Finiteness of strictly n-regular quadratic forms

by

Alicia Marino

Advisor: Wai Kiu Chan

Professor of Mathematics

Wesleyan University

Middletown, CT

May, 2017

A Dissertation in Mathematics

submitted in partial fulfillment of the

requirements for the degree of Doctor of Philosophy

For my mother, my father, and Frankie

Abstract

A quadratic form is a homogeneous polynomial of degree two. In the arithmetic theory of integral quadratic forms, a main question is the representation problem: given an integral quadratic form f, for which integers a does there exist a solution to $f(x) = a$? We call an integral quadratic form regular if the existence of solutions locally everywhere implies the existence of a solution over the rational integers. We can strengthen this notion of regularity to strict regularity by demanding that the solutions are primitive, i.e. the coordinates of the solutions are coprime. In 2014, Andrew Earnest et al. [8] proved that there are finitely many equivalence classes of primitive positive definite integral strictly regular quadratic forms in four variables. The main result of this thesis extends their result in the context of a higher dimensional analogue of strict regularity. We obtain the following result: for $n \geq 2$, there are only finitely many equivalence classes of primitive positive definite integral strictly n-regular quadratic forms of $n + 4$ variables.

Acknowledgements

First and foremost, I extend my sincere gratitude to Professor Wai Kiu Chan. His support and mentorship over the past years has been invaluable. I appreciate his academic guidance as much as I appreciate his wisdom and advice outside of mathematics. Without him, none of this would have been possible.

I would also like to thank the mathematical community at Wesleyan. In particular, I extend my thanks to my committee members, Professor Chris Rasmussen and Professor David Pollack, for their comments and support throughout my graduate career. I thank my officemates, Leah Karker and Sarah Vigliotta, for all of their help, memories, and laughter. I also thank the current graduate students: Andre Oliveira, Cameron Bishop, Noelle Sawyer, Freda Li, and Zonia Menendez for helping me through my last year of graduate school and making it extremely enjoyable. Finally, I also thank Caryn Canalia for being an amazing administrative assistant as well as a great friend.

To my wonderful family, friends, Lenore, and Jensen: I thank you most sincerely. You have supported me all of my life and without you, none of this would be possible. Thank you for consistently bringing joy to my life. I love you.

Contents

Introduction

This work is motivated by the representation problem of quadratic forms over the integers:

> *Given an integer a and an integral m-ary quadratic form f, is there an integral vector $\boldsymbol{c} = (c_1, \ldots, c_m)$ such that $f(\boldsymbol{c}) = a$?*

If this is the case then we say that a is represented by f. By the Hasse-Minkowski Theorem, we know that a rational solution exists (i.e. $\mathbf{c} \in \mathbb{Q}^m$) if and only if solutions exist over $\mathbb{Q}_p$ for every prime p and over $\mathbb{R}$. However, there is no such local-to-global principle when restricting to integral solutions. As an example, consider the binary quadratic form $f(x, y) = x^2 + 14y^2$. One can check that there exists $\mathbf{c} \in \mathbb{Z}_p^2$ for every prime p and $\mathbf{c} \in \mathbb{R}^2$ such that $f(\mathbf{c}) = 2$; however, it is easy to see that there is no solution to $x^2 + 14y^2 = 2$ for integers x, y.

We say that an integral quadratic form is regular if the existence of solutions over $\mathbb{R}$ and $\mathbb{Z}_p$ for every prime p implies the existence of a solution over $\mathbb{Z}$. Dickson was the first to study regular quadratic forms systematically in [5] and later Watson showed that there are finitely many similarity classes of positive definite regular ternary quadratic forms [14, 15]. Forty years later, Earnest studied a higher dimensional analogue to regularity [6] and proved a finiteness

result in this context. More specifically, he studied 2-regular quadratic forms in 4 variables, those for which a local-to-global principle of representations holds not only for the integers, but for integral binary quadratic forms as well. The formal definition of the representation of quadratic forms by quadratic forms will be given in Chapter 1. This result was generalized by Chan-Oh in [4] where they proved that, for $n \geq 2$, there are finitely many similarity classes of positive definite integral n-regular quadratic forms in $n+3$ variables. The case when $n = 1$ is discussed by Earnest in [7], where he constructed an infinite family of similarity classes of positive definite regular quaternary quadratic forms. However, by restricting to positive definite strictly regular quaternary quadratic forms, Earnest-Kim-Meyer [8] did achieve a finiteness result. The main result in this thesis is a generalization of Earnest-Kim-Meyer's theorem.

Theorem 1. *For $n \geq 2$, there are only finitely many equivalence classes of strictly n-regular primitive positive definite integral quadratic lattices of rank $n+4$.*

In Chapter 1 we will provide necessary background on quadratic forms. However, our discussion here will be conducted in the geometric language of quadratic spaces and quadratic lattices. Thus, in Section 1.1 we will discuss the background and notation in this setting. The rest of Chapter 1 contains the definitions of the various regularity conditions and some basic propositions concerning them.

Chapter 2 contains a few main tools used in the proof of the main result. In Section 2.1 we discuss the theory of successive minima and in Section 2.2 the background of the Watson transformations. These will lead us into Chapter 3, which contains the proof of the main result. Finally, in Chapter 4, we will provide proofs of the local representation results needed in the proof of the main theorem.

Chapter 1

Background and Definitions

Let R be an integral domain of characteristic not 2 and let F be its field of fractions. A quadratic form over F is a homogeneous polynomial of degree 2 with coefficients from F. In general, a quadratic form over F in m variables $x_1, \ldots, x_m$ is of the form

$$f(x_1, \ldots, x_m) = \sum_{i,j=1}^{m} a_{ij} x_i x_j,$$

where the coefficients a_{ij} are elements of F. For the purposes of this thesis, F will be either $\mathbb{Q}$ or the p-adic numbers $\mathbb{Q}_p$ and R will be $\mathbb{Z}$ or $\mathbb{Z}_p$, accordingly. We can assume that $a_{ij} = a_{ji}$ by replacing each coefficient with $\frac{a_{ij}+a_{ji}}{2}$. Now, we can associate to any quadratic form a symmetric matrix, $M_f = (a_{ij})$, called the Gram matrix of f. If $\{a_{ij}\} \subseteq R$, we call the quadratic form *integral*. In addition, when $\{a_{ij}\}$ are coprime we say that the form is *primitive*.

Let f be a quadratic form over F and M_f be its Gram matrix. Then for $\mathbf{x} = (x_1, \ldots, x_m)$,

$$\mathbf{x} \cdot M_f \cdot \mathbf{x}^t = f(\mathbf{x}).$$

Thus we can recover a quadratic form from its Gram matrix. Two quadratic forms, f and g, are equivalent over R, denoted $f \cong g$, if there exists a matrix $T \in GL_m(R)$ such that

$$TM_fT^t = M_g.$$

In other words, we have that $g(\mathbf{x}) = f(\mathbf{x}T)$.

If there exists $\mathbf{c} = (c_1, \ldots, c_m) \in R^m$ such that $f(\mathbf{c}) = a$, then we say that a is *represented* by f over R, and denote this by $a \longrightarrow f$. Note that the choice of R should be clear from context. It is easy to see that if $a \longrightarrow f$ and $f \cong g$ then in fact $a \longrightarrow g$. If $c_1, \ldots, c_m$ are coprime, then we say that a is *primitively represented* by f over R, and this is denoted by $a \xrightarrow{*} f$.

We will be considering a higher dimensional analogue to this representation question. Let $n \leq m$ and let g be an n-ary quadratic form with Gram matrix M_g. We say that g is *represented* by f over R, denoted $g \longrightarrow f$, if there exists an $n \times m$ matrix T with coefficients in R such that $TM_fT^t = M_g$. Note that in the one variable case, that is if $g = ax^2$ for some $a \in F$, then $a \longrightarrow f$ if and only if $g \longrightarrow f$. If we can extend T to an invertible matrix in $GL_m(R)$ then we say that g is *primitively represented* by f over R, denoted $g \xrightarrow{*} f$. As before, if

$g = ax^2$ for $a \in F$, $g \xrightarrow{*} f$ is equivalent to $a \xrightarrow{*} f$.

1.1 Quadratic spaces and lattices

In this work we study quadratic forms from a more geometric perspective. Let V be an m-dimensional vector space over F. Let

$$B : V \times V \longrightarrow F$$

be a symmetric bilinear form. This means that B satisfies the following properties:

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

for all $x, y, z \in V$ and $\alpha \in F$. The mapping $Q : V \longrightarrow F$ defined by $Q(x) = B(x, x)$ is called the quadratic form associated with B. One can easily verify the following fundamental properties:

(1) $Q(\alpha x) = \alpha^2 Q(x)$ for all $\alpha \in F$ and $x \in V$,

(2) $2B(x, y) = Q(x + y) - Q(x) - Q(y)$ for all $x, y \in V$.

We define a quadratic space as a composite object (V, B), or equivalently, (V, Q), since (2) implies that we can uniquely recover the quadratic form Q

from the bilinear form B, and vice versa. We will always assume that V is *nondegenerate*, i.e. that $B(x, V) = 0$ if and only if $x = 0$. When we write V^α, we mean the vector space V provided with a new bilinear form B^α defined by $B^\alpha(x, y) = \alpha B(x, y)$. Suppose V has a basis $\{v_1, \ldots, v_m\}$. The Gram matrix associated to this basis is $A = \big(B(v_i, v_j)\big)$. The *discriminant* of the quadratic space is $dV = \det(A)$ viewed as an element in $F^\times/(F^\times)^2$.

If (V, B_V) and (W, B_W) are two quadratic spaces, an injective linear transformation $\sigma : V \longrightarrow W$ is called a *representation* if $B_W(\sigma x, \sigma y) = B_V(x, y)$ for all $x, y \in V$. If, in addition, σ is bijective, then it is called an *isometry*. If such an isometry exists we say that V and W are *isometric*. The *orthogonal group* of V, $O(V)$, is the group of isometries of V into V.

If there exists a nonzero vector $v \in V$ such that $Q(v) = 0$ then we say that V is *isotropic*, otherwise V is said to be *anisotropic*. Additionally, if $F = \mathbb{Q}$ and $Q(v) > 0$ for all $v \neq 0 \in V$ then V is said to be *positive definite*.

1.1.1 Quadratic lattices

Let V be a quadratic space over F as defined earlier. Let R be the ring of integers in F and $R^\times$ be the units of R. If $R = \mathbb{Z}_p$ for some prime p, then Δ refers to a nonsquare unit in R when $p > 2$; and $\Delta = 5$ if $p = 2$. An R-module

L is a *lattice* in V if there is a basis $\{x_1, \ldots, x_m\}$ for V such that

$$L \subseteq Rx_1 + \ldots + Rx_m.$$

If $FL = V$ then we say L is a lattice *on* V. Since R is a principal ideal domain, L has an R-basis $\{v_1, \ldots, v_m\}$. In this case, the *rank* of L is the number of elements in a basis for L.

The discriminant of L, dL, is the determinant $\det(B(v_i, v_j))$ as an element of $F^\times/(R^\times)^2$. The *scale* of L, denoted $\mathfrak{s}L$, is the R-module generated by $B(L, L)$ in F. The *norm* of L, denoted $\mathfrak{n}L$, is the R-module generated by $Q(L)$ in F. We say that L is *integral* if $\mathfrak{s}L \subseteq R$. From (2) we see that

$$2\mathfrak{s}L \subseteq \mathfrak{n}L \subseteq \mathfrak{s}L.$$

When $F = \mathbb{Q}$, a *normalized* lattice refers to one with $\mathfrak{n}L = 2\mathbb{Z}$.

Let L be an R-lattice in the quadratic space V over F. For $a \in R$, we say that a is *represented* by L if there exists a vector $v \in L$ such that $Q(v) = a$. If in fact v is a primitive vector of L, meaning the coordinates of v with respect to a basis of L are coprime, then a is *primitively represented* by L. If L represents all elements of R then L is called *universal*. Let K be an R-lattice in the quadratic space V over F. Then K is *represented* by L, denoted $K \longrightarrow L$, if there exists $\sigma \in O(V)$ such that $\sigma(K) \subseteq L$. We say that K is *primitively represented* by L, denoted $K \xrightarrow{*} L$, if $\sigma(K)$ is a direct summand of L, which is itself denoted

$\sigma(K) \overset{*}{\subseteq} L$. In this case, we say that $\sigma(K)$ is a primitive sublattice of L. When $\sigma(K) = L$, K and L are said to be isometric.

1.1.2 Localizations and Jordan decompositions

Let V be a quadratic space over $\mathbb{Q}$. For a prime p, we define V_p as $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. If L is a $\mathbb{Z}$-lattice in V, the localization L_p in V_p is the $\mathbb{Z}_p$-lattice in V_p generated by L. We will call a $\mathbb{Z}_p$-lattice L_p *unimodular* if $\mathfrak{s}L_p = \mathbb{Z}_p$ and $dL_p \in \mathbb{Z}_p^\times$. For $a \in \mathbb{Z}_p$, L_p is (a)-*modular*, or simply *modular*, if $L_p^{\frac{1}{a}}$ is unimodular, where $L_p^{\frac{1}{a}}$ is the lattice L_p equipped with a scaling, $B^{\frac{1}{a}}$.

