J. Korean Math. Soc. **39** (2002), No. 4, pp. 525–542

A LOCAL-GLOBAL PRINCIPLE FOR REPRESENTATIONS OF BINARY FORMS BY CERTAIN QUINARY FORMS

Myung-Hwan Kim and Byeong-Kweon Oh

Abstract. In this article, we prove a certain local-global principle for representation of binary forms by an infinite family of quinary positive integral quadratic forms.

1. Introduction

One of the most fundamental questions in representation theory of integral quadratic forms is about the local-global principle, which is as follows:

Let M and N be positive integral quadratic forms of rank m and n, respectively, such that M represents N locally at every prime spot. Under what condition does M represent N globally?

Concerning this question, we let $\mathfrak{R}_m(n)$ be the set of all positive integral quadratic forms M of rank m satisfying the following property:

($\mathfrak{R}$) *M represents all positive integral quadratic forms N of rank n provided that $N \to M$ over $\mathbb{Z}_p$ at all p and* $\min(N) > C(M)$ *for some positive constant $C(M)$ depending only on M and n.*

We define $R(n)$ to be the minimum rank m for which $\mathfrak{R}_m(n)$ equals the set of all positive integral quadratic forms of rank m. In 1929 Tartakowsky [22] proved

$$R(1) = 5$$

Received August 14, 2001.
2000 Mathematics Subject Classification: 11E12, 11H06.
Key words and phrases: local-global principle, representation of quadratic forms.
This work was partially supported by KOSEF (99-0701-01-5-2).

and in 1978, J. S. Hsia, Y. Kitaoka and M. Kneser [5] made a breakthrough by proving that

$$R(n) \leq 2n+3.$$

On the other hand, Y. Kitaoka [9] gave examples of positive integral quadratic forms of rank $n+3$ that are not contained in $\mathfrak{R}_{n+3}(n)$. Therefore, we have

$$n+4 \leq R(n) \leq 2n+3.$$

Recently, M. Jöchner [8] proved

$$R(2) = 6.$$

See [8] for other interesting results in this direction.

As appeared in Kitaoka's examples, the primitiveness condition on local representations seems to play an important role in studying the local-global principle for representations of integral quadratic forms. Regarding this, we define $\mathfrak{R}_m^*(n)$ to be the set of all positive integral quadratic forms M of rank m satisfying the following property:

($\mathfrak{R}^*$) *M represents all positive integral quadratic forms N of rank n provided that $N \to M$ primitively over $\mathbb{Z}_p$ at all p and* $\min(N) > C^*(M)$ *for some positive constant $C^*(M)$ depending only on M and n.*

We define $R^*(n)$ to be the minimum rank m for which $\mathfrak{R}_m^*(n)$ equals the set of all positive integral quadratic forms of rank m. It is clear that

$$\mathfrak{R}_m(n) \subseteq \mathfrak{R}_m^*(n) \quad \text{and} \quad R^*(n) \leq R(n).$$

In [10, 11], Kitaoka proved that

$$\mathfrak{R}_{2n+2}^*(n) = \mathfrak{R}_{2n+2}(n) \text{ for } n \geq 2$$

and

$$\mathfrak{R}_{2n+1}^*(n) = \mathfrak{R}_{2n+1}(n) \text{ for } n \geq 3.$$

It is well known that

$$R^*(1) = 4$$

(see [1] and [4]) and from the recent result of [8] follows that

$$5 \leq R^*(2) \leq 6.$$

In this paper, we find an infinite family of quinary positive integral quadratic forms that is contained in $\mathfrak{R}_5^*(2)$. More precisely, we prove that every quinary positive even (or odd) integral quadratic form with even (or odd, respectively) squarefree discriminant that contains a quaternary sublattice of class number 1 as an orthogonal direct summand is contained in $\mathfrak{R}_5^*(2)$. Furthermore, an explicit estimation of the constant $C^*(M)$ is provided. See [3] and [23] for their estimation of $C(M)$ when $n = 1$, and [2, 12 – 18] for recent results of authors on representations of integral quadratic forms related to the local-global principle.

We shall adopt lattice theoretic language. A $\mathbb{Z}$*-lattice* L is a finitely generated free $\mathbb{Z}$-module in $\mathbb{R}^n$ equipped with a non-degenerate symmetric bilinear form B such that $B(L, L) \subseteq \mathbb{Z}$. The corresponding quadratic map is denoted by Q.

For a $\mathbb{Z}$-lattice L with basis vectors $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$, i.e., $L = \mathbb{Z}\mathbf{e}_1 + \mathbb{Z}\mathbf{e}_2 + \cdots + \mathbb{Z}\mathbf{e}_n$, we often write

$$L = (B(\mathbf{e}_i, \mathbf{e}_j)).$$

For sublattices L_1, L_2 of L, $L = L_1 \perp L_2$ means $L = L_1 \oplus L_2$ and $B(\mathbf{v}_1, \mathbf{v}_2) = 0$ for all $\mathbf{v}_1 \in L_1, \mathbf{v}_2 \in L_2$. We call L *diagonal* if it admits an orthogonal basis and in this case, we simply write

$$L = \langle Q(\mathbf{e}_1), Q(\mathbf{e}_2), \cdots, Q(\mathbf{e}_n)\rangle,$$

where $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ is an orthogonal basis of L. We call L *non-diagonal* otherwise. L is called *positive definite* or simply *positive* if $Q(\mathbf{e}) > 0$ for any $\mathbf{e} \in L, \mathbf{e} \neq \mathbf{0}$. As usual,

$$dL = \det(B(\mathbf{e}_i, \mathbf{e}_j))$$

is called the *discriminant* of L. A $\mathbb{Z}$-lattice (or $\mathbb{Z}_2$-lattice) L is called *even* when $Q(L) \subseteq 2\mathbb{Z}$ (or $\subseteq 2\mathbb{Z}_2$, respectively) and odd otherwise. Note that every even lattice with odd rank has even discriminant.

