JOURNAL OF NUMBER THEORY 17, 337–342 (1983)

Spinor Equivalence of Quadratic Forms

J. W. BENHAM* AND J. S. HSIA†

Department of Mathematics, The Ohio State University, 231 West 18th Avenue, Columbus, Ohio 43210

Communicated by N. Ankeny

Received December 15, 1981

THEOREM: Let f be an integral quadratic form in three or more variables and g any form in the genus of f. There exist an effectively determinable prime p and a form g', belonging to the proper spinor genus of g, such that g' is a p-neighbor of f in the graph of f. Using this, an alternative decision procedure for the spinor equivalence of quadratic forms is given.

It is well known that a simple procedure can be constructed for deciding whether two definite integral quadratic forms are equivalent. On the other hand, no such procedure was known for indefinite forms until quite recently. This latter difficulty is due to the fact that the group of integral automorphs of such forms generally has infinite order. Siegel [8] (see also [2]) gave an algorithm which used the geometry of quadratic forms; e.g., Hermite majorants, Siegel domains, etc. But, the various constants involved that arise from reduction theory can be rather large so as to render this approach somewhat awkward to apply in practice. However, Cassels [2, 3] has succeeded with a clever decision procedure that applies to forms in three or more variables and which is completely different from Siegel's algorithm. His method is based on the theory of spinor genus. We shall present here still another alternative approach which is based also on spinor genus theory as well as on certain graph-theoretic considerations. The seed of the present viewpoint had already been planted in Kneser's remarkable article [5] wherein he studied definite quadratic forms via arithmetically indefinite forms. This method, when extended in the special case of ternary quadratic forms, yields a global graph with respect to a suitable prime $\mathfrak{p}$ at which the local image is isomorphic to the Bruhat–Tits building of the spin group at $\mathfrak{p}$. By means of this graph, certain representation-theoretic results for positive ternary quadratic forms were obtained in [7]. We shall exploit it here from

* Current address: Department of Mathematics, Seton Hall University, South Orange, NJ 07079.

† Research partially supported by NSF Grant MCS 80-02985.

0022-314X/83 $3.00

the standpoint of classification theory; namely, *classifying integral quadratic forms in three or more variables up to proper spinor equivalence*, which is known to include the classification of forms up to proper equivalence in the indefinite case. The approach taken here is rather closely related to that by Cassels, and may be viewed as "*a variation of a theme of Cassels's.*" The main result and its corollary given below, however, are of independent interest.

1

Let F be an algebraic number field and R its ring of algebraic integers. We consider a finite dimensional vector space V over F which is endowed with a non-degenerate quadratic form q and its associated symmetric bilinear form b satisfying $q(x+y)-q(x)-q(y)=b(x,y)$, and L a quadratic R-lattice spanning V. We always assume that $n=$ rank of L is greater than or equal to three. If $\mathfrak{p}$ is a discrete prime spot, we shall denote by $\operatorname{disc}(L_\mathfrak{p})$, by abuse of notation, to be the usual discriminant of $L_\mathfrak{p}$ when n is even, but only half of the discriminant when n is odd. We say L is *good* at $\mathfrak{p}$ (or simply $L_\mathfrak{p}$ is good) if $q(L_\mathfrak{p}) \subseteq R_\mathfrak{p}$ and $\operatorname{disc}(L_\mathfrak{p})$ is a unit. Suppose K is another R-lattice on V that is also good at $\mathfrak{p}$. Then, $L_\mathfrak{p}$ and $K_\mathfrak{p}$ are $R_\mathfrak{p}$-maximal lattices so that by local theory there is a local basis $\{e_1, f_1, ..., e_t, f_t, z_{2t+1}, ..., z_n\}$ for $L_\mathfrak{p}$ satisfying $q(e_i)=q(f_i)=0$, $b(e_i,f_j)=\delta_{ij}$, $0=b(e_i,e_j)=b(f_i,f_j)$ for $i \neq j$, $b(e_i,z_k)=b(f_i,z_k)=0$, the subspace $\operatorname{span}\{z_{2t+1}, ..., z_n\}$ is anisotropic, and