Suppose L_p is a lattice in V_p. The following theory of Jordan decomposition is detailed in [13, §91C.]. There is always an orthogonal splitting for L_p into modular lattices of rank 1 and 2, depending upon p. A *Jordan splitting* of L_p is a decomposition

$$L_p = L_1 \perp \ldots \perp L_t$$

where each L_i is modular and the components satisfy $\mathfrak{s}L_1 \supset \ldots \supset \mathfrak{s}L_t$. The L_i are called the Jordan components of that Jordan splitting of L_p. If p is odd, then each Jordan component has an orthogonal basis, but when $p = 2$ some L_i may not have an orthogonal basis.

There could be more than one Jordan splitting of L_p. However, if

$$L_1 \perp \ldots \perp L_t = M_1 \perp \ldots \perp M_k$$

are two Jordan splittings for L_p, then it is known [13, 91:9] that $t = k$, rank(L_i) = rank(M_i), and $\mathfrak{s}L_i = \mathfrak{s}M_i$ for every i. When $p = 2$ and the unimodular component is improper, meaning the norm of the unimodular component is $2\mathbb{Z}_2$, the unimodular component is isometric to an orthogonal sum of either

$$\mathbb{H} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \text{ or } \mathbb{A} = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right).$$

The former, called the hyperbolic plane, primitively represents every element of $2\mathbb{Z}_2$.

The following is a classic theorem in the study of quadratic spaces.

Theorem (Hasse-Minkowski Theorem)**.** *Let V and W be two nondegenerate quadratic spaces over $\mathbb{Q}$. Then V is isometric to W if and only if V_p is isometric to W_p for all primes p and over $\mathbb{R}$.*

The analogous statement, however, does not hold for quadratic lattices. If two quadratic lattices L and M on V are isometric, then we know that L_p and K_p are in fact isometric over $\mathbb{Z}_p$ for every prime p. The converse of this statement, though, need not be true. The *genus* of L, denoted gen(L), is the set of all lattices in V that are locally isometric to L at every prime p. We say that a is represented by gen(L) if a is represented by L_p for every prime p. Similarly, a lattice K is represented by gen(L) if K is represented by L_p for every prime P. We have analogous definitions for primitive representations of an integer or

a lattice by gen(L). Contained in the genus of L is the *class* of L, which is the set of lattices in V that are isometric to L.

Lemma 1. *Let K be a positive definite quaternary quadratic $\mathbb{Z}$-lattice with square discriminant. Then there exists a prime p such that K_p is anisotropic.*

Proof. Let $U = \mathbb{Q}K$. Suppose that U is isotropic at all primes p. Then the Hasse invariant [13, Section 63] $S_p(U_p)$ is 1 when p is odd and -1 when $p = 2$. Since K is positive definite, $S_\infty(U_\infty) = 1$. It then follows that

$$S_\infty(U_\infty) \prod_p S_p(U_p) = -1.$$

This contradicts Hilbert's Reciprocity Law [13, Chapter 7]. Hence there is a prime p such that U_p is anisotropic, i.e., K_p is anisotropic. □

The following is an extension of [8, Proposition 3.1] for odd primes.

Proposition 1. *For an odd prime p, let K_p be a $\mathbb{Z}_p$-lattice of rank m and let $e-1$ be the order of p in the scale of the last Jordan component of a Jordan decomposition of K_p. If K_p is anisotropic, then K_p does not primitively represent any element in $p^e\mathbb{Z}_p$.*

Proof. Since $p \neq 2$, we may assume K_p has the form $K_p = \mathbb{Z}_p[v_1, \ldots, v_m]$ where $Q(v_1) \leq \ldots \leq Q(v_m)$. Suppose there exists a primitive vector $v = a_1v_1 + \cdots + a_mv_m$ in K_p such that $Q(v) = a$, where $\mathrm{ord}_p(a) > e-1$. Since v is primitive, it

must be the case that for some i, $a_i \in \mathbb{Z}_p^\times$. We see that

$$\begin{aligned} & Q(v) \equiv 0 \mod p^e\mathbb{Z}_p \\ \Rightarrow\ & a_i^2 Q(v_i) \equiv -\sum_{j\neq i} a_j^2 Q(v_j) \mod p^e\mathbb{Z}_p \\ \Rightarrow\ & a_i^2 \equiv -Q(v_i)^{-1}\sum_{j\neq i} a_j^2 Q(v_j) \mod p^{e-\mathrm{ord}_p(Q(v_i))}\mathbb{Z}_p. \end{aligned}$$

Since $e - \mathrm{ord}_p(Q(v_i)) \geq 1$, by [13, 63:1], there exists $\lambda \in \mathbb{Z}_p^\times$ such that

$$-Q(v_i)^{-1}\sum_{j\neq i} a_j^2 Q(v_j) = \lambda^2.$$

There then exists a nonzero vector in K_p, namely $w = \lambda v_i + \sum_{j\neq i} a_j v_j$, such that $Q(w) = 0$. Thus w is an isotropic vector, which is a contradiction. □

We generalize the previous result to include the prime 2; however, it is at the cost of not explicitly computing the integer e.

Lemma 2. *Let K_p be an anisotropic quadratic $\mathbb{Z}_p$-lattice. Then there is a positive integer $e = e(K_p)$ such that K_p does not primitively represent any p-adic integer in $p^e\mathbb{Z}_p$.*

Proof. The set $P(K_p) := K_p \backslash pK_p$ is a compact subset of K_p. Since the quadratic map $Q : K_p \to \mathbb{Z}_p$ is continuous, $Q(P(K_p))$ is also compact. Suppose that for any positive integer α, there is some element $v_\alpha \in P(K_p)$ such that $Q(v_\alpha) \in p^\alpha\mathbb{Z}_p$. Then $\{Q(v_\alpha)\}_{\alpha\geq 0}$ is a Cauchy sequence with limit 0. Since $Q(P(K_p))$ is compact, $0 \in Q(P(K_p))$ and it follows that K_p is isotropic. This is a contradiction. □

We will say that a real-valued function of several variables is bounded if the absolute value of the function is bounded above by a constant which does not depend upon these variables. In this work, we bound the number of isometry classes of a certain type of quadratic lattice. This will be achieved if the discriminants of those lattices are shown to be bounded.

1.2 Regularity conditions

From now on, all $\mathbb{Z}$-lattices are assumed to be positive definite. Let L be a $\mathbb{Z}$-lattice. A version of the Hasse-Minkowski theorem [13, 66:3] says that any positive integer a such that $a \longrightarrow L_p$ for every prime p is in fact represented by $\mathbb{Q}L$. We call L *regular* if L represents all integers that are represented by its genus. Similarly, we say that L is *n-regular* if it globally represents all rank-n lattices that are represented by its genus. The focus of this work is on these concepts in the primitive setting. An integer a is *primitively represented* by L if there is a primitive vector, $\mathbf{v}$, (i.e. a vector whose coordinates with respect to a basis of L are coprime) in L such that $Q(\mathbf{v}) = a$. If L primitively represents all integers that are primitively represented by its genus, then L is called *strictly regular*. Finally, if L primitively represents all rank-n lattices that are primitively represented by its genus then we say that L is *strictly n-regular*. The following two propositions about the relationship of these conditions will be useful in the

proof of the main result.

Proposition 2. *If L is strictly n-regular, then L is n-regular.*

Proof. Let M be a rank-n lattice which is represented by the genus of L. By the Hasse-Minkowski Principle, we may assume that M is in $\mathbb{Q}L$. Then $M_p \overset{*}{\subseteq} L_p$ at all but finitely many p. Let $S = \{p : M_p \overset{*}{\nsubseteq} L_p\}$, which is a finite set. For each $p \in S$, let σ_p be an isometry of $\mathbb{Q}L$ such that $\sigma_p M_p \subseteq L_p$. Using [13, 81:14], we may define a lattice N on $\mathbb{Q}M$ by

$$N_p = \begin{cases} M_p & \text{if } p \notin S, \\ \sigma_p^{-1}(\mathbb{Q}_p(\sigma_p M_p) \cap L_p) & \text{if } p \in S. \end{cases}$$

Notice that $M \subseteq N$, and that if $p \notin S$ then $N_p \overset{*}{\subseteq} L_p$. If $p \in S$ then

$$\mathbb{Q}_p(\sigma_p M_p) \cap L_p \subseteq L_p,$$

so $\sigma_p N_p \subseteq L_p$. To show that $\sigma_p N_p$ is primitively contained in L_p, we need to show that $L_p/\sigma_p N_p$ is torsion free. Let $v_p \in L_p$ and $r \neq 0 \in \mathbb{Z}_p$ such that $rv_p \in \sigma_p N_p$. Then $v_p = r^{-1} r v_p \in \mathbb{Q}_p(\sigma_p M_p)$. Thus $v_p \in \sigma_p N_p$ and $L_p/\sigma_p N_p$ is torsion free.

Now $N_p \xrightarrow{*} L_p$ at every p and by the strict n-regularity of L we have that $N \xrightarrow{*} L$. Additionally, since $M_p \subseteq N_p$ for all p, we know that $M \subseteq N$ and hence $M \longrightarrow L$. Thus L is n-regular by definition. □

Proposition 3. *Suppose L is strictly n-regular. Then L is strictly $(n-1)$-regular.*

Proof. Let M be a rank-$(n-1)$ lattice in $\mathbb{Q}L$ which is primitively represented by the genus of L. At all but finitely many primes p, we have $M_p \overset{*}{\subseteq} L_p$. Let S be the finite set of primes for which this does not hold. Then for every $p \in S$ there exists an isometry σ_p on $\mathbb{Q}_p L$ such that $M_p \overset{*}{\subseteq} \sigma_p L_p$. Using [13, 81:14], we define a global lattice N in the genus of L by

$$N_p = \begin{cases} L_p & \text{if } p \notin S, \\ \sigma_p L_p & \text{if } p \in S. \end{cases}$$

Then $M_p \overset{*}{\subseteq} N_p$ for all p, and so M is primitively contained in N. Now we choose a vector $v \in N$ such that $M \oplus \mathbb{Z}[v]$ is primitive in N. Then $M \oplus \mathbb{Z}[v]$ is primitively represented by the genus of L and by the strict n-regularity of L we know that $M \oplus \mathbb{Z}[v] \xrightarrow{*} L$. Thus $M \xrightarrow{*} L$ and hence L is strictly $(n-1)$-regular. $\square$

Chapter 2

Preliminaries

In what follows, we always assume that L is an integral $\mathbb{Z}$-lattice on a positive definite quadratic space (V, Q) over $\mathbb{Q}$ of dimension m. For $k \leq m$, a $k \times k$ *section* of L is defined to be the primitive sublattice of L spanned by the first k vectors in a Minkowski reduced basis of L. In general, if $\{x_1, \ldots, x_k\}$ is a Minkowski reduced basis of L, then

- $0 < Q(x_1) < \cdots < Q(x_k)$, and
- $|2B(x_i, x_j)| \leq Q(x_i)$ for $1 \leq i < j \leq k$.

2.1 Successive minima

For $1 \leq j \leq m$ we define the j^{th} *minimum* of L, denoted $\mu_j(L)$, to be the positive integer such that

(1) $\dim(\text{span}\{x \in L : Q(x) \leq \mu_j(L)\}) \geq j$, and

(2) $\dim(\text{span}\{x \in L : Q(x) < \mu_j(L)\}) < j$.

We call the integers $\mu_1(L), \ldots, \mu_m(L)$ the *successive minima* of L. There exist m linearly independent vectors m_j in L such that $Q(m_j) = \mu_j(L)$ [2, Section 12.2]. Moreover, we have the Hadamard inequality [11, Theorem 2.1.1]

$$dL \leq \prod_{j=1}^{m} \mu_j(L).$$

Thus, to bound the discriminant of a lattice it suffices to bound the successive minima of the lattice. The following results will be used in the proof of the main theorem.

Lemma 3. *Let M be a primitive sublattice of L of rank k. If N is a lattice of rank n which is (primitively) represented by L but not (primitively) represented by M, then there exists a constant $C = C(n,k)$ such that*

$$\mu_{k+1}(L) \leq C \max\{\mu_n(N), \mu_k(M)\}.$$

Moreover, the constant C can be taken to be 1 when $\max\{n,k\} \leq 4$.

Proof. Since N is represented by L, we can replace N with an isometric copy inside L and thus consider N as a sublattice of L. In addition, if N is a primitive sublattice of L, then N cannot be a sublattice of M. Therefore in either case we can replace N with a copy in L which is not in M. Let $y_1, \ldots, y_n$ and

$x_1, \ldots, x_k$ be Minkowski reduced bases for N and M respectively. Since N is not a sublattice of M, we know that there exists some $j \in \{1, \ldots, n\}$ such that $y_j \notin M$. Furthermore, y_j cannot be in $\mathbb{Q}M$ since $M \overset{*}{\subseteq} L$. Thus $\mu_{k+1}(L)$ must be bounded by $\max\{Q(y_n), Q(x_k)\}$ since both the $\{y_i\}$ and the $\{x_j\}$ are Minkowski reduced. By [2, Chapter 12, Theorem 3.1] there is a constant C depending on n and k such that

$$\mu_{k+1}(L) \leq C \max\{\mu_n(N), \mu_k(M)\}.$$

By [2, Theorem 3.1], every lattice of rank less than or equal to 4 has a Minkowski basis $\{v_i\}$ such that $Q(v_i)$ is the ith successive minimum of the lattice. Therefore, we can choose C to be 1 in this case. □

We reproduce the following lemmas from [4] because they will be crucial to the main result discussed later.