We define $RL := R \otimes_{\mathbb{Z}} L$ for any commutative ring R containing $\mathbb{Z}$. For a $\mathbb{Z}$-lattice L and a prime p, we define

$$L_p := \mathbb{Z}_p L$$

and call it the localization of L at p. If $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$ is an orthogonal basis of the quadratic space $V = \mathbb{Q}L$ or $\mathbb{Q}_p L$, we write in short

$$V = (Q(\mathbf{e}_1), Q(\mathbf{e}_2), \cdots, Q(\mathbf{e}_n)).$$

Let ℓ and L be $\mathbb{Z}$-lattices (or $\mathbb{Z}_p$-lattices). We say L *represents* ℓ and write

$$\ell \to L$$

if there is an injective $\mathbb{Z}$-linear (or $\mathbb{Z}_p$-linear, respectively) map σ from ℓ into L that preserves the bilinear forms. Such a map is called a *representation.* A representation $\sigma : \ell \to L$ is called a *primitive* representation if $\sigma(\ell)$ is a direct summand of L. We say that L *primitively* represents ℓ and write

$$\ell \to^* L$$

if there exists a primitive representation from ℓ to L.

We define

$$[a, b, c] := \begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

for convenience. For unexplained terminology, notation, and basic facts about global or local lattices, we refer the readers to O'Meara [19].

2. Primitive representations over $\mathbb{Z}_p$

Let L be a $\mathbb{Z}$-lattice and $\mathfrak{a}_{(p)} \subsetneqq \mathbb{Z}_p$ be an ideal. By abuse of terminology, we say that L is $\mathfrak{a}_{(p)}$-maximal if L_p is an $\mathfrak{a}_{(p)}$-maximal $\mathbb{Z}_p$-lattice. Note that for an ideal $\mathfrak{a} \subsetneqq \mathbb{Z}$, L is $\mathfrak{a}$-maximal if and only if L is $\mathfrak{a}_p$-maximal for all prime p (see [19]).

Let ℓ be a binary $\mathbb{Z}_2$-maximal $\mathbb{Z}$-lattice. Then ℓ_2 is isometric to one of the following 16 binary $\mathbb{Z}_2$-lattices:

$$\langle 1, \alpha \rangle, \quad \langle 3, \beta \rangle, \quad \langle \alpha, 2 \rangle, \quad \langle \beta, 2\gamma \rangle, \quad [2, 1, 2], \quad [0, 1, 0],$$

where $\alpha = 1, 3, 5, 7$, $\beta = 3, 7$, and $\gamma = 5, 7$. The next two lemmas are useful in the proof of our main theorem in Section 3.

LEMMA 2.1. *For an odd prime* p, *let* $L_{(p)} = L'_{(p)} \perp \langle p\eta \rangle$ *be a quinary* $\mathbb{Z}_p$*-lattice with* $dL_{(p)} \in p\mathbb{Z}_p^*$ *and let* $\ell_{(p)} = \langle \delta_1 p^{u_1}, \delta_2 p^{u_2} \rangle$ *be a (binary)* $\mathbb{Z}_p$*-lattice with* $\delta_i \in \mathbb{Z}_p^*$, $u_1 \leq u_2$. *Then* $\ell_{(p)}$ *cannot be primitively represented by* $L_{(p)}$ *if and only if* $L'_{(p)}$ *has a nonsquare discriminant,* u_1 *is an odd integer less than* u_2, *and* $\delta_1 \eta \notin \mathbb{Z}_p^{*2}$.

Proof. The necessity is straightforward. For the sufficiency, suppose that $\ell_{(p)}$ is primitively represented by $L_{(p)}$. Since $\langle \delta_2 p^{u_2} \rangle$ is primitively represented by $L_{(p)}$, it is also primitively represented by the orthogonal complement $K_{(p)}$ of $\langle \delta_1 p^{u_1} \rangle$ in $L_{(p)}$. From Hasse symbol computation it follows that $\mathbb{Q}_p K_{(p)}$ is anisotropic and that the p-order of the scale of each modular component of the Jordan decomposition of $K_{(p)}$ is less than u_2, which is impossible. □

Let $K_{(2)}$ be a quinary (odd) unimodular $\mathbb{Z}_2$-lattice or even $\mathbb{Z}_2$-lattice whose Jordan decomposition has even unimodular component of rank 4 and $2\mathbb{Z}_2$-modular component of rank 1. When $K_{(2)}$ is even, one can easily check that $K_{(2)}$ primitively represents all binary $\mathbb{Z}_2$-lattices. For the odd case, we have the following:

LEMMA 2.2. *Let $K_{(2)}$ be a quinary unimodular $\mathbb{Z}_2$-lattice. Then $K_{(2)}$ primitively represents all binary $\mathbb{Z}_2$-lattices unless*

$$K_{(2)} \simeq \langle 1, 1, 1, 1, dK_{(2)} \rangle.$$

In the exceptional case, $K_{(2)}$ primitively represents all binary $\mathbb{Z}_2$-lattices but

$$[4\alpha, 2\beta, 4\gamma] \quad \text{and} \quad \langle dK_{(2)} \rangle \perp \langle 8\delta \rangle,$$

where α, β, γ, $\delta \in \mathbb{Z}_2$.

Proof. This is a direct consequence of Hensel's Lemma. See also [6, 7]. □

3. Quaternary sublattices of class number 1

In this section, we assume that every $\mathbb{Z}$-lattice is positive unless stated otherwise.

For a binary $\mathbb{Z}$-lattice ℓ, if $\ell = [a, b, c]$, $0 \le 2b \le a \le c$, for some basis $\{\mathbf{e}_1, \mathbf{e}_2\}$, which always exists, we say that $[a, b, c]$ is *Minkowski reduced* and that $\{\mathbf{e}_1, \mathbf{e}_2\}$ is a *Minkowski reduced basis.*

For an odd prime p, we denote a nonsquare unit in $\mathbb{Z}_p$ by Δ_p. For two elements $\alpha, \beta \in \mathbb{Z}_p$, we write $\alpha \sim \beta$ if $\alpha\beta^{-1} \in \mathbb{Z}_p^{*2}$.

