ACTA ARITHMETICA
LXXXIX.3 (1999)

Effective version of Tartakowsky's Theorem

by

J. S. Hsia (Columbus, Ohio) and M. I. Icaza (Talca)

Dedicated to the memory of Dennis R. Estes

1. Introduction and notation. In 1929 W. Tartakowsky [T] proved a remarkable result which stated that all forms in a genus of positive definite integral quadratic forms in five or more variables represent the same sufficiently large numbers. Namely

THEOREM 1.1. *Let $f(x) = f(x_1, \dots, x_m)$, $m \geq 5$, be a positive definite integral quadratic form. Let N be a natural number such that N is p-adically represented by $f(x)$ for all prime numbers p. Then there exists a constant C such that if $N \geq C$ the equation $f(x) = N$ is soluble in $\mathbb{Z}$.*

Tartakowsky's work does not lead to any estimate for the size of C. Effectiveness of this result was first addressed by G. L. Watson in 1960 [W]. Watson proved, using a combination of analytic and arithmetic methods, that if N satisfies the conditions in Tartakowsky's Theorem but $f(x) = N$ is not soluble in $\mathbb{Z}$ then $N \ll |d|^{5/(m-4)+1/m}$ if $5 \leq m \leq 9$, and $N \ll |d|$ when $m \geq 10$. Here d denotes the determinant $\det f$.

In Watson's work the implied constants were not *explicitly* given. In fact, the question of estimating them was posed in Kitaoka's book [Ki3] (Problem 2, p. 254), and this seems not to have been addressed before. The aim of this paper is to present an explicit estimate for the size of the constant C in Tartakowsky's Theorem (see Theorem 3.1 and Corollary 3.1), thereby answering the case $n = 1$ of Kitaoka's question. This is done by using purely arithmetic arguments as opposed to Tartakowsky's and Watson's previous work which rely on analytic results.

1991 *Mathematics Subject Classification*: 11E12, 11D85, 11E25, 11E39.

Research of the first author supported in part by NSF DMS9401015 & N.S.A. MDA904-98-1-0031.

Research of the second author supported by Fondecyt 3940002, 1970214 & FONDAP Mat. Aplicadas.

Although the basic approach is to follow the arithmetic proof in [Kn] (see also [HKK]), exploiting the particular case at hand of representing numbers (instead of forms), it still requires substantial effort (for us) to actually bear down the numerous details. For the local integral representations we use O'Meara's results in [OM1], [OM2]. Keeping careful tracks of the detailed estimates occurring at various stages we produce the needed global estimate. Once we have obtained this initial global estimate we go further on refining some of the local arguments involved to improve them (see table (16) below). These new improvements involve rather non-trivial and necessarily tedious arguments. However, they allow us on the one hand to obtain a better value for the exponent of the determinant in Watson's work for $m = 5, 6$ and on the other hand, for those forms whose determinants do not involve primes with too large exponents, our improved results yield still better estimates. As Kitaoka pointed out to us, our main result already can be applied to his Theorem in [Ki2] (see also [Ki3], Problem 2 (C2), p. 254) to obtain for $n = 2$ an exponent of 25 instead of the value 32.2 stated there. Our refinement applied to the case $m = 5$ further improves this value to 21.4.

We took particular care in the proofs in these sections so that the results remain valid over any dyadic unramified prime. It follows then that our main theorem and the refinement arguments also remain valid for any totally real algebraic number field whose absolute discriminant is an odd integer. This is an added advantage of the present approach whereas the analytic component of Watson's does not as easily render this extension without more measurable effort.

In general we follow the terminology and notations from [OM2]. It is convenient to introduce the following notations. Since we are concerned with positive definite spaces we always use p to refer to a finite prime. By $\langle\alpha\rangle$ we mean either a rank one local or a global free lattice (depending on the context) with a basis vector u such that $Q(u) = \alpha$, and by $[\alpha]$ we mean a corresponding local or global space. Similarly, if X is a subset of a lattice then $\langle X\rangle$, resp. $[X]$, denotes the sublattice, resp. subspace generated by X. If α and β are two non-zero scalars, then $\alpha \cong \beta$ means that $\langle\alpha\rangle \cong \langle\beta\rangle$.

Let $\mathcal{O}$ be the ring of integers in an unramified dyadic local field F (i.e., the element 2 is a prime element of $\mathcal{O}$), and let $\mathfrak{A}$ be an ideal of $\mathcal{O}$. Then an $\mathfrak{A}$-modular $\mathcal{O}$-lattice L is *proper* if its norm $\mathfrak{n}L$ equals $\mathfrak{A}$; otherwise, it is *improper*. For convenience, we shall also refer to L as *ν-modular* if the order $\operatorname{ord}_p \mathfrak{A}$ is ν. When $\nu = 0$ it is called *unimodular*.

Recall from [OM2] that $A(\alpha, \beta)$ denotes the inner product matrix of a free binary unimodular lattice $J = \mathcal{O}x + \mathcal{O}y$ where $Q(x) = \alpha$, $Q(y) = \beta$, $B(x, y) = 1$. Denote by $\mathbb{H}$ the hyperbolic plane $A(0, 0)$ and by $\mathbb{A}$ the anisotropic $2\mathcal{O}$-maximal lattice $A(2, 2\varrho)$. If a lattice L has an inner product matrix A, then the scaled lattice L^α has αA for its inner product ma-

trix. A binary unimodular $\mathcal{O}$-lattice is of one of three types: (i) $A(1,0)$ and $A(1,4\varrho)$ are *even*, (ii) $\mathbb{H}$ and $\mathbb{A}$ are *odd*, and (iii) $A(\varepsilon,2\delta)$ is *mixed*.

2. Some lemmas. We give in this section some lemmas which are needed for the proof of the main result. Unless otherwise stated, all lattices are non-degenerate and are defined over $\mathbb{Z}$ and their scales are contained in $\mathbb{Z}$.

LEMMA 2.1. *Let L be a positive definite lattice of rank $l \geq 3$, and q a prime such that L_q is isotropic. There is a positive integer r such that L represents every lattice N which is representable by some member in the spinor genus* $\operatorname{spn} q^r L$. *If $l \geq 4$ then* $\operatorname{spn} q^r L$ *may be replaced by* $\operatorname{gen} q^r L$.

P r o o f. The first part is Lemma 1.2 of [HKK]. The second assertion is because in the extra condition on the dimension of L, every integer representable by the genus is automatically representable by *every* spinor genus. ∎

LEMMA 2.2. *Let M be a positive definite lattice of rank $m \geq 4$ and determinant D. For each prime p, we have*

$$Q(M_p) \supseteq p^{[\operatorname{ord}_p D/(m-3)]}\mathbb{Z}_p \qquad \text{if } p \neq 2,$$
$$Q(M_p) \supseteq 2^{[\operatorname{ord}_2 D/(m-3)]+1}\mathbb{Z}_2 \qquad \text{if } p = 2.$$

P r o o f. If $p \neq 2$ then $M_p \cong \langle p^{s_1}\mu_1\rangle \perp \ldots \perp \langle p^{s_m}\mu_m\rangle$ where $s_1 \leq \ldots \leq s_m$ and μ_j's $\in \mathbb{Z}_p^\times$. By the theory of non-dyadic integral local representations (see [OM1]) we conclude that $Q(\langle p^{s_1}\mu_1\rangle \perp \ldots \perp \langle p^{s_4}\mu_4\rangle)$ contains $p^{[\operatorname{ord}_p D/(m-3)]}\mathbb{Z}_p$.

The case $p = 2$ is quite a bit more complicated and we leave it for Section 5. ∎

LEMMA 2.3. *Let K be a sublattice of L of index t on a space V of dimension greater than one. There is a class number relation $h(K) \leq \lambda(t)h(L)$, where $\lambda(t)$ is the number of sublattices of L of index t.*

P r o o f. Let $K = K_1, \ldots, K_g$ be lattices from the distinct classes in the genus of K. Then $K_j = \Lambda_j K$ for some $\Lambda_j \in J_V$. Set $L_j := \Lambda_j L$. Upon replacing Λ_j by $\sigma\Lambda_j$ for a suitable $\sigma \in P_V = O^+(V)$, we may suppose that $L_i \cong L_j$ if and only if $L_i = L_j$.

We observe that if $[L : K] = t$, then clearly $[L_j : K_j] = t$ for all j. On the other hand, should $K_i \subseteq L_j$ then still $[L_j : K_i] = t$. To see this, note that

$$K_i \subseteq L_j \subseteq L_j^\# \subseteq K_i^\#.$$

We also have

$$K_j \subseteq L_j \subseteq L_j^\# \subseteq K_j^\#.$$

It follows that

$$\det K_j = \det L_j \cdot [L_j : K_j][K_j^{\#} : L_j^{\#}] = \det L_j \cdot t^2$$

and

$$\det K_i = \det L_j \cdot [L_j : K_i][K_i^{\#} : L_j^{\#}] = \det L_j \cdot [L_j : K_i]^2.$$

Since $\det K_j = \det K_i$, the claim follows, and hence also the assertion of the lemma. ∎

LEMMA 2.4. *Let M be an integral $\mathbb{Z}$-lattice, N a sublattice and $K = N^{\perp}$ in M. Then* $\det K$ *divides* $\det M \cdot \det N$.

