PROPERLY PRIMITIVE TERNARY INDEFINITE QUADRATIC GENERA OF MORE THAN ONE CLASS

BURTON W. JONES AND E. H. HADLOCK

Introduction. The form $f=ax^2+by^2+cz^2+2ryz+2sxz+2txy$ is properly primitive when $(a, b, c, r, s, t)=1$ and (a, b, c) is odd. With f there is associated a determinant d. The greatest common divisor of the cofactors of the elements of d is designated by Ω. Then Δ is defined by $d=\Omega^2\Delta$. For an indefinite form $d\Delta$ must be positive, where Ω is chosen so that $\Omega\Delta$ is negative. Also Ω' and Δ' are defined by $\Omega=\Omega'\Omega''$ and $\Delta=\Delta'\Delta''$ where Ω'' and Δ'' are the greatest powers of 2 dividing Ω and Δ respectively, so that Ω' and Δ' are odd. With f there is associated a reciprocal form $F=AX^2+BY^2+CZ^2+2RYZ+2SXZ+2TXY$, where ΩA, ΩB, $\cdots$, ΩT are the cofactors of the elements of d.

The purpose of this paper is to show genera containing more than one[1] class of properly primitive indefinite forms. The method is that which C. L. Siegel used in a specific example communicated to the first of the authors by letter and which is here generalized to include many forms. By employing this method in Lemma 3 of this paper, many genera are explicitly shown containing at least two classes.

LEMMA 1. *Let $\Omega'=\Omega_1^2$, $\Delta'=-\Delta_1^2$, and Ω'' and Δ'' both be odd powers of* 2. *Let the quadratic characters with respect to Ω and the characters with respect to* 4 *and* 8, *when they exist, have the value one. Let p and q be distinct primes and prime to twice the determinant with $p\equiv 1 \pmod 4$ and $q\equiv \pm 1 \pmod 8$. Then properly primitive indefinite forms f and F exist for which $a=1$ or p^2 and $b=-\Omega q^2$. Moreover*

$$\left(\frac{F}{q_\Delta}\right)=\left(\frac{-1}{q_\Delta}\right)$$

for each odd prime factor q_Δ of Δ.

We show the existence of a form f in which $a=1$ or p^2, $b=\Omega b'$, $b'=-q^2$, $r=\Omega r'$, and $t=0$. Take $a=1$ or p^2 and $b'=-q^2$. The character

Presented to the Society, November 29, 1952 by E. H. Hadlock; received by the editors May 18, 1952.

[1] See the *Arithmetic theory of quadratic forms* by Burton W. Jones, p. 189, and A. Meyer, Journal für Mathematik vol. 116 (1896) pp. 317, 318.

$$\left(\frac{a}{p_\Omega}\right) = 1$$

when $a=1$ or p^2 for each odd prime factor p_Ω of Ω. Also

$$\left(\frac{-1}{a}\right) = 1 = \left(\frac{2}{a}\right).$$

From the definition of a cofactor $C=ab'$ so that

$$\left(\frac{-1}{c}\right) = \left(\frac{-1}{aq^2}\right) = 1 = \left(\frac{2}{aq^2}\right).$$

Also

$$\left(\frac{F}{q_\Delta}\right) = \left(\frac{C}{q_\Delta}\right) = \left(\frac{-1}{q_\Delta}\right).$$

From the expression for the determinant $d=\Omega^2\Delta$ of f there is obtained

$$(1) \qquad aA + q^2s^2 = \Omega\Delta, \quad \text{where} \quad \Omega A = bc - r^2.$$

We seek integers A and s for which (1) is true and then integers c and r for which $\Omega A = bc - r^2$. If $a=1$, then for $s\neq 0$, A is given by the first equation in (1). In order for (1) to have a solution in A and s when $a=p^2$, it is necessary and sufficient for $s^2\equiv\Omega\Delta q_1 \pmod{p^2}$ to have a solution where $q^2q_1\equiv 1 \pmod{p^2}$. But

$$\left(\frac{\Omega\Delta q_1}{p}\right) = \left(\frac{\Omega\Delta}{p}\right) = \left(\frac{-\Omega_1^2\Delta_1^2\Omega''\Delta''}{p}\right) = 1,$$

since $\Omega''\Delta''$ is an even power of 2 and $p\equiv 1 \pmod 4$. Hence $s^2\equiv\Omega\Delta q_1 \pmod{p^2}$ has a solution for s. Then the integral value of A is given by the first equation of (1). In order for $\Omega A = bc - r^2$ to have a solution in c and r it is necessary and sufficient for $r'^2\equiv -A\Omega_2 \pmod{q^2}$ where $r=\Omega r'$, $\Omega\Omega_2\equiv 1 (\bmod\ q^2)$. From (1), $\Omega\Delta\equiv aA \pmod{q^2}$ so that

$$\left(\frac{-A\Omega_2}{q}\right) = \left(\frac{-A\Omega}{q}\right) = \left(\frac{-\Delta}{q}\right) = \left(\frac{\Delta_1^2\Delta''}{q}\right) = \left(\frac{2}{q}\right) = 1$$

