ACTA ARITHMETICA
LVIII.2 (1991)

One-class spinor genera of positive quadratic forms

by

A. G. EARNEST (Carbondale, Ill.) and J. S. HSIA* (Columbus, Ohio)

Dedicated to the memory of G. L. Watson

Using the Minkowski–Siegel mass formula, Magnus [10] proved in 1937 that there exist only finitely many inequivalent positive definite primitive integral quadratic forms of class number one (i.e., for which the equivalence class and genus coincide). Subsequently, Watson [15] proved by algebraic methods that there are no such forms of rank exceeding 10, and in a sequence of papers published between 1963 and 1984 (see [19] and the references given there), sought to determine all classes of forms of class number one in ranks 3 through 10.

It is known that there exist positive definite integral quadratic forms of small rank which have class number exceeding one, but which satisfy the weaker condition that their class and spinor genus coincide (see [13; pp. 114–115] for such examples of rank 3 and 4; see, e.g., [11], [2], or [13] for descriptions of the spinor genus). Binary forms of fundamental discriminants having this property correspond to imaginary quadratic fields for which the ideal class group is a group of exponent 4 [6]. Estes and Nipp have recently shown that quaternion orders whose norm forms satisfy this property are precisely those which admit a natural factorization [5].

The question of whether forms having the property described in the previous paragraph exist in ranks exceeding 4 was posed to the second author by W. Kantor. It is the purpose of this note to answer this question in the negative. Specifically, we prove the following:

THEOREM. *Let f be a positive definite integral quadratic form of rank exceeding 4. Then the class and spinor genus of f coincide if and only if the class and genus of f coincide.*

Let f be a form of rank n satisfying the conditions of the theorem. Throughout the paper, L will be a quadratic lattice corresponding to the form $2f$, in the sense of [11]; that is, L is a lattice on a quadratic space (V, Q)

* Research partially supported by the National Science Foundation.

such that L has a basis $\{v_1, \ldots, v_n\}$ for which the $n\times n$-matrix $(B(v_i, v_j))$ is equal to $(\partial^2 f/\partial x_i \partial x_j)$, where B is the symmetric bilinear form on V defined by $2B(u, v) = Q(u+v)-Q(u)-Q(v)$. Note that the norm ideal nL is contained in $2\mathbf{Z}$. As the properties to be studied here are invariant under scaling, it will be assumed throughout that $nL = 2\mathbf{Z}$. $d(L) = \det(B(v_i, v_j))$ will denote the discriminant of L; for a prime p, write $d_p(L) = p^s$, where $p^s \| d(L)$. $h(L)$, $h_s(L)$ and $g(L)$ will denote the numbers of isometry classes of the genus of L, isometry classes in the spinor genus of L, and spinor genera in the genus of L, respectively. As the spinor genus is contained in the genus, $h(L) = 1$ clearly implies $h_s(L) = 1$.

The main tool to be used in the proof of the theorem for forms of rank 5 and 6 is the Minkowski–Siegel mass formula. A history of the development of this classical formula and references to the pertinent literature are given, e.g., in [3]. In the present context, the mass is given by

$$m(L) = \sum_{i=1}^{h(L)} \frac{1}{|O(L_i)|},$$

where $L_1, \ldots, L_{h(L)}$ are representatives of the distinct isometry classes in the genus of L and $O(L_i)$ is the orthogonal group of L_i. It will also be necessary to consider the analogous sums $m_s(L)$ taken over representatives of the isometry classes in the spinor genus of L. A proof analogous to that of [9; Satz 1] shows that the mass of a genus is always equally distributed among the spinor genera in the genus; thus, $m_s(L) = m(L)/g(L)$. Now, for a prime p, define $m_p(L) = d_p(L)^{(n+1)/2}/\alpha_p(L)$, where $\alpha_p(L) = \alpha_p(2f)$ is the p-adic density of the form $2f$, and define

$$M_p(L) = m_p(L)(1-p^{-2})(1-p^{-4})\ldots(1-p^{2-2s})(1-\varepsilon p^{-s}),$$

where $n = 2s$ or $2s-1$, $\varepsilon = 0$ when n is odd or $p = 2$, and otherwise ε is the Legendre symbol $\left(\frac{(-1)^s d(L)}{p}\right)$ ($m_p(L)$ is essentially the "p-mass" defined in [3], and $M_p(L)$ is this p-mass divided by its "standard value"). It is useful to note that $M_p(L) = 1$ when $p \nmid 2d(L)$, and that both $m_p(L)$ and $M_p(L)$ are invariant under scaling and duality. With these notations, the mass formula takes the form

$$(*) \qquad m(L) = 2\pi^{-n(n+1)/4} \prod_{j=1}^{n} \Gamma(j/2) \prod_p m_p(L)$$

where the last product extends over all rational primes p.