Lemma 4. *[4, Lemma 3.3] Let M be a $k \times k$ section of L for some $k < rank(L)$. If $\mathfrak{n}(M^{\perp}) \subseteq a\mathbb{Z}$, then $\mu_{k+1}(L) \geq \frac{a}{(dM)^2}$.*

Lemma 5. *[4, Lemma 3.4] Let ℓ be a lattice of rank $k \geq 3$ and let L be a $(k-1)$-regular lattice such that rank$(L) > k$. If $\ell \longrightarrow L$, then $\mu_{k+1}(L) \leq C$ where $C = C(\ell)$ is a constant depending only on ℓ.*

Lemma 6. *[4, Lemma 3.5] Let ℓ be a lattice of rank $k \geq 5$ and let L be a $(k-2)$-regular lattice such that rank$(L) > k$. If $\ell \longrightarrow L$, then $\mu_{k+1}(L) \leq C$ where $C = C(\ell)$ is a constant depending only on ℓ.*

Chan-Earnest-Oh in [3] make use of character sum estimates to prove the following result on bounding the first three minima for regular quadratic lattices of rank at least 4.

Lemma 7. *[3, Corollary 3.2] There exists an absolute constant C_3 such that $\mu_3(L) < C_3$ for all regular lattices of rank at least 4.*

2.2 Watson transformations

In his 1953 Ph.D. thesis, G.L. Watson introduced a family of regularity preserving transformations, later named the Watson transformations by recent authors. Detailed explanations of these transformations can be found in [1] and [4]. For an R-lattice L, where R is $\mathbb{Z}$ or $\mathbb{Z}_p$, and a positive integer r we define the Watson transformation of L at r to be

$$\Lambda_r(L) = \{x \in L : Q(x+y) - Q(y) \equiv 0 \mod r \text{ for all } y \in L\}.$$

We use these transformations to associate with L a new lattice that represents more integers, but in a way that preserves regularity conditions. For our purposes, $r = 2p$, where p is any prime. We will want to continue to work with normalized lattices, and so $\lambda_{2p}(L)$ will denote $\Lambda_{2p}(L)$ after a suitable scaling by which $\mathfrak{n}\lambda_{2p}(L) = 2\mathbb{Z}$. There are some basic properties of these transformation that will be used. The proof of the following proposition can be found in [1].

Proposition 4. *[1, Proposition 2.1] Let L be a normalized $\mathbb{Z}$-lattice and let p be a prime. The operation λ_{2p} satisfies the following properties:*

1. $(\lambda_{2p}(L))_p = \lambda_{2p}(L_p)$.

2. *For any prime $q \neq p$*

$$\lambda_{2p}(L_q) = L_q^{\eta}$$

   where $\eta \in \mathbb{Z}_q^{\times}$. In particular, L_q is universal if and only if $\lambda_{2p}(L_q)$ is universal.

3. *For any prime q*

$$\lambda_{2p}(\lambda_{2q}(L)) = \lambda_{2q}(\lambda_{2p}(L)).$$

4. *If L and L' are in the same genus, then so are $\lambda_{2p}(L)$ and $\lambda_{2p}(L')$.*

5. *For each $\mathbb{Z}$-lattice M' in the genus of $\lambda_{2p}(L)$ there is a lattice M in the genus of L such that $\lambda_{2p}(M) = M'$.*

The following lemmas from [4] describe the structure of the new lattice $\Lambda_{2p}(L)$. Suppose that for any prime p, $L_p = M_p \perp N_p$ where M_p is the leading Jordan component and $\mathfrak{s}N_p \subseteq p\mathfrak{s}M_p$.

Lemma 8. *[4, Lemma 2.1] Suppose M_p is unimodular and $\mathfrak{n}N_p \subseteq 2p\mathbb{Z}_p$. Then*

$$\Lambda_{2p}(L)_p = pM_p \perp N_p.$$

The next two lemmas from [4] specifically discuss the application of λ_4 when $\mathfrak{s}L = 2\mathbb{Z}$.

Lemma 9. *[4, Lemma 2.3] Suppose $\mathfrak{s}L = 2\mathbb{Z}$ and $\mathfrak{s}N_2 \subseteq 8\mathbb{Z}_2$.*

1. *If rank$(M_2) \geq 3$ then $\lambda_4(L)_2$ is split by a unimodular $\mathbb{Z}_2$-lattice.*

2. *If rank$(M_2) = 2$ then*

$$\lambda_4(L_2) \cong \begin{cases} M_2^3 \perp N_2^{\frac{1}{2}} & \text{if } \frac{dM}{4} \equiv 5 \mod 8, \\ M_2 \perp N_2^{\frac{1}{2}} & \text{if } \frac{dM}{4} \equiv 1 \mod 4, \\ \mathbb{P} \perp N_2^{\frac{1}{4}} & \text{if } \frac{dM}{4} \equiv 3 \mod 4, \end{cases}$$

   where $\mathbb{P}$ is an even binary unimodular $\mathbb{Z}_2$-lattice.

3. *If rank$(M_2) = 1$ then $\lambda_4(L_2) \cong M_2 \perp N_2^{\frac{1}{4}}$.*

Lemma 10. *[4, Lemma 2.4] If rank$(M_2) = 1$ and $N_2 = J_2 \perp K_2$ where J_2 is a (4)-modular $\mathbb{Z}_2$-lattice and $\mathfrak{s}K_2 \subseteq 8\mathbb{Z}_2$ then*

$$\lambda_4(L_2) \cong \begin{cases} M_2^2 \perp N_2^{\frac{1}{2}} & \text{if } J_2 \text{ is proper}, \\ M_2 \perp N_2^{\frac{1}{4}} & \text{if } J_2 \text{ is improper}. \end{cases}$$

In particular, since $2p^2\mathbb{Z} \subseteq \mathfrak{n}\Lambda_{2p}(L) \subseteq 2p\mathbb{Z}$, it follows that $\lambda_{2p}(L) = (\Lambda_{2p}(L))^l$ where $l = \frac{1}{p}$ or $l = \frac{1}{p^2}$. The Watson transformation operation was created to work with the sets $\{x \in L : Q(x) \equiv 0 \mod r\}$, however, this set is not always equal to $\Lambda_r(L)$. In the following propositions we show when these two sets are equal.

Proposition 5. *Let L be a normalized $\mathbb{Z}$-lattice.*

(1) If $\mathfrak{s}(L) = 2\mathbb{Z}$ then

$$\Lambda_4(L_2) = \{x \in L_2 : Q(x) \in 4\mathbb{Z}\}.$$

(2) If $Q(L_p) \neq 2\mathbb{Z}_p$ then

$$\Lambda_{2p}(L_p) = \{x \in L_p : Q(x) \in 2p\mathbb{Z}_p\}.$$

Proof. For (1) it follows from the definition of the Watson transformation that

$$\begin{aligned}\Lambda_4(L_2) &= \{x \in L_2 : Q(x+y) - Q(y) \in 4\mathbb{Z}_2\} \\ &= \{x \in L_2 : 2B(x,y) + Q(x) \in 4\mathbb{Z}_2\}.\end{aligned}$$

From our assumptions on the scale of L, we see that $B(x,y) \equiv 0 \mod 2$. Thus we have that

$$\Lambda_4(L_2) = \{x \in L_2 : Q(x) \in 4\mathbb{Z}_2\}.$$

Now we prove (2). If $p = 2$, then we suppose that $\mathfrak{s}L_2 = \mathbb{Z}_2$, otherwise $\mathfrak{s}L_2 = 2\mathbb{Z}_2$ and we are done. From our assumptions on the scale and norm of L, we know that L_p must have a unimodular component. Additionally, since $Q(L_p) \neq 2\mathbb{Z}_p$, it must be the case that the unimodular component is anisotropic. Then we write L_p as $L_p = M_p \perp N_p$, where M_p is anisotropic unimodular and $\mathfrak{s}N_p \subseteq 2p\mathbb{Z}_p$. By Lemma 8 we see that $\Lambda_{2p}(L_p) = pM_p \perp N_p$, and thus

$$\Lambda_{2p}(L_p) = \{x \in L_p : Q(x) \in 2p\mathbb{Z}_p\}.$$

□

Lemma 11. *Let K_p be a $\mathbb{Z}_p$-lattice. Then for any isometry σ_p of K_p,*

$$\Lambda_{2p}(\sigma_p(K_p)) = \sigma_p(\Lambda_{2p}(K_p)).$$

Proof. Let $x \in \Lambda_{2p}(\sigma_p(K_p))$ and $x' \in K_p$ such that $x = \sigma_p(x')$. Then for any $y \in \sigma_p(K_p)$ we have that $Q(x+y)-Q(y) \in 2p\mathbb{Z}_p$. Consequently, $Q(x'+y')-Q(y') \in 2p\mathbb{Z}_p$ for all $y' \in K_p$. By definition, $x' \in \Lambda_{2p}(K_p)$ and thus $x \in \sigma_p(\Lambda_{2p}(K_p))$.

Conversely, let $x \in \sigma_p(\Lambda_{2p}(K_p))$. Then there exists an $x' \in \Lambda_{2p}(K_p)$ such that $x = \sigma_p(x')$, and $Q(x'+y')-Q(y') \in 2p\mathbb{Z}_p$ for all $y' \in K_p$. By applying σ_p we see that $Q(x+y)-Q(y) \in 2p\mathbb{Z}_p$ for all $y \in \sigma_p(K_p)$. Thus $x \in \Lambda_{2p}(\sigma_p(K_p))$. □

Lemma 12. *Let L be a normalized $\mathbb{Z}$-lattice and either $\mathfrak{s}L_2 = 2\mathbb{Z}_2$ when $p = 2$ or $Q(L_p) \neq 2\mathbb{Z}_p$. Then:*

1. *If $K \overset{*}{\subseteq} \Lambda_{2p}(L_p)$ then $\Lambda_{2p}(\mathbb{Q}_pK \cap L_p) = K$.*
2. *If σ is a primitive representation of a $\mathbb{Z}_p$-lattice K by L_p, then $\sigma(\Lambda_{2p}(K))$ is a primitive sublattice of $\Lambda_{2p}(L_p)$.*

Proof. For the first claim, let $x \in \Lambda_{2p}(\mathbb{Q}_pK \cap L_p)$. Then $x \in \mathbb{Q}_pK$ and $x \in L_p$ such that $Q(x) \in 2p\mathbb{Z}_p$. Thus, by Proposition 5, $x \in (\mathbb{Q}_pK \cap \Lambda_{2p}(L_p)) = K$ since K is primitive in $\Lambda_{2p}(L_p)$. Now let $x \in K = (\mathbb{Q}_pK \cap \Lambda_{2p}(L_p))$. Then $x \in \mathbb{Q}_pK \cap L_p$

such that $Q(x+y)-Q(y) \in 2p\mathbb{Z}_p$ for all $y \in L_p$. Since $\mathbb{Q}_pK \cap L_p \subseteq L_p$ we have that $Q(x+y)-Q(y) \in 2p\mathbb{Z}_p$ for all $y \in \mathbb{Q}_pK \cap L_p$. Thus $x \in \Lambda_{2p}(\mathbb{Q}_pK \cap L_p)$.

We now prove the second assertion. Notice that $\sigma(\Lambda_{2p}(K)) = \Lambda_{2p}(\sigma(K))$ by Lemma 11, and if $x \in \sigma(\Lambda_{2p}(K))$ then $x \in L_p$ such that $Q(x) \in 2p\mathbb{Z}_p$. Hence $\sigma(\Lambda_{2p}(K)) \subseteq \Lambda_{2p}(L_p)$ by Proposition 5. We need to show that $\Lambda_{2p}(L_p)/\sigma(\Lambda_{2p}(K))$ is torsion free. Let $x \in \Lambda_{2p}(L_p)$ such that $rx \in \sigma(\Lambda_{2p}(K))$ for some $r \in \mathbb{Z}$, $r \neq 0$. Since $\sigma(\Lambda_{2p}(K)) \subseteq \sigma(K)$ and $L_p/\sigma(K)$ is torsion free, it must be the case that $x \in \sigma(K)$. Additionally, since $x \in \Lambda_{2p}(L_p)$ it must be that $Q(x+y)-Q(y) \in 2p\mathbb{Z}$ for all $y \in L_p$. Since $\sigma(K) \subseteq L_p$, we have that $Q(x+y)-Q(y) \in 2p\mathbb{Z}$ for all $y \in \sigma(K)$. Hence $x \in \Lambda_{2p}(\sigma(K)) = \sigma(\Lambda_{2p}(K))$. Then $\Lambda_{2p}(L_p)/\sigma(\Lambda_{2p}(K))$ is torsion free and $\sigma(\Lambda_{2p}(K))$ is a primitive sublattice of $\Lambda_{2p}(L_p)$. □

It will be necessary to know when the strict n-regularity of a lattice is preserved through applications of the Watson transformation.