Let L be a quaternary $\mathbb{Z}$-lattice with class number 1. We partition all odd primes into the following three sets:

$$\begin{aligned} W &= \{\, p \mid L_p \text{ is not unimodular} \,\}, \\ U &= \{\, p \mid L_p \text{ is unimodular with } d(L_p) = 1 \,\}, \\ V &= \{\, p \mid L_p \text{ is unimodular with } d(L_p) = \Delta_p \,\}. \end{aligned}$$

For a positive integer k, we define

$$L(\delta k) := L \perp \langle \delta k \rangle,$$

where $\delta = 1$ if L is odd, and $\delta = 2$ if L is even. Let V_0 be the set of all odd prime divisors of k. We define $V_1 := V \cap V_0$ and $V_2 := V \setminus V_1$.

Lemma 3.1. *Let $p > 3$ be a prime and $a, b, c \in \mathbb{F}_p$. If $b^2 - ac \not\equiv 0 \pmod p$, then the set $\{\, ax^2 + 2bx + c \mid x \in \mathbb{F}_p \,\}$ contains both a nonzero square and a nonsquare.*

Proof. See [21]. □

Theorem 3.2. *Assume that $d := dL(2k)$ is a squarefree integer. Let ℓ be a binary $\mathbb{Z}$-lattice such that*

$$\ell_p \to^* L(2k)_p$$

at all p. Then for any $\epsilon > 0$, there exists a constant $C > 0$ depending only on ϵ such that

$$\text{if } \min(\ell) > C \cdot d^{5+\epsilon}, \text{ then } \ell \to L(2k).$$

Proof. Let $\ell = [a, b, c]$ be Minkowski reduced. We define

$$\ell_s(t) := [a - 2kt^2, sa + b, s^2 a + 2sb + c] = \begin{pmatrix} a - 2kt^2 & sa + b \\ sa + b & s^2 a + 2sb + c \end{pmatrix},$$

where s, t are integers. We assume for the time being that a is large enough so that $\ell_s(t)$ is positive, and determine how large a should be at the end of the proof. Since the class number of L is 1, if $\ell_s(t)_p \to L_p$ for all p (including ∞), then $\ell_s(t) \to L$ and hence $\ell \cong \ell_s(0) \to L(2k)$. We will find such s and t in the following.

Note that for an odd prime p,

$$\mathbb{Q}_p(\ell_s(t)) \to \mathbb{Q}_p L \text{ if and only if } \ell_s(t)_p \to L_p$$

(see [Theorem 2, 20]).

(a) $p \in U$: In this case, $\ell_s(t)_p \to L_p$ for any integers s and t.

(b) $p \in W \cup V_1 \cup \{2\}$: By the Chinese Remainder Theorem, it suffices to find integers s and t at each $p \in W \cup V_1 \cup \{2\}$ such that $\ell_s(t)_p \to L_p$.

b-1) $p \in W$: Let

$$L_p = \langle 1, 1, \delta, p\eta \rangle \quad \text{and} \quad \ell_p = [\alpha p^u, \beta p^v, \gamma p^w],$$

where $\alpha, \beta, \gamma, \delta, \eta \in \mathbb{Z}_p^*$ and u, v, w are nonnegative integers. Note that if $ord_p(d\ell_p)$ is even or $d(\mathbb{Q}_p\ell) = -\delta\eta p\Delta_p$, then $\ell_p \to L_p$.

If $d\ell \not\equiv 0 \pmod p$, then any s,t satisfying $t \equiv 0 \pmod p$ can be taken so that $\ell_s(t)_p$ is unimodular, which implies $\ell_s(t)_p \to L_p$. Let $d\ell \equiv 0 \pmod p$. Then take s,t satisfying $s \equiv 0 \pmod p), t \not\equiv 0 \pmod p$ if $u = v = w = 0, d\ell \equiv 0 \pmod p$; take s,t satisfying $st \not\equiv 0 \pmod p$ if $u = 0, v, w \neq 0$; and take s,t satisfying $st \not\equiv 0 \pmod p$ if $u, v \neq 0, w = 0$, so that $\ell_s(t)_p$ is unimodular, which again implies $\ell_s(t)_p \to L_p$.

It only remains to treat the case when $u, v, w \neq 0$. If $2k \sim \delta$, then $\ell_s(t)_p \to L_p$ by taking any s and t satisfying $t \not\equiv 0 \pmod p$. So, we may assume that $2k \sim \delta\Delta_p$.

Let $u < v, w$. In this case, we take s,t satisfying $s, t \not\equiv 0 \pmod p$. If u is even, then $\ell_s(t)_p \to L_p$ follows immediately. Let u be odd. Since

$$\ell_p \simeq \langle \alpha p^u, \alpha(p^w\alpha\gamma - p^{2v-u}\beta^2) \rangle,$$

we have $\alpha \sim \eta$ by Lemma 2.1, and hence

$$d(\ell_s(t)_p) \sim -2kp^u\alpha \sim -p^u\eta\delta\Delta_p.$$

This implies $\ell_s(t)_p \to L_p$.

Let $u = v < w$. Then

$$d(\ell_s(t)_p) = p^u(p^w\alpha\gamma - p^u\beta^2 - 2kt^2(s^2\alpha + 2s\beta + p^{w-u}\gamma)).$$

If $p \neq 3$, then take s,t satisfying

$$-2kt^2(s^2\alpha + 2s\beta + p^{w-u}\gamma) \sim -\eta\delta\Delta_p,$$

which is possible by Lemma 3.1. Then $\ell_s(t)_p \to L_p$ follows immediately. Let $p = 3$. If u is even, then take s, t satisfying $t \not\equiv 0 \pmod 3$ and $s^2\alpha + 2s\beta \not\equiv 0 \pmod 3$ so that $\ell_s(t)_3 \to L_3$. Let u be odd. If $w, u, w-u$ are all bigger than 1, take s, t satisfying $t \not\equiv 0 \pmod 3$, $ord_3(s) = 1$. Then $ord_3(d(\ell_s(t)_3))$ is even, from which follows $\ell_s(t)_3 \to L_3$. The remaining possibilities can be handled in a similar manner and are omitted.

