國立臺灣大學理學院數學系

碩士論文

Department of Mathematics

College of Science

National Taiwan University

Master Thesis

論 290 定理

On the 290-theorem

朱建鑫

Jian-Sin Jhu

指導教授：陳其誠教授

Advisor : Professor Ki-Seng Tan

中華民國 105 年 6 月

June, 2016

doi:10.6342/NTU201600288

致謝

在短暫的兩年研究期間，陳其誠教授除了在數學研究上給予我諸多協助，更樹立一個待人接物的典範。能夠接受陳老師的指導，實是我的福氣。因此，這篇論文能夠順利完成，我想要向陳其誠老師致上最高的敬意與感謝！另外，論文口試期間，承蒙口試委員們的鼓勵與指正，使得本論文更加完整。我也要感謝膺任、建樺以及家成學長，願意與我討論許多數學以及研究相關的問題，給予我許多建議與幫助。最後，我要感謝啟樺、世緯還有賴北，從大學時代一直到研究生時期，陪我度過許多辛苦卻令人無限懷念的日子。

朱建鑫

2016.06

doi:10.6342/NTU201600288

中文摘要

這篇文章中，我們研究 Manjul Bhargava 與 Jonathan Hanke 的 290 定理。主要是透過分類一些被稱作上升子的特殊基本二次形，建立起決定任一正定整係數二次形是否為宇態二次形的準則。

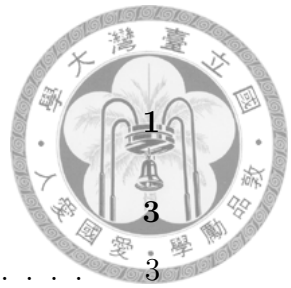
doi:10.6342/NTU201600288

Abstract

In this thesis, we study the 290-theorem of Manjul Bhargava and Jonathan Hanke. Via the classification of certain basic quadratic forms called escalators, we can establish an efficient criterion to determine whether a positive integral quadratic form is universal.

doi:10.6342/NTU201600288

Contents



doi:10.6342/NTU201600288

doi:10.6342/NTU201600288

1 Introduction

The main aim of this thesis is to study a theorem of Manjul Bhargava and Jonathan Hanke that characterises all universal quadratic forms.

A quadratic form $Q(x_1, ..., x_n)$ takes integer values for all vectors $(x_1, ..., x_n)$ in $\mathbb{Z}^n$, if and only if $Q(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$, and if this holds it is called a *integral quadratic form*. An integral quadratic form $Q(x_1, ..., x_n)$ is said to represent an integer $z \in \mathbb{Z}$, if $Q(a_1, ..., a_n) = z$, for some *non-zero* $(a_1, ..., a_n) \in \mathbb{Z}^n$, and $Q(x_1, ..., x_n)$ is positive-definite if it represents only positive integers. Finally, by a universal quadratic form we mean a positive-definite integral quadratic form that represents every natural number.

In history, many universal quadratic forms has been studied. A classical example comes from the famous Lagrange's *four squares theorem* which actually says the form $x^2+y^2+z^2+w^2$ is universal. Also, in [9] Ramanujan listed 54 other universal quadratic forms of type $ax^2 + by^2 + cz^2 + dw^2$, where a, b, c, d are certain natural numbers.

Bhargava and Hanke [6] proves the following theorem which was originally conjectured by Conway in 1993.

Theorem 1. *A positive-definite integral quadratic form is universal if and only if it represents the following* 29 *integers:*

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29,$$
$$30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290.$$

Definition 1.1. *Those* 29 *integers listed in* Theorem 1 *are called critical integers.*

Bhargava and Hanke [6] also proves that the 29 critical integers are minimal in the sense of the following:

Theorem 2. *For each critical integer c, there is a non-universal positive-definite integral quadratic form represents other* 28 *critical integers except for c.*

The proofs of the theorems relies on the concept of *escalators* of a given quadratic form $Q(x)$. To explain it, we apply the correspondence between quadratic forms and

doi:10.6342/NTU201600288

lattices (see §2.4), roughly speaking, the lattice of an escalator is generated by the lattice of $Q(x)$ together with a vector having square norm equal to the smallest positive integer a not represented by $Q(x)$ (see §3 for details). In particular, this escalator represents a. By continuing the escalating procedure, one will obtain escalators that represent all critical integers. Then one check if they are universal. It turns out one needs at most 7 steps of escalating to achieve the goal. However, there usually are numerous escalators of a given form. There is only one escalator of the zero form, namely the one-dimensional form x^2, which has 3 escalators, all 2-dimensional, and these 2-dimensional forms have totally 34 escalators, all 3-dimensional. These 3-dimensional forms have 6560 escalators, all 4-dimensional. Call these basic escalators. Fortunately, the proofs can be completed by just working on 4-dimensional basic escalators.

There is an effective (and efficient) algorithm to check if a basic 4-dimensional escalator locally represents an integer m (see Lemma 4.18, 4.19). Although the Hasse-Minkowski theorem, or the local-global principle, does not always holds for integral forms, it is applicable to 1658 forms out of all 6560 basic 4-dimensional escalators so that one can determines if these forms represent an integer m by checking the corresponding local representability.

For other basic 4-dimensional escalators, one needs to apply analytic method. By estimating the constants involved in a modified formula of Siegel (see (6.2.1)) and by using the Deligne's bounds of the Fourier coefficients of Hecke eigenforms, Bhargava and Hanke are able to find for each basic 4-dimensional escalator a lower bound B such that the local-global principle holds for $m > B$. Fortunately, the lower bound B is of reasonable size so that one can use machine to check if each $m \leq B$ is represented by the corresponding escalator. With the information of representability of all 4-dimensional basic escalators obtained, the theorems are then proved by a few deductions.

This thesis is organised in the following way. In §2, we review some basic facts and definitions including the correspondence between equivalence classes of integral quadratic forms and integral-square-norm lattices. Escalators are discussed in §3.

doi:10.6342/NTU201600288

We review the local theory in §4 and the local-global principle in §5. The analytic method is studied in §6, and finally, the proofs are completed in §7.

2 Notation and setting

For simplicity, write x for the vector $(x_1, \ldots, x_n)$ and denote $Q(x) = Q(x_1, ..., x_n)$. Let P be a partition of $\{1, 2, \ldots, n\}$. For each $J \in P$, let x_J denote the vector whose components are x_i for $i \in J$. For a subset $S \subseteq P$, let x_S be the vector whose components are x_i for all $i \in \bigcup_{J \in S} J$.

2.1 The Gram matrix

Definition 2.1. *The Gram matrix A of a quadratic form $Q(x)$ is the unique symmetric matrix A such that*

$$Q(x) = x^T A x, \quad \textit{for all } x.$$

Call $D_Q := \det(A)$ the determinant of $Q(x)$.

If $Q(x)$ is integral, then the entries of A are contained in $\frac{1}{2}\mathbb{Z}$.

Definition 2.2. *Let $Q(x)$ be an integral quadratic form with A as Gram matrix. Let N_Q be the minimal positive integer such that $N_Q \cdot (2A)^{-1}$ is a matrix whose entries are integers and diagonal entries lie in $2\mathbb{Z}$. Call N_Q the level of $Q(x)$.*

For example, the Gram matrix of

$$Q(x_1, x_2) := x_1^2 + 3x_1x_2 + 5x_2^2 \tag{2.1.1}$$

is

$$A = \begin{pmatrix} 1 & 3/2 \\ 3/2 & 5 \end{pmatrix} \text{ with } A^{-1} = \begin{pmatrix} 20/11 & -6/11 \\ -6/11 & 4/11 \end{pmatrix},$$

while $D_Q = 11/4$ and $N_Q = 11$.

doi:10.6342/NTU201600288

2.2 Integrally equivalence class

Two quadratic form $Q(x)$ and $Q'(x)$ with Gam matrix A and A' are integrally equivalent if and only if there exists some $B \in \mathrm{GL}(n, \mathbb{Z})$ such that

$$A' = B^T AB.$$

We shall refer this equivalence relation as the integral equivalence relation. Integrally equivalent quadratic forms have the same determinant. We define the determinant of an integral equivalence class as the that of any of its members.

Lemma 2.3. *The number of integral equivalence classes of the same determinant is finite.*

Proof. See [1, §9.2, corollary 1, p.129]. □

2.3 The Minkowski-reduced forms

Definition 2.4. *Let $Q(x)$ be a positive-definite integral quadratic form in n variables and let $A = (a_{ij})$ be its Gram matrix. Call $Q(x)$ Minkowski-reduced if*

$$Q(x) \geq a_{ii}, \quad \textit{whenever } \text{g.c.d.}(x_i, \ldots, x_n) = 1,$$

$$a_{i,i+1} \geq 0, \quad \textit{for } i = 1, \ldots, n-1.$$

The form $Q(x_1, x_2)$ in (2.1.1) is not Minkowski-reduced, because $Q(-1, 1) < a_{22}$. However, $Q(x_1 - x_2, x_2) = x_1^2 + x_1x_2 + 3x_2^2$ is Minkowski-reduced and is integrally equivalent to $Q(x_1, x_2)$. Indeed, each positive-definite integral quadratic form is integrally equivalent to at least one Minkowski-reduced form [2, p.27].

2.4 The corresponding lattices

Let L be a full-rank lattice in the Euclidean space $\mathbb{R}^n$. Suppose L is a $\mathbb{Z}$-*lattice* in the sense that $\|v\|^2 \in \mathbb{Z}$, for all vector $v \in L$. Let $\varphi : \mathbb{Z}^n \longrightarrow L$ be an isomorphism of abelian groups. Then $Q(x) := \|\varphi(x)\|^2$ is a positive-definite integral quadratic form in n variables. The form $Q(x)$ depends on L as well as the choice of φ, while its integral

doi:10.6342/NTU201600288

equivalence class depends only on L. Conversely, if $Q(x_1, ...x_n)$ is a positive-definite integral quadratic form with Gram matrix A, then the assignment $(u, v) \mapsto u^T Av$ defines an inner product on $\mathbb{R}^n$, and hence by the Gram Schmidt process, there is an orthogonal automorphism φ of $\mathbb{R}^n$ such that $Q(x) = \|\varphi(x)\|^2$, for all $x \in \mathbb{Z}^n$. Then we see that $Q(x)$ is exactly the quadratic form induced by φ and the lattice $L := \varphi(\mathbb{Z}^n)$.

Thus, we have a bijection between equivalence classes and $\mathbb{Z}$-lattices with integral square norms. In this thesis, for convenience we will use the identification between a quadratic form $Q(x)$ and the lattice $L = L(Q)$ via certain implicitly chosen φ. Therefore, when we say that a lattice has certain property, it means the corresponding quadratic form has such property. For example, the lattice $\mathbb{Z}^4$ is universal, by Largrange's theorem.

Under the above correspondence, if $e_1, ..., e_n$ is the standard basis of $\mathbb{R}^n$ so that $f_i := \varphi(f_i)$ is the corresponding $\mathbb{Z}$-basis of L, then the entries of the Gram matrix $A = (a_{ij})$ of $Q(x)$ can be expressed as

$$a_{ij} = (f_i, f_j). \tag{2.4.1}$$

Suppose $L \subset \mathbb{R}^n$ is a full $\mathbb{Z}$-lattice and let $f_1, ..., f_n$ be a $\mathbb{Z}$-basis of L. By (2.4.1), the lattice $2L$ is contained in the dual lattice L^* of L. Here

$$L^* := \{x \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z}, \text{for all } y \in L\} \tag{2.4.2}$$

which is spanned by the dual basis $f_1^*, ..., f_n^*$ satisfying

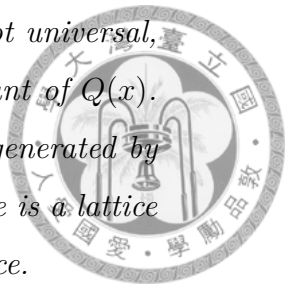
$$(f_i^*, f_j) = \delta_{i,j}, \tag{2.4.3}$$

where $\delta_{i,j}$ denotes the Kronecker symbol.