Proposition 6. *If L is a strictly n-regular normalized quadratic $\mathbb{Z}$-lattice such that $\mathfrak{s}L = 2\mathbb{Z}$ or $Q(L_p) \neq 2\mathbb{Z}_p$, then $\Lambda_{2p}(L)$ is strictly n-regular.*

Proof. Suppose N is a lattice of rank n that is primitively represented by the genus of $\Lambda_{2p}(L)$. If $q \neq p$, then $(\Lambda_{2p}(L))_q = \Lambda_{2p}(L_q) = L_q$, and hence $N_q \xrightarrow{*} L_q$. Otherwise, from Proposition 4 we know that

$$(\Lambda_{2p}(L))_p = \Lambda_{2p}(L_p) = \{x \in L_p : Q(x) \in 2p\mathbb{Z}_p\}.$$

Since $N_p \xrightarrow{*} \Lambda_{2p}(L_p)$, there is a primitive sublattice H_p of $\Lambda_{2p}(L_p)$ such that $\sigma_p H_p = N_p$ for some isometry σ_p of $\mathbb{Q}_p L$. Using [13, 81:14], we define a lattice G on $\mathbb{Q}N$ by

$$G_q = \begin{cases} N_q & \text{if } q \neq p, \\ \sigma_p(\mathbb{Q}_p H_p \cap L_p) & \text{if } q = p. \end{cases}$$

Note that $N \subseteq G$ since $N_q \subseteq G_q$ at every prime q. We claim that $\Lambda_{2p}(G_p) = N_p$. By Lemma 11,

$$\Lambda_{2p}(G_p) = \Lambda_{2p}(\sigma_p(\mathbb{Q}_p H_p \cap L_p) = \sigma_p(\Lambda_{2p}(\mathbb{Q}_p H_p \cap L_p)).$$

Since H_p is primitive in $\Lambda_{2p}(L_p)$, we apply Lemma 12 and see that $\Lambda_{2p}(G_p) = \sigma_p(H_p)$. Hence, $\Lambda_{2p}(G_p) = N_p$. For $q \neq p$, $\Lambda_{2p}(G_q) = G_q = N_q$. Thus, $\Lambda_{2p}(G) = N$.

The lattice $\mathbb{Q}_p H_p \cap L_p$ is primitively contained in L_p. Therefore, $G_p \xrightarrow{*} L_p$. By the strict n-regularity of L, G is primitively represented by L and thus, by Lemma 12, $\Lambda_{2p}(G) \xrightarrow{*} \Lambda_{2p}(L)$. Thus $N \xrightarrow{*} \Lambda_{2p}(L)$, and so Λ_{2p} preserves strict n-regularity. □

Proposition 7. *Let L be a strictly n-regular normalized $\mathbb{Z}$-lattice with rank $L \geq 5$. For any prime p, there exists a strictly n-regular normalized lattice $\Delta_p(L)$ such that $\Delta_p(L)_p$ represents every element in $2\mathbb{Z}_p$ and $\Delta_p(L)_q$ is isometric to L_q up to a scaling factor for all $p \neq q$. Additionally, we can ensure that $\Delta_p(L)_p$ represents $\mathbb{H}$.*

This proposition follows from Lemmas 8, 9, 10, and Proposition 6. For more detail, the reader is referred to the proof of the analogous statement for n-regular lattices in [4, Theorem 2.5].

The proof of Proposition 7 requires a number of applications of λ_{2p}. In practice, we will only apply the proposition for a bounded prime p, meaning p does not depend on the lattice L, when the number of applications of λ_{2p} is clearly bounded as well. If this is the case, we say that p is *admissible* to L. If $S = \{p_1, \ldots, p_s\}$ is a finite set of primes each of which is admissible to L, we say that S is admissible to L and define

$$\Delta_S(L) = \Delta_{p_1}(\ldots(\Delta_{p_s}(L))).$$

Note that by Proposition 4 [3], the order of the Δ_{p_i} in this definition does not alter $\Delta_S(L)$. We claim that if S is admissible to L, then $\mu_i(L)$ is bounded if $\mu_i(\Delta_S(L))$ is also bounded.

Proposition 8. *Let S be a finite set of primes admissible to a $\mathbb{Z}$-lattice L of rank m. For $1 \leq i \leq m$, if $\mu_i(\Delta_S(L))$ is bounded then $\mu_i(L)$ is bounded.*

Proof. For any prime q, $\Lambda_{2q}(L) \subseteq L$ and thus it is clear that if $\mu_i(\Lambda_{2q}(L))$ is bounded then $\mu_i(L)$ is bounded. When we consider $\lambda_{2q}(L)$ we are simply scaling the quadratic map of $\Lambda_{2q}(L)$ by $\frac{1}{q}$ or $\frac{1}{q^2}$. Thus if $\mu_i(\lambda_{2q}(L))$ is bounded and q is bounded, then $\mu_i(L)$ is bounded.

Since S is admissible to L, we know that for each prime $q \in S$, q is bounded and the number of applications of λ_{2q} is bounded. Additionally, there are only finitely many primes in S. Thus, if $\mu_i(\Delta_S(L))$ is bounded then $\mu_i(L)$ is bounded as well. □

Proposition 9. *Let M be a quaternary $\mathbb{Z}_p$-lattice.*

(1) The lattice $\lambda_{2p}(M)$ is isotropic if and only if M is isotropic.

(2) If dM is a square in $\mathbb{Z}_p$ then $d\lambda_{2p}(M)$ is a square in $\mathbb{Z}_p$.

Proof. For the proof of (1), recall that $\lambda_{2p}(M)$ is a lattice on $\mathbb{Q}_pM$. Since $\lambda_{2p}(M)$ is obtained by scaling the quadratic map on $\Lambda_{2p}(M)$, we see that $\lambda_{2p}(M)$ is isotropic (or anisotropic) if M is isotropic (or anisotropic).

For the second assertion, recall that $\Lambda_{2p}(M) \subseteq M$ and thus $d\Lambda_{2p}(M) = dM[M : \Lambda_{2p}(M)]^2$. Since dM is a square in $\mathbb{Z}_p$ it is now clear that $d\Lambda_{2p}(M)$ is a square as well. Then by applying λ_{2p} we are simply scaling the bilinear map by some fixed amount $l = \frac{1}{p}$ or $l = \frac{1}{p^2}$. Thus $d\lambda_{2p}(M) = l^4 d\Lambda_{2p}(M)$. □

In the proof of the main result, when there is a set S of primes admissible to L we will apply Proposition 7 and work with the new lattice $\Delta_S(L)$, thanks to Proposition 8. For the sake of clarity, we will still refer to the lattice as L with the understanding that we have applied the necessary Watson transformations. If M is a primitive sublattice of L of rank ℓ with bounded discriminant, then

after applying Proposition 7 to L for some admissible set S, M will refer to the new sublattice of L obtained by applying to M the same Watson transformations and scalings as required of L. Since S is admissible and by Lemma 12, it should be clear that this new M is also a primitive sublattice of the new L of rank ℓ and M has bounded discriminant.

Chapter 3

Main Result

In what follows, L refers to a positive definite normalized quadratic $\mathbb{Z}$-lattice, which is strictly n-regular of rank $n+4$. We say a quantity is bounded if it is bounded by an absolute constant. For a $\mathbb{Z}_q$-lattice G, let $\mathfrak{l}(G)$ denote the last Jordan component of a Jordan decomposition of G.

3.1 Propositions

We will use the strict n-regularity of L to bound the successive minima of L. Therefore, it will be crucial to construct primitive sublattices of rank n. It is not always the case, however, that a sublattice whose basis vectors are primitive vectors of L is itself a primitive sublattice. The following lemma will then be used in the construction of primitive sublattices of L.

Lemma 13. *Let L_p be a quadratic $\mathbb{Z}_p$-lattice and let N_p be a primitive sublattice of L_p. Suppose v is in the orthogonal complement of N_p such that $\mathbb{Z}_p[v]$ splits L_p. If $w \in L$ such that $B(N_p \perp \mathbb{Z}_p[v], w) = 0$ then $N_p \perp \mathbb{Z}_p[v+w]$ is a primitive sublattice of L_p.*

Proof. Let $E_p = N_p \perp \mathbb{Z}_p[v+w]$. To show that E_p is a primitive sublattice of L_p, it suffices to show that L_p/E_p is torsion free. Proceeding by contradiction, suppose $y \in L_p$ represents a torsion element in L_p/E_p. Then there exists an $r \in p\mathbb{Z}_p$ such that $ry = x + a(v+w) \in E_p$, where $x \in N_p$ and $a \in \mathbb{Z}_p$. Note that we can assume that ry is a primitive element of E_p, so $x \overset{*}{\in} N_p$ or $a \in \mathbb{Z}_p^\times$. Since $L_p = L_p' \perp \mathbb{Z}_p[v]$, we can write y uniquely as $y = l + bv$ where $b \in \mathbb{Z}_p$ and $l \in L_p'$. However, we also know that $y = \frac{1}{r}x + \frac{a}{r}(v+w) = \frac{1}{r}(x+aw) + \frac{a}{r}v$. As a result, $r \mid a$, which implies $a \notin \mathbb{Z}_p^\times$ and hence $x \overset{*}{\in} N_p$. But then $x \overset{*}{\in} L_p$ since $N_p \overset{*}{\subseteq} L_p$. Therefore, $\frac{1}{r}x \notin L_p$ which is a contradiction since y and $\frac{a}{r}(v+w)$ are in L_p. Hence L_p/E_p is torsion free. □

The following is essential to the proof of the main theorem for $n \geq 3$.

Proposition 10. *Let M be a lattice of rank $n \geq 6$ and L be a strictly $(n-3)$-regular lattice of rank $> n$. If $M \xrightarrow{*} L$, then $\mu_{n+1}(L)$ is bounded by a constant depending only on M.*

Proof. Let p be a prime such that $p \nmid 2dM$ and $-dM \notin (\mathbb{Z}_p^\times)^2$ if $n = 6$. Since

M_p is unimodular,

$$M_p \cong \langle 1, \ldots, 1, dM \rangle$$

$$\cong \mathbb{H} \perp \mathbb{H} \perp \langle 1, -\Delta \rangle \perp T,$$

where T is a unimodular sublattice of rank $n-6$. Then M_p contains a primitive sublattice isometric to

$$\langle -p \rangle \perp \langle p\Delta \rangle \perp T.$$

Let $\{x_{1,p}, \ldots, x_{n-4,p}\}$ be a basis for this lattice. For primes $q \mid 2dM$, let $\{x_{1,q}, \ldots, x_{n-4,q}\}$ be a basis for a primitive sublattice of M_q of rank $n-4$. By applying [9, Lemma 1.6], we obtain a lattice

$$N = \mathbb{Z}[x_1] \oplus \ldots \oplus \mathbb{Z}[x_{n-4}]$$

such that x_i is sufficiently close to $x_{i,q}$ for $1 \leq i \leq n-4$ and for all $q \mid 2pdM$. In particular, $N_q \cong \mathbb{Z}_q[x_{1,q}, \ldots, x_{n-4,q}]$ and $N_q \overset{*}{\subseteq} M_q$ for all $q \mid 2pdM$. Additionally, for all but one primes q that do not divide $2pdM$ we have $dN \in \mathbb{Z}_q^\times$, and at the exceptional case we have $dN \in q\mathbb{Z}_q^\times \cup \mathbb{Z}_q^\times$. As a consequence, $N_q \overset{*}{\subseteq} M_q$ for all primes q and hence $N \overset{*}{\subseteq} M$. Since $p > 2$ and N_p and $T \perp \langle -p, p\Delta \rangle$ are isometric primitive sublattices of the unimodular $\mathbb{Z}_p$-lattice M_p, we know that their orthogonal complements in M_p are isometric [10, Corollary 5.4.1]. Thus the orthogonal complement of N_p in M_p is isometric to $\langle 1, -\Delta, p, -p\Delta \rangle$.

Choose $a \in \mathbb{Z}$ such that a is represented by the orthogonal complement of N in M. Write $a = p^e a_0$ where $p \nmid a_0$. By Proposition 1, we know that no element

of $p^2\mathbb{Z}_p$ is primitively represented by $\langle 1, -\Delta, p, -p\Delta\rangle$. However, we claim that $N_p \perp \langle p^2 a\rangle \xrightarrow{*} L_p$ or $N_p \perp \langle p^4 a\rangle \xrightarrow{*} L_p$. Write $L_p = M_p \perp \mathbb{Z}_p[v]$, where $Q(v) = p^t u$ and $u \in \mathbb{Z}_p^\times$. Since $\langle 1, -\Delta, p, -p\Delta\rangle$ is universal over $\mathbb{Z}_p$, it must represent $-p^t u$ and a. Let x, w be the vectors such that $Q(w) = -p^t u$ and $Q(x) = a$.

If $e + 2 \geq t$, let z be defined as

$$z = \Big(\frac{a_0}{4u} - p^{\alpha - t}\Big)w + \Big(\frac{a_0}{4u} + p^{\alpha - t}\Big)v,$$

where $\alpha = e+4$ if $t = e+2$ and $\alpha = 2+e$ otherwise. In this case, $\frac{a_0}{4u} + p^{\alpha-t} \in \mathbb{Z}_p^\times$. Then $z \overset{*}{\in} L_p$ such that $Q(z) = p^4 a$ or $Q(z) = p^2 a$. Hence if $e + 2 \geq t$ we have $\langle p^4 a\rangle \xrightarrow{*} L_p$ or $\langle p^2 a\rangle \xrightarrow{*} L_p$. On the other hand, if $e + 2 < t$, then

$$\begin{aligned} Q(px + v) &= p^2 a + p^t u \\ &= p^{e+2}(a_0 + p^{t-(e+2)}u). \end{aligned}$$

By [13, 63.1], there exists $\lambda \in \mathbb{Z}_p^\times$ such that $a_0 = (a_0 + p^{t-(e+2)}u)\lambda^2$. Then $z = \lambda p x + \lambda v$ is a primitive vector in L_p such that $Q(z) = p^2 a$. Hence if $e + 2 < t$, we have that $\langle p^2 a\rangle \xrightarrow{*} L_p$.