Let $u = w < v$. The proof of this case is almost identical to the above except when $p = 3$ and u is odd. We may assume that $\alpha\gamma \equiv 2 \pmod 3$ because the set $\{ s^2 + 1 \mid s \in \mathbb{F}_3 \}$ contains both a nonzero square and a nonsquare in $\mathbb{F}_3$. Let t be any integer which is not divisible by 3. It is tedious but not difficult to find an integer $s \pmod 9$ for which $ord_3(d(\ell_s(t)_3))$ is even. This implies $\ell_s(t)_3 \to L_3$.

Let $u = v = w$. Then

$$d(\ell_s(t)_p) = p^u(p^u(\alpha\gamma - \beta^2) - 2kt^2(s^2\alpha + 2s\beta + \gamma))$$

and the proof of this case is also very similar to the above except when $p = 3$, u is odd and $\alpha\gamma - \beta^2 \equiv 0 \pmod 3$. Note that $\alpha \sim \eta$. If we take s, t satisfying $t \not\equiv 0 \pmod 3$, $2s\beta + \gamma \equiv 0 \pmod 3$, then $\ell_s(t)_3 \cong \langle -2k, 3^u\alpha \rangle \to L_3$.

Let $v < u, w$. We take s, t satisfying $s \sim 2\beta\eta$, $t \not\equiv 0 \pmod p$. Then

$$\begin{aligned} d(\ell_s(t)_p) &= p^v(p^{u+w-v} - p^v\beta^2 - 2kt^2(s^2p^{u-v} + 2s\beta + p^{w-v}\gamma)) \\ &\sim -k\beta s p^v \sim -\delta\Delta_p\eta p^v. \end{aligned}$$

The rest is trivial.

Let $v = w < u$. We take s, t satisfying $-2kt^2(2s\beta + \gamma) \in \mathbb{Z}_p^*$. Then

$$d(\ell_s(t)_p) \sim -2kt^2(2s\beta + \gamma)p^v$$

and the rest is trivial.

Finally, let $w < u, v$. The proof of this case is exactly same as that of the case when $u < v, w$ and is omitted.

b-2) $p \in V_1$: Let

$$L_p = \langle 1, 1, 1, \Delta_p \rangle \text{ and } \ell_p = [\alpha p^u, \beta p^v, \gamma p^w],$$

where $\alpha, \beta, \gamma \in \mathbb{Z}_p^*$ and u, v, w are nonnegative integers. Let $\tau = 2k/p$. Note that if $ord_p(d\ell_p)$ is odd or $d(\mathbb{Q}_p\ell) = -1$, then $\ell_p \to L_p$. We only provide proofs for the cases when $1 \le u = w < v$ and $1 \le u = w = v$

because all other cases can be proved in a very similar manner as in b-1).

Let $1 \le u = w < v$. We may assume that u is odd because

$$d(\ell_s(t)_p) = p^{u+1}\big(p^{u-1}\alpha\gamma - p^{2v-u-1}\beta^2 - \tau t^2(s^2\alpha + 2sp^{v-u}\beta + \gamma)\big).$$

If $u \neq 1$, then we may further assume that $p = 3$ by Lemma 3.1. If $\alpha\gamma \equiv 1 \pmod 3$, then one can easily find s, t for which $d(\ell_s(t)_3) = -3^{u+1}$ and hence $\ell_s(t)_3 \to L_3$. Let $\alpha\gamma \equiv -1 \pmod 3$. Then we can take s, t satisfying

$$ord_3(s^2\alpha + 2s3^{v-u}\beta + \gamma) = 1 \quad \text{and} \quad t \not\equiv 0 \pmod 3,$$

from which $\ell_s(t)_p \to L_p$ follows immediately. Let $u = 1$. If $\alpha\gamma \equiv -1 \pmod p$, take any s and t satisfying $t \equiv 0 \pmod p$. Then $d(\ell_s(t)_p) = -p^2$ and hence $\ell_s(t)_p \to L_p$. Assume that $t \not\equiv 0 \pmod p$. If $\alpha\gamma - \tau\gamma t^2 \equiv -1 \pmod p$, then s satisfying $s \equiv 0 \pmod p$ will do. So assume that

$$\alpha\gamma \not\equiv -1 \quad \text{and} \quad \alpha\gamma - \tau\gamma t^2 \not\equiv -1 \pmod p.$$

If $\alpha - \tau t^2 \equiv 0 \pmod p$, then $d(\ell_s(t)_p) = -p^{u+1}$ for all s satisfying $s \not\equiv 0 \pmod p$ and hence $\ell_s(t)_p \to L_p$. Let $\alpha - \tau t^2 \not\equiv 0 \pmod p$. Then $p \neq 3$ and hence Lemma 3.1 can be applied to find s such that $d(\ell_s(t)_p) = -p^2$. From this follows $\ell_s(t)_p \to L_p$.

Let $1 \le u = v = w$. The proof is almost identical to the above except when $u = 1$ and $\alpha\gamma - \beta^2 \not\equiv 0 \pmod p$. In the exceptional case, we have

$$\begin{aligned} d(\ell_s(t)_p) &= p^2(\alpha\gamma - \beta^2 - \tau t^2(\alpha s^2 + 2s\beta + \gamma)) \\ &= p^2((\alpha\gamma - \beta^2)(1 - \alpha^{-1}\tau t^2) - \tau t^2(\alpha s + \beta)^2\alpha^{-1}) \\ &= p^2(-\alpha\tau t^2 s^2 - 2\tau\beta t^2 s + (\alpha - \tau t^2)\gamma - \beta^2). \end{aligned}$$

