Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 51 (2005)
Heft: 3-4: L'enseignement mathématique

Artikel: On successive minima of indefinite quadratic forms
Autor: Bochnak, J. / Kucharz, W.
DOI: https://doi.org/10.5169/seals-3600

L'Enseignement Mathématique, t. 51 (2005), p. 319–330

ON SUCCESSIVE MINIMA OF INDEFINITE QUADRATIC FORMS

by J. BOCHNAK and W. KUCHARZ *)

1. INTRODUCTION

The classical theorem of Minkowski on successive minima of definite quadratic forms (cf. [6] or [3], p. 205) can be stated as follows:

THEOREM 1.1 (Minkowski). *Let g be a non-singular positive definite quadratic form in n variables with real coefficients. Then there are n linearly independent points $a_1, \ldots, a_n$ in $\mathbf{Z}^n$ such that*

$$g(a_1) \cdots g(a_n) \leq \gamma_n^n D(g),$$

where γ_n is the Hermite constant.

In the statement above, $D(g)$ is the determinant of g, that is, $D(g) = \det(g_{ij})$, where $g = \sum g_{ij} x_i x_j$ with $g_{ij} = g_{ji}$. Recall that the *Hermite constant* γ_n is defined as follows. Let $\mathcal{E}_n$ be the set of all non-singular positive definite quadratic forms in n variables with real coefficients. For any g in $\mathcal{E}_n$ put

$$\gamma(g) = \inf\left\{ \frac{g(x)}{D(g)^{\frac{1}{n}}} \mid x \in \mathbf{Z}^n,\ g(x) > 0 \right\}.$$

Then, by definition,

$$\gamma_n = \sup\{\gamma(g) \mid g \in \mathcal{E}_n\}.$$

Only the first 8 values of γ_n (and $\gamma_{24} = 4$) are known explicitly. Clearly, since $\gamma(g)^n \leq \gamma_n^n$, the constant γ_n^n in the Minkowski theorem is optimal; it cannot be replaced by a smaller one.

*) Both authors acknowledge with gratitude the support of the Research in Pairs program at the Mathematisches Forschungsinstitut Oberwolfach.

The goal of this paper is to prove an analogous theorem for indefinite quadratic forms.

First, given integers n and s with $n \geq 1$, define the Watson number $w_{n,s}$ by setting

$$w_{n,s} = c_{n,s} 2^{\{n\}},$$

where $\{n\} = n$ for n even, $\{n\} = n - 1$ for n odd, and

$$c_{n,s} = \begin{cases} 1 \\ 1/2 \\ 1/3 \\ 1/4 \end{cases} \quad \text{for} \quad s \equiv \begin{cases} 0 \text{ or } \pm 1 & (\mathrm{mod}\ 8) \\ \pm 3 & (\mathrm{mod}\ 8) \\ \pm 2 & (\mathrm{mod}\ 8) \\ 4 & (\mathrm{mod}\ 8). \end{cases}$$

One has $\gamma_n^n = w_{n,n}$ if $n \leq 8$ (this result is classical, due to Gauss for $n \leq 3$, Korkine and Zolotareff for $n = 4, 5$, and Blichfeldt for $n = 6, 7, 8$; for the references see [3], p. 332).

Let $\mathcal{E}_{n,s}$ be the set of all non-singular real quadratic forms in n variables with signature s (in particular $\mathcal{E}_n = \mathcal{E}_{n,n}$). Again, we can define the "Hermite constant" $\alpha_{n,s}$ of $\mathcal{E}_{n,s}$ imitating the definition of γ_n. For any f in $\mathcal{E}_{n,s}$ let

$$\alpha(f) = \inf \left\{ \frac{|f(x)|}{|D(f)|^{\frac{1}{n}}} \;\middle|\; x \in \mathbf{Z}^n,\ |f(x)| > 0 \right\}$$

and let

$$\alpha_{n,s} = \sup\{\alpha(f) \mid f \in \mathcal{E}_{n,s}\}.$$

Contrary to the case of positive definite forms, the numbers $\alpha_{n,s}$ with $|s| < n$ are known explicitly. By a theorem of Watson (cf. [8], [9]), for $n \geq 2$ and $|s| < n$, one has

