Y. Kitaoka
Nagoya Math. J.
Vol. 141 (1996), 1–27

THE MINIMUM AND THE PRIMITIVE REPRESENTATION OF POSITIVE DEFINITE QUADRATIC FORMS II

YOSHIYUKI KITAOKA

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

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

We know that the assertion $A_{m,n}$ is true if $n \geq 2m + 3$. A suceeding natural problem is whether it is the best or not. It is known that this is the best if $m = 1$, that is $\mathrm{A}_{1,4}$ is false. But in the case of $m \geq 2$, what we know at present, is that there is an example N so that $\mathrm{A}_{m,n}$ is false if $n - m = 3$. We do not know such examples when $n - m = 4$. Anyway, analyzing the counter-example, we come to the following two assertions $\mathrm{APW}_{m,n}$ and $\mathrm{R}_{m,n}$.

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

$\mathrm{R}_{m,n}$: *There is a lattice M' containing M such that M'_p is primitively represented by N_p for every prime p and* $\min(M')$ *is still large if* $\min(M)$ *is large.*

If the assertion $\mathrm{R}_{m,n}$ is true, then the assertion $\mathrm{A}_{m,n}$ is reduced to the apparently weaker assertion $\mathrm{APW}_{m,n}$. If the assertion $\mathrm{R}_{m,n}$ is false, then it becomes possible to make a counter-example to the assertion $\mathrm{A}_{m,n}$. As a matter of fact, $\mathrm{APW}_{1,4}$ is true but $\mathrm{R}_{1,4}$ is false in general, and it yields examples of N such that $\mathrm{A}_{1,4}$ is false.

We proved that the assertion $\mathrm{R}_{m,2m+1}$ (resp. $\mathrm{R}_{m,2m+2}$) is true if $m \geq 3$ (resp. $m \geq 2$), respectively. The aim of this paper is study the case of $n = 2m$ for $m \geq 4$. In Section 1, we study $\min \sum_{i=1}^{t} \lceil br_i/N \rfloor^2 q_i$ where q_i is a positive number, r_i, N are integers, b runs over integers $\not\equiv 0 \bmod N$ and $\lceil x \rfloor$ $(-0.5 \leq \lceil x \rfloor < 0.5)$

Received November 11, 1994.

denotes the decimal part of x. In Section 2, we study the distribution of isotropic vectors on a quadratic space over a finite field. In Section 3 the transformation matrix of two specified basis $\{v_1, \ldots, v_m\}$, $\{w_1, \ldots, w_m\}$ of a positive definite quadratic forms over $\mathbf{Z}$ is studied, where $(B(v_i, v_j))$ is reduced in the sense of Minkowski and $(B(w_i, w_j))$ gives a Jordan splitting at a prime p. In Section 4, we show the assertion $\mathrm{R}_{m,2m}(m \geq 6)$ is true.
We denote by $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Z}_p$ and $\mathbf{Q}_p$ the ring of integers, the field of rational numbers and their p-adic completions.

Terminology and notation on quadratic forms are those from [3]. We denote a quadratic form and the associated bilinear form by Q and B $(B(x, x) = Q(x))$ respectively. For a lattice on M on a quadratic space V over $\mathbf{Q}$, the scale $s(M)$ denotes $\{B(x, y) \mid x, y \in M\}$ and the norm $n(M)$ denotes a $\mathbf{Z}$-module spanned by $\{Q(x) \mid x \in M\}$. Even for the localization M_p they are similarly defined. $\mathrm{d}M$, $\mathrm{d}M_p$ denote the discriminant of M, M_p respectively. A positive lattice means a lattice on a positive definite quadratic space over $\mathbf{Q}$. For a real number x, $[x]$ denotes the largest integer which does not exceed x.

1. Minimum

DEFINITION. For a real number x, we define the decimal part $\lceil x \rfloor$ by the conditions

$$-1/2 \leq \lceil x \rfloor < 1/2 \text{ and } x - \lceil x \rfloor \in \mathbf{Z}.$$

Note that $\lceil x \rfloor^2 = \lceil -x \rfloor^2$ 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

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

If S is reduced in the sense of Minkowski or in a Siegel domain $\mathfrak{S}$, then S is (c_1, c_2)-diagonal for some positive numbers c_1, c_2 (see Ch. 2 in [3]).

LEMMA 1. *Let $M = \mathbf{Z}[v_1, \ldots, v_m]$ 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*

$$\min(M + \mathbf{Z}[w/N]) \asymp_{c_1,c_2} \min\Bigl(\min(M),\ \min_{b\in\mathbf{Z}, N\nmid b} \sum_{i=1}^m \lceil br_i/N \rfloor^2 Q(v_i)\Bigr).$$

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

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

putting

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

we have

$$\begin{aligned}\min\nolimits_Q(M + \mathbf{Z}[w/N]) &\asymp_{c_1,c_2} \min\nolimits_{Q'}(M + \mathbf{Z}[w/N]) \\ &= \min\Bigl(\sum_{i=1}^m (b_i + br_i/N)^2 Q(v_i)\Bigr),\end{aligned}$$

where integers b, b_i $(i = 1, \ldots, m)$ should satisfy $b_i + br_i/N \neq 0$ for some i. By noting that under the restriction $N \mid b$, the minimum is equal to $\min_{Q'}(M)$, and that the condition $N \nmid b$ yields $b_i + br_i/N \neq 0$ for some i because of the primitivity of w in M, the above is equal to

$$\min\Bigl(\min(M),\ \min_{b\in\mathbf{Z}, N\nmid b} \sum_{i=1}^m \lceil br_i/N \rfloor^2 Q(v_i)\Bigr). \qquad \square$$

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

LEMMA 2. *Suppose that $\min_{b\in\mathbf{Z}, N\nmid b} \sum_{i=1}^m \lceil br_i/N \rfloor^2 Q(v_i)$ in Lemma 1 is attained at $b = B$ and then putting $N' = (B, N)$, we have*

$$\begin{aligned}\min(M + \mathbf{Z}[w/N]) &\asymp_{c_1,c_2} \min(M + \mathbf{Z}[w/(N/N')]) \\ &\asymp_{c_1,c_2} \min\Bigl(\min(M),\ \min_{\substack{b\in\mathbf{Z} \\ (b, N/N')=1}} \sum_{i=1}^m \lceil br_i/(N/N') \rfloor^2 Q(v_i)\Bigr).\end{aligned}$$

Proof. By virtue of

$$\min_{b\in\mathbf{Z},N\nmid b}\left(\sum_{i=1}^{m}\lceil br_i/N\rceil^2 Q(v_i)\right)=\min_{(b,N)=N'}\left(\sum_{i=1}^{m}\lceil br_i/N\rceil^2 Q(v_i)\right)$$
$$=\min_{(b,N/N')=1}\left(\sum_{i=1}^{m}\lceil br_i/(N/N')\rceil^2 Q(v_i)\right)\geq\min_{b\in\mathbf{Z},(N/N')\nmid b}\left(\sum_{i=1}^{m}\lceil br_i/(N/N')\rceil^2 Q(v_i)\right),$$

we have

$$\begin{aligned}
&\min(M+\mathbf{Z}[w/N])\asymp_{c_1,c_2}\min\left(\min(M),\ \min_{b\in\mathbf{Z},N\nmid b}\sum_{i=1}^{m}\lceil br_i/N\rceil^2 Q(v_i)\right)\\
&=\min\left(\min(M),\ \min_{(b,N/N')=1}\sum_{i=1}^{m}\lceil br_i/(N/N')\rceil^2 Q(v_i)\right)\\
&\geq\min\left(\min(M),\ \min_{b\in\mathbf{Z},(N/N')\nmid b}\sum_{i=1}^{m}\lceil br_i/(N/N')\rceil^2 Q(v_i)\right)\\
&\gg_{c_1,c_2}\min(M+\mathbf{Z}[w/(N/N')])\\
&\geq\min(M+\mathbf{Z}[w/N]),
\end{aligned}$$

because of $M+\mathbf{Z}[w/N]\supset M+\mathbf{Z}[w/(N/N')]$. □

LEMMA 3. *Let α_i be positive numbers with $\alpha_i<1/2$ for $i=1,\dots,t$ and N a natural number. Put*

$$X(\alpha_1,\dots,\alpha_t;N):=\left\{(r_1,\dots,r_t)\bmod N\ \middle|\ \begin{array}{l}|\lceil rr_i/N\rceil|<\alpha_i \text{ for } i=1,\dots,t \text{ and}\\ \text{for some integer } r \text{ with } (r,N)=1\end{array}\right\}.$$

Then we have

$$|X(\alpha_1,\dots,\alpha_t;N)|<3^tN\prod_{i=1}^{t}\max(\alpha_iN,1).$$

Proof. Suppose that $(r_1,\dots,r_t)$ is an element in $X(\alpha_1,\dots,\alpha_t;N)$ and $|\lceil rr_i/N\rceil|<\alpha_i$ for some integer r relatively prime to N. We can choose integer b_i so that $b_i\equiv rr_i \bmod N$ and $|b_i/N|<\alpha_i$. Then we have $r_t\equiv Rb_t \bmod N$ for an integer R with $rR\equiv 1\bmod N$, and hence

$$\begin{aligned}
|X|&\leq N|\{(b_1\dots,b_t)\bmod N\mid |b_i/N|<\alpha_i\ (i=1,\dots,t)\}|\\
&\leq N\prod_{i=1}^{t}(2[\alpha_iN]+1)<3^tN\prod_{i=1}^{t}\max(\alpha_iN,1).
\end{aligned}$$
□

PROPOSITION 1. *Let $q_1,\dots,q_t$, c be positive numbers with $c/q_i<1/4$ for $i=1,\dots,t$, and N and N' a natural number and a divisor of N, respectively. Let S be a* *subset of* $(\mathbf{Z}/N\mathbf{Z})^t$ *such that for every element* $(r_1, \ldots, r_t) \in S$

$$\min_{b \in \mathbf{Z}, N \nmid b} \left(\sum_{i=1}^{t} \lceil br_i/N \rceil^2 q_i \right)$$

is given at b *with* $N' = (b, N)$. *If*

$$| S \bmod N/N' | > 3^t (N/N') \, \Pi \max(\sqrt{c/q_i} \cdot N/N', 1),$$

then there exists an element $(r_1, \ldots, r_t) \in S$ *such that*

$$\min_{b \in \mathbf{Z}, N \nmid b} \left(\sum_{i=1}^{t} \lceil br_i/N \rceil^2 q_i \right) \geq c.$$