We take t satisfying $t \not\equiv 0 \pmod p$. If $\alpha - \tau t^2 \equiv 0 \pmod p$, then take s satisfying $\alpha s + \beta \not\equiv 0 \pmod p$ so that $d(\ell_s(t)_p) \sim -p^2\alpha^{-1}\tau \sim -p^2$. Let $\alpha - \tau t^2 \not\equiv 0 \pmod p$. If $p \neq 3$, then because

$$(\tau\beta t^2)^2 - (-\alpha\tau t^2)((\alpha - \tau t^2)\gamma - \beta^2) = \tau t^2(\alpha\gamma - \beta^2)(\alpha - \tau t^2) \not\equiv 0 \pmod p$$

we can apply Lemma 3.1 to conclude that $d(\ell_s(t)_p) \sim -p^2$. We may conclude the same even if $p = 3$ from case by case consideration. In either case it follows that $\ell_s(t)_p \to L_p$.

b-3) $p=2$: Since L_2 is even unimodular $\mathbb{Z}_2$-lattice, L_2 is isometric to either

$$[0,1,0]\perp[0,1,0] \quad \text{or} \quad [0,1,0]\perp[2,1,2].$$

Since the former represents all binary even $\mathbb{Z}_2$-lattices, assume that L_2 is isometric to the latter. Then L_2 represents all binary primitive even $\mathbb{Z}_2$-lattices except $[4,2,4]$. So any binary even $\mathbb{Z}_2$-lattice that represents a 2-adic integer θ with $ord_2(\theta)=1$ is represented by L_2. Thus by taking any s and t satisfying $t\not\equiv a/2 \pmod 2$, we obtain $\ell_s(t)_2\rightarrow L_2$.

(c) $p\in V_2$: Let T be the product of those primes $p\in W\cup V_1\cup\{2\}$ for which we took t satisfying $t\equiv 0 \pmod p$ in order for L_p to represent $\ell_s(t)_p$ in (b).

Note that every binary $\mathbb{Z}_p$-lattice whose scale is $\mathbb{Z}_p$ can be represented by L_p. It suffices to find a suitable integer S such that $\gcd(a-2kT^2, Sa+b, p)=1$ so that $\ell_S(T)_p\rightarrow L_p$ for all $p\in V_2$. Let

$$B:=3^{\nu}\times\prod_{p\in W\cup V_1} p,$$

where $\nu=1$ if $3\in W\cup V_1$ and $\nu=0$ otherwise, and take $s'\le B$ such that $\ell_{s'}(T)_p\rightarrow L_p$ for all $p\in W\cup V_1\cup\{2\}$. Then clearly, $\ell_{Bh+s'}(T)_p\rightarrow L_p$ for all integers h and $p\in W\cup V_1\cup\{2\}$.

Let A be the set of all primes dividing $a-2kT^2$ and let

$$A\cap V_2=\{q_1,q_2,\dots,q_e\}.$$

We may assume that $e\ge 1$. Note that $\gcd(Ba, q_1q_2\cdots q_e)=1$. By Lemma 3 in [12], if we let g be the smallest integer satisfying

$$2g+1\ge (q_1+e-1)2^e/(q_1-1),$$

then there exists an integer S in the set

$$\{\,B(-g)+s', B(-g+1)+s',\dots,s',\dots,B(g-1)+s', Bg+s'\,\}$$

such that $Sa+b$ is not divisible by q_i for all i, $1\le i\le e$. If we take this S, then $\ell_S(T)_p\rightarrow L_p$ for all $p\in V_2$.

Note that the with S and T chosen above, $\ell_S(T)_p\rightarrow L_p$ holds not only at all $p\in V_2$ but also at all $p\in W\cup V_1\cup\{2\}\cup U$. Furthermore, if

$$\min(\ell)=a>3d^5(g+2)^2,$$

then

$$\begin{aligned} d(\ell_S(T)) &= ac - b^2 - 2kT^2(S^2a + 2Sb + c) \\ &\geq \frac{ac}{4} - b^2 + \frac{3ac}{4} - 2kT^2(S^2c + |S|c + c) \\ &\geq \frac{3ac}{4} - 2kT^2(|S| + 1)^2 c \\ &\geq \frac{3c}{4}(a - \frac{8}{3}kT^2B^2(g+2)^2) \\ &\geq \frac{3c}{4}(a - 3d^5(g+2)^2) > 0, \end{aligned}$$

where the last line follows from $2k \leq d, T \leq d$, and $2B \leq 3d$.

Note that $a > a - 2kT^2 \geq q_1 q_2 \cdots q_e$ and that $3(g+2)^2 \leq 12e^2 4^e$. Let e_0 be the largest positive integer e for which $12e^2 4^2 \geq 5^e$ and let $C_0 := 12e_0^2 4^{e_0}$. We assume that $3 \leq q_1 < q_2 < \cdots < q_e$.

Let any small enough $\epsilon > 0$ be given. Choose a smallest prime q such that $\epsilon \log_5(\sqrt{q}/5) > 5$. Let q be the j-th smallest odd prime. Then define

$$C = C(\epsilon) := \max\{C_0, 5^{2j}\}.$$

It suffices to show that $a > C(\epsilon)d^{5+\epsilon}$ implies $a > 3d^5(g+2)^2$.

If $e \leq e_0$, then

$$a > C(\epsilon)d^{5+\epsilon} > C_0 d^5 \geq 12e^2 4^e d^5 \geq 3(g+2)^2 d^5.$$

So, we may assume $e > e_0$. If $e \leq 2j$, then

$$a > C(\epsilon)d^{5+\epsilon} \geq 5^{2j} d^{5+\epsilon} > 5^e d^5 > 3(g+2)^2 d^5.$$

So, we may further assume $e > 2j$. Let $e \leq \epsilon \log_5 d$. Then

$$a > C(\epsilon)d^{5+\epsilon} \geq C(\epsilon)d^5 5^e > d^5 5^e > 3d^5(g+2)^2.$$

Let $e > \epsilon \log_5 d$. Note that $a > q^{e/2}$ by the choice of q and the assumption $e > 2j$. Then

$$\frac{q^{e/2}}{5^e d^5} = \left(\frac{\sqrt{q}}{5}\right)^e \cdot \frac{1}{d^5} > \left(\frac{\sqrt{q}}{5}\right)^{\epsilon \log_5 d} \cdot \frac{1}{d^5} = d^{\epsilon \log_5(\sqrt{q}/5)} \cdot \frac{1}{d^5} > 1,$$

which implies $a > q^{e/2} > 5^e d^5 > 3d^5(g+2)^2$ as desired.