Proof. This is well known. See Lemma 2.26 of [Ki1]. ∎

LEMMA 2.5. *Let $p \neq 2$ and M_p be a $\mathbb{Z}_p$-lattice of rank $m \geq 5$ and determinant D. Assume the scale $\mathfrak{s}M_p$ equals $\mathbb{Z}_p$. Then*:

(i) *if* $\operatorname{ord}_p D \leq m-2$ *then* $Q(M_p) = \mathbb{Z}_p$;

(ii) *if* $\operatorname{ord}_p D \leq m-4$ *and v is a primitive vector in M_p with* $\alpha_p := \operatorname{ord}_p Q(v) = 0, 1$ *then* $Q(\langle v\rangle^{\perp}) = \mathbb{Z}_p$.

Proof. (i) If $\operatorname{ord}_p D \leq m-3$, then M_p contains a ternary unimodular component so that $Q(M_p) = \mathbb{Z}_p$. If $\operatorname{ord}_p D = m-2$, then $M_p = M_p(0) \perp X$ where $M_p(0)$ denotes the first (unimodular) Jordan component of M_p of rank $m_0 \geq 2$. The assertion is clear if $m_0 \geq 3$. Should $m_0 = 2$ then X is a $p\mathbb{Z}_p$-modular lattice of rank $m-2$ and $Q(X) \supseteq p\mathbb{Z}_p^{\times}$.

(ii) The assertion is clear if $m_0 = \operatorname{rank}(M_p(0)) \geq 5$. So, assume that $\operatorname{ord}_p D = m-4, m_0 = 4$ and $\operatorname{rank}(X) = m-4$. Set $K(v) := \langle v\rangle^{\perp}$ in M_p. For $m \geq 6$, we have $K(v) \supseteq$ (binary unimodular) $\perp$ (binary $p\mathbb{Z}_p$-modular) and then $Q(K(v)) = \mathbb{Z}_p$.

For $m = 5$, the assertion is easy to see if the Witt index of $M_p(0)$ is 2. But, if $M_p(0) \cong A(0,0) \perp \langle 1, -\Delta\rangle$ then $X \cong \langle p\varepsilon\rangle$ for some $\varepsilon \in \mathbb{Z}_p^{\times}$. Here Δ is a non-square unit in the notation of [OM2]. Write $v = u + z$, $u \in M_p(0)$, $z \in X$. If u is a primitive vector then we may assume that $v = u$ by a suitable basis change and then by the hypothesis on $Q(v)$, the conclusion is clear. If u is imprimitive then z must be primitive and so $\alpha_p = \operatorname{ord}_p Q(z) = 1$. A change of basis allows us to assume that $v \in A(0,0)$ and then $K(v) \cong \langle -Q(v)\rangle \perp \langle 1, -\Delta\rangle \perp \langle p\varepsilon\rangle$ and we have the desired conclusion. ∎

LEMMA 2.6. *Let $M_2 = M_2(0) \perp X$, where $M_2(0)$ is an initial (unimodular) Jordan component of a 2-adic lattice M_2. Assume that $\mathfrak{n}M_2(0) = 2\mathbb{Z}_2$. Then*:

(i) *if $M_2(0) \supseteq \mathbb{A}$ and $v \in M_2$ has* $\operatorname{ord}_2(Q(v)) = 1$ *then* $Q(M_2) = Q(\langle v\rangle \perp \langle v\rangle^{\perp})$;

(ii) *if $M_2(0) = \mathbb{H}$ and $\mathfrak{n}X = 2\mathbb{Z}_2$ then the same conclusion as in* (i) *holds*;

(iii) *if* $v_j \in \mathbb{H}$ $(j = 1, 2)$ *and* $\operatorname{ord}_2 Q(v_j) = j$ *then* $Q(\langle v_1\rangle \perp \langle v_1\rangle^{\perp}) \cup Q(\langle v_2\rangle \perp \langle v_2\rangle^{\perp}) = Q(\mathbb{H}) = 2\mathbb{Z}_2$.

P r o o f. (i) Select $\overline{v} \in M_2$ such that $B(v, \overline{v}) = 1$ and $\mathbb{Z}_2 v + \mathbb{Z}_2\overline{v} \cong \mathbb{A}$. This is possible because the orthogonal group $O(M_2)$ acts transitively on the set of vectors whose lengths have order 1. The assertion follows from the fact that $Q(\mathbb{A}) = Q(\langle v\rangle \perp \langle v - Q(v)\overline{v}\rangle)$.

(ii) This follows from the equivalence of $\mathbb{H} \perp \langle 2\varepsilon\rangle$ and $\mathbb{A} \perp \langle 2\varepsilon\Delta\rangle$, for $\varepsilon \in \mathbb{Z}_2^{\times}$ and $\Delta = \det \mathbb{A}$ by Theorem 93.29 of [OM2].

(iii) Let $\{\xi, \eta\}$ be a hyperbolic pair representing $\mathbb{H}$. Since $\operatorname{ord}_2 Q(v_j) = j$, $j = 1, 2$, we see that v_j is primitive in $\mathbb{H}$, and $\langle v_j\rangle \perp \langle v_j\rangle^{\perp}$ is isometric to $2^j A(1, 0)$. Now, $Q(\langle v_1\rangle \perp \langle v_1\rangle^{\perp}) = 2\mathbb{Z}_2^{\times} \cup 8\mathbb{Z}_2$ and $Q(\langle v_2\rangle \perp \langle v_2\rangle^{\perp})$ contains $4\mathbb{Z}_2^{\times}$, yielding the assertion. ∎

3. The main result. Let

$$f(x_1, \dots, x_m) = \sum_{1 \le i \le j \le m} a_{i,j} x_i y_j, \qquad a_{i,j} \in \mathbb{Z},$$

be a positive definite primitive integral quadratic form; i.e., $\gcd(a_{i,j}) = 1$. If f is classic (i.e., $a_{i,j} \in 2\mathbb{Z}$ for $i \ne j$) the associated inner product matrix is certainly a primitive integer matrix. If f is non-classic then the matrix corresponding to $2f$ is primitive. Consider therefore a positive $\mathbb{Z}$-lattice M of rank $m \ge 5$ which is primitive in the sense that its scale $\mathfrak{s}M$ is $\mathbb{Z}$. This implies that at every prime p the initial component $M_p(0)$ of each Jordan decomposition of M_p is unimodular. Let $D = \det M$. We fix a prime q not dividing $2D$ and let $T := \{p \mid 2D : \operatorname{ord}_p D \ge m - 3\} \cup \{q\}$. From Lemma 2.2 we have

$$\begin{aligned} Q(M_p) &\supseteq p^{[\operatorname{ord}_p D/(m-3)]}\mathbb{Z}_p && \text{for } p \ne 2, \\ Q(M_q) &= \mathbb{Z}_q && \text{for } p = q, \\ Q(M_2) &\supseteq 2^{[\operatorname{ord}_2 D/(m-3)]+1}\mathbb{Z}_2 && \text{for } p = 2. \end{aligned}$$

For each $p \in T \setminus \{2, q\}$ select a primitive vector $v(p) \in M_p$ such that $Q(v(p)) \in \mathbb{Z}_p^{\times}$. At q, choose $v(q) \in M_q$ to be one of the four vectors so that $\operatorname{ord}_q Q(v(q)) \le 1$ and $Q(v(q))$ spans $\mathbb{Z}_q^{\times} \cup q\mathbb{Z}_q^{\times}$ mod $\mathbb{Z}_q^{\times 2}$. If $\mathfrak{n}M_2 = \mathbb{Z}_2$ then we may also select $v(2)$ with $Q(v(2)) \in \mathbb{Z}_2^{\times}$. Otherwise, the initial Jordan component $M_2(0)$ of M_2 is improper unimodular. There are two cases to distinguish. First, whenever $M_2(0) \supseteq \mathbb{A}$, we select a vector $v(2) \in M_2$ with $Q(v(2)) = 2$. Lemma 2.6(i) shows that $Q(\langle v(2)\rangle \perp \langle v(2)\rangle^{\perp}) = Q(M_2)$. Lemma 2.6(ii) says this case also includes the set-up where $M_2(0) \cong \mathbb{H}$ and $\mathfrak{n}(M_2(0)^{\perp}) = 2\mathbb{Z}_2$. On the other hand, when $\mathfrak{n}(M_2(0)^{\perp}) \subseteq 4\mathbb{Z}_2$ the isometry class of $M_2(0)$ is uniquely determined by Theorem 93.29 of [OM2]. Then there are two choices for the vector $v(2) := v_j(2) \in \mathbb{H}$ $(j = 1, 2)$ according

to Lemma 2.6(iii). Hence, for $p \in T$ we see that

$$\text{(1)} \qquad \operatorname{ord}_2 Q(v(2)) = \begin{cases} 0 & \text{if } \mathfrak{n}M_2 = \mathbb{Z}_2, \\ 1 & \text{if } M_2(0) \supseteq \mathbb{A}, \\ 1,2 & \text{if } M_2(0) = \mathbb{H},\ \mathfrak{n}(M_2(0)^{\perp}) \subseteq 4\mathbb{Z}_2. \end{cases}$$

