THE DEFINITE OCTONARY QUADRATIC FORMS OF DETERMINANT 1

BY

DENNIS ESTES AND GORDON PALL

1. G. Eisenstein remarked in 1847 that if h_n denotes the number of classes of positive n-ary quadratic forms with integral matrices and determinant 1, then $h_n = 1$ if $1 \leqq n \leqq 8$ (the one class being that of $x_1^2 + \cdots + x_n^2$), but $h_n > 1$ if $n > 8$. He erred as regards $n = 8$, since as first shown by Korkine and Zolotareff in 1873 there is another applicable class when $n = 8$ whose forms have all diagonal terms even, and so represent no odd numbers. The few proofs that $h_8 = 2$ are referred to by L. J. Mordell, and by Van der Blij and Springer. These proofs involve lengthy computations (Mordell's, while neat in itself, using values of the minimal constants γ_6, γ_7, γ_8) or are based on deep developments, such as the Minkowski formula for the weight of a genus, or on properties of spinor genera (in Kneser's proof). The purpose of this note is to give a simple, self-contained proof that $h_8 = 2$.

It should first be observed that the forms under consideration comprise two genera, one typified by the form $f_8 = x_1^2 + \cdots + x_8^2$ containing forms which represent odd numbers, and the other consisting of forms which represent only even numbers, the latter genus containing in particular the form $2g$, where g has the matrix

$$G = \begin{bmatrix} I & \frac{1}{2}V \\ \frac{1}{2}V' & I \end{bmatrix}, \qquad \text{where}$$

$$(1) \qquad I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 \end{bmatrix}$$

whence $V'V = 3I$. Notice that g is an integral positive form of determinant $\frac{1}{2}^8$, and that $h_8 = 2$ requires that there be only one class of such octonary forms. Note that g transforms into f_8 by an integral transformation of determinant 2^4:

$$(2) \qquad \begin{bmatrix} I & 0 \\ -V' & 2I \end{bmatrix} \begin{bmatrix} I & \frac{1}{2}V \\ \frac{1}{2}V' & I \end{bmatrix} \begin{bmatrix} I & -V \\ 0 & 2I \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}.$$

2. We prove in this section

THEOREM 1. *The integral positive octonaries of determinant* $\frac{1}{2}^8$ *form one class.*

We may denote by fT the form obtained from a form f by the transformation of matrix T. Hence if A is the matrix of f, the matrix of fT is $T'AT$.

Received February 19, 1968.

LEMMA 1. *Consider integral octonaries g_1 of determinant $\frac{1}{2}^8$, and f_1 with an integral matrix of determinant* 1. *If $g_1 T = f_1$, with T integral and* $\det T = 16$, *then $S = 2T^{-1}$ is integral and $f_1 S = 4g_1$. Conversely, if $f_1 S = 4g_1$ with S integral and* $\det S = 16$, *then if $T = 2S^{-1}$ is integral, $g_1 T = f_1$.*

Proof. Let E be the matrix of f_1, H that of g_1. Thus H has denominator 2, and E^{-1} is integral. But $T'HT = E$, hence $T'H = ET^{-1}$. Hence T^{-1} has denominator 2, $f_1 T^{-1} = g_1$, $f_1 S = 4g_1$. The converse follows easily.

LEMMA 2. *Let the octonary f_1 of determinant* 1 *be congruent* (mod 4) *to f_8. Let S be integral,* $\det S = 16$, *S^{-1} have denominator* 2, *and $f_1 S = 4g_1$ with g_1 integral. Then there exists a permutation matrix W and unimodular matrix U such that*

$$WSU = \begin{bmatrix} 2I & V \\ 0 & I \end{bmatrix}. \tag{3}$$

Proof. The left factor W allows us to permute the rows of S, and U allows us to make the elements to the left of the main diagonal zero, those on the diagonal to be positive integers $m_1, \cdots, m_8$ with product 16, and those to the right of any m_i to be reduced modulo m_i (0 if $m_i = 1$, either 1 or -1 at will if $m_i = 2$). The elements above any m_j equal to 2 must be 0, since if 1 occurs to the right of one 2 and above another, the denominator of S^{-1} is at least 4. Now $m_1 = 2$, since if it were 1, the first coefficient of $f_1(WSU)$ would be odd: but it must be made divisible by 4. Similarly, since $c^2 + 1$ and $a^2 + b^2 + 1$ cannot be divisible by 4, we must have $m_2 = m_3 = 2$. If $m_4 = 1$ and a later $m_j = 2$, we can interchange the fourth and j-th rows, and columns, and so secure $m_4 = 2$. Thus the $2I$ and I in (3) can be placed as shown. The expression for V then follows readily from the condition that the coefficients of the terms in $x_i x_j$ $(5 \leqq i < j \leqq 8)$ are to be divisible by 4, rows and columns 5 to 8 being permuted as needed.

