$

and $2p_0$ is represented by ℓ for any $\ell \in \mathscr{C}$. We put

$$S = \{1, 2, 3, 5, 7, 10, 14, 2p_0\}.$$

Then from the construction of S, it is a 2-full set whose minimal universality criterion set is exactly $\{1, 2, 3, 5, 7, 10, 14\}$. By applying same argument in the proof of Theorem 3.1.6, one may also find infinitely many 2-full sets whose minimal universality criterion set is $\{1, 2, 3, 5, 7, 10, 14\}$. □

3.2 Higher rank cases

Recall that Φ_n is the set of all quadratic forms of rank n. In this section, we show that there are infinitely many minimal Φ_n-universality criterion sets for any $n \ge 9$.

Proposition 3.2.1. *For any $n \ge 9$, there are infinitely many minimal Φ_n-universality criterion sets.*

Proof. Let $S_n^0 = \{L_1, L_2, \dots, L_s\}$ be a minimal Φ_n-universality criterion set. Assume that $L_i = I_{k_i} \perp \ell_i$, where $\min(\ell_i) \ge 2$. If $n_0 = \max\{k_i\} < n$, then $I_{n_0} \perp \ell_1 \perp \cdots \perp \ell_s$ represents all $\mathbb{Z}$-lattices in S_n^0, but it does not represent I_n. This is a contradiction. Therefore $n_0 = n$, that is, $I_n \in S_n^0$. Similarly, one may easily show that there is an integer j such that L_j represents $D_m[1]$ for some integer $m \equiv 0 \pmod 4$ with $n-4 \le m < n$. Note that $L_j = D_m[1] \perp M$ for some $\mathbb{Z}$-lattice M with rank less than or equal to 4. Without loss of generality, assume that $L_1 = I_n$ and $L_2 = D_m[1] \perp M$. Since any $\mathbb{Z}$-lattice that represents both L_1 and L_2 should represent $I_n \perp D_m[1]$. Furthermore, since I_n is 4-universal, L_j cannot represent $D_m[1]$ for any $j \geq 3$. Now we show that for any $\mathbb{Z}$-lattice N with rank $n-m$,

$$S_n^0(N) = \{I_n, D_m[1] \perp N, L_3, \ldots, L_s\}$$

is also a minimal Φ_n-universality criterion set. Assume that a $\mathbb{Z}$-lattice $\mathcal{L}$ represents all $\mathbb{Z}$-lattices in $S_n^0(N)$. Since $I_n \perp D_m[1]$ is represented by $\mathcal{L}$, $L_2 = D_m[1] \perp M$ is also represented by $\mathcal{L}$. Therefore, $\mathcal{L}$ is n-universal from the assumption that S_n^0 is a minimal Φ_n-universality criterion set. By using similar argument, one may easily show that $S_n^0(N)$ is, in fact, minimal. □

Remark 3.2.2. Summing up all, the minimal Φ_n-universality criterion set is unique for any $n = 1, 2$ and 8, and there are infinitely many minimal Φ_n-universality criterion sets for any $n \geq 9$. However, when $n = 3, 4, 5, 6$, and 7 nothing is known at present. We conjecture that a minimal Φ_4-universality criterion set is unique.

Chapter 4

Recoverable $\mathbb{Z}$-lattices

In this chapter, we introduce the notion on recoverable $\mathbb{Z}$-lattices and give some properties on those $\mathbb{Z}$-lattices, and we show some necessary conditions and some sufficient conditions for $\mathbb{Z}$-lattices to be recoverable.

4.1 Some properties of recoverable $\mathbb{Z}$-lattices

In [8], Elkies and his collaborators gave an example of a set S of ternary $\mathbb{Z}$-lattices such that the sizes of minimal S-universality criterion sets vary. To explain their example more precisely, let S be the set of all ternary sublattices of $\langle 1,1,2\rangle$. Then, clearly, $S_0=\{\langle 1,1,2\rangle\}$ is a minimal S-universality criterion set. Furthermore, they proved that

$$S_1=\{\langle 1,1,16\rangle,\langle 2,2,2\rangle\}$$

is also a minimal S-universality criterion set. The point is that any $\mathbb{Z}$-lattice that represents both $\langle 1,1,16\rangle$ and $\langle 2,2,2\rangle$, which are all sublattices of $\langle 1,1,2\rangle$, also represents $\langle 1,1,2\rangle$ itself. From this point of view, the following definition seems to be quite natural:

Definition 4.1.1. Let ℓ be a $\mathbb{Z}$-lattice and let $S_0=\{\ell_1,\ell_2,\dots,\ell_t\}$ be a set of proper sublattices of ℓ. We say ℓ is *recoverable by* S_0 if every S_0-universal $\mathbb{Z}$-lattice represents ℓ itself.

From the above, the ternary $\mathbb{Z}$-lattice $\langle 1,1,2\rangle$ is recoverable by S_1. We simply say ℓ is *recoverable* if there is a finite set of proper sublattices satisfying the above property. Note that if ℓ is recoverable, then there is a minimal S-universality criterion set whose cardinality is greater than 1, where S is the set of all sublattices of ℓ.

Lemma 4.1.2. *A $\mathbb{Z}$-lattice ℓ is not recoverable if and only if there is a $\mathbb{Z}$-lattice L that represents all proper sublattices of ℓ, but not ℓ itself.*

Proof. First, suppose that ℓ is not recoverable. Let S be the set of all proper sublattices of L and let $S_0 = \{\ell_1, \ell_2, \dots, \ell_t\}$ be a minimal S-universality criterion set. Since ℓ is not recoverable from the assumption, there is a $\mathbb{Z}$-lattice ℓ that represents all $\mathbb{Z}$-lattices in S_0, whereas it does not represent ℓ itself. Note that L represents all proper sublattices of ℓ. The converse is trivial. □

Lemma 4.1.3. *Let a be a positive integer. For any $\mathbb{Z}$-lattice ℓ, if ℓ^a is recoverable, then so is ℓ.*

Proof. Assume that ℓ^a is recoverable by $\{\ell_1^a, \ell_2^a, \dots, \ell_t^a\}$, where ℓ_i is a proper sublattice of ℓ for any $i = 1, 2, \dots, t$. Assume that a $\mathbb{Z}$-lattice M represents ℓ_i for any i. Then $\ell_i^a \to M^a$ for any i, and hence $\ell^a \to M^a$. Therefore, $\ell \to M$ and ℓ is recoverable by $\{\ell_1, \ell_2, \dots, \ell_t\}$. □

Remark 4.1.4. Any unary $\mathbb{Z}$-lattice ℓ cannot be recoverable. Let $\ell = \langle 1\rangle$. Note that $\langle 2,2,5\rangle$ represents all squares of integers except for 1 (see [9]). Then $\langle 2,2,5\rangle$ represents all proper sublattices of ℓ, but not ℓ itself. Therefore ℓ is not recoverable by Lemma 4.1.2. Moreover, since every unary $\mathbb{Z}$-lattice is obtained by scaling ℓ, it is not recoverable by Lemma 4.1.3.

Remark 4.1.5. Note that the converse of the above lemma does not hold in general. Let $\ell = \langle 1,4\rangle$. Let L be any $\mathbb{Z}$-lattice representing both $\ell_1 = \langle 1,16\rangle$ and $\ell_2 = \langle 4,4\rangle$. Since L represents ℓ_1, we may assume that $L = \mathbb{Z}e_1 + L_1$, where $Q(e_1) = 1$ and $B(e_1, L_1) = 0$. Furthermore, since L represents $\ell_2 = \langle 4,4\rangle$, there are nonnegative integers a, b and vectors $x, y \in L_1$ such that

$$Q(ae_1 + x) = a^2 + Q(x) = Q(be_1 + y) = 4 \text{ and } B(ae_1 + x, be_1 + y) = 0.$$

If $a=2$, then $x=0$ and $b=0$. Hence $\langle 4\rangle \to L_1$. If $a=1$, then

$$b=0 \text{ and } Q(y)=4 \quad \text{or} \quad b=1,\ Q(x)=Q(y)=3, \text{ and } B(x,y)=-1.$$

For the latter case, $Q(x+y)=4$. If $a=0$, then $Q(x)=4$. Therefore L_1 represents 4 in any case, which implies that L represents ℓ. Hence ℓ is recoverable by $\{\ell_1,\ell_2\}$.

Now, we show that $\ell^2=\langle 2,8\rangle$ is not recoverable. To show this, let S be the set of all binary $\mathbb{Z}$-lattices with minimum greater than or equal to 9, and let $S_0=\{m_1,\dots,m_t\}$ be a finite minimal S-universality criterion set. Then $m_1\perp\cdots\perp m_t$ represents all binary $\mathbb{Z}$-lattices with minimum greater than or equal to 9. Now define

$$L=K\perp m_1\perp\cdots\perp m_t$$

where

$$K=\begin{bmatrix}2&1&1&0\\1&8&0&0\\1&0&8&4\\0&0&4&10\end{bmatrix}.$$

Clearly, $\ell^2=\langle 2,8\rangle$ is not represented by L. Let ℓ_1 be any proper sublattice of ℓ^2. If $\min(\ell_1)\ge 9$, then ℓ_1 is represented by $m_1\perp\cdots\perp m_t$. Hence we may assume that $\min(\ell_1)=2$ or 8. For the former case, $\ell_1\simeq\langle 2,8m^2\rangle$, where $m\ge 2$. Since $\langle 8m^2\rangle\to m_1\perp\cdots\perp m_t$, ℓ_1 is represented by L. For the latter case, one may easily show that

$$\ell_1\simeq\langle 8,8m^2\rangle \quad \text{or} \quad \ell_1\simeq\begin{bmatrix}8&4\\4&2+8n^2\end{bmatrix} \quad \text{for some } m,n\ge 1.$$

Note that K represents each binary $\mathbb{Z}$-lattices for $m=1$ or $n=1$, and for $m\ge 2$ or $n\ge 2$, one may use the fact that any integer greater than 9 is represented by $m_1\perp\cdots\perp m_t$ to show that ℓ_1 is represented by L. Therefore L represents all proper sublattices of ℓ^2, but not ℓ^2 itself. Consequently, ℓ is not recoverable.