Therefore we can always choose a suitable positive constant $C = C(\epsilon)$ depending only on ϵ such that $\ell_S(T)$ is positive. This completes the proof. $\square$

Observe that the constant $C^*(M)$ introduced in $(\mathfrak{R}^*)$ is $C(\epsilon)(dM)^{5+\epsilon}$, which depends only on $M = L(2k)$ and the $rank(\ell) = 2$.

REMARK 3.3. The primitiveness condition on local representations cannot be omitted in Theorem 3.2 (see [9]). For example, let

$$\ell = \langle 140 \cdot 3^{2m}, 30 \cdot 7^{2m} \rangle, \quad L = [2,1,2] \perp [2,1,4].$$

For any integer $k > 70$ satisfying $k \equiv 2 \pmod{21}$, suppose that $\ell \to L(2k)$. Then there exist integers t and r such that $\ell(t,r) \to L$, where

$$\begin{aligned} \ell(t,r) :=& [140 \cdot 3^{2m} - 2kt^2, -2ktr, 30 \cdot 7^{2m} - 2kr^2] \\ =& \begin{pmatrix} 140 \cdot 3^{2m} - 2kt^2 & -2ktr \\ -2ktr & 30 \cdot 7^{2m} - 2kr^2 \end{pmatrix}. \end{aligned}$$

But one can easily check that $\ell(t,r)_3 \not\to L_3$ if $t \neq 0$ or $t = r = 0$ and that $(\ell(t,r))_7 \not\to L_7$ if $r \neq 0$ for all m. Note that $\ell_p \not\to^* L(2k)_p$ at $p = 3,7$ although $\ell_p \to L(2k)_p$ at all p.

We now turn to the odd version of Theorem 3.2.

THEOREM 3.4. *Assume that $d := dL(k)$ is an odd squarefree integer. Let ℓ be a binary $\mathbb{Z}$-lattice such that*

$$\ell_p \to^* (L(k))_p$$

at all p. Then for any $\epsilon > 0$, there exists a constant $C > 0$ depending only on ϵ such that

$$\textit{if } \min(\ell) > C \cdot d^{5+\epsilon}, \textit{ then } \ell \to L(k).$$

Proof. Let $\ell = [a, b, c]$ be Minkowski reduced. We define

$$\ell_s(t) := [a - kt^2, sa + b, s^2a + 2sb + c].$$

Since the proof is completely identical to that of Theorem 3.2 except at $p \neq 2$, we only consider $p = 2$. We will find integers s and t for which $\ell_s(t)_2 \to L_2$. Then the theorem follows from replacing T and B in the previous theorem by

$$T' = 2^{ord_2(t) - ord_2(T)}T \quad \text{and} \quad B' = 4B.$$

Since L_2 is quaternary odd unimodular $\mathbb{Z}_2$-lattice, L_2 represents all $\mathbb{Z}_2$-maximal $\mathbb{Z}_2$-lattices except the following cases:

Table 3.1

L_2	exceptions	L_2	exceptions
$\langle 1,1,1,1\rangle$	$\langle 1,7\rangle$, $[0,1,0]$	$\langle 1,1,1,5\rangle$	$\langle 1,3\rangle$, $[0,1,0]$
$\langle 1,1,3,3\rangle$	$[2,1,2]$	$\langle 1,1,3,7\rangle$	$[2,1,2]$
$\langle 1,1,1,3\rangle$	$\langle 3,7\rangle$	$\langle 1,1,1,7\rangle$	$\langle 3,3\rangle$
$\langle 1,3,3,3\rangle$	$\langle 1,5\rangle$	$\langle 1,7,7,7\rangle$	$\langle 1,1\rangle$.

Note also that if $ord_2(d(\mathbb{Q}_2\ell))$ is odd, then $\ell_2 \to L_2$.

(a) Firstly, we consider the case when $L(k)_2$ primitively represents all binary $\mathbb{Z}_2$-lattices. Since $S_2(L) = -(dL, dL \cdot k)$, we know that $L \not\simeq \langle 1,1,1,\epsilon\rangle$, where $S_2(L)$ is the 2-adic Hasse symbol of L and $\epsilon \equiv 1 \pmod 4$. If $\ell_s(t)_2$ is an odd lattice, then

$$\ell_s(t)_2 \to L_2 \text{ if and only if } \mathbb{Q}_2(\ell_s(t)) \to \mathbb{Q}_2 L$$

by Table 3.1. Furthermore, if $\ell_s(t)_2$ represents a unit $\eta \equiv -k \pmod 4$, then one can easily check that $\ell_s(t)_2 \to L_2$. Let $\ell_2 = [\alpha 2^u, \beta 2^v, \gamma 2^w]$, where $\alpha, \beta, \gamma \in \mathbb{Z}_2^*$. Note that

$$d(\ell_s(t)_2) = 2^{u+w}\alpha\gamma - 2^{2v} - kt^2(s^2 2^u\alpha + s2^{v+1}\beta + 2^w\gamma).$$

If $u \geq 2$, we take t satisfying $ord_2(t) = 0$. Then $\langle 2^u\alpha - kt^2\rangle \to \ell_s(t)_2$, which implies $\ell_s(t)_2 \to L_2$. If $u = 1, v \geq 1, w \geq 2$, we take s, t satisfying $s \equiv 1 \pmod 2, ord_2(t) = 0$ so that $ord_2(d(\ell_s(t)_2)) = 1$ and hence $\ell_s(t)_2 \to L_2$. Since the remaining subcases can be treated in a very similar manner, we only list the choices of s and t for all possible subcases in Table 3.2 after the proof.