$$\alpha_{n,s}^n = w_{n,s}.$$

The inequality $\alpha_{n,s}^n \geq w_{n,s}$ is proved in [9] by explicitly exhibiting a form $f_{n,s}$ in $\mathcal{E}_{n,s}$, with coefficients in $\mathbf{Z}$, satisfying

$$\alpha(f_{n,s})^n = w_{n,s}.$$

We shall only need the existence of such a form $f_{n,s}$. Our main result can be regarded as a theorem on successive minima for indefinite quadratic forms.

THEOREM 1.2. *For any indefinite quadratic form f in $\mathcal{E}_{n,s}$ there are n linearly independent points $a_1, \ldots, a_n$ in $\mathbf{Z}^n$ such that*

$$0 < |f(a_1) \cdots f(a_n)| \leq w_{n,s} |D(f)|.$$

Moreover, the constant $w_{n,s}$ is optimal.

Clearly, the inequality $\alpha_{n,s}^n \geq w_{n,s}$, mentioned above implies the optimality of the constant $w_{n,s}$ in Theorem 1.2. Observe that our theorem implies $\alpha_{n,s}^n = w_{n,s}$.

To the best of our knowledge no results similar to Theorem 1.2 are known, except the contributions of Barnes ([1], [2]), in which he considers an analogous problem for forms in 2 and 3 variables not representing 0 over $\mathbf{Z}$. We wish to thank Professor A. Schinzel who informed us about Barnes' papers. The proof of Theorem 1.2 depends on a relatively recent result of Margulis [5] about the density of values of irrational indefinite quadratic forms at integral points (cf. Section 2). It seems probable that any attempt at proving Theorem 1.2 prior to Margulis' result would be either unsuccessful or would require very long and complicated computation.

Theorems 1.1 and 1.2 can be placed in a larger context of classical investigations in the geometry of numbers, concerning the problem of successive minima of "distance functions" (cf. [3], Chap. 8 for more information). Recall that a distance function $\eta : \mathbf{R}^n \to \mathbf{R}$ is simply a non-negative continuous function satisfying $\eta(tx) = |t|\eta(x)$ for all t in $\mathbf{R}$ and x in $\mathbf{R}^n$. For any positive real number λ, put

$$S_\lambda = \{x \in \mathbf{R}^n \mid 0 < \eta(x) < \lambda\}$$

(in the literature the inequality $0 < \eta(x)$ is often omitted, which does not affect the problem under consideration if $\eta^{-1}(0) = \{0\}$). Given a lattice $\Lambda \subset \mathbf{R}^n$ of rank n, one defines the kth successive minimum $\lambda_k = \lambda_k(\eta, \Lambda)$ of the distance function η with respect to Λ to be the infimum of the positive real numbers λ such that the set S_λ contains k linearly independent lattice points. Clearly

$$\lambda_1 \leq \cdots \leq \lambda_n$$

and

$$\lambda_1 = \inf\{\eta(x) \mid x \in \Lambda,\ 0 < \eta(x)\}.$$

Let

$$\lambda(\eta) = \sup_\Lambda \frac{\lambda_1^n}{d(\Lambda)}, \qquad \overline{\lambda}(\eta) = \sup_\Lambda \frac{\lambda_1 \cdots \lambda_n}{d(\Lambda)},$$

where $d(\Lambda)$ is the determinant of Λ. If $\lambda(\eta) > 0$, the quotient

$$A_\eta = \frac{\overline{\lambda}(\eta)}{\lambda(\eta)} \geq 1$$

is called the *anomaly* of η. Numerous works of Rogers, Chabauty, Mahler, Rankin and others show that A_η is quite often strictly greater than 1 (cf. [3],

Chap. 8 for references). The situation where A_η equals 1 seems to be counter-intuitive.

