ACTA ARITHMETICA
LXIII.1 (1993)

Primitive minima of positive definite quadratic forms

by

ALOYS KRIEG (Münster)

1. Introduction. The main purpose of the reduction theory is to construct a fundamental domain of the unimodular group acting discontinuously on the space of positive definite quadratic forms. This fundamental domain is for example used in the theory of automorphic forms for GL_n (cf. [11]) or in the theory of Siegel modular forms (cf. [1], [4]). There are several ways of reduction, which are usually based on various minima of the quadratic form, e.g. the Korkin–Zolotarev method (cf. [10], [3]), Venkov's method (cf. [12]) or Voronoï's approach (cf. [13]), which also works in the general setting of positivity domains (cf. [5]). The most popular method is Minkowski's reduction theory [6] and its generalizations (cf. [9], [15]).

Minkowski's reduction theory is based on attaining certain minima, which can be characterized as the successive primitive minima of the quadratic form. Besides these we have successive minima, but a reduction according to successive minima only works for $n \leq 4$ (cf. [14]). In this paper we introduce so-called *primitive minima*, which lie between successive and successive primitive minima (cf. Theorem 2). Using primitive minima we obtain a straightforward generalization of Hermite's inequality in Theorem 1. As an application we get a simple proof for the finiteness of the class number. Finally we describe relations with Rankin's minima (cf. [8]) and with Venkov's reduction (cf. [12]).

2. Various minima. Let $\mathcal{P}_n$ denote the set of all real positive definite $n \times n$ matrices. $\mathrm{GL}_n(\mathbb{Z})$ stands for the unimodular group of degree n, i.e. the group of units in the ring $M_n(\mathbb{Z})$. An integral $n \times k$ matrix $P \in M_{n\times k}(\mathbb{Z})$, $n \geq k$, is called *primitive*, if the g.c.d. of all the k-rowed minors of P is 1. This is equivalent to the fact that there exists a matrix $(P, *) \in \mathrm{GL}_n(\mathbb{Z})$ (cf. [7]). Moreover, set

$$A[B] := (B^t)AB$$

for matrices A, B of appropriate size.

A matrix $S = (s_{jk}) \in \mathcal{P}_n$ is called *Minkowski-reduced* whenever

(M.1) $S[g] \geq s_{kk}$ for all $g = (\gamma_1, \dots, \gamma_n)^t \in \mathbb{Z}^n$ with g.c.d. $(\gamma_k, \dots, \gamma_n) = 1\,,\ 1 \leq k \leq n\,,$

(M.2) $s_{k,k+1} \geq 0$ for $0 < k < n\,.$

The set of Minkowski-reduced matrices is a fundamental domain of $\mathcal{P}_n$ with respect to the discontinuous group of mappings

$$\mathcal{P}_n \to \mathcal{P}_n\,, \quad S \mapsto S[U]\,, \quad U \in \mathrm{GL}_n(\mathbb{Z})\,.$$

In order to determine a unimodular matrix U such that $S[U]$ is Minkowski-reduced proceed as follows (cf. [4]): Given $S \in \mathcal{P}_n$ define its *minimum* by

$$\mu(S) := \inf\{S[h] \mid 0 \neq h \in \mathbb{Z}^n\}\,. \tag{1}$$

Determine $g_1 \in \mathbb{Z}^n$ with $\mu(S) = S[g_1]$. As soon as $g_1, \dots, g_k\,,\ 0 < k < n$, are given, choose $g_{k+1} \in \mathbb{Z}^n$ such that

$$S[g_{k+1}] = \inf\{S[h] \mid (g_1, \dots, g_k, h) \in M_{n\times(k+1)}(\mathbb{Z}) \text{ is primitive}\}\,. \tag{2}$$

If necessary replace g_{k+1} by $-g_{k+1}$ in order to get $g_k S g_{k+1} \geq 0$. In this way we construct a unimodular matrix $U = (g_1, \dots, g_n)$ such that $T = S[U]$ is Minkowski-reduced. The diagonal entries of T are given by (1) and (2) and may therefore be called the *successive primitive minima* of S.