One may easily check that every additively indecomposable $\mathbb{Z}$-lattice is not recoverable. We further prove that every indecomposable $\mathbb{Z}$-lattice L is not recoverable if the rank of L is less than 4.

Proposition 4.1.6. *Any indecomposable binary $\mathbb{Z}$-lattice is not recoverable.*

Proof. Suppose that ℓ is indecomposable and $\{x, y\}$ is a Minkowski-reduced basis for ℓ. Let S be the set of all proper sublattices of ℓ and let $S_0 = \{\ell_1, \ell_2, \ldots, \ell_t\}$ be a minimal S-universality criterion set. Now, we put $\ell_i = \mathbb{Z}x_i + \mathbb{Z}y_i$ where $\{x_i, y_i\}$ is a Minkowski-reduced basis for ℓ_i for $i = 1, 2, \ldots, t$. Then we define

$$L = (\mathbb{Z}x_1 + \mathbb{Z}y_1) \perp (\mathbb{Z}x_2 + \mathbb{Z}y_2) \perp \cdots \perp (\mathbb{Z}x_t + \mathbb{Z}y_t).$$

Since S_0 is an S-universality criterion set and L represents ℓ_i for any i with $1 \leq i \leq t$, L represents all proper sublattices of ℓ.

Now, suppose on the contrary that ℓ is represented by L and $\phi : \ell \to L$ is a representation. Since ℓ_i is a sublattice of ℓ for $i = 1, 2, \ldots, t$, without loss of generalitiy, we may assume that $\phi(x) = x_1$. Then we put $\phi(y) = \alpha x_1 + \beta y_1 + z$ where $\alpha, \beta \in \mathbb{Z}$ and $z \in (\mathbb{Z}x_2 + \mathbb{Z}y_2) \perp \cdots \perp (\mathbb{Z}x_t + \mathbb{Z}y_t)$. Since ℓ is indecomposable, β cannot be zero. Then

$$d\ell = d\phi(\ell) = d(\mathbb{Z}x_1 + \mathbb{Z}(\alpha x_1 + \beta y_1 + z)) \geq d(\mathbb{Z}x_1 + \mathbb{Z}(\alpha x_1 + \beta y_1)) \geq d\ell_1 > d\ell$$

holds, which is a contradiction. Therefore, L does not represent ℓ and then, by lemma 4.1.2, ℓ is not recoverable. □

Proposition 4.1.7. *Let L be an indecomposable ternary $\mathbb{Z}$-lattice. Then there are no proper sublattices $L_1, L_2, \ldots, L_t$ of L such that L is represented by $L_1 \perp L_2 \perp \cdots \perp L_t$.*

Proof. Suppose that the assertion is false. Then there are sublattices $L_1, L_2, \ldots, L_t$ of L such that L is represented by $L_1 \perp L_2 \perp \cdots \perp L_t$. We may assume that all L_i's are of rank 3 and let

$$\phi : L \rightarrow L_1 \perp L_2 \perp \cdots \perp L_t$$

be a representation. Let $\{u, v, w\}$ be a Minkowski reduced basis for L and put $\phi(u) = x_1$. Clearly, there exists a Minkowski reduced basis for L_1 consisting of x_1. Let $\{x_1, x_2, x_3\}$ be such a Minkowski reduced basis for L_1, and assume that

$$\phi(v) = a_1x_1 + x + y,$$

where $x \in \mathbb{Z}x_2 + \mathbb{Z}x_3$ and $y \in L_2 \perp \cdots \perp L_t$.

First, assume that $x = 0$. Since

$$2|a_1|Q(x_1) = 2|B(x_1, a_1x_1 + y)| \leq Q(x_1),$$

we have $a_1 = 0$. Put

$$\phi(w) = b_1x_1 + b_2x_2 + b_3x_3 + z$$

where $z \in L_2 \perp \cdots \perp L_t$, then $\phi(L) = \mathbb{Z}x_1 + \mathbb{Z}y + \mathbb{Z}(b_1x_1 + b_2x_2 + b_3x_3 + z)$. If $b_3 \neq 0$, then

$$\begin{aligned} \mu_3(L) = Q(b_1x_1 + b_2x_2 + b_3x_3 + z) &= Q(b_1x_1 + b_2x_2 + b_3x_3) + Q(z) \\ &\geq \mu_3(L_1) + Q(z) \geq \mu_3(L) + Q(z), \end{aligned}$$

which implies that $z = 0$. Therefore, $\phi(L)$ is decomposable, which is a contradiction. Hence we have $b_3 = 0$.

Observe that

$$L_1 = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3 \subseteq L = \mathbb{Z}u + \mathbb{Z}v + \mathbb{Z}w \simeq \phi(L) = \begin{bmatrix} a & 0 & e \\ 0 & b & d \\ e & d & c \end{bmatrix}.$$

Then $b_1x_1 + b_2x_2 = \alpha u + \beta v + \gamma w$ for some integers α, β and γ. If $\gamma \neq 0$, then

$$\mu_3(L) = Q(b_1x_1 + b_2x_2) + Q(z) \geq Q(w) + Q(z) = \mu_3(L) + Q(z).$$

Therefore, $z = 0$, which is a contradiction. Hence $b_1x_1 + b_2x_2 = \alpha u + \beta v$.

On the other hand, one may similarly show that $x_1 = \alpha_1 u + \beta_1 v$. Since the fact that $Q(x_1) = Q(u)$ and $B(u, v) = 0$, we have $x_1 = \pm u$, $b_1x_1 + b_2x_2 = \beta v$ or $x_1 = \pm v$, $b_1x_1 + b_2x_2 = \alpha u$. In any case, $\phi(L)$ is decomposable, which is a contradiction.

Now, assume that $x \neq 0$. Since

$$\begin{aligned}\mu_2(L) = Q(v) = Q(a_1x_1 + x + y) &= Q(a_1x_1 + x) + Q(y)\\ &\geq \mu_2(L_1) + Q(y) \geq \mu_2(L) + Q(y),\end{aligned}$$

we have $y = 0$. Put

$$\phi(v) = a_1x_1 + a_2x_2 + a_3x_3 \quad \text{and} \quad \phi(w) = b_1x_1 + b_2x_2 + b_3x_3 + z$$

where $a_1, a_2, a_3, b_1, b_2, b_3$ are integers and $z \in L_2 \perp \cdots \perp L_t$. If $b_3 \neq 0$, then

$$\mu_3(L) = Q(b_1x_1 + b_2x_2 + b_3x_3) + Q(z) \geq \mu_3(L_1) + Q(z) \geq \mu_3(L) + Q(z)$$

and so $z = 0$. Then $\phi(L) \subseteq L_1$, which is a contradiction. Thus, $b_3 = 0$. Suppose that $a_3 \neq 0$. Since

$$\mu_2(L) = Q(a_1x_1 + a_2x_2 + a_3x_3) \geq \mu_3(L_1) \geq \mu_3(L),$$

we have $\mu_2(L) = \mu_3(L) = \mu_2(L_1) = \mu_3(L_1)$. Then

$$\mu_2(L) = \mu_3(L) = Q(b_1x_1 + b_2x_2 + z) \geq \mu_2(L_1) + Q(z) = \mu_2(L) + Q(z)$$

and so $z = 0$, which is a contradiction. Therefore $a_3 = 0$.

Since $a_2 \neq 0$, we have

$$\mu_2(L) = Q(a_1x_1 + a_2x_2) \geq \mu_2(L_1) = Q(x_2) \geq \mu_2(L)$$

and this in turn means that $\mu_2(L) = Q(a_1x_1 + a_2x_2) = \mu_2(L_1) = Q(x_2)$. Let $\mathbb{Z}x_1 + \mathbb{Z}x_2 = \begin{bmatrix} s & r \\ r & t \end{bmatrix}$. For $Q(x_2) = Q(a_1x_1 + a_2x_2)$, we have

$$t = a_1^2 s + 2a_1a_2r + a_2^2 t = s\left(a_1 + \frac{ra_2}{s}\right)^2 + \left(t - \frac{r^2}{s}\right)a_2^2 \geq a_2^2\left(t - \frac{s}{4}\right).$$

If $|a_2| \geq 2$, then $t \geq 4t - 3s > t$, which is a contradiction. If $a_2 = \pm 1$, then $\phi(L) = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}y$ is decomposable, which is a contradiction. This completes the proof. □

From the above proposition, we immediately obtain the following corollary.

Corollary 4.1.8. *An indecomposable ternary $\mathbb{Z}$-lattice is not recoverable.*

4.2 Recoverable binary $\mathbb{Z}$-lattices

In this section, we focus on recoverable binary $\mathbb{Z}$-lattices. We find some necessary conditions and some sufficient conditions for binary $\mathbb{Z}$-lattices to be recoverable.