In the application of the above formula, the computation of the local densities merits further comment. For odd primes p, the values of $\alpha_p(L)$ can be routinely computed as described, e.g., in [12] (with the correction to formula (23) noted in [16]). The calculation of $\alpha_2(L)$ is considerably more tedious and highly susceptible to error. For these calculations, the authors adopted the approach of [16]. Here, with L and f related as described above, $\alpha_2(L) = 2^{n-1} N^*(f, f)$ (see [16; p. 105]), where the definition and computation of $N^*(f, f)$ are described in detail in [16]. An alternative approach to determining the 2-adic contribution to the mass can be found in [3].

Transformations which reduce the discriminant but do not increase the class number or spinor class number also play a role in the proof of the theorem. Such transformations were introduced by Watson in [14]. Here we will use the slightly modified lattice-theoretic version defined and denoted by μ_p by Gerstein [7]. It can be shown as in the proof of [7; Theorem 3.6] that these transformations have the property $h_s(\mu_p L) \leqslant h_s(L)$. For the purpose of this paper, a lattice L will be called *μ_p-maximal* if $\mu_p L = L$ or, in the case $p = 2$, $n((\mu_2 L)_2) = \mathbf{Z}_2$. For later reference, we note that local density computations show that $M_p(L) \geqslant 4$ whenever p is odd, $p | d(L)$ and L is μ_p-maximal. Moreover, $M_2(L) \geqslant 1/8$ whenever $n = 5$ and L is μ_2-maximal; the value 1/8 is attained, e.g., when

$$L_2 \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \perp \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \perp \langle 2u \rangle,$$

$u \in U_2$ (here U_2 denotes the group of 2-adic units).

The final ingredient needed in the proof is the explicit determination of the local spinor norm groups $\theta(O^+(L_p))$ obtained for odd primes p by Kneser [8] and for $p = 2$ by the authors [4]. In particular, these spinor norm computations show that when a genus splits into multiple spinor genera there exists at least one prime at which the localization of the lattice has a very special structure. This fact will be exploited in order to obtain estimates for the corresponding local factors appearing in the mass formula.

Proof of Theorem — rank 5. To prove the theorem, it suffices to show that $h_s(L) = 1$ implies $h(L) = 1$ for the lattices L under consideration or, equivalently, that $h_s(L) > 1$ whenever $g(L) > 1$. In light of the obvious inequality $|O(L)| \geqslant 2$, it thus suffices to show that $m_s(L) > 1/2$ whenever $g(L) > 1$.

Assume now that $g(L) > 1$. Then there exists at least one prime q such that $\theta(O^+(L_q)) \not\supseteq U_q \dot{Q}_q^2$ [11; 102:9]. Fix such a prime q for the remainder of this section. Without loss of generality, it may be assumed that L is μ_p-maximal for all primes $p \neq q$ (otherwise, a lattice $\hat{L}$ with this property and satisfying $h_s(\hat{L}) \leqslant h_s(L)$ can be obtained from L via a suitable sequence of μ_p-transformations for $p \neq q$; L may then be replaced by $\hat{L}$ for the remainder of the argument). For such L, the standard idèlic formula for computing $g^+(L)$ (see [11; 102:7]) then yields $g(L) \leqslant 4$; in fact, $g(L) \leqslant 2$ unless $q = 2$ and $\theta(O^+(L_2)) \cap U_2 \dot{Q}_2^2 = \dot{Q}_2^2$.

Specializing the mass formula (*) to the case $n = 5$ gives

$$m(L) = 2\pi^{-15/2} \prod_{j=1}^{5} \Gamma(j/2) \prod_p m_p(L)$$

$$= 2\pi^{-15/2}(\tfrac{3}{8}\pi^{3/2})\zeta(2)\zeta(4) \prod_p M_p(L) = \frac{1}{720} \prod_p M_p(L).$$

To complete the proof, we now proceed to analyze the product $\prod_p M_p(L)$.