Besides these the *successive minima* $\mu_1(S), \dots, \mu_n(S)$ of $S \in \mathcal{P}_n$ were introduced (cf. [14]). Determine $g_1 \in \mathbb{Z}^n$ as in (1), i.e.

$$\mu_1(S) = \mu(S) = S[g_1]\,.$$

As soon as $g_1, \dots, g_k, 0 < k < n$, are given, choose $g_{k+1} \in \mathbb{Z}^n$ such that

$$\mu_{k+1}(S) = S[g_{k+1}] = \inf\{S[h] \mid h \in \mathbb{Z}^n\,,\ \mathrm{rank}(g_1, \dots, g_k, h) = k+1\}\,. \tag{3}$$

Using Steinitz' theorem we have the alternative definition

$$\mu_k(S) = \inf\left\{ t \in \mathbb{R} \;\middle|\; \begin{array}{l} \text{there is } H = (h_1, \dots, h_k) \in M_{n\times k}(\mathbb{Z})\,, \\ \mathrm{rank}\, H = k\,,\ S[h_j] \leq t\,,\ 1 \leq j \leq k \end{array} \right\}, \quad 1 \leq k \leq n\,. \tag{4}$$

Comparing (3) and (4) it is interesting to investigate the analogue for primitive matrices in place of maximal rank matrices. We define

$$\nu_k(S) = \inf\left\{ t \in \mathbb{R} \;\middle|\; \begin{array}{l} \text{there is a primitive } H = (h_1, \dots, h_k) \\ \text{in } M_{n\times k}(\mathbb{Z})\,, S[h_j] \leq t\,,\ 1 \leq j \leq k \end{array} \right\}, \quad 1 \leq k \leq n\,. \tag{5}$$

We call $\nu_k(S)$ the *k-th primitive minimum* of S. Obviously one has

$$\mu_k(S) \leq \nu_k(S)\,, \quad 1 \leq k \leq n\,, \quad \nu_1(S) = \mu_1(S) = \mu(S)\,. \tag{6}$$

3. A generalization of Hermite's inequality. For $S \in \mathcal{P}_n$ we have

$$\mu(S) = \nu_1(S) \le \nu_2(S) \le \ldots \le \nu_n(S)\,. \tag{7}$$

Since UP, $U \in \mathrm{GL}_n(\mathbb{Z})$, is primitive if and only if P is, we conclude

$$\nu_k(S[U]) = \nu_k(S) \quad \text{for } U \in \mathrm{GL}_n(\mathbb{Z})\,,\ 1 \le k \le n\,. \tag{8}$$

Note that a primitive matrix can be completed to a unimodular matrix. Hence given $1 \le k \le n$ there exists $U_k \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$S[U_k] = T = (t_{ij})\,, \quad t_{11} \le t_{22} \le \ldots \le t_{nn}\,, \quad t_{kk} = \nu_k(S)\,. \tag{9}$$

THEOREM 1. *Given $S \in \mathcal{P}_n$ one has*

$$\nu_1(S) \ldots \nu_n(S) \le (\tfrac{4}{3})^{n(n-1)/2} \det S\,.$$

Proof. We use induction on n; the case $n = 1$ is obvious. According to (8) and (9) we may assume $s_{11} = \mu(S) = \nu_1(S) =: \mu$ without restriction. By the method of completing squares we obtain a decomposition

$$S = \begin{pmatrix} \mu & 0 \\ 0 & T \end{pmatrix} \left[\begin{pmatrix} 1 & a^t \\ 0 & I \end{pmatrix} \right] = \begin{pmatrix} \mu & \mu a^t \\ \mu a & T + \mu a a^t \end{pmatrix}, \quad T \in \mathcal{P}_{n-1}\,,\ a \in \mathbb{R}^{n-1}\,,$$

where I is the $(n-1) \times (n-1)$ identity matrix. Given $0 < k < n$ there exists a primitive matrix $G = (g_1, \ldots, g_k) \in M_{(n-1)\times k}(\mathbb{Z})$ such that

$$T[g_j] \le \nu_k(T)\,, \quad 1 \le j \le k\,.$$

Next choose $g = (\gamma_1, \ldots, \gamma_k)^t \in \mathbb{Z}^k$ such that the entries of $g + G^t a$ belong to the interval $[-\frac{1}{2}; \frac{1}{2}]$. Now

$$H = \begin{pmatrix} 1 & g^t \\ 0 & G \end{pmatrix} \in M_{n\times(k+1)}(\mathbb{Z}) \quad \text{and} \quad H' = \begin{pmatrix} g^t \\ G \end{pmatrix} \in M_{n\times k}(\mathbb{Z})$$

are primitive. One has

$$S \begin{bmatrix} \gamma_j \\ g_j \end{bmatrix} = \mu(\gamma_j + a^t g_j)^2 + T[g_j] \le \tfrac{1}{4}\,\nu_1(S) + \nu_k(T)\,, \quad 1 \le j \le k\,.$$