Let $p \in T$. By the Chinese Remainder Theorem, select $v \in M$ such that

$$\text{(2)} \quad v \equiv \begin{cases} v(p) \pmod{pM_p} & \text{if } p \neq 2, q, \\ v(q) \pmod{q^2 M_q} & \text{if } p = q, \\ v(2) \pmod{2M_2} & \text{if } p = 2,\ M_2(0) \ncong \mathbb{H}, \\ v_j(2) \pmod{2^j M_2} & \text{if } p = 2,\ M_2(0) \cong \mathbb{H},\ \mathfrak{n}(M_2(0)^{\perp}) \subseteq 4\mathbb{Z}_2. \end{cases}$$

Note that $\operatorname{ord}_p Q(v) = \operatorname{ord}_p Q(v(p))$ for all $p \in T$.

Let $M := \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_m$ be expressed in a Minkowski reduced basis (Chap. XII of [C], §1.3 of [Ki1]). Write $v = \sum b_i e_i$, $b_i \in \mathbb{Z}$. The requirements from (2) on v are such that we can choose v so that

$$\text{(3)} \qquad 0 \leq b_i < 2q^2(\operatorname{Rad} D)$$

for each i, where $\operatorname{Rad} D := \prod_{p|D,\, p\in T} p$. We have

$$Q(v) = \sum_{i,j} B(e_i, e_j) b_i b_j.$$

From reduction theory (Lemma 1.3.3 of [Ki1]), one sees that

$$(B(e_i, e_j)) \leq m \operatorname{diag}(Q(e_1), \ldots, Q(e_m)) \leq m Q(e_m) I_m.$$

Therefore,

$$Q(v) \leq m^2 Q(e_m) \max_i b_i^2.$$

Since $Q(e_m) \leq \Gamma'_m D$, where

$$\text{(4)} \qquad \Gamma'_m := \left(\frac{2}{\pi}\right)^m \left\{\Gamma\left(2 + \frac{m}{2}\right)\right\}^2 \left(\frac{5}{4}\right)^{m-4},$$

it follows that

$$\text{(5)} \qquad Q(v) \leq m^2 \Gamma'_m 2^2 q^4 D(\operatorname{Rad} D)^2.$$

Let $K(v) = \langle v \rangle^{\perp}$ and define for this vector $v \in M$ the sublattice $\widetilde{N}(v) := q^{r(v)} K(v) \perp \langle v \rangle$ where $r(v)$ satisfies the conditions of Lemma 2.1. (Note that at most eight vectors $v \in M$ are used! See also the remark at the end of this section.) We claim that

$$Q(\operatorname{gen} M) = \bigcup_v Q(\operatorname{gen} \widetilde{N}(v)).$$

To see this, let $a \in Q(\operatorname{gen} M)$. If $p \notin T$ then $0 = \operatorname{ord}_p D \leq m - 4$ and $q^{r(v)} K(v)_p = K(v)_p$ and then from Lemma 2.5(ii) we have $Q(K(v)_p) = \mathbb{Z}_p$. If $p \in T \setminus \{2, q\}$ then $Q(M_p) = Q(\widetilde{N}(v)_p)$ by the construction of v close to

$v(p)$. At $p = q$, any element from $\mathbb{Z}_q$ belongs to the square-class of one of the four values $Q(v(q))$ constructed above. At $p = 2$, the claim follows from Lemma 2.6.

Next, we want to show that for each vector v so constructed, one has $Q(\operatorname{gen}\widetilde{N}(v)) \subseteq Q(M)$ apart from finitely many exceptions.

By Lemma 2.4, we have $\operatorname{ord}_p \det K(v) \le \operatorname{ord}_p D + \operatorname{ord}_p Q(v)$ for all p. Applying Lemma 2.2 to $K(v)$ we have for $p \in T$ the following:

$$\begin{aligned} &Q(q^{r(v)}K(v)_p) \supseteq p^{[\operatorname{ord}_p D/(m-4)]}\mathbb{Z}_p, && p \ne 2, q,\\ &Q(q^{r(v)}K(v)_q) = q^{2r}\mathbb{Z}_q, && p = q,\\ &Q(q^{r(v)}K(v)_2) \supseteq 2^{[(2+\operatorname{ord}_2 D)/(m-4)]+1}\mathbb{Z}_2, && p = 2. \end{aligned} \tag{6}$$

For $p \notin T$, $(q^{r(v)}K(v))_p = K(v)_p$ contains at least a ternary unimodular component so that $Q(q^{r(v)}K(v)_p) = \mathbb{Z}_p$.

Since $Q(q^{r(v)}K(v)_p)$ contains an ideal according to Lemma 2.2, each element of $Q(\widetilde{N}(v)_p)$ belongs to a finite number of sets of the form

$$Q(q^{r(v)}K(v)_p) + Q(v)c_p^2, \qquad 0 \ne c_p \in \mathbb{Z}_p.$$

For each p define h_p to be the least integer such that $p^{h_p}\mathbb{Z}_p \subseteq Q(q^{r(v)}K(v)_p)$. It follows from Lemma 2.2 that

$$\begin{cases} h_p = 0 & \text{if } p \notin T,\\ h_p \le [\operatorname{ord}_p D/(m-4)] & \text{if } p \in T \setminus \{2, q\},\\ h_q = 2r & \text{if } p = q,\\ h_2 \le [(2 + \operatorname{ord}_2 D)/(m-4)] + 1 & \text{if } p = 2. \end{cases} \tag{7}$$

Select $x \in \mathbb{Z}$ such that $x \equiv c_p \pmod{p^{h_p}}$, $p \in T$ except when $p = 2$ and $\mathfrak{n}M_2 = \mathbb{Z}_2$ in which case we require that $x \equiv c_2 \pmod{2^{h_2+1}}$. Then

$$Q(v)x^2 < R_m(r, q, D), \tag{8}$$

where

$$R_m(r, q, D) := 2^4 m^2 \Gamma'_m q^{4r+4} D(\operatorname{Rad} D)^2 \prod_{p \in T\setminus\{q\}} p^{2h_p}. \tag{9}$$

Here r is the maximum value of the $r(v)$'s.

Suppose next that $A \in Q(\operatorname{gen} M)$. Then there exists a v such that A belongs to $Q(q^{r(v)}K(v)_p) + Q(v)c_p^2$ for some $0 \ne c_p \in \mathbb{Z}_p$ at each $p \in T$. Suppose further that $A > R_m(r, q, D)$. We have

$$0 < A - Q(v)x^2 = A - Q(v)c_p^2 + Q(v)(c_p^2 - x^2), \tag{10}$$

which belongs to $Q(q^r K(v)_p)$ for $p \in T \setminus \{2, q\}$ by the choice of x and Hensel's lemma.

Consider $p = 2$. Suppose first that $\mathfrak{n}M_2 = \mathbb{Z}_2$. Then $\mathrm{ord}_2(Q(v(2))) = 0$ and $h_2 \le [\mathrm{ord}_2 D/(m-4)]$. If $A - Q(v)c_2^2 \notin 2^{h_2}\mathbb{Z}_2$ then from (9) and $c_2^2 - x^2 = (c_2 - x)(c_2 - x + 2x) \equiv 0 \pmod{2^{h_2+2}}$ when $x \equiv c_2 \pmod{2^{h_2+1}}$, we see that $A - Q(v)x^2$ is represented by $(q^{r(v)}K(v))_2$. A similar argument goes through when $\mathfrak{n}M_2 \subseteq 2\mathbb{Z}_2$, needing only that $x \cong c_2 \pmod{2^{h_2}}$. Therefore, we see that $A - Q(v)x^2$ is always represented by the genus $\mathrm{gen}(q^{r(v)}K(v))$, and hence by $\mathrm{spn}(q^{r(v)}K(v))$ since $m \ge 5$. It follows that $K(v)$ represents $A - Q(v)x^2$ by Lemma 2.1, and A is represented by $K(v) \perp \langle v \rangle \subseteq M$ as long as $A > R_m(r, q, D)$.