Let n be a positive integer and let S be the set of all binary $\mathbb{Z}$-lattices with minimum greater than or equal to n. Then there is a finite minimal S-universality criterion set $S_n = \{m_1, \dots, m_t\}$ by [11]. Put $M = m_1 \perp \cdots \perp m_t$. Then M represents all binary $\mathbb{Z}$-lattices with minimum greater than or equal to n. In this section, $\mathcal{M}(n)$ stands for a $\mathbb{Z}$-lattice representing all binary $\mathbb{Z}$-lattices with minimum greater than or equal to n with $\min(\mathcal{M}(n)) = n$. From the above argument, such a $\mathbb{Z}$-lattice always exists.

Proposition 4.2.1. *For any two integers a and b such that $2 \le a < b$ and a does not divide b, the diagonal $\mathbb{Z}$-lattice $\ell = \langle a, b\rangle$ is not recoverable.*

Proof. Since a does not divide b, there exists the unique positive integer h such that $h^2a < b < (h+1)^2a$. For any integer h with $h \ge 2$, we define a $\mathbb{Z}$-lattice $K(h)$ by

$$K(h) = \mathop{\perp}_{\substack{i,j:2\le i\le h\\ 1\le j\le[\frac{i}{2}]}} \begin{bmatrix} i^2a & ija \\ ija & j^2a+b \end{bmatrix}.$$

Then we put

$$L(h) = \begin{cases} (\mathbb{Z}x+\mathbb{Z}y) \perp \mathcal{M}(b+1) & \text{if } h = 1, \\ (\mathbb{Z}x+\mathbb{Z}y) \perp K(h) \perp \mathcal{M}(b+1) & \text{if } h \ge 2, \end{cases} \quad \text{where } \mathbb{Z}x+\mathbb{Z}y = \begin{bmatrix} a & 1 \\ 1 & b \end{bmatrix}.$$

We claim that $L(h)$ represents all proper sublattices of ℓ, whereas $L(h)$ does not represent ℓ itself.

First, we will prove that $L(h)$ represents all proper sublattices of ℓ. Let ℓ' be a proper sublattice of ℓ.

(Case 1) If $\min(\ell') > b$, then $\mathcal{M}(b+1)$ represents ℓ' and so does $L(h)$.
(Case 2) If $\min(\ell') = b$, then $\ell' \simeq \langle b, \alpha^2 a\rangle$ for some integer α with $\alpha^2 a > b$. Since $\alpha^2 a$ is represented by $\mathcal{M}(b+1)$, $L(h)$ represents ℓ'.
(Case 3) Assume that $a < \min(\ell') < b$. In this case, we have $h \geq 2$. Note that

$$\ell' \simeq \begin{bmatrix} i^2a & ija \\ ija & j^2a+\beta^2 b \end{bmatrix}$$

for some integers i, j and β with $2 \leq i \leq h$, $0 \leq j \leq \left[\frac{i}{2}\right]$, $\beta \geq 1$. If $\beta = 1$, then clearly $\ell \to K(h) \to L(h)$. Assume that $\beta \geq 2$. Since $(\beta^2-1)b > b$, we have

$$\ell' \simeq \begin{bmatrix} i^2a & ija \\ ija & j^2a+\beta^2 b \end{bmatrix} \to \begin{bmatrix} i^2a & ija \\ ija & j^2a+b \end{bmatrix} \perp \mathcal{M}(b+1),$$

which implies that $L(h)$ represents ℓ'.
(Case 4) If $\min(\ell') = a$, then $\ell' \simeq \langle a, \beta^2 b\rangle$ for some integer β with $\beta \geq 2$. Since $\beta^2 b$ is represented by $\mathcal{M}(b+1)$, $L(h)$ represents ℓ'.

Next, we will show that $L(h)$ does not represent ℓ. When $h = 1$, it is clear that $L(1)$ does not represent ℓ. Assume $h \geq 2$. Let

$$K_{ij} = \mathbb{Z}k_1 + \mathbb{Z}k_2 = \begin{bmatrix} i^2a & ija \\ ija & j^2a+b \end{bmatrix}$$

for some $2 \leq i \leq h$ and $1 \leq j \leq \left[\frac{i}{2}\right]$. Then $Q(sk_1+tk_2) = (si+tj)^2a + t^2b$ for any integers s and t. Since $\min(K_{ij}) = i^2a > a$, K_{ij} does not represent a. If $b = Q(sk_1+tk_2) = (si+tj)^2a+t^2b$, then $t^2 = 1$ and $si+tj = 0$. Furthermore, since $j = |si| \leq \left[\frac{i}{2}\right]$, we have $s = j = 0$. This is a contradiction. Therefore K_{ij} does not represent b. Since a does not divide b, from the above fact, we have

$$Q(K(h)) \subseteq \{ua + vb \mid u, v \in \mathbb{N} \cup \{0\}\} - \{a, b\}.$$

Suppose that $L(h)$ represents ℓ. Let $u \in L$ be a vector with $Q(u) = b$. Since $u \in L$, u can be written as $\alpha x + \beta y + z + w$ for some integers α, β and a vector $z \in K(h)$, $w \in \mathcal{M}(b+1)$. Since $Q(u) = Q(\alpha x + \beta y) + Q(z) + Q(w)$ and $Q(w) > b$, we have $w = 0$. One may easily show that $z = 0$ or $Q(z) = \delta a$ for some integer δ with $\delta \geq 2$. If $|\beta| \geq 2$, then $Q(\alpha x + \beta y) \geq \beta^2(b-1) > b$. If $\beta = 0$, then $Q(\alpha x)$ is a multiple of a, and so is $Q(u)$. On the other hand, if $|\beta| = 1$, then $Q(\alpha x + \beta y) > b$ unless $\alpha = 0$. Hence, we have $u = y$ or $u = -y$. Similarly one may show that if $v \in L$ with $Q(v) = a$, then $v = x$ or $v = -x$. However, we have $B(\pm x, \pm y) \neq 0$. This is a contradiction. □

Lemma 4.2.2. *For any odd positive integer m, $\langle 1, m\rangle$ is not recoverable.*

Proof. For $k = 1$ or 3, $\langle 1, k\rangle$ is not recoverable since $\langle 1\rangle \perp \mathcal{M}(k{+}1)$ represents all proper sublattices of $\langle 1, k\rangle$, but not $\langle 1, k\rangle$ itself. Now, we may assume that $m \geq 5$. Let N be any even 2-universal quinary even $\mathbb{Z}$-lattice. Note that such a $\mathbb{Z}$-lattice exists, for example, D_5 is one of such quinary lattices. Define a $\mathbb{Z}$-lattice

$$L = \langle 1\rangle \perp N \perp \mathcal{M}(m + 1).$$

It is obvious that $\langle 1, m\rangle$ is not represented by L.

Let ℓ be a proper sublattice of $\langle 1, m\rangle$. Firstly, suppose that $\min(\ell) = 1$. Then $\ell \simeq \langle 1, m\beta^2\rangle$ with an integer $\beta \geq 2$. Since $\langle m\beta^2\rangle \to \mathcal{M}(m + 1)$, we have $\ell \to L$.

Secondly, suppose that $\min(\ell) > 1$. From the fact that $m \geq 5$, we have $\min(\ell) \geq 4$. Choose a Minkowski reduced basis for ℓ so that

$$\ell \simeq \begin{bmatrix} a & b \\ b & c \end{bmatrix} \text{ with } 0 \leq 2b \leq a \leq c.$$

(Case 1) If $a \equiv c \equiv 0 \pmod 2$, then $\ell \to N$ and so $\ell \to L$.
(Case 2) We consider the case when $a \equiv c \equiv 1 \pmod 2$. Put

$$\ell' = \begin{bmatrix} a-1 & b-1 \\ b-1 & c-1 \end{bmatrix}.$$

Since $d\ell' \geq \frac{3c}{4}(a - 4) > 0$, ℓ' is positive definite. Then $\ell' \to N$ and so $\ell \to L$.
(Case 3) Suppose that $a \equiv 1 \pmod 2$ and $c \equiv 0 \pmod 2$. Put

$$\ell' = \begin{bmatrix} a-1 & b \\ b & c \end{bmatrix}.$$

Since $d\ell' = \left(\frac{ac}{4} - b^2\right) + \frac{c}{4}(3a - 4) > 0$, ℓ' is positive definite. Then $\ell' \to N$. Therefore, $\langle 1\rangle \perp N$ represents ℓ and so does L.

(Case 4) When $a \equiv 0 \pmod 2$ and $c \equiv 1 \pmod 2$, one may show that $\ell \to L$ by the similar way in (Case 3). □

Lemma 4.2.3. *For any positive integer m with $m \equiv 2 \pmod 4$, the binary $\mathbb{Z}$-lattice $\langle 1, m\rangle$ is not recoverable.*

Proof. Since $\langle 1\rangle \perp \mathcal{M}(3)$ represents all proper sublattices of $\langle 1, 2\rangle$ but not $\langle 1, 2\rangle$ itself, the binary $\mathbb{Z}$-lattice $\langle 1, 2\rangle$ is not recoverable.

Let $m = 6$ and put

$$L = \langle 1\rangle \perp \begin{bmatrix} 4 & 0 & 2 \\ 0 & 5 & 1 \\ 2 & 1 & 7 \end{bmatrix} \perp \mathcal{M}(7).$$

Then one may easily show that L represents all proper sublattices of $\langle 1, 6\rangle$, but not $\langle 1, 6\rangle$ itself.

