MINIMUM OF POSITIVE DEFINITE QUADRATIC FORMS

YOSHIYUKI KITAOKA (北岡良之)

Department of Mathematics, School of Science
Nagoya University (名古屋大学)

We are concerned with representation of positive definite quadratic forms by a positive definite quadratic form. Let us consider the following assertion

\[ A_{m,n} : \text{Let } M, N \text{ be positive definite quadratic lattices over } \mathbb{Z} \text{ with } \text{rank}(M) = m \text{ and } \text{rank}(N) = n \text{ respectively. We assume that the localization } M_p \text{ is represented by } N_p \text{ for every prime } p, \text{ that is there is an isometry from } M_p \text{ to } N_p. \text{ Then there exists a constant } c(N) \text{ dependent only on } N \text{ so that } M \text{ is represented by } N \text{ if } \min(M) > c(N), \text{ where } \min(M) \text{ denotes the least positive number represented by } M. \]

We know that the assertion \( A_{m,n} \) is true if \( n \geq 2m + 3 \) and there are several results. But the present problem is whether the condition \( n \geq 2m + 3 \) is the best possible or not. It is known that this is the best if \( m = 1 \), that is \( A_{1,4} \) is false. But in the case of \( m \geq 2 \), what we know at present, is that \( A_{m,n} \) is false if \( n - m \leq 3 \). We do not know anything in the case of \( n - m = 4 \). Anyway, analyzing the counter-example, we come to the following two assertions \( APW_{m,n} \) and \( R_{m,n} \).

\[ APW_{m,n} : \text{There exists a constant } c'(N) \text{ dependent only on } N \text{ so that } M \text{ is represented by } N \text{ if } \min(N) > c'(N) \text{ and } M_p \text{ is primitively represented by } N_p \text{ for every prime } p. \]

\[ R_{m,n} : \text{There is a lattice } M' \text{ containing } M \text{ such that } M'_p \text{ is primitively represented by } N_p \text{ for every prime } p \text{ and } \min(M') \text{ is still large if } \min(M) \text{ is large.} \]

If the assertion \( R_{m,n} \) is true, then the assertion \( A_{m,n} \) is reduced to the apparently weaker assertion \( APW_{m,n} \). If the assertion \( R_{m,n} \) is false, then it becomes possible to make a counter-example to the assertion \( A_{m,n} \). As a matter of fact, \( APW_{1,4} \) is true but \( R_{1,4} \) is false, and it yields examples of \( N \) such that \( A_{1,4} \) is false.

Anyway it is important to study the behaviour of the minimum of quadratic lattices when we vary them. Our aim is to show
Theorem. The assertion $R_{m,n}$ is true if $n - m > 3$, $n \geq 2m + 1$ or $n = 2m \geq 12$.

Remark. If the assertion $R_{m,n}$ is false, we can construct a counter-example to the assertion $A_{m,n}$ as above. When the case of $n < 2m$ seems to have a different nature from the case of $n \geq 2m$.

To prove it, we are involved in analytic number theory. The rest is a brief summary of the proof.

We denote by $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_p$ and $\mathbb{Q}_p$ the ring of integers, the field of rational numbers and their $p$-adic completions. Terminology and notation on quadratic forms are those from [K]. For a lattice on $M$ on a quadratic space $V$ over $\mathbb{Q}$, the scale $s(M)$ denotes $\{B(x,y) \mid x,y \in M\}$, and the norm $n(M)$ denotes a $\mathbb{Z}$-module spanned by $\{Q(x)\mid x \in M\}$. Even for the localization $M_p$ it is similarly defined. $dM, dM_p$ denote the discriminant of $M, M_p$ respectively. A positive lattice means a lattice on a positive definite quadratic space over $\mathbb{Q}$. We give proofs only for a few assertions.

**Definition.** For a real number $x$, we define the decimal part $[x]$ by the conditions

$$-1/2 \leq [x] < 1/2 \quad \text{and} \quad x - [x] \in \mathbb{Z}.$$  

Note that $[x]^2 = [-x]^2$ for every real number $x$.