COROLLARY. *The integral octonaries of determinant $\frac{1}{2}^8$ which can be carried into f_8 by integral transformations of determinant* 16 *form a single class.*

LEMMA 3. *Every integral positive octonary of determinant $\frac{1}{2}^8$ can be transformed into f_8 by some integral transformation of determinant* 16.

The proof will be completed following Lemma 5.

LEMMA 4 (Hermite). *Let f be a positive n-ary form with real coefficients, and m the minimum of f for integral values not all zero of the variables. Then*

$$m \leqq \left(\tfrac{4}{3}\right)^{(n-1)/2} d^{1/n} \quad \textit{where} \quad d = \det f. \tag{4}$$

Proof (by induction). Take m as first coefficient, and complete squares:

$$f(x_1, \cdots, x_n) = m(x_1 + \cdots)^2 + \phi(x_2, \cdots, x_n). \tag{5}$$

Here the $(n-1)$-ary form ϕ has determinant d/m, and if m' denotes its minimum for integers $x_2, \cdots, x_n$ not all zero, $m' \leqq (\frac{4}{3})^{(n-2)/2}(d/m)^{1/(n-1)}$. An integer x_1 can be chosen so that $0 \leqq (x_1 + \cdots)^2 \leqq \frac{1}{4}$. Hence f represents (with integers $x_1, \cdots, x_n$ not all 0) a number not exceeding $m/4 + m'$; and (4) follows from $m \leqq m/4 + m'$.

LEMMA 5. *Every integral positive quinary of determinant $\frac{1}{4}$ can be carried by an integral transformation of determinant* 2 *into* $x_1^2 + \cdots + x_5^2$.

Proof. By (4) with $d = \frac{1}{4}$ and $n = 5$, $m < 2$; hence $m = 1$, and 1 can be taken as the leading coefficient. If the cross-product coefficients involving x_1 are even the term x_1^2 splits off, and we proceed with a quaternary of determinant $\frac{1}{4}$, which again represents 1 by Lemma 4; and so forth until (since $\frac{1}{4}$ is not an integer) we reach a situation expressed by $x^2 + xy + \cdots$. We may as well assume this situation at the start, and take the quinary to be

$$x_1^2 + x_1 x_2 + \phi(x_2, \cdots, x_5).$$

Let us now replace x_2 by $2x_2$, a transformation of determinant 2, and then complete squares. This gives a form $y_1^2 + \phi_1$, where ϕ_1 is integral and $\det \phi_1 = 1$. Also,

$$\begin{aligned}\phi_1(y_2, \cdots, y_5) &= ky_2^2 + 2r_3 y_2 y_3 + 2r_4 y_2 y_4 + 2r_5 y_2 y_5 + \cdots \\ &= k(y_2 + (r_3/k)y_3 + \cdots)^2 + \cdots,\end{aligned}$$

where k is odd, and r_3, r_4, r_5 are integers. Thus ϕ_1 can be carried by a transformation which is integral mod 2 and has determinant 1 into a form $kz^2 + \phi_2(z_3, z_4, z_5)$, where k is odd and the coefficients of ϕ_2 are integral mod 2. This implies, we maintain, that ϕ_1 has an integral matrix. For if not its dyadic canonical form must involve a term xy (since $x^2 + xy + y^2 + kz^2$ is dyadically equivalent to $xy - 3kz^2$), and hence ϕ_1 represents zero dyadically; thus the Hasse invariant $c_2(\phi_1)$ equals 1, since ϕ_1 has a square determinant; and since $\det \phi_1 = 1$, $c_\infty = -1$ and ϕ_1 is indefinite. Thus ϕ_1 must have an integral matrix, and so by use of (4) with $d = 1$ and $n = 4, 3, 2$, ϕ_1 can be transformed into a sum of four squares.

To proceed: (4) gives $m < 2$, hence $m = 1$, if f is integral and either $n = 8$ and $d = \frac{1}{2}^8$, or $n = 7$ and $d = \frac{1}{2}^6$, or $n = 6$ and $d = \frac{1}{2}^4$. Hence we can take the given octonary to be

$$x_1^2 + a_2 x_1 x_2 + \cdots + a_8 x_1 x_8 + \cdots,$$

can find a unimodular transformation replacing $a_2 x_2 + \cdots + a_8 x_8$ by sy_2 with s in Z, and have $x_1^2 + sx_1 y_2 + h(y_2, \cdots, y_8)$. We replace y_2 by $2y_2$ (a transformation of determinant 2), and, completing squares, obtain $y_1^2 + \phi(y_2, \cdots, y_8)$ with $\det \phi = \frac{1}{2}^6$. Two repetitions of this procedure reduces the proof to Lemma 3. Hence the proof of Theorem 1 is completed.