Using the notations of $h_p, r, q, \Gamma'_m, R_m(r, q, D)$ explained in this section, our main result is the following:

THEOREM 3.1. *Let M be a positive definite primitive integral quadratic $\mathbb{Z}$-lattice of rank $m \ge 5$ and determinant D, and A a positive integer representable by M_p for every prime p. There is a constant $R_m(r, q, D)$ from* (9) *in the notation of this section such that if $A > R_m(r, q, D)$ then A is represented by M.* ∎

REMARKS. (i) Consider the quantity

$$P(m, D) := (\mathrm{Rad}\, D)^2 \prod_{q \ne p \in T} p^{2h_p}$$

appearing in the definition of $R_m(r, q, D)$. From (7) and the fact that $\mathrm{ord}_p D \ge m - 3$ we have

$$P(m, D) \le 2^{(2m-4)/(m-4)} D^{2/(m-4)+2/(m-3)}. \tag{11}$$

(ii) We may take $r(v)$ to be the number of steps in the q-neighborhood constructions of all the classes in the spinor genus of $K(v)$ from a single vertex. While $r(v) \le h_s(K(v)) - 1$, where $h_s(K(v))$ is the number of classes in the $\mathrm{spn}(K(v))$, in practice $r(v)$ is often significantly smaller than $h_s(K(v))$. Since the rank of $K(v) \ge 4$, any number which is representable by $\mathrm{gen}(K(v))$ is representable by *every* spinor genus. This means that we can use $h_s(K(v))$ to be $h(K(v))/g$, where g is the number of (proper) spinor genera within the genus of $K(v)$, a number which is readily computable in practice. Using the estimate of $Q(v)$ from (5) the index $t = [M : \langle v \rangle \perp K(v)]$ can be estimated, and then Lemma 2.3 provides an estimate for $r(v)$, hence for r in terms of factors only from M. It is unnecessary to give such an explicit r since, as mentioned above, the determination of r in practice can be computed either directly from the graph-neighbor method or from the upper bound $h(K(v))/g$ cited. See the example given at the end of Section 4. In fact, we may take $r = 1$ if q is sufficiently large (see [BH]). But, this latter method, although still effective in principle, involves estimates from density theorems of class field theory which may be regarded as not purely algebraic or arithmetic, in addition to being not very explicit.

(iii) When $M_2(0) \cong \mathbb{H}$ and $\mathfrak{n}(M_2(0)^\perp) \subseteq 4\mathbb{Z}_2$, instead of using the two vectors $v_j(2)$, $j = 1, 2$, one may select a single vector $v(2) \in M_2(0)^\perp$ such that $Q(v(2))\mathbb{Z}_2 = \mathfrak{n}(M_2(0)^\perp)$. (Of course, $\mathrm{ord}_2(Q(v(2)))$ can then exceed 2.) In this situation one needs just four vectors v instead of eight.

(iv) When $\mathrm{ord}_p D \le m - 4$ for all $p \,|\, 2D$, i.e. $T = \{q\}$, then the proof of Theorem 3.1 shows that the constant $R_m(r, q, D) = m^2 \Gamma'_m q^{4r+4} D(\mathrm{Rad}\, D)^2$ may be used.

Using the previous remarks we may state our main theorem in

COROLLARY 3.1. *Let M be a positive definite primitive integral quadratic $\mathbb{Z}$-lattice of rank $m \ge 5$ and determinant D, and A a positive integer representable by M_p for every prime p. Let r, q and Γ'_m be as stated in the previous theorem. Then A is represented by M provided that*

$$A > 4^{(3m-10)/(m-4)} m^2 \Gamma'_m q^{4r+4} D^{1+2/(m-4)+2/(m-3)}. \ \blacksquare$$

Finally we note here that for $m = 5$ our exponent of the determinant in the constant $R_m(r, q, D)$ yields D^4 while Watson gives $D^{5.2}$. For $m = 6$ both Watson's and ours give the value $D^{2.67}$. For larger m, Watson's values are better. We can make some refinements which improve these values. See Section 4. A main point here is that our arithmetic estimate for the constant $R_m(r, q, D)$ can be given *explicitly* while the implied constant in [W] does not. We shall look at an example in the next section.

4. Refining estimates on h_p and an example. In this section even though references are to the rings $\mathbb{Z}_p$ all the local arguments at primes p apply to any local field in which p is either a unit or $p = 2$ is an unramified dyadic prime. In other words, we do not use at all the property that the residue class field at 2 has just two elements, a property which could have simplified some of the proofs below. This is aimed at making the results of this paper applicable to more general number fields (see Appendix). The refined estimates will be useful, especially at the smaller dimensions where our exponents of the determinants of the quadratic forms will be sharper than those of Watson's. Furthermore, for those forms whose determinants do not involve primes with too large an exponent, our improved estimates yield still better estimates. As mentioned in the Introduction, Kitaoka pointed out to us that these improvements, particularly for dimension 5, give the better value of 21.4 instead of 32.2 in his Theorem in [Ki2]. We also note that our theorem by itself improves this value only down to 25. The refinements make it necessary to get into rather technical and non-trivial structure and classification results for lattices over local rings.

Recall that h_p is defined as the smallest integer such that $Q(q^{r(v)} K(v)_p)$ contains the ideal $p^{h_p}\mathbb{Z}_p$, and (7) provides an estimate. Some further im-

provements can be made. We still write $M_p = M_p(0) \perp X$ where $M_p(0)$ is the initial component of a Jordan decomposition of M_p with rank m_0.

(I) Consider first the case when $\operatorname{ord}_p D = m-3$. If $p \neq 2, q$, then by the choice of $v(p)$ and the construction of v in (2) one sees that $Q(\langle v\rangle_p^{\perp}) = \mathbb{Z}_p$ so that we may use $h_p = 0$ instead of $[(m-3)/(m-4)]$ from (7).

Let $p = 2$. The condition $\operatorname{ord}_2 D = m-3$ assures that the initial rank $m_0 \geq 3$. If $m_0 = 3$, then $Q(v(2)) \in \mathbb{Z}_2^{\times}$ and X is a 2-modular component of rank $m-3$. Local theory tells us that $M_2(0) \cong B \perp \langle \varepsilon \rangle$ where $B \cong \mathbb{H}$ or $\mathbb{A}$. We select $v(2) \in M_2(0)$ with $Q(v(2)) = \varepsilon$. By choosing the vector $v \in M$ with $v \equiv v(2) \pmod{2M_2}$ from (2), one sees that $Q(v(2)) \cong Q(v)$ and $\langle v\rangle^{\perp} \cong \langle v(2)\rangle^{\perp}$ so that $Q(q^{r(v)}K(v)_2) = 2\mathbb{Z}_2$. Hence, $h_2 = 1$. In (8) we may select $x \equiv c_2 \pmod 2$ instead of (mod 4). When $m_0 = 4$ we may decompose M_2 such that $M_2(0)$ is isotropic. If $M_2(0)$ is proper then we select $v(2) \in M_2(0)$ so that $Q(\langle v(2)\rangle^{\perp}) = \mathbb{Z}_2$ and hence $h_2 = 0$. Otherwise, $h_2 = 1$. In either case, any choice of x suffices in (8). When $m_0 \geq 5$ the same conclusions as in the $m_0 = 4$ case prevail. Summarizing, for $\operatorname{ord}_p D = m-3$ we have:

$$
\begin{aligned}
&h_p = 0 \quad \text{for any } x,\ p \neq 2,\\
&h_2 \leq 1 \quad \text{for } x \equiv c_2 \pmod 2,\ m_0 = 3,\\
&h_2 = 0 \quad \text{for any } x,\ m_0 \geq 4,\ \mathfrak{n}M_2 = \mathbb{Z}_2,\\
&h_2 = 1 \quad \text{for any } x,\ m_0 \geq 4,\ \mathfrak{n}M_2 = 2\mathbb{Z}_2.
\end{aligned} \tag{12}
$$

(II) Now consider $\operatorname{ord}_p D = m-2$. Let $p \neq 2$. Clearly when $m_0 \geq 4$ we have $h_p = 0$. The same for $m_0 = 3$ since we can select our $v(p) \in M_p$ so that its orthogonal complement contains $\mathbb{H}$. For $m_0 = 2$, X must be a p-modular component of rank $m-2 \geq 3$. We select $v(p) \in X$ with $Q(v(p)) \in p\mathbb{Z}_p^{\times}$. The choice of v in (2) is still valid since such a choice would still have $\langle v\rangle$ splitting M_p. It follows that $Q(K(v)_p) = \mathbb{Z}_p$. Hence, $h_p = 0$ and any choice of x would do in (8).