Statements about different quadratic forms in $\mathcal{E}_{n,s}$ at integral points are equivalent to statements about the single form

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_n^2, \quad p = \frac{n+s}{2}$$

and different lattices (cf.[3], pp. 20-23). It follows that Theorem 1.1 (resp. Theorem 1.2) implies that for $\eta = |x_1^2 + \cdots + x_n^2|^{\frac{1}{2}}$ (resp. $\eta = |x_1^2 + \cdots + x_l^2 - x_{l+1}^2 - \cdots - x_n^2|^{\frac{1}{2}}$, where $l = \frac{n+s}{2}$ and $|s| < n$), the anomaly A_η is equal to 1.

2. Strategy for the proof of Theorem 1.2

The strategy for the proof of Theorem 1.2 is inspired by Watson's papers [8] and [9], dealing with the problem of finding absolute positive normalized minima of forms in $\mathcal{E}_{n,s}$.

Let $T(n,s)$ be the statement of Theorem 1.2 for the pair of integers (n,s) (necessarily satisfying $n \geq 2$, $|s| < n$, $n \equiv s \pmod 2$). In the subsequent sections we shall prove the following three assertions:

(A) $T(n, n-2)$ holds for $2 \leq n \leq 6$ (cf. Corollary 3.3).

(B) For $n \geq 2$, $T(n,s) \Rightarrow T(n+2,s)$ (cf. Corollary 4.2).

(C) If $s \equiv s' \pmod 8$, then $T(n,s') \Rightarrow T(n,s)$ (cf. Corollary 5.2).

Assuming these assertions we now prove Theorem 1.2.

Proof of Theorem 1.2. Making use of (A) and (B), it follows by induction that $T(n,s)$ holds for all $n \geq 2$ and s satisfying $0 \leq s \leq 4$ (s subject to the usual restrictions $|s| < n$, $n \equiv s \pmod 2$). Since $T(n,s)$ trivially implies $T(n,-s)$, we conclude that $T(n,s)$ holds for $|s| \leq 4$. The following table, in which $T(n,s)$ is abbreviated to (n,s), helps to understand the situation:

n/s	-5	-4	-3	-2	-1	0	1	2	3	4	5
2						$(2,0)$					
3					$(3,-1)$	$\downarrow$	$(3,1)$				
4				$(4,-2)$		$(4,0)$	$\downarrow$	$(4,2)$			
5			$(5,-3)$		$(5,-1)$	$\downarrow$	$(5,1)$	$\downarrow$	$(5,3)$		
6		$(6,-4)$		$(6,-2)$		$(6,0)$	$\downarrow$	$(6,2)$	$\downarrow$	$(6,4)$	
7	$(7,-5)$		$(7,-3)$		$(7,-1)$	$\downarrow$	$(7,1)$	$\downarrow$	$(7,3)$	$\downarrow$	$(7,5)$
						$\vdots$		$\vdots$		$\vdots$	

In order to prove $T(n,s)$ in the remaining cases, that is for $|s| > 4$, we choose s' with $|s'| \leq 4$ and $s \equiv s' (\mathrm{mod}\ 8)$. Since we have already demonstrated that $T(n,s')$ holds, so does $T(n,s)$ in view of (C). The proof of Theorem 1.2 is complete. □

The next proposition reduces the proof of assertions (A), (B) and (C) to the case of forms with coefficients in $\mathbf{Z}$, at least when $n \geq 3$. Recall that a form in $\mathcal{E}_{n,s}$ is said to be irrational if it is not a multiple of a form with coefficients in $\mathbf{Z}$. By the celebrated result of Margulis [5], for every non-singular indefinite irrational form f in $n \geq 3$ variables the set $f(\mathbf{Z}^n)$ is dense in $\mathbf{R}$.