3. THEOREM 2. *The form $f_8 = x_1^2 + \cdots + x_8^2$ is in a genus of one class.*

Proof. Any class in the genus of f_8 contains a form f^* congruent to f_8 (mod 8). By Lemma 2 and Theorem 1, after some permutation of the variables of f^*, f^* is transformed into $4g_1$, where $g_1 \equiv g$ (mod 2) and g_1 is in the class of g, by the transformation

$$S = \begin{bmatrix} 2I & V \\ 0 & I \end{bmatrix} \quad \text{where} \quad T = 2S^{-1} = \begin{bmatrix} I & -V \\ 0 & 2I \end{bmatrix}. \tag{6}$$

It will suffice to prove that 1 has 16 representations by f^*.

An integral column vector $\xi = \{x_1, \cdots, x_8\}$ will be called a *unit of g* if $\xi' G \xi = 1$. This equation amounts to $(T^{-1}\xi)'(T'GT)(T^{-1}\xi) = 1$, or $(S\xi)' I_8 (S\xi) = 4$, where I_8 is the matrix of f_8. Hence ξ is a unit of G if and only if $\eta = S\xi$ is a representation of 4 by f_8 such that $S^{-1}\eta$ is integral, that is, if $\eta = \{y_1, \cdots, y_8\}$,

$$y_i + y_{i+4} \equiv y_5 + y_6 + y_7 + y_8 \pmod 2 \qquad (i = 1, 2, 3, 4). \tag{7}$$

We count 16 values η from 2 0 0 0 0 0 0 0; and permuting the first four and last four components alike we count $64 + 96 + 64$ values η from

1 1 1 0 0 0 0 1, 1 1 0 0 1 1 0 0 and 1 0 0 0 0 1 1 1.

Thus g has 240 units.

For any integral column vectors ξ, η write

$$\begin{aligned} (\xi, \eta) &= (\xi + \eta)' G (\xi + \eta) - \xi' G \xi - \eta' G \eta \\ &= \sum 2 g_{ij} x_i x_j \quad \text{where} \quad G = (g_{ij}). \end{aligned} \tag{8}$$

Hence $(\xi, -\eta) = -(\xi, \eta)$; and if $\eta \neq 0$, $(2\eta)' G (2\eta) \geqq 4$.

LEMMA 6. *If ξ and η are units and $\xi \equiv \eta$ (mod 2), then $\xi = \eta$ or $\xi = -\eta$.*

Proof. Otherwise, $(\xi, \eta) \geqq 4 - 1 - 1 > 0$, $(\xi, -\eta) \geqq 4 - 1 - 1 > 0$.

LEMMA 7. *$\xi' G \xi \equiv 1$ (mod 2) has exactly 120 solutions ξ (mod 2). Hence for any η such that $\eta' G \eta$ is odd, there is exactly one pair of units ξ and $-\xi$ of g such that $\xi \equiv \eta$ (mod 2).*

Proof. We need only count the octuplets $x_1, \cdots, x_8$ (mod 2) for which

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &+ (x_2 + x_3 + x_4 + 2x_5)^2 + (x_1 + x_3 + x_4 + 2x_6)^2 \\ &+ (x_1 + x_2 + x_4 + 2x_7)^2 + (x_1 + x_2 + x_3 + 2x_8)^2 \equiv 4 \pmod 8: \end{aligned}$$

x_1, x_2, x_3 odd, x_4 even, and adjust x_5 mod 2; x_1, x_2 odd, x_3, x_4 even, and adjust x_7 mod 2; x_1 odd, x_2, x_3, x_4 even, and adjust x_5 mod 2; $x_1, \cdots, x_4$ even and adjust x_5 mod 2. In all, $4 \cdot 8 + 6 \cdot 8 + 4 \cdot 8 + 8 = 120$.

Let U denote a unimodular transformation replacing g by g_1. If ξ ranges over a complete set of residues mod 2 for which $\xi' G \xi$ is odd, $U^{-1}\xi$ ranges over the same residues, since $g \equiv g_1 \pmod 2$. Hence the units of g and g_1 are alike in their residues mod 2. The form f_8 has 16 units, these being given by the vectors $(S\xi)/2$ which ase integral. Hence f^* has 16 units. Theorem 2 follows.

It follows immediately that if $1 \leqq n \leqq 7$, a positive definite n-ary form with an integral matrix and determinant 1 is in the class of $x_1^2 + \cdots + x_n^2$. For, if h is such a form,

$$h(x_1, \cdots, x_n) + x_{n+1}^2 + \cdots + x_8^2$$

is in the class of f_8, and the number of representations of 1 is 16. Hence h represents 1.

At the referee's suggestion we add that the deepest thing used is the elementary theory of the Hasse symbol, such as, for example in Chapter II of Jones's *Arithmetic theory of quadratic forms.*

References

1. L. J. Mordell, *The definite quadratic forms in eight variables with determinant unity*, J. Math. Pures Appl., vol. IX (1938), pp. 41–36.
2. F. van der Blij and T. A. Springer, *The arithmetics of octaves and of the group G_2*, Indagationes Mathematicae, vol. 21 (1959), pp. 406–418.

University of Southern California
Los Angeles, California
Louisiana State University
Baton Rouge, Louisiana