We may assume that $m \geq 10$. Put

$$L' = \mathbb{Z}e + \mathbb{Z}x + \mathbb{Z}y + \mathbb{Z}z = \langle 1, 3, 5, m-1\rangle.$$

Let N be an even 2-universal quinary even $\mathbb{Z}$-lattice and let $\mathcal{N}$ be the $\mathbb{Z}$-lattice obtained from N by scaling $\mathbb{Q} \otimes N$ by 2. Now, define

$$L = L' \perp \mathcal{N} \perp \mathcal{M}(m+1).$$

We show that any proper sublattice of $\langle 1, m\rangle$ is represented by L, whereas $\langle 1, m\rangle$ itself is not represented by L. Suppose, on the contrary, that $\langle 1, m\rangle \to L$. Then one may easily show that

$$\langle m\rangle \longrightarrow \langle 3, 5\rangle \perp \mathcal{N}.$$

Thus, $m \equiv 3\alpha^2 + 5\beta^2 \pmod 4$ for some integers α and β. Since $m \equiv 2 \pmod 4$, this is a contradiction.

Let $\mathbb{Z}u + \mathbb{Z}v = \langle 1, m\rangle$, and let ℓ be a proper sublattice of $\langle 1, m\rangle$. Then there are integers a, b, and c such that $\ell = \mathbb{Z}(au) + \mathbb{Z}(bu + cv)$. Suppose that $|c| \geq 2$. Since $\ell \subseteq \mathbb{Z}u + \mathbb{Z}(cv)$ and $\mathbb{Z}u + \mathbb{Z}(cv) = \langle 1, c^2m\rangle \to L$, we have $\ell \to L$. Thus, we may assume that $\ell = \mathbb{Z}(au) + \mathbb{Z}(bu + v)$ for some integers

a and b with $0 \le b < a$ and $a \ge 2$. In this case, we have

$$\ell = \begin{bmatrix} a^2 & ab \\ ab & m+b^2 \end{bmatrix}.$$

First, we consider the case when $a \equiv b \equiv 0 \pmod 2$. Since $\begin{bmatrix} a^2 & ab \\ ab & m+b^2-6 \end{bmatrix}$ is represented by $\mathcal{N}$, $\begin{bmatrix} a^2 & ab \\ ab & m+b^2 \end{bmatrix}$ is represented by $\langle 1,5\rangle \perp \mathcal{N}$. Thus, L represents ℓ.

Next, we consider the case when $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$. Since $\begin{bmatrix} a^2 & ab \\ ab & m+b^2-3 \end{bmatrix}$ is represented by $\mathcal{N}$, $\begin{bmatrix} a^2 & ab \\ ab & m+b^2 \end{bmatrix}$ is represented by $\langle 3\rangle \perp \mathcal{N}$. Thus, L represents ℓ.

Third, we consider the case when $a \equiv b \equiv 1 \pmod 2$. Since there is a vector $w \in \mathcal{N}$ with $Q(w) = m-2$,

$$\mathbb{Z}(e+x+y) + \mathbb{Z}(x+w) = \begin{bmatrix} 9 & 3 \\ 3 & m+1 \end{bmatrix}$$

is represented by L. Hence we may assume $a \ge 4$. Consider the $\mathbb{Z}$-lattice $\ell' = \begin{bmatrix} a^2-9 & ab-3 \\ ab-3 & m+b^2-3 \end{bmatrix}$. Since $s(\ell') \subseteq 4\mathbb{Z}$ and $d\ell' > 0$, ℓ' is represented by $\mathcal{N}$. Choose vectors $w_1, w_2 \in \mathcal{N}$ such that

$$\ell' \simeq \begin{bmatrix} a^2-9 & ab-3 \\ ab-3 & m+b^2-3 \end{bmatrix} = \mathbb{Z}w_1 + \mathbb{Z}w_2 \subseteq \mathcal{N}.$$

Since $\mathbb{Z}(e+x+y+w_1) + \mathbb{Z}(x+w_2) = \begin{bmatrix} a^2 & ab \\ ab & m+b^2 \end{bmatrix}$, ℓ is represented by L.

Finally, we consider the case when $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$. First, assume that $a = 3$. Then $b = 0$ or 2. If $b = 0$, then

$$\ell = \langle 9, m\rangle \longrightarrow \langle 1,5,m-1\rangle \perp \mathcal{N} {\rightarrow} L.$$

If $b = 2$, then $\ell = \begin{bmatrix} 9 & 6 \\ 6 & m+4 \end{bmatrix} \simeq \begin{bmatrix} 9 & 3 \\ 3 & m+1 \end{bmatrix}$, which is represented by L.

Now, suppose that $a \geq 4$. Consider the $\mathbb{Z}$-lattice $\ell'' = \begin{bmatrix} a^2-9 & ab-4 \\ ab-4 & m+b^2-6 \end{bmatrix}$. Since $s(\ell'') \subseteq 4\mathbb{Z}$ and $d\ell'' > 0$, ℓ'' is represented by $\mathcal{N}$. Choose vectors $w_1', w_2' \in \mathcal{N}$ such that

$$\begin{bmatrix} a^2-9 & ab-4 \\ ab-4 & m+b^2-6 \end{bmatrix} = \mathbb{Z}w_1' + \mathbb{Z}w_2' \subseteq 2N.$$

Since

$$\mathbb{Z}(e+x+y+w_1') + \mathbb{Z}(-e+y+w_2') = \begin{bmatrix} a^2 & ab \\ ab & m+b^2 \end{bmatrix},$$

ℓ is represented by L. □

4.3 Recoverable numbers

From several lemmas in Section 4.2, one may conclude that if a binary $\mathbb{Z}$-lattice ℓ is recoverable, then $\ell = \langle a, 4ma \rangle$ for some positive integers a and m. In this section, we introduce the notion of a recoverable number which is related with a recoverable $\mathbb{Z}$-lattice. We prove that any square of an integer is a recoverable number. We also determine whether or not some numbers are recoverable.

Definition 4.3.1. A positive integer m is called *recoverable* if $\langle 1, 4m \rangle$ is a recoverable binary $\mathbb{Z}$-lattice.

Proposition 4.3.2. *Any positive definite diagonal $\mathbb{Z}$-lattice $\ell = \langle 1, 4m^2 \rangle$ with $m \in \mathbb{Z}$ is recoverable. Therefore, m^2 is a recoverable number for any positive integer m.*

Proof. Let S be the set of all proper sublattices of ℓ and let L be an S-universal $\mathbb{Z}$-lattice. Since $\langle 1, 16m^2 \rangle \to L$, we have $L = \mathbb{Z}e_1 \perp L' = \langle 1 \rangle \perp L'$. For $\langle 4, 4m^2 \rangle \to L$, one of the following holds:

(i) there is a vector $y \in L'$ such that $\mathbb{Z}(2e_1) + \mathbb{Z}y = \langle 4, 4m^2 \rangle$;

(ii) there are vectors $x, y \in L'$ and and integer a such that $\mathbb{Z}(e_1 + x) + \mathbb{Z}(ae_1 + y) = \langle 4, 4m^2 \rangle$;

(iii) there are vectors $x, y \in L'$ and an integer a such that $\mathbb{Z}x + \mathbb{Z}(ae_1 + y) = \langle 4, 4m^2 \rangle$.

If (i) holds, then $Q(y) = 4m^2$.
If (ii) holds, then $\mathbb{Z}x + \mathbb{Z}y = \begin{bmatrix} 3 & -1 \\ -a & 4m^2 - a^2 \end{bmatrix}$. Hence $Q(ax + y) = 4m^2$.
If (iii) holds, then $\mathbb{Z}x + \mathbb{Z}y = \langle 4, 4m^2 - a^2 \rangle$. Hence $Q(mx) = 4m^2$. In any case, we have $\langle 4m^2 \rangle \to L'$ and so $\ell \to L$. This completes the proof. □

Let $\mathscr{L}$ be the set of all binary $\mathbb{Z}$-lattices, and let $\mathscr{L}_{13}$ be the set of all binary $\mathbb{Z}$-lattices whose second minimum is greater than or equal to 13. Define a map $\phi_9 : \mathscr{L}_{13} \to \mathscr{L}$ by

$$\phi_9\,(K) = \begin{bmatrix} a & b \\ b & c-9 \end{bmatrix}, \text{ where } \begin{bmatrix} a & b \\ b & c \end{bmatrix} \text{ is a Minkowski-reduced form of } K.$$

Note that ϕ_9 is well defined, for $d(\phi_9(K)) > 0$.

Lemma 4.3.3. *Let L be a $\mathbb{Z}$-lattice and let K be a binary $\mathbb{Z}$-lattice. If $\phi_9^k(K)$ is represented by L for some nonnegative integer k, then*

$$K \longrightarrow L \perp 9I_5.$$

Here, $9I_5$ is the $\mathbb{Z}$-lattice obtained from I_5 by scaling $\mathbb{Q} \otimes I_5$ by 9.

Proof. Let K be a binary $\mathbb{Z}$-lattice in $\mathscr{L}_{13}$ and let $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ be the Minkowski-reduced form of K. Since $0 \le 2b \le a \le c$ and $c \ge 13$, we have

$$d(\phi_9(K)) = a(c-9) - b^2 = \left(\frac{ac}{4} - b^2\right) + a\left(\frac{3c}{4} - 9\right) > 0,$$

which implies that $\phi_9(K) \in \mathscr{L}$. Thus ϕ_9 is well defined.