PROPOSITION 2.1. *Let f be a non-singular indefinite irrational form in $n \geq 3$ variables. Then for every $\varepsilon > 0$ there are linearly independent points $a_1, \ldots, a_n$ in $\mathbf{Z}^n$ such that*

$$0 < |f(a_1) \cdots f(a_n)| < \varepsilon .$$

Proof. Let $b_1, \ldots, b_n$ be linearly independent points in $\mathbf{Z}^n$ such that $f(b_i) \neq 0$ for all i. Let

$$\mu = \max \{|f(b_i)| \mid 1 \leq i \leq n\} .$$

By Margulis' theorem there exists an integral point x such that

$$0 < |f(x)| < \varepsilon / \mu^{n-1} .$$

Write $x = \Sigma \lambda_i b_i$, where λ_i is in $\mathbf{R}$ for all i, and choose k with $\lambda_k \neq 0$. Set $a_i = b_i$ for $i \neq k$ and $a_k = x$. Then the integral points $a_1, \ldots, a_n$ are linearly independent, and $0 < |f(a_1) \ldots f(a_n)| < \varepsilon$, as required. □

For any f in $\mathcal{E}_{n,s}$ set

$$\beta(f) = \min \left\{ \frac{|f(a_1) \cdots f(a_n)|}{|D(f)|} \;\middle|\; a_1, \ldots, a_n \in \mathbf{Z}^n \text{ are linearly independent, and } f(a_i) \neq 0 \text{ for } 1 \leq i \leq n \right\}.$$

Let $\mathcal{E}_{n,s}(\mathbf{Z})$ denote the subset of $\mathcal{E}_{n,s}$ consisting of all forms with coefficients in $\mathbf{Z}$ and let

$$\beta_{n,s} = \sup \{\beta(f) \mid f \in \mathcal{E}_{n,s}(\mathbf{Z})\} .$$

Clearly, $\alpha(f)^n \leq \beta(f)$ for all f in $\mathcal{E}_{n,s}(\mathbf{Z})$, and hence the equality $\alpha(f_{n,s})^n = w_{n,s}$, preceding the statement of Theorem 1.2, implies

$$w_{n,s} \leq \beta_{n,s}\,. \tag{2.2}$$

The following corollary is an immediate consequence of Proposition 2.1.

COROLLARY 2.3. *Let $n \geq 3$ and $|s| < n$. Then $T(n,s)$ holds if and only if $w_{n,s} = \beta_{n,s}$.*

3. PROOF OF $T(n, n-2)$ FOR $2 \leq n \leq 6$

LEMMA 3.1. *$T(2,0)$ holds true.*

Proof. Let f be in $\mathcal{E}_{2,0}$. If $f(y) = 0$ for some $y \in \mathbf{Z}^2 \setminus \{0\}$, then f is equivalent over $\mathbf{Z}$ to $ax_1x_2 + bx_2^2$ for some real numbers a and b satisfying $0 \leq b < a$. In particular, $|D(f)| = a^2/4$. Let c_1 and c_2 be linearly independent points in $\mathbf{Z}^2$ with $0 < |f(c_i)| \leq a$ for $i = 1,2$. Then

$$0 < |f(c_1)f(c_2)| \leq a^2 = 4|D(f)| = w_{2,0}|D(f)|\,,$$

which proves $T(2,0)$ for f as above.

Suppose $f(x) \neq 0$ for all x in $\mathbf{Z}^2 \setminus \{0\}$. Then $f = \xi_1^2 - \xi_2^2$, where ξ_1 and ξ_2 are linear forms. The quadratic form $h = \xi_1^2 + \xi_2^2$ is in $\mathcal{E}_2$, $D(h) = |D(f)|$, and $0 < |f(x)| \leq h(x)$ for all x in $\mathbf{Z}^2 \setminus \{0\}$. By Theorem 1.1, there exist linearly independent points a_1 and a_2 in $\mathbf{Z}^2$ such that

$$h(a_1)h(a_2) \leq \gamma_2^2 D(h)\,.$$

Since $\gamma_2^2 = w_{2,2} < w_{2,0}$, we get

$$0 < |f(a_1)f(a_2)| \leq h(a_1)h(a_2) < w_{2,0}D(h) = w_{2,0}|D(f)|\,,$$

which completes the proof. □

Henceforth it is sufficient for our purposes to consider quadratic forms with coefficients in $\mathbf{Z}$. However, forms with other coefficients will also appear in some proofs.