**Definition.** For positive numbers $a, b$, we write

$$a \ll_m b$$

if there is a positive number $c$ dependent only on $m$ such that $a/b < c$. If both $a \ll_m b$ and $b \ll_m a$ hold, then we write

$$a \asymp_m b.$$  

If $m$ is an absolute constant, then we omit $m$.

**Definition.** For positive numbers $c_1, c_2$, we say that a positive definite matrix $S^{(m)} = (s_{i,j})$ is $(c_1, c_2)$-diagonal if we have

$$c_1 \text{diag}(s_{1,1}, \cdots, s_{m,m}) < S < c_2 \text{diag}(s_{1,1}, \cdots, s_{m,m}).$$

If $S$ is in the Siegel domain $\mathfrak{S}$, then there exist positive numbers $c_1, c_2$ dependent on $\mathfrak{S}$ so that $S$ is $(c_1, c_2)$-diagonal (see Ch.2 in [K]).
Lemma 1. Let $M = \mathbb{Z}[v_1, \ldots, v_m]$ be a positive lattice and assume that $(B(v_i, v_j))$ is $(c_1, c_2)$-diagonal. For a primitive element $w = \sum_{i=1}^{m} r_i v_i$ in $M$ and for a natural number $N$, we have

$$\min(M + \mathbb{Z}[w/N]) \asymp c_1, c_2 \min \left( \min(M), \min \sum_{i=1}^{m} \left( br_i/N \right)^2 Q(v_i) \right).$$

Proof. Since there are positive constants $c_1, c_2$ so that

$$c_1 \sum_{i=1}^{m} x_i^2 Q(v_i) < Q(\sum_{i=1}^{m} x_i v_i) < c_2 \sum_{i=1}^{m} x_i^2 Q(v_i),$$

putting

$$Q'(\sum_{i=1}^{m} x_i v_i) := \sum_{i=1}^{m} x_i^2 Q(v_i),$$

we have

$$\min_{Q}(M + \mathbb{Z}[w/N]) \asymp c_1, c_2 \min_{Q'}(M + \mathbb{Z}[w/N]) = \min \left( \sum_{i=1}^{m} (b_i + br_i/N)^2 Q(v_i) \right),$$

where integers $b_i, b (i = 1, \ldots, m)$ should satisfy $b_i + br_i/N \neq 0$ for some $i$. By noting that under the restriction $N \parallel b$, the minimum is $\min(M)$, and that the condition $N \nmid b$ yields $b_i + br_i/N \neq 0$ for some $i$, it is equal to

$$\min \left( \min(M), \min \sum_{i=1}^{m} \left( br_i/N \right)^2 Q(v_i) \right).$$

Remark. Let $M$ and $M'$ be positive lattices of rank $M = \operatorname{rank} M'$. Then the condition $M' \supset M$ implies $\min(M') \leq \min(M) \leq [M' : M]^2 \min(M')$.

Theorem 1. Let $q_1, \ldots, q_t$ be positive numbers, and $r_1, \ldots, r_t$ non-zero integers with $r_1 = 1$, and finally $N$ a natural number. Then we have

$$K := \min \left( \sum_{j=1}^{t} \left( br_j/N \right)^2 q_j \right) \geq \min \left( \left( \frac{r_1}{2r_2} \right)^2 q_1, \cdots, \left( \frac{r_{t-1}}{2r_t} \right)^2 q_{t-1}, N^{-2} \sum_{j=1}^{t} r_j^2 q_j \right).$$
Proof. Suppose that

\[ K \leq \left( \frac{r_j}{2r_{j+1}} \right)^2 q_i \] for \( j = 1, \ldots, t - 1 \).

We will show that \( K \) is attained at \( b = 1 \). Suppose that an integer \( b \) give the minimum \( K \) and \( |b| \leq N/2 \). The condition \( N \not| b \) implies \( b \neq 0 \). First, we claim

\[ |br_j| \leq N/2 \text{ for } j = 1, \ldots, t. \]

When \( j = 1 \), it is true because of \( r_1 = 1 \). Suppose that (2) is true for \( j = i \); then we have \( |br_i| \leq N/2 \) and hence \( K \geq |br_i/N|^2 q_i = (br_i/N)^2 q_i \), which yields \( |b| \leq \sqrt{K/q_i} N/|r_i| \).

