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

(M.1) $s_{k,k+1} \geq 0$ 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
\[
\mathcal{P}_n \rightarrow \mathcal{P}_n, \quad S \mapsto S[U], \quad U \in \text{GL}_n(\mathbb{Z}) .
\]

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
\[
(1) \quad \mu(S) := \inf \{ S[h] \mid 0 \neq h \in \mathbb{Z}^n \} .
\]
Determine $g_1 \in \mathbb{Z}^n$ with $\mu(S) = S[g_1]$. As soon as $g_1, \ldots, g_k$, $0 < k < n$, are given, choose $g_{k+1} \in \mathbb{Z}^n$ such that
\[
(2) \quad S[g_{k+1}] = \inf \{ S[h] \mid (g_1, \ldots, g_k, h) \in M_{n \times (k+1)}(\mathbb{Z}) \text{ is primitive} \} .
\]
If necessary replace $g_{k+1}$ by $-g_{k+1}$ in order to get $g_k Sg_{k+1} \geq 0$. In this way we construct a unimodular matrix $U = (g_1, \ldots, g_n)$ 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* $\mu_1(S), \ldots, \mu_n(S)$ 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 $g_1, \ldots, g_k$, $0 < k < n$, are given, choose $g_{k+1} \in \mathbb{Z}^n$ such that
\[
(3) \quad \mu_{k+1}(S) = S[g_{k+1}] = \inf \{ S[h] \mid h \in \mathbb{Z}^n, \quad \text{rank}(g_1, \ldots, g_k, h) = k+1 \} .
\]
Using Steinitz’ theorem we have the alternative definition
\[
(4) \quad \mu_k(S) = \inf \left\{ t \in \mathbb{R} \mid \begin{array}{l}
\text{there is } H = (h_1, \ldots, h_k) \in M_{n \times k}(\mathbb{Z}), \\
\text{rank } H = k, \ S[h_j] \leq t, \ 1 \leq j \leq k \end{array} \right\} ,
\]
\[
1 \leq k \leq n .
\]
Comparing (3) and (4) it is interesting to investigate the analogue for primitive matrices in place of maximal rank matrices. We define
\[
(5) \quad \nu_k(S) = \inf \left\{ t \in \mathbb{R} \mid \begin{array}{l}
\text{there is a primitive } H = (h_1, \ldots, h_k) \text{ in } M_{n \times k}(\mathbb{Z}), S[h_j] \leq t, \ 1 \leq j \leq k \\
1 \leq k \leq n .
\end{array} \right\} ,
\]
We call $\nu_k(S)$ the *k-th primitive minimum* of $S$. Obviously one has
\[
(6) \quad \mu_k(S) \leq \nu_k(S), \quad 1 \leq k \leq n, \quad \nu_1(S) = \mu_1(S) = \mu(S) .
\]
3. A generalization of Hermite’s inequality. For \( S \in \mathcal{P}_n \) we have
\begin{equation}
\mu(S) = \nu_1(S) \leq \nu_2(S) \leq \ldots \leq \nu_n(S). 
\end{equation}

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

\begin{equation}
\nu_k(S[U]) = \nu_k(S) \quad \text{for} \quad U \in \text{GL}_n(\mathbb{Z}), \; 1 \leq k \leq n.
\end{equation}

Note that a primitive matrix can be completed to a unimodular matrix. Hence given \( 1 \leq k \leq n \) there exists \( U_k \in \text{GL}_n(\mathbb{Z}) \) such that
\begin{equation}
S[U_k] = T = (t_{ij}), \quad t_{11} \leq t_{22} \leq \ldots \leq t_{nn}, \quad t_{kk} = \nu_k(S).
\end{equation}

**Theorem 1.** Given \( S \in \mathcal{P}_n \) one has
\[ \nu_1(S) \ldots \nu_n(S) \leq \left( \frac{4}{3} \right)^{n(n-1)/2} \det S. \]

**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
\[ S = \begin{pmatrix} \mu & 0 \\ 0 & T \end{pmatrix} \begin{pmatrix} 1 & a^t \\ 0 & I \end{pmatrix} = \begin{pmatrix} \mu a & \mu a^t \\ \mu a^t & T + \mu a a^t \end{pmatrix}, \quad T \in \mathcal{P}_{n-1}, \; a \in \mathbb{R}^{n-1}, \]
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
\[ T[g_j] \leq \nu_k(T), \; 1 \leq j \leq k. \]