3 Escalation

The proofs of the main theorems are built on the concept of escalation. We also refer to the rank of a lattice as its dimension.

doi:10.6342/NTU201600288



Definition 3.1. *If a positive-definite integral quadratic form $Q(x)$ is not universal, we call the smallest positive integer that $Q(x)$ cannot represent the truant of $Q(x)$. We define an escalation of a non-universal L to be any integral lattice generated by L and a vector whose square-norm is the truant of L. An escalator lattice is a lattice which is obtained by consecutive escalations of the zero-dimensional lattice.*

Note that if a non-universal L is a full lattice in $\mathbb{R}^n$, then its escalation is a full lattice in either $\mathbb{R}^n$ or $\mathbb{R}^{n+1}$.

Lemma 3.2. *There are only finitely many escalator lattice of a given dimension n.*

Proof. We prove by induction on n. The unique escalation of the one-dimensional lattice is the lattice $\mathbb{Z} \subset \mathbb{R}$ corresponding to the quadratic form x^2. Hence the case $n = 1$ is proved. Suppose $L = \mathbb{Z}f + L_1$ is an n-dimensional escalation of an escalator lattice L_1 such that $\|f\|^2$ equals the truant a of L_1.

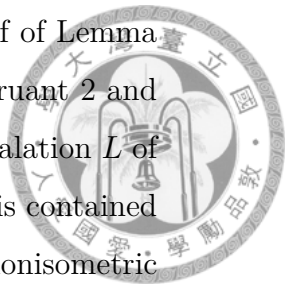
We first consider the case where L_1 is of dimension $n-1$ and let $f_1, ..., f_{n-1}$ be a $\mathbb{Z}$-basis. Write $f = \alpha e_n + f'$, where $e_n \in \mathbb{R}^n$ is the standard unit vector perpendicular to $\mathbb{R}^{n-1}$ and $f' \in R^{n-1}$. By (2.4.1), the value

$$(f', f_i) = (f, f_i)$$

must be either an integer or a half integer. Hence by (2.4.3), the vector $f' \in \frac{1}{2}L_1^*$. The discrete subgroup $\frac{1}{2}L_1^* \subset \mathbb{R}^{n-1}$ contains only finitely many vectors f' with $\|f'\|^2 < a$. For each such f', the number α must equal $\pm\sqrt{a - \|f'\|^2}$. Hence a given L_1 can only have finitely many escalations. This together with the induction hypothesis implies that there are finitely many n-dimensional escalation of escalator lattice of dimension $n-1$. Finally, we note that if L_1 is n-dimensional with $f_1, ..., f_n$ as a $\mathbb{Z}$-basis and L is an n-dimensional integral lattice containing L_1, then by (2.4.1), for every $f \in L$, the values (f, f_i), $i = 1, ..., n$ are in $\frac{1}{2}\mathbb{Z}$, and hence $L \in \frac{1}{2}L_1^*$, by (2.4.3). Therefore, $L/L_1 \subset \frac{1}{2}L_1^*/L_1$ which is finite, and hence there are only finitely many such L. In particular, there can only be finitely many n-dimensional escalator lattices containing L_1.

□

doi:10.6342/NTU201600288



To determine escalator lattices of low dimensions, we follow the proof of Lemma 3.2. The only 1-dimensional escalator lattice is $L_1 = \mathbb{Z} \subset R$ with with truant 2 and $L_1^* = L_1$. Denote $f_1 = 1 \in L_1$. Since no vector in $\frac{1}{2}L_1$ represents 2, an escalation L of L_1 must be 2-dimensional with $L = \mathbb{Z}f + L_1$ and $f = \alpha e_2 + xf_1$. Now x is contained in $\frac{1}{2}\mathbb{Z}$ satisfying $x^2 < 2$. Therefore, $x = 0, \pm\frac{1}{2}, \pm 1$. These gives three nonisometric two-dimensional escalators having Minkowski-reduced matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The corresponding lattices are $\mathbb{Z}\sqrt{2}e_2 + \mathbb{Z}f_1$, $\mathbb{Z}(\frac{\sqrt{7}}{2}e_2 + \frac{1}{2}f_1) + \mathbb{Z}f_1$, and $\mathbb{Z}e_2 + \mathbb{Z}f_1$ whose truants are respectively 5, 3, and 3. It turns out that all these three lattices have no 2-dimensional escalations. Escalating them, we obtain 34 three-dimensional nonisometric escalator lattices which have no three-dimensional escalations, and there are actually 6560 four-dimensional nonisometric escalations of these 34 lattices, [6]. We call these *the basic* escalators.

Lemma 3.3. *Each universal positive-definite integral quadratic form must contain a universal escalator lattice. Conversely, the truant of any non-universal form is the same as the truant of some non-universal escalator lattice within it.*

Proof. Let Q be a positive-definite integral quadratic form and denote $L = L(Q)$. There exists a maximal sequence of escalator lattices

$$\{0\} \subset L_1 \subset L_2 \subset \ldots \subset L_k$$

within L. Since L_k is maximal, it is either universal or having the same truant as that of L. Because $L_k \subset L$, if L_k is universal, so is L. □

4 The $\mathbb{Z}_p$-theory

To see if an integral quadratic form represents an integer m, we can first check if it represents m locally. In this section, we study the local theory of quadratic forms. Let p be a finite prime number. A quadratic form $Q(x)$ is called $\mathbb{Z}_p$-integral if and

doi:10.6342/NTU201600288

only if $Q(x) \in \mathbb{Z}_p[x]$. Two $\mathbb{Z}_p$-integral quadratic forms Q and Q' are $\mathbb{Z}_p$-equivalent if and only if their Gram matrices A and A' satisfy

$$A' = B^T AB, \text{ for some } B \in \mathrm{GL(n, \mathbb{Z}_p)}.$$

4.1 The normalized form

Definition 4.1. *A quadratic form $Q(x)$ is $\mathbb{Z}_p$-elementary if and only if either $Q(x)$ is one-dimensional equal to ux^2, $u \in \mathbb{Z}_p^*$, or $p = 2$ and $Q(x)$ is 2-dimensional with Gram matrix $\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$, such that $a_{11}, a_{22} \in \mathbb{Z}_2$ and $2a_{12}, 2a_{21} \in \mathbb{Z}_2^*$.*

Definition 4.2. *An n-dimensional $\mathbb{Z}_p$-integral quadratic form $Q(x)$ is a normalized form if and only if there is a partition P of $\{1, ..., n\}$ such that*

$$Q(x) = \sum_{J \in P} p^{\nu_J} Q_J(x_J), \tag{4.1.1}$$

where each Q_J is $\mathbb{Z}_p$-elementary and each $\nu_J \geq 0$.

Lemma 4.3. *Every quadratic form $Q(x)$ is $\mathbb{Z}_p$-equivalent to a normalized form.*

Proof. Let $A = (a_{ij})$ denote the Gram matrix of $Q(x)$. We prove by induction on n, the dimension of $Q(x)$. If $\dim Q = 1$, the lemma obviously holds. We first consider the case in which $p \neq 2$. Suppose $\min\{\mathrm{ord}_p(a_{ij}) \mid 1 \leq i, j \leq n)$ occurs at some $i = j$. We may assume it occurs at $i = j = 1$. By completing the squares, we can cancel $a_{12}, \ldots, a_{1n}$ as well as $a_{21}, \ldots, a_{n1}$. Then

$$Q(x) \simeq p^{\mathrm{ord}_p a_{11}} \cdot x_1^2 \oplus Q' \tag{4.1.2}$$

with $\dim Q' = n - 1$. Then the proof is completed by the induction hypothesis.

Suppose $\min\{\mathrm{ord}_p(a_{ij} \mid 1 \leq i, j \leq n)$ does not occur at diagonal entries. We may assume it equals to $\mathrm{ord}_p a_{12}$. Then we add the second column and the second row into the first ones. By this process, a_{11} is replaced by $a_{11} + 2a_{12} + a_{22}$. Since $\mathrm{ord}_p(a_{11}+2a_{12}+a_{22}) = \mathrm{ord}_p(a_{12}) = \min\{\mathrm{ord}_p(a_{ij}) \mid 1 \leq i, j \leq n)$, the proof is reduced the previous case.

doi:10.6342/NTU201600288

Now we consider the $p = 2$ case. Similarly, if $\min\{\mathrm{ord}_p(a_{ij}) \mid 1 \le i, j \le n)$ occurs at some diagonal entry, the lemma is proved by completing the squares. Otherwise, we may assume

$$\min\{\mathrm{ord}_p(a_{ij}) \mid 1 \le i, j \le n) = \mathrm{ord}_p(a_{12}) = k.$$

Write the leading 2×2 submatrix as

$$p^{k-1} \begin{pmatrix} p^{\alpha} b_{11} & b_{12} \\ b_{12} & p^{\beta} b_{22} \end{pmatrix} := p^{k-1} E, \tag{4.1.3}$$

where $\alpha, \beta \ge 1$ and $\mid b_{12} \mid_p = \mid b_{21} \mid_p = 1$. Then,

$$|\det E|_p = |p^{\alpha+\beta} b_{11} b_{22} - b_{12} b_{21}|_p = 1. \tag{4.1.4}$$

Since its determinant is a unit in $\mathbb{Z}_2$, the matrix E is invertible. Write

$$A = \begin{pmatrix} p^{k-1} E & p^{k-1} C \\ p^{k-1} C^T & U \end{pmatrix},$$

for some matrices C and U. Define $F := -E^{-1} C$ and put

$$B := \begin{pmatrix} I_2 & F \\ F^T & I_{n-2} \end{pmatrix}.$$

Then

$$B^T A B = \begin{pmatrix} p^{k-1} E & 0 \\ 0 & A' \end{pmatrix},$$

for some $(n-2) \times (n-2)$ matrix A'. This means $Q(x) \simeq p^k Q_1 \oplus Q'$, where Q_1 has $p^{-1} E$ as its Gram matrix and $\dim Q' = n - 2$. By the induction hypothesis, the proof is complete. □

Lemma 4.4. *Let $Q(x)$ be an integral quadratic form. Then the following statements are equivalent:*

(a) $p \mid N_Q$,

(b) $p \mid D_{2Q}$,

doi:10.6342/NTU201600288

(c) *if $Q(x)$ is $\mathbb{Z}_p$-equivalent to a normalized form expressed by* (4.1.1)*, then either some $v_J \geq 1$, or $p = 2$ and some Q_J is 1-dimensional.*

Proof. By lemma 4.3, we may assume that $Q(x)$ is $\mathbb{Z}_p$-equivalent to a normalized form expressed by (4.1.1). We have $\mathrm{ord}_p(D_{2Q}) = \sum_{J\in P} \lambda'_J$, where

$$\lambda'_J = \begin{cases} \nu_J + \mathrm{ord}_p(2), & if \ \dim Q_J = 1; \\ 2\nu_J, & if \ \dim Q_J = 2, \end{cases}$$

and also $\mathrm{ord}_p(N_Q) = \max_{J\in P} \lambda''_i$, where

$$\lambda''_i = \begin{cases} \nu_J + 2\,\mathrm{ord}_p(2), & if \ \dim Q_J = 1, \\ \nu_J, & if \ \dim Q_J = 2. \end{cases}$$

□

4.2 The reduction maps

Let $Q(x)$ be a normalized form expressed by (4.1.1) and set

$$S_0 := \{J \in P \mid \nu_J = 0\},\ S_1 := \{J \in P \mid \nu_J = 1\}, \text{ and } S_2 := \{J \in P \mid \nu_J \geq 2\}.$$

Definition 4.5. *For a given $m \in \mathbb{Z}_p$, define*

$$\begin{aligned} R_{p^k,Q}(m) &:= \{x \in \mathbb{Z}_p^n/p^k\mathbb{Z}_p^n \mid \ Q(x) \equiv m \pmod{p^k}\}, \\ R^{Zero}_{p^k,Q}(m) &:= \{x \in R_{p^k,Q}(m) \mid \ x \equiv 0 \pmod{p}\}, \\ R^{Good}_{p^k,Q}(m) &:= \{x \in R_{p^k,Q}(m) \mid \ p^{\nu_J} x_J \not\equiv 0 \pmod{p},\ for\ some\ J \in P\}, \\ R^{Bad}_{p^k,Q}(m) &:= \{x \in R_{p^k,Q}(m) \mid \ x \not\equiv 0\ but\ x_{S_0} \equiv 0 \pmod{p}\}, \end{aligned}$$

and let $r_{p^k,Q(m)}$, $r^{Zero}_{p^k,Q(m)}$, $r^{Good}_{p^k,Q(m)}$ and $r^{Bad}_{p^k,Q(m)}$ denote respectively the cardinality of the sets $R_{p^k,Q}(m)$, $R^{Zero}_{p^k,Q}(m)$, $R^{Good}_{p^k,Q}(m)$ and $R^{Bad}_{p^k,Q}(m)$.