Thus, we have found a primitive vector z in the orthogonal complement of N_p in L_p such that $Q(z) = p^{2+\epsilon} a$, where

$$\epsilon = \begin{cases} 0 & \text{if } e + 2 \neq t, \\ 2 & \text{if } e + 2 = t. \end{cases}$$

Since z can be written as $z_0 + \delta v$ where $\delta \in \mathbb{Z}_p^\times$ and $B(z_0, N) = B(z_0, v) = 0$, we can apply Lemma 13, which implies that $N_p \perp \mathbb{Z}_p[z]$ is a primitive sublattice of L_p. Let y be a vector in the orthogonal complement of N in L such that $Q(y) = p^{2+\epsilon}a$. Define $K \subseteq L$ by

$$K_q = \begin{cases} N_p \perp \mathbb{Z}_p[y] & \text{if } q = p \\ \mathbb{Q}_q(N_q \perp \mathbb{Z}_q[y]) \cap L_q & \text{if } q \neq p. \end{cases}$$

Since $p^2\mathbb{Z}_p \overset{*}{\not\longrightarrow} \langle 1, -\Delta, p, -p\Delta \rangle$, we know that $N_p \perp \mathbb{Z}_p[y] \overset{*}{\not\longrightarrow} M_p$ and hence K_p is not primitively represented by M_p. Thus it must be the case that K is not primitively represented by M. However, if $q \neq p$, then $K_q \overset{*}{\subseteq} L_q$. At the prime p, $K_p \overset{*}{\longrightarrow} L_p$ since $N_p \perp \mathbb{Z}_p[z] \overset{*}{\longrightarrow} L_p$. Thus by the strict $(n-3)$-regularity, $K \overset{*}{\longrightarrow} L$. Since $N \perp \langle p^{2+\epsilon}a \rangle \subseteq K$, we must have

$$\mu_{n-3}(K) \leq C \max\{\mu_{n-4}(N), p^{2+\epsilon}a\},$$

where C is a constant depending only on M. This means that $\mu_{n-3}(K)$ is bounded by a constant depending only on M. It follows then that $\mu_{n+1}(L)$ is also bounded by a constant depending only on M since

$$\mu_{n+1}(L) \leq C \max\{\mu_{n-3}(K), \mu_n(M)\}$$

by Lemma 3. □

The remaining propositions in this section will be used to prove the main theorem in the case when $n = 2$.

Proposition 11. *Let L be a normalized strictly 2-regular lattice. Let M be a quaternary primitive sublattice in L of bounded discriminant and let a be the generator of $\mathfrak{n}M^{\perp}$. If M is anisotropic at some prime ℓ, then $p^{ord_p(a)}$ is bounded for all $p \neq \ell$.*

Proof. Fix a full rank sublattice $M' := \langle u, v\rangle \perp B \subseteq M$. Write $u = \ell^{\mathrm{ord}_\ell(u)}u'$ and $v = \ell^{\mathrm{ord}_\ell(v)}v'$ such that $\ell \nmid u'v'$. Choose an integer β such that β is the smallest positive integer satisfying

(1) $\beta \equiv \mathrm{ord}_\ell(uv) \mod 2$,

(2) $\beta \geq \max\{\mathrm{ord}_\ell(\mathfrak{l}(M)), \mathrm{ord}_\ell(a)\}$.

Choose a prime s such that

(3)
- if $\ell \neq 2$ then $\left(\frac{s}{\ell}\right) = \left(\frac{-u'v'}{\ell}\right)$, and
- if $\ell = 2$ then $s \equiv -u'v' \mod 8$.

(4) If $p \neq \ell$ and $p \mid 2dM'$ then

- if $p \neq 2$ then $\left(\frac{s}{p}\right) = \left(\frac{\ell^\beta}{p}\right)$, and
- if $p = 2$ then $s \equiv \ell^\beta \mod 8$.

Note that with this construction $\beta - \mathrm{ord}_\ell(a)$ is bounded and the choice of s depends only on M, so s can be chosen to be bounded. Let $K = \langle u, \ell^{\beta+\delta}vs\rangle$,

where $\delta = 4$ if $\ell = 2$ and $\delta = 0$ otherwise. Then $\mathbb{Q}_\ell K \cong \mathbb{H}$. Since M_ℓ is anisotropic, $\mathbb{Q}_\ell K \not\to \mathbb{Q}_\ell M$ and thus K is not represented by M.

We claim that K is in fact represented by L. For $p \neq \ell$, if $p \nmid 2dM'$ then $p \nmid dM$, and M_p is unimodular. In this case, M_p is 2-universal. On the other hand, if $p \mid 2dM'$, then $s\ell^{\beta+\delta} \in (\mathbb{Z}_p^\times)^2$ and $K_p \longrightarrow M_p$. Finally, by Claim 1 in Section 4.2, $K_\ell \longrightarrow L_\ell$. Thus K is represented by L via the 2-regularity of L, but $K \not\to M$.

By Lemma 4,

$$p^{\mathrm{ord}_p(a)}\ell^{\mathrm{ord}_\ell(a)} \leq (dM)^2\ell^{\beta+\delta}uvs.$$

Since $\ell \mid dM$, ℓ is bounded and $\beta - \mathrm{ord}_\ell(a)$ is bounded. Thus we conclude that $p^{\mathrm{ord}_p(a)}$ is also bounded. □

The following two propositions will be used to bound the fifth successive minimum in the proof of the main theorem. The argument of the proof depends greatly on the discriminant of M in Proposition 11, and thus we break the proof into two cases. For the next two propositions, suppose L is a strictly 2-regular lattice of rank 6 such that $\mu_4(L)$ is bounded. Let M be a quaternary primitive sublattice in L of bounded discriminant, for example, a (4×4)-section of L. Let a be the generator of $\mathfrak{n}M^\perp$. Note that dM is bounded.

Proposition 12. *If dM is not a square, then $\mu_5(L)$ is bounded.*

Proof. Let p be a prime such that $p \nmid 2dM$ and dM is a nonsquare modulo p.

Since M_p is unimodular, $M_p \cong \langle 1, -\Delta, 1, -1\rangle$, where Δ is a nonsquare in $\mathbb{Z}_p^\times$. Then M_p contains a primitive sublattice isometric to $\langle 1, -\Delta, p\rangle \perp \langle -p\rangle$. Let $z_p \in M_p$ such that $Q(z_p) = -p$. It must be the case that z_p is a primitive vector in M_p, hence the orthogonal complement of $\mathbb{Z}_p[z_p]$ in M_p is isometric to $\langle 1, -\Delta, p\rangle$ [10, Corollary 5.4.1].

For each $q \mid 2dM$, let z_q be a primitive vector of M_q. By applying [9, Lemma 1.6] we obtain $z \in M$ such that z is sufficiently close to z_q for all $q \mid 2pdM$, and $Q(z) \in q\mathbb{Z}_q^\times \cup \mathbb{Z}_q^\times$ for all $q \nmid 2pdM$. Then $z \overset{*}{\in} M$. We let T be the orthogonal complement of $\mathbb{Z}[z]$ in M. By [10, Corollary 5.4.1] T_p is isometric to $\langle 1, -\Delta, p\rangle$. Choose $x_p, y_p \in T_p$ such that $Q(x_p) = 1$ and $Q(y_p) = \Delta$, and let x_q, y_q be primitive vectors in T_q for $q \mid 2dM$. By [9, Lemma 1.6] we obtain $x, y \overset{*}{\in} T$ such that $Q(x) \in (\mathbb{Z}_p^\times)^2$ and $Q(y) \in \Delta(\mathbb{Z}_p^\times)^2$. The orthogonal complement of $\langle -p\rangle$ in M_p must be isometric to T_p and by Proposition 1, T_p does not primitively represent any element of $p^2\mathbb{Z}_p$. Then $\langle -p, p^2\rangle \overset{*}{\not\longrightarrow} M_p$ and $\langle -p, p^2\Delta\rangle \overset{*}{\not\longrightarrow} M_p$. We claim that either $\langle -p, p^2\rangle$ or $\langle -p, p^2\Delta\rangle$ is primitively represented by L_p.

Suppose that the orthogonal complement of M_p in L_p is isometric to $\langle p^{t_1}u_1, p^{t_2}u_2\rangle$, where $t_1, t_2 \in \mathbb{N}$ with $t_1 \leq t_2$ and $u_1, u_2 \in \mathbb{Z}_p^\times$. First suppose $t_1 = 0$. Since $-u_1 + p^2u_2 \longrightarrow T_p$, L_p primitively represents p^2u_2. If $t_1 = t_2 = 1$, then $p^2u_2 - pu_2 \longrightarrow T_p \perp \langle pu_1\rangle$ and L_p primitively represents p^2u_2. If $t_2 = 2$, then clearly $p^2u_2 \overset{*}{\longrightarrow} L_p$. Lastly, suppose $t_2 \geq 3$. Then $p^2u_2 \longrightarrow T_p$, and $p^2(u_2 + p^{t_2-2}u_2) \overset{*}{\longrightarrow} L_p$. By [13, 63.1] there exists $\lambda \in \mathbb{Z}_p^\times$ such that $\lambda^2(u_2 +$

$p^{t_2-2}u_2) = u_2$. Thus, $p^2u_2 \xrightarrow{*} L_p$. Therefore, in any case we can find vectors $v \overset{*}{\in} M_p^{\perp}$ and $w \in T_p$ such that $Q(v+w) = p^2u_2$. By Lemma 13, $\langle -p, p^2u_2\rangle$ is primitively represented by L_p.

Define $z' \in M$ by

$$z' = \begin{cases} px & \text{if } \left(\frac{u_2}{p}\right) = 1 \\ py & \text{if } \left(\frac{u_2}{p}\right) = -1, \end{cases}$$

and $K \subseteq L$ by

$$K_q = \begin{cases} \mathbb{Z}_p[z, z'] & \text{if } q = p \\ (\mathbb{Q}[z, z'] \cap L)_q & \text{if } q \neq p. \end{cases}$$

Then $K_p \overset{*}{\not\to} M_p$, so $K \overset{*}{\not\to} M$. However, K_q is primitively represented by L_q for every prime q. By the strict 2-regularity of L, L primitively represents K. Thus by Lemma 3,

$$\mu_5(L) \leq \max\{\mu_2(K), \mu_4(M)\},$$

and so $\mu_5(L)$ is bounded by a constant depending on M. □

Proposition 13. *If dM is a square, then $\mu_5(L)$ is bounded.*

Proof. Assume dM is a square. By Lemma 1, there is a prime ℓ such that M_ℓ is anisotropic. Since $\ell \mid dM$, ℓ is bounded. By Proposition 11, $p^{\mathrm{ord}_p(a)}$ is bounded for all $p \neq \ell$. If there are in fact two primes at which M is anisotropic, then by applying Proposition 11 twice, once at ℓ and the second at the other anisotropic

prime, we get that a is bounded. We use a construction similar to that in the proof of Proposition 11 to show that, in this case, $\mu_5(L)$ is also bounded.

Fix a full rank sublattice $M' := \langle u, v\rangle \perp B \subseteq M$. Write $u = \ell^{\mathrm{ord}_\ell(u)}u'$ and $v = \ell^{\mathrm{ord}_\ell(v)}v'$ such that $\ell \nmid u'v'$. Choose an integer β such that β is the smallest positive integer satisfying

(1) $\beta \equiv \mathrm{ord}_\ell(uv) \mod 2$,

(2) $\beta \geq \max\{\mathrm{ord}_\ell(\mathfrak{l}(M)), \mathrm{ord}_\ell(a)\}$.

Choose a prime s such that

(3)
- if $\ell \neq 2$ then $\left(\frac{s}{\ell}\right) = \left(\frac{-u'v'}{\ell}\right)$, and
- if $\ell = 2$ then $s \equiv -u'v' \mod 8$.

(4) If $p \neq \ell$ and $p \mid 2dM'$ then
- if $p \neq 2$ then $\left(\frac{s}{p}\right) = \left(\frac{\ell^\beta}{p}\right)$, and
- if $p = 2$ then $s \equiv \ell^\beta \mod 8$.

Note that with this construction s and β can be chosen to be bounded. Let $K = \langle u, \ell^{\beta+\delta}vs\rangle$, where $\delta = 4$ if $\ell = 2$ and $\delta = 0$ otherwise. Then $\mathbb{Q}_\ell K \cong \mathbb{H}$. Since M_ℓ is anisotropic, $\mathbb{H} \not\to \mathbb{Q}_\ell M$ and hence K is not represented by M.

However, K is represented by L. For $p \neq \ell$, if $p \nmid 2dM'$ then $p \nmid dM$, and M_p is unimodular. In this case, M_p is isometric to $\mathbb{H} \perp \mathbb{H}$ and K is thus represented

by M. On the other hand, if $p \mid 2dM'$, then $s\ell^{\beta+\delta} \in (\mathbb{Z}_p^\times)^2$ and $K_p \longrightarrow M_p$. Finally, $K_\ell \longrightarrow L_\ell$ by Claim 1 proved in Section 4.2. Thus $K \longrightarrow L$ by the 2-regularity of L, but $K \not\longrightarrow M$.

By Lemma 3,

$$\mu_5(L) \leq \max\{u, \ell^{\beta+\delta}vs, \mu_4(M)\}.$$

Thus we may conclude that ℓ is the only prime at which M is anisotropic.

For a prime p, fix a Jordan decomposition of L_p for which $\{v_{1,p}, \ldots, v_{6,p}\}$ is a basis. For $1 \leq i \leq 6$, let $\gamma_{i,p}$ be the p-adic order of the norm ideal of the Jordan component that contains $v_{i,p}$. Then by the definition of Jordan decompositions, $\gamma_{1,p} \leq \ldots \leq \gamma_{6,p}$.