Now using (1), we have \( |br_{i+1}| \leq \sqrt{K/q_i} \cdot N/|r_i| \cdot |r_{i+1}| \leq |r_i|/(2|r_{i+1}|) \cdot N/|r_i| \cdot |r_{i+1}| = N/2 \). Thus (2) has been shown inductively.

The condition (2) implies \( |br_j| \leq N/2 \) and then

\[ K = \sum_{j=1}^{t} (br_j/N)^2 q_j = b^2/N^2 \sum_{j=1}^{t} r_j^2 q_j \geq N^{-2} \sum_{j=1}^{t} r_j^2 q_j. \]

This completes the proof. \( \Box \)

Corollary 1. Suppose \( t = 2 \). Then we have

\[ K \gg \sqrt{q_1 q_2} / N \text{ if } r_2^2 \gg \sqrt{q_1 / q_2} N \text{ or if both } (r_2, N) = 1 \text{ and } \sqrt{q_1 / q_2} N \ll 1. \]

Corollary 2. Let \( q_j, r_j, t, N, K \) be those in Theorem 1, and put

\[ \Delta := \prod_{k=1}^{t} q_k, \Delta_j := \Delta^{-(j-1)/t} \prod_{k \leq j} q_k, \eta_j := \frac{|r_j|}{N^{(j-1)/t} \Delta_j^{1/2}} \]

for \( j = 1, \ldots, t \). Then we have

(i) \[ 4 \left( \frac{\Delta}{N^2} \right)^{-1/t} K \geq \min \left( \eta_1^2, \ldots, (\eta_{t-1}/\eta_t)^2, \sum_{j=1}^{t} \eta_j^2 (\Delta/N^2)^{1-i/t} \left( \prod_{j<k \leq t} q_k \right)^{-1} \right) \geq \min((\eta_1^2, \ldots, (\eta_{t-1}/\eta_t)^2, \eta_t^2) \]

(ii) \( \eta_1 = 1 \),

(iii) if \( q_1 \geq q_2 \geq \cdots \geq q_t \), then we have \( \Delta_j \geq 1 \) for \( j = 1, \ldots, t \).

To understand \( K \), it is better to give an estimate from above.
Proposition 1. Let \( q_1, \cdots, q_l \) be positive numbers, and \( r_1, \cdots, r_t \) integers, and finally \( N \) a natural number with \( (r_1, \cdots, r_t, N) = 1 \). Put

\[
\Delta = \prod_{i=1}^{l} q_i, \quad K := \min_{b \in \mathbb{Z}, N \nmid b} \left( \sum_{j=1}^{t} \left\lfloor br_j/N \right\rfloor^2 q_j \right).
\]

Then we have the following:

(1) \( K \geq \min\{q_1, \cdots, q_l\} \) or \( K \ll_{t} (\Delta/N^2)^{1/4} \)

(2) \( K \ll_{t} (\Delta/N^2)^{1/4} \) if \( (\Delta/N^2)^{1/4} \ll_{t} \min\{q_1, \cdots, q_l\} \).

We must study the distribution of isotropic vectors in a quadratic space over a finite prime field to take account of the condition at a finite prime in the assertion \( R_{m,n} \).

Lemma 2. Let \( V = F_p[e_1, e_2] \) be a regular quadratic space over the field \( F_p \) with quadratic form \( Q \). Then for every positive integer \( H < p \), we have

\[
| \sum_{1 \leq x \leq H} \chi(Q(xe_1 + e_2)) | \leq 2\sqrt{p} \log p + 1,
\]

where \( \chi \) stands for the quadratic residue symbol with \( \chi(0) = 0 \).

The proof is routine.

Theorem 2. Let \( V = F_p[e_1, \cdots, e_m] \) \( (m \geq 3) \) be a quadratic space over \( F_p \). Then we have the following assertions:

(i) Suppose that \( Q(e_i) = 0, B(e_i, e_j) \neq 0 \) for some \( i, j \) \( (i \neq j) \). Then for any \( x_k \in F_p \) \( (k \neq i, j) \), there are elements \( y_i \in F_p, y_j = \pm 1 \) and \( u \in V \) so that

\[
v := y_i e_i + y_j e_j + \sum_{k \neq i, j} x_k e_k
\]

is isotropic and \( B(u, v) \neq 0 \).