since $a=1$ or p^2, Δ'' is an odd power of 2, and $q\equiv\pm 1 \pmod 8$. Then c is an integer and its value is given by $c=-(A+\Omega r'^2)/q^2$. Moreover $(a, b) = (a, -\Omega q^2) = 1$ so that f is primitive. Since a is odd, f is properly primitive. Also f is indefinite since $d=\Omega^2\Delta = -\Omega^2\Delta_1^2\Delta'' < 0$ and $a=p^2>0$. We must show that Ω is the g.c.d. of the cofactors of the elements of d. By the expressions for the cofactors of c, r, s, and t it is obvious that C, R, S, and T are integers. A is an integer and its value is given by the first equation in (1). In order to show that B is an integer, we suppose that B is rational and not an integer. Since $ac-s^2$ is an integer it follows that the denominator of B divides Ω since $\Omega B=ac-s^2$. From $b\Omega B-ar^2=\Omega^2\Delta$ it follows that $b'B=ar'^2+\Delta$. But $ar'^2+\Delta$ is an integer. Hence the denominator of B must divide b'. But $(b', \Omega)=1$. Hence B is an integer. It follows that Ω is the greatest common divisor when we show that F is properly primitive. A common divisor σ of the coefficients of F must divide $C=-p^2q^2$. From the expression for the determinant of F it follows that $\sigma \mid \Omega\Delta^2$. But $(p^2q^2, \Omega\Delta^2)=1$. Hence $\sigma=1$. Finally C is odd.

LEMMA 2. *The relation between the integers represented by* $f=ax^2+by^2+cz^2+2ryz+2sxz$ *of Lemma* 1 *where* $a=1$ *or* p^2, $b=-\Omega q^2$, $r=\Omega r'$, p *and* q *are distinct odd primes, neither of which divides* $\Omega\Delta$, *and the integers represented by*

$$g = bu^2 + av^2 + dz^2 \tag{2}$$

is given by $g=abf$. *The variables* u *and* v *are given by*

$$u = ax + sz, \quad v = by + rz, \quad \text{and} \quad z = z. \tag{3}$$

$abf=g$ may be obtained directly by first multiplying f by a and then the resulting equation, when simplified, by ab. Dividing the previous equation by a and substituting the expression $abc-bs^2-ar^2$ for d, we obtain (2). Next we observe that for every integer represented by f, the corresponding value of g is an integer and a multiple of ab. For a given set of integral values u, v, and z for which g is a multiple of ab, and $v\equiv 0 \pmod{\Omega}$, we must show that x and y may be taken to be integers. $g/\Omega\equiv 0 \pmod{q^2}$ implies from

$$-\frac{g}{\Omega} = aq^2 f = q^2 u^2 - a\Omega v_1^2 - \Omega\Delta z^2, \qquad v = \Omega v_1, \tag{4}$$

that

$$a\Omega v_1^2 \equiv -\Omega\Delta z^2 \pmod{q^2}. \tag{5}$$

From $\Omega^2\Delta=d=\Omega q^2 s^2-a(\Omega c q^2+r^2)$,

$$-\Omega^2\Delta z^2 \equiv a\Omega^2 r'^2 z^2 \pmod{q^2} \tag{6}$$

for $r=\Omega r'$. Since $(a\Omega, q)=1$ we have from (5) and (6)

$$v_1 \equiv \pm r'z \pmod{q^2}. \tag{7}$$

Hence by choosing the plus sign in (7) it is seen by (3) that y

$=(v-rz)/b=(\Omega v_1-\Omega r'z)/-\Omega q^2=-(v_1-r'z)/q^2$ is an integer. If $a=p^2$, then $g\equiv 0 \pmod{p^2}$ implies by (2) that $bu^2\equiv -dz^2 \pmod{p^2}$. But $d=abc-ar^2-bs^2$. Hence $-d\equiv bs^2 \pmod{p^2}$ so that $bu^2\equiv bs^2z^2 \pmod{p^2}$. Since $(b, p)=1$, then $u\equiv \pm sz \pmod{p^2}$ and by (3) $x=(u-sz)/p^2$ is an integer when the plus sign is chosen in the previous congruence. Moreover it follows by (2) and the expression for d that f is an integer when z is given and $u=ak_1+sz$, $v_1=q^2k_2+r'z$, and k_1, k_2 have arbitrary integral values.

LEMMA 3. *If Ω' is an odd square and Δ' a negative odd square, if Ω'' and Δ'' are each odd powers of 2 and $\Omega''\Delta''\geqq 64$, then*

$$f = ax^2 - \Omega q^2y^2 + cz^2 + 2r'\Omega yz + 2sxz, \qquad a = 1 \text{ or } p^2 \tag{8}$$

of Lemma 1 represents primitively no γ^2 where $(\gamma, pq\Omega\Delta)=1$, $\gamma\equiv \pm 3a^{1/2} \pmod 8$ and neither of the distinct primes $p\equiv 1 \pmod 4$ nor $q\equiv 1$ or $-1 \pmod 8$ divides $\Omega\Delta$.