$$K_\mathfrak{p} = \mathfrak{p}^{a_1}e_1 + \mathfrak{p}^{-a_1}f_1 + \cdots + \mathfrak{p}^{a_t}e_t + \mathfrak{p}^{-a_t}f_t + R_\mathfrak{p}z_{2t+1} + \cdots + R_\mathfrak{p}z_n,$$

where $a_1, ..., a_t$ are nonnegative exponents. It follows that $[L_\mathfrak{p} : L_\mathfrak{p} \cap K_\mathfrak{p}] = [K_\mathfrak{p} : L_\mathfrak{p} \cap K_\mathfrak{p}] = \mathfrak{N}(\mathfrak{p})^{a_1+\cdots+a_t}$ where $\mathfrak{N}(\mathfrak{p})$ is the number of residue classes mod $\mathfrak{p}$.

To define the global graph $\mathbf{R}(L:\mathfrak{p})$ we take for the vertices those lattices K in the genus $\mathscr{G}$ of L such that $K_\mathfrak{q}=L_\mathfrak{q}$ at all primes $\mathfrak{q} \neq \mathfrak{p}$. A distance function on the vertices may be defined by setting $\operatorname{dist}(L,K,\mathfrak{p})=r$ if and only if $[L_\mathfrak{p} : L_\mathfrak{p} \cap K_\mathfrak{p}[= \mathfrak{N}(\mathfrak{p})^r$. L and K are *neighbors* when $r=1$. Two vertices are connected by a simple edge when and only when they are neighbors. This graph has its local image $\mathbf{R}_\mathfrak{p}(L_\mathfrak{p})$ which, in the special case when $n=3$, is canonically isomorphic to the Bruhat–Tits building for the spin group of $V_\mathfrak{p}$ (see [7]). The graph $\mathbf{R}(L:\mathfrak{p})$ is connected, and is a tree if and only if the Witt index of $V_\mathfrak{p}$ is unity (hence, only when $n \leqslant 4$). It is clear that if $K \in |\mathbf{R}(L:\mathfrak{p})|$ then $\mathbf{R}(L:\mathfrak{p})=\mathbf{R}(K:\mathfrak{p})$, and should $K \in \operatorname{cls}^+(L)$ then the neighbors of K fall into the same proper classes as the neighbors of L. Which proper classes actually belong to $|\mathbf{R}(L:\mathfrak{p})|$ is answered by the following result:

PROPOSITION 1. *If* $K \in |\mathbf{R}(L : \mathfrak{p})|$ *then* $\mathbf{R}(L : \mathfrak{p})$ *contains a representative of every proper class in the proper spinor genus* $\operatorname{spn}^+(K)$. *The number of proper spinor genera represented by* $|\mathbf{R}(L : \mathfrak{p})| = g^+(L : \mathfrak{p})$ *is at most two, and which is determined by condition* (1.1) *given below.*

Proof. The first statement is an immediate consequence of the main theorem in indefinite quadratic forms theory (see [6, Sect. 104]) since L is good at the spot $\mathfrak{p}$ implies that $V_{\mathfrak{p}}$ is isotropic. The second statement is proved in [1, Sect. 4]. See also [7], where an identification of the local graph for ternary $\mathbb{Z}_p$-lattices with the Bruhat–Tits building for $SL_2(\mathbb{Q}_p)$ is used, whereas [1] eliminates this identification by a completely different proof which also has the advantage that is readily generalizes to arbitrary dimension. ∎

The proof actually shows that the vertices which are even distances apart belong to the same proper spinor genus. In view of this proposition it is clear that if we can show that any two proper spinor genera in the genus can be linked by a suitable prime spot $\mathfrak{p}$ which can be effectively determined, then we have a decision procedure for classifying forms up to spinor-equivalence. The main result below accomplishes this.