For the proof of the second assertion, we use induction on k. Note that $9I_5$ represents all binary $\mathbb{Z}$-lattices whose scale are subsets of $9\mathbb{Z}$. First, suppose that $\phi_9(K)$ is represented by L and let $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ is a Minkowski-reduced form of K. Then, it is obvious that

$$K \simeq \begin{bmatrix} a & b \\ b & c \end{bmatrix} = \begin{bmatrix} a & b \\ b & c-9 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 9 \end{bmatrix} \longrightarrow L \perp 9I_5.$$

Now, assume the assertion is true for k and $\phi_9^{k+1}(K) \to L$. Let $K' = \phi_9(K)$ and $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ is a Minkowski-reduced form of K. Then $\phi_9^k(K') = \phi_9^{k+1}(K) \to L$. It follows from the induction hypothesis that $K' \to L \perp 9I_5$. This implies that

$$K' = \begin{bmatrix} a & b \\ b & c-9 \end{bmatrix} = \begin{bmatrix} \alpha_1 & \beta_1 \\ \beta_1 & \gamma_1 \end{bmatrix} + \begin{bmatrix} \alpha_2 & \beta_2 \\ \beta_2 & \gamma_2 \end{bmatrix}$$

where $\begin{bmatrix} \alpha_1 & \beta_1 \\ \beta_1 & \gamma_1 \end{bmatrix} \to L$ and $\begin{bmatrix} \alpha_2 & \beta_2 \\ \beta_2 & \gamma_2 \end{bmatrix} \to 9I_5$. Since $\begin{bmatrix} \alpha_2 & \beta_2 \\ \beta_2 & \gamma_2+9 \end{bmatrix}$ is also a binary $\mathbb{Z}$-lattice whose scale is a subset of $9\mathbb{Z}$, we have $\begin{bmatrix} \alpha_2 & \beta_2 \\ \beta_2 & \gamma_2+9 \end{bmatrix} \to 9I_5$. Then,

$$K \simeq \begin{bmatrix} a & b \\ b & c \end{bmatrix} = \begin{bmatrix} \alpha_1 & \beta_1 \\ \beta_1 & \gamma_1 \end{bmatrix} + \begin{bmatrix} \alpha_2 & \beta_2 \\ \beta_2 & \gamma_2+9 \end{bmatrix} \longrightarrow L \perp 9I_5.$$

□

Lemma 4.3.4. *All proper sublattices of $\langle 1,1 \rangle$ are represented by both*

$$L_1 = \langle 1,2,3 \rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \perp 9I_5 \quad \textit{and} \quad L_2 = \langle 1,2,6 \rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \perp 9I_5.$$

Proof. Let ℓ be a proper sublattice of $\langle 1,1 \rangle$. If the scale of ℓ is a subset of $9\mathbb{Z}$, then $9I_5$ represents ℓ and so do both L_1 and L_2. Now, suppose that ℓ is a proper sublattice of $\langle 1,1 \rangle$ whose scale is not a subset of $9\mathbb{Z}$. Since ℓ is a proper sublattice of $\langle 1,1 \rangle$, we have $\ell \simeq \begin{bmatrix} a^2 & ab \\ ab & b^2+c^2 \end{bmatrix}$ for some integers a, b and c with $0 \le 2b \le a$. Put $d = d\ell$. Then we have $\ell_3 \simeq \langle \varepsilon, \varepsilon d \rangle$ for some $\varepsilon \in (\mathbb{Z}_3)^\times$. Note that d is a square and so $\mathrm{ord}_3(d)$ cannot be one. Moreover, since $d(\phi_9(\ell)) = d\ell - 9\mu_1(\ell)$, we also conclude that $\mathrm{ord}_3(d(\phi_9^k(\ell)))$ cannot be one.

Let $\begin{bmatrix}\alpha & \beta\\ \beta & \gamma\end{bmatrix}$ is a Minkowski-reduced form of ℓ and assume that $\gamma \geq 13$. Since $\phi_9(\ell) = \begin{bmatrix}\alpha & \beta\\ \beta & \gamma-9\end{bmatrix}$, there exists a unimodular matrix T_1 such that

$$^tT_1 \begin{bmatrix}\alpha & \beta\\ \beta & \gamma\end{bmatrix} T_1 = \begin{bmatrix}a^2 & ab\\ ab & b^2+c^2\end{bmatrix}.$$

Then we have

$$^tT_1 \begin{bmatrix}\alpha & \beta\\ \beta & \gamma-9\end{bmatrix} T_1 = \begin{bmatrix}a^2 & ab\\ ab & b^2+c^2\end{bmatrix} - 9{}^tT_1AT_1, \quad \text{where } A = \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}.$$

If we do this procedure repeatedly, then there are unimodular matrices $T_1, T_2, \dots, T_k$ such that

$$\begin{aligned}&^t(T_k\cdots T_1)M_k(T_k\cdots T_1)\\ &\qquad = \begin{bmatrix}a^2 & ab\\ ab & b^2+c^2\end{bmatrix} - 9{}^tT_1\left(A + \cdots {}^t\,T_{k-1}(A +^t T_kAT_k)T_{k-1}\cdots\right)T_1,\end{aligned}$$

where $M_k = \phi_9^k(\ell)$. If we put

$$A' =^t T_1\left(A + \cdots {}^tT_{k-1}(A +^t T_kAT_k)T_{k-1}\cdots\right)T_1 = \begin{bmatrix}s & t\\ t & u\end{bmatrix},$$

then we have

$$\phi_9^k(\ell) = M_k \simeq \begin{bmatrix}a^2-9s & ab-9t\\ ab-9t & b^2+c^2-9u\end{bmatrix}.$$

Firstly, suppose that $a \in 3\mathbb{Z}$. Since the scale of ℓ is not a subset of $9\mathbb{Z}$, we have $b^2+c^2 \in \mathbb{Z}_3^\times$ and so $\ell_3 \simeq \langle b^2+c^2, (b^2+c^2)d\rangle$. Since b^2+c^2-9u is a unit square multiple of b^2+c^2 by the local square theorem, we have $b^2+c^2 \to (\phi_9^k(\ell))_3$. Then

$$(\phi_9^k(\ell))_3 \simeq \langle b^2+c^2, (b^2+c^2)d(\phi_9^k(\ell))\rangle.$$

Secondly, suppose that $a \notin 3\mathbb{Z}$. Then $\ell_3 \simeq \langle a^2, a^2 d\rangle \simeq \langle 1, d\rangle$. Since $a^2 - 9s$ is a unit square multiple of a^2 by the local square theorem, we have $a^2 \to (\phi_9^k(\ell))_3$. Then

$$(\phi_9^k(\ell))_3 \simeq \langle a^2, a^2 d(\phi_9^k(\ell))\rangle \simeq \langle 1, d(\phi_9^k(\ell))\rangle.$$

In any cases, we have

$$(\phi_9^k(\ell))_3 \simeq \langle \varepsilon, \varepsilon d(\phi_9^k(\ell))\rangle \text{ for some } \varepsilon \in (\mathbb{Z}_3)^\times. \tag{4.3.1}$$

First, we consider the case when

$$L_1 = \langle 1,2,3\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \perp 9I_5.$$

Let K be a binary $\mathbb{Z}$-lattice, and let $\{x, y\}$ be a Minkowski-reduced basis for K, that is, $K = \mathbb{Z}x + \mathbb{Z}y = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$ with $0 \le 2b \le a \le c$. If $c \le 12$, then K is represented by $\langle 1,2,3\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix}$, except for the following 15 $\mathbb{Z}$-lattices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}, \qquad (a=1)$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix}, \qquad (a=2)$$

$$\begin{bmatrix} 4 & 0 \\ 0 & 6 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 1 & 13 \end{bmatrix}, \begin{bmatrix} 4 & 2 \\ 2 & 7 \end{bmatrix}, \qquad (a=4)$$

$$\begin{bmatrix} 6 & 0 \\ 0 & 7 \end{bmatrix}, \begin{bmatrix} 6 & 0 \\ 0 & 10 \end{bmatrix}, \begin{bmatrix} 6 & 3 \\ 3 & 7 \end{bmatrix}, \begin{bmatrix} 6 & 3 \\ 3 & 10 \end{bmatrix}, \qquad (a=6)$$

$$\begin{bmatrix} 7 & 1 \\ 1 & 10 \end{bmatrix}, \begin{bmatrix} 10 & 2 \\ 2 & 10 \end{bmatrix}. \qquad (a=7 \text{ or } 10)$$

For any binary $\mathbb{Z}$-lattice K, since $\mu_2(\phi_9(K)) \le \max\{\mu_1(K), \mu_2(K) - 9\}$, there exists a nonnegative integer k' such that $\mu_2(\phi_9^{k'}(K)) \le 12$. Thus, there exists a nonnegative integer k such that $\phi_9^k(\ell) \in \mathscr{L}$ and $\mu_2(\phi_9^k(\ell)) \le 12$. If

$\phi_9^k(\ell) \to \langle 1,2,3\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix}$, then

$$\ell \longrightarrow \langle 1,2,3\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \perp 9I_5$$

by Lemma 4.3.3. Thus, we may assume that $\phi_9^k(\ell)$ is isometric to one of 15 lattices given above. On the other hand, Equation (4.3.1) shows that $\phi_9^k(\ell)$ is isometric to one of the following $\mathbb{Z}$-lattices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix}.$$

Note that those lattices are not proper sublattices of $\langle 1,1\rangle$.