Proof. Suppose that the assertion is false; then for every $(r_1, \ldots, r_t) \in S$

$$\min_{b \in \mathbf{Z}, N \nmid b} \left(\sum_{i=1}^{t} \lceil br_i/N \rceil^2 q_i \right) < c,$$

where the minimum is given at b with $N' = (b, N)$. This yields

$$\min_{b \in \mathbf{Z}, N \nmid b} \left(\sum_{i=1}^{t} \lceil br_i/N \rceil^2 q_i \right) = \min_{(b,N)=N'} \left(\sum_{i=1}^{t} \lceil br_i/N \rceil^2 q_i \right)$$
$$= \min_{(b,N/N')=1} \left(\sum_{i=1}^{t} \lceil br_i/(N/N') \rceil^2 q_i \right) < c$$

and hence $(r_1, \ldots, r_t) \bmod (N/N') \in X(\sqrt{c/q_1}, \ldots, \sqrt{c/q_t}\,; N/N')$. Lemma 3 implies

$$| S \bmod N/N' | \leq | X(\sqrt{c/q_1}, \ldots, \sqrt{c/q_t}\,; N/N') |$$
$$< 3^t (N/N') \, \Pi \max(\sqrt{c/q_i} \cdot N/N', 1),$$

which contradicts, the assumption. □

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

$$K := \min_{b \in \mathbf{Z}, N \nmid b} \left(\sum_{j=1}^{t} \lceil br_j/N \rceil^2 q_j \right)$$
$$\geq \min\left(\left(\frac{r_1}{2r_2}\right)^2 q_1, \ldots, \left(\frac{r_{t-1}}{2r_t}\right)^2 q_{t-1}, N^{-2} \sum_{j=1}^{t} r_j^2 q_j \right).$$

Proof. Suppose that

$$K \leq \left(\frac{r_j}{2r_{j+1}}\right)^2 q_j \text{ for } j = 1, \ldots, t-1. \tag{1}$$

We will show that K is attained at $b = 1$. Suppose that an integer b gives the minimum K and $|b| \leq N/2$. The condition $N \nmid b$ implies $b \neq 0$. First, we claim

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

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

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

where the equality occurs for $b = \pm 1$. This completes the proof. □

COROLLARY 1. *Let q_j, r_j, N, K be those in Theorem, and put*

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

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

(i) $$4\left(\frac{\Delta}{N^2}\right)^{-1/t} K$$
$$\geq \min\left((\eta_1/\eta_2)^2, \ldots, (\eta_{t-1}/\eta_t)^2, \sum_{j=1}^{t} \eta_j^2 (\Delta/N^2)^{1-j/t} \left(\prod_{j<k\leq t} q_k\right)^{-1}\right)$$
$$\geq \min((\eta_1/\eta_2)^2, \ldots, (\eta_{t-1}/\eta_t)^2, \eta_t^2)$$

(ii) $\eta_1 = 1$,

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

Proof. $\eta_1 = 1$ is trivial. We have for $j < t$,

$$\left(\frac{r_j}{r_{j+1}}\right)^2 q_j = \frac{\eta_j^2 N^{2(j-1)/t} \prod_{k<j} q_k \cdot \Delta^{-(j-1)/t}}{\eta_{j+1}^2 N^{2j/t} \prod_{k<j+1} q_k \cdot \Delta^{-j/t}} q_j$$
$$= \left(\frac{\eta_j}{\eta_{j+1}}\right)^2 \left(\frac{\Delta}{N^2}\right)^{1/t},$$

and hence

$$\left(\frac{r_j}{r_t}\right)^2 q_j \cdots q_{t-1} = \left(\frac{\eta_j}{\eta_t}\right)^2 \left(\frac{\Delta}{N^2}\right)^{(t-j)/t},$$

and then by putting $j = 1$

$$\frac{r_t^2}{N^2} q_t = \eta_t^2 (\Delta / N^2)^{1/t}.$$

Therefore we have

$$\left(\frac{r_j}{N}\right)^2 q_j = \eta_j^2 (\Delta / N^2)^{1-(j-1)/t} \Big(\prod_{j<k\le t} q_k \Big)^{-1}.$$

The inequality in (i) follows trivially from the above.
Suppose $q_1 \ge q_2 \ge \cdots \ge q_t$; then we have

$$\begin{aligned}\Delta_j = \prod_{k<j} q_k \cdot \Delta^{-(j-1)/t} &= \prod_{k<j} q_k^{1-(j-1)/t} \cdot \prod_{k\ge j} q_k^{-(j-1)/t} \\ &\ge q_j^{\Sigma_{k<j}(1-(j-1)/t)} \cdot q_j^{\Sigma_{k\ge j} -(j-1)/t} = 1. \qquad \square\end{aligned}$$

COROLLARY 2. *Suppose $t = 2$ in Theorem. Then we have*

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

Proof. It follows from Theorem that

$$4\left(\frac{q_1 q_2}{N^2}\right)^{-1/2} K \ge \min\left(\frac{\sqrt{q_1/q_2}N}{r_2^2}, \frac{r_2^2}{\sqrt{q_1/q_2}N} + \frac{1}{\sqrt{q_2/q_1}N}\right).$$

Hence the first assertion is clear. Next we assume $(r_2, N) = 1$ and take an integer R_2 such that $r_1 \equiv R_2 r_2 \bmod N$ and $0 < R_2 < N$, and we note that $B := br_2$ runs over the same set $\bmod N$ as b. Interchanging the suffices 1 and 2, we have

$$4\left(\frac{q_1 q_2}{N^2}\right)^{-1/2} K \ge \min\left(\frac{\sqrt{q_2/q_1}N}{R_2^2}, \frac{R_2^2}{\sqrt{q_2/q_1}N} + \frac{1}{\sqrt{q_1/q_2}N}\right).$$

The second assertion follows from $\sqrt{q_2/q_1}N R_2^{-2} \ge (\sqrt{q_1/q_2}N)^{-1} \gg 1$. $\square$

COROLLARY 3. *Let $q_1, \dots, q_t$ be positive numbers and $N\,(> 2)$ a natural number. Let $x_1, \dots, x_t, x$ be integers and suppose that one of $2x_1, \dots, 2x_t, 2x$ is not congruent to $0 \bmod N$. Then there are integers $r_1, \dots, r_t$ such that $\sum_{i=1}^t r_i x_i \not\equiv x \bmod N$ and*

$$\min_{b\in\mathbf{Z}, N\nmid b}\left(\sum_{i=1}^{t}\lceil br_i/N\rceil^2 q_i\right) \gg \left(N^{-2}\prod_{i=1}^{t} q_i\right)^{1/t}.$$

Proof. We may suppose $q_1 \geq q_2 \geq \cdots \geq q_t$. For integers $r_1 = \pm 1, r_2, \ldots, r_t$, let Δ, Δ_i, η_i be those in Corollary 1. By virtue of $\Delta_i \geq 1$, we can choose r_i so that $\eta_i \asymp 1$ for $i > 1$. We note that this property also holds for $r_i + 1$ instead of r_i because of $\Delta_i \geq 1$. If $\sum_{i=1}^{t} r_i x_i \not\equiv x \bmod N$, then Corollary 1 implies the assertion. Suppose

$$\sum_{i=1}^{t} R_i x_i \equiv x \bmod N \text{ for } R_1 = \pm 1,\ R_i = r_i,\ r_i + 1\ (i > 1).$$

Substituting $R_j = r_j, r_j + 1$, we have $x_j \equiv 0 \bmod N$ for $j > 1$. Hence we have $x_1 \equiv -x_1 \equiv x \bmod N$, and then $2x \equiv 2x_1 \equiv 0 \bmod N$. This is the contradiction. □

PROPOSITION 2. *Let $q_1, \ldots, q_t$ be positive numbers, $r_1, \ldots, r_t$ integers, and N a natural number with $(r_1, \ldots, r_t, N) = 1$. Put*

$$\Delta = \prod_{i=1}^{t} q_i, \quad K := \min_{b\in\mathbf{Z}, N\nmid b}\left(\sum_{j=1}^{t}\lceil br_i/N\rceil^2 q_j\right).$$

Then we have

$$K \geq \min\{q_1, \ldots, q_t\} \text{ or } K \ll_t (\Delta/N^2)^{1/t}.$$

Proof. Define a positive lattice $M := \mathbf{Z}[v_1, \ldots, v_t]$ by $(B(v_i, v_j)) = \mathrm{diag}(q_1, \ldots, q_t)$ and put $M' := M + \mathbf{Z}[(\sum r_i v_i)/N]$. Then we have $[M' : M] = N$ and hence $\mathrm{d}M = N^2\,\mathrm{d}M'$. The general theory of positive definite quadratic forms implies $\min(M') \ll_t (\mathrm{d}M')^{1/t} = (\Delta/N^2)^{1/t}$. On the other hand, Lemma 1 implies $\min(M') \asymp_t \min(\min(M), K)$, and hence if $K < \min(M) = \min\{q_1, \ldots, q_t\}$, we have $K \asymp_t \min(M') \ll_t (\mathrm{d}M')^{1/t} = (\Delta/N^2)^{1/t}$. □

EXAMPLE. In Proposition 2, put $t = 2$, $r_1 = r_2 = 1$, $q_1 = 1$, $q_2 = N^{2+\varepsilon}$ ($\varepsilon > 0$). Then we have

$$K = N^{-2} + N^{\varepsilon},\ (\Delta/N^2)^{1/t} = N^{\varepsilon/2}.$$

Hence $K \ll_t (\Delta/N^2)^{1/t}$ is false in this case.

PROPOSITION 3. *Let $t, q_i, r_i, N, \Delta, K$ be those in Proposition 2. Then there is a positive number δ_t dependent on t such that*

$$K \ll_t (\Delta/N^2)^{1/t} \textit{ if } (\Delta/N^2)^{1/t} < \delta_t \min\{q_1, \ldots, q_t\}.$$

Proof. We use induction on t. The assertion is clearly true for $t = 1$, since $K = \Delta/N^2$. We may suppose $q_1 \leq \cdots \leq q_t$ without loss of generality. Put $M = (r_2, \ldots, r_t, N)$. First, suppose $M \neq 1$; then for $b := N/M$ ($\not\equiv 0 \bmod N$), br_1/N is not an integer and therefore we have

$$K \leq \sum_{i=1}^{t} \lceil br_i/N \rfloor^2 q_i = \lceil br_1/N \rfloor^2 q_1 \leq q_1/4,$$

which implies $K \ll_t (\Delta/N^2)^{1/t}$ by virtue of Proposition 2.