If $f=\gamma^2$ has a primitive solution (x, y, z), then u, v_1, z can have no common prime factors except p and q. For suppose a prime g divides z, u, and v_1 and is prime to p and q. Then from (3) it divides x, y, and z. In fact, if $a=p^2$ and $p\equiv 5 \pmod 8$, p cannot divide z since $f=\gamma^2$, $z\equiv 0 \pmod p$ implies $\gamma^2\equiv -\Omega q^2 \pmod p$ and

$$\left(\frac{-\Omega}{p}\right)=\left(\frac{-2}{p}\right)=-1.$$

Then, by (4),

$$(qu)^2 - \Omega a v_1^2 = a(q\gamma)^2 + \Omega\Delta z^2. \tag{9}$$

From (9)

$$(qu)^2 - \Omega(a^{1/2}v_1)^2 = \rho\sigma \tag{10}$$

where

$$\rho = q\gamma a^{1/2} + (-\Omega\Delta)^{1/2}z, \qquad \sigma = q\gamma a^{1/2} - (-\Omega\Delta)^{1/2}z. \tag{11}$$

Now $\rho\equiv\sigma\equiv q\gamma a^{1/2}\equiv \pm 3 \pmod 8$ and hence $(\Omega \mid |\theta|)=(2\mid |\theta|)=-1$ where $\theta=\rho$ or σ. Hence there is a prime p_θ dividing θ to an odd power which is $\equiv \pm 3 \pmod 8$. When $p\equiv 1 \pmod 8$, $p\neq p_\theta\equiv \pm 3 \pmod 8$. When $p\equiv 5 \pmod 8$, then $p_\theta\neq p$ since $z\not\equiv 0 \pmod p$; $p_\theta\neq q$ since $q\equiv 1$ or $-1 \pmod 8$. Then $(\Omega\mid p_\theta)=(2\mid p_\theta)=-1$ and (10) implies $qu\equiv a^{1/2}v_1\equiv 0 \pmod{p_\theta}$. Hence $u\equiv v_1\equiv 0 \pmod{p_\theta}$ and p_θ is therefore prime to z. If p_θ divided both ρ and σ it would divide $q\gamma a^{1/2}$ and $\Omega\Delta z$ which we have just shown is impossible. Hence p_θ occurs to an even power in the left side of (10) and to an odd power on the right which is impossible.

THEOREM. *If* Ω' *is an odd square,* Δ' *is a negative odd square,* Ω'' *and* Δ'' *are each odd powers of* 2, $\Omega''\Delta''\geqq 64$, *each of the quadratic characters with respect to* Ω *and the characters with respect to* 4 *and* 8 *have the value one, then there exist genera of properly primitive indefinite forms containing at least two classes.*

For f of Lemma 1, define $f_1=f$ when $a=1$ or $a=p^2$ and $p\equiv 1 \pmod 8$, $f_2=f$ when $a=p^2$ and $p\equiv 5 \pmod 8$. For f_1 and f_2 take $b=-\Omega q^2$, $t=0$ and then s, r, and c are determined as in Lemma 1. From Lemma 1 it is seen that

$$\left(\frac{F}{q_\Delta}\right)=\left(\frac{-1}{q_\Delta}\right)$$

depends only upon Δ so that f_1 and f_2 belong to the same genus of forms. By Lemma 3, f_1 represents primitively no γ^2 where $\gamma\equiv\pm 3$ (mod 8) and f_2 represents primitively no γ^2 where $\gamma\equiv\pm 1$ (mod 8). Therefore the genus containing f_1 and f_2 contains at least two classes since neither f_1 nor f_2 belong to the same class. For there exists no odd square represented primitively by both f_1 and f_2. Since Ω and Δ may have different values subject to the restrictions imposed upon them in the hypothesis, it follows that genera of properly primitive indefinite forms containing at least two classes exist.

EXAMPLE. Given $\Omega=18$, $\Delta=-3872$, and $q=7$, then $b=-\Omega q^2=-882$. First take $p=17\equiv 1$ (mod 8) so that $a=p^2=289$. Then $q_1=59$, $s=112$, $A=-2368$, $\Omega_2=-19$, $r'=23$, $r=414$, $c=-146$. Second take $p=5\equiv 5$ (mod 8) so that $a=p^2=25$. Then $q_1=-1$, $s=14$, $A=-3172$, $r'=10$, $r=180$, and $c=28$. According to the definitions of f_1 and f_2 of the theorem, $f_1=289x^2-882y^2-146z^2+828yz+224xz$ and $f_2=25x^2-882y^2+28z^2+360yz+28xz$. The forms f_1 and f_2 have the same value $\Omega^2\Delta=-1{,}254{,}528$ for their determinants. f_1 and f_2 belong to the same genus of forms, but they do not belong to the same class.

UNIVERSITY OF COLORADO AND
UNIVERSITY OF FLORIDA