At $p = 2$, we have $m_0 \geq 2$. Suppose first $m_0 = 2$ and $M_2(0)$ is improper. Then select a vector $v(2) \in M_2(0)$ with $\operatorname{ord}_2 Q(v(2)) = 1$. This means that $\langle v(2)\rangle^{\perp}$ is a proper 2-modular lattice of rank $m-1 \geq 4$ and therefore, $Q(M_2) = Q(\langle v(2)\rangle^{\perp}) = 2\mathbb{Z}_2$ and $h_2 = 1$. If $M_2(0)$ is proper then $Q(v(2)) \in \mathbb{Z}_2^{\times}$. Local theory shows that $\langle v(2)\rangle^{\perp}$ contains an isotropic $(m-2)$-dimensional 2-modular component which may replace X. Hence, $Q(X) = 2\mathbb{Z}_2$ (resp. $4\mathbb{Z}_2$) if X is proper (resp. improper), implying that $h_2 = 1$ (resp. 2). However, even if X is improper we may simply take $x \equiv c_2 \pmod 2$ instead of (mod 4) in (8). This is because the right hand side of (10) is represented by $q^{r(v)}K(v)_2$ since $Q(v)(c_2^2 - x^2) \in 4\mathbb{Z}_2$.

Consider next $m_0 = 3$. Since the rank of X is $m-3$ and $\operatorname{ord}_2 D = m-2$, by the properties of a Jordan decomposition X must contain a

2-modular component, say, $M_2(1)$. If $M_2(1)$ is proper (e.g., when its rank, say, m_1 is odd) then $M_2(0)$ can be assumed to be isotropic by a suitable basis change and then $v(2)$ may be selected so that its orthogonal complement in $M_2(0)$ is $\mathbb{H}$, which gives $h_2 = 1$. On the other hand, if $M_2(1)$ is improper then m_1 is even, and $v(2)$ may be chosen so that $\langle v(2)\rangle^{\perp} \cong$ (binary improper unimodular) $\perp$ (binary improper 2-modular) $\perp \ldots$ Hence, $h_2 = 1$.

Finally, when $m_0 \geq 4$ it is easy to see that $h_2 = 1$ always suffices. Summarizing, for $\operatorname{ord}_p D = m - 2$ we have:

$$
\begin{aligned}
&h_p = 0 \quad \text{for any } x,\ p \neq 2,\\
&h_2 \leq 2 \quad \text{for } x \equiv c_2 \pmod 2,\ M_2(0) \text{ binary proper},\\
&h_2 = 1 \quad \text{for any } x,\ M_2(0) \text{ binary improper},\\
&h_2 = 1 \quad \text{for } x \equiv c_2 \pmod 2,\ m_0 \geq 3.
\end{aligned} \tag{13}
$$

(III) Consider $\operatorname{ord}_p D = m - 1$. Let $p \neq 2$. If $m_0 \geq 4$, then clearly $h_p = 0$. If $m_0 = 3$, one can select the vector $v(p)$ so that its orthogonal complement contains a copy of $\mathbb{H}$, yielding $h_p = 0$. If $m_0 = 2$, then $K(v)_p$ contains a sublattice which represents $p\mathbb{Z}_p$, giving $h_p = 1$. If $m_0 = 1$, then X is p-modular and represents $p\mathbb{Z}_p$, giving $h_p = 1$. So, $h_p = 1$ always suffices.

Let $p = 2$. If $m_0 = 1$, then $\langle v(2)\rangle^{\perp} = X$ is 2-modular of rank $m_1 \geq 4$ so that $h_2 \leq 2$. Here the choice of $x \equiv c_2 \pmod 2$ suffices.

If $m_0 = 2$ then $m_1 = m - 3 \geq 2$ and $m_2 = 1$. Suppose $M_2(0)$ is proper; then $\langle v(2)\rangle^{\perp}$ contains a sublattice of the kind (binary 2-modular) $\perp$ (a proper binary 4-modular) which represents at least $4\mathbb{Z}_2$. It follows that $h_2 \leq 2$. Otherwise, $\operatorname{ord}_2 Q(v(2)) = 1$ and then $\langle v\rangle^{\perp}$ contains at least a proper ternary isotropic 2-modular component so that $Q(\langle v\rangle^{\perp}) \supseteq 2\mathbb{Z}_2$. Hence, $h_2 = 1$.

Let $m_0 = 3$. Then $M_2(0)$ is either isometric to $\langle \varepsilon\rangle \perp \mathbb{A}$ when anisotropic or to $\langle \varepsilon\rangle \perp \mathbb{H}$ when isotropic. If it is isotropic then $h_2 = 1$ by selecting $v(2)$ with $Q(v(2)) = \varepsilon$. Consider the anisotropic case. Whenever $m \geq 6$ we have $m_1 = m - 5$ and $m_2 = 2$. Should $m = 6$, then $\mathfrak{n}X = 2\mathbb{Z}_2$ and a suitable basis change will make $M_2(0)$ isotropic. When $m > 6$, $Q(\langle v(2)\rangle^{\perp}) = 2\mathbb{Z}_2$ and $h_2 = 1$.

The case of $m = 5$ has the worst possible scenario. Here $m_1 = 0$ and $m_2 = 2$. So, $h_2 = 3$ occurs when X is improper 4-modular; otherwise, $h_2 = 2$. We may take $x \equiv c_2 \pmod 4$ in all these subcases.

For $m_0 \geq 4$ we can decompose M_2 so that $M_2(0)$ is isotropic. Selecting $v(2) \in M_2(0)$ so that its orthogonal complement contains a copy of $\mathbb{H}$ implies that $h_2 \leq 1$. Summarizing, for $\operatorname{ord}_2 D = m - 1$ we have:

$$
\begin{aligned}
&h_p \le 1 \quad \text{for } x \equiv c_p \pmod p,\ p \ne 2,\\
&h_2 = 3 \quad \text{for } x \equiv c_2 \pmod 4,\ m = 5,\ m_0 = 3,\ \operatorname{ord}_2 D = 4,\\
&\qquad\qquad M_2(0)^{\perp} \text{ improper},\\
&h_2 \le 2 \quad \text{for } x \equiv c_2 \pmod 4,\ m_0 = 2,\ M_2(0) \text{ proper},\\
&h_2 = 1 \quad \text{for } x \equiv c_2 \pmod 2,\ m_0 = 2,\ M_2(0) \text{ improper},\\
&h_2 \le 1 \quad \text{for } x \equiv c_2 \pmod 4,\ m_0 \ge 3 \text{ otherwise.}
\end{aligned} \tag{14}
$$

Using the values of h_p from (12)–(14) we can refine the estimates for

$$P_m(r, D) \le \prod_{q \ne p \in T} p^{2h_p+2}.$$

The exponent 2 comes from $(\operatorname{Rad} D)^2$ in (5) whereas the exponent $2h_p$ comes from the selection of the scalar x in (8). Let D_p be the p-part of D and $P_m(r, D)_p$ be the p-part of $P_m(r, D)$.

Suppose $\operatorname{ord}_p D = m-3$. By (12), any x is permissible but for one exceptional case. This means that $P_m(r, D)_p$ is just $(\operatorname{Rad} D_p)^2 = p^2$ but for one exceptional case where an extra factor of 2^2 is needed. For $\operatorname{ord}_p D = m-2$ we see from (13) that a factor of 2^4 is needed. Hence, $P_m(r, D)_p \le 2^4(\operatorname{Rad} D_p)^2$. When $\operatorname{ord}_p D = m-1$ formulas from (14) show that $P_m(r, D)_p \le 2^4 p^4$ always suffices. [Actually, the importance of x supercedes those of h_p by virtue of (8) so that a further small improvement can be made using the estimates of x (instead of those of h_p) from (12)–(14).] Finally, for $\operatorname{ord}_p D \ge m$ we use the original estimates (7). Summarizing, we have:

$$P_m(r, D)_p \le \begin{cases} 2^2 D_p^{2/(m-3)} & \text{when } \operatorname{ord}_p D = m-3,\\ 2^4 D_p^{2/(m-2)} & \text{when } \operatorname{ord}_p D = m-2,\\ 2^4 D_p^{4/(m-1)} & \text{when } \operatorname{ord}_p D = m-1,\\ 2^{4/(m-4)} D_p^{2/(m-4)+2/m} & \text{when } \operatorname{ord}_p D \ge m. \end{cases} \tag{15}$$

The powers of 2 only enter when dealing with $P_m(r, D)_2$. These refinements improve the estimates for the exponents of D in the constant $R_m(r, q, D)$, especially, when $\operatorname{ord}_p D \le m-1$ for $p \mid D$; namely, we have the table:

(16)

m	any D	$\operatorname{ord}_p D \le m-3$	$\operatorname{ord}_p D \le m-2$	$\operatorname{ord}_p D \le m-1$	Watson
5	3.4	2	2	2	5.2
6	2.34	1.67	1.67	1.8	2.67
7	1.953	1.5	1.5	1.67	1.81
8	1.75	1.4	1.4	1.572	1.375
9	1.623	1.34	1.34	1.5	1.112

Since the local analysis is treated in a manner which remains valid for the ring of integers of any local field in which the element 2 is either a unit

or a prime, the general number field case (whose absolute discriminant is an odd integer) can be treated similarly.