Let π be a fixed prime element of $F_{\mathfrak{p}}$, and let $\{e_1, f_1, \ldots, e_t, f_t, z_{2t+1}, \ldots, z_n\}$ be a basis for $L_{\mathfrak{p}}$ as described above. Let G be the special orthogonal group (defined over F) with respect to the quadratic form q, $\mathbf{A}$ the adele ring of F, and $G_{\mathbf{A}}$ the adele group of G; i.e., the restricted direct product of the groups $G_{F_{\mathfrak{p}}}$ with respect to their compact open subgroups $G_{R_{\mathfrak{p}}}$, where $G_{F_{\mathfrak{p}}}$ and $G_{R_{\mathfrak{p}}}$ are, respectively, then set of points of G with coordinates in $F_{\mathfrak{p}}$ and $R_{\mathfrak{p}}$. Put $\sum(\mathfrak{p})$ for the adele given componentwise by $\sum(\mathfrak{p})_{\mathfrak{q}} = 1$ for all primes $\mathfrak{q} \neq \mathfrak{p}$ and $\sum(\mathfrak{p})_{\mathfrak{p}} = S_{e_1 - f_1} \cdot S_{e_1 - \pi f_1}$, where S_w denotes the symmetry with respect to the line $F_{\mathfrak{p}} w$. It is clear that the action of $\sum(\mathfrak{p})$ does not depend on the choice of π. Let G_L be the stabilizer of L under the action of $G_{\mathbf{A}}$, and θ be the spinor norm function. Define the idele $j(\mathfrak{p}) \in J_F$ to have 1 at every component away from $\mathfrak{p}$, and $j(\mathfrak{p})_{\mathfrak{p}} = \pi$. Since L is good at $\mathfrak{p}$, a direct computation shows that $\theta(0^+(L_{\mathfrak{p}}))$ consists of all the even-ordered elements in $F_{\mathfrak{p}}$ so that $j(\mathfrak{p})$ is well-defined modulo $\theta(G_L)$. We also have $\theta(\sum(\mathfrak{p})) \equiv j(\mathfrak{p})$ mod $\theta(G_L)$. Now, if K is a neighbor of L and $K = \sum(\mathfrak{p}) L$ with respect to the above local basis, then the graph $\mathbf{R}(L : \mathfrak{p})$ contains just a single proper spinor genus exactly when $K \in \operatorname{spn}^+(L)$. In other words,

$$g^+(L : \mathfrak{p}) = 1 \qquad \text{if and only if} \quad j(\mathfrak{p}) \in P_D J_F^{\mathscr{L}}, \tag{1.1}$$

where P_D is the subgroup of principal ideles with respect to $D = \theta(0^+(V)) = \theta(G_F)$, and $J_F^{\mathscr{L}}$ consists of those ideles whose finite components lie in $\theta(0^+(L_{\mathfrak{p}}))$. See [6, Sect. 101].

2

The objective in this section is to prove the "spinor linkage theorem." For any M in the genus of L, we say cls^+L and cls^+M are *linked* at $\mathfrak{p}$ if $|\mathbf{R}(L:\mathfrak{p})|$ contains lattices from cls^+M. Thus, L and M are linked at $\mathfrak{p}$ if and only if there exists $M' \in \text{cls}^+M$ such that $M'_\mathfrak{q} = L_\mathfrak{q}$ at all spots $\mathfrak{q} \neq \mathfrak{p}$ and L is good at $\mathfrak{p}$. Linkage of proper spinor genera at $\mathfrak{p}$ is defined analogously. Proposition 1 implies that cls^+L and cls^+M are linked at $\mathfrak{p}$ if and only if spn^+L is linked at $\mathfrak{p}$ with spn^+M.

THEOREM 2. *Given M in the genus of L, there exists a prime $\mathfrak{p}$ that links spn^+M and spn^+L. More precisely, there exists $M' \in \text{spn}^+M$ such that M' is a neighbor of L in the graph $\mathbf{R}(L:\mathfrak{p})$.*

Proof. Choose an adele $\sum \in G_\mathbf{A}$ such that $M = \sum L$. Let X be the set of all real spots on F, and let T be a finite set of discrete primes on F satisfying the following:

(i) T contains all dyadic prime spots,

(ii) L_q is unimodular at all finite $q \notin T$,

(iii) $L_\mathfrak{q} = M_\mathfrak{q}$ for all $\mathfrak{q} \notin T$.