Let $S = \{p \neq \ell : p \mid dM \text{ or } \mathrm{ord}_p(a) > 0\}$. If $p \mid dM$, then p is clearly bounded. If $\mathrm{ord}_p(a) > 0$, then by Proposition 11, p is also bounded. Additionally, for $p \in S$ we know L contains a sublattice of rank 5 whose p-adic order of its discriminant is bounded. Thus, we know that S is admissible to L, and we apply Proposition 7. Recall that by Proposition 8 if $\mu_5(\Delta_S(L))$ is bounded then in fact $\mu_5(L)$ is bounded. Following the remarks at the end of Section 2.2, L will now refer to $\Delta_S(L)$ and by Proposition 9 and Lemma 12 we may replace M with the sublattice of $\Delta_S(L)$ obtained by applying to M all of the Watson transformations and scalings that were applied to L. Note that by Lemma 12, M is still a primitive sublattice of L with bounded discriminant. We will similarly replace a, $v_{i,p}$, $\gamma_{i,p}$ accordingly. Now, if $p \neq \ell$ and $p \notin S$, then M_p is unimodular

and thus $\mathbb{H} \perp \mathbb{H}$ is represented by L_p. By Proposition 7, for $p \neq \ell$, $\mathbb{H}$ is represented by L_p.

We first assume that $\gamma_{5,\ell} > \mathrm{ord}_\ell(\mathfrak{l}(M_\ell))+4$. By Claim 2 proved in Section 4.2, we can write $L_\ell = L_0 \perp L_1$ where $M_\ell \longrightarrow L_0$ and the orthogonal complement of M_ℓ in L_ℓ is represented by L_1. Then $\{\ell\}$ is admissible to L and by Proposition 7 we may assume that

$$L_\ell \cong \mathbb{A} \perp \mathbb{A}^\ell \perp N_\ell,$$

for some sublattice N_ℓ of L_ℓ. Recall that $\mathbb{A}$ is the binary anisotropic $\mathbb{Z}_\ell$ lattice $\langle 1, -\Delta \rangle$ when $\ell > 2$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ when $\ell = 2$. Then $M_\ell^\perp \longrightarrow N_\ell$ and thus $\mathrm{ord}_\ell(a) \geq \mathrm{ord}_\ell(\mathfrak{n}(N_\ell))$. Let η be the smallest positive even integer greater than or equal to $\mathrm{ord}_\ell(a)$. Let $\tilde{r}$ be a prime such that $\tilde{r} \in -(\mathbb{Z}_p^\times)^2$ for $p \in S$. Let $\tilde{t}$ be a prime such that $\tilde{t} > 2\ell^{\eta - \mathrm{ord}_\ell(a)}(dM)^2$ and $\tilde{t} \in (\mathbb{Z}_p^\times)^2$ for all $q \mid 2\tilde{r}$. We can choose $\tilde{r}$ and $\tilde{t}$ to be bounded. Since $\tilde{t}$ is a square at $\tilde{r}$ and $\tilde{t} \equiv 1 \mod 8$, we have that $\ell^\eta \tilde{r} \equiv \tilde{c}^2 \mod \tilde{t}$ for some $0 < \tilde{c} < \tilde{t}$. Thus we can find an integer $\tilde{d}$ such that $\tilde{t}\tilde{d} = \tilde{c}^2 + \ell^\eta \tilde{r}$.

Consider the binary lattice

$$\tilde{K} = \begin{pmatrix} 2\tilde{t} & 2\tilde{c} \\ 2\tilde{c} & 2\tilde{d} \end{pmatrix}.$$

If $p \notin S$, then $\mathbb{H} \perp \mathbb{H}$ is represented by L_p, and consequently $\tilde{K}_p \longrightarrow L_p$. If $p \in S$, then $\tilde{K}_p \cong \langle 2\tilde{t}, -2\tilde{t} \rangle$ and thus $\tilde{K}_p$ is represented by L_p. However, $\mathbb{Q}_\ell \tilde{K}_\ell \cong \mathbb{H}$ and thus $\tilde{K}$ is not represented by M. By Claim 3 proved in Section 4.2, $\tilde{K}_\ell \longrightarrow L_\ell$.

By the 2-regularity of L, $\tilde{K}$ is represented by L. By Lemma 3, $\mu_4(L) \leq \max\{2\tilde{t}, 2\tilde{d}, \mu_4(M)\}$. By Lemma 4, we get the inequality

$$\ell^{\mathrm{ord}_\ell(a)} \leq (dM)^2 \max\{2\tilde{t}, 2\tilde{d}, \mu_4(M)\}.$$

If $2\tilde{d} < \max\{2\tilde{t}, \mu_4(M)\}$, then $\mathrm{ord}_\ell(a)$ is bounded. Otherwise, $\ell^{\mathrm{ord}_\ell(a)} \leq 2\tilde{d}(dM)^2$. Since $\tilde{t}\tilde{d} < \tilde{t}^2 + \ell^\eta \tilde{r}$,

$$\ell^{\mathrm{ord}_\ell(a)} < \frac{2\tilde{t}^2(dM)^2}{\tilde{t} - 2\ell^{\eta - \mathrm{ord}_\ell(a)}\tilde{r}(dM)^2},$$

and hence $\mathrm{ord}_\ell(a)$ is bounded. However, in this case $\mathrm{ord}_\ell(a) = \gamma_{5,\ell}$ then $\gamma_{5,\ell} < D$, where D is a constant depending on M.

Suppose $\gamma_{5,\ell} < \max\{\mathrm{ord}_\ell(\mathfrak{l}(M_\ell)) + 4, D\}$. Let r be a prime such that $r \in -(\mathbb{Z}_p^\times)^2$ for $p \in S \cup \{\ell\}$. Let t be a prime such that $t \nmid dM$ and $t \in (\mathbb{Z}_p^\times)^2$ for all primes $p \mid 2r$. Note that we can choose both t and r to be bounded. Then $-r$ is a square modulo t, and thus there exist bounded integers c and d such that $c^2 + r = td$. Consider

$$K = \begin{pmatrix} 2t & 2c \\ 2c & 2d \end{pmatrix}.$$

Suppose that $p \notin S \cup \{\ell\}$. Then $\mathbb{H} \perp \mathbb{H}$ is represented by L_p and consequently K_p is represented by L_p in this case. For $p \in S$, $\mathbb{H}$ is represented by L_p. Similarly, since $\gamma_{5,\ell}$ is bounded $\{\ell\}$ is admissible to L. By Proposition 7, we may assume $\mathbb{H}$ is represented by L_ℓ as well. At the primes in $S \cup \{\ell\}$, $K_p \cong \langle 2t, -2t \rangle$ and we see that K_p is in fact represented by L_p. Thus, by the 2-regularity of L we see

that K is in fact represented by L. However, it is clear that at ℓ, $\mathbb{Q}K_\ell \cong \mathbb{H}$ and thus $K_\ell \not\longrightarrow M_\ell$ since M_ℓ is anisotropic by Proposition 9. Then

$$\mu_5(L) \leq \max\{2t, 2d, \mu_4(M)\},$$

by Lemma 3.

□

Proposition 14. *Let M be a quinary lattice and $m \in \mathbb{Z}$ such that $m \longrightarrow M$ and $mdM \in \mathbb{Q}^{\times^2}$. Then there exists a prime p, which depends only on M, and an even integer $\alpha = \alpha(m,p)$ such that for any $a \in p^\alpha\mathbb{Z}$, $\langle m, a\rangle \overset{*}{\not\longrightarrow} M$.*

Proof. Since M is quinary, we know that $\mathbb{Q}M$ is universal and $dM \longrightarrow \mathbb{Q}M$. Thus $\mathbb{Q}M \cong \mathbb{Q}[z] \perp U$ where $Q(z) = dM$ and U is a 4-dimensional quadratic space over $\mathbb{Q}$ with square discriminant. Let $\mathcal{S} = \{x \overset{*}{\in} M : Q(x) = m\}$. For $x \in \mathcal{S}$, let $E^{(x)}$ be the orthogonal complement of $\mathbb{Z}[x]$ in M. Since mdM is a square, $\mathbb{Q}E^{(x)} \cong U$ for any $x \in \mathcal{S}$. By Lemma 1, there exists a prime p such that for any $x \in S$ we have that $(E^{(x)})_p$ is anisotropic. Then, by Lemma 2, there is an even integer $\alpha(E^{(x)})$ such that $E^{(x)}$ does not primitively represent any element in $p^{\alpha(E^{(x)})}\mathbb{Z}_p$. Since $dE^{(x)} \leq mdM$, there are only finitely many non-isometric $E^{(x)}$. Let $\mathcal{S}^\perp$ be the collection of all the lattices $E^{(x)}$ for $x \in \mathcal{S}$. Let α be the largest of all $\alpha(E)$ such that $E \in \mathcal{S}^\perp$. Then for any $a \in p^\alpha\mathbb{Z}_p$, $\langle m, a\rangle \overset{*}{\not\longrightarrow} M$. □

3.2 Main Result

We are now ready to prove the main result. Once again, the main result of this thesis is the following theorem.

Theorem. *For $n \geq 2$, there are only finitely many isometry classes of strictly n-regular normalized positive definite integral quadratic lattices of rank $n + 4$.*

Proof. Let L be a strictly n-regular normalized lattice of rank $n+4$. It is sufficient to show that the discriminant of L is bounded above by an absolute constant. To this end, we will make use of the Hadamard inequality [6, Proposition 2.3]

$$dL \leq \prod_{i=1}^{n+4} \mu_i(L),$$

where dL is the discriminant of L and $\mu_i(L)$ is the i^{th} successive minima of L.

We first handle the case when $n \geq 3$. Then L is regular by Propositions 2 and 3, and at least of rank 7. Therefore, by Lemma 7, the first three successive minima of L are bounded. Since strict n-regularity implies $(n-1)$-regularity we also know that $\mu_4(L), \ldots, \mu_{n+3}(L)$ are bounded by Lemmas 5 and 6. Let M be a rank-$(n+3)$ primitive sublattice of L with bounded discriminant. By Proposition 10, $\mu_{n+4}(L)$ is bounded by a constant depending on M. Hence dL is bounded.

Now, we handle the $n = 2$ case. Let L be a strictly 2-regular normalized lattice of rank 6. By Proposition 2 and Proposition 3, L is regular. By Lemma 7

and Lemma 5, the first four successive minima of L are bounded. Then we may consider a quaternary primitive sublattice of L with bounded discriminant. By Proposition 12 and Proposition 13, the fifth successive minima of L is bounded.

From this point forward, M will refer to a quinary primitive sublattice of L with bounded discriminant. Fix an integer m such that $m \xrightarrow{*} M$ and $mdM \in \mathbb{Q}^{\times^2}$. Fix $z \overset{*}{\in} M$ such that $Q(z) = m$. Let w be a vector in the orthogonal complement of $\mathbb{Z}[z]$ in M such that $Q(w) = a$ for some $a \in \mathbb{Z}$. By Proposition 14, there exists a prime p and an even positive integer α such that $\langle m, p^\alpha a\rangle \not\xrightarrow{*} M$.

Suppose that $\gamma_{6,p} > \mathrm{ord}_p(\mathfrak{l}(M_p))$. Let $L_p = L_0 \perp L_1$ where L_0 is the orthogonal sum of the first five vectors in a Jordan decomposition; see Claim 4 in Section 4.2. It follows from the assumption $\gamma_{6,p} > \mathrm{ord}_p(\mathfrak{l}(M_p))$ that $M_p \longrightarrow L_0$. Thus $\mathrm{ord}_p(dL_0) \leq \mathrm{ord}_p(dM)$. Then $\{p\}$ is admissible to L and we can then apply Proposition 7. We may then assume

$$L_p \cong \mathbb{H} \perp K_p \perp \langle p^t\epsilon\rangle,$$

where $t = \mathrm{ord}_p(\mathfrak{l}(L_p))$. Then L_p contains a sublattice isometric to $\langle m, -m\rangle \perp K_p \perp \langle p^t\epsilon\rangle$. Since $\mathbb{Q}_p[\langle -m\rangle \perp K_p]$ is universal, we know that $p^\alpha ad^2 \longrightarrow \langle -m\rangle \perp K_p$ for some $d \in \mathbb{Z}$. Let $e = \alpha + \mathrm{ord}_p(ad^2)$. If $t \leq e + 3$, then $\gamma_{6,p}$ is bounded. Thus we may assume without loss of generality that $t > e + 3$. By [13, 63:4] there exists $\lambda \in \mathbb{Z}_p^\times$ such that

$$\lambda^2 p^\alpha ad^2 + \lambda^2 p^t\epsilon = p^\alpha ad^2.$$

Then $p^\alpha ad^2$ is primitively represented by $\langle -m\rangle \perp K_p \perp \langle p^t\epsilon\rangle$ in a way where we can apply Lemma 13 to claim that $\langle m, p^\alpha ad^2\rangle \xrightarrow{*} L_p$.

Define $K \subseteq L$ by

$$K_q = \begin{cases} \mathbb{Z}_p[z, p^{\frac{\alpha}{2}}dw] & \text{if } q = p, \\ (\mathbb{Q}_q[z,w] \cap L_q & \text{if } q \neq p. \end{cases}$$

For every prime q, K_q is primitively represented by L_q so by the strict 2-regularity of L, K is primitively represented by L. However, $\langle m, p^\alpha ad^2\rangle$ is not primitively represented by M_p, so K is in fact not primitively represented by M. Therefore, by Lemma 3,

$$\begin{aligned} \mu_6(L) &\leq \max\{\mu_2(K), \mu_5(M)\} \\ &\leq \max\{m, p^\alpha ad^2\}. \end{aligned}$$

Thus $\gamma_{6,p}$ is bounded, with a bound depending only on M.