LEMMA 3.2. *Let f be in $\mathcal{E}_{n,n-2}(\mathbf{Z})$, where $n \geq 3$.*

(i) *If $f(x) = 0$ for some x in $\mathbf{Z}^n \setminus \{0\}$, then $\beta(f) \leq 4\gamma_{n-2}^{n-2}$.*

(ii) *If $f(x) \neq 0$ for all x in $\mathbf{Z}^n \setminus \{0\}$, then $\beta(f) \leq \gamma_n^n$.*

Proof. (i) The quadratic form f is equivalent over $\mathbf{Z}$ to

$$x_2(ax_1 + a_2x_2 + \cdots + a_nx_n) + g(x_3, \ldots, x_n),$$

where $0 \leq a_2 < a$ and g is in $\mathcal{E}_{n-2,n-2}(\mathbf{Z})$ (g is thus positive definite). Let $c_1 = (-1, 1, 0, \ldots, 0) \in \mathbf{Z}^n$ and

$$c_2 = \begin{cases} (0, 1, 0, \ldots, 0) \in \mathbf{Z}^n & \text{if } a_2 \neq 0 \\ (1, 1, 0, \ldots, 0) \in \mathbf{Z}^n & \text{if } a_2 = 0. \end{cases}$$

Then c_1 and c_2 are linearly independent and

$$0 < |f(c_i)| \leq a \qquad \text{for} \qquad i = 1, 2.$$

By Theorem 1.1, there are linearly independent points $\overline{c_3}, \ldots, \overline{c_n}$ in $\mathbf{Z}^{n-2}$ such that

$$0 < g(\overline{c_3}) \cdots g(\overline{c_n}) \leq \gamma_{n-2}^{n-2} D(g).$$

Let $c_i = (0, 0, \overline{c_i}) \in \mathbf{Z}^n$ for $i = 3, \ldots, n$. Clearly, $f(c_i) = g(\overline{c_i})$ for $i = 3, \ldots, n$. Since $|D(f)| = \frac{a^2}{4} D(g)$, it follows that for the linearly independent points $c_1, c_2, \ldots, c_n$ in $\mathbf{Z}^n$ one has

$$0 < |f(c_1) \cdots f(c_n)| \leq a^2 g(\overline{c_3}) \cdots g(\overline{c_n}) \leq a^2 \gamma_{n-2}^{n-2} D(g) = 4\gamma_{n-2}^{n-2} |D(f)|,$$

which implies the required inequality $\beta(f) \leq 4\gamma_{n-2}^{n-2}$.

(ii) The quadratic form f can be written as $f = \xi_1^2 + \cdots + \xi_{n-1}^2 - \xi_n^2$, where the ξ_i are linear forms in n variables with real coefficients. The quadratic form $h = \xi_1^2 + \cdots + \xi_n^2$ satisfies $D(h) = |D(f)|$ and $0 < |f(x)| \leq h(x)$ for all x in $\mathbf{Z}^n \setminus \{0\}$. Since h is non-singular and positive definite, Theorem 1.1 implies, $\beta(h) \leq \gamma_n^n$, and hence $\beta(f) \leq \beta(h) \leq \gamma_n^n$. □

As already mentioned in Section 1, $\gamma_n^n = w_{n,n}$ for $n \leq 8$. However, only the values of γ_n for $n \leq 4$ are needed in this paper. In particular, one has the following table (where $\gamma_0^0 = 1$ by definition):

n	2	3	4	5	6
γ_n^n	4/3	2	4		
$4\gamma_{n-2}^{n-2}$	4	4	16/3	8	16
$w_{n,n-2}$	4	4	16/3	8	16

COROLLARY 3.3. *$T(n, n-2)$ holds for $2 \leq n \leq 6$.*

Proof. $T(2, 0)$ is proved in Lemma 3.1. Hence by (2.2) and Corollary 2.3, it suffices to show $\beta_{n,n-2} \leq w_{n,n-2}$ for $3 \leq n \leq 6$. To this end let f be in $\mathcal{E}_{n,n-2}(\mathbf{Z})$.