Remark 4.6. *We have*

$$R_{p^k,Q}(m) = R^{Zero}_{p^k,Q}(m) \sqcup R^{Good}_{p^k,Q}(m) \sqcup R^{bad}_{p^k,Q}(m).$$

Also, if $p \nmid m$, then $R_{p^k,Q}(m) = R^{Good}_{p^k,Q}(m)$; if $p \nmid N_Q$, then $R^{Bad}_{p^k,Q}(m) = \emptyset$.

Now, reduction maps of various types are in order.

doi:10.6342/NTU201600288

4.2.1 The reduction map of good type

Definition 4.7. *Let* $\pi_G : R^{Good}_{p^k,Q}(m) \longrightarrow R^{Good}_{p^{k-1},Q}(m)$ *denote the reduction map sending* $x \pmod{p^k\mathbb{Z}_p}$ *into* $x \pmod{p^{k-1}\mathbb{Z}_p}$.

Lemma 4.8. *For* $k \geq 2\,\mathrm{ord}_p\, 2 + 1$, *the map* π_G *is surjective with multiplicity* p^{n-1}, *namely,*

$$r^{Good}_{p^{k+1},Q}(m) = p^{(n-1)} \cdot r^{Good}_{p^k,Q}(m).$$

Proof. This is a direct consequence of Hensel's Lemma [10, §I.3 Theorem 3]. □

4.2.2 The reduction map of zero type

If $x \in R^{Zero}_{p^k,Q}(m)$, then $x \mid p$ and hence $p^2 \mid m$.

Definition 4.9. *If* $R^{Zero}_{p^k,Q}(m)$ *is nonempty, define the reduction map*

$$\pi_Z : R^{Zero}_{p^k,Q}(m) \longrightarrow R_{p^{k-2},Q}(\frac{m}{p^2})$$

to be the one sending $x \pmod{p^k\mathbb{Z}_p}$ *into* $\frac{x}{p} \pmod{p^{k-1}\mathbb{Z}_p}$.

Obviously, the following lemma holds.

Lemma 4.10. *This map is surjective with multiplicity* p^n

4.2.3 The reduction map of bad type

Define $Q'(x) = \sum_{J\in P} p^{\nu'_J} Q_J$ and $Q''(x) = \sum_{J\in P} p^{\nu''_J} Q_J$, where

$$\nu'_J = \begin{cases} \nu_J + 1, & if\ J \in S_0; \\ \nu_J - 1, & if\ J \notin S_0, \end{cases} \qquad \nu''_J = \begin{cases} \nu_J, & if\ J \in S_0 \bigcup S_1; \\ \nu_J - 2, & if\ J \in S_2. \end{cases}$$

Denote, for $i = 0, 1, 2$,

$$R^{x_{S_i}\not\equiv 0}_{p^k,Q}(m) := \{x \in R_{p^{k-2},Q}(m) \mid x_{S_i} \not\equiv 0 \pmod{p^k}\},$$

and also

$$R^{Bad,\ x_{S_1}\not\equiv 0}_{p^k,Q}(m) = \{x \in R^{Bad}_{p^k,Q}(m) \mid x_{S_1} \not\equiv 0 \pmod{p}\},$$
$$R^{Bad,\ x_{S_1}\equiv 0}_{p^k,Q}(m) = \{x \in R^{Bad}_{p^k,Q}(m) \mid x_{S_1} \equiv 0 \pmod{p}\}.$$

doi:10.6342/NTU201600288

Definition 4.11. *If $S_1 \neq \emptyset$ define*

$$\pi_{B'} : R_{p^k,Q}^{Bad,\ x_{\mathbb{S}_1}\not\equiv 0}(m) \longrightarrow R_{p^{k-1},Q'}^{Good}(\frac{m}{p})$$

to be the map sending $x_J \pmod{p^k}$ into $\frac{x_J}{p} \pmod{p^{k-1}}$, for $J \in S_0$; and $x_J \pmod{p^k}$ into $x_J \pmod{p^{k-1}}$, otherwise.

Lemma 4.12. *The map $\pi_{B'}$ is surjective with multiplicity $p^{\#S_1 \bigcup S_2}$.*

Proof. We can choose arbitrary lift of $x_J \pmod{p^{k-1}}$ for $J \in S_1 \bigcup S_2$. □

Definition 4.13. *If $S_1 = \emptyset$ or $x_{S_1} \equiv 0 \pmod{p}$, define*

$$\pi_{B''} : R_{p^k,Q}^{Bad,\ x_{S_1}\equiv 0}(m) \longrightarrow R_{p^{k-2},Q''}^{x_{S_2}\not\equiv 0}(\frac{m}{p^2})$$

to be the map sending $x_J \pmod{p^k}$ into $\frac{x_j}{p} \pmod{p^{k-2}}$, if $J \in S_0 \bigcup S_1$; $x_J \pmod{p^k}$ into $x_J \pmod{p^{k-2}}$, otherwise.

Similarly, the folllowing lemma holds.

Lemma 4.14. *The map $\pi_{B''}$ is surjective with multiplicity $p^{\#S_0 \bigcup S_1 + 2\#S_2}$.*

4.2.4 The depth

Definition 4.15. *We define the depth of each type of solution of $R_{p^k,Q}(m)$ to be the maximal difference $k - k'$ for any $x \in R_{p^k,Q}(m)$ to be mapped into $R_{p^{k'},Q^*}(m^*)$ under consecutive application of the maps π_G, π_Z, and $\pi_{B'}$, or $\pi_{B''}$ for some Q^* and m^**

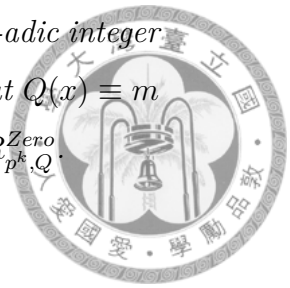
Under these definitions, we can easily gain the depth of each type:

Lemma 4.16. *The Good-, Zero-, Bad-type depths of $R_{p^k,Q}(m)$ are bounded above by $k-1$, $ord_p(m)$, and $ord_p(N_Q)+1$ respectively.*

4.3 The representability

We say that an n-dimensional $\mathbb{Z}_p$-integral form $Q(x)$ *represents* a p-adic integer m, if and only if there is some *non-zero* $x \in \mathbb{Z}_p^n$ such that $Q(x) = m$, while when referring to "$Q(x)$ representing $m \pmod{p^k}$", we use the following definition.

doi:10.6342/NTU201600288



Definition 4.17. *An n-dimensional $\mathbb{Z}_p$-integral form $Q(x)$ represents a p-adic integer m modulo p^k if and only if there is some $x \in \mathbb{Z}_p^n$, $x \not\equiv 0 \pmod{p}$ such that $Q(x) \equiv m \pmod{p^k}$. In other words, $x \pmod{p^k}$ is contained in $R_{p^k,Q}$ but not in $R_{p^k,Q}^{Zero}$.*

For $n \geq 3$, we have the following useful results. Define

$$R_Q(m) := \{\tilde{x} \in \mathbb{Z}_p^n \mid \ Q(\tilde{x}) = m, \ \tilde{x} \not\equiv 0 \pmod{p}\},$$

and for $i = 0, 1, 2$,

$$R_Q^{\tilde{x}_{S_i} \equiv 0}(m) := \{\tilde{x} \in \mathbb{Z}_p^n \mid \ Q(\tilde{x}) = m, \ \tilde{x}_{S_i} \equiv 0 \pmod{p}\},$$

$$R_Q^{\tilde{x}_{S_i} \not\equiv 0}(m) := \{\tilde{x} \in \mathbb{Z}_p^n \mid \ Q(\tilde{x}) = m, \ \tilde{x}_{S_i} \not\equiv 0 \pmod{p}\}.$$

Lemma 4.18. *Let Q be an n-dimensional $\mathbb{Z}_p$-integral quaderatic form. If $n \geq 3$ and $p \nmid N_Q$, then $Q(x)$ represents every p-adic integer m.*

Proof. First assume that $p \neq 2$. Then $Q(x)$ is $\mathbb{Z}_p$-equivalent to the normalized form $u_1x_1^2 + \cdots + u_nx_n^2$, with $u_1, ..., u_n \in \mathbb{Z}_p^*$. By [10, §1.62 Corollary 2, p. 393 Theorem 5], $Q(x)$ represents $m \pmod{p}$, and hence $R_{p,Q}^{Good}(m)$ is non-empty. Then we apply Lemma 4.8.

Suppose $p = 2$. By Lemma 4.4, n must be even, and hence $n \geq 4$. Thus,

$$Q(x) = Q_1(x_1, x_2) + Q_2(x_3, x_4) + Q'(x'),$$

where x' is either (if $n = 4$) trivial or equals $(x_5, ...x_n)$ (if $n > 4$) and

$$Q_1(x_1, x_2) = 2^{\alpha_1}a_1x_1^2 + u_1x_1x_2 + 2^{\beta_1}b_1x_2^2, \ \ a_1, b_1, u_1 \in \mathbb{Z}_2^*, \ \ \alpha_1, \beta_1 > 0,$$

$$Q_2(x_3, x_4) = 2^{\alpha_2}a_2x_3^2 + u_2x_3x_4 + 2^{\beta_2}b_2x_4^2, \ \ a_1, b_1, u_1 \in \mathbb{Z}_2^*, \ \ \alpha_2, \beta_2 > 0.$$

Because $Q_1(1, 1) \in \mathbb{Z}_2^*$ and $Q_1(x_1 + 2, x_2) \equiv Q_1(x_1, x_2) + 2u_1x_2 \pmod{8}$, we see that $Q_1(x_1, x_2)$ represents all odd integers modulo 8. Therefore, $Q_1(x_1, x_2) + Q_2(x_3, x_4)$ represents all integers modulo 8 and so is $Q(x)$. Then apply again Lemma 4.8.

□

Lemma 4.19. *Let Q be an n-dimensional $\mathbb{Z}_p$-integral quaderatic form with $n \geq 3$ and $p \mid N_Q$. A integer m is represented by $Q(x)$ over $\mathbb{Z}_p$ if and only if some quotient of m by square factor is represented by $Q(x)$ modulo $p^{ord_p(4N_Q)+2}$.*

doi:10.6342/NTU201600288

Proof. If $Q(x) = m$ in $\mathbb{Z}_p$ and $x = p^\nu x'$ with $x' \in \mathbb{Z}_p$ such that $x' \not\equiv 0 \pmod{p}$, then $Q(x') \equiv \frac{m}{p^{2\nu}} \pmod{p^{\mathrm{ord}_p(4N_Q)+2}}$ as desired.

To prove the implication in the other direction, we may assume that $Q(x)$ represents m modulo $p^{ord_p(4N_Q)+2}$. Put $k = \mathrm{ord}_p(4N_Q) + 2$. Suppose $Q(x) \equiv m \pmod{p^k}$ and $x \not\equiv 0 \pmod{p}$, then $x \notin R^{Zero}_{p^k,Q}(m)$.

If $x \in R^{Good}_{p^k,Q}(m)$, then we apply Lemma 4.8 to ensure the existence of some $\tilde{x} \in R_Q^{\tilde{x}\not\equiv 0}(m)$ such that $\tilde{x} \equiv x \pmod{p^k}$. In particular, $R_Q(m)$ is non-empty.