Since $\gamma_{6,p}$ is bounded, we apply Proposition 7 to assume

$$L_p \cong \mathbb{H} \perp J_p.$$

The quadratic space $\mathbb{Q}_p J_p$ is universal, so $mc^2 \xrightarrow{*} J_p$ for some $c \in \mathbb{Q}^\times$. For each isometry class of J_p there exists such a c, and since $\mathrm{ord}_p(\mathfrak{l}(J_p))$ is bounded, we let $\mathcal{C}$ be the finite collection of such c. For each $c_i \in \mathcal{C}$ we apply Proposition 14 to get an even integer α_i. Let α' be the maximum of all α_i. Then, by Proposition 14, $\langle mc^2, p^{\alpha'}a\rangle \not\xrightarrow{*} M$ for any $c \in \mathcal{C}$.

Define $K' \subseteq L$ by

$$K'_q = \begin{cases} \mathbb{Z}_p[cz, p^{\frac{\alpha'}{2}} w] & \text{if } q = p \\ (\mathbb{Q}_q[z, w] \cap L_q & \text{if } q \neq p. \end{cases}$$

For $q \neq p$, K'_q is clearly primitively represented by L_q. At p, we know that $\mathbb{H}$ primitively represents $p^{\alpha'} a$. Since $mc^2 \xrightarrow{*} J_p$, we thus have that K'_p is primitively represented by L_p. By the strict 2-regularity of L, we have that $K' \xrightarrow{*} L$. However, $K'_p \not\xrightarrow{*} M_p$ since $K'_p \cong \langle mc^2, p^{\alpha'} a \rangle$. Therefore $K' \not\xrightarrow{*} M$, and by Lemma 3

$$\mu_6(L) \leq \max\{\mu_2(K'), \mu_5(M)\}.$$

Therefore, by Proposition 8, this concludes the proof. □

Chapter 4

Proofs of local representations

This chapter is dedicated to providing proofs of local representations used in the proof of the main theorem. The notations used will be those of O'Meara, and for a more detailed treatment of these ideas see [12].

4.1 Notation

Fix U, V as quadratic spaces over $\mathbb{Q}_p$ for some prime p and L and l as $\mathbb{Z}_p$-lattices.

Definition 1. *[12] Suppose that $U \longrightarrow V$. We define (V/U) so that*

$$V \cong U \perp (V/U).$$

Otherwise, put $(V/U) = \emptyset$. For lattices L and l on V and U respectively, define $L/l = \mathbb{Q}_p L/\mathbb{Q}_p l$.

For a p^i-*modular* lattice L, we have

$$x \in l \text{ and } x \notin pl \Longrightarrow B(x,l) = p^i\mathbb{Z}_p.$$

By [13, 82:17], this definition is equivalent to the previous one in Section 1.1. Recall that a modular lattice l is called proper if $\mathfrak{n}l = \mathfrak{s}l$, and improper if $\mathfrak{n}l \subset \mathfrak{s}l$. Improper modular lattices exist only when $p = 2$.

Definition 2. *[12] Let $l = \perp l_\lambda$ be a Jordan decomposition. Define $\mathfrak{l}_i = \perp l_\mu$ where μ extends over values for which $\mathfrak{s}l_\mu \supseteq p^i\mathbb{Z}_p$. Let $\mathfrak{l}_i^\perp = \perp l_\mu$ where μ extends over values for which $\mathfrak{s}l_\mu \subset p^i\mathbb{Z}_p$. In the case of the lattice $L = \perp L_\lambda$, we use $\mathfrak{L}_i$ and $\mathfrak{L}_i^\perp$ instead.*

The following is a summary of results which will help in answering these representation questions, and more details can be found in [12, 13]. Let def $=$ dim$V$ $-$ dim$U$ and SU, SV be the Hasse invariants of U, V respectively. Then $U \longrightarrow V$ if and only if

$$\text{def} = 0 : U \cong V,$$

$$\text{def} = 1 : U \perp (dU \cdot dV) \cong V,$$

$$\text{def} = 2 : dU \cdot dV = -1 \text{ implies } U \perp \mathbb{H} \cong V,$$

$$\text{def} \geq 3 : \text{none}.$$

4.1.1 If $p \neq 2$

If $p \neq 2$, we use the following theorem for local representation of lattices.

Theorem 2. *[12, Theorem 1] Let $l = \perp l_\lambda$ and $L = \perp L_\lambda$ be Jordan decompositions of l and L, respectively. Then $l \longrightarrow L$ if and only if*

$$\mathbb{Q}_p \mathfrak{l}_i \longrightarrow \mathbb{Q}_p \mathfrak{L}_i$$

for all i.

4.1.2 If $p = 2$

There is more theory needed in the case when $p = 2$. Set $\mathfrak{L}_{(i)} = \perp L_\mu$ where i extends over all values of μ for which $\mathfrak{n}L_\mu \supseteq 2^i\mathbb{Z}_2$ and $\mathfrak{L}_{(i)}^{\perp} = \perp L_\mu$ with $\mathfrak{n}L_\mu \subset 2^i\mathbb{Z}_2$. We define $\mathfrak{l}_{[i]} = \perp l_\mu$ where i extends over all values of μ for which $\mathfrak{s}l_\mu \supseteq 2^i\mathbb{Z}_2$ and, in addition, those for which l_μ is improper and $\mathfrak{s}l_\mu = 2^{i+1}\mathbb{Z}_2$. Similarly, $\mathfrak{l}_{[i]}^{\perp} = \perp l_\mu$ with μ extending over the values for which $\mathfrak{s}l_\mu \subset 2^{i+1}\mathbb{Z}_2$ and those for which l_μ is proper with $\mathfrak{s}l_\mu = 2^{i+1}\mathbb{Z}_2$. With these definitions in mind we notice that

$$\mathfrak{L}_{(i)} = \mathfrak{L}_{i-1} \text{ or } \mathfrak{L}_i, \quad \mathfrak{l}_{[i]} = \mathfrak{l}_i \text{ or } \mathfrak{l}_{i+1}.$$

We now define two families of ideals, Δ_i and δ_i, which are dependent on L and l, respectively. If L has a proper 2^{i+1}-modular component, we set $\Delta_i = 2^{i+1}\mathbb{Z}_2$, if this is not the case but L has a proper 2^{i+2}-modular component we

set $\Delta_i = 2^{i+2}\mathbb{Z}_2$. If both cases fail, we set $\Delta_i = 0$. The family δ_i is defined analogously with l. Let $D_i = d(\mathfrak{L}_i)\mathbb{Z}_2$, unless $\mathfrak{L}_i = 0$ in which case let $D_i = 0$. Similarly, let $d_i = d(\mathfrak{l}_i)\mathbb{Z}_2$ unless $\mathfrak{l}_i = 0$ in which case we let $d_i = 0$.

An ideal $\mathfrak{p} \subset \mathbb{Q}_2$ is said to be represented by the space U, denoted $\mathfrak{p} \longrightarrow U$, if there is an $a \in Q(U)$ such that $a\mathbb{Z}_2 = \mathfrak{p}$. We write $\mathfrak{p} \longrightarrow \beta$ if $\mathfrak{p} \longrightarrow \mathbb{Q}_2 x$ where $Q(x) = \beta$.

Definition 3. *[12] We say that l has a **lower type** than L if the following hold for all i:*

(1)

$$dim\mathfrak{l}_i \leq dim\mathfrak{L}_i,$$

(2)

$$d_i D_i \longrightarrow 1 \text{ if } dim\mathfrak{l}_i = dim\mathfrak{L}_i,$$

(3)

$$\delta_i \subseteq \Delta_i + 2^{i+2}\mathbb{Z}_2 \text{ and } \Delta_{i-1} \subseteq \delta_{i-1} + 2^{i+1}\mathbb{Z}_2 \text{ if } dim\mathfrak{l}_i = dim\mathfrak{L}_i,$$

(4)

$$\Delta_{i-1} \subseteq \delta_i + 2^{i+1}\mathbb{Z}_2 \text{ if } dim\mathfrak{L}_i - 1 = dim\mathfrak{l}_i > 0 \text{ and } d_i D_i \longrightarrow 2^{i+1},$$

(5)

$$\delta_i \subseteq \Delta_i + 2^{i+2}\mathbb{Z}_2 \text{ if } dim\mathfrak{L}_i - 1 = dim\mathfrak{l}_i > 0 \text{ and } d_i D_i \longrightarrow 2^{i}.$$

Theorem 3. *[12, Theorem 3] Let l have a lower type than L. Then $l \longrightarrow L$ if and only if the following conditions hold for all i:*

(I)

$$\Delta_i \longrightarrow \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]},$$

(II)

$$\delta_i \longrightarrow \mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]},$$

(III)

$$\mathfrak{L}_{(i+2)}/\mathfrak{l}_{[i]} \cong \mathbb{Q}_2\mathbb{H} \textit{ implies } \Delta_i\delta_i \subseteq \delta_i^2,$$

(IV)

$$2^i(1+4\omega) \longrightarrow (2^i \perp \mathfrak{L}_(i+1))/\mathfrak{l}_i,$$

(V)

$$2^i(1+4\omega) \longrightarrow (2^i \perp \mathfrak{L}_(i+1))/\mathfrak{l}_{[i]}.$$

4.2 Proofs

Let K, L, and M be defined as in the proof of Proposition 11, with $K = \langle u, \ell^{\beta+\delta}vs\rangle$ and all $u, \ell, \beta, \delta, v, s$, defined as before.

Claim 1. *The $\mathbb{Z}_\ell$-lattice K_ℓ is represented by L_ℓ.*

Proof. Let $T = M \perp M^\perp$ and $K' = \langle u \rangle$. Making use of the facts that $K' \longrightarrow T$ and $T \longrightarrow L$, we will show that K_ℓ is represented by L_ℓ by showing that K_ℓ is in fact represented by T_ℓ. For convenience, we let $i_u = \mathrm{ord}_\ell(u)$ and $i_v = \mathrm{ord}_\ell(v) + \beta + \delta$, and we note that $i_u < i_v$ since $\beta \geq i_u$.

We first consider the case when $\ell \neq 2$. By Theorem 2, $K_\ell \longrightarrow T_\ell$ if and only if $\mathbb{Q}_\ell \mathcal{K}_i \longrightarrow \mathbb{Q}_\ell \mathcal{T}_i$ for every i. If $i < i_v$, then $\mathcal{K}_i = \mathcal{K}'_i$ and $\mathbb{Q}_\ell \mathcal{K}_i \longrightarrow \mathbb{Q}_\ell \mathcal{T}_i$ must be satisfied. Recall that $\beta \geq \max\{\mathrm{ord}_\ell(\mathfrak{l}(M)), \mathrm{ord}_\ell(a)\}$. Now, let $i \geq i_v$. Then $\dim \mathbb{Q}_\ell \mathcal{K}_i = 2$ and $\dim \mathbb{Q}_\ell \mathcal{T}_i \geq 5$. Thus $\mathbb{Q}_\ell \mathcal{K}_i \longrightarrow \mathbb{Q}_\ell \mathcal{T}_i$.

Now we suppose that $\ell = 2$. Note that $\mathcal{K}_i = \mathcal{K}_{[i]}$ for every i since K_2 does not have any improper components. We have

$$\mathcal{K}_i = \begin{cases} 0 & \text{if } i < i_u, \\ K' & \text{if } i_u \leq i < i_v, \\ K_2 & \text{if } i_v \leq i. \end{cases}$$

Recall that $\mathcal{T}_{(i_v)}$ is the orthogonal sum of Jordan components of T whose norms contain $2^{i_v}\mathbb{Z}_2$, and we have the inequalities $i_v > \mathrm{ord}_2(\mathfrak{l}(M))$ and $i_v > \mathrm{ord}_2(a)$. Thus by the choice of β, $\mathcal{T}_{(i_v)}$ must at least be quinary.

We claim that K_2 is of lower type than T_2. If $i < i_v - 2$, then $\mathcal{K}_i = \mathcal{K}'_i$ so $\dim \mathcal{K}_i \leq \dim \mathcal{T}_i$. If the hypotheses of conditions (2)-(5) in Definition 3 are met, then $K' \longrightarrow T$ and $\mathcal{K}_i = \mathcal{K}'_i$ imply that conditions (2)-(5) must hold. If $i \geq i_v$,

then $\mathcal{T}_i$ has at least rank 5 and $\mathcal{K}_i$ has rank 2. Thus condition (1) is satisfied and the hypotheses of conditions (2)-(5) are never met.