For each $\mathfrak{q} \in T$, choose $x_\mathfrak{q} \in R_\mathfrak{q} \cap \theta(\sum_\mathfrak{q}) \cdot F_\mathfrak{q}^{\times 2}$ and set $a_\mathfrak{q} = \text{ord}_\mathfrak{q}(x_\mathfrak{q}) + \text{ord}_\mathfrak{q}(4) + 1$. By the approximation theorem, we can find a $c \in R$ which is positive with respect to all $\mathfrak{q} \in X$ and congruent to $x_\mathfrak{q}$ $\text{mod}\,\mathfrak{q}^{a_\mathfrak{q}}$ for $\mathfrak{q} \in T$. Thus, $c \in D = \theta(G_F)$.

Now, we write $(c) = (\prod_{\mathfrak{q}\in T} \mathfrak{q}^{e_\mathfrak{q}}) \cdot \mathfrak{a}$, where $\mathfrak{a}$ is relatively prime to $\mathfrak{q}$ for all $\mathfrak{q} \in T$. Define a modulus $\mathfrak{m} = (\prod_{\mathfrak{q}\in T} \mathfrak{q}^{a_\mathfrak{q}}) \cdot (\prod_{\mathfrak{q}\in X} \mathfrak{q})$. By a density theorem from class field theory (see [4, Chap. V]), each ray class in the ray class group $I_F^\mathfrak{m}/S_\mathfrak{m}$ contains infinitely many primes. In particular, we may choose a prime $\mathfrak{p}$ in the ray class $\mathfrak{a} \cdot S_\mathfrak{m}$. Write $\mathfrak{p} = \mathfrak{a} \cdot (b)$, where b is a ray mod $\mathfrak{m}$. Then,

$$(cb) = \left(\prod_{\mathfrak{q}\in T} \mathfrak{q}^{e_\mathfrak{q}}\right) \mathfrak{p}.$$

So, $cb \in R$, $\text{ord}_\mathfrak{p}(cb) = 1$, $cb >_\mathfrak{q} 0$ for all $\mathfrak{q} \in X$. And for each $\mathfrak{q} \in T$, we have $\text{ord}_\mathfrak{q}(cb - x_\mathfrak{q}) \geqq \min(\text{ord}_\mathfrak{q}\, c(b-1),\ \text{ord}_\mathfrak{q}(c - x_\mathfrak{q}))$. Since $b \equiv 1 \ \text{mod}^\times \mathfrak{m})$, we see $\text{ord}_\mathfrak{q}\, c(b-1) \geqq a_\mathfrak{q}$. But, by the choice of c, $\text{ord}_\mathfrak{q}(c - x_\mathfrak{q}) \geqq a_\mathfrak{q}$ also. Hence, $\text{ord}_\mathfrak{q}(cb - x_\mathfrak{q}) \geqq a_\mathfrak{q}$ for all $\mathfrak{q} \in T$. This implies, by the Local Square Theorem, that $cb \in x_\mathfrak{q} \cdot F_\mathfrak{q}^{\times 2}$, $\mathfrak{q} \in T$.

Putting $d = cb$, we have $d \cdot \theta(\sum_\mathfrak{q}) \cdot F_\mathfrak{q}^{\times 2} = F_\mathfrak{q}^{\times 2}$ at all $\mathfrak{q} \in T$. Also, since $\theta(\sum_\mathfrak{q}) \in \theta(0^+(L_\mathfrak{q})) = U_\mathfrak{q} \cdot F_\mathfrak{q}^{\times 2}$ for each $\mathfrak{q} \notin T$, we have $d \cdot \theta(\sum_\mathfrak{q}) \in U_\mathfrak{q} \cdot F_\mathfrak{q}^{\times 2}$ for $\mathfrak{q} \notin T \cup \{\mathfrak{p}\}$, and $d \cdot \theta(\sum_\mathfrak{p}) \in \pi U_\mathfrak{p} \cdot F_\mathfrak{p}^{\times 2}$. Hence,

$$\theta\left(\sum\right) \in (d^{-1}) \cdot j(\mathfrak{p}) \cdot J_F^\mathfrak{L} \subseteq j(\mathfrak{p}) \cdot P_D \cdot J_F^\mathfrak{L}.$$