Consider first the case $q = 2$. In order for $\theta(O^+(L_2)) \not\supseteq U_2\dot{Q}_2^2$ to hold, L_2 must have a Jordan splitting of the type $L_2 \cong \langle 2^{e_1}u_1, 2^{e_2}u_2, \ldots, 2^{e_5}u_5\rangle$ with $u_i \in U_2$ for $1 \leqslant i \leqslant 5$, $1 = e_1 \leqslant e_2 \leqslant \ldots \leqslant e_5$, at most two consecutive exponents equal, and $e_{j+1} - e_j \geqslant 4$ whenever $e_{j+1} \neq e_j$ [4; Theorem 3.14]. If $1 < e_2 < \ldots < e_5$, then $M_2(L) \geqslant 2^{24}3^2 5$ and $m_s(L) \geqslant m(L)/4 > 1/2$. In all remaining cases, $g(L) = 2$ and $M_2(L) \geqslant 2^6 3^2 5$; thus $m_s(L) = m(L)/2 \geqslant M_2(L)/1440 > 1/2$.

Now consider the case that q is odd. L_q must have a Jordan splitting of the type $L_q \cong \langle u_1, q^{e_2}u_2, \ldots, q^{e_5}u_5\rangle$ with $u_i \in U_q$ for $1 \leqslant i \leqslant 5$ and $1 \leqslant e_2 < \ldots < e_5$ [8; Satz 3]. In this case

$$m_q(L) = 2^{-4}q^{-e_2+e_4+2e_5} \quad \text{and} \quad M_q(L) = 2^{-4}q^{(e_4-e_2)+2e_5-6}(q^2-1)(q^4-1).$$

Since $e_4 - e_2 \geqslant 2$ and $e_5 \geqslant 4$,

$$M_q(L) \geqslant q^4(q^2-1)(q^4-1)/16.$$

Now

$$m_s(L) = \frac{1}{2}m(L) = \frac{1}{1440}M_2(L)M_q(L)\prod_{p\neq 2,q} M_p(L) \geqslant \frac{1}{11520}M_q(L).$$

So if $q \geqslant 5$, or if $q = 3$ and $e_5 \geqslant 5$, then $m_s(L) > 1/2$, as desired.

The only case requiring further analysis occurs when $q = 3$ and $L_3 \cong \langle u_1, 3u_2, 3^2u_3, 3^3u_4, 3^4u_5\rangle$, in which case $M_3(L) = 2^3 3^4 5 < \frac{1}{2}(11, 520)$. Moreover, it may be assumed that $p \nmid d(L)$ for $p \neq 2, 3$, and (since $g(L) > 1$) that $\theta(O^+(L_2)) \neq \dot{Q}_2$. From [4] and a computation of 2-adic densities, it follows that whenever L is μ_2-maximal but $\theta(O^+(L_2)) \not\supseteq \dot{Q}_2$, $M_2(L) \geqslant 5/16$ (and thus $m_s(L) > 1/2$) except in the case that

$$L_2 \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \perp P \perp \langle 2u\rangle, \quad u \in U_2, \quad P \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Finally, if L has both 2-adic and 3-adic splittings of these exceptional types, then $m_s(L) = 3^2/2^5$. Since $m_s(L)$ is not of the form $1/|O(L)|$, it again follows that $h_s(L) > 1$.

Proof of Theorem – rank exceeding 5. The proof of the theorem for forms of rank 6 can be carried out similarly to that given for rank 5 in the preceding section. The only additional feature is the appearance in the mass formula of a factor equal to the value of an L-series. Specifically, when $n = 6$ the formula (*) specializes to

$$m(L) = \frac{\zeta_D(3)}{360\pi^3}\prod_p M_p(L),$$

where

$$(-) \qquad \zeta_D(3) = \prod_p\left(1 - \left(\frac{-dL}{p}\right)p^{-3}\right)^{-1} = \sum_{m\,\text{odd}}\left(\frac{-dL}{m}\right)m^{-3},$$