If $n = 3$ or $n = 4$, then Lemma 3.2 and the table above imply

$$\beta(f) \leq \max\{4\gamma_{n-2}^{n-2},\ \gamma_n^n\} = 4\gamma_{n-2}^{n-2} = w_{n,n-2}\,.$$

If $n = 5$ or $n = 6$, then by Meyer's theorem (cf. [7], p. 43), $f(x) = 0$ for some x in $\mathbf{Z}^n \setminus \{0\}$. Hence in view of Lemma 3.2 (i) and the table,

$$\beta(f) \leq 4\gamma_{n-2}^{n-2} = w_{n,n-2}\,.$$

Thus the required inequality is proved for $3 \leq n \leq 6$. □

4. Proof of the implication $T(n, s) \Rightarrow T(n + 2, s)$

Proposition 4.1. *Let n and s be integers satisfying $n \geq 2$, $|s| < n$, and $n \equiv s \pmod 2$. Then*

$$\beta_{n+2,s} \leq 4\beta_{n,s}\,.$$

Proof. We have to show that

$$\beta(f) \leq 4\beta_{n,s}$$

for all f in $\mathcal{E}_{n+2,s}(\mathbf{Z})$.

First consider the case $(n, s) = (2, 0)$ with f in $\mathcal{E}_{4,0}(\mathbf{Z})$ satisfying $f(x) \neq 0$ for all x in $\mathbf{Z}^4 \setminus \{0\}$. Such an f can be written as $f = \xi_1^2 + \xi_2^2 - \xi_3^2 - \xi_4^2$, where the ξ_i are linear forms in 4 variables with real coefficients. The quadratic form $h = \xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2$ is non-singular and positive definite, and hence Theorem 1.1 implies

$$\beta(h) \leq \gamma_4^4 = 4\,.$$

Since $D(h) = |D(f)|$, $0 < |f(x)| \leq h(x)$ for all x in $\mathbf{Z}^4 \setminus \{0\}$, one has

$$\beta(f) \leq \beta(h) \leq 4 \leq 4\beta_{2,0}\,,$$

the last inequality being a consequence of an obvious one, $\beta_{2,0} \geq 1$.

Assume now that f is in $\mathcal{E}_{n+2,s}(\mathbf{Z})$, $n \geq 2$, and $f(x) = 0$ for some x in $\mathbf{Z}^{n+2} \setminus \{0\}$ (if $n \geq 3$, the last condition is automatically satisfied due to Meyer's theorem). It follows that f is equivalent over $\mathbf{Z}$ to the quadratic form

$$x_2(a_1x_1 + a_2x_2 + \cdots + a_{n+2}x_{n+2}) + g(x_3, \ldots, x_{n+2})\,,$$

where the a_i are integers, $0 \leq a_2 < a_1$, and g is in $\mathcal{E}_{n,s}(\mathbf{Z})$. Clearly,

$$4|D(f)| = a_1^2|D(g)|\,.$$

Let $\overline{b_1}, \ldots, \overline{b_n}$ be linearly independent points in $\mathbf{Z}^n$ such that

$$0 < |g(\overline{b_1}) \cdots g(\overline{b_n})| \leq \beta_{n,s}|D(g)|\,.$$

Setting $b_i = (0, 0, \overline{b_i}) \in \mathbf{Z}^{n+2}$, one has

$$f(b_i) = g(\overline{b_i}) \quad \text{for} \quad 1 \leq i \leq n\,.$$

For $c_1 = (-1, 1, 0, \ldots, 0) \in \mathbf{Z}^{n+2}$ and

$$c_2 = \begin{cases} (0, 1, 0, \ldots, 0) \in \mathbf{Z}^{n+2} & \text{if } a_2 \neq 0 \\ (1, 1, 0, \ldots, 0) \in \mathbf{Z}^{n+2} & \text{if } a_2 = 0\,, \end{cases}$$

the following inequalities are satisfied:

$$0 < |f(c_j)| \leq a_1 \quad \text{for} \quad j = 1, 2\,.$$

Hence for the linearly independent points $c_1, c_2, b_1, \ldots, b_n$ in $\mathbf{Z}^{n+2}$, one has

$$\begin{aligned} 0 < |f(c_1)f(c_2)f(b_1)\cdots f(b_n)| &\leq a_1^2|g(\overline{b_1})\cdots g(\overline{b_n})| \\ &\leq a_1^2\beta_{n,s}|D(g)| \leq 4\beta_{n,s}|D(f)|\,, \end{aligned}$$