(ii) Suppose \( m \geq 4 \) and \( \dim \text{Rad} V \leq m - 3 \). Let \( r \) be a natural number. Then there exist a subset \( T = \{t_1, \cdots, t_4\} \subset \{1, 2, \cdots, m\} \) and a positive number \( c_r \) which satisfy the following property:

Let \( S_1, S_2 \) be subsets of \( F_p \) and assume that \( |S_1| = 3 \) and \( S_2 \) is a union of at most \( r \) sets of consecutive integers. If \( p > c_r \) and \( |S_2| > 5r \sqrt{p} \log p \), then there are elements \( x_1 \in F_p, x_2 = \pm 1, x_3 \in S_1, x_4 \in S_2, y_i \in F_p \) for \( i \not\in T \) and \( u \in V \) such that

\[
v = \sum_{j=1}^{4} x_j e_{t_j} + \sum_{i \not\in T} y_i e_i
\]

is isotropic and \( B(u, v) \neq 0 \).  

To combine stories at the infinite prime and at a finite prime, we need the following.

**Theorem 3.** Let \( p \) be a prime number and \( r, m \) positive integers with \( r < m \). Let \( S^{(m)} \) be a regular symmetric integral matrix and we write \( S = \begin{pmatrix} S_1 & S_2 \\ S_3 & S_4 \end{pmatrix} \) and let \( D_1 \in M_{m-r}(\mathbb{Z}_p), D_2 \in M_r(\mathbb{Z}_p) \) be regular matrices and suppose that \( p^{t_1}, \ldots, p^{t_{m-r}} \) (resp. \( p^{t_{m-r+1}}, \ldots, p^{t_m} \)) be elementary divisors of \( D_1 \) (resp. \( D_2 \)) and \( t_1 \leq \cdots \leq t_m \). Let \( A^{(m)} = \begin{pmatrix} A_1^{(r,m-r)} & A_2^{(r)} \\ A_3^{(m-r)} & A_4^{(m-r,r)} \end{pmatrix} \) be an integral matrix with \( \det A = \pm 1 \). Assume that for a natural number \( e \),

\[
A_4 \equiv 0 \mod p^e, \quad t_{m-r} + e + t_1 \leq \min(t_m + 1, t_{m-r+1})
\]

\[
S[A] \equiv \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \mod p^{t_{m+1}}.
\]

Then \( S_4 \) and \( D_1 \) have the same elementary divisors and \( S_3 \equiv 0 \mod p^{e+t_1} \), and the matrix \( S_4^{-1}S_3 \) is integral over \( \mathbb{Z}_p \) and both \( S_1 - S_4^{-1}[S_3] \) and \( D_2 \) have the same elementary divisors over \( \mathbb{Z}_p \).

Now we can show the following, and by using them we can show the theorem.

**Proposition 2.** Let \( M \) be a positive lattice such that \( \text{rank}(M) \geq 4 \), \( s(M) \subset p\mathbb{Z} \). Then there is a positive number \( \delta \) satisfying the following condition:

If \( p > \delta \), then there is a lattice \( M' \) containing \( M \) such that \( [M' : M] \) is a power of prime \( p \), \( s(M'_p) = \mathbb{Z}_p \), and \( \min(M') \geq p^{3/4} \).

**Remark.** In the Proposition 2, let \( N \) be a positive lattice of rank \( 2m \) and assume that \( M_p \) is represented by \( N_p \) and that \( N_p \) is unimodular if \( p > \delta \). Then \( M'_p \) is primitively represented by \( N_p \).

**Proposition 3.** Let \( M \) and \( N \) be positive lattices of rank \( (M) = m \geq 6 \) and rank \( (N) = 2m \) respectively, and \( p \) a prime number, and suppose that \( M_p \) is represented by \( N_p \). Then there is a lattice \( M'(\supset M) \) such that \( M'_q = M_q \) if \( q \neq p \), \( M'_p \) is primitively represented by \( N_p \) and \( \min(M') > c(N_p)\min(M)^{cr} \), where \( c(N_p) \) depends only on \( N_p \) and \( c_p \) depends only on \( m \).

**REFERENCES**