$(-)$ denoting the Jacobi symbol (see [3; p. 266]). The factor $\zeta_D(3)$ is bounded from below (independently of $D = -dL$) by $2 - \sum_{m\,\text{odd}} m^{-3} = 2 - \lambda(3) > 0.94$ [1]. So $\zeta_D(3)/\pi^3 > 0.03$ and

$$m(L) > \frac{1}{12000}\prod_p M_p(L).$$

Straightforward computations of the local densities involved now show that in all instances $\prod_p M_p$ is sufficiently large to ensure $m_s(L) > 1/2$. Here the relevant lower bounds for the values of M_p are as follows: if L is μ_2-maximal, then $M_2(L) \geqslant 5/2^3 5^2 7$; if $\theta(O^+(L_p)) \not\supseteq U_p\dot{Q}_p^2$, then $M_p(L) > p^{23/2}(p^2-1)(p^4-1)/2^5$ when p is odd and $M_2(L) > 2^{14}3^2 5$ when $p = 2$.

Due to the explicit knowledge of *all* primitive positive quadratic forms of class number one and rank exceeding 6 (not just those having restricted local structures, as is currently the case in ranks 5 and 6), it is unnecessary to extend the computations involving the mass formula to these higher ranks.

To complete the proof of the theorem, suppose there exists an L satisfying $h_s(L) = 1$, $g(L) > 1$ and $\operatorname{rk} L \geqslant 7$. As before, fix a prime q for which $\theta(O^+(L_q)) \not\supseteq U_q\dot{Q}_q^2$. By applying transformations μ_p for $p \neq q$, obtain a lattice $\hat{L}$ such that $\theta(O^+(\hat{L}_q)) \not\supseteq U_q\dot{Q}_q^2$, $h_s(\hat{L}) = 1$ and $\hat{L}$ is μ_p-maximal for all $p \neq q$ (thus $\theta(O^+(\hat{L}_p)) \supseteq U_p\dot{Q}_p^2$ for $p \neq q$). Then $\hat{L}_q \cong \langle q^{e_1}u_1, \ldots, q^{e_n}u_n\rangle$ with $0 \leqslant e_1 \leqslant \ldots \leqslant e_n$ and $u_i \in U_q$ for $1 \leqslant i \leqslant n$. If $q \neq 2$, then $\theta(O^+(\hat{L}_q)) \not\supseteq U_q\dot{Q}_q^2$ forces $e_i \neq e_j$ for $i \neq j$. Let $t = [\![\frac{1}{2}e_3]\!]$, let $L' = \mu_q^t\hat{L}$, and write $L'_q \cong \langle u_1, q^{f_2}u_2, \ldots, q^{f_n}u_n\rangle$. Then $0 \leqslant f_2, f_3 \leqslant 1$ and it follows that $\theta(O^+(L'_q)) \supseteq U_q\dot{Q}_q^2$. Thus $g(L') = 1$ and $h(L') = h_s(L') = 1$. Moreover, as $f_j \geqslant (j-3)$ for $4 \leqslant j \leqslant n$ and $n \geqslant 7$, it follows that $q^{10}|d(L')$. If $q = 2$, then $e_1 = 1$ and $e_{j+2} - e_j \geqslant 4$ for $j = 1, \ldots, n-2$. Let $t = [\![\frac{1}{2}(e_3 - 2)]\!]$, let $L' = \mu_2^t\hat{L}$, and write $L'_2 \cong \langle 2u_1, 2^{f_2}u_2, \ldots, 2^{f_n}u_n\rangle$. Now $2 \leqslant f_3, f_4 \leqslant 3$ implies that $\theta(O^+(L'_2)) \supseteq U_2\dot{Q}_2^2$; so again $g(L') = 1$ and $h(L') = h_s(L') = 1$. Here $f_5 - f_3 = e_5 - e_3 \geqslant 4$, and so $f_j \geqslant 6$ for $j \geqslant 5$. Since $n \geqslant 7$, it follows that $2^{22}|d(L')$.

In summary, there must exist a lattice of class number one whose discriminant is either divisible by 2^{22} or by q^{10} for some odd prime q. Consequently, a form whose determinant is divisible by such a prime power must appear among the forms of class number one described in [17], [18] and [19]. However, it can be seen by inspection that no form having determinant divisible by a prime power exceeding 2^{16} or q^8, for an odd prime q, occurs in these lists. This contradiction establishes that no L with $h_s(L) = 1$, $g(L) > 1$ and $\operatorname{rk} L \geqslant 7$ exists, and completes the proof of the theorem.