Now we may apply Theorem 3. Since $\mathcal{K}_i = \mathcal{K}_{[i]}$ for every i, conditions (IV) and (V) are the same. Similar to before, if $i < i_v - 2$ conditions (I)-(V) are satisfied since $K' \longrightarrow T$ and $\mathcal{K}_i = \mathcal{K}'_i$. Now suppose $i \geq i_v - 2$. Then $\mathcal{T}_{(i)}$ has at least rank 5 and $\mathcal{K}_i$ has at most rank 2. Thus $\dim \mathcal{T}_{(i+2)}/\mathcal{K}_i \geq 3$. We know for any ideal $\mathfrak{p}$, $\mathfrak{p} \longrightarrow \mathcal{T}_{(i+2)}/\mathcal{K}_i$ by [12, Proposition 16]. Thus conditions (I) and (II) are satisfied, as well as condition (III) since $\mathcal{T}_{(i+2)}/\mathcal{K}_i \ncong \mathbb{Q}_2\mathbb{H}$. For condition (IV), we see that $2^i \longrightarrow (2^i \perp \mathcal{T}_{(i+1)})/\mathcal{K}_i$ since $\mathbb{Q}_2\mathcal{K}_i \longrightarrow \mathbb{Q}_2\mathcal{T}_{(i+2)}$. Therefore, $K_2 \longrightarrow M_2 \perp M_2^{\perp}$ and hence $K_2 \longrightarrow L_2$. □

Now we let L and M be defined as in the proof of Proposition 13 when $\gamma_{5,\ell} > \mathrm{ord}_\ell(\mathfrak{l}(M_\ell)) + 4$. All of the other unexplained notations are those used in the proof of Proposition 13.

Claim 2. *If $\gamma_{5,\ell} > ord_\ell(\mathfrak{l}(M_\ell)) + 4$, then we can write $L_\ell = L_0 \perp L_1$ where $M_\ell \longrightarrow L_0$.*

Proof. Let $f = \mathrm{ord}_\ell(\mathfrak{l}(M_\ell))$ and let $T = M \perp M^{\perp}$. Recall that $\{v_{1,\ell}, \ldots, v_{6,\ell}\}$ is a basis for a Jordan decomposition of L_ℓ and $\gamma_{i,\ell}$ is the ℓ-adic order of the norm ideal of the Jordan component that contains $v_{i,\ell}$. We wish to show that

$$M_\ell \longrightarrow L_0 := \mathbb{Z}_\ell[v_{1,\ell}, \ldots, v_{4,\ell}].$$

We first suppose ℓ is odd. If $i < f$ then $\mathcal{L}_i \cong \mathcal{T}_i$. It is clear that $\mathbb{Q}_\ell \mathcal{M}_i$ is represented by $\mathbb{Q}_\ell \mathcal{T}_i$, and thus $\mathbb{Q}_\ell \mathcal{M}_i$ is represented by $\mathbb{Q}_\ell \mathcal{L}_i$. When $i = f$, we have $\mathbb{Q}_\ell \mathcal{M}_f = \mathbb{Q}_\ell M_\ell$. Then $\mathbb{Q}_\ell M_\ell$ is represented by $\mathbb{Q}_\ell \mathcal{L}_f$ since M is represented by L. Thus $\dim \mathbb{Q}_\ell \mathcal{L}_f \geq 4$. Since $\gamma_{5,\ell} > f + 4$, it must be the case that

$$\mathcal{L}_f \cong \mathbb{Z}_\ell[v_{1,\ell}, \ldots, v_{4,\ell}].$$

Hence, when $\ell \neq 2$, $M_\ell \longrightarrow \mathbb{Z}_\ell[v_{1,\ell}, \ldots, v_{4,\ell}]$.

Now suppose that $\ell = 2$. We first show that M_2 is of lower type than $(L_0)_2$. For L_0, we use the notation $(\mathcal{L}_\prime)_i$ for the lattices in Definition 2. We know that $(\mathcal{L}_\prime)_i \cong \mathcal{L}_i$ for all $i \leq f$. Additionally, for all i, $\dim \mathcal{M}_i \leq \dim \mathcal{L}_i$. For $i \geq f$, $\mathcal{L}_{\prime i} = L_0$ and $\mathcal{M}_i = M_2$. Thus we know that $\dim \mathcal{M}_i \leq \dim \mathcal{L}_{\prime i}$ for all i. If $i \leq f$, then $\mathcal{L}_{\prime i} = \mathcal{L}_i$ and conditions (2)-(5) must be satisfied. If $i > f$, then

$$\mathcal{M}_i = M_2 = \mathcal{M}_f \text{ and } \mathcal{L}_{\prime i} = (L_0)_2 = \mathcal{L}_{\prime f}$$

so the conditions must be satisfied as well. Thus, M_2 is of lower type than $(L_0)_2$.

Now we must check the conditions of Theorem 3. If $i \leq f$, then it is the case that $\mathcal{L}_{(i+2)} \cong \mathcal{L}_{\prime(i+2)}$ so conditions (I)-(V) must be met. If $i > f$, then $\mathcal{M}_i$ and $\mathcal{L}_{\prime i}$ remain unchanged from when $i = f$ so the conditions must still be satisfied. Hence M_2 is represented by L_0 and our claim holds. □

Let $\tilde{K}$, L, and M be defined as in the proof of Proposition 13 when $\gamma_{5,\ell} > \text{ord}_\ell(\mathfrak{l}(M_\ell)) + 4$.

Claim 3. *$\tilde{K}_\ell$ is represented by L_ℓ.*

Proof. Recall that $\tilde{K}_\ell \cong \langle 2\tilde{t}, 2\ell^\eta \tilde{t}\tilde{r}\rangle$, $L_\ell \cong \mathbb{A} \perp \mathbb{A}^\ell \perp N_\ell$, and η is the smallest positive even integer greater than or equal to $\mathrm{ord}_\ell(a)$. Then

$$\tilde{\mathcal{K}}_i = \begin{cases} 0 & \text{if } i < 1, \\ \langle 2\tilde{t}\rangle & \text{if } 1 \leq i \leq \eta, \\ \tilde{K}_\ell & \text{if } \eta < i. \end{cases}$$

We first suppose ℓ is odd. For $i \leq \eta$, $\mathbb{Q}_\ell\tilde{\mathcal{K}}_i$ is represented by $\mathbb{Q}_\ell\mathcal{L}_i$ since $0 \longrightarrow \mathbb{Q}_\ell\mathbb{A}$ and $[2\tilde{t}] \longrightarrow \mathbb{Q}_\ell\mathbb{A}$. If $i > \eta$, $\mathbb{Q}_\ell\tilde{K}_\ell$ is represented by $\mathbb{Q}_\ell\mathcal{L}_i$ since $\mathcal{L}_i$ has at least rank 5.

Now we let $\ell = 2$. Then

$$\mathcal{L}_{(i)} = \begin{cases} 0 & \text{if } i < 1, \\ \mathbb{A} & \text{if } i = 1, \\ \mathbb{A} \perp \mathbb{A}^\ell & \text{if } i = 2, \end{cases}$$

and $\mathcal{L}_{(\eta)}$ has at least rank 5 since η is greater than or equal to $\mathrm{ord}_\ell(a)$.

We now show that $\tilde{K}_2$ has lower type than L_2. It is clear that $\dim\tilde{\mathcal{K}}_i < \dim\mathcal{L}_i$ for every i, and if $\dim\tilde{\mathcal{K}}_i \neq 0$ it is never the case that $\dim\tilde{\mathcal{K}}_i + 1 = \dim\mathcal{L}_i$. Thus $\tilde{K}_2$ has lower type than L_2.

Now, we use Theorem 3 to show that K_2 is represented by L_2. Note that since $\tilde{K}_2$ has an orthogonal decomposition, $\tilde{\mathcal{K}}_i = \tilde{\mathcal{K}}_{(i)}$ and so conditions (IV) and

(V) are the same. We break the argument into cases dependent upon the index i.

- Let $i = -1$. In this case,

$$\mathcal{L}_{(1)}/\tilde{\mathcal{K}}_{-1} = \mathbb{Q}_2\mathbb{A}, \Delta_{-1} = 0, \text{ and } \delta_{-1} = 0.$$

  Clearly $0 \longrightarrow \mathbb{Q}_2\mathbb{A}$, and $\mathbb{Q}_2\mathbb{A} \ncong \mathbb{Q}_2\mathbb{H}$. Finally, for condition (IV) it is clear that $2^{-1} \longrightarrow 2^{-1} \perp \mathbb{Q}_2\mathbb{A}$.

- Let $i = 0$. We now have

$$\mathcal{L}_{(2)}/\tilde{\mathcal{K}}_0 = \mathbb{Q}_2(\mathbb{A} \perp \mathbb{A}^2), \Delta_0 = 0, \text{ and } \delta_0 = 2\mathbb{Z}.$$

  We see that $2\mathbb{Z}_2 \longrightarrow \mathbb{Q}_2(\mathbb{A} \perp \mathbb{A}^2)$ since $2 \longrightarrow \mathbb{Q}_2(\mathbb{A} \perp \mathbb{A}^2)$, and $\mathbb{Q}_2(\mathbb{A} \perp \mathbb{A}^2) \ncong \mathbb{Q}_2\mathbb{H}$. Finally, it is clear that $2^0 \longrightarrow 2^0 \perp \mathbb{Q}_2(\mathbb{A} \perp \mathbb{A}^2)$.

- Let $1 \leq i \leq \eta$. In this case, $\mathcal{L}_{(i+2)}/\tilde{\mathcal{K}}_i$ is at least 3 dimensional since $\dim\mathcal{L}_{(i+2)} \geq 4$ and $\tilde{\mathcal{K}}_i = \langle 2\tilde{t} \rangle$. Thus by [13, Proposition 16] Δ_i and δ_i are represented by $\mathcal{L}_{(i+2)}/\tilde{\mathcal{K}}_i$. Additionally, $\mathcal{L}_{(i+2)}/\tilde{\mathcal{K}}_i \ncong \mathbb{Q}_2\mathbb{H}$ and conditions (I), (II), and (III) are met. For condition (IV), $2^i \perp [2\tilde{t}] \longrightarrow 2^i \perp \mathcal{L}_{(i+2)}$ since $\mathbb{A} \perp \mathbb{A}^2 \subseteq \mathcal{L}_{(i+2)}$.

- Finally, let $i > \eta$. In this case, $\mathcal{L}_{(i+2)}$ has at least rank 5 and $\tilde{\mathcal{K}}_i = \tilde{K}_2$, so $\dim\mathcal{L}_{(i+2)}/\tilde{\mathcal{K}}_i \geq 3$. Thus conditions (I), (II), and (III) must be satisfied. Since $\dim\mathcal{L}_{(i+1)} \geq 5$, $\mathbb{Q}_2\tilde{K}_2 \longrightarrow \mathbb{Q}_2\mathcal{L}_{(i+1)}$ and thus $2^i \longrightarrow (2^i \perp \mathcal{L}_{(i+1)})/\mathbb{Q}_2\tilde{K}_2$. Therefore, condition (IV) is satisfied.

By Theorem 3 $\tilde{K}_2 \longrightarrow L_2$. Thus we have shown that $\tilde{K}_\ell \longrightarrow L_2$. □

Let L and M be defined as in the proof of Theorem 1 for the case $n = 2$ when M has rank 5.

Claim 4. *For a prime p, suppose that $\gamma_{6,p} > ord_p(\mathfrak{l}(M_p))$. Then the last component of a Jordan decomposition of L_p has an orthogonal decomposition.*

Proof. Let $f = \mathrm{ord}_p(\mathfrak{l}(M_p))$ and L_1 be the last component of a Jordan decomposition of L_p. We claim that L_1 has an orthogonal decomposition. Suppose on the contrary that L_1 is indecomposable. In this case, it is necessary that $p = 2$ and the rank of L_1 is at least 2. Since $\mathrm{ord}_2(\mathfrak{l}(L_2)) > f$, $\dim\mathfrak{L}_f \leq 4$. Since $M \longrightarrow L$, M_2 is of lower type than L_2 and $5 = \dim\mathfrak{M}_f \leq \dim\mathfrak{L}_f$. This is a contradiction, and thus L_1 has an orthogonal decomposition. □

Bibliography

[1] J. Bochnak and B. K. Oh. Almost regular quaternary quadratic forms. *Annales de linstitut Fourier*, 58:1499–1549, 2008.

[2] J.W.S. Cassels. *Rational quadratic forms.* London Mathematical Society Monographs, 1978.

[3] W. K. Chan, A. G. Earnest, and B. K. Oh. Regularity properties of positive definite integral quadratic forms. *Contemporary Mathematics*, 344:59–71, 2004.

[4] W. K. Chan and B. K. Oh. Finiteness theorems for positive definite n-regular quadratic forms. *Trans. Amer. Math. Soc.*, 355(6):2385–2396, Jan 2003.

[5] L. E. Dickson. Ternary quadratic forms and congruences poop. *Ann. of Math.*, 28:333–341, 1926.

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

[7] A. G. Earnest. An application of character sum inequalities to quadratic forms. *Number Theory, Canadian Math. Soc. Conference Proceedings*, 15:155–158, 1995.

[8] A. G. Earnest, J. Y. Kim, and N. D. Meyer. Strictly regular quaternary quadratic forms and lattices. *J. Number Theory*, 144:256–266, 2014.

[9] J.S. Hsia, Y. Kitaoka, and M. Kneser. Representation of positive definite quadratic forms. *J. Reine Angew. Math.*, 301:132–141, 1978.

[10] Yoshiyuki Kitaoka. *Arithmetic of Quadratic Forms*. Cambridge University Press, 1999.

[11] Jacques Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag Berlin Heidelberg, 2003.

[12] O. T. O'Meara. The integral representations of quadratic forms over local fields. *Amer. J. Math.*, 80:843–878, 1958.

[13] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer-Verlag, Berlin, 1973.

[14] G. L. Watson. Some problems in the theory of numbers. *Ph.D. Thesis, University of London*, 1953.

[15] G. L. Watson. The representation of integers by positive ternary quadratic forms. *Mathematika*, 1:104–110, 1954.