The preimages of the above $\mathbb{Z}$-lattices under the map ϕ_9 are as follows:

$$\begin{aligned} \phi_9^{-1}\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 10 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 10 \end{bmatrix}, \begin{bmatrix} 5 & 2 \\ 2 & 10 \end{bmatrix}, \begin{bmatrix} 10 & 3 \\ 3 & 10 \end{bmatrix} \right\}, \\ \phi_9^{-1}\left(\begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix}\right) &= \left\{ \begin{bmatrix} 2 & 1 \\ 1 & 13 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 1 & 11 \end{bmatrix}, \begin{bmatrix} 8 & 3 \\ 3 & 11 \end{bmatrix} \right\}. \end{aligned}$$

One may easily check that all elements in the preimages of $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix}$ are represented by $\langle 1,2,3\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix}$. Then, by Lemma 4.3.3, we have

$$\ell \longrightarrow \langle 1,2,3\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \perp 9I_5.$$

Therefore, all proper sublattices of $\langle 1,1\rangle$ are represented by L_1.

Now, we consider the case when

$$L_2 = \langle 1,2,6\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \perp 9I_5.$$

Let K be a binary $\mathbb{Z}$-lattice and let $\{x,y\}$ be a Minkowski-reduced basis for

K, that is, $K = \mathbb{Z}x + \mathbb{Z}y = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$ with $0 \le 2b \le a \le c$. If $c \le 12$, then K is represented by $\langle 1,2,6\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix}$, except for the following 29 $\mathbb{Z}$-lattices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 12 \end{bmatrix}, \qquad (a = 1)$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 10 \end{bmatrix}, \qquad (a = 2)$$

$$\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 7 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 10 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix}, \qquad (a = 3)$$

$$\begin{bmatrix} 4 & 0 \\ 0 & 12 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 1 & 10 \end{bmatrix}, \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}, \qquad (a = 4)$$

$$\begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} 5 & 2 \\ 2 & 5 \end{bmatrix}, \begin{bmatrix} 5 & 2 \\ 2 & 7 \end{bmatrix}, \qquad (a = 5)$$

$$\begin{bmatrix} 6 & 3 \\ 3 & 7 \end{bmatrix}, \begin{bmatrix} 6 & 3 \\ 3 & 10 \end{bmatrix}, \qquad (a = 6)$$

$$\begin{bmatrix} 7 & 0 \\ 0 & 12 \end{bmatrix}, \begin{bmatrix} 7 & 1 \\ 1 & 7 \end{bmatrix}, \begin{bmatrix} 7 & 2 \\ 2 & 10 \end{bmatrix}, \begin{bmatrix} 7 & 3 \\ 3 & 12 \end{bmatrix}, \qquad (a = 7)$$

$$\begin{bmatrix} 10 & 0 \\ 0 & 12 \end{bmatrix}, \begin{bmatrix} 10 & 3 \\ 3 & 12 \end{bmatrix}, \begin{bmatrix} 10 & 4 \\ 4 & 10 \end{bmatrix}, \begin{bmatrix} 10 & 5 \\ 5 & 10 \end{bmatrix}. \qquad (a = 10)$$

As we proved before, there exists a nonnegative integer k such that $\phi_9^k(\ell) \in \mathscr{L}$ and $\mu_2(\phi_9^k(\ell)) \le 12$. If $\phi_9^k(\ell) \to \langle 1,2,6\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix}$, then

$$\ell \longrightarrow \langle 1,2,6\rangle \perp \begin{bmatrix} 2 & 1 \\ 1 & 5 \end{bmatrix} \perp 9I_5$$

by Lemma 4.3.3. Thus, we may assume that $\phi_9^k(\ell)$ is isometric to one of 29 $\mathbb{Z}$-lattices given above. On the other hand, Equation (4.3.1) shows that $\phi_9^k(\ell)$

is isometric to one of the following $\mathbb{Z}$-lattices:

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}2&1\\1&4\end{bmatrix},\begin{bmatrix}2&1\\1&10\end{bmatrix},\begin{bmatrix}5&0\\0&5\end{bmatrix},\begin{bmatrix}5&2\\2&7\end{bmatrix}. \tag{4.3.2}$$

Note that those $\mathbb{Z}$-lattices are not proper sublattices of $\langle 1,1\rangle$. The preimages of the above $\mathbb{Z}$-lattices under the map ϕ_9 are as follows:

$$\begin{aligned}
\phi_9^{-1}\left(\begin{bmatrix}1&0\\0&1\end{bmatrix}\right)&=\left\{\begin{bmatrix}1&0\\0&10\end{bmatrix},\begin{bmatrix}2&1\\1&10\end{bmatrix},\begin{bmatrix}5&2\\2&10\end{bmatrix},\begin{bmatrix}10&3\\3&10\end{bmatrix}\right\},\\
\phi_9^{-1}\left(\begin{bmatrix}2&1\\1&4\end{bmatrix}\right)&=\left\{\begin{bmatrix}2&1\\1&13\end{bmatrix},\begin{bmatrix}4&1\\1&11\end{bmatrix},\begin{bmatrix}8&3\\3&11\end{bmatrix}\right\},\\
\phi_9^{-1}\left(\begin{bmatrix}2&1\\1&10\end{bmatrix}\right)&=\left\{\begin{bmatrix}2&1\\1&19\end{bmatrix},\begin{bmatrix}10&1\\1&11\end{bmatrix}\right\},\\
\phi_9^{-1}\left(\begin{bmatrix}5&0\\0&5\end{bmatrix}\right)&=\left\{\begin{bmatrix}5&0\\0&14\end{bmatrix},\begin{bmatrix}10&5\\5&14\end{bmatrix}\right\},\\
\phi_9^{-1}\left(\begin{bmatrix}5&2\\2&7\end{bmatrix}\right)&=\left\{\begin{bmatrix}5&2\\2&16\end{bmatrix},\begin{bmatrix}7&2\\2&14\end{bmatrix},\begin{bmatrix}8&3\\3&14\end{bmatrix}\right\}.
\end{aligned}$$

One may easily check that all elements in the preimages of $\mathbb{Z}$-lattices in (4.3.2) are represented by $\langle 1,2,6\rangle \perp \begin{bmatrix}2&1\\1&5\end{bmatrix}$ except for the $\mathbb{Z}$-lattice $\begin{bmatrix}2&1\\1&10\end{bmatrix}$. However, $\begin{bmatrix}2&1\\1&10\end{bmatrix}$ is not a proper sublattice of $\langle 1,1\rangle$. Then, by Lemma 4.3.3, we have

$$\ell \longrightarrow \langle 1,2,6\rangle \perp \begin{bmatrix}2&1\\1&5\end{bmatrix} \perp 9I_5.$$

Therefore, all proper sublattices of $\langle 1,1\rangle$ are represented by L_2. □

Proposition 4.3.5. *If m is a positive integer with $ord_3(m)=1$, then m is not a recoverable number.*

Proof. If m is a positive integer with $\mathrm{ord}_3(m)=1$, then either $\frac{m}{3}\equiv 1 \pmod 3$ or $\frac{m}{3}\equiv 2 \pmod 3$ holds. Since the other case can be treated in a similar manner, we only consider the case when $\frac{m}{3}\equiv 2 \pmod 3$. Define the $\mathbb{Z}$-lattice

L by

$$\langle 1,2,3,4m-1\rangle \perp \begin{bmatrix}2 & 1\\ 1 & 5\end{bmatrix} \perp 9I_5 \perp \mathcal{M}(4m+1).$$

Clearly, L does not represent $\langle 1,4m\rangle$. By the definition of L, for any proper sublattice of $\langle 1,4m\rangle$ which is of the form $\begin{bmatrix}a^2 & ab\\ ab & b^2+4m\end{bmatrix}$ with $a\geq 2$, it suffices to show that $\begin{bmatrix}a^2 & ab\\ ab & b^2+1\end{bmatrix}$ is represented by $\langle 1,2,3\rangle \perp \begin{bmatrix}2 & 1\\ 1 & 5\end{bmatrix} \perp 9I_5$. This follows from Lemma 4.3.4. □

Proposition 4.3.6. *An integer m is a recoverable number if $4m$ is represented by all of the following $\mathbb{Z}$-lattices:*

$$\begin{bmatrix}4 & 0\\ 0 & 8\end{bmatrix}, \begin{bmatrix}4 & 1\\ 1 & 8\end{bmatrix}, \begin{bmatrix}4 & 2\\ 2 & 8\end{bmatrix}, \begin{bmatrix}4 & 3\\ 3 & 8\end{bmatrix}, \begin{bmatrix}4 & 4\\ 4 & 8\end{bmatrix}, \begin{bmatrix}4 & 5\\ 5 & 8\end{bmatrix},$$
$$\begin{bmatrix}4 & 0\\ 0 & 9\end{bmatrix}, \begin{bmatrix}4 & 1\\ 1 & 9\end{bmatrix}, \begin{bmatrix}4 & 2\\ 2 & 9\end{bmatrix}, \begin{bmatrix}4 & 3\\ 3 & 9\end{bmatrix}, \begin{bmatrix}4 & 4\\ 4 & 9\end{bmatrix}, \begin{bmatrix}4 & 5\\ 5 & 9\end{bmatrix}.$$

In particular, 5569 is a recoverable number.

Proof. Suppose that there is a $\mathbb{Z}$-lattice L such that it represents every proper sublattice of $\langle 1,4m\rangle$, but not $\langle 1,4m\rangle$ itself.