Hereafter we suppose $M = 1$. We choose a sufficiently small constant δ_t. By the assumption, we have $\Delta/N^2 < \delta_t^t q_1^t \leq \delta_t^t q_1 q_2^{t-1}$ and hence $q_2 \cdots q_t/N^2 < \delta_t^t q_2^{t-1} < \delta_{t-1}^{t-1} q_2^{t-1}$ if $\delta_t^t < \delta_{t-1}^{t-1}$. Then the induction hypothesis implies

$$\min_{b \in \mathbf{Z}, N \nmid b} \sum_{i=2}^{t} \lceil br_i/N \rfloor^2 q_i < c_{t-1}(q_2 \cdots q_t/N^2)^{1/(t-1)}$$

for some constant c_{t-1}. Therefore, for the integer b which gives the minimum of the left-hand side in the above inequality, we have

$$K \leq \sum_{i=1}^{t} \lceil br_i/N \rfloor^2 q_i \leq q_1/4 + c_{t-1}(q_2 \cdots q_t/N^2)^{1/(t-1)}.$$

Here we have

$$(q_2 \cdots q_t/N^2)^{1/(t-1)} = q_1^{-1/(t-1)}(\Delta/N^2)^{1/(t-1)} < q_1^{-1/(t-1)}(\delta_t q_1)^{t/(t-1)} = \delta_t^{t/(t-1)} q_1$$

and hence $K \leq (1/4 + c_{t-1}\delta_t^{t/(t-1)})q_1 < q_1$ if $1/4 + c_{t-1}\delta_t^{t/(t-1)} < 1$. Proposition 2 implies $K \ll_t (\Delta/N^2)^{1/t}$, which completes the proof. $\square$

Proposition 4. *Let* t, q_i, r_i, N, K *be those in* Proposition 2. *If* $N \gg_t 1$, *then we have*

$$K \ll_t N^{-2/t} \max_i q_i.$$

Proof. If $N \gg_t 1$, then $\min_{N \nmid b} \sum_{i=1}^t \lceil br_i/N \rfloor^2 \ll_t N^{-2/t}$ follows from Proposition 3. Thus there is an integer $b \not\equiv 0 \bmod N$ such that $\sum_{i=1}^t \lceil br_i/N \rfloor^2 \ll_t N^{-2/t}$, and hence we have $K \leq \sum_{i=1}^t \lceil br_i/N \rfloor^2 q_i \ll_t N^{-2/t} \max_i q_i$. $\square$

Proposition 5. *Let* t *be a natural number,* p *a prime number and* $r_i = R_i p^{e_i}$ *integers with* $(p, R_i) = 1$ *for* $i = 1, 2, \ldots, t$. *We assume that* $e_1 = 0 \leq e_2 \leq e_3 \leq \cdots$

$\le e_t$ and define a sequence of integers $v_0 := 1 < v_1 < v_2 < \cdots < v_k < v_{k+1} := t+1$ by

$$\begin{aligned} & e_{v_0} = \cdots = e_{v_1-1} \\ < & e_{v_1} = \cdots = e_{v_2-1} \\ < & \quad \cdots \\ < & e_{v_k} = \cdots = e_{v_{k+1}-1}. \end{aligned}$$

For a natural number e_{t+1} $(\ge e_t)$ and positive numbers $q_1, q_2, \ldots, q_t$, we put

$$K := \min_{b \in \mathbf{Z}, N \nmid b} \left(\sum_{j=1}^{t} \lceil br_j / N \rceil^2 q_j \right) \quad \text{where } N := p^{e_{t+1}}$$

$$K_j := \min_{b \in \mathbf{Z}, p^{E_j} \nmid b} \left(\sum_{i < v_j} \lceil bR_i / p^{E_j} \rceil^2 q_i p^{-2(e_{v_{j-1}} - e_i)} \right) \text{ for } j = 1, \ldots, k+1$$

where $E_j := e_{v_j} - e_{v_{j-1}}$. Then we have $K \ge \min\{K_1, \ldots, K_{k+1}\}$.

Proof. Putting $v := v_1$, $e := e_{v_1}$, $s = e_{t+1}$, we claim that

$$K \ge \min\left\{ K_1, \min_{b \in \mathbf{Z}, p^{s-e} \nmid b} \left(\sum_{i<v} \lceil br_i / p^{s-e} \rceil^2 q_i p^{-2e} + \sum_{i \ge v} \lceil br_i p^{-e} / p^{s-e} \rceil^2 q_i \right) \right\}. \tag{1}$$

Let us show the claim. For an integer c, we put

$$K(c) := \min_{b} \sum_{i=1}^{t} \lceil br_i / p^s \rceil^2 q_i,$$

where b runs over the set of integers satisfying $b \equiv c \bmod p^{s-e}$ and $b \not\equiv 0 \bmod p^s$. It is easy to see

$$K(0) = \min_{B \in \mathbf{Z}, p^e \nmid B} \sum_{i<v} \lceil Br_t / p^e \rceil^2 q_t = K_1.$$

Next, for an integer c $(\not\equiv 0 \bmod p^{s-e})$ we assume $K(c)$ is attained at b $(\equiv c \bmod p^{s-e})$. Then we have

$$K(c) = \sum_{i<v} \lceil br_i / p^s \rceil^2 q_i + \sum_{i \ge v} \lceil cr_i / p^s \rceil^2 q_i.$$

Now we show

$$| \lceil br_i p^{-s} \rceil | \ge | \lceil br_i p^{-(s-e)} \rceil | p^{-e} \quad \text{for } i < v. \tag{2}$$

We define integers B, B_1, B_2 by

$$B \equiv br_i \bmod p^s, \ -p^s/2 \le B < p^s/2,$$

$$B = B_1 + B_2 p^{s-e},\ -p^{s-e}/2 \le B_1 < p^{s-e}/2.$$

We have only to show $|B/p^s| \ge |B_1/p^{s-e}|p^{-e}$, and may assume $B \ge 0$ without loss of generality. If $0 \le B_1 < p^{s-e}/2$, then we have $B_2 \ge 0$ and then $B/p^s = B_1/p^s + B_2/p^e \ge B_1/p^s = (B_1/p^{s-e})p^{-e}$, which is the required inequality. If $-p^{s-e}/2 \le B_1 < 0$, then we have $B_2 > 0$ and hence $B/p^s = (B_1 + p^{s-e} + (B_2 - 1)p^{s-e})/p^s \ge (B_1 + p^{s-e})/p^s = (B_1/p^{s-e} + 1)p^{-e} \ge |B_1/p^{s-e}|p^{-e}$, because of $x + 1 \ge |x|$ for a real number $x := B_1/p^{s-e}$ in $[-1/2, 0)$. Thus we have shown the inequality (2) and

$$\begin{aligned} K(c) &\ge \sum_{i<v} \lceil br_i/p^{s-e}\rceil^2 q_i p^{-2e} + \sum_{i\ge v} \lceil cr_i/p^s\rceil^2 q_i \\ &= \sum_{i<v} \lceil cr_i/p^{s-e}\rceil^2 q_i p^{-2e} + \sum_{i\ge v} \lceil cr_i/p^s\rceil^2 q_i. \end{aligned}$$

Hence the identity $K = \min\{K(c) \mid c \in \mathbf{Z}\}$ implies

$$K \ge \min\{K(0),\ \min_{c\not\equiv 0 \bmod p^{s-e}} (\sum_{i<v} \lceil cr_i/p^{s-e}\rceil^2 q_i p^{-2e} + \sum_{i\ge v} \lceil cr_i/p^s\rceil^2 q_i)\}$$

implies the inequality (1).

Now the assertion of the lemma is shown by induction on k. By the claim (1), we have $K \ge \min\{K_1, K'\}$, and

$$K' := \min_{b\in\mathbf{Z}, N'\nmid b} \left(\sum_{i<v_1} \lceil bR_i/N'\rceil^2 q_i p^{-2e_{v_1}} + \sum_{i\ge v_1} \lceil br_i p^{-e_{v_1}}/N'\rceil^2 q_i\right)$$

where $N' := p^{s-e_{v_1}}$. Put

$$V_i := v_{i+1} \text{ for } i = 1, \ldots, k-1, \text{ and } V_0 := 1,\ V_k := t+1,$$

$$e'_i := \begin{cases} 0 & \text{if } i < v_1, \\ e_i - e_{v_1} & \text{if } i \ge v_1, \end{cases} \quad Q_i := \begin{cases} q_i p^{-2e_{v_1}} & \text{if } i < v_1, \\ q_i & \text{if } i \ge v_1. \end{cases}$$

Then we have

$$\begin{aligned} e'_{v_j} - e'_{v_{j-1}} &= e_{v_{j+1}} - e_{v_j} \text{ for } j = 1, \ldots, k \\ Q_i p^{-2(e'_{v_{j-1}} - e'_i)} &= q_i p^{-2(e_{v_j} - e_i)} \text{ for } i < v_j\ (j = 1, \ldots, k). \end{aligned}$$

Therefore we can apply the induction hypothesis to K'. □

2. Distribution of isotropic vectors

In this section, we study the distribution of isotropic vectors in a quadratic space over a finite prime field. p denotes an odd prime number and F_p stands for the prime field $\mathbf{Z}/p\mathbf{Z}$ through this section.

THEOREM 1. *Let $V = F_p[e_1, e_2]$ be a regular quadratic space over F_p with quadratic form Q. Then for every positive integer $H < p$, we have*

$$\left| \sum_{1 \le x \le H} \chi(Q(xe_1 + e_2)) \right| \le 2\sqrt{p}\log p + 1,$$

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

To prove this, we prepare several lemmas.

LEMMA 1. *Let H be an integer such that $1 \le H < p$. For a function $c(x)$ on F_p defined by*

$$c(x) := \begin{cases} 1 & \text{if } 1 \le x \le H, \\ 0 & \text{otherwise,} \end{cases}$$

we put

$$h(y) := p^{-1} \sum_{x \in F_p} c(z) e(-yz/p),$$

where $e(x)$ denotes $\exp(2\pi i x)$. Then we have

$$c(x) = \sum_{y \in F_p} h(y) e(xy/p).$$

Proof. The assertion follows from

$$\sum_{y \in F_p} h(y) e(xy/p) = p^{-1} \sum_{y \in F_p} \sum_{z \in F_p} c(z) e((-yz + xy)/p)$$
$$= p^{-1} \sum_{z \in F_p} c(z) \sum_{y \in F_p} c(y(x - z)/p) = c(x).$$

□

LEMMA 2. *For $a, b \in F_p$ with $a^2 - 4b \neq 0$, let us define the function $\phi(x)$ on F_p by $\phi(x) := x^2 + ax + b$. Then we have*

$$\sum_{x \in F_p} \chi(\phi(x)) = -1,$$

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

Proof. See Theorem 8.2 in [1]. □

LEMMA 3. *For the above functions* χ *and* ψ, *we have*

$$\Big| \sum_{x\in F_p} \chi(\psi(x))e(xy/p) \Big| \leq 2\sqrt{p}.$$

Proof. We use Theorem 2G on p. 45 in [5]. We put $f(x) := \psi(x)$ and $g(x) := x$ there. Then $Y^2 - f(X)$ is absolutely irreducible because of $\psi(x) = (x + a/2)^2 + b - a^2/4$ and $b - a^2/4 \neq 0$ in F_p, and so is $Z^p - Z - g(X)$ by Theorem 1B on p. 92 in [5]. Hence the condition (ii) in Theorem 2G is satisfied and we have the assertion. □