Let us look at an explicit example. This example is selected merely to illustrate that the method discussed here is effective and that our refinements do imply a substantial improvement in the exponent of the determinant. It is a "simplest example" in the following sense. From the quaternary tables ([N], p. 23) pick the smallest genus ($D = 24$) with class number exceeding 1. This gives the forms

$$f = X^2 + Y^2 + Z^2 + 2W^2 + XY,$$
$$g = X^2 + Y^2 + Z^2 + 3W^2 + XY + XZ.$$

Let the integral lattice associated with $2f$ be F and set $M := F \perp \langle 1\rangle$. Write $M = \langle e_1, e_2\rangle \perp \langle e_3\rangle \perp \langle e_4\rangle \perp \langle e_5\rangle$ where $Q(e_1) = Q(e_2) = Q(e_3) = 2$, $Q(e_4) = 4$, $Q(e_5) = 1$, $B(e_1, e_2) = 1$. Let $T = \{2, 5\}$. Here $q = 5$. Define the following vectors of M : $v_1 := e_5$, $v_2 := e_3$, $v_3 := e_4+e_5$, $v_4 := e_3+e_4+2e_5$. If $K(v_i) := \langle v_i\rangle^{\perp}$ and $\widetilde{N}(v_i) := 5^{r(v_i)}K(v_i) \perp \langle v_i\rangle$, one easily sees the following holds:

$$Q(\operatorname{gen} M) = \bigcup_{v_i} Q(\operatorname{gen} \widetilde{N}(v_i)),$$

$$\begin{aligned}
&K(v_1) = \langle e_1, e_2\rangle \perp \langle e_3\rangle \perp \langle e_4\rangle, && \det(K(v_1)) = 24, && h = 2,\\
&K(v_2) = \langle e_1, e_2\rangle \perp \langle e_4\rangle \perp \langle e_5\rangle, && \det(K(v_2)) = 12, && h = 1,\\
&K(v_3) = \langle e_1, e_2\rangle \perp \langle e_3\rangle \perp \langle e_4 - e_5\rangle, && \det(K(v_3)) = 120, && h = 3,\\
&K(v_4) = \langle e_1, e_2\rangle \perp \langle e_3 - e_5, e_4 - 2e_5\rangle, && \det(K(v_4)) = 60, && h = 4.
\end{aligned} \tag{17}$$

The last column in (17) gives the class number of the lattice. The first two values can be read off directly from [N], and so is the third value after scaling the lattice by $1/2$. The fourth one is out of the range of these tables; we owe it to Gordon Nipp who communicated to us its value and the class number $h(M) = 4$. (The latter value does not play a direct role here.) Hence, we have $r := \max_{v_i} r(v_i) = \max_{v_i} h(K(v_i)) - 1 = 3$.

According to (9) and (15) we have

$$R_5(3, 5, 24) = 2^4 \cdot 5^2 \cdot \Gamma_5' \cdot 5^{16} \cdot 24 \cdot P_5(5, 24)_2 = 2^{11} \cdot 3 \cdot 5^{18} \cdot \Gamma_5',$$

and $\Gamma_5' \approx 17.6847$. So, $R_5(3, 5, 24) \approx 7.33 \cdot 10^{18}$.

On the other hand, from the proof of the main theorem, one sees that the constant $R_m(r, q, D)$ in (8) is built from two factors: sizes of $Q(v)$ and of the scalar x. The estimate in (5) is a general estimate which does not exploit the particular nature of the approximating vector v. In practice, this feature can be improved. For instance, in the present example, $Q(v_i) \le 10$ for $1 \le i \le 4$. As for x, we have $h_2 = 1$ from (13). Since $h_5 = 2r = 6$, we

have $x \le 2 \cdot 5^6$ and so in (8) we have $Q(v)x^2 \le 10 \cdot 2^2 \cdot 5^{12} = 9.7656 \cdot 10^9$ which is clearly a more preferable bound.

5. Completion of proof of Lemma 2.2. The purpose here is to give a proof for the second part of Lemma 2.2 in a slightly more general setting. Throughout below we shall assume $\mathcal{O}$ is the ring of integers in a local field F in which 2 is a prime element. We need the following extra notation.

Let M be an integral $\mathcal{O}$-lattice (i.e., $\mathfrak{s}M \subseteq \mathcal{O}$) and $\operatorname{rank} M = m \ge 5$. Suppose $M = M_1 \perp \ldots \perp M_t$ is a Jordan splitting of M with $m_j := \operatorname{rank} M_j$ and $\sigma_j := \operatorname{ord}_2(\mathfrak{s}M_j)$. We write $M \sim (s_1, s_2, \ldots, s_m)$ where $s_1 = s_2 = \ldots = s_{m_1} = \sigma_1, \ldots, s_{m_{t-1}+1} = \ldots = s_{m_{t-1}+m_t} = s_m = \sigma_t$. If a Jordan component M_j is proper then we decompose M_j into an orthogonal basis. Otherwise, M_j is an orthogonal sum of binary improper σ_j-modular sublattices. Let $\widetilde{M}$ be either a 4-dimensional or a 5-dimensional sublattice of M appearing in the initial components of a Jordan decomposition of M. Since 2 is a prime the norm ideals of a Jordan splitting of M are invariants. While $\widetilde{M}$ depends on the choice of the Jordan decomposition, its rank is uniquely determined. Note that $\operatorname{rank} \widetilde{M} = 5$ occurs only when (s_4, s_5) is an improper binary modular lattice. Hence, $\widetilde{M}$ is either $\sim (s_1, \ldots, s_4)$ or $\sim (s_1, \ldots, s_5)$. If $\operatorname{rank} \widetilde{M} = 5$ then the last Jordan component of $\widetilde{M}$ is improper and is either (s_4, s_5) or (s_2, s_3, s_4, s_5).

We now assume that M is an integral $\mathcal{O}$-lattice with $\mathfrak{s}M = \mathcal{O}$. Then $\widetilde{M}$ is either a 4- or 5-dimensional sublattice of M. Here $\sigma_1 = 0$.

Suppose first that $\operatorname{rank} \widetilde{M} = 5$. Since

$$s_4 \le \left[\frac{s_4 + \ldots + s_m}{m-3}\right] \le \left[\frac{\operatorname{ord}_2 D}{m-3}\right],$$

it suffices to prove that $Q(\widetilde{M}) \supseteq 2^{s_4+1}\mathcal{O}$. Now (s_4, s_5) is an improper binary modular component which is either $2^\alpha \mathbb{H}$ or $2^\alpha \mathbb{A}$ where $\alpha = s_4$. In the former case, we have $Q((s_4, s_5)) \supseteq 2^{\alpha+1}\mathcal{O}$. If $s_2 = \ldots = s_5$ then $(s_2, s_3, s_4, s_5) \sim 2^{s_2} \cdot (\mathbb{H} \perp \ldots)$. Therefore, we consider the case where $s_3 < s_4$ and $(s_4, s_5) \cong 2^{s_4}\mathbb{A}$.

Let $L :\sim (s_1, s_2, s_3)$. If L represents $2^{s_4+1}\varepsilon$ for some $\varepsilon \in \mathcal{O}^\times$ then a suitable basis change for $\widetilde{M}$ will convert (s_4, s_5) into $2^{s_4}\mathbb{H}$. We have three cases.

(1) Suppose $s_1 < s_2 < s_3$. If $s_1 \equiv s_2 \equiv s_3 \pmod 2$ then (s_1, s_2, s_3) contains a 3-dimensional 2^{s_3}-modular lattice which surely represents an element from $2^{s_4+1}\mathcal{O}^\times$. If exactly two such s_i have the same order parity then some s_j has the same order parity as $s_4 + 1$ in which case $(s_j, s_4, s_5) \supset 2^{s_4}\mathbb{H}$.

(2) Suppose $s_1 < s_2 = s_3$, $s_1 \not\equiv s_4 + 1 \pmod 2$ and $s_2 \equiv s_4 + 1 \pmod 2$. If (s_2, s_3) is proper then it represents an element from $2^{s_4+1}\mathcal{O}^\times$. If on

the other hand $(s_2, s_3) \approx 2^{s_2}\mathbb{A}$ then $(s_2, s_3, s_4, s_5) \supseteq 2^{s_4-1}\mathbb{A} \perp 2^{s_4}\mathbb{A}$. But $Q(2^{s_4-1}\mathbb{A} \perp 2^{s_4}\mathbb{A}) = 2^{s_4}\mathcal{O}$.