Since $\langle 1,16m\rangle \to L$, we have $\langle 1\rangle \to L$. Let $L=\langle 1\rangle \perp L'$.

For $\langle 4,4m\rangle \to L$, one of the following holds:

(i) there is a vector $y\in L'$ such that $\mathbb{Z}(2e_1)+\mathbb{Z}y=\langle 4,4m\rangle$;

(ii) there are vectors $x,y\in L'$ and and integer a such that $\mathbb{Z}(e_1+x)+\mathbb{Z}(ae_1+y)=\langle 4,4m\rangle$;

(iii) there are vectors $x,y\in L'$ and an integer a such that $\mathbb{Z}x+\mathbb{Z}(ae_1+y)=\langle 4,4m\rangle$.

When (i) or (ii) holds, $4m$ is represented by L', which is a contradiction. Therefore, L' represents 4 and $\langle 4,4m-a^2\rangle$ for some odd integer a.

Since $\langle 9,4m\rangle$ is represented by L, similarly one may show that L' represents either 8 or 9.

Suppose that L' represents 4 and 8. Then L' represents at least one of the following binary $\mathbb{Z}$-lattices:

$$\begin{bmatrix}4 & 0\\0 & 8\end{bmatrix}, \begin{bmatrix}4 & 1\\1 & 8\end{bmatrix}, \begin{bmatrix}4 & 2\\2 & 8\end{bmatrix}, \begin{bmatrix}4 & 3\\3 & 8\end{bmatrix}, \begin{bmatrix}4 & 4\\4 & 8\end{bmatrix}, \begin{bmatrix}4 & 5\\5 & 8\end{bmatrix}.$$

Here, we have

$$\begin{bmatrix}4 & 3\\3 & 8\end{bmatrix} \simeq \begin{bmatrix}4 & 1\\1 & 6\end{bmatrix}, \begin{bmatrix}4 & 4\\4 & 8\end{bmatrix} \simeq \begin{bmatrix}4 & 0\\0 & 4\end{bmatrix}, \text{ and } \begin{bmatrix}4 & 5\\5 & 8\end{bmatrix} \simeq \begin{bmatrix}2 & 1\\1 & 4\end{bmatrix}.$$

Suppose that L' represents 4 and 9. Then L' represents at least one of the following binary $\mathbb{Z}$-lattices:

$$\begin{bmatrix}4 & 0\\0 & 9\end{bmatrix}, \begin{bmatrix}4 & 1\\1 & 9\end{bmatrix}, \begin{bmatrix}4 & 2\\2 & 9\end{bmatrix}, \begin{bmatrix}4 & 3\\3 & 9\end{bmatrix}, \begin{bmatrix}4 & 4\\4 & 9\end{bmatrix}, \begin{bmatrix}4 & 5\\5 & 9\end{bmatrix}, \begin{bmatrix}4 & 6\\6 & 9\end{bmatrix}.$$

Here, we have

$$\begin{bmatrix}4 & 3\\3 & 9\end{bmatrix} \simeq \begin{bmatrix}4 & 1\\1 & 7\end{bmatrix}, \begin{bmatrix}4 & 4\\4 & 9\end{bmatrix} \simeq \begin{bmatrix}4 & 0\\0 & 5\end{bmatrix}, \text{ and } \begin{bmatrix}4 & 5\\5 & 9\end{bmatrix} \simeq \begin{bmatrix}3 & 1\\1 & 4\end{bmatrix}.$$

Suppose that $\begin{bmatrix}4 & 6\\6 & 9\end{bmatrix}$ is represented by L'. Then there are x and y in L' such that $Q(x) = 4$, $Q(y) = 9$ and $B(x, y) = 12$. Since $Q(3x - 2y) = 0$, we have $3x = 2y$. Therefore, there exists a vector z in L' with $Q(z) = 1$. Then we have $L' = \langle 1\rangle \perp L''$. Note that L' represents $\langle 4, 4m - a^2\rangle$. Moreover, since 9 is represented by L' from the assumption, it is true that L' represents $\langle 9, 4m - b^2\rangle$ for some integer b with $4m - b^2 > 0$. Since the above argument does not depend on $4m$, we conclude that L'' represents 4 and either 8 or 9. Then, L' represents at least one of above 12 $\mathbb{Z}$-lattices.

Hence, m is a recoverable number if $4m$ is represented by all of the above 12 $\mathbb{Z}$-lattices. In particular, since $4\cdot 5569$ is represented by all of 12 $\mathbb{Z}$-lattices, 5569 is a recoverable number. □

Proposition 4.3.7. *For any integer m with $2 \leq m \leq 35$, m is a recoverable number only when m is a square.*

Proof. Let p_i be the i-th prime when we arrange all prime numbers in the ascending order. Let m be a positive integer which is not a square. Then there exists a positive integer M such that $p_M^2 < 4m < p_{M+1}^2$. We define a $\mathbb{Z}$-lattice $\mathcal{K}(p_i)$ by

$$\mathcal{K}(p_i) = \underset{1 \le j \le [\frac{p_i}{2}]}{\perp} \begin{bmatrix} p_i^2 & p_i j \\ p_i j & j^2 + 4m \end{bmatrix}$$

and a $\mathbb{Z}$-lattice L_m by

$$L_m = \langle 1, 4m-1 \rangle \perp \left(\underset{2 \le i \le M}{\perp} \mathcal{K}(p_i) \right) \perp \mathcal{M}(4m+1).$$

Let ℓ' be a proper sublattice of $\ell = \langle 1, 4m \rangle$.
(Case 1) If $\min(\ell') > 4m$, then $\mathcal{M}(4m+1)$ represents ℓ' and so does L_m.
(Case 2) If $\min(\ell') = 4m$, then $\ell' \simeq \langle 4m, \alpha^2 \rangle$ for some integer α with $\alpha^2 \ge 4m$. Since $4m$ is not a square, we have $\alpha^2 > 4m$ and so α^2 is represented by $\mathcal{M}(4m+1)$. Thus, L_m represents ℓ'.
(Case 3) Assume that $1 < \min(\ell') < 4m$. There exists the unique positive integer h such that $h^2 < 4m < (h+1)^2$. Note that

$$\ell' \simeq \begin{bmatrix} i^2 & ij \\ ij & j^2 + 4m\beta^2 \end{bmatrix}$$

for some integers i, j and β with $2 \le i \le h$, $0 \le j \le \left[\frac{i}{2}\right]$, $\beta \ge 1$. Since $i \ge 2$, i has at least one prime factor p. Put $i = pk$ for some integer k. Then

$$\ell' \simeq \begin{bmatrix} (pk)^2 & (pk)j \\ (pk)j & j^2 + 4m\beta^2 \end{bmatrix} \longrightarrow \begin{bmatrix} p^2 & pj \\ pj & j^2 + 4m\beta^2 \end{bmatrix} \simeq \begin{bmatrix} p^2 & pj' \\ pj' & j'^2 + 4m\beta^2 \end{bmatrix}$$

where j' is the positive integer such that $0 \le j' \le \left[\frac{p}{2}\right]$ and either j' or $-j'$ is congruent to j modulo p. Since $4m < p_{M+1}^2$, we have $i \le p_M$. Hence ℓ' is represented by L_m. Thus, L_m represents all proper sublattices of $\langle 1, 4m \rangle$.

If there is no integer solution $x_{1,1}, \dots, x_{M,\frac{p_M-1}{2}}$ of

$$4m = \sum_{i=1}^{M} \left(\sum_{j=1}^{\frac{p_i-1}{2}} p_i^2 x_{i,j} \right), \tag{4.3.3}$$

then L_m does not represent $\langle 1, 4m \rangle$. Therefore, if Equation (4.3.3) has no integer solution, m is not a recoverable number. For $2 \le m \le 30 = \left[\frac{11^2}{4}\right]$, Equation (4.3.3) has no integer solution except for $m = 10, 13, 18, 26, 27, 28, 29$.

First, we consider the case when $m = 10$. Although there is an integer solution of $4x_{1,1}^2 + 9x_{2,1}^2 = 40$, there is no integer solution of $4x_{1,1}^2 + 4x_{1,1}x_{2,1} + 9x_{2,1}^2 = 40$. Then we consider a following $\mathbb{Z}$-lattice:

$$L'_{40} = \langle 1 \rangle \perp K \perp \mathcal{K}(5) \perp \langle 39 \rangle \perp \mathcal{M}(41)$$

where

$$K = \begin{bmatrix} 4 & 2 & 2 & 0 \\ 2 & 9 & 0 & 2 \\ 2 & 0 & 41 & 0 \\ 0 & 2 & 0 & 41 \end{bmatrix}.$$

By the same argument, one may easily prove that L'_{40} represents all sublattices of $\langle 1, 40 \rangle$. However, since 15 and 40 are not represented by K. Thus, L'_{40} does not represent $\langle 1, 40 \rangle$.

Similarly, for an integer m with $m = 13, 18$ or $26 \le m \le 35$, we can find a lattice L that represents all proper sublattices of $\langle 1, 4m \rangle$ but not $\langle 1, 4m \rangle$ itself. We list a $\mathbb{Z}$-lattice L such that L represents all proper sublattices of $\langle 1, 4m \rangle$ but not $\langle 1, 4m \rangle$ itself for each $m = 13, 18$ or $26 \le m \le 35$ in the following tables.