LEMMA 4. *For the function* $h(x)$ *in Lemma* 1, *we have*

$$\sum_{y\in F_p^\times} | h(y) | \leq \log p.$$

Proof. Since $\sum_{y\in F_p^\times} | h(y) | = p^{-1} \sum_{y\in F_p^\times} | \sum_{1\leq z\leq H} e(-yz/p) |$, the inequality on p. 56 in [6] gives the required one. □

LEMMA 5. *Let* H *be an integer such that* $1 \leq H < p$, *the functions* χ *and* ψ *as above. Then putting*

$$\Phi := \sum_{1\leq x\leq H} \chi(\psi(x)),$$

we have

$$| \Phi | \leq 2\sqrt{p}\log p + 1.$$

Proof. It is easy to see, using the function $c(x)$ and $h(x)$ in Lemma 1

$$\begin{aligned}
\Phi &= \sum_{y\in F_p} \chi(\psi(x))c(x) \\
&= \sum_{x\in F_p} \chi(\psi(x)) \sum_{y\in F_p} h(y)e(xy/p) \\
&= \sum_{x\in F_p} \chi(\psi(x))h(0) + \sum_{y\in F_p^\times} h(y) \sum_{x\in F_p} \chi(\psi(x))e(xy/p) \\
&= -p^{-1} \sum_{z\in F_p} c(z) + \sum_{y\in F_p^\times} h(y) \sum_{x\in F_p} \chi(\psi(x))e(xy/p) \\
&= -H/p + \sum_{y\in F_p^\times} h(y)\{ \sum_{x\in F_p} \chi(\psi(x))e(xy/p)\}.
\end{aligned}$$

Hence we have

$$| \Phi | \leq H/p + \sum_{y\in F_p^\times} | h(y) |\cdot 2\sqrt{p} \leq H/p + 2\sqrt{p}\log p \leq 2\sqrt{p}\log p + 1. \quad \square$$

Proof of Theorem 1. Putting $\phi(x) := Q(xe_1 + e_2)$, we show

$$\Big| \sum_{1 \le x \le H} \chi(\phi(x)) \Big| \le 2\sqrt{p} \log p + 1.$$

If $Q(e_1) \ne 0$, then we can apply Lemma 5 because of $\phi(x) = Q(e_1)\{x^2 + 2B(e_1, e_2)Q(e_1)^{-1}x + Q(e_2)Q(e_1)^{-1}\}$, where the bilinear form $B(x, y)$ is defined by $2B(x, y) := Q(x+y) - Q(x) - Q(y)$. If $Q(e_1) = 0$, then we have $B(e_1, e_2) \ne 0$ and $\phi(x) = 2B(e_1, e_2)(x + Q(e_2)/(2B(e_1, e_2)))$, and then Pólya-Vinogradov's inequality (Problem α) in **b**. on p. 102 in [6]) yields the inequality. □

THEOREM 2. *Let* $V = F_p[e_1, \ldots, e_m]$ $(m \ge 3)$ *be a quadratic space over* F_p. *Then we have the following assertions*:
(i) *Suppose that* $Q(e_i) = 0$, $B(e_i, e_j) \ne 0$ *for some* i, j $(i \ne j)$. *Then for any* $x_k \in F_p$ $(k \ne i, j)$, *there are elements* $y_i \in F_p$, $y_j = \pm 1$ *and* $u \in V$ *so that*

$$v := y_i e_i + y_j e_j + \sum_{k \ne i,j} x_k e_k$$

is isotropic and $B(u, v) \ne 0$.
(ii) *Suppose* $m \ge 4$ *and* $\dim \mathrm{Rad}\, V \le m - 3$. *Then there exists a subset* $T = \{t_1, t_2, t_3\} \subset \{1, 2, \ldots, m\}$ *which satisfies the following property*:

Let S_1, S_2 *be subsets of* F_p *and assume that* $|S_1| = 3$ *and* S_2 *is a set of consecutive integers. If* $p > 5$ *and* $|S_2| > 5\sqrt{p} \log p$, *then there are elements* $x_1 = \pm 1$, $x_2 \in S_1$, $x_3 \in S_2$, $y_i \in F_p$ *for* $i \notin T$ *and* $u \in V$ *such that*

$$v = \sum_{j=1}^{3} x_j e_{t_j} + \sum_{i \notin T} y_i e_i$$

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

Proof of (i). Suppose that $Q(e_i) = 0$, $B(e_i, e_j) \ne 0$ for some i, j $(i \ne j)$ and x_k $(k \ne i, j)$ is given. Putting $v := y_i e_i + y_j e_j + \sum_{k \ne i,j} x_k e_k$, we have

$$\begin{aligned} Q(v) &= 2y_i B(e_i, y_j e_j + \sum_{k \ne i,j} x_k e_k) + Q(y_j e_j + \sum_{k \ne i,j} x_k e_k) \\ &= 2y_i (y_j B(e_i, e_j) + B(e_i, \sum_{k \ne i,j} x_k e_k)) + Q(y_j e_j + \sum_{k \ne i,j} x_k e_k). \end{aligned}$$

Because of $B(e_i, e_j) \ne 0$, we can take $y_j = \pm 1$ so that $y_j B(e_i, e_j) + B(e_i, \sum_{k \ne i,j} x_k e_k) \ne 0$ and then we can choose y_i so that v is isotropic. For $u := e_i$, we have

$$B(u, v) = y_j B(e_j, e_j) + B(e_i, \sum_{k \ne i,j} x_k e_k) \ne 0. \qquad \square$$

To prove the assertion (ii), we prepare two lemmas.

LEMMA 6. *Let* $W = F_p[w_1, \ldots, w_n]$ $(n \geq 3)$ *be a quadratic space over* F_p *and assume that* $Q(w_1) \neq 0$, *and* $\dim \operatorname{Rad} W \leq n-2$. *For a subset* $S \subset F_p$ *with* $|S| = 3$, *there exist an element* $x \in S$ *and suffices* $i, j > 1$ $(i \neq j)$ *such that* $F_p[w_i + xw_j, w_1]$ *is a regular quadratic space.*

Proof. Putting $w_i' := w_i - \dfrac{B(w_1, w_i)}{Q(w_1)} w_1$, we have a decomposition $W = F_p[w_1] \perp F_p[w_2', \ldots, w_n']$. It is easy to see, for i, j

$$
\begin{aligned}
& F_p[w_i + xw_j, w_1] \text{ is not regular for any } x \in S \\
\Leftrightarrow\ & Q(w_i + xw_j)Q(w_1) = B(w_i + xw_j, w_1)^2 \text{ for any } x \in S \\
\Leftrightarrow\ & (Q(w_j)Q(w_1) - B(w_j, w_1)^2)x^2 + 2(B(w_i, w_j)Q(w_1) - B(w_1, w_i)B(w_1, w_j))x \\
& \quad + Q(w_i)Q(w_1) - B(w_i, w_1)^2 = 0 \text{ for any } x \in S \\
\Leftrightarrow\ & \begin{cases} Q(w_k)Q(w_1) = B(w_k, w_1)^2 & \text{for } k = j, i, \\ B(w_i, w_j)Q(w_1) = B(w_1, w_i)B(w_1, w_j). \end{cases}
\end{aligned}
$$

Moreover we have

$$
\begin{aligned}
Q(w_i') &= Q(w_1)^{-1}(Q(w_1)Q(w_i) - B(w_1, w_i)^2), \\
B(w_i', w_j') &= Q(w_1)^{-1}(Q(w_1)B(w_i, w_j) - B(w_1, w_j)B(w_i, w_1)).
\end{aligned}
$$

Now suppose that $F_p[w_i + xw_j, w_1]$ is not regular for any $i, j > 1$ $(i \neq j)$ and for any $x \in S$. Then the above implies $Q(w_i') = B(w_i', w_j') = 0$ for the above i, j, which implies $Q(F_p[w_2', \ldots, w_n']) = 0$, and then contradicts $\dim \operatorname{Rad} W \leq n - 2$. $\square$

LEMMA 7. *Let* $W = F_p[w_1, \ldots, w_n]$ $(n \geq 3)$ *be a quadratic space over* F_p *and suppose* $Q(w_1) \neq 0$, $\dim \operatorname{Rad} W \leq n-2$. *Then we have the following*:

Let S_1, S_2 *be subsets of* F_p *and assume that* $|S_1| = 3$ *and* S_2 *is a set of consecutive integers. If* $p > 5$ *and* $|S_2| > 5\sqrt{p} \log p$, *then there are elements* $x \in S_1$, $y \in S_2$, *and indeces* $i, j > 1$ $(i \neq j)$ *such that* $Q(w_i + xw_j + yw_1) \in (F_p^\times)^2$.

Proof. By virtue of Lemma 6, there exist suffices $i, j > 1$ $(i \neq j)$ and $x \in S_1$ such that $F_p[w_i + xw_j, w_1]$ is regular. Suppose $Q(w_i + xw_j + yw_1) \notin (F_p^\times)^2$ for any $y \in S_2$. By putting $t := |\{y \in S_2 \mid Q(w_i + xw_j + yw_1) = 0\}|$, $Q(w_1) \neq 0$ yields $0 \leq t \leq 2$ and the supposition implies $\sum_{y \in S_2} \chi(Q(w_i + xw_j + yw_1)) = -(|S_2| - t)$, where χ denotes the quadratic residue symbol. Theorem 1 yields

$|\sum_{y\in S_2}\chi(Q(w_i+xw_j+yw_1))|\le 2(2\sqrt{p}\log p+1)$, and hence we have $|S_2| \le 2(2\sqrt{p}\log p+1)+2$. If $|S_2|>5\sqrt{p}\log p$, which yields $p=3$ or 5. □

Proof of (ii) *in Theorem* 2. First, suppose that $Q(e_i)=0$ for every i; then the assumption $\dim \mathrm{Rad}\, V\le m-3$ yields that there are indeces i, j $(i\ne j)$ such that $B(e_i, e_j)\ne 0$. Let T be a set $\{t_1, t_2, t_3\}$ with $t_1=j$ and $i\notin T$. For $x_2\in S_1$, $x_3 \in S_2$, the assertion (i) implies that $ye_i+x_1e_{t_1}+x_2e_{t_2}+x_3e_{t_3}$ for some $y\in F_p$ and $x_1=\pm 1$ is a required element.