Let $G'_{\mathbb{A}}$ be the subgroup of $G_{\mathbb{A}}$ whose local components everywhere have trivial spinor norms. Then, since $j(\mathfrak{p}) \equiv \theta(\sum(\mathfrak{p})) \mod \theta(G_L)$ and θ: $G_{\mathbb{A}} \to J_F/J_F^2$ induces an isomorphism from $G_{\mathbb{A}}/G_F G'_{\mathbb{A}} G_L$ onto $J_F/P_D J_F^{\mathscr{G}}$, we see that $\sum \in \sum(\mathfrak{p}) \cdot G_F G'_{\mathbb{A}} G_L$. Therefore, $\mathrm{spn}^+(\sum(\mathfrak{p})L) = \mathrm{spn}^+ \sum L = \mathrm{spn}^+ M$, and $M' = \sum(\mathfrak{p})L$ is the desired lattice. ∎

An immediate consequence of Proposition 1 and Theorem 2 is

COROLLARY 3. *If L and M are R-lattices of rank $\geqq 3$ in the same genus, then there exists a prime $\mathfrak{p}$ and a lattice M' properly isometric to M such that $L_{\mathfrak{q}} = M'_{\mathfrak{q}}$ for all primes $\mathfrak{q} \neq \mathfrak{p}$.*

Remark. By the theorem, there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ such that the cosets $j(\mathfrak{p}_i) \cdot P_D J_F^{\mathscr{G}}$, $1 \leqq i \leqq g$, are distinct, where $g = [J_F : P_D J_F^{\mathscr{G}}]$, so that one can capture all the proper classes in the genus $\mathscr{G}$ from the graphs $\mathbf{R}(L : \mathfrak{p}_1), \ldots, \mathbf{R}(L : \mathfrak{p}_g)$. If M, L, $\mathfrak{p}$ are as in the theorem, then one sees that M and L are properly spinor equivalent if and only if $j(\mathfrak{p}) \in P_D J_F^{\mathscr{G}}$.

3

The method described above for proper spinor equivalence applies equally well to definite or indefinite lattices as the next examples show.

(1) Let $f(X, Y, Z, W) = X^2 + Y^2 + 16Z^2 + 16W^2$, and $g(X, Y, Z, W) = 2X^2 + 2Y^2 + 5Z^2 + 2XZ + 2YZ + 16W^2$. Associate to f the quadratic $\mathbb{Z}$-lattice L with orthogonal basis defined by $q(e_1) = q(e_2) = 1$ and $q(e_3) = q(e_4) = 16$, and let M be a lattice correspondent to g. It can be shown, using, for example [6, Sect. 93], that M belongs to the genus of L. We want to know whether $M \in \mathrm{spn}^+ L$. Since $M' = \mathbb{Z}(e_1 + e_2) + \mathbb{Z}(e_1 - e_2) + \mathbb{Z}(\frac{1}{2}e_3 + e_1) + \mathbb{Z}e_4$ lies in the proper class of M, we may assume that $M = M'$. Since $[L : L \cap M] = 2$, we have $L_q = M_q$ for all $q \neq 2$. Let T denote the finite set of primes from the proof of Theorem 2, we may set $T = \{2\}$.

Now, let $\sigma \in 0^+(V_2) = G_{\mathbb{Q}_2}$ be the transformation whose matrix with respect to the basis $\{e_1, e_2, e_3, e_4\}$ is given by

$$\begin{pmatrix} 2/3 & -1/3 & 8/3 & 0 \\ 1/3 & -2/3 & -8/3 & 0 \\ 1/6 & 1/6 & -1/3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let $\sum \in G_{\mathbb{A}}$ be given componentwise by $\sum_q = 1$ for $q \neq 2$ and $\sum_2 = \sigma$. Then, $M = \sum L$. Using a formula due to Zassenhaus [9], we have $\theta(\sum_2) =$