$\square$

m	L
13	$\langle 1,51\rangle \perp \begin{bmatrix} 4 & 2 & 2 & 0 \\ 2 & 9 & 0 & 2 \\ 2 & 0 & 53 & 0 \\ 0 & 2 & 0 & 53 \end{bmatrix} \perp \mathcal{K}(5) \perp \mathcal{K}(7) \perp \mathcal{M}(53)$
18	$\langle 1,71\rangle \perp \begin{bmatrix} 4 & 2 & 2 & 0 \\ 2 & 9 & 0 & 2 \\ 2 & 0 & 73 & 0 \\ 0 & 2 & 0 & 73 \end{bmatrix} \perp \mathcal{K}(5) \perp \mathcal{K}(7) \perp \mathcal{M}(73)$
26	$\langle 1,103\rangle \perp \begin{bmatrix} 4 & 2 & 2 & 0 \\ 2 & 25 & 5 & 10 \\ 2 & 5 & 105 & 0 \\ 0 & 10 & 0 & 108 \end{bmatrix} \perp \mathcal{K}(3) \perp \mathcal{K}(7) \perp \mathcal{M}(105)$
27	$\langle 1,107\rangle \perp \begin{bmatrix} 9 & 2 & 3 & 0 \\ 2 & 25 & 5 & 10 \\ 3 & 5 & 111 & 0 \\ 0 & 10 & 0 & 112 \end{bmatrix} \perp \mathcal{K}(2) \perp \mathcal{K}(7) \perp \mathcal{M}(109)$
28	$\langle 1,103\rangle \perp \begin{bmatrix} 9 & 2 & 3 & 0 \\ 2 & 25 & 5 & 10 \\ 3 & 5 & 113 & 0 \\ 0 & 10 & 0 & 116 \end{bmatrix} \perp \mathcal{K}(2) \perp \mathcal{K}(7) \perp \mathcal{M}(113)$
29	$\langle 1,115\rangle \perp \begin{bmatrix} 4 & 2 & 2 & 0 \\ 2 & 25 & 5 & 10 \\ 2 & 5 & 117 & 0 \\ 0 & 10 & 0 & 120 \end{bmatrix} \perp \mathcal{K}(3) \perp \mathcal{K}(7) \perp \mathcal{M}(117)$

Table 4.1: A $\mathbb{Z}$-lattice L which represents all proper sublattices of $\langle 1,4m\rangle$ but not $\langle 1,4m\rangle$ itself for each $m = 13, 18, 26, 27, 28, 29$.

m	L
31	$\langle 1,123\rangle \perp \begin{bmatrix} 4 & 2 & 2 & 0 & 0 \\ 2 & 49 & 7 & 14 & 21 \\ 2 & 7 & 125 & 0 & 0 \\ 0 & 14 & 0 & 128 & 0 \\ 0 & 21 & 0 & 0 & 133 \end{bmatrix} \perp \mathcal{K}(3) \perp \mathcal{K}(5) \perp \mathcal{K}(11) \perp \mathcal{M}(125)$
32	$\langle 1,127\rangle \perp \begin{bmatrix} 4 & 2 & 2 & 0 & 0 \\ 2 & 49 & 7 & 14 & 21 \\ 2 & 7 & 129 & 0 & 0 \\ 0 & 14 & 0 & 132 & 0 \\ 0 & 21 & 0 & 0 & 137 \end{bmatrix} \perp \mathcal{K}(3) \perp \mathcal{K}(5) \perp \mathcal{K}(11) \perp \mathcal{M}(129)$
33	$\langle 1,131\rangle \perp \begin{bmatrix} 4 & 2 & 2 & 0 & 0 \\ 2 & 49 & 7 & 14 & 21 \\ 2 & 7 & 133 & 0 & 0 \\ 0 & 14 & 0 & 136 & 0 \\ 0 & 21 & 0 & 0 & 141 \end{bmatrix} \perp \mathcal{K}(3) \perp \mathcal{K}(5) \perp \mathcal{K}(11) \perp \mathcal{M}(133)$
34	$\langle 1,135\rangle \perp \begin{bmatrix} 4 & 2 & 0 & 0 & 2 & 0 & 0 \\ 2 & 9 & 2 & 0 & 3 & 0 & 0 \\ 0 & 2 & 25 & 2 & 5 & 10 & 0 \\ 0 & 0 & 2 & 49 & 7 & 14 & 21 \\ 2 & 3 & 5 & 7 & 137 & 0 & 0 \\ 0 & 0 & 10 & 14 & 0 & 140 & 0 \\ 0 & 0 & 0 & 21 & 0 & 0 & 145 \end{bmatrix} \perp \mathcal{K}(2) \perp \mathcal{K}(7) \perp \mathcal{M}(109)$
35	$\langle 1,139\rangle \perp \begin{bmatrix} 4 & 0 & 2 & 2 & 0 \\ 0 & 9 & 3 & 3 & 0 \\ 2 & 3 & 25 & 5 & 10 \\ 2 & 3 & 5 & 141 & 0 \\ 0 & 0 & 10 & 0 & 144 \end{bmatrix} \perp \mathcal{K}(7) \perp \mathcal{K}(11) \perp \mathcal{M}(141)$

Table 4.2: A ℤ-lattice L which represents all proper sublattices of $\langle 1, 4m\rangle$ but not $\langle 1, 4m\rangle$ itself for each $m = 31, 32, 33, 34, 35$.

Bibliography

[1] M. Bhargava, *On the Conway-Schneeberger fifteen theorem*, Quadratic forms and their applications, Contem. Math., **272**(2000), 27–37.

[2] J. W. S. Cassels, *Rational quadratic forms*, Academic Press, 1978.

[3] J. H. Conway, *Universal quadratic forms and the fifteen theorem*, Quadratic forms and their applications, Contemp. Math., **272**(2000), 23–26.

[4] J. H. Conway, and N. J. A. Sloane, *Sphere packings*, lattices and groups, Springer-Verlag, 1988.

[5] J. H. Conway, and N. J. A. Sloane, *Low dimensional lattices. I. Quadratic forms of small determinant*, Proc. Royal. Soc. Lond. A. **418**(1988), 17–41.

[6] L. E. Dickson, *Quaternary quadratic forms representing all integers*, Amer. J. Math. **49**(1927), 39–56.

[7] A. G. Earnest, *The representation of binary quadratic forms by positive definite quaternary quadratic forms*, Trans. Amer. Math. Soc., **345**(1994), 853–863.

[8] N. D. Elkies, D. M. Kane, and S. D. Kominers, *Minimal S - universality criteria may vary in size*, J. Théor. Nombres Bordeaux **25**(2013), 557–563.

[9] Y.-S. Ji, M.-H. Kim, and B.-K. Oh, *Positive definite quadratic forms representing integers of the form $an^2 + b$*, Ramanujan J. **27**(2012), 329–342.

[10] B. M. Kim, M.-H. Kim, and B.-K. Oh, *2-universal positive definite integral quinary quadratic forms*, Integral quadratic forms and lattices (Seoul, 1998), Contemp. Math., **249**(1999) 51–62.

[11] B. M. Kim, M.-H. Kim, and B.-K. Oh, *A finiteness theorem for representability of quadratic forms by forms*, J. reine angew. Math. **581**(2005), 23–30.

[12] M.-H. Kim, *Recent developments on universal forms*, Algebraic and Arithmetic Theory of Quadratic Forms, Contemp. Math., **344**(2004), 215–228.

[13] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Press, 1993.

[14] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Math. **49**(1926), 407–464.

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

[16] S. D. Kominers, *The 8-universality criterion is unique*, Preprint, arXiv:0807-2099, 2008.

[17] S. D. Kominers, *Uniqueness of the 2-universality criterion*, Note Mat. **28**(2008), 203–206.

[18] B.-K. Oh, *Universal $\mathbb{Z}$-lattices of minimal rank*, Proc. Amer. Math. Soc. **128**(2000), 683–689.

[19] O. T. O'Meara, *Introduction to quadratic forms*, Springer Verlag, New York, 1963.

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

[21] S. Ramanujan, *On the expression of a number in the form* $ax^2+by^2+cz^2+du^2$, Proc. Camb. Phil. Soc. **19**(1916), 11–21.

[22] W. Tartakovski, *Die Gesamtheit der Zahlen,die durch eine positive quadratische Form* $F(x_1,\dots,x_s)$ *(*$s \geq 4$*) darstellbar sind*, IZv. Akad. Nauk SSSR. **7**(1929), 111–122, 165–195.

국문초록

변수의 개수가 유계인, 양의 정부호이고 정수 계수인 이차형식의 집합 S에 대하여, 모든 S_0-보편형식이 S-보편형식이 되는 S의 부분집합 S_0를 S-보편성 판정 집합이라 한다.

이 논문에서는 최소 S-보편성 판정 집합에 관한 다양한 성질에 관하여 연구한다. 먼저 집합 S가 자연수의 부분집합인 경우, 최소 S-보편성 판정 집합이 유일함을 증명한다. 또한, 9 이상의 정수 n에 대하여 모든 n차 이차형식의 집합을 S라 할 때, 최소 S-보편성 판정 집합은 항상 유일하지 않음을 증명한다.

이차형식 f의 모든 부분이차형식들의 집합 S_f에 대하여, $\{f\}$ 이외의 최소 S_f-보편성 판정 집합이 존재할 때, f를 복구 가능한 이차형식이라 한다. 이 논문에서는 복구 가능한 이차형식이 되기 위한 몇 가지 충분조건과 몇 가지 필요조건을 증명한다.

주요어휘**:** 이차형식의 표현, 최소 S-보편성 판정 집합
학번**:** 2013-20241