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
\[ S \begin{pmatrix} \gamma_j \\ g_j \end{pmatrix} = \mu(\gamma_j + a^t g_j)^2 + T[g_j] \leq \frac{1}{4} \nu_1(S) + \nu_k(T), \; 1 \leq j \leq k. \]

Since \( H' \) is primitive we conclude
\[ \nu_k(S) \leq \frac{1}{4} \nu_1(S) + \nu_k(T). \]

Now (7) leads to
\[ S \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \nu_1(S) \leq \nu_k(S) \leq \frac{1}{4} \nu_1(S) + \nu_k(T). \]

Since \( H \) is primitive, we now have
\[ \nu_{k+1}(S) \leq \frac{1}{4} \nu_1(S) + \nu_k(T) \quad \text{and} \quad \nu_{k+1}(S) \leq \frac{3}{4} \nu_k(T). \]

According to \( \nu_1(S) \det T = \det S \) the induction hypothesis yields
\[ \nu_1(S) \ldots \nu_n(S) \leq \left( \frac{4}{3} \right)^{n-1} \nu_1(T) \ldots \nu_{n-1}(T) \]
\[ \leq \left( \frac{4}{3} \right)^{n(n-1)/2} \nu_1(S) \det T = \left( \frac{4}{3} \right)^{n(n-1)/2} \det S. \]
In view of (7) we obtain Hermite’s inequality (cf. [7]) as

**COROLLARY 1.** Given \( S \in P_n \) one has

\[
\mu(S)^n \leq \left(\frac{4}{3}\right)^{n(n-1)/2} \det S.
\]

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

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

\[
h_n(N) = O(N^{n(n+1)/2}) \quad \text{as} \quad N \to \infty.
\]

**Proof.** By (9) it suffices to count the number of integral \( S \in P_n \) with \( \det S = N \) and \( s_{kk} \leq \nu_n(S) \), \( 1 \leq k \leq n \). In view of \( \nu_k(S) \geq 1 \) Theorem 1 implies

\[
0 < s_{kk} \leq \nu_n(S) \leq \nu_1(S) \ldots \nu_n(S) \leq (\frac{4}{3})^{n(n-1)/2} N.
\]

Next \( S \in P_n \) yields \( s_{jj}s_{kk} - s_{jk}^2 > 0 \), hence \( |s_{jk}| < (\frac{4}{3})^{n(n-1)/2} N \) for \( 1 \leq j < k \leq n \). 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 \( S = (s_{ij}) \in P_n \) be Minkowski-reduced. Given \( 1 \leq k \leq n \) one has

\[
\mu_k(S) \leq \nu_k(S) \leq s_{kk} \leq \alpha_k \mu_k(S) \leq \alpha_k \nu_k(S),
\]

where

\[
\alpha_k = \begin{cases} 
1 & \text{if } k \leq 4, \\
\left(\frac{5}{4}\right)^{k-4} & \text{if } k \geq 4.
\end{cases}
\]

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

If \( k \geq 5 \) 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

\[
x_1^2 + x_2^2 + x_3^2 + x_4^2 + (x_1 + x_2 + x_3 + x_4)x_5 + \frac{5}{4}x_5^2.
\]

One easily checks

\[
\mu_k(S) = \nu_j(S) = 1, \quad 1 \leq k \leq 5, \quad 1 \leq j \leq 4, \quad \nu_5(S) = \frac{5}{4}.
\]

Next consider the minima

\[
\delta_k(S) := \inf\{\det(S[P]) \mid P \in M_{n \times k}(\mathbb{Z}) \text{ primitive}\}
\]

\[
= \inf\{\det(S[G]) \mid G \in M_{n \times k}, \ \text{rank} \ G = k\}, \quad 1 \leq k \leq n,
\]

which were introduced by Rankin [8].
Proposition 1. Given $S \in \mathcal{P}_n$ and $1 \leq k \leq n$ one has

$$\nu_1(S) \cdots \nu_k(S) \leq \left(\frac{4}{3}\right)^{(k-1)/2} \delta_k(S).$$

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 $\nu_j(S[P]) \geq \nu_j(S)$ for $1 \leq j \leq k,$ the claim follows.

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

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

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

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

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

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

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

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

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

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

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

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

References