Next suppose that $Q(e_i)\ne 0$ for some index i. For simplicity, we may assume $i=1$:

$$Q(e_1)\ne 0$$

and put

$$w_i := e_i - \frac{B(e_i, e_1)}{Q(e_1)}e_1.$$

Putting $W=F_p[w_2, \ldots, w_m]$, we have $V=F_p[e_1]\perp W$ and $\dim \mathrm{Rad}\, W = \dim \mathrm{Rad}\, V\le m-3=\dim W-2$. We note that for an element $v:=\sum_{i=1}^m x_ie_i\in V$,

$$(1)\quad \begin{cases} v &= \sum_{i=1}^m x_i\left(w_i+\dfrac{B(e_i, e_1)}{Q(e_1)}e_1\right) = Q(e_1)^{-1}B(e_1, v)e_1+\sum_{i=2}^m x_iw_i, \\ Q(v) &= Q(e_1)^{-1}B(e_1, v)^2+Q(\sum_{i=2}^m x_iw_i). \end{cases}$$

Case (I). Suppose that there is an index k (≥ 2) such that $Q(w_k)\ne 0$. By applying Lemma 7 to the quadratic space W scaled by $-Q(e_1)^{-1}$, there are distinct indeces i, j, k with $i, j\ge 2$ and $x_j\in S_1$, $x_k\in S_2$ suth that

$$-Q(e_1)^{-1}Q(w_i+x_jw_j+x_kw_k)=r^2$$

for some element $r\in F_p^\times$. By putting

$$v:=x_1e_1+x_ie_i+x_je_j+x_ke_k$$

for $x_1\in F_p$, $x_i=1$, (1) implies $Q(v)=Q(e_1)^{-1}B(e_1, v)^2-Q(e_1)r^2$. Now we choose x_1 so that $B(e_1, v)=\sum_{h=1,i,j,k}x_hB(e_h, e_1)=Q(e_1)r$ because of the assumption $B(e_1, e_1)=Q(e_1)\ne 0$. Hence we have $Q(v)=0$ and $B(e_1, v)= Q(e_1)r\ne 0$ and have completed the proof of (ii) in the case of (I), by taking $t_1=i$, $t_2=j$, $t_3=k$.

Case (II). Suppose that $Q(w_i)=0$ if $i\ge 2$. Since $\dim \mathrm{Rad}\, W\le \dim W-2$, there are indeces $i, j\ge 2$ $(i\ne j)$ such that $B(w_i, w_j)\ne 0$. For simplicity, we may assume $B(w_2, w_3)\ne 0$. First, suppose $m\ge 5$; then put $z:=x_2w_4+x_3w_5$ for

$x_2 \in S_1$, $x_3 \in S_2$ and $v' := yw_2 + x_1w_3 + z$ for $y, x_1 \in F_p$. Since $Q(v') = 2y(x_1B(w_2, w_3) + B(w_2, z)) + 2x_1B(w_3, z) + Q(z)$, we choose $y \in F_p$ and $x_1 = \pm 1$ so that $x_1B(w_2, w_3) + B(w_2, z) \neq 0$ and $Q(v') = -Q(e_1)$. By putting $v := xe_1 + ye_2 + x_1e_3 + x_2e_4 + x_3e_5$ for $x \in F_p$, we can choose x so that $B(e_1, v) = Q(e_1)$, and then $Q(v) = 0$ follows from (1) and we complete the proof of the assertion (ii) in case of $m \geq 5$, putting $t_1 := 3$, $t_2 := 4$, $t_3 := 5$ and $u := e_1$.

Next suppose $m = 4$. We are assuming that $Q(e_1) \neq 0$ and $Q(w_2) = Q(w_3) = Q(w_4) = 0$, and $B(w_2, w_3) \neq 0$. For an element $v = x_4e_1 + x_3e_2 + x_1e_3 + x_2e_4 \in V$, (1) implies

$$Q(v) = Q(e_1)^{-1}B(e_1, v)^2 + x_3(2x_1B(w_2, w_3) + 2x_2B(w_2, w_4)) + 2x_1x_2B(w_3, w_4).$$

Suppose $x_2 \in S_1$ and choose $x_1 = \pm 1$ so that $a := 2x_1B(w_2, w_3) + 2x_2B(w_2, w_4) \neq 0$. Now we claim that there is an element $x_3 \in S_2$ so that $\chi(ax_3 + 2x_1x_2B(w_3, w_4)) = \chi(-Q(e_1))$. If it is false, then we have

$$\sum_{x_3 \in S_2} \chi(ax_3 + 2x_1x_2B(w_3, w_4)) = -\chi(-Q(e_1))(|S_2| - t),$$

where $t = |\{x_3 \in S_2 \mid ax_3 + 2x_1x_2B(w_3, w_4) = 0\}| = 0$ or 1. By applying Pólya-Vinogradov's inequality, we have $|S_2| - t \leq 2\sqrt{p}\log p$, which contradicts $|S_2| > 5\sqrt{p}\log p$. Therefore there exists $x_3 \in S_2$ so that $ax_3 + 2x_1x_2B(w_3, w_4) = -Q(e_1)^{-1}r^2$ for some $r \in F_p^\times$. Then we have $Q(v) = Q(e_1)^{-1}B(e_1, v)^2 - Q(e_1)^{-1}r^2$. Now we choose x_4 so that $B(e_1, v) = r$ because of $Q(e_1) \neq 0$. Then v is isotropic and for $u := w_2$ we have

$$B(u, v) = x_1B(w_2, w_3) + x_2B(w_2, w_4) = a/2 \neq 0,$$

which completes the proof of the assertion (ii) with $t_1 := 3$, $t_2 := 4$, $t_3 := 2$. □

3. Transformation matrix

Let us give a result to combine the reduced form at the infinite prime with a Jordan decomposition at a finite prime.

THEOREM. *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 $S = \begin{pmatrix} S_1^{(r)} & S_2 \\ S_3 & S_4 \end{pmatrix}$ and let $D_1 \in M_{m-r}(\mathbf{Z}_p)$, $D_2 \in M_r(\mathbf{Z}_p)$ 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) over $\mathbf{Z}_p$ and $t_1 \leq \cdots$*

$\le t_m$. *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,*

$$A_4 \equiv 0 \bmod p^e,\ t_{m-r} < e + t_1 \le \min(t_m + 1,\ t_{m-r+1})$$

$$S[A] \equiv \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \bmod p^{t_m+1}.$$

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

Proof. We note

$$A^{-1} \equiv \begin{pmatrix} 0^{(m-r,r)} & A_3^{-1} \\ A_2^{-1} & -A_2^{-1}A_1A_3^{-1} \end{pmatrix} \bmod p^e\mathbf{Z}_p.$$

By virtue of

$$p^{-t_1} S[A] \equiv p^{-t_1} \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \bmod p^{t_m - t_1 + 1} \text{ and } t_m - t_1 + 1 \ge e,$$

we have

$$S \equiv \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \left[\begin{pmatrix} 0 & A_3^{-1} \\ A_2^{-1} & -A_2^{-1}A_1A_3^{-1} \end{pmatrix} \right] \bmod p^{e+t_1}$$

$$\equiv \begin{pmatrix} 0^{(r)} & 0^{(r,m-r)} \\ 0^{(m-r,r)} & D_1[A_3^{-1}] \end{pmatrix} \bmod p^{e+t_1},$$

by $D_2 \equiv 0 \bmod p^{t_{m-r+1}}$. Hence S_4 and D_1 have the same elementary divisors over $\mathbf{Z}_p$ and we have $S_3 \equiv 0 \bmod p^{e+t_1}$ and then $S_4^{-1}S_3$ is integral over $\mathbf{Z}_p$ by the condition $t_{m-r} < e + t_1$. By the identity

$$S = \begin{pmatrix} S_1 - S_4^{-1}[S_3] & 0 \\ 0 & S_4^{(m-r)} \end{pmatrix} \left[\begin{pmatrix} 1_r & 0 \\ S_4^{-1}S_3 & 1_{n-r} \end{pmatrix} \right],$$

both D_2 and $S_1 - S_4^{-1}[S_3]$ have the same elementary divisors over $\mathbf{Z}_p$. □

4. Theorem

The following is the destination of this paper.

THEOREM. *Let m be an integer ≥ 6 and N a positive lattice of rank $2m$. For a positive number κ, there is a positive number $\kappa_1 = \kappa_1(\kappa, N)$ satisfying the following condition*:

Let M be a positive lattice of $\mathrm{rank}(M) = m$ *and* $\min(M) > \kappa_1$ *and M_p is represented by N_p for every prime p. Then there is a lattice $M' \supset M$ such that* $\min(M') > \kappa$ *and M'_p is primitively represented by N_p for every prime p.*

The rest of this section is devoted to the proof.
We fix a basis $\{v_1, \ldots, v_m\}$ of M so that $(B(v_i, v_j))$ is reduced in the sense of Minkowski, and we define a transformation matrix $A = (a_{ij})$ by

$$(w_1, \ldots, w_m) = (v_1, \ldots, v_m)A \tag{1}$$

for another basis $\{w_1, \ldots, w_m\}$ of M.

LEMMA 1. *Let M be a positive lattice such that* $\mathrm{rank}(M) \geq 4$, $s(M) \subset p\mathbf{Z}$ *and suppose that M_p contains a p-modular sublattice of rank ≥ 3. Then there is a positive number δ_ε for $0 < \varepsilon < 1/6$ satisfying the following condition*:

If $p > \delta_\varepsilon$, then there is an element $w \in M$ such that $(M + p^{-1}\mathbf{Z}[w])_p$ contains a hyperbolic unimodular plane with $s(M + p^{-1}\mathbf{Z}[w])\mathbf{Z}_p = \mathbf{Z}_p$ and $\min(M + p^{-1}\mathbf{Z}[w]) \gg p^{1/3-2\varepsilon}(p^{-1}\min(M)) \geq \min(M)^{1/3-2\varepsilon}$

Proof. Put $S_1 := \{[p^{1/3}], [p^{1/3}] \pm 1\}$ and $S_2 := \{x \in \mathbf{Z} \mid p^{2/3-\varepsilon} < x < p^{2/3+\varepsilon}\}$. If $p\ (> 5)$ is sufficiently large, then we have $|S_2| > 5\sqrt{p}\log p$, which is supposed in the rest of the proof. By applying Theorem 2 in Section 2 to a quadratic space $V := M^{(p^{-1})}/pM^{(p^{-1})}$ over $\mathbf{Z}/p\mathbf{Z}$, there exist a subset $\{t_1, t_2, t_3\} \subset \{1, \ldots, m\}$, $x_1 (\equiv \pm 1 \bmod p)$, $x_2 \bmod p \in S_1$, $x_3 \bmod p \in S_2$ and $y_i \in \mathbf{Z}$ for $i \neq t_j$, such that $w := \sum_{j=1}^3 x_j v_{t_j} + \sum_{i \neq t_j} y_i v_i$ satisfies $Q(w) \equiv 0 \bmod p^2$ and $B(w, M) \not\equiv 0 \bmod p^2$. This implies $s(M + p^{-1}\mathbf{Z}[w])\, \mathbf{Z}_p = \mathbf{Z}_p$, and for an element $u \in M$ with $B(w, u) \not\equiv 0 \bmod p^2$, $\mathbf{Z}_p[u, p^{-1}w]$ is a unimodular hyperbolic plane. Putting $w = \sum r_i v_i$, we have

$$\begin{aligned}
&\min(M + p^{-1}\mathbf{Z}[w]) \\
&\asymp \min(\min(M), \min_{p \nmid b} \sum_{i=1}^{m} \lceil br_i/p \rfloor^2 Q(v_i)) \\
&\gg \min(\min(M), \min_{p \nmid b} \sum_{j=1}^{3} \lceil bx_j/p \rfloor^2 Q(v_{t_j})) \\
&\gg \min(M) \min(1, \min_{p \nmid b} \sum_{j=1}^{3} \lceil bx_j/p \rfloor^2) \\
&\gg \min(M)\min(1, \min((4x_2^2)^{-1}, 4^{-1}(x_2/x_3)^2, p^{-2}(1 + x_2^2 + x_3^2)))
\end{aligned}$$ by Theorem in

Section 1
$\gg \min(M)\min(1, p^{-2/3-2\varepsilon})$
$\gg p^{-2/3-2\varepsilon}\min(M)$.