Since H' is primitive we conclude

$$\nu_k(S) \le \tfrac{1}{4}\nu_1(S) + \nu_k(T)\,.$$

Now (7) leads to

$$S \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \nu_1(S) \le \nu_k(S) \le \tfrac{1}{4}\nu_1(S) + \nu_k(T)\,.$$

Since H is primitive, we now have

$$\nu_{k+1}(S) \le \tfrac{1}{4}\nu_1(S) + \nu_k(T) \quad \text{and} \quad \nu_{k+1}(S) \le \tfrac{4}{3}\nu_k(T)\,.$$

According to $\nu_1(S)\det T = \det S$ the induction hypothesis yields

$$\begin{aligned}\nu_1(S) \ldots \nu_n(S) &\le (\tfrac{4}{3})^{n-1}\nu_1(S)\nu_1(T)\ldots\nu_{n-1}(T) \\ &\le (\tfrac{4}{3})^{n(n-1)/2}\nu_1(S)\det T = (\tfrac{4}{3})^{n(n-1)/2}\det S\,. \ \blacksquare\end{aligned}$$

In view of (7) we obtain Hermite's inequality (cf. [7]) as

COROLLARY 1. *Given* $S \in \mathcal{P}_n$ *one has*

$$\mu(S)^n \le (\tfrac{4}{3})^{n(n-1)/2} \det S\,.$$

Denote the class number by $h_n(N)$, $N \ge 1$, i.e. $h_n(N)$ is the number of $\mathrm{GL}_n(\mathbb{Z})$-equivalence classes of integral $S \in \mathcal{P}_n$ with $\det S = N$.

COROLLARY 2. *The class numbers* $h_n(N)$, $N \ge 1$, *are finite. One has*

$$h_n(N) = O(N^{n(n+1)/2}) \qquad \text{as } N \to \infty\,.$$

Proof. By (9) it suffices to count the number of integral $S \in \mathcal{P}_n$ with $\det S = N$ and $s_{kk} \le \nu_n(S)$, $1 \le k \le n$. In view of $\nu_k(S) \ge 1$ Theorem 1 implies

$$0 < s_{kk} \le \nu_n(S) \le \nu_1(S) \ldots \nu_n(S) \le (\tfrac{4}{3})^{n(n-1)/2} N\,.$$

Next $S \in \mathcal{P}_n$ yields $s_{jj}s_{kk} - s_{jk}^2 > 0$, hence $|s_{jk}| < (\frac{4}{3})^{n(n-1)/2} N$ for $1 \le j < k \le n$. Thus the number of these S is $O(N^{n(n+1)/2})$ as $N \to \infty$. ∎

For other proofs of Corollary 2 we refer to [7].

4. Relations with other types of minima. The first relation is derived in

THEOREM 2. *Let* $S = (s_{ij}) \in \mathcal{P}_n$ *be Minkowski-reduced. Given* $1 \le k \le n$ *one has*

$$\mu_k(S) \le \nu_k(S) \le s_{kk} \le \alpha_k \mu_k(S) \le \alpha_k \nu_k(S)\,,$$

where

$$\alpha_k = \begin{cases} 1 & \text{if } k \le 4\,, \\ (\frac{5}{4})^{k-4} & \text{if } k \ge 4\,. \end{cases}$$

Proof. $\nu_k(S) \le s_{kk}$ follows from $s_{11} \le \ldots \le s_{nn}$. The remaining parts are consequences of (6) and [14], Satz 7 and (45). ∎

If $k \ge 5$ there are quadratic forms S with $\nu_k(S) > \mu_k(S)$. Just as in [14] consider the matrix S attached to the quadratic form

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + (x_1 + x_2 + x_3 + x_4)x_5 + \tfrac{5}{4}x_5^2\,.$$

One easily checks

$$\mu_k(S) = \nu_j(S) = 1\,, \quad 1 \le k \le 5\,,\ 1 \le j \le 4\,, \quad \nu_5(S) = \tfrac{5}{4}\,.$$

Next consider the minima

$$\begin{aligned} \delta_k(S) :=\ & \inf\{\det(S[P]) \mid P \in M_{n\times k}(\mathbb{Z}) \text{ primitive}\} \\ =\ & \inf\{\det(S[G]) \mid G \in M_{n\times k}\,,\ \operatorname{rank} G = k\}\,, \quad 1 \le k \le n\,, \end{aligned}$$

which were introduced by Rankin [8].

