

THE MINIMUM DETERMINANT OF MINKOWSKI-REDUCED QUINARY QUADRATIC FORMS

E. S. BARNES and D. W. TRENERRY

(Received 12 March 1981)

Communicated by A. J. van der Poorten

Abstract

Minkowski established a lower bound for the determinant D of a Minkowski-reduced quadratic form in terms of the product of its diagonal coefficients a_{ii} ($i = 1, \dots, n$). Oppenheim and Barnes found, for $n = 3$ and $n = 4$ respectively, the precise minimum of D in terms of the a_{ii} ; in each case the minimum is a polynomial in the a_{ii} . Here it is shown that no such result exists when $n = 5$; however a polynomial in a_{11}, \dots, a_{55} is determined which gives the minimum of D when a_{55} is sufficiently large.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 10 E 25; secondary 10 E 20.

Introduction

A positive definite quadratic form $f(\mathbf{x}) = \sum_1^n a_{ij}x_i x_j$ ($a_{ij} = a_{ji}$), of determinant $D = \det(a_{ij})$, is Minkowski-reduced if, for all $i = 1, \dots, n$ and for all integral $\mathbf{x} = (x_1, \dots, x_n)$,

$$(1.1) \quad \text{if g.c.d.}(x_i, x_{i+1}, \dots, x_n) = 1, \text{ then } f(\mathbf{x}) \geq a_{ii}.$$

It is known that a finite number of inequalities (1.1) imply all the rest, so that the set of reduced forms is a polyhedral cone in the $\frac{1}{2}n(n+1)$ -dimensional space of the coefficients a_{ij} ($1 \leq i \leq j \leq n$). Indeed, for $n < 5$, Minkowski established that it suffices to use, in (1.1), only those \mathbf{x} with all x_i equal to 0 or ± 1 and when $n = 5$, those with one coordinate 2 and the rest ± 1 .

The reduction conditions (1.1) with one or two coordinates non-zero yield

$$(1.2) \quad a_{11} \leq a_{22} \leq \dots \leq a_{nn}$$

and

$$(1.3) \quad |2a_{ij}| \leq a_{ii} \quad (1 \leq i < j \leq n);$$

these show that, for any fixed a_{ii} satisfying (1.2), all coefficients a_{ij} are bounded.

Minkowski showed that a constant λ_n exists for each n such that all reduced forms satisfy the inequality

$$(1.4) \quad a_{11}a_{22} \cdots a_{nn} \leq \lambda_n D;$$

and the best possible value of λ_n is known for $n \leq 5$. We set now, for typographical convenience,

$$(1.5) \quad a_{11} = a, \quad a_{22} = b, \quad a_{33} = c, \quad a_{44} = d, \quad a_{55} = e,$$

where, by (1.2),

$$(1.6) \quad 0 < a \leq b \leq c \leq d \leq e.$$

Oppenheim (1946) sharpened (1.4) for $n = 3$ (where $\lambda_3 = 2$), pointing out that for all a, b, c

$$(1.7) \quad \min D = \frac{1}{4}(2abc + ab(c - b) + ac(b - a)).$$

Barnes (1978) extended this result to show that when $n = 4$, for all a, b, c, d ,

$$(1.8)$$

$$\min D = \frac{1}{4}(abcd + acd(b - a) + abd(c - b) + abc(d - c) + \frac{1}{4}a^2(b - c)^2),$$

immediately implying (1.4) with $\lambda_4 = 4$.

One might expect that results similar to (1.7) and (1.8) would hold in higher dimensions. We show here however that, for $n = 5$, while a similar result holds whenever e is sufficiently large, there is no single polynomial yielding the minimum value of D for all a, b, c, d, e . More precisely, we prove:

THEOREM 1. *Let $f(\mathbf{x}) = \sum_1^5 a_{ij}x_i x_j$ be a Minkowski-reduced quinary form whose diagonal coefficients are given by (1.5). There exists a number $e_0 = e_0(a, b, c, d)$ such that for all $e \geq e_0$*

$$(1.9)$$

$$D \geq \frac{1}{16}a\{2bcde + 2bcd(e - d) + bc(4e - d)(d - c) + bd(4e - c)(c - b) + cd(4e - d - b)(b - a) + ae(c - b)^2 + b^2(d - c)^2\}.$$

Equality holds in (1.9), for example, for the form

$$(1.10) \quad \begin{aligned} \psi_0(\mathbf{x}) = & ax_1^2 + ax_1x_2 + ax_1x_4 + bx_2^2 + bx_2x_3 + bx_2x_4 \\ & + cx_3^2 + cx_3x_4 + cx_3x_5 + dx_4^2 + dx_4x_5 + ex_5^2. \end{aligned}$$

THEOREM 2. *If $c \geq a + b$ and*

$$(1.11) \quad \begin{aligned} \psi_1(\mathbf{x}) = & ax_1^2 + ax_1x_3 + ax_1x_4 + bx_2^2 + bx_2x_3 + bx_2x_4 \\ & + cx_3^2 + cx_3x_4 + cx_3x_5 + dx_4^2 + dx_4x_5 + ex_5^2, \end{aligned}$$

then ψ_1 is Minkowski-reduced and, for the values $(a, b, c, d, e) = (1, 2, 3, 3, 3)$,

$$D(\psi_1) = \frac{54}{4} < D(\psi_0) = \frac{57}{4}.$$

We note that Van der Waerden (1969) determined $\lambda_5 = 8$ in (1.4) and that (1.9) is immediately seen to conform with the inequality $abcde \leq 8D$.

We use the notations of Barnes (1978). In particular, $\mathfrak{D} = \mathfrak{D}(a, b, c, \dots)$ is the convex polytope defined as the intersection of the cone \mathfrak{M} of Minkowski-reduced forms in $R^{n(n+1)/2}$ with the hyperplanes $a_{11} = a, a_{22} = b, \dots$ ($0 < a \leq b \leq \dots$); \mathfrak{D}^+ is similarly defined with respect to the cone \mathfrak{M}^+ of ‘properly reduced’ forms satisfying $a_{i,i+1} \geq 0$ ($i = 1, \dots, n - 1$). We recall that the minimum value of D is attained only at a vertex of \mathfrak{D} (or \mathfrak{D}^+).

To avoid fractional coefficients, we write throughout

$$f_{ij} = 2a_{ij} \quad (i < j).$$

2. Proof of Theorem 1

It was shown in Barnes (1978) that, for quaternary M -reduced forms, the minimