Acta Math. Univ. Comenianae
Vol. LXI, 1(1992), pp. 91–93

DIFFERENCES BETWEEN VALUES OF A QUADRATIC FORM

A. SCHINZEL

J. W. S. Cassels, A. Pfister and the writer proved independently in 1989 the following theorem: let $f(x,y)$ be a primitive quadratic form, n an odd integer. Then n is a difference of two values of f over $\mathbb{Z}$ (see [**2**], Proposition 4.3). Using this result J. Bochnak proved (unpublished) that the same condition holds if either the discriminant of f is not divisible by 16 or $n \not\equiv 2 \pmod 4$. The aim of this paper is to prove the following more general theorem.

Theorem. *Let f be a primitive quadratic form in k variables, $n \in \mathbb{Z}$. If either $f \not\equiv \pm g^2$ (mod 4) for every linear form g or $n \not\equiv 2$ (mod 4), then n is a difference of two values of f and for $k > 1$ in infinitely many ways.*

Proof. Let us consider the representation of n by

$$f(x_1, \dots, x_k) - f(x_{k+1}, \dots, x_{2k}) = f \perp (-f)$$

in the ring of p-adic integers $\mathbb{Z}_p$. If p is odd, we have (see [**3**], Theorem 33)

$$f \sim f_0 \perp p f_1 \perp \cdots \perp p^l f_l = h,$$

where f_j is either 0 or a form of a unit determinant in $\mathbb{Z}_p$. Since f is primitive we have $f_0 \neq 0$ and by the quoted theorem

$$f_0 = \sum_{i=1}^{m} a_i x_i^2, \qquad m \geq 1.$$

We take

$$x_1 = \frac{n + a_1}{2a_1}, \qquad x_{k+1} = \frac{n - a_1}{2a_1}$$

and since $x_1 - x_{k+1} = 1$

$$h(x_1, 0, \dots, 0) - h(x_{k+1}, 0, \dots, 0) = n$$

Received November 25, 1991.
1980 *Mathematics Subject Classification* (1991 *Revision*). Primary 11E25.

is a representation of n by $h\perp(-h)$, hence there exists a representation of n by $f\perp(-f)$ in $\mathbb{Z}_p$. For $p=2$ consider first the case of f non-classic and apply Theorem 33a of [**3**] to $2f$. We obtain

$$2f \sim f_0 \perp 2f_1 \perp \cdots \perp 2^l f_l = 2h, \tag{1}$$

where f_j is either 0 or a form of a unit determinant in $\mathbb{Z}_2$. Since f is primitive and non-classic we have $f_0 \neq 0$ and by Theorem 33a either $f_0 = 2x_1x_2 + g_0(x_3, \ldots, x_m)$ or $f_0 = 2x_1^2 + 2x_1x_2 + 2x_2^2 + g_0(x_3, \ldots, x_m)$.

In the first case we have

$$h(n, 1, 0, \ldots, 0) - h(0, \ldots, 0) = n,$$

in the second case

$$h(n-1, 1, 0, \ldots, 0) - h(n-1, 0, \ldots, 0) = n,$$

thus n is represented by $f\perp(-f)$.

Assume now that f is classic. Then by Theorem 33 of [**3**]

$$f \sim f_0 \perp 2f_1 \perp \cdots \perp 2^l f_l = g,$$

where f_i satisfy the same conditions as in formula (1). Since f is primitive we have $f_0 \neq 0$ and by Theorem 33 of [**3**]

$$f_0 = \sum_{i=1}^{m_0} a_i x_i^2, \qquad a_i \text{ odd} \qquad m_0 \geq 1.$$

If $n \equiv 1 \pmod 2$ we have the representation

$$h\left(\frac{n+a_1}{2a_1}, 0, \ldots, 0\right) - h\left(\frac{n-a_1}{2a_1}, 0, \ldots, 0\right) = n.$$

If $n \equiv 2 \pmod 4$ we use $f \not\equiv \pm g^2 \pmod 4$, hence either $m_0 \geq 2$ or $m_0 = 1$,

$$f_1 = \sum_{i=2}^{1+m_1} a_i x_i^2, \qquad a_i \text{ odd} \qquad m_1 \geq 1.$$

In the first case we have the representation

$$h\left(\frac{n+a_1-a_2}{2a_1}, 1, 0, \ldots, 0\right) - h\left(\frac{n-a_1-a_2}{2a_1}, 0, \ldots, 0\right) = n.$$

In the second case, we have the representation

$$h\left(0,\frac{n+2a_2}{4a_2},0,\dots,0\right)-h\left(0,\frac{n-2a_2}{4a_2},0,\dots,0\right)=n.$$

If $n\equiv 0 \pmod 4$ we have the representation

$$h\left(\frac{n}{4a_1}+1,0,\dots,0\right)-h\left(\frac{n}{4a_1}-1,0,\dots,0\right)=n.$$

Thus in every case we have a representation of n by $f\perp(-f)$ in every $\mathbb{Z}_p$, hence by Lemma 4.1, Chapter 7 and Theorem 1.5, Chapter 9 of [**1**] if rank of $f\geq 2$, n has a representation by $f\perp(-f)$. If rank of $f=1$, $f=\varepsilon g^2$, where $\varepsilon=\pm 1$, g is a linear form, hence $n\not\equiv 2 \pmod 4$ and we solve $g(x_1,\dots,x_k)=\frac{\varepsilon n+1}{2}$, $g(x_{k+1},\dots,x_{2k})=\frac{\varepsilon n-1}{2}$ (n odd) or $g(x_1,\dots,x_k)=\frac{\varepsilon n}{4}+1$, $g(x_{k+1},\dots,x_{2k})=\frac{\varepsilon n}{4}-1$ ($n\equiv 0 \bmod 4$).

It remains to prove that if $k>1$ the number of representations is infinite. Let

$$f=\sum_{i=1}^{k}a_ix_i^2+\sum_{i<j}^{k}a_{ij}x_ix_j.$$

The equation

$$f(x_1,\dots,x_k)-f(x_1-r_1,\dots,x_k-r_k)=n \tag{2}$$

is equivalent to

$$\sum_{j=1}^{k}x_j\left(2a_jr_j+\sum_{j<k}a_{jk}r_k+\sum_{i<j}a_{ij}r_i\right)=n+f(r_1,\dots,r_k).$$

Hence if for $k>1$ and some $r_1,\dots,r_k$ (2) has one solution in integers it has infinitely many.

References

1. Cassels J. W. S., *Rational quadratic forms*, Academic Press, 1978.
2. Huisman J., *The underlying real algebraic structure of complex elliptic curves* (to appear).
3. Jones B. W., *The arithmetic theory of quadratic forms*, J. Wiley, 1950.

A. Schinzel, Mathematical Institute PAN, P.O.Box 137, 00-950 Warszawa, Poland