(b) We now treat the other case. If $u \geq 2, w \geq 2$, then $v = 0$ by the primitiveness of representation. Consider the two choices of s, t: $s \equiv 0 \pmod 4, ord_2(t) = 0$ and $s \equiv 2 \pmod 4, ord_2(t) = 0$. Both make $\ell_s(t)_2$ odd unimodular but yield different discriminants. Therefore by Table 3.1, one of the two should be represented by L_2. Let $u \geq 3, v \geq 2, w = 0$. Since $\gamma \not\equiv dL \cdot k \pmod 8$ by the primitiveness condition, if we take $ord_2(t) = 0$, then $\ell_s(t)_2$ is odd unimodular and $d(\ell_s(t)_2) \not\equiv -d(L_2)$. This implies that $\ell_s(t)_2 \to L_2$. Now let $u = 0, v \geq 2, w = 2$. If we take $s \equiv 0 \pmod 4, ord_2(t) = 1$, then $d(\ell_s(t)_2) \equiv 4(\alpha - k)\gamma \pmod{16}$. If $\alpha k \equiv 3 \pmod 4$, then $ord_2(d(\ell_s(t)_2))$ is odd and hence $\ell_s(t)_2 \to L_2$. Similarly, if $\gamma k \equiv 3 \pmod 4$, the desired result follows by taking $s \equiv 1 \pmod 2, ord_2(t) = 1$. So we may assume that $\alpha k \equiv \gamma k \equiv 1 \pmod 4$. Consider the two choices of s, t:

$$s \equiv 1 \pmod 2, \quad ord_2(t) = 0 \quad \text{and} \quad s \equiv 0 \pmod 2, \quad ord_2(t) = 1.$$

Both make $\ell_s(t)_2$ odd but yield different discriminants over $\mathbb{Q}_2$. Therefore one of the two should be represented by L_2.

Since the remaining subcases can be treated in a very similar manner, we only list the choices of s and t for all possible subcases in Table 3.3. □

REMARK 3.5. As was mentioned in the introduction, $R^*(2) = 5$ or 6. Although we found an infinite family of quinary positive integral quadratic forms that is contained in $\mathfrak{R}_5^*(2)$, we could not observe any rule in order for a given quinary form to be a member of $\mathfrak{R}_5^*(2)$. We could not find a single quinary positive integral quadratic form that is not a member of $\mathfrak{R}_5^*(2)$, which seems to be the only way to conclude $R^*(2) = 6$, if this is true. If not, proving $R^*(2) = 5$ seems to be a very difficult problem.

Table 3.2

$u \geq 2:$ $ord_2(t) = 0;$

$u = 1, v \geq 1, w \geq 2:$ $s \equiv 1 \pmod 2, ord_2(t) = 0;$

$u = 1, v \geq 1, w = 1:$ $s \equiv 0 \pmod 2, ord_2(t) = 0;$

$u = 1, v \geq 1, w = 0:$ $ord_2(t) = 1;$

$u = 1, v = 0, w \geq 2:$ $s \equiv 1 \pmod 2, ord_2(t) = 1;$

$u = 1, v = 0, w = 1:$ $ord_2(t) = 0, 2;$

$u = 1, v = 0, w = 0:$ $s \equiv 0 \pmod 2, ord_2(t) = 1, 2;$

$u = 0, v \geq 2, w \geq 2:$ $s \equiv 1 \pmod 2, ord_2(t) = 0;$

$u = 0, v \geq 2, w = 1:$ $ord_2(t) = 1;$

$u = 0, v \geq 2, w = 0:$ $ord_2(t) = 2$ or $s \equiv 0 \pmod 4, ord_2(t) = 1;$

$u = 0, v = 1, w \geq 2:$ $s \equiv 1 \pmod 2, ord_2(t) = 0;$

$u = 0, v = 1, w = 1:$ $ord_2(t) = 2$ or $s \equiv 1 \pmod 2, ord_2(t) = 1;$

$u = 0, v = 1, w = 0:$ $s \equiv 1 \pmod 2, ord_2(t) = 0, 1;$

$u = 0, v = 0, w \geq 2:$ $s \equiv 0 \pmod 2, ord_2(t) = 1;$

$u = 0, v = 0, w = 1:$ $ord_2(t) = 1$ or $s \equiv 0 \pmod 2, ord_2(t) = 0;$

$u = 0, v = 0, w = 0, ord_2(\alpha\gamma - \beta^2) \geq 2:$ $s \equiv 0 \pmod 4, ord_2(t) = 0;$

$u = 0, v = 0, w = 0, ord_2(\alpha\gamma - \beta^2) = 1:$ $ord_2(t) = 1.$

Table 3.3

$u \geq 2, v = 0, w \geq 2:$ $s \equiv 0, 2 \pmod 4, ord_2(t) = 0;$

$u \geq 2, v \geq 1, w = 1:$ $s \equiv 1 \pmod 2, ord_2(t) = 0;$

$u \geq 2, v = 0, w = 1:$ $ord_2(t) = 2$ or $s \equiv 0 \pmod 4, ord_2(t) = 0;$

$u \geq 3, v \geq 2, w = 0:$ $ord_2(t) = 0;$

$u \geq 3, v = 1, w = 0:$ $s \equiv 0, 1 \pmod 2, ord_2(t) = 0;$

$u \geq 3, v = 0, w = 0:$ $s \equiv 0 \pmod 2, ord_2(t) = 1, 2;$

$u = 2, v \geq 2, w = 0:$ $s \equiv 0, 1 \pmod 2, ord_2(t) = 0;$

Table 3.3 (continued)

$u=2, v=1, w=0:$ $ord_2(t)=0;$

$u=2, v=0, w=0:$ $s \equiv 0 \pmod 2, ord_2(t)=2$ or $s \equiv 0 \pmod 4, ord_2(t)=1;$