(3) Finally, the case of $s_1 = s_2 < s_3$, $s_3 \not\equiv s_4 + 1 \pmod 2$ and $s_1 = s_2 \equiv s_4 + 1 \pmod 2$ goes through as case (2).

Consider next the case of rank $\widetilde{M} = 4$. We separate into two subcases depending on $\widetilde{M}$ being (I) diagonalizable or (II) non-diagonalizable. We shall show that $Q(\widetilde{M})$ contains $2^{s_4}\mathcal{O}$ in subcase (I) and that it contains $2^{s_4+1}\mathcal{O}$ in subcase (II), which is sufficient for our purpose.

Consider now (I). If $\widetilde{M}$ is unimodular, then $s_4 = \sigma_1 = 0$. An examination of Table II of [OM1] shows that $\widetilde{M}$ represents $2\mathcal{O} = 2^{s_4+1}\mathcal{O}$. If $\widetilde{M}$ contains a 3-dimensional Jordan component, then either $\widetilde{M} \sim (0, 0, 0, s_4)$ or $\sim (0, \sigma_2, \sigma_2, \sigma_2)$. In the former case, $\widetilde{M}$ contains a quaternary 2^{s_4}-modular sublattice when s_4 is even, and it contains a ternary isotropic 2^{s_4-1}-modular sublattice by a suitable change of basis. In either situation, the assertion of (I) holds. Next, in the latter case, $\sigma_2 = s_4$. Here $\widetilde{M}$ contains a quaternary 2^{s_4}-modular sublattice when s_4 is even, and it contains (after a suitable basis change) a ternary isotropic 2^{s_4}-modular sublattice when s_4 is odd, and again we see that the assertion of (I) holds. A similar argument shows the same when at least three of the s_i's $(i = 1, 2, 3, 4)$ have the same order parity.

Therefore, without loss of generality, we may assume that $\widetilde{M}$ contains a full sublattice $J \cong 2^{\beta-1} \cdot \langle \varepsilon_1, \varepsilon_2 \rangle \perp 2^{\beta} \cdot \langle \varepsilon_3, \varepsilon_4 \rangle$. If J is anisotropic then $Q(J) = 2^{\beta-1}\mathcal{O} \supseteq 2^{s_4-1}\mathcal{O}$. So, we take J to be isotropic and consider the various possibilities of $\langle \varepsilon_3, \varepsilon_4 \rangle$.

(a) First, let $\langle \varepsilon_3, \varepsilon_4 \rangle \cong A(1, 0)$. One sees that $Q(J) = 2^{\beta-1}\mathcal{O} \supseteq 2^{s_4-1}\mathcal{O}$ when $\langle \varepsilon_1, \varepsilon_2 \rangle$ is not of the mixed type. Otherwise, J contains a ternary proper isotropic $2^{\beta}\mathcal{O} \supseteq s^{s_4}\mathcal{O}$.

(b) Let $\langle \varepsilon_3, \varepsilon_4 \rangle = A(1, 4\varrho)$. The same conclusion as (a) prevails.

(c) Let $\langle \varepsilon_3, \varepsilon_4 \rangle$ be mixed, say, isometric to $A(\zeta, 2\eta)$. The following claim can be shown by using [OM1]:

Claim. *Let N be isometric to either $A(1, 0) \perp 2 \cdot A(\varepsilon, 2\delta)$ or $A(1, 4\varrho) \perp 2 \cdot A(\varepsilon, 2\delta)$. Then $Q(N) = \mathcal{O}$.*

Returning to (c), in view of the claim we now need only consider the subcase where $\langle \varepsilon_1, \varepsilon_2 \rangle$ is also of the mixed type. So, $J \cong 2^{\beta-1}A(\gamma, 2\delta) \perp 2^{\beta}A(\zeta, 2\eta)$, which contains a proper quaternary 2^{β}-modular sublattice. Hence, $Q(J) \supseteq 2^{\beta}\mathcal{O} \supseteq 2^{s_4}\mathcal{O}$. This completes the diagonal case of (I).

Consider the case (II) of a non-diagonalizable $\widetilde{M}$. In view of what was proved above, we may restrict ourselves to $\widetilde{M} \cong 2^{\alpha_1}\mathbb{A} \perp 2^{\alpha_2}\langle \mu_2 \rangle \perp 2^{\alpha_3}\langle \mu_3 \rangle$, where $\max\{\alpha_1, \alpha_2, \alpha_3\} = s_4$.

Suppose that $\alpha_2 \equiv \alpha_3 \pmod 2$ and, say, $\alpha_2 \le \alpha_3$. Then $\widetilde{M} \supseteq 2^{\alpha_1}\mathbb{A} \perp 2^{\alpha_3}\langle \mu_2, \mu_3\rangle$. If $\alpha_1 \equiv \alpha_3 \pmod 2$ then $\widetilde{M}$ contains $2^{s_4}(\mathbb{A} \perp \langle \mu_2, \mu_3\rangle)$, which is a proper 2^{s_4}-modular lattice. Therefore, by part (I) it represents all of $2^{s_4}\mathcal{O}$.

Now, let $\alpha_1 \not\equiv \alpha_3 \pmod 2$. One sees that if $\alpha_1 > \alpha_3$ then $\alpha_1 = s_4$ and $\widetilde{M} \supseteq 2^{s_4}(\mathbb{A} \perp 2\langle \mu_2, \mu_3\rangle) \cong 2^{s_4}(\mathbb{H} \perp \ldots)$. And if $\alpha_1 < \alpha_3$, then $\alpha_3 = s_4$ and $\widetilde{M} \supseteq 2^{s_4-1}(\mathbb{A} \perp 2\langle \mu_2, \mu_3\rangle) \cong 2^{s_4-1}(\mathbb{H} \perp \ldots)$. In any case, assertion (II) holds.

Finally, consider the case where $\alpha_2 \not\equiv \alpha_3$. We can assume that $\alpha_2 \equiv \alpha_1 \pmod 2$. Then $\widetilde{M} \supseteq 2^{\alpha}(\mathbb{A} \perp \langle \mu_2\rangle) \perp 2^{\alpha_3}\langle \mu_3\rangle$ where $\alpha = \max\{\alpha_1, \alpha_2\}$. If $\alpha > \alpha_3$, then $\widetilde{M}$ contains $2^{\alpha-1}(\langle \mu_3\rangle \perp 2(\mathbb{A} \perp \langle \mu_2\rangle)) \cong 2^{\alpha-1}(\langle \mu_3'\rangle \perp 2(\mathbb{H} \perp \langle \mu_2\rangle))$, yielding $Q(\widetilde{M}) \supseteq 2^{\alpha+1}\mathcal{O} = 2^{s_4+1}\mathcal{O}$. A similar argument goes through for $\alpha < \alpha_3$. This proves assertion (II).

Summarizing, we have proven the following:

PROPOSITION 5.1. *Let F be a local field in which 2 is a prime element, $\mathcal{O}$ its ring of integers, and M an $\mathcal{O}$-lattice of rank $m \ge 4$. If $M \sim (s_1, \ldots, s_m)$ then $Q(M)$ contains $2^{s_4+1}\mathcal{O}$. Furthermore, if $\widetilde{M}$ is a quaternary diagonalizable sublattice, then $Q(M) \supseteq 2^{s_4}\mathcal{O}$.* ∎

6. Appendix: The number field case. In order to study the number field version of the main result in Section 3, we first make some observations. With the obvious changes, Lemmas 2.1 and 2.3 follow immediately. Lemma 2.2 for non-dyadic local fields goes through with the same proof; the unramified dyadic case follows from Proposition 5.1. Lemma 2.4 for number fields F holds by replacing det with $N_{F/\mathbb{Q}}\,\mathrm{vol}$. Lemmas 2.5 and 2.6 remain valid for non-dyadic and unramified dyadic local fields respectively. When passing from the classical case to number fields, we need to replace Minkowski reduction with Humbert reduction. Also, we make use of the fact that any integral lattice defined over a number field is sandwiched between two free lattices with indices bounded by constants depending only on the field.