If $x \in R^{Bad,\ x_{S_1}\not\equiv 0}_{p^k,Q}(m)$, then $\pi_{B'}(x) \in R^{Good}_{p^{k-1},Q'}(\frac{m}{p})$ and since $k - 1 \geq 2\,\mathrm{ord}_p 2 + 1$, Lemma 4.8 is applicable. Therefore, there there exists some $\tilde{t} \in R_{Q'}^{\tilde{x}_{S_0}\not\equiv 0}(\frac{m}{p})$ such that $\tilde{t} \equiv \pi_{B'}(x) \pmod{p^{k-1}}$. Consider the commutative diagram

$$\begin{array}{ccc} R_Q^{\tilde{x}_{S_1}\not\equiv 0}(m) & \xrightarrow{\varphi'} & R_{Q'}^{\tilde{x}_{S_0}\not\equiv 0}(\frac{m}{p}) \\ \downarrow & & \downarrow \\ R^{Bad,\ x_{S_1}\not\equiv 0}_{p^k,Q}(m) & \xrightarrow{\pi_{B'}} & R^{Good}_{p^{k-1},Q'}(\frac{m}{p}), \end{array}$$

where down-arrows are respectively reduction modulo p^k and p^{k-1}, while φ' is the bijection sending $\tilde{x}$ to $\tilde{t}$ with $\tilde{t}_{S_0} = \frac{1}{p} \cdot \tilde{x}_{S_0}$ and $\tilde{t}_{S_1 \cup S_2} = \tilde{x}_{S_1 \cup S_2}$. The diagram shows $R_Q^{\tilde{x}_{S_1}\not\equiv 0}(m)$, end hence $R_Q(m)$ is non-empty.

If $x \in R^{Bad,\ x_{S_1}\equiv 0}_{p^k,Q}(m)$, then we apply the reduction map $\pi_{B''}$ consecutively k' times until the image of x launches either $R^{Bad,\ x_{S_1}\not\equiv 0}_{p^{k-2k'},Q^*}(\frac{m}{p^{2k'}})$ or $R^{Good}_{p^{k-2k'},Q^*}(\frac{m}{p^{2k'}})$. Since we have $N_{Q^*} \leq p^{-2k'} N_Q$, Lemma 4.8 is applicable to $Q^*(x)$ and $\frac{m}{p^{2k'}}$. To reduce the proof to the previous cases, we only need to consider the bijection

$$\varphi'' : R_Q^{\tilde{x}_{S_0}\equiv 0}(m) \cap R_Q^{\tilde{x}_{S_1}\equiv 0}(m) \longrightarrow R_{Q''}(\frac{m}{p^2})$$

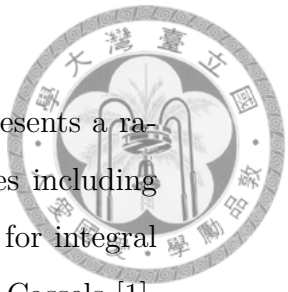
as well as the associated commutative diagrams:

$$\begin{array}{ccc} R_Q^{\tilde{x}_{S_0}\equiv 0}(m) \cap R_Q^{\tilde{x}_{S_1}\equiv 0}(m) & \xrightarrow{\varphi''} & R_{Q''}(\frac{m}{p^2}) \\ \downarrow & & \downarrow \\ R^{Bad,\ x_{S_1}\equiv 0}_{p^k,Q}(m) & \xrightarrow{\pi_{B''}} & R_{p^{k-1},Q''}(\frac{m}{p^2}). \end{array}$$

Here, if $\tilde{t} = \varphi''(\tilde{x})$, then $\tilde{t}_{S_0 \cup S_1} = \frac{1}{p}\tilde{x}_{S_0 \cup S_1}$ and $\tilde{t}_{S_2} = \tilde{x}_{S_2}$. □

doi:10.6342/NTU201600288

5 The local-global principle



The Hasse-Minkowski theorem says a $\mathbb{Q}$-rational quadratic form represents a rational number if and only it represents this number locally at all primes including the infinite prime. This local-global principle also holds to some extend for integral forms. In this section, we review such wonderful theory, our reference is Cassels [1]. The main result is Theorem 5.3 below. For convenience, denote

$$\mathbb{Z}_\infty = \mathbb{R}.$$

Definition 5.1. *Two integral quadratic forms are in the same genus if and only if they are $\mathbb{Z}_p$-equivalent at all primes including the infinite one. The number of integral equivalence classes in a given genus is called the class number.*

Lemma 5.2. *The class number of a genus is finite.*

Proof. Two forms in the same genus must be of the same determinant, while the number of integral equivalence classes in the collection of forms of a given determinant is finite (Lemma 2.3). □

Theorem 5.3. *Let $Q(x)$ be an integral form in n variables of determinant $d \neq 0$. Let $a \neq 0$ be an integer which is represented by $Q(x)$ over $\mathbb{Z}_p$, for $p = \infty, 2, 3, \ldots$, then there exists some form $Q^*(x)$ in the same genus of $Q(x)$ representing a.*

The above two theorems will be proved at the end of this section.

5.1 Basic results

The following results are consequence of Lemma 4.3 or linear algebra over $\mathbb{Z}$ or $\mathbb{Z}_p$. We omit their proofs.

Lemma 5.4. *Let p be a finite prime number. Suppose f_1 and f_2 are two $\mathbb{Z}_p$-integral forms and that $D_{f_1} = D_{f_2}$ is a unit in $\mathbb{Z}_p$, then these two forms are $\mathbb{Z}_p$-equivalent.*

Lemma 5.5. *Let p be a finite prime number and let $c_1, \ldots, c_J$ be linearly independent elements in $\mathbb{Z}_p^n$. Then the following three conditions are all equivalent:*

doi:10.6342/NTU201600288

(i) *There exist* $c_{J+1}, \ldots, c_n$ *such that* $c_1, \ldots, c_n$ *forms a basis for* $\mathbb{Z}_p^n$.

(ii) *The* $n \times J$ *matrix* $c_1, \ldots, c_J$ *contains a* $J \times J$ *minor whose determinant is a* p*-adic unit.*

(iii) *If* $a = l_1 c_1 + \cdots + l_J c_J \in \mathbb{Z}_p^n$ *for some* $l_1, \cdots, l_J \in \mathbb{Q}_p$, *then it must imply the result* $l_1, \cdots, l_J \in \mathbb{Z}_p$.

Lemma 5.6. *Let* $c_1, \ldots, c_J$ *be elements in* $\mathbb{Z}^n$. *Then the following three conditions are all equivalent:*

(i) *There exist* $c_{J+1}, \ldots, c_n$ *such that* $c_1, \ldots, c_n$ *forms a basis for* $\mathbb{Z}^n$.

(ii) *The determinants of the* $J \times J$ *submatrices of the* $n \times J$ *matrix* $(c_1, \ldots, c_n)$ *have no common divisor larger than 1.*

(iii) *If* $a = l_1 c_1 + \cdots + l_J c_J \in \mathbb{Z}^n$ *for some* $l_1, \cdots, l_J \in \mathbb{Q}$, *then it must imply the result* $l_1, \cdots, l_J \in \mathbb{Z}$.

5.2 The approximation of $\mathbb{Z}_p$-forms

We first prove the following lemma on the simultaneous approximation. Let P denote a given collection of finitely many prime numbers.

Lemma 5.7. *Let* $K > 1$ *be an integer and let* $m_k^{(p)} \in \mathbb{Z}_p$, $1 \le k \le K$, $p \in P$, *be given such that for every* $p \in P$,

$$\max_{1 \le k \le K} |m_k^{(p)}|_p = 1. \tag{5.2.1}$$

Then for each $\epsilon > 0$, *there exist* $m_k \in \mathbb{Z}$, $1 \le k \le K$, *with*

$$\gcd(m_1, \ldots, m_k) = 1,$$

such that

$$|m_k - m_k^{(p)}|_p < \varepsilon, \quad \textit{for all } p \in P. \tag{5.2.2}$$

Proof. By the Chinese Remainder Theorem, we pick $m_1 \neq 0$ such that (5.2.2) holds for $k = 1$. Let P^* be the set of primes p^* which divide m_1 but are not in P. Again,

doi:10.6342/NTU201600288

apply the Chinese Remainder Theorem, we can find an $m_2 \in \mathbb{Z}$ such that (5.2.2) holds for $k = 2$, and

$$p^* \nmid m_2 \tag{5.2.3}$$

for all $p^* \in P^*$. Now, for $k > 2$ we choose $m_k \in \mathbb{Z}$ to satisfy (5.2.2). We may assume that $\varepsilon < 1$. Then (5.2.1) implies $\gcd(m_1, \ldots, m_k)$ is not divisible by any $p \in P$. The condition 5.2.3 ensures that it is not divisible by any other primes. Thus, the proof is complete. □

For a $\mathbb{Z}_p$-integral quadratic form $f(x)$ in n-variables with $D_f \neq 0$, let O_f denote the subgroup of $\mathrm{GL}(n, \mathbb{Z}_p)$ consisting of matrice τ such that $f(x) = f(\tau x)$. For such τ, we have $(\det \tau)^2 = 1$, and hence $\det \tau = \pm 1$.

Lemma 5.8. *Let $f(x)$ be a $\mathbb{Z}_p$-integral quadratic form in n-variables with $D_f \neq 0$. Then there exists $\tau_f \in \mathrm{O}_f$ such that $\det \tau_f = -1$.*

Proof. We first consider the case where $f(x)$ is $\mathbb{Z}_p$-elementary. If $f(x) = x^2$, then take $\tau_f = -1$. If $\dim f = 2$, then D_{2f} is a unit in $\mathbb{Z}_2^*$ and is $\equiv -u^2 \pmod{16}$, for some $u \in \mathbb{Z}_2^*$. This implies $D_{2f} = -\mu^2 + 16$ for some $\mu \in \mathbb{Z}_2^*$. Lemma 5.4 says $2f$ is $\mathbb{Z}_p$-equivalent to $2g(x) := 4x_1^2 + 2\mu x_1 x_2 + 4x_2^2$, and hence $f(x)$ is $\mathbb{Z}_p$-equivalent to $g(x)$. Take $\tau_g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and if $f(x) = g(Tx)$, take $\tau_f = T^{-1}\tau_g T$.

In general, by Lemma 4.3, we can assume that $f(x) = p^{\nu_{J_1}} f_1(x_{J_1}) + f_2(x_{J_2})$, where f_1 is $\mathbb{Z}_p$-elementary and $J_1 \sqcup J_2 = \{1, ..., n\}$. Take τ_f such that $\tau_f x_J = \tau_{f_1} x_J$ and $\tau_f x_{J_2} = x_{J_2}$. □

Lemma 5.9. *Let P be a finite set of prime numbers and let $Q(x)$ be an integral form of determinant $d \neq 0$. For each $p \in P$, let f_p be a $\mathbb{Z}_p$-integral form of determinant d which is $\mathbb{Z}_p$-equivalent to $Q(x)$. Then there exists a form $Q^*(x)$ which is integrally equivalent to $Q(x)$ and whose coefficients are arbitrarily close p-adically to f_p for each $p \in P$.*

Proof. By the hypothesis, for each $p \in P$, there exists a p-adic integral matrix T_p such that $f_p(x) = Q(T_p x)$. Since $D_{f_p} = D_f = d \neq 0$ and $(\det T_p)^2 = 1$, the determinant

doi:10.6342/NTU201600288

$\det T_p = \pm 1$. By Lemma 5.8, we may assume that $\det T_p = 1$. It is sufficient to construct a global integral matrix T with $\det T = 1$, which is p-adically arbitrarily close to each T_p. For such T, the quadratic form $Q^*(x) = Q(Tx)$ satisfies the required condition.