Remark. The theorem proved above remains valid when the class and spinor genus are replaced by the proper class and proper spinor genus, respectively; that is, under the assumptions of the theorem, the proper class and proper spinor genus of f coincide if and only if the proper class and genus of f coincide. The modifications of the prior arguments which are required to prove this result are as follows. Note first that the transformations μ_p do not increase the proper class number or the number of proper classes in a proper spinor genus. If the proper class and proper spinor genus coincide, then it follows easily that the class and spinor genus must also coincide. Hence, as shown earlier, this cannot occur when the rank exceeds 10. Moreover, there is no distinction between class and proper class, or spinor genus and proper spinor genus, when the rank is odd. For ranks 8 and 10, the forms (from [17], [18]) which give rise to $h_s(L) = 1$ can be seen by inspection to admit improper automorphs; thus, class and proper class again coincide. Finally, the mass formula can be used to resolve the remaining case of rank 6. For if $m_s^+(L)$ denotes the value obtained by summing the reciprocals of the orders of the rotation groups $O^+(L_i)$ over a complete set of representatives for the proper classes in the proper spinor genus of L, then it is straightforward to show that $m_s^+(L) = 2m(L)$. It thus follows from the computations described earlier that $m_s^+(L) > 1/2$ whenever $g^+(L) \geqslant 2$, yielding the desired result.

References

[1] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, Dover, New York 1965.

[2] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, New York 1978.

[3] J. H. Conway and N. J. A. Sloane, *Low-dimensional lattices. IV. The mass formula*, Proc. Roy. Soc. London Ser. A 419 (1988), 259–286.

[4] A. G. Earnest and J. S. Hsia, *Spinor norms of local integral rotations, II*, Pacific J. Math. 61 (1975), 71–86 (see also ibid. 115 (1984), 493–494).

[5] D. R. Estes and G. L. Nipp, *Factorization in quaternion orders*, J. Number Theory 33 (1989), 224–236.

[6] D. R. Estes and G. Pall, *Spinor genera of binary quadratic forms*, ibid. 5 (1973), 421–432.

[7] L. J. Gerstein, *The growth of class numbers of quadratic forms*, Amer. J. Math. 94 (1972), 221–236.

[8] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. (Basel) 7 (1956), 323–332.

[9] — *Darstellungsmasse indefiniter quadratischer Formen*, Math. Z. 77 (1961), 188–194.

[10] W. Magnus, *Über die Anzahl der einem Geschlecht enthaltenen Klassen von positiv-definiten quadratischen Formen*, Math. Ann. 114 (1937), 465–475; 115 (1938), 643–644.

[11] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, New York 1963.

[12] G. Pall, *The weight of a genus of positive n-ary quadratic forms*, Proc. Sympos. Pure Math. 8 (1965), 95–105.

[13] G. L. Watson, *Integral Quadratic Forms*, Cambridge University Press, Cambridge 1960.

[14] — *Transformations of a quadratic form which do not increase the class number*, Proc. London Math. Soc. (3) 12 (1962), 577–587.

[15] G. L. Watson, *The class-number of a positive quadratic form*, ibid. 13 (1963), 549–576.

[16] — *The 2-adic density of a quadratic form*, Mathematika 23 (1976), 94–106.

[17] — *One-class genera of positive quadratic forms in nine and ten variables*, ibid. 25 (1978), 57–67.

[18] — *One-class genera of positive quadratic forms in eight variables*, J. London Math. Soc. (2) 26 (1982), 227–244.

[19] — *One-class genera of positive quadratic forms in seven variables*, Proc. London Math. Soc. (3) 48 (1984), 175–192.

DEPARTMENT OF MATHEMATICS
SOUTHERN ILLINOIS UNIVERSITY
Carbondale, Illinois 62901-4408, U.S.A.

DEPARTMENT OF MATHEMATICS
OHIO STATE UNIVERSITY
Columbus, Ohio 43210-1174, U.S.A.

Received on 25.8.1989
and in revised form on 20.3.1990 (1960)