Throughout this section F will be a totally real number field in which 2 does not ramify, $[F : \mathbb{Q}] = l$, $\mathcal{O}$ the ring of integers in F, and $\mathfrak{d}_F$ the absolute discriminant of F. Let $\Sigma := \{\sigma_i\}_{i=1}^{l}$ be the set of all real embeddings of F into $\mathbb{R}$, $\{\varepsilon_i\}_{i=1}^{l-1}$ a system of fundamental units of F, and Ω the set of all integral bases $\underline{\omega} = \{\omega_i\}$ of F. We define

$$\varrho := \prod_{i=1}^{l-1} \max_{\sigma\in\Sigma} |\sigma(\varepsilon_i^2)| \tag{18}$$

and

$$\beta := \min_{\underline{\omega}\in\Omega} \max_{\substack{1\le i\le l\\ \sigma\in\Sigma}} |\sigma(\omega_i)|. \tag{19}$$

Let c_1, c_3 be two of the reduction constants defined in [Hu], p. 53. We have the following number field version:

THEOREM 6.1. *Let M be a primitive positive definite integral $\mathcal{O}$-lattice of rank $m \ge 5$ and $A \in \mathcal{O}$ a totally positive integer representable by $M_{\mathfrak{p}}$ at all $\mathfrak{p}$. There is a constant $N_m(r, q, \operatorname{vol} M, F)$ from (25) in the notation of this section such that if $N_{F/\mathbb{Q}}(A) > \varrho^l N_m(r, q, \operatorname{vol} M, F)$ then M represents A.*

P r o o f. The proof is similar to the classical case. We make the following adaptations.

The primes $p, q, 2$ are replaced by $\mathfrak{p}, \mathfrak{q}, \mathfrak{p}_2$ where $\mathfrak{p}_2$ is a generic (dyadic) prime above 2. Next, $T = \{\mathfrak{p} : \mathfrak{p} \mid 2 \operatorname{vol} M, \operatorname{ord}_{\mathfrak{p}}(\operatorname{vol} M) \ge m-3\} \cup \{\mathfrak{q}\}$. The constructions of the local vectors $v(\mathfrak{p})$ and $v(\mathfrak{p}_2)$ are as before and in formulas (1), (2) we only need to substitute $\mathbb{Z}_2$ by the corresponding local dyadic rings $\mathcal{O}_{\mathfrak{p}_2}$.

Let $L \subseteq M$ be a free lattice with $[M : L] = t \le \lambda_F$, where λ_F is a constant depending only on the field F (one may take $\lambda_F = \mathfrak{d}_F^{1/2} l!/l^l$). Suppose $\{e_i\}_{i=1}^m$ is a Humbert reduced basis for the lattice L. Then $tv = \sum_{i=1}^m b_i e_i$ with $b_i \in \mathcal{O}$. By classical reduction theory, we have, for each $\sigma \in \Sigma$,

$$Q(tv)^\sigma < (b_j^\sigma)' m \operatorname{diag}(Q(e_1), \dots, Q(e_m))^\sigma (b_j^\sigma)$$

and also

$$\operatorname{diag}(Q(e_1), \dots, Q(e_m))^\sigma \le c_1 Q(e_m)^\sigma I_m,$$

where c_1 (depending only on F) is one of the Humbert reduction constants. Formula (3) is replaced by

$$Q(tv)^\sigma < m^2 c_1\, Q(e_m)^\sigma (\max_j b_j^\sigma)^2. \tag{20}$$

Now, b_j is chosen modulo $2\mathfrak{q}^2 \prod_{\mathfrak{p}\mid \operatorname{vol} M} \mathfrak{p}$. Since $\{\sum a_i\omega_i : a_i \in \mathbb{Z},\ 0 \le a_i < p\}$ contains a full set of representatives for $\mathcal{O}/\prod_{\mathfrak{p}\mid p} \mathfrak{p}$, by the definition of β in (19) we have

$$0 \le (b_j^\sigma)^2 < 2^2 \beta^2 q^4 \prod_{\substack{\mathfrak{p}\cap\mathbb{Z}=(p)\\ \mathfrak{p}\mid \operatorname{vol} M}} p^2. \tag{21}$$

From Humbert reduction there is a constant c_3 depending only on the base field F such that

$$N_{F/\mathbb{Q}}(Q(e_m)) \le c_3^l N_{F/\mathbb{Q}}(\det L) \le c_3^l t^2 N_{F/\mathbb{Q}}(\operatorname{vol} M). \tag{22}$$

Since we may take $t = [\lambda_F]$, putting $\gamma := (2^2 c_1 c_3 \beta^2 m^2 [\mathfrak{d}_F^{1/2} l!/l^l]^{2(1-l)/l})^l$, inequality (5) becomes

$$N_{F/\mathbb{Q}}(Q(v)) \le \gamma q^{4l} N_{F/\mathbb{Q}}(\operatorname{vol} M) \prod_{\substack{\mathfrak{p}\cap\mathbb{Z}=(p)\\ \mathfrak{q}\neq\mathfrak{p}\in T}} p^{2l}. \tag{23}$$

The discussions leading to (6) and (7) remain valid needing only to be replaced by their natural number-theoretic assertions; in particular, (6) and (7) have their $\mathfrak{p}, \mathfrak{q}, \mathfrak{p}_2$ analogs.

Let

$$h_p := \max_{\mathfrak{p}|p} h_{\mathfrak{p}} = \max_{\mathfrak{p}|p} \left[\frac{\operatorname{ord}_{\mathfrak{p}}(\operatorname{vol} M)}{m-4}\right].$$

We select the integer $x \in \mathcal{O}$ so that $x \equiv c_{\mathfrak{p}} \pmod{\mathfrak{p}^{h_p}}$, $\mathfrak{p} \in T$, $\mathfrak{p} \,|\, p$, and $x \equiv c_{\mathfrak{p}_2} \pmod{2^{h_2+1}}$ in the exceptional cases. If we let T_0 be the set of primes of $\mathbb{Q}$ lying below T, then in place of (8) and (9) we have

$$N_{F/\mathbb{Q}}(Q(v)x^2) < N_m(r, q, \operatorname{vol} M, F) \tag{24}$$

where

$$N_m(r, q, \operatorname{vol} M, F) := \gamma q^{4l+4r} N_{F/\mathbb{Q}}(\operatorname{vol} M) \prod_{p\in T_0\setminus q} p^{2l+2h_p}. \tag{25}$$

Again r is the maximal value of the $r(v)$'s.

If $N_{F/\mathbb{Q}}(A) > \varrho^l N_m(r, q, \operatorname{vol} M, F) > \varrho^l N_{F/\mathbb{Q}}(Q(v)x^2)$ then by Proposition 3.4 of [BI] there exists a unit $\varepsilon \in \mathcal{O}^\times$ such that $(\varepsilon^2 A)^\sigma > (Q(v)x^2)^\sigma$ for all $\sigma \in \Sigma$, i.e. $\varepsilon^2 A - Q(v)x^2 \in \mathcal{O}$ is a totally positive integer. Then the discussion from (10) to the end of the proof of Theorem 3.1 shows that $\varepsilon^2 A$, and hence also A itself, is represented by $K(v) \perp \langle v\rangle \subseteq M$. ∎

References

[BI] R. Baeza and M. I. Icaza, *Decomposition of positive definite integral quadratic forms as sums of positive definite quadratic forms*, in: Proc. Sympos. Pure Math. 58, Amer. Math. Soc., 1995, 63–72.

[BH] J. W. Benham and J. S. Hsia, *Spinor equivalence of quadratic forms*, J. Number Theory 17 (1983), 337–342.

[C] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, 1978.

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

[Hu] P. Humbert, *Réduction de formes quadratiques dans un corps algébrique fini*, Comment. Math. Helv. 23 (1949), 50–63.

[Ki1] Y. Kitaoka, *Siegel Modular Forms and Representation by Quadratic Forms*, Tata Lecture Notes, Springer, 1986.

[Ki2] —, *A note on representation of positive definite binary quadratic forms by positive definite quadratic forms in 6 variables*, Acta Arith. 54 (1990), 317–322.

[Ki3] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge Univ. Press, 1993.
[Kn] M. Kneser, *Quadratische Formen*, Göttingen Lecture Notes, 1973/74.
[N] G. L. Nipp, *Quaternary Quadratic Forms—Computer Generated Tables*, Springer, 1991.
[OM1] O. T. O'Meara, *The integral representations of quadratic forms over local rings*, Amer. J. Math. 86 (1958), 843–878.
[OM2] —, *Introduction to Quadratic Forms*, Springer, 1973.
[T] W. Tartakowsky, *Die Gesamtheit der Zahlen, die durch eine positive quadratische Form $F(x_1,\dots,x_s)$ $(s \geq 4)$ darstellbar sind*, Izv. Akad. Nauk SSSR 7 (1929), 111–122, 165–195.
[W] G. L. Watson, *Quadratic diophantine equations*, Philos. Trans. Roy. Soc. London Ser. A 253 (1960), 227–254.

Department of Mathematics
Ohio State University
231 W. 18th Avenue
Columbus, Ohio 43210-1174
U.S.A.
E-mail: jshsia@math.ohio-state.edu

Instituto de Matematica y Fisica
Universidad de Talca
Avenida Lircay s/n
Talca
Chile
E-mail: icazap@inst-mat.utalca.cl

Received on 11.8.1998 (3441)