Write $T_p = (c_1^{(p)}, \ldots, c_n^{(p)})$ so that the columns $c_i^{(p)}$, $i = 1, ..., n$, form a basis for $\mathbb{Z}_p^n$, and denote

$$\|x\|_p = \max_{1 \le k \le n} | x_k |_p, \quad \text{for } x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n.$$

For $J = 1, ..., n$, we claim that *for every* $\varepsilon > 0$, *there exist* $c_1, \ldots, c_J \in \mathbb{Z}^n$ *extendable to a basis* $c_1, ..., c_j, b_{J+1}, \ldots, b_n$ *of* $\mathbb{Z}^n$ *such that*

$$\|c_j - c_j^{(p)}\|_p < \varepsilon, \quad \textit{for } p \in P, \ 1 \le j \le J. \tag{5.2.4}$$

Then the lemma is proved by taking $J = n$. We prove the claim by induction on J.

For $J = 1$ the claim follows from Lemma 5.5, 5.7 and 5.6. Suppose the claim holds for J and $c_1, \ldots, c_J, b_{J+1}, \ldots, b_n$. Then

$$c_{J+1}^{(p)} = l_1^{(p)} c_1 + \ldots + l_J^{(p)} c_J + m_{J+1}^{(p)} b_{J+1} + \ldots + m_n^{(p)} b_n,$$

for some $l_1^{(p)}, \ldots, l_J^{(p)}, m_{J+1}^{(p)}, \ldots, m_n^{(p)} \in \mathbb{Z}_p$. By Lemma 5.5, we have $\max_{J<j\le n} | m_j^{(p)} |_p = 1$. By Chinese Remainder Theorem, we can find $l_j \in \mathbb{Z}$ such that $| l_i - l_j^{(p)} |_p < \varepsilon$ for all $j \le J$ and $p \in P$. Assume that $J < n - 1$ so that $K := n - J > 1$ and Lemma 5.6 applicable. It ensures that we can find $m_j \in \mathbb{Z}$ for $J < j \le n$ satisfying $| m_j - m_j^{(p)} |_p < \varepsilon$ and $\gcd(m_{J+1}, \ldots, m_n) = 1$. Put

$$c_{J+1} = l_1 c_1 + \ldots + l_{J-} c_J + m_{J+1} b_{J+1} + \ldots + m_n b_n.$$

Then $\|c_{J+1} - c_{J+1}^{(p)}\|_p < \epsilon$, for all $p \in P$. Moreover, since $\gcd(m_{J+1}, \ldots, m_n) = 1$, by Lemma 5.6, $c_1, \ldots, c_{J+1}$ can be extended to a basis of $\mathbb{Z}^n$. Hence the claim holds for $J + 1$.

Now suppose $J = n - 1$. We may assume that b_n is chosen to have

$$\det(c_1, ..., c_{n-1}, b_n) = 1$$

doi:10.6342/NTU201600288

and that $c_1, \ldots, c_{n-1}$ are sufficiently close to $c_1^{(p)}, \ldots, c_{n-1}^{(p)}$ so that $c_1, \ldots, c_{n-1}, c_n^{(p)}$ forms a basis of $\mathbb{Z}_p^n$ and the determinant $\det_p := \det(c_1, \ldots, c_{n-1}, c_n^{(p)})$ sufficiently close to 1. Let $\widehat{c_n}^{(p)} := \frac{1}{\det_p} c_n^{(p)}$. Then $\det(c_1, \ldots, c_{n-1}, \widehat{c_n}^{(p)}) = 1$. Hence

$$\widehat{c_n}^{(p)} = \widehat{l_1}^{(p)} c_1 + \ldots + \widehat{l_{n-1}}^{(p)} c_{n-1} + b_n,$$

By Chinese Remainder Theorem, we pick $l_1, \ldots, l_{n-1}$ sufficiently close to $\widehat{l_1}^{(p)}, \ldots, \widehat{l_{n-1}}^{(p)}$, such that the vector

$$c_n := l_1 c_1 + \ldots + l_{n-1} c_{n-1} + b_n,$$

satisfies

$$\|c_n - c_n^{(p)}\|_p \leq \max\{\|c_n - \widehat{c_n}^{(p)}\|_p, \|\widehat{c_n}^{(p)} - c_n^{(p)}\|_p\} < \varepsilon.$$

The proof is complete. □

Lemma 5.10. *Let $f(x)$ and $g(x)$ be $\mathbb{Z}_p$-integral forms with Gram matrices F and G respectively. If*

$$2F \equiv 2G \pmod{p^{\delta+2\lambda+1}}, \tag{5.2.5}$$

where δ is defined by $\mid D_{2F} \mid_p = p^{-\delta}$ and $\lambda = \delta_{2,p}$ (the Kronecker symbol), then $f(x)$ and $g(x)$ are $\mathbb{Z}_p$-equivalent

Proof. Set

$$S := \frac{1}{2} F^{-1}(G - F) = \frac{1}{2}(2F)^{-1}(2G - 2F). \tag{5.2.6}$$

Suppose $2G \equiv 2F \pmod{p^\mu}$ with $\mu \geq \delta + 2\lambda + 1$.Then

$$2(\det 2F)S = (\text{adj } 2F)(2G - 2F) \equiv 0 \pmod{p^\mu}. \tag{5.2.7}$$

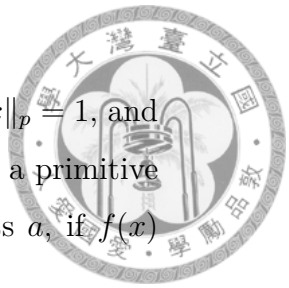
Since adj $2F$ is a $\mathbb{Z}_p$-integral matrix, $S \equiv 0 \pmod{p^{\mu-\delta-\lambda}}$. Put $F_1 = (I + S)^t F(I+S)$, so that

$$(G - F_1) = -S^t F S = -\frac{1}{2} S^t (G - F). \tag{5.2.8}$$

Then $2G - 2F_1) \equiv 0 \pmod{p^{2\mu-\delta-2\lambda}}$. Since $(2\mu - \delta - 2\lambda) > \mu$, we may replace F by F_1 and repeat the procedure to complete the proof. □

doi:10.6342/NTU201600288

5.3 The proofs of Theorem 5.3



For a finite prime number, we say an element $x \in \mathbb{Z}_p^n$ is primitive if $\|x\|_p = 1$, and $a \in \mathbb{Z}_p$ is primitively represented by a quadratic form $f(x)$ if there exists a primitive element $b \in \mathbb{Z}_p^n$ with $a = f(b)$. For $p = \infty$, $f(x)$ primitively represents a, if $f(x)$ represents a.

Theorem 5.11. *Let $n \in \mathbb{N}$ and $d \neq 0$ be given. Let f_p be a n-dimensional $\mathbb{Z}_p$-integral form of determinant d, for all $p = \infty, 2, 3, \ldots$. Suppose there exists a rational form $R(x)$ which is $\mathbb{Q}_p$-equivalent to $f_p(x)$ for each p. Then there is a $\mathbb{Z}$-integral form $Q(x)$ which is $\mathbb{Z}_p$-equivalent to f_p for each p, and $\mathbb{Q}$-equivalent to $R(x)$. Moreover, if each $f_p(x)$ primitively represents a rational integer a, then $Q(x)$ represents a.*

Proof. We prove by induction on the dimension n. When $n = 1$, $f_p(x) = dx_1^2$ for all p. The theorem holds for $Q(x) = dx_1^2$. Indeed, if $f_p(x)$ primitively represents a, for all p, then $d = a$, and hence $Q(1) = a$ as required. For the rest of the proof, assume that $n \geq 2$ and the theorem holds for $n - 1$.

Next, we claim that there is an integer c primitively represented by f_p for all p over $\mathbb{Z}_p$ and by $R(x)$ over $\mathbb{Q}$. To show it, let b be any non-zero integer such that $b = R(x)$ where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Q}^n$. Let $B = (B_{ij})$ be the gram matrix of $R(x)$ and write $B_{ij} = U_{ij}/V_{ij}$ with $U_{ij}, V_{ij} \in Z$, $\gcd(U_{ij}, V_{ij}) = 1$. Also write $x_i = s_i/t_i$, $s_i, t_i \in \mathbb{Z}$ with $\gcd(s_i, t_i) = 1$. Let P be the set of primes dividing $2bd$, U_{ij}, V_{ij}, s_i and t_i. For $p \notin P$, $R(x)$ is a $\mathbb{Z}_p$-integral form primitively representing b. Since d is a p-adic unit, by Lemma 5.4, f_p is $\mathbb{Z}_p$-equivalent to $R(x)$, and hence primitively represents b. For $p \in P$, since f_p is $\mathbb{Q}_p$-equivalent to $R(x)$, f_p represents b over $\mathbb{Q}_p$. Suppose $b = f_p(x_p)$ for $x_p \in \mathbb{Q}_p^n$. We may choose $\beta(p) \in \mathbb{Z}$ so that $\|p^{\beta(p)} x_p\|_p = 1$. Then take $c = b \prod_{p \in P} p^{2\beta(p)}$ for the claim.

Now let a be an integer primitively represented by f_p over $\mathbb{Z}_p$, for all p. By lemma 5.5, we may assume $f_p(1, 0, \ldots, 0) = a$ for all p. Also, by Hasse-Minkowski Theorem, $R(x)$ represents a over $\mathbb{Q}$, and we may assume $R(1, 0, \ldots, 0) = a$. By completing the square, we have

$$4a f_p(x) = (2ax_1 + b_{2p}x_2 + \ldots + b_{np}x_n)^2 + f_p^*(x_2, \ldots, x_n)$$

doi:10.6342/NTU201600288

for some $b_{2p}, \ldots, b_{np} \in \mathbb{Z}_p$, where $f_p^*(x)$ is a $\mathbb{Z}_p$-integral form in $(n-1)$-variables with determinant $d^* = a^{(n-2)}d$. Similarly,

$$4aR(x) = (2ax_1 + c_2x_2 + \ldots + b_nx_n)^2 + R^*(x_2, \ldots, x_n)$$

for some $c_2, \ldots, c_n \in \mathbb{Q}$ and some rational form $R^*(x)$ in $(n-1)$-variables. Taking $y_1 = 2ax_1 + b_{2p}x_2 + \ldots + b_{np}x_n$, we can write

$$4af_p = y_1^2 + f_p^*(x_2, ..., x_n).$$

Similarly, by taking $z_1 = 2ax_1 + c_2x_2 + \ldots + b_nx_n$, we can write

$$4aR = z_1^2 + R^*(x_2, ...x_n).$$

Since y_1^2 is $\mathbb{Q}_p$-equivalent to z_1^2, by Witt's Theorem, $f_p^*(x_2, \ldots, x_n)$ is $\mathbb{Q}_p$-equivalent to $R^*(x_2, \ldots, x_n)$. By the induction hypothesis, there exists a global integral form $Q^*(x_2, \ldots, x_n)$ of determinant $d^* = D_{f_p^*} = (4a)^n d/a^2$ which is $\mathbb{Z}_p$-equivalent to $f_p^*(x_2, \ldots, x_n)$ for all p and $\mathbb{Q}$-equivalent to R^*. By Chinese Remainder Theorem, we can find $b_2, \ldots, b_n \in \mathbb{Z}$ arbitrarily close p-adically to $b_{2p}, \ldots, b_{np}$ for all $p \mid 2ad$. Moreover, by Lemma 5.9, we can replace Q^* by an equivalent form that is p-adically sufficiently close to f_p^* for all $p \mid 2ad$ so that the quadratic form $Q(x)$ defined by

$$4aQ(x) = (2ax_1 + b_2x_2 + \ldots + b_nx_n)^2 + Q^*(x_2, \ldots, x_n) \tag{5.3.1}$$

is an integral form. Since $D_{Q^*} = d^*$, $D_Q = d$. Obviously, $Q(1, 0, ..., 0) = a$. Since $Q(x)$ is sufficiently close p-adically to f_p for $p \mid 2d$, by lemma 5.10, $Q(x)$ and f_p are $\mathbb{Z}_p$-equivalent for these p. For $p \nmid 2d$, $p \neq \infty$, by Lemma 5.4, $Q(x)$ is automatically $\mathbb{Z}_p$-equivalent to f_p. For $p = \infty$, $Q(x)$ also $\mathbb{Z}_p$-equivalent to $f_p(x)$, because they have the same signature. Therefore, by Hasse-Minkowski Theorem, $Q(x)$ is $\mathbb{Q}$-equivalent to $R(x)$. The proof is complete. □