By putting $\min(M) = pa$, we have $a \geq 1$ and $p^{-2/3-2\varepsilon}\min(M) = \min(M)^{1/3-2\varepsilon}$. $a^{2/3+2\varepsilon} \geq \min(M)^{1/3-2\varepsilon}$. □

LEMMA 2. *Suppose $p \neq 2$. Let M be a positive lattice such that $s(M) \subset p\mathbf{Z}$ and M_p is a $p\mathbf{Z}_p$-maximal quaternary lattice of* $\mathrm{ind}(\mathbf{Q}_pM) \leq 1$. *Moreover we assume that the rank of a p-modular component of M_p is at most 2. Then there is an element $w \in M$ such that $s(M + p^{-1}\mathbf{Z}[w])\mathbf{Z}_p = \mathbf{Z}_p$ and* $\min(M + p^{-1}\mathbf{Z}[w]) \gg p^{1/4}$.

Proof. For some integers ε_1, ε_2 relatively prime to p, we can take a basis $\{w_1, \dots, w_4\}$ of M such that

$$(B(w_i, w_j)) \equiv \mathrm{diag}(p, \varepsilon_1 p, p^2, \varepsilon_2 p^2) \mod p^3.$$

The assumption on M_p implies that $-\varepsilon_2$ is not a quadratic residue $\bmod p$. For any integers f, g, $s(M + p^{-1}\mathbf{Z}[fw_3 + gw_4])\mathbf{Z}_p = \mathbf{Z}_p$ is clear, unless $f \equiv g \equiv 0 \bmod p$. By putting $s_i := a_{i3}$, $t_i := a_{i4}$ for a_{ij} defined by (1) and $r_i := fs_i + gt_i$ we have $fw_3 + gw_4 = \sum r_i v_i$ and

$$\min(M + p^{-1}\mathbf{Z}[fw_3 + gw_4]) \asymp \min(\min(M), K_{f,g}),$$

where

$$K_{f,g} := \min_{b \not\equiv 0 \bmod p} \sum_{i=1}^{4} \lceil br_i/p \rfloor^2 Q(v_i).$$

Now we choose $1 \leq \alpha, \beta \leq 4$ by the condition $d_{\alpha,\beta} := s_\alpha t_\beta - s_\beta t_\alpha \not\equiv 0 \bmod p$. Then we have

$$K_{f,g} \geq \min_{b \not\equiv 0 \bmod p} (\lceil br_\alpha/p \rfloor^2 Q(v_\alpha) + \lceil br_\beta/p \rfloor^2 Q(v_\beta))$$

and Corollary 3 in Section 1 with $x_1 = x_2 = 1$, $x = 0$ there implies the existence of integers f, g such that

$$K_{f,g} \gg (Q(v_\alpha)Q(v_\beta))^{1/2}p^{-1} \tag{2}$$

since $f \equiv g \equiv 0 \bmod p$ is equivalent to $r_\alpha \equiv r_\beta \equiv 0 \bmod p$. First, suppose α or $\beta \geq 3$; then we have

$$Q(v_1)^2Q(v_2)Q(v_3) = (Q(v_1)Q(v_2))(Q(v_1)Q(v_3)) \ll (Q(v_\alpha)Q(v_\beta))^2 \ll (pK_{f,g})^4.$$

On the other hand, we have

$$Q(v_1)^2Q(v_2)Q(v_3) \asymp Q(v_1)d\mathbf{Z}[v_1, v_2, v_3] \geq p\cdot p^4 = p^5,$$

since elementary divisors of $(B(w_i, w_j))$ over $\mathbf{Z}_p$ are p, p, p^2, p^2. Thus we have $K_{f,g} \gg p^{1/4}$ and then $\min(M + p^{-1}\mathbf{Z}[fw_3 + gw_4]) \gg p^{1/4}$ under the assumption α or $\beta \geq 3$. Next, we suppose that α or $\beta \geq 3$ is impossible; then we have $\{\alpha, \beta\} = \{1,2\}$. By the way of choice of α, β, we have $d_{31} \equiv d_{32} \equiv d_{41} \equiv d_{42} \equiv 0 \bmod p$ and then $s_3 \equiv t_3 \equiv s_4 \equiv t_4 \equiv 0 \bmod p$. Now we can apply Theorem in Section 3 with $r = 2$, $m = 4$, $t_1 = t_2 = 1$, $t_3 = t_4 = 2$, $e = 1$, $S = \begin{pmatrix} S_1^{(2)} & S_2 \\ S_3 & S_4 \end{pmatrix} := (B(v_i, v_j))$, $D_1 = \mathrm{diag}(p, \varepsilon_1 p)$, $D_2 = \mathrm{diag}(p^2, \varepsilon_2 p^2)$ and then we have $S_1 - S_4^{-1}[S_3] \equiv S_3 \equiv 0 \bmod p^2$ and S_4 is p-modular. Therefore $S_1 \equiv 0 \bmod p^2$ holds and it implies $Q(v_1) \equiv Q(v_2) \equiv 0 \bmod p^2$, and by (2) there are integers f, g such that

$$K_{f,g} \geq p \geq p^{1/4}. \qquad \square$$

PROPOSITION 1. *Let M be a positive lattice such that $\mathrm{rank}(M) \geq 4$, $s(M) \subset p\mathbf{Z}$. Then there is a positive number δ 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, $s(M'_p) = \mathbf{Z}_p$ and $\min(M') \geq p^{1/4}$. If $\mathrm{rank}(M) \geq 5$ in addition, M'_p contains a unimodular hyperbolic plane.

Proof. Let a lattice $\hat{M}$ be a lattice such that $[\hat{M} : M]$ is a power of p and $\hat{M}_p$ is $p\mathbf{Z}_p$-maximal. $\min(\hat{M}) \geq p$ is clear. If $\hat{M}_p$ contains a p-modular sublattice of rank ≥ 3, then the assertion follows from Lemma 1 with $\varepsilon = 1/24$ if $p > \delta_{1/24}$. Otherwise, both $\mathrm{ind}(\mathbf{Q}_p M) \leq 1$ and $\mathrm{rank}(M_p) = 4$ hold and then Lemma 2 implies the assertion. $\square$

By virtue of Proposition 1, if $\mathrm{rank}(M) \geq 4$ and $s(M) \subset p\mathbf{Z}$ for a sufficiently large prime number p, then there exists a lattice $M'(\supset M)$ such that $s(M') \subset \mathbf{Z}$ and $\min(M')$ is larger than a given number κ in advance. The assumption $m \geq 4$ is crucial. In the following examples, $\min(M)$ is arbitrarily large but $\min(M') \leq 4 + 5p$ for every $M'(\supset M)$ with $s(M')\mathbf{Z}_p = \mathbf{Z}_p$.

EXAMPLE 1. Let $M = \mathbf{Z}[v_1, v_2]$ be a positive lattice defined by the reduced matrix

$$(B(v_i, v_j)) = \begin{pmatrix} p(1+p^s)^2 & p(1+p^s) \\ p(1+p^s) & p + 4(1+p)p^{2s} \end{pmatrix}$$

where p is an odd prime number and s is a natural number. Then $d(M) = 4(1+p)(1+p^s)^2 p^{2s+1}$ and $M_p \cong \langle p\rangle \perp \langle p^{2s}\rangle$. Moreover, by putting $M' := M + \mathbf{Z}[p^{-t}w]$ for $w \in M$, the condition $s(M'_p) = \mathbf{Z}_p$ compels $M' = \mathbf{Z}[p^{-s}(v_1 - v_2), v_1]$ and then $\min(M') \leq Q(p^{-s}(v_1 - v_2)) = 4 + 5p$.

EXAMPLE 2. Let $M = \mathbf{Z}[v_1, v_2] \perp \mathbf{Z}[v_3]$, where v_1, v_2 are those in Example 1 and $Q(v_3) := ap$, where a is a natural number relatively prime to p satisfying that $a > (1+p^s)^2$ and $-a$ is not a square in $\mathbf{Z}_p$. Then we have $\min(M) = p(1+p^s)^2$ and by putting $M' := M + \mathbf{Z}[p^{-t}w]$ for $w \in M$, the condition $s(M'_p) = \mathbf{Z}_p$ compels $M' = \mathbf{Z}[p^{-s}(v_1 - v_2), v_1, v_3]$ and then $\min(M') \leq Q(p^{-s}(v_1 - v_2)) = 4 + 5p$.

EXAMPLE 3. Let v_1, v_2 and v_3 be as in the previous example. Put $M := \mathbf{Z}[v_1, v_2] \perp \mathbf{Z}[v_3] \perp (\perp_{i=4}^{m-3} \mathbf{Z}[v_i])$ with $Q(v_i) > a(1+p^s)^2$ and put $Q(v_i) \in (\mathbf{Z}_p^\times)^2$ for $i \geq 4$; then if, for a lattice $\tilde{M} \supset M$, $\tilde{M}_p$ is primitively represented by $N_p = \langle 1_m\rangle \perp \langle -1\rangle \perp \langle -1\rangle \perp \langle -\delta\rangle (\delta \in \mathbf{Z}_p^\times \backslash (Z_p^\times)^2)$, then we have $\tilde{M} = \mathbf{Z}[p^{-s}(v_1 - v_2), v_1, v_3, \dots, v_m]$ and $\min(\tilde{M}) \leq 4 + 5p$.

In Example 3, a local extension of M is uniquely determined under the condition that it is primitively represented by N_p. If this is not the case, is there an extension M' with $\min(M)$ being small? If so, we can make a counter-example to the assertion $A_{m,n}$.