PROPOSITION 1. *Given $S \in \mathcal{P}_n$ and $1 \le k \le n$ one has*

$$\nu_1(S)\dots\nu_k(S) \le (\tfrac{4}{3})^{k(k-1)/2}\delta_k(S)\,.$$

Proof. Choose a primitive $P \in M_{n\times k}(\mathbb{Z})$ with $\delta_k(S) = \det(S[P])$. Apply Theorem 1 to $S[P]$. In view of the obvious inequalities $\nu_j(S[P]) \ge \nu_j(S)$ for $1 \le j \le k$, the claim follows. ∎

Given $T \in \mathcal{P}_k$ and $S \in \mathcal{P}_n$, $1 \le k \le n$, we define

$$\nu_T(S) := \inf\{\mathrm{tr}(S[P]T) \mid P \in M_{n\times k}(\mathbb{Z}) \text{ primitive}\}\,,$$

where tr is the trace. Clearly the minimum is attained and one has

$$\nu_I(S) \ge \nu_1(S) + \ldots + \nu_k(S)\,, \quad I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathcal{P}_k\,,$$

where equality holds at least for $k \le 4$. If $k = n$ and $T \in \mathcal{P}_n$ has no non-trivial automorphs, then Venkov [12] showed that

$$\{S \in \mathcal{P}_n \mid \mathrm{tr}(ST) = \nu_T(S)\}$$

is a fundamental domain of $\mathcal{P}_n$ with respect to the action of the unimodular group.

PROPOSITION 2. *Let $S \in \mathcal{P}_n$, $T \in \mathcal{P}_k$, $1 \le k \le n$. Then one has*

$$\nu_T(S) \ge k\delta_k(S)^{1/k}(\det T)^{1/k} \ge k(\tfrac{3}{4})^{(k-1)/2}\mu(S)\mu(T)\,.$$

Proof. Choose a primitive $P \in M_{n\times k}(\mathbb{Z})$ with $\nu_T(S) = \mathrm{tr}(S[P]T)$. Then apply the result of Barnes and Cohn [2] to $S[P]$ and T:

$$\nu_T(S) = \mathrm{tr}(S[P]T) \ge k(\det(S[P]))^{1/k}(\det T)^{1/k}\,.$$

One has $\det(S[P]) \ge \delta_k(S)$. Now the claim follows by virtue of Proposition 1, Corollary 1 and (7). ∎

References

[1] A. N. Andrianov, *Quadratic Forms and Hecke Operators*, Grundlehren Math. Wiss. 286, Springer, Berlin 1987.

[2] E. S. Barnes and M. J. Cohn, *On the inner product of positive quadratic forms*, J. London Math. Soc. (2) 12 (1975), 32–36.

[3] D. Grenier, *Fundamental domains for the general linear group*, Pacific J. Math. 132 (1988), 293–317.

[4] H. Klingen, *Introductory Lectures on Siegel Modular Forms*, Cambridge University Press, Cambridge 1990.

[5] M. Koecher, *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen I*, Math. Ann. 141 (1960), 384–432.

[6] H. Minkowski, *Diskontinuitätsbereich für arithmetische Äquivalenz*, J. Reine Angew. Math. 129 (1905), 220–274.

[7] M. Newman, *Integral Matrices*, Academic Press, New York 1972.
[8] R. A. Rankin, *On positive definite quadratic forms*, J. London Math. Soc. 28 (1953), 309–319.
[9] S. S. Ryshkov, *On the Hermite–Minkowski reduction theory for positive quadratic forms*, J. Soviet Math. 6 (1976), 651–671.
[10] S. S. Ryshkov and E. P. Baranovskiĭ, *Classical methods in the theory of lattice packings*, Russian Math. Surveys 34 (4) (1979), 1–68.
[11] A. Terras, *Harmonic Analysis on Symmetric Spaces and Applications II*, Springer, New York 1988.
[12] A. B. Venkov, *On the reduction of positive quadratic forms*, Izv. Akad. Nauk SSSR Ser. Mat. 4 (1940), 37–52 (in Russian).
[13] G. Voronoï, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. 133 (1907), 97–178.
[14] B. L. van der Waerden, *Die Reduktionstheorie der positiven quadratischen Formen*, Acta Math. 96 (1956), 263–309.
[15] H. Weyl, *Theory of reduction for arithmetical equivalence*, Trans. Amer. Math. Soc. 48 (1940), 126–164.

MATHEMATISCHES INSTITUT
WESTFÄLISCHE WILHELMS–UNIVERSITÄT
EINSTEINSTR. 62
W-4400 MÜNSTER
FEDERAL REPUBLIC OF GERMANY
E-mail: ALOYS@MATH.UNI-MUENSTER.DE

Received on 30.4.1992 (2257)