which implies $\beta(f) \leq 4\beta_{n,s}$. □

COROLLARY 4.2. *For each $n \geq 2$, $T(n, s)$ implies $T(n + 2, s)$.*

Proof. According to (2.2) and Lemma 3.1, $T(2, 0)$ is equivalent to the equality $\beta_{2,0} = w_{2,0}$. Hence, by Corollary 2.3, it suffices to show that if $\beta_{n,s} = w_{n,s}$, then $\beta_{n+2,s} = w_{n+2,s}$. This can be done as follows. Since $w_{n+2,s} = 4w_{n,s}$, Proposition 4.1 implies

$$\beta_{n+2,s} \leq 4\beta_{n,s} = 4w_{n,s} = w_{n+2,s}\,.$$

Thus $\beta_{n+2,s} \leq w_{n+2,s}$, which combined with (2.2) gives $\beta_{n+2,s} = w_{n+2,s}$. □

5. PROOF OF THE IMPLICATION $T(n, s') \Rightarrow T(n, s)$

PROPOSITION 5.1. *Let f be in $\mathcal{E}_{n,s}(\mathbf{Z})$ and let s' be an integer satisfying $|s'| \leq n$ and $s \equiv s' (\mathrm{mod}\ 8)$. Then there is a form f' in $\mathcal{E}_{n,s'}(\mathbf{Z})$ such that for every prime number p, the forms f and f' are equivalent over the ring $\mathbf{Z}_p$ of p-adic integers. In particular, $D(f) = D(f')$.*

Proof. First we shall construct a quadratic form g in $\mathcal{E}_{n,s'}$, with coefficients in $\mathbf{Q}$, which is equivalent to f over the field $\mathbf{Q}_p$ of p-adic numbers, for each prime p. The notation of Serre's book ([7], Chap. IV, §§2,3) will be used without further explanation. One has $d_\infty(f) = (-1)^q = (-1)^{q'}$ and $\varepsilon_\infty(f) = (-1)^{q(q-1)/2} = (-1)^{q'(q'-1)/2}$, where $q = (n-s)/2$ and $q' = (n-s')/2$. Let $d = D(f)$ and let $\varepsilon_v = \varepsilon_v(f)$ be the Hasse-Minkowski invariant for v a prime number or $v = \infty$. It follows from ([7], p. 44, Proposition 7) that there exists a form g in $\mathcal{E}_{n,s'}$, with coefficients in $\mathbf{Q}$, satisfying $D(g) = d$ and $\varepsilon_v(g) = \varepsilon_v = \varepsilon_v(f)$ for all v. By ([7], p. 39, Theorem 7), for every prime number p, the forms f and g are equivalent over $\mathbf{Q}_p$.

Having g as above, ([4], p. 141, statement θ_n) implies the existence of a form f' in $\mathcal{E}_{n,s'}(\mathbf{Z})$ which is equivalent to f over $\mathbf{Z}_p$ for all prime numbers p. □

To prove the next corollary we need the powerful Siegel-Watson theorem (cf. [4], p. 131, Theorem 1.5): Let f be a non-singular indefinite integral quadratic form in $n \geq 4$ variables and let $b \neq 0$ be an integer. Suppose that b is represented by f over all $\mathbf{Z}_p$. Then b is represented by f over $\mathbf{Z}$. Further, let P be a finite set of primes and for $p \in P$ let $a_p \in \mathbf{Z}_p^n$ be any representation of b by f. Then there is a representation $a \in \mathbf{Z}^n$ of b by f such that a is arbitrarily p-adically close to a_p for every $p \in P$.

COROLLARY 5.2. *Let n, s and s' be integers satisfying $|s| < n$, $|s'| < n$, $n \equiv s \pmod 2$, and $s \equiv s' \pmod 8$. Then*

$$\beta_{n,s'} = \beta_{n,s}.$$

In particular, $T(n, s')$ is equivalent to $T(n, s)$.