The proof of Theorem 5.3. If $p \nmid a$, $Q(x)$ must primitively represents a. Otherwise, we assume $Q(x_p) = a$ over $\mathbb{Z}_p$. Then $\|x_p p^{\beta(p)}\|_p = 1$ for some non-positive integers $\beta(p)$. We set $\hat{a} = a \prod_{p|a} p^{2\beta(p)}$. Since

$$|\ \hat{a}\ |_p = |\ a\ | \cdot |\ \prod_{p|a} p^{2\beta(p)}\ | = |\ f(x_p)\ | \cdot \frac{1}{p^{2\beta(p)}} \leq 1 \tag{5.3.2}$$

doi:10.6342/NTU201600288

so $\hat{a} \in \mathbb{Z}$. It is clear that $Q(x)$ primitively represents $\hat{a}$. Theorem 5.11 applied to the case where $f_p = Q(x)$ and $R(x) = Q(x)$ says there exists in the genus of $Q(x)$ a $\mathbb{Z}$-integral form $Q^*(x)$ that globally represents $\hat{a}$. Assume $Q^*(\xi) = \hat{a}$ for some $\xi \in \mathbb{Z}^n$.Then

$$Q^*(\xi \cdot \prod_{p|a} p^{-\beta(p)}) = a. \tag{5.3.3}$$

□

5.4 Example and conclusion

In some cases, we can apply the arithmetic method discussed in this section and the section before to find the set of integers which are represented by a four-dimensional escalator L_4. Suppose L_4 is the escalator of a three-dimensional sublattice L_3, which is unique in its genus. By Theorem 5.3, such L_3 represents all integers which is locally represented over $\mathbb{Z}_p$. We can use the information of L_3 to show that the direct sum of L_3 with orthogonal complement in L_4 represents all sufficiently large integers n locally represented by it. Thus, we only need to check the representability of small n to determine the set of integers which are represented by the four-dimensional escalator L_4.

For example, we consider the quadratic form $x^2 + y^2 + z^2$ and its corresponding lattice L_3. It is well known that a natural number n is represented by L_3 if and only if n is not of the form $4^a(8k + 7)$ [5]. Now $L_3^* = L_3$, and hence L_4 is generated by L_3 together with a vector $f = \alpha e_4 + f'$, such that $\|f\|^2 = 7$ and $f' \in \frac{1}{2}L_3$. If $f' \in L_3$, then $L_4 = L_3 \oplus \alpha e_4 =: L_3 \oplus [m]$, where $m = \alpha^2 = 1, 2, 3, 4, 5, 6$. If $f' \notin L_3$, then L_4 contains $L_3 \oplus 2\alpha e_4 := L_3 \oplus [m]$, where $m = 4\alpha^2 < 28$. In this case we can check that $4 \nmid m$ and $m \neq 21$. In both cases, we have L_4 conatins $L_3 \oplus [m]$ with $m \leq 27$ and $m \not\equiv 0 \pmod 8$. If L_4 were not universal and let u be the smallest natural number missed by L_4, then u is also missed by L_3. By the minimality, $u \equiv 7 \pmod 8$. Since L_4 represents 7, u is at least 15.

If $m \not\equiv 3, 7 \pmod 8$, then $u - m$ is not of the form $4^a(8k + 7)$. If $u - m > 0$, then it is represented by L_3, and hence u would be represented by L_4, which is absurd.

doi:10.6342/NTU201600288

Therefore, $u \leq m$. Thus, if $m \leq 14$, then L_4 is universal. One can check that in this case all possible L_4 are universal.

If $m \equiv 3, 7 \pmod 8$, then $u - 4m$ is not of the form $4^a(8k+7)$ and is represented by L_3 in case $u > 4m$. This implies $u \leq 4m$. Thus, if $m = 3$, then L_4 is universal. One can check that all possible L_4 in this case are also universal.

Among 34 three-dimensional basic escalator, 20 are unique in their genus. Moreover, the escalations of 17 of these 20 escalator lattices can be handled by this process. We can apply such arithmetic method to determine the sets of integers represented by 1658 of the 6560 basic four-dimensional escalators [6].

6 Analytic method

For basic 4-dimensional escalators on which the arithmetic method does not work well, one can apply the analytic method discussed in this section. The aim is to find for each form a lower bound of reasonable size such that every positive integer greater than this bound is represented by the given form if and only if it is locally represented by the form.

6.1 The theta function associated to 4-dimensional escalators

For a basic four-dimensional escalator $Q(x)$, we define the theta function associated with $Q(x)$ as

$$\Theta_Q(z) := \sum_{x \in \mathbb{Z}^4} e^{2\pi i Q(x) z} = \sum_{m \geq 0} r_Q(m) e^{2\pi i m z}$$

The theta function $\Theta_Q(z)$ is a modular form[6] of weight 2, and hence there exist an Eisenstein series $E(z)$ and a cusp form $f(x)$ such that

$$\Theta_Q(z) = E(z) + f(z).$$

We observe that $r_Q(m) > 0$ if and only if $Q(x)$ represents m. We have to compare the growth rates of Fourier coefficients $a_E(m)$ of $E(x)$ and $a_f(m)$ of $f(x)$ to establish an effective criterion for $r_Q(m) > 0$ for m sufficiently large by checking if m is locally represented by $Q(x)$.

doi:10.6342/NTU201600288

6.2 Fourier coefficients of Eisenstein series E(z)

Let $a_E(m)$ be as before. According to Segel's theory[8], we have

$$a_E(m) = \prod_{p=\infty,2,3,\ldots} \beta_p(m), \tag{6.2.1}$$

where

$$\beta_p(m) = \begin{cases} \lim\limits_{k\to\infty} \dfrac{r_{p^k,Q}(m)}{p^{(n-1)k}}, & \text{if } p \neq \infty; \\ \mu(\{x \in \mathbb{R}^4 \mid Q(x) = m\}), & \text{if } p = \infty, \end{cases} \tag{6.2.2}$$

and μ denotes the three-dimensional Lebesgue measure. By direct computation, we get

$$\beta_\infty(m) = \frac{2\omega_4 m}{\sqrt{det(Q)}}, \tag{6.2.3}$$

where ω_4 is the measure of four-dimensional unit ball. However, the evaluation of $a_E(m)$ needs more discussion.

Definition 6.1. *The discriminant of a non-singular quadratic form $f(x)$ in a field F is defined to be $d_F f := D_f \cdot (F^*)^2 \in F^* \Big/ (F^*)^2$.*

Definition 6.2. *A binary non-singular quadratic form $f(x)$ over a field F is called a hyperbolic plane if $f \simeq 2xy$, and an even-dimensional non-singular quadratic form is called hyperbolic if it is F-equivalent to a direct sum of some hyperbolic planes.*

The proofs of the following two basic lemmas can be found in[5]

Lemma 6.3. *Let $f(x)$ be a non-singular binary quadratic form in $\mathbb{F}_p$, $p \neq 2$, then the following are all equivalent:*

(i) *$f(x)$ is a hyperbolic plane.*

(ii) *$f(x)$ is isotropic, that is, there is some $a \in \mathbb{F}_p^*$ such that $f(a) = 0$.*

(iii) *$d_F f = -1$.*

Lemma 6.4. *Let $f(x)$ and $g(x)$ be two non-singular quadratic forms over $\mathbb{F}_p$, $p \neq 2$, then$f(x)$ is $\mathbb{F}_p$-equivalent to $g(x)$ if and only if $\dim f(x) = \dim g(x)$ and $d_{\mathbb{F}_p} f = d_{\mathbb{F}_p} g$.*

doi:10.6342/NTU201600288

Now, we compute $r_{p,Q}(m)$ as follow.

Lemma 6.5. *Let $Q(x)$ be positive integral quadratic form of dimension $2k$ and let $p \neq 2$ be a prime number not dividing N_Q. For an integer $m \not\equiv 0 \pmod{p}$, we have*

$$r_{p,Q}(m) = \frac{1}{p-1}(p^{2k} - r_{p,Q}(0)).$$

Proof. Put $Q^{(m)}(x) = mQ(x)$. Since the discriminants of $d_{\mathbb{F}_p}Q^{(m)} = d_{\mathbb{F}_p}Q$, Lemma 6.4 says $Q^{(m)}(x) \simeq Q(x)$ over $\mathbb{F}_p$. Therefore, the two sets $\{a \in \mathbb{F}_p^{2k} \mid Q(a) = 1\}$ and $\{a \in \mathbb{F}_p^{2k} \mid Q(a) = m\}$ have an one-to-one correspondence, hence $r_{p,Q}(m) = r_{p,Q}(1)$. By counting, we obtain the desired equality. □

Lemma 6.6. *Let $Q(x)$ be a four-dimensional positive integral quadratic form with $p \neq 2$ and $p \nmid N_Q$. The following holds:*

(i) *If $Q(x)$ is hyperbolic, then* $r_{p,Q}(m) = \begin{cases} p^3 + p(p-1), & for\ \ m \equiv 0 \pmod{p}; \\ p^3 - p, & for\ \ m \not\equiv 0 \pmod{p}. \end{cases}$

(ii) *If $Q(x)$ is not hyperbolic, then* $r_{p,Q}(m) = \begin{cases} p^3 - p(p-1), & for\ m \equiv 0 \pmod{p}; \\ p^3 + p, & for\ m \not\equiv 0 \pmod{p}. \end{cases}$

Proof. To prove (i), write $Q = Q_1 \oplus Q_2$ with $Q_1 \simeq Q_2 \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then

$$\begin{aligned} r_{p,Q}(0) &= r_{p,Q_1}(0) \cdot r_{p,Q_2}(0) + (r_{p,Q_1}(1))^2 \cdot (p-1) \\ &= (2p-1)^2 + (p-1)^3 \\ &= p^3 + p(p-1). \end{aligned}$$

By Lemma 6.5, $r_{p,Q}(m) = p^3 - p$ if $m \not\equiv 0 \pmod{p}$.

For (ii), by Lemma 6.4, we can write $Q = Q_1 \oplus Q_2$ with $Q_1 \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and Q_2 is not hyperbolic, and hence not isotropic , by Lemma 6.3. Thus,

$$\begin{aligned} r_{p,Q}(0) &= 1 \cdot r_{p,Q_1}(0) + (p^2-1) r_{p,Q_1}(1) \\ &= 1 \cdot (2p-1) + (p^2-1)(p-1) \\ &= p^3 - p(p-1). \end{aligned}$$

doi:10.6342/NTU201600288

By Lemma 6.5, $r_{p,Q}(m) = p^3 + p$ if $m \not\equiv 0 \pmod{p}$. □

Let χ denote the Dirichlet character such that $\chi(p) := \left(\frac{D_Q}{p}\right)$, for $p \nmid N_Q$ and let $\mathscr{L}(s,\chi)$ denote the Dirichlet L-function. Namely,

$$\mathscr{L}(s,\chi) := \prod_p (1-\chi(p))^{-s}, \quad s \in \mathbb{C},$$

where in the product p runs through all finite primes.