$\det((1+\sigma)/2)\cdot\mathbb{Q}_2^{\times 2}=6\cdot\mathbb{Q}_2^{\times 2}$. Using same notations from proof of Theorem 2, we have $c=6$, $\mathfrak{a}=3\cdot\mathbb{Z}$, $a_2=3$, and we may take $p=3$ in the arithmetic progression $\{3+8t \mid t\in\mathbb{N}\}$. Therefore, g is properly spinor equivalent to f if and only if $j(3)\in P_D J_{\mathbb{Q}}^{\mathfrak{c}}$. This is easy to check when one knows the local spinor norms of integral rotations. Here for odd primes q, $\theta(G_{\mathbb{Z}_q})=U_q\cdot\mathbb{Q}_q^{\times 2}$ and $\theta(G_{\mathbb{Z}_2})=\mathbb{Q}_2^{\times 2}\cup 2\mathbb{Q}_2^{\times 2}\cup 5\mathbb{Q}_2^{\times 2}\cup 10\mathbb{Q}_2^{\times 2}$, and $D=\mathbb{Q}^+$. Thus, one sees that g is *not* properly spinor equivalent to f.

(2) Let $f(X,Y,Z)=X^2-7Y^2-6YZ-11Z^2$, and $g(X,Y,Z)=X^2-3Y^2-2YZ-23Z^2$. See [2, p. 132]. Let L be the indefinite ternary $\mathbb{Z}$-lattice associated to f with a basis $\{e_1,e_2,e_3\}$ given by $q(e_1)=1$, $q(e_2)=-7$, $q(e_3)=-11$, $b(e_1,e_2)=0=b(e_1,e_3)$, $b(e_2,e_3)=-6$. Associate M to g. Then, M may be assumed to have the basis $\{e_1, \frac{1}{2}(e_2-e_3), \frac{1}{2}(3e_2+e_3)\}$. Since $[L:L\cap M]=2$ and $\operatorname{disc}(L)=2^4\cdot 17$, $T=\{2,17\}$. Set $\sum_{17}=1$ and $\sum_2$ be given, with respect to the basis $\{e_1,e_2,e_3\}$, by the matrix

$$\begin{pmatrix} -1 & 0 & 0 \\ 1 & 1/6 & -7/6 \\ 0 & -5/6 & -1/6 \end{pmatrix}.$$

Then, $\theta(\sum_{17})=\mathbb{Q}_{17}^{\times 2}$ and $\theta(\sum_2)=q(e_1)\,q(e_2+e_3)\cdot\mathbb{Q}_2^{\times 2}=6\mathbb{Q}_2^{\times 2}$ since $\sum_2$ is the product of two symmetries $S_{e_1}\cdot S_{e_2+e_3}$. Thus, $c=38$, $\mathfrak{a}=19\mathbb{Z}$, and we may take $p=19$ from the progression $\{19+8\cdot 17t\}$. One checks that $j(19)\in P_D J_{\mathbb{Q}}^{\mathfrak{c}}$ so that f and g are spinor-equivalent (and hence, equivalent in this case).

References

1. J. W. Benham and J. S. Hsia, On spinor exceptional representations, *Nagoya Math. J.* **87** (1982), 247–260.
2. J. W. S. Cassels, "Rational Quadratic Forms," Academic Press, New York/London, 1978.
3. J. W. S. Cassels, Rationale quadratische Formen, *Jahresber. Deutsch. Math.-Verein.* **82** (1980), 81–93.
4. G. J. Janusz, "Algebraic Number Fields," Academic Press, New York, 1973.
5. M. Kneser, Klassenzahlen definiter quadratischer Formen, *Arch. Math. (Basel)* **8** (1957), 241–250.
6. O. T. O'Meara, "Introduction to Quadratic Forms," Springer-Verlag, Berlin/Heidelberg/New York, 1963.
7. R. Schulze-Pillot, Darstellung durch definite ternäre quadratische Formen, *J. Number Theory* **14** (1982), 237–250.
8. C. L. Siegel, Zur Theorie der quadratischen Formen, *Nachr. Akad. Wiss. Göttingen* **11a** (1972), 21–46.
9. H. J. Zassenhaus, On the spinor norm, *Arch. Math. (Basel)* **13** (1962), 434–451.