LEMMA 3. *Let p be an odd prime and $F_p := \mathbf{Z}/p\mathbf{Z}$. Suppose that V be a quadratic space over F_p with basis $\{z_1, \dots, z_t\}$ and integers $r_1 = 1, r_2, \dots, r_t$ are given. If $Q(V) \neq \{0\}$, then there are integers $x_1 = r_1\ (=1), x_i = r_i, r_i \pm 1 (i > 1)$ satisfying $Q(\sum_{i=1}^t x_i z_i) \neq 0$.*

Proof. We use induction on t. The case of $t = 1$ is clear. Suppose that the assertion is false for $t > 1$. Since the equation

$$Q(\sum_{i=1}^{t} x_i z_i) = x_t^2 Q(z_t) + 2x_t(\sum_{i=1}^{t-1} B(z_t, z_i)x_i) + Q(\sum_{i=1}^{t-1} x_i z_i) = 0,$$

has the three solutions $x_t = r_t, r_t \pm 1$, we have

$$Q(z_t) = 0,\ \sum_{i=1}^{t-1} B(z_t, z_i)x_i = 0,\ Q(\sum_{i=1}^{t-1} x_i z_i) = 0,$$

for $x_1 = 1, x_i = r_i, r_i \pm 1$ for $i = 2, \dots, t-1$. From the induction hypothesis,

$Q(F_p[z_1, \ldots, z_{t-1}]) = 0$ follows. Making use of the middle equality above for $x_t = r_i, r_i + 1$, we have $B(z_t, z_i) = 0$ for $i = 2, \ldots, t-1$ and hence $B(z_t, z_1) = 0$. Thus we have the contradiction $Q(V) = \{0\}$. $\square$

LEMMA 4. *Let $L = \mathbf{Z}_p[w_1, \ldots, w_t]$ be a quadratic lattice over $\mathbf{Z}_p$ such that $(B(w_i, w_j)) = \mathrm{diag}(\varepsilon_1 p^{a_1}, \ldots, \varepsilon_t p^{a_t})$, $(\varepsilon_i \in \mathbf{Z}_p^\times$, $a_1 = 0 \leq a_2 \leq \cdots \leq a_t)$, and assume $a_1 < a_2$ if $p = 2$. Let $\{z_1, \ldots, z_t\}$ be another basis of L and let $r_1 = 1, r_2, \ldots, r_t$ be integers. Then for integers $x_1 = 1$, $x_i = r_i, r_i \pm 1 (i > 1)$, we have $Q(\sum_{i=1}^t x_i z_i) \in \mathbf{Z}_p^\times$.*

Proof. If $p \neq 2$, then we have only to apply Lemma 3 to L/pL. Suppose $p = 2$ and ${}^t(z_1, \ldots, z_t) = B\,{}^t(w_1, \ldots, w_t)$ for some $B \in GL_t(\mathbf{Z}_2)$. By virtue of $\sum_{i=1}^t x_i z_i = (x_1, \ldots, x_t) B\,{}^t(w_1, \ldots, w_t)$, we have only to show that $\sum_{i=1}^t x_i b_{i1} \not\equiv 0 \bmod 2$, which implies $Q(\sum_{i=1}^t x_i z_i) \in \mathbf{Z}_2^\times$. If $\sum_{i=1}^t x_i b_{i1} \equiv 0 \bmod 2$ for $x_1 = 1$, $x_i = r_i, r_i + 1$ $(i > 1)$, we have $b_{i1} \equiv 0 \bmod 2$ for $i \geq 1$, which is the contradiction. $\square$

LEMMA 5. *Let p be a prime number and M a positive lattice of $\mathrm{rank}(M) = m$, $s(M) \subset \mathbf{Z}$. Suppose that*

$$M_p \cong \langle \mathrm{diag}(\varepsilon_1 p^{a_1}, \ldots, \varepsilon_m p^{a_m}) \rangle$$

where $\varepsilon_i \in \mathbf{Z}_p^\times$ and $0 \leq a_1 \leq \cdots \leq a_m$. Divide the set $\{1, \ldots, m\}$ to disjoint subsets S and $T := \{h_1, \ldots, h_{m-r}\}$ $(h_1 < \cdots < h_{m-r}$ and $0 \leq r := |S| < m)$, and suppose $a_{h_1} < a_{h_2}$ if $p = 2$ and let s be a natural number $\leq a_{h_1}/2$. Let $\{w_1, \ldots, w_m\}$ be a basis of M such that $(B(w_i, w_j))$ is sufficiently close to $\mathrm{diag}(\varepsilon_1 p^{a_1}, \ldots, \varepsilon_m p^{a_m})$ in $M_m(\mathbf{Z}_p)$. Let $A = (a_{ij})$ be the transformation matrix defined by (1), and choose integers $k_1 < \cdots < k_{m-r}$ so that the determinant of $(a_{k_i, h_j})_{1 \leq i,j \leq m-r}$ is relatively prime to p. Then there are integers f_i $(i \in T)$ such that for $w = \sum_{i \in T} f_i w_i$ we have

$$\min(M + p^{-s}\mathbf{Z}[w]) \gg (p^{-2s} \prod_{i=1}^{m-r} Q(v_{k_i}))^{1/(m-r)},$$

$$(M + p^{-s}\mathbf{Z}[w])_p \cong (\perp_{i \in S} \langle \varepsilon_i p^{a_i} \rangle) \perp \langle \varepsilon_{h_1} p^{a_{h_1} - 2s} \rangle \perp K_p,$$

for some lattice K_p of $\mathrm{rank}(K_p) = m - r - 1$ and $s(K_p) \subset p^{a_{h_2}}\mathbf{Z}_p$. If $r \leq m/2 - 1$ in addition, then we have $\min(M + \mathbf{Z}[p^{-s}w]) \gg \min(M)^{1/(m-r)}$.

Proof. Let $r_1, \ldots, r_{m-r}$ be integers, and for $B = (a_{k_i h_j})_{1 \leq i,j \leq m-r}$ we define integers f_{h_i} by

$$(f_{h_1},\ldots,f_{h_{m-r}}) \equiv (r_1,\ldots,r_{m-r})^t B^{-1} \bmod p^s.$$

By putting $R_i := \sum_{j\in T} a_{ij} f_j$, we have

$$^t(R_{k_1},\ldots,R_{k_{m-r}}) = B^t(f_{h_1},\ldots,f_{h_{m-r}}) \equiv {}^t(r_1,\ldots,r_{m-r}) \bmod p^s$$

$$\min(M+\mathbf{Z}[p^{-s}w]) \asymp \min(\min(M), \min_{p^s \nmid b} \sum_{i=1}^{m} \lceil bR_i/p^s \rceil^2 Q(v_i))$$

$$\min_{p^s \nmid b} \sum_{i=1}^{m} \lceil bR_i/p^s \rceil^2 Q(v_i) \gg \min_{p^s \nmid b} \sum_{i=1}^{m-r} \lceil br_i/p^s \rceil^2 Q(v_{k_i}).$$

Since $Q(v_{k_1}) \ll \cdots \ll Q(v_{k_{m-r}})$, Corollary 1 in Section 1 yields that there exist integers $r_{m-r}=1, r_{m-r-1},\ldots, r_1$ such that

$$\min_{p^s \nmid b} \sum_{i=1}^{m-r} \lceil br_i/p^s \rceil^2 Q(v_{k_i}) \gg (p^{-2s} \prod_{i=1}^{m-r} Q(v_{k_i}))^{1/(m-r)}.$$

By applying Lemma 4 to $L := \mathbf{Z}_p[w_{h_1},\cdots,w_{h_{m-r}}]$ scaled by $p^{-a_{h_1}}$, and a basis $^t(z_1,\ldots,z_{m-r}) := {}^tB^{-1t}(w_{h_1},\ldots,w_{h_{m-r}})$, there exist integers $r'_{m-r}=1$, $r'_i = r_i$ or $r_i \pm 1 (1 \le i < m-r)$ such that $\operatorname{ord}_p Q(\sum_i r'_i z_i) = a_{h_1}$. Define integer f'_{h_i} by $(f'_{h_1},\cdots,f'_{h_{m-r}}) \equiv (r'_1,\cdots,r'_{m-t})^t B^{-1} \bmod p^s$; then $w' := \sum_i f'_{h_i} w_{h_i} \equiv \sum_i r'_i z_i \bmod p^s L$ and hence $\operatorname{ord}_p Q(w') = a_{h_1}$. Thus we may assume $\operatorname{ord}_p Q(w) = a_{h_1}$. Hence w splits $\mathbf{Z}_p[w_i\ (i\in T)]$, and

$$K_p = \mathbf{Z}_p\left[w_i - \frac{B(w,w_i)}{Q(w)} w \mid i \in T\right]$$

which implies the second assertion. Finally we assume $m \ge 2r+2$; then we have $\prod_{i=1}^{m-r-1} Q(v_{k_i}) \asymp d\mathbf{Z}[v_{k_1},\ldots,v_{k_{m-r-1}}] \ge p^{a_1+\cdots+a_{m-r-1}} \ge p^{a_{m-r-1}} \ge p^{a_{r+1}} \ge p^{a_{h_1}}$ since $m \ge h_{m-r} > \cdots > h_1$ implies $m-r \ge h_{m-r}-r > \cdots > h_1 - r$ and hence $h_1 - r \le 1$. $\square$

Remark. In Lemma 5, the assumption $a_{h_1} < a_{h_2}$ is not satisfied in general. But we can modify it by enlarging as follows: If $a_{h_1} = a_{h_2}$, then for $M' := M + \mathbf{Z}[w_{h_1}/p]$ we have $\min(M') \asymp_p \min(M)$ and $M'_p \cong \langle \operatorname{diag}(\varepsilon_1 p^{a_1},\ldots,\varepsilon_{h_1-1}p^{a_{h_1-1}}, \varepsilon_{h_1}p^{a_{h_1}-2}, \varepsilon_{h_1+1}p^{a_{h_1+1}},\ldots,\varepsilon_m p^{a_m})\rangle \perp K_p$.