Corollary 6.7. *For $p \nmid 2N_Q$, we have*

$$r_{p,Q} = \begin{cases} p^3 + p(p-1)\chi(p), & if\ m \equiv 0 \pmod{p}; \\ p^3 - p\chi(p), & if\ m \not\equiv 0 \pmod{p}. \end{cases}$$

Proof. As in the above proof, write $Q = Q_1 \oplus Q_2$ so that Q is hyperbolic if and only if $Q_2 \simeq Q_1$. By Lemma 6.4, $Q_2 \simeq Q_1$ if and only if $d_{\mathbb{F}_p}(Q_2) = d_{|F_p}(Q_1)$, or equivalently, $d_{\mathbb{F}_p}(Q) = -1$. □

Definition 6.8. *Let p be a finite prime. We say that an integer m is p-stable with respect to an integral form $Q(x)$, if it is locally represented by $Q(x)$ at p and for each $k \gg 1$,*

$$r^{Good}_{p^k,Q}(mp^{2\nu}) + r^{Bad}_{p^k,Q}(mp^{2\nu})$$

is constant for all $\nu \geq 1$. Furthermore, we define Stable(m) *to be the set containing all primes at which m is stable.*

Lemma 6.9. *Let $Q(x)$ be a four dimensional integral form of level N and let m be an integer. Then m is p-stable for every $p \nmid 2N$.*

Proof. Since $p \nmid D_Q$, $r^{Bad}_{p^k,Q}(mp^{2\nu}) = 0$ for each $\nu \geq 1$. Because $r^{Good}_{p,Q}(mp^{\nu}) = r_{p,Q}(0)$, the lemma is a consequence of Corollary 6.7 and Lemma 4.8. □

We say that an integer m is supported on a set S of finite primes if $\mathrm{ord}_p(m) = 0$ whenever $p \notin S$. This means all prime factors of m lie in S.

doi:10.6342/NTU201600288

Lemma 6.10. *Let $Q(x)$ be a $2n$-dimensional integral form of level N and let m be an integer. Suppose $m = (m')^2 \cdot t$ and $p \in \mathrm{Stable}(t)$ with $\nu := \mathrm{ord}_p(m') \geq 1$. Then*

$$\frac{\beta(m)}{\beta(t)} \geq C_p(t),$$

where

$$C_p(t) := \min\{\frac{p^{n-2}}{p^{n-2}-1} \cdot \frac{\beta_p^{Good}(p^2t) + \beta_p^{Bad}(p^2t)}{\beta_p(t)}, 1\}.$$

Proof. For a $\mu \in \mathbb{Z}_p^*$, the form $Q(\mu x)$ is $\mathbb{Z}_p$-equivalent to $Q(x)$. Therefore, without loss of generality, we may assume $m' = p^\nu$. For simplicity, write $r_{p^k}^{Good\cup Bad}(m)$ for $r_{p^k,Q}^{Good}(m) + r_{p^k,Q}^{Bad}(m)$. By Lemma 4.10, we have the recursive formula

$$\begin{aligned} r_{p^k}(m) =& r_{p^k}^{Good\cup Bad}(m) + r_{p^k,Q}^{Zero}(m) \\ =& r_{p^k}^{Good\cup Bad}(m) + p^n \cdot r_{p^{k-2}}\Big(\frac{m}{p^2}\Big), \end{aligned}$$

and hence

$$r_{p^k}(m) = \sum_{i=0}^{\nu-1} p^{ni} r_{p^k}^{Good\cup Bad}\Big(\frac{m}{p^{2i}}\Big) + p^{n\nu} r_{p^{k-2\nu},Q}\Big(t\Big).$$

Put $K = \beta_p^{Good\cup Bad}(p^2t)$. Since $p \in \mathrm{Stable}(t)$, letting $k \to \infty$, we get

$$\beta_p(m) = K \cdot \frac{\Big(\frac{1}{p^{n-2}}\Big)^v - 1}{\frac{1}{p^{n-2}} - 1} + \frac{\beta_p(t)}{p^{(n-2)v}}.$$

Therefore, by setting

$$L := \frac{p^{n-2}}{p^{n-2}-1} \cdot \frac{K}{\beta_p(t)},$$

we obtain

$$\begin{aligned} \frac{\beta_p(m)}{\beta_p(t)} =& \frac{1}{p^{(n-2)\nu}} + \frac{K}{\beta_p(t)} \cdot \frac{\Big(\frac{1}{p^{n-2}}\Big)^\nu - 1}{\frac{1}{p^{n-2}} - 1} \\ =& \frac{1}{p^{(n-2)\nu}}\Big((1-L) + L \cdot p^{(n-2)\nu}\Big). \end{aligned}$$

Therefore, we have the desired

$$\frac{\beta_p(m)}{\beta_p(t)} = \begin{cases} \frac{1-L}{p^{(n-2)\nu}} + L \geq L, & \text{if } 1 \geq L; \\ \frac{(L-1)(p^{(n-2)\nu}-1)}{p^{(n-2)\nu}} + 1 \geq 1, & \text{if } L \geq 1. \end{cases}$$

□

doi:10.6342/NTU201600288

Lemma 6.11. *Let notation be as in* Lemma 6.9. *Suppose* $n = 2$ *and* $p \nmid 2N$. *If if* $p \nmid t$ *and* $\chi(p) = -1$, *then* $C_p(t) \geq \frac{p}{p+1}$; *otherwise* $C_p(t) = 1$.

Proof. By Lemma 5.4, we have $Q(x) \simeq x_1^2 + x_2^2 + x_3^2 + D_Q x_4^2$ over $\mathbb{Z}_p$. Consequently, $r_{p,Q}(a) = r_{p,Q}^{Good}(a)$ for every a. If $p \mid t$, then since $r_{p,Q}(p^2 t) = r_{p,Q}(t) = r_{p,Q}(0)$, by Lemma 4.8, we have

$$\frac{p^2}{p^2-1} \cdot \frac{\beta_p(p^2 t)}{\beta_p(t)} = \frac{p^2}{p^2-1} > 1.$$

Hence $C_p(t) = 1$. If $p \nmid t$, then $r_{p,Q}(p^2 t) = r_{P,Q}(0)$ and $r_{p,Q}(t) = r_{p,Q}(1)$. By Corollary 6.7 and Lemma 4.8, we have

$$\begin{aligned} \tfrac{p^2}{p^2-1} \cdot \tfrac{\beta_p(p^2 T')}{\beta_p(T')} &= \tfrac{p^2}{p^2-1} \cdot \tfrac{p^3+p(p-1)\chi(p)}{p^3-p\chi(p)} \\ &= \begin{cases} \tfrac{p^2}{p^2-1} \cdot \tfrac{p^3+p^2-p}{p^3-p} > 1, & \text{if } \chi(p) = 1; \\ \tfrac{p^2}{p^2-1} \cdot \tfrac{p^3-p^2+p}{p^3+p} > \tfrac{p}{p+1}, & \text{if } \chi(p) = -1. \end{cases} \end{aligned}$$

□

The following is the main theorem of this section. By Lemma 6.9, we can write $m = (m')^2 \cdot t$ such that m' supported on Stable(t) and $\mathrm{ord}_p(t) \leq 1$, for $p \nmid 2N$. There could be more than one choice of t', let T denote the set of all possible choices. Let $C_p(t)$ be as in Lemma 6.9 and denote

$$\delta_2 = \begin{cases} C_2(t), & \text{if } 2 \mid m'; \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 6.12. *Let* $Q(x)$ *be a four-dimensional basic escalator of level* N *and determinant* D *and let* m *be locally represented by* $Q(x)$. *Then we have the following estimation*

$$a_E(m) \geq C_E \cdot m \cdot \prod_{p \mid m, p \nmid 2N, \chi(p) = -1} \frac{p-1}{p+1},$$

where

$$C_E = \min_{t \in T} \left\{ \frac{2\omega_4 \cdot D^{1/2}}{\mathscr{L}(2,\chi)} \cdot \prod_{p \mid 2N} \frac{\beta_p(t)}{1 - \frac{\chi(p)}{p^2}} \cdot \prod_{\substack{p \mid N \\ p \in \mathrm{Stable}(t)}} C_p(t) \cdot \delta_2 \right\}.$$

doi:10.6342/NTU201600288

Proof. Obviously, for $p \nmid m'$, $\beta_p(m) = \beta_p(t')$. On the other hand, if $p \mid m'$, with $\mathrm{ord}_p(m') = \nu \geq 1$, then since $p \in \mathrm{Stable}(t')$, by Lemma 6.9, $\frac{\beta(m)}{\beta(t)} \geq C_p(t)$. Thus, by (6.2.1), (6.2.2) and (6.2.3),

$$a_E(m) \geq a_E(t) \cdot (m')^2 \cdot \prod_{p|m'} C_p(t). \tag{6.2.4}$$

Lemma 6.11 says

$$\prod_{p|m'} C_p(t) \geq \prod_{\substack{p\nmid 2Nt \\ \chi(p)=-1}} \frac{p}{p+1} \cdot \prod_{\substack{p|N \\ p\in \mathrm{Stable}(t)}} C_p(t) \cdot \delta_2. \tag{6.2.5}$$

To estimate $a_E(t)$, we first note that by Lemma 6.6,

$$\begin{aligned}
\prod_{p\nmid 2N} \beta_p(t) &= \prod_{p\nmid 2Nt} \beta_p(t) \cdot \prod_{p\nmid 2N, p|t} \beta_p(t) \\
&= \prod_{p\nmid 2Nt} \Big(1 - \frac{\chi(p)}{p^2}\Big) \cdot \prod_{p\nmid 2N, p|t} \frac{p^3 + p(p-1)\chi(p)}{p^3} \\
&\geq \prod_{p\nmid 2Nt} \Big(1 - \frac{\chi(p)}{p^2}\Big) \cdot \prod_{p\nmid 2N, p|t} \frac{(p+\chi(p))(p^2-\chi(p))}{p^3} \\
&= \prod_{p\nmid 2N} \Big(1 - \frac{\chi(p)}{p^2}\Big) \cdot \prod_{p\nmid 2N, p|t} \frac{(p+\chi(p))(p^2-\chi(p))}{p(p^2-\chi(p))} \\
&\geq \prod_{p\nmid 2N} \Big(1 - \frac{\chi(p)}{p^2}\Big) \cdot \prod_{\substack{p\nmid 2N, p|t, \\ \chi(p)=-1}} \Big(1 - \frac{1}{p}\Big) \\
&= \frac{1}{\mathscr{L}(2,\chi)} \cdot \prod_{p|2N} \frac{1}{1-\frac{\chi(p)}{p^2}} \cdot \prod_{\substack{p\nmid 2N, p|t, \\ \chi(p)=-1}} \Big(1 - \frac{1}{p}\Big).
\end{aligned}$$

Therefore,

$$\begin{aligned}
a_E(t) &= \beta_\infty(t) \cdot \prod_{p|2N} \beta_p(t) \cdot \prod_{p\nmid 2N} \beta_p(t) \\
&\geq \frac{\beta_\infty(t)}{\mathscr{L}(2,\chi)} \cdot \prod_{p|2N} \frac{\beta_p(t)}{1-\frac{\chi(p)}{p^2}} \cdot \prod_{\substack{p\nmid 2N, p|t, \\ \chi(p)=-1}} \Big(1 - \frac{1}{p}\Big).
\end{aligned}$$

Thus, by (6.2.3), (6.2.4) and (6.2.5)

$$a_E(m) \geq \Big(\frac{2\omega_4 \cdot D^{1/2}}{\mathscr{L}(2,\chi)} \cdot \prod_{p|2N} \frac{\beta_p(t)}{1-\frac{\chi(p)}{p^2}} \cdot \prod_{p|N, p\in stable(t)} C_p(t) \cdot \delta_2\Big) \cdot m \cdot \prod_{\substack{p|m, p\nmid 2N, \\ \chi(p)=-1}} \frac{p-1}{p+1}.$$

Then take minimum for $t \in T$ and complete the proof. □

doi:10.6342/NTU201600288

6.3 Fourier coefficients of the cusp form $f(z)$

In order to estimate the growth rate of the Fourier coefficients $a_f(m)$ of the cusp form $f(z)$, we apply general theory of Hecke eigenforms to write $f(z)$ as a linear combination of Hecke eigenforms

$$f(z) = \sum_{i=1}^{r} \gamma_i g_i(z),$$

where $\gamma_i \in \mathbb{C}$. Suppose we write $g_i(z) = \sum_{m\geq 0} b_i(m) e^{2\pi i m z}$, then $a_f(m) = \sum_{i=1}^{r} \gamma_i b_i(m)$. By the Deligne's bound [7] on Hecke eigenforms, we obtain the estimation

$$|b_i(m)| \leq \tau(m)\sqrt{m},$$

where $\tau(m)$ is the number of positive divisors of m; hence,

$$|a_f(m)| \leq C_f \tau(m)\sqrt{m}, \tag{6.3.1}$$

where $C_f = \sum_{i=1}^{r} |\gamma_i|$.