$u=1, v \geq 1, w \geq 2:$ $s \equiv 1 \pmod 2, ord_2(t)=0;$

$u=1, v \geq 1, w=1:$ $s \equiv 0 \pmod 2, ord_2(t)=0;$

$u=1, v \geq 1, w=0:$ $ord_2(t)=1;$

$u=1, v=0, w \geq 3:$ $s \equiv 0 \pmod 2, ord_2(t)=0;$

$u=1, v=0, w=2:$ $s \equiv \alpha+\beta+3 \pmod 4, ord_2(t)=0$ or $s \equiv 0 \pmod 2, ord_2(t)=0;$

$u=1, v=0, w=1:$ $ord_2(t)=1;$

$u=1, v=0, w=0:$ $ord_2(t)=2$ or $s \equiv 0 \pmod 4, ord_2(t)=1;$

$u=0, v \geq 2, w \geq 3:$ $s \equiv 1 \pmod 2, ord_2(t)=0;$

$u=0, v \geq 2, w=2:$ see above;

$u=0, v \geq 2, w=1:$ $ord_2(t)=1;$

$u=0, v \geq 2, w=0:$ $ord_2(t)=2$ or $s \equiv 0 \pmod 4, ord_2(t)=1;$

$u=0, v=1, w \geq 4:$ $s \equiv 1 \pmod 2, ord_2(t)=1$ or $s \equiv 2 \pmod 4, ord_2(t)=0;$

$u=0, v=1, w=3:$ $s \equiv 0 \pmod 4, ord_2(t)=0$ or $ord_2(t)=2;$

$u=0, v=1, w=2:$ $s \equiv 1 \pmod 2, ord_2(t)=0;$

$u=0, v=1, w=1:$ $ord_2(t)=1;$

$u=0, v=1, w=0:$ $s \equiv 0,1 \pmod 2, ord_2(t)=1;$

$u=0, v=0, w \geq 2:$ $ord_2(t)=2$ or $s \equiv 1 \pmod 2, ord_2(t)=1;$

$u=0, v=0, w=1:$ $ord_2(t)=2$ or $s \equiv 0 \pmod 2, ord_2(t)=0;$

$u=0, v=0, w=0, ord_2(\alpha\gamma-\beta^2) \geq 3:$ $s \equiv 0 \pmod 4, ord_2(t)=0;$

$u=0, v=0, w=0, ord_2(\alpha\gamma-\beta^2)=2:$ $s \equiv 1,3 \pmod 4, ord_2(t)=1;$

$u=0, v=0, w=0, ord_2(\alpha\gamma-\beta^2)=1:$ $ord_2(t)=2.$

References

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

[2] W.-K. Chan, M.-H. Kim, and S. Raghavan, *Ternary universal integral quadratic forms over real quadratic fields*, Japan. J. Math. **22** (1996), 263–273.

[3] J. S. Hsia and M. I. Icaza, *Effective version of Tartakowsky's Theorem*, Acta Arith. **89** (1999), 235–253.

[4] J. S. Hsia and M. Jöchner, *Almost strong approximations for definite quadratic spaces*, Invent. Math. **129** (1997), 471–487.

[5] J. S. Hsia, Y. Kitaoka, and M. Kneser, *Representations of positive definite quadratic forms*, J. Reine. Angew. Math. **301** (1978), 132–141.

[6] D. G. James, *Primitive representations by unimodular quadratic forms*, J. Number Theory **44** (1993), 356–366.

[7] ———, *Representations by unimodular $\mathbb{Z}$-lattices*, Math. Z. **215** (1994), 465–475.

[8] M. Jöchner, *On the representations of positive definite quadratic forms, Integral Quadratic Forms and Lattices, M.-H. Kim et al (ed.)*, Contemp. Math. **249** (1999), 73–86.

[9] Y. Kitaoka, *Modular forms of degree n and representation by quadratic forms II*, Nagoya Math. J. **87** (1982), 127–146.

[10] ———, *Some remarks on representations of positive definite quadratic forms*, Nagoya Math. J. **115** (1989), 23–41.

[11] ———, *The minimum and the primitive representation of positive definite quadratic forms*, Nagoya Math. J. **133** (1994), 127–153.

[12] B. M. Kim, M.-H. Kim, and B.-K. Oh, 2-*universal positive definite integral quinary quadratic forms, Integral Quadratic Forms and Lattices, M.-H. Kim et al (ed.)*, Contemp. Math. **249** (1999), 51–62.

[13] M.-H. Kim, J. K. Koo, and B.-K. Oh, *Representations of binary forms by certain quinary positive integral quadratic forms*, J. Number Theory **89** (2001), 97–113.

[14] B. M. Kim, M.-H. Kim, and S. Raghavan, *2-universal positive definite integral quinary diagonal quadratic forms*, Ramanujan J. **1** (1997), 333–337.

[15] M.-H. Kim and B.-K. Oh, *A lower bound for the number of squares whose sum represents integral quadratic forms*, J. Korean Math, Soc. **33** (1996), 651–655.

[16] ———, *Representations of positive definite senary integral quadratic forms by a sum of squares*, J. Number Theory **63** (1997), 89–100.

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

[18] ———, *Extension of a problem of Kloosterman to lower ranks* (preprint).

[19] O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, New York-Heidelberg, 1973.

[20] ———, *The integral representations of quadratic forms over local fields*, Amer. J. Math. **80** (1958), 843–878.

[21] O. Perron, *Bemerkungen über die Verteilung der quadratischen Reste*, Math. Z. **56** (1952), 122–130.

[22] W. Tartakowsky, *Die Gesamtheit der Zahlen, die durch eine positive quadratische Form* $F(x_1, \ldots, x_s) (s \geq 4)$ *darstellbar sind*, Isv. Akad. Nauk SSSR **7**

(1929), 111–122, 165–195.

[23] G. L. Watson, *Quadratic diophantine equations*, Philos. Trans. Roy. Soc. London Ser. A **253** (1960/1961), 227–254.

Myung-Hwan Kim
Department of Mathematics
Seoul National University
Seoul 151-742, Korea
E-mail: mhkim@math.snu.ac.kr

Byeong-Kweon Oh
Department of Mathematics
Ohio State University
Columbus, Ohio 43210, U.S.A.
E-mail: bkoh@ohio-state.edu