When $p=2$, a lattice does not have any orthogonal basis in general, but the following is useful to reduce to a lattice having an orthogonal basis. If $H_2 = \mathbf{Z}_2[w_1, w_2]$ is isometric to $(B(w_i,w_j)) = 2^a\begin{pmatrix}0&1\\1&0\end{pmatrix}$, then

$$H_2 + \mathbf{Z}_2[(w_1+w_2)/2] = \mathbf{Z}_2[(w_1+w_2)/2, (w_1-w_2)/2] \cong \langle \operatorname{diag}(2^{a-1}, -2^{a-1})\rangle.$$

If $(B(w_i, w_j)) = 2^a\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, then

$$H_2 + \mathbf{Z}_2[w_1/2] = \mathbf{Z}_2[w_1/2, w_2 - w_1/2] \cong \langle \mathrm{diag}(2^{a-1}, 3\cdot 2^{a-1})\rangle.$$

LEMMA 6. *Let $0 \le r \le m \le n$ be integers and $M = K_1 \perp K_2$, N be regular quadratic lattices over $\mathbf{Z}_p$ with $\mathrm{rank}(M) = m$, $\mathrm{rank}(K_1) = r$ and $\mathrm{rank}(N) = n$. (If $r = 0$, then we assume $K_1 = 0$) Suppose that there is a quadratic space V such that $\mathbf{Q}_pN \cong \mathbf{Q}_pK_1 \perp V$ and $\mathrm{ind}(V) \ge m - r$, and that M is represented by N. Then there is a constant $c = c(K_1, N)$ such that there is a lattice M' in N isometric to M with $[\mathbf{Q}_pM' \cap N : M'] < c$.*

Proof. Put $S := \{K \subset N \mid K \cong K_1\}$ and let $\{H_1, \dots, H_t\}$ be the set of representatives of $O(N)\backslash S$. Since M is represented by N, there exist an isometry σ from M to N and an integer i $(1 \le i \le t)$ so that $\sigma(K_1) = H_i$. By virtue of $\mathbf{Q}_pH_i \cong \mathbf{Q}_pK_1$, we have $\mathbf{Q}_pH_i^{\perp} \cong V$ and hence $\mathrm{ind}(\mathbf{Q}_pH_i^{\perp}) \ge m - r$. Since K_2 is represented by $H_i^{\perp}$, we can apply Lemma 3 in [2] and therefore there is a constant c_i such that there is a lattice K_2' $(\subset H_i^{\perp})$ satisfying $K_2' \cong K_2$ and $[\mathbf{Q}_pK_2' \cap H_i^{\perp} : K_2'] < c_i$. Now $M' := H_i \perp K_2'$ $(\cong M)$ satisfies

$$\begin{aligned}[\mathbf{Q}_pM' \cap N : M'] &= [\mathbf{Q}_pM' \cap N : \mathbf{Q}_pM' \cap (H_i \perp H_i^{\perp})][\mathbf{Q}_pM' \cap (H_i \perp H_i^{\perp}) : M'] \\ &\le [N : H_i \perp H_i^{\perp}][H_i \perp (\mathbf{Q}_pK_2' \cap H_i^{\perp}) : H_i \perp K_2'] \\ &\le [N : H_i \perp H_i^{\perp}]c_i.\end{aligned}$$

Thus the number $c(K_1, N) := \max_i[N : H_i \perp H_i^{\perp}]c_i$ is what we want. □

PROPOSITION 2. *Let M and N be positive lattices of $\mathrm{rank}(M) = m$ and $\mathrm{rank}(N) = n$ respectively, and p a prime number, and suppose that $n \ge 2m - [m/2] + 3$ and M_p is represented by N_p. Then there is a lattice M' $(\supset M)$ such that $M_q' = M_q$ if $q \ne p$, M_p' is primitively represented by N_p and $\min(M') > c(N_p)\min(M)^{c_p}$, where $c(N_p)$ depends only on N_p and c_p depends only on m.*

Proof. First, we note that if once, for a lattice $\hat{M} \supset M$, an isometry σ from $\hat{M}_p$ to N_p with $[\mathbf{Q}_p\sigma(\hat{M}_p) \cap N_p : \sigma(\hat{M}_p)] < c$ has been constructed, then $\hat{M}$ has an extension M' such that $M_p' = \sigma^{-1}(\mathbf{Q}_p\sigma(\hat{M}_p) \cap N_p)$ is primitively represented by N_p, $M_q' = \hat{M}_q$ for $q \ne p$ and $[M' : \hat{M}] < c$, which yields $\min(M') > c^{-2}\min(\hat{M})$.
Let h_1 be an integer such that N_p contains a $p^{h_1}\mathbf{Z}_p$-maximal lattice.
Let h be an integer and $S(h)$ the set of regular submodules K_p of N_p such that the scale of each Jordan component of K_p contains $p^h\mathbf{Z}_p$. Then there is a finite subset

$X(h)$ of $S(h)$ so that any $L \in S(h)$ is transformed to an element in $X(h)$ by $O(N_p)$. Hence we can define an integer $n(h)\,(> h_1)$ so that for $L \in S(h)$, $L^{\perp}$ in N_p contains a maximal lattice whose norm contains $p^{n(h)}\mathbf{Z}_p$. We note that $n(h)$ depends only on h and N_p.

First, suppose $s(M_p) \subset p^{h_1+2}\mathbf{Z}_p$; then by the iterative application of Lemma 5 and the remark after it for $p = 2$, there is a lattice $\hat{M}(\supset M)$ such that $\min(\hat{M}) \gg_p \min(M)^{c_p}$ and $\hat{M}_p \cong \langle \mathrm{diag}(\varepsilon_1 p^{a_1}, \ldots, \varepsilon_m p^{a_m})\rangle$ with $h_1 \leq a_1 \leq \cdots \leq a_m$ and $a_{[m/2]} \leq h_1 + 1$. Since N_p contains $p^{h_1}\mathbf{Z}_p$-maximal lattice, $\hat{M}_p$ is represented by N_p. We note that for a regular quadratic space V over $\mathbf{Q}_p$, $\dim(V) \geq 2t + 3$ implies $\mathrm{ind}(V) \geq t$. By applying Lemma 6 to $\hat{M}_p = K_1 \perp K_2$ where $K_1 \cong \langle \mathrm{diag}(\varepsilon_1 p^{a_1}, \ldots, \varepsilon_{[m/2]} p^{a_{[m/2]}})\rangle$ and $K_2 \cong \langle \mathrm{diag}(\varepsilon_{[m/2]+1} p^{a_{[m/2]+1}}, \ldots, \varepsilon_m p^{a_m})\rangle$, there is a constant $c(h_1, N_p)$ such that there is an isometry σ from $\hat{M}_p$ to N_p such that $[\mathbf{Q}_p\sigma(\hat{M}_p) \cap N_p : \sigma(\hat{M}_p)] < c(h_1, N_p)$.

Next suppose that $M_p = J_1 \perp J_2$ with $\mathrm{rank}(J_1) = r$ and that the scale of every Jordan component of J_1 contains $p^h\mathbf{Z}_p$ and $s(J_2) \subset p^{h+1}\mathbf{Z}_p$ with an integer $h \leq h_1 + 1$. If $s(J_2) \subset p^{n(h)}\mathbf{Z}_p$ and $r \leq [m/2] - 1$, then by virtue of Lemma 5, there exists a lattice $\hat{M}\ (\supset M)$ such that $\min(\hat{M}) \gg \min(M)^{1/(m-r)}$, and $\hat{M}_p \cong J_1 \perp \langle \varepsilon p^{n(h)+\delta}\rangle \perp K_p$ for $\varepsilon \in \mathbf{Z}_p^{\times}$, $\delta = 0$ or 1 and some lattice K_p of $s(K_p) \subset p^{n(h)}\mathbf{Z}_p$. By virtue of the choice of $n(h)$, $\hat{M}_p$ is represented by N_p. Thus by iterating this, there exists a lattice $\bar{M} \supset M$ such that (i) $\min(\bar{M}) \gg \min(M)^c$ for some positive number c dependent only on m, (ii) $\bar{M}_p = \langle \varepsilon_1 p^{a_1}\rangle \perp \cdots \perp \langle \varepsilon_m p^{a_m}\rangle$ with $a_1 \leq \cdots \leq a_m$ and $a_{i+1} - a_i < c_p(N)$ for some positive number dependent on N_p for $i \leq [m/2] - 1$, and (iii) $\bar{M}_p$ is represented by N_p. Now we can apply Lemma 6 with $r = [m/2]$ because of $n - [m/2] \geq 2(m - [m/2]) + 3$, and complete the proof. $\square$

Proof of Theorem. Let M and N be positive lattices of $\mathrm{rank}(M) = m$ and $\mathrm{rank}(N) = n$ and suppose that M_p is represented by N_p for every prime p. We note that M_p is primitively represented by N_p if and only if M_p/pM_p is represented by N_p/pN_p over $\mathbf{Z}_p/p\mathbf{Z}_p$ when N_p is umimodular and $p > 2$. We assume that $s(N) \subset \mathbf{Z}$ without loss of generality. Let δ be a natural number given in Proposition 1 and we assume that N_p is unimodular if $p > \delta$.

(i) Suppose that there is a prime p such that $s(M_p) \subset p\mathbf{Z}_p$ and $p > \delta$. By enlarging M to M', we may assume that M'_q is primitively represented by N_q if $q \neq p$ and $M'_p = M_p$. If $m \geq 4$, then we can use Proposition 1 and conclude that there is a lattice $\hat{M} \supset M'$ such that $s(\hat{M}_p) = \mathbf{Z}_p$ and $\min(\hat{M}) \geq p^{1/4}$. If $n = 2m$ in addition, the condition $s(\hat{M}_p) = \mathbf{Z}_p$ implies that $\hat{M}_p$ is primitively represented by N_p. (If $n < 2m$, then the property $s(\hat{M}_p) = \mathbf{Z}_p$ does not yield the primitively-

representedness of $\tilde{M}_p$ by N_p.)
(ii) Denote by S the set of primes p such that M_p is not primitively represented by N_p. Excluding the case (i), we assume that the condition $s(M_p) \subset p\mathbf{Z}_p$ yields $p < \delta$ and hence $S \subset \{p \mid p < \delta\}$ by $n = 2m$. If $n \geq 2m - [m/2] + 3 = m + [(m + 1)/2] + 3$, then by iterative use of Proposition 2, there is a lattice $\tilde{M}(\supset M)$ such that $\min(\tilde{M}) > c(N)\min(M)^c$ for some constants $c(N)$, c where $c(N)$ depends on N but c does not depend on M, N.

Remark. Let us examine the above proof in the case of $\operatorname{rank}(N) = 2m - 1$. We assume $m \geq 5$; then at the step (i), we may assume that $\tilde{M}_p$ contains a unimodular hyperbolic plane and hence $\tilde{M}_p$ is primitively represented by N_p. Thus we can clear the case (i). But at the setp (ii), the cardinality of the set S is not less than a constant independent of M. So, after applying Proposition 2 iteratively, $\min(\tilde{M})$ may be small.

REFERENCES

[1] L-K. Hua, Introduction to number theory, Springer-Verlag, 1982.
[2] Y. Kitaoka, Local densities of quadratic forms, in "Advanced Studies in Pure Mathematics, **13** (Investigation in Number Theory)" (1988), 433–460.
[3] ——, Arithmetic of quadratic forms, Cambridge University Press, 1993.
[4] ——, The minimum and the primitive representation of positive definite quadratic forms, Nagoya Math. J., **133** (1994), 127–153.
[5] W. M. Schmidt, Equations over Finite Fields. An elementary Approach, Springer Lecture Notes in Math., vol. 536, Springer-Verlag. 1976.
[6] I. M. Vinogradov, Elements of Number Theory, Dover Publications, 1954.

Graduate School of Polymathematics
Nagoya University
Chikusa-ku, Nagoya 464-01
Japan