6.4 The criterion of representability

Let $Q(x)$ be a basic escalator. Combining the bounds of the Fourier coefficients of $E(z)$ and $f(z)$, we know that any number m locally represented by $Q(x)$ and satisfying

$$\frac{\sqrt{m}}{\tau(m)} \prod_{\substack{p\nmid N, p\mid m,\\ \chi(p)=-1}} \frac{p-1}{p+1} > \frac{C_f}{C_E} \tag{6.4.1}$$

is represented by Q.

Definition 6.13. *For a given basic escalator $Q(x)$, an positive integer m is called an eligible integer of the form if m is locally represented by $Q(x)$ but fails to satisfy the inequity* 6.4.1. *Furthermore, define*

$$B(m) = \frac{\sqrt{m}}{\tau(m)} \prod_{\substack{p\nmid N, p\mid m,\\ \chi(p)=-1}} \frac{p-1}{p+1}.$$

doi:10.6342/NTU201600288

In order to determine the set of integers represented by a basic quaternary escalator $Q(x)$, it is necessary to handle the eligible integers. Thus, we require more information about the function $B(m)$.

Lemma 6.14. *$B(m)$ is a multiplicative function, and $B(p) > 1$ for each prime $p > 7$. Moreover, for any positive m and prime p,*

$$B(mp^{\nu}) > B(m) \text{ if } \begin{cases} \nu \geq 1, & \text{for } p \geq 11; \\ \nu \geq 2, & \text{for } p = 5, 7; \\ \nu \geq 5, & \text{for } p = 3; \\ \nu \geq 11, & \text{for } p = 2. \end{cases} \tag{6.4.2}$$

Proof. First, $B(m)$ is obviously multiplicative and by direct computation, the inequality $B(p) > 1$ is obtained for $p > 7$. We need to check the inequality 6.4.2. Suppose $m = m_1 p^{\nu_1}$ with $p \nmid m_1$, then

$$\begin{aligned} B(mp^{\nu}) =& \frac{p^{\frac{\nu}{2}}\sqrt{m_1 p^{\nu_1}}}{(1+\nu+\nu_1)\tau(m_1)} \prod_{\substack{q \mid m_1 p, q \nmid N_Q, \\ \chi(q)=-1}} \frac{q-1}{q+1} \\ \geq& \Big(\frac{1+\nu_1}{1+\nu+\nu_1}\Big)\Big(\frac{p^{\frac{\nu}{2}}(p-1)}{p+1}\Big)\frac{\sqrt{m_1 p^{\nu_1}}}{(1+\nu_1)\tau(m_1)} \prod_{\substack{q \nmid N_Q, q \mid m_1, \\ \chi(q)=-1}} \frac{q-1}{q+1} \\ \geq& \frac{1+\nu_1}{1+\nu+\nu_1} \cdot \frac{p^{\frac{\nu}{2}}(p-1)}{p+1} B(m) \\ \geq& \frac{p^{\frac{\nu}{2}}}{1+\nu} \cdot \frac{p-1}{p+1} B(m). \end{aligned}$$

Therefore, the proof is completed by solving the inequality

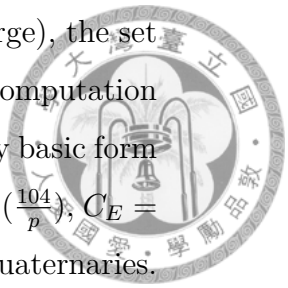
$$\frac{p^{\frac{\nu}{2}}}{1+\nu} \cdot \frac{p-1}{p+1} > 1.$$

□

Corollary 6.15. *For a basic escalator $Q(x)$, the set of all eligible integers of $Q(x)$ is finite.*

Proof. Since $B(m)$ is a multiplicative function and $B(p) \leq \frac{C_f}{C_E}$ holds only for finitely many p, the assertion follows from Lemma 6.14 and its proof. □

doi:10.6342/NTU201600288



Since the number of eligible integers is finite (although maybe very large), the set of positive integers represented by the form $Q(x)$ could be determined by computation [6, §4.3]. In the Bhargave and Hanke's paper [6], they present a quaternary basic form $Q(\tilde{x}) = x^2+2y^2+4z^2+31w^2+yz-yw+3zw$. The level $N_Q = 3774$, $\chi(p) = (\frac{104}{p})$, $C_E = \frac{36}{125}$, and $C_f \approx 2331.99$, giving the largest bound $\frac{C_f}{C_E} < 8100.65$ of 6560 quaternaries. In this case, there are 28 billion square-free eligible integers.

7 Proofs of the main theorems

7.1 Summary

By checking with machine using the above arithmetic and analytic methods, we classify all basic four-dimensional escalator lattices L into three types:

Type I: L is universal.

Type II : L is not universal but miss at most three positive integers, every missed number is a critical integer.

Type III : Otherwise.

We find that among all basic four-dimensional escalator lattices, there are 6402 lattices of Type I, 153 one of type II, and 5 ones of Type III.

7.2 The 10-14 switch

The lattice escalators of Type III all have truants 14 and are given by

$$\begin{pmatrix} 1 & 0 & -1/2 & -3 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 1 \\ -3 & 0 & 1 & 10 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1/2 & -2 \\ 0 & 2 & 1 & -2 \\ -1/2 & 1 & 5 & 3 \\ -2 & -2 & 3 & 10 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1/2 & -2 \\ 0 & 2 & 1 & -2 \\ -1/2 & 1 & 5 & 1 \\ -2 & -2 & 1 & 10 \end{pmatrix},$$

doi:10.6342/NTU201600288

$$\begin{pmatrix} 1 & 0 & -1/2 & -1 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 3 \\ -1 & 0 & 3 & 10 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & -1/2 & -1 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 2 \\ -1 & 0 & 2 & 10 \end{pmatrix}.$$

These five lattices are escalated from the three-dimensional escalator L_3 given by $\begin{pmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1 \\ 1/2 & 1 & 5 \end{pmatrix}$, whose truant is 10.

Now instead of escalating L_3 by adding a new vector of square norm 10, we add a vector of square norm 14 to it. There are 330 lattices obtained in this way, they are all 4-dimensional. Call them *the auxiliary quaternaries*.

Lemma 7.1. *The escalator of a basic lattice L of* Type III *contains an auxiliary quaternary.*

Proof. Let $M = L + \mathbb{Z}e$, with $\|e\|^2 = 14$. Then $L' = L_3 + \mathbb{Z}e$ is an auxiliary quaternary contained in M. □

One finds that 226 of these 330 auxiliary quaternaries recurred in the 6555 basic escalator lattices of Type I and II. By machine computation, we can classify the remaining 104 forms L into three types:

Type I: L is universal.

Type II: L not universal but miss at most three positive integers, every missed number is a critical integer.

Type IV : L represents all integers except for those of forms $10n^2$ and $13n^2$.

7.3 The proof of Theorem 1

So far, all basic quaternary escalators and auxiliary quaternaries are classified.

Definition 7.2. *Let C_{290} denote the collection of all integers missed by at least one of all basic quaternary escalators and auxiliary quaternaries.*

doi:10.6342/NTU201600288

The result of computation tells the following:

Lemma 7.3. *C_{290} is exactly the set of all critical integers listed in* Theorem 1.

Lemma 7.4. *The zero lattice can be escalated at most 7 times.*

Proof. If a basic 4-dimensional escalator is of Type II, then it becomes universal after at most three escalating. If it is of Type III, then any of its escalator L' contains an auxiliary quaternary. If this auxiliary quaternary, which misses 10, is of Type II, then L', which represents 10, misses at most two integers, and hence becomes universal after at most two escalations. If this auxiliary quaternary, which represents 10, is of Type II, then L' is exactly this auxiliary, and hence becomes universal at most 3 escalations. If the auxiliary quaternary is of Type IV, then it is universal. □

Proof of Theorem 1. First, let Q be a positive-definite integral quadratic form, then there exists a maximal sequence of escalator lattices

$$\{0\} \subset L_1 \subset L_2 \subset \ldots \subset L_k$$

within $L(Q)$ (k $\leq$ 7). If $L(Q)$ is universal, then L_k is also universal. Conversely, suppose $L(Q)$ is not universal, then truant(L)=truant(L_k); otherwise, if truant(L) $\geq$ truant(L_k), then one can obtain a escalator L_{k+1} within $L(Q)$ properly containing L_k. □

7.4 The proof of Theorem 2

Now we complete the prove of Theorem 2.

The proof of Theorem 2. First, we know that all critical integers except 203 and 290 arise as the truants of 1, 2, 3, 4 dimensional escalator lattices. For 203 and 290, we consider the special escalator lattice

$$L_{145} := \begin{pmatrix} 1 & 0 & -1/2 \\ 0 & 2 & -1/2 \\ -1/2 & -1/2 & 4 \end{pmatrix} \oplus [29].$$

doi:10.6342/NTU201600288

L_{145} has 145 as its truant, and its escalation

$$\begin{pmatrix} 1 & 0 & -1/2 \\ 0 & 2 & -1/2 \\ -1/2 & -1/2 & 4 \end{pmatrix} \oplus [29] \oplus [145]$$

has the truant 290. Remarkably, L_{145} is the only basic four-dimensional escalator lattice dose not represent 203. We set a lattice $L_{203} := L_{145} \oplus [58]$. Since the only square multiples of 58 less than 203 are 0 and 58 itself, L_{203} represents

$$\{0, 1, \ldots, 144\} \bigcup \{0 + 58, 1 + 58, \ldots, 144 + 58\},$$

but dose not represent 203. This is, 203 is the truant of L_{203}. Since L_{203} represents 145, we may pick a vector v of norm 145 in the lattice L_{203}, and set L'_{203} as the lattice generated by L_{145} and the vector v. Because L_{145} cannot represent 145, v is form of $(*, *, *, *, 1)$, which implies $L_{203} = L'_{203}$.

So far, we have proven that each critical integer is the truant of some escalator lattice. For any critical integer m, let L be an escalator lattice whose truant is m, and define $L_m = L \oplus [m+1]^{\oplus 4} \oplus [mx+1]$. We claim that L_m represents all nonzero integers except for m.

By Lagrange's four theorem, $[m+1]^{\oplus 4}$ represents all integers of the form $(m+1)n$. Every integer a can be expressed as $a = (m+1)q + r$, where $0 \leq r \leq m$. Therefore, L_m represent all nonzero integers except for m, since L represents all integers in the interval $[0, m-1]$ while $[2m+1]$ represents $2m+1$. Thus, the proof is complete.

□

8 References

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

[2] G.L.Watson, *Integral quadratic forms*, Cambridge University Press, 1960.

[3] Jonathan Hanke, *local densities and explicit bounds for representatability by a quadratic form*, Duke Math. J.124(2004), no 2, 351-388.

doi:10.6342/NTU201600288

[4] Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics 7. Springer-Verlag, New York, 1973.

[5] Larry J.Gerstein, *Basic quadratic forms*, American Mathematical Society, 2008.

[6] Manjul Bhargava and Jonathan Hanke, *Universal quadratic forms and 290 theorem*, Invent. Math.,2005.

[7] P. Delign, *La conjecture de Weil, I, Inst.* Hautes Etudes Sci. Publ. Math. **43**(1974), 273-307. MR 0340258.

[8] C. L. Siegel, *¨Uber die Analytische Theorie der quadratischen Formen*. Ann. of Math. *36* (1935), 527–606; Gestammelte Abhandlungen, band I, 1966, pp. 326–405.

[9] [Ram16] S. Ramanujan, *On the expression of a number in the form ax2 + by2 + cz2 + du2*. Proc. Camb. Phil. Soc. 19 (1916), 11?21.

[10] Z. I. Borevich and T.R. Shafarevich, *Number Thory*, Academic Press, 1966.

doi:10.6342/NTU201600288