Proof. Let f be in $\mathcal{E}_{n,s}(\mathbf{Z})$. By Proposition 5.1, there is a form f' in $\mathcal{E}_{n,s'}(\mathbf{Z})$ which is equivalent to f over $\mathbf{Z}_p$ for every prime p. The Siegel-Watson theorem implies that f and f' represent the same non-zero integers over $\mathbf{Z}$. Moreover, if representations of n integers $b_1, \ldots, b_n$ by f are given by n linearly independent points in $\mathbf{Z}^n$, then some representation of the same integers by f' can be also given by linearly independent points in $\mathbf{Z}^n$. Indeed, let $f(a_i) = b_i$, where $a_i \in \mathbf{Z}^n$ for $1 \leq i \leq n$. Fix a prime p. Let $f = f' \circ \phi$ for some isomorphism ϕ over $\mathbf{Z}_p$ and let $a_i^{(p)} = \phi(a_i)$. If $a_1, \ldots, a_n$ are linearly independent in $\mathbf{Z}^n$, then $a_1^{(p)}, \ldots, a_n^{(p)}$ are linearly independent in $\mathbf{Z}_p^n$. In particular,

$$\det \begin{pmatrix} a_1^{(p)} \\ \vdots \\ a_n^{(p)} \end{pmatrix} \neq 0 .$$

By the Siegel-Watson theorem, one can choose $a_1', \ldots, a_n'$ in $\mathbf{Z}^n$ such that $f'(a_i') = b_i$ for $1 \leq i \leq n$ and a_i' is p-adically arbitrarily close to $a_i^{(p)}$. Then

$$\det \begin{pmatrix} a_1' \\ \vdots \\ a_n' \end{pmatrix} \neq 0 ,$$

and hence $a_1', \ldots, a_n'$ are linearly independent in $\mathbf{Z}^n$.

We can now complete the proof. Since $D(f) = D(f')$, the fact established above implies $\beta(f) \leq \beta(f')$. Thus $\beta_{n,s} \leq \beta_{n,s'}$, the form f in $\mathcal{E}_{n,s}(\mathbf{Z})$ being arbitrary. Consequently one gets

$$\beta_{n,s} = \beta_{n,s'}$$

by interchanging s and s'.

Finally observe that for s and s' under consideration,

$$w_{n,s} = w_{n,s'} .$$

By Corollary 2.3, the last two equalities imply the equivalence of $T(n, s)$ and $T(n, s')$ for $n \geq 3$. If $n = 2$, then $s = s' = 0$, and there is nothing to prove. □

REFERENCES

[1] BARNES, E. S. The minimum of the product of two values of a quadratic form. I. *Proc. London Math. Soc (3) 1* (1951), 257–283.

[2] —— On indefinite ternary quadratic forms. *Proc. London Math. Soc. (3) 2* (1952), 219–233.

[3] CASSELS, J. W. S. *An Introduction to the Geometry of Numbers.* Springer-Verlag, 1971.

[4] —— *Rational Quadratic Forms.* Academic Press, London, 1978.

[5] DANI, S. G. and G. MARGULIS. Values of quadratic forms at integral points: an elementary approach. *L'Enseignement Math. (2) 36* (1990), 143–174.

[6] MINKOWSKI, H. *Geometrie der Zahlen.* Leipzig and Berlin, 1898.

[7] SERRE, J.-P. *A Course in Arithmetic.* Springer-Verlag, 1993.

[8] WATSON, G. L. One-sided inequalities for integral quadratic forms. *Quart. J. Math. Oxford Ser. (2) 9* (1958), 99–108.

[9] —— Asymmetric inequalities for indefinite quadratic forms. *Proc. London Math. Soc. (3) 18* (1968), 95–113.

(Reçu le 28 septembre 2005)

J. Bochnak

Department of Mathematics
Vrije Universiteit
De Boelelaan 1081a
NL-1081 HV Amsterdam
The Netherlands
e-mail: bochnak@cs.vu.nl

W. Kucharz

Department of Mathematics and Statistics
University of New Mexico
Albuquerque, NM 87131-1141
U. S. A.
e-mail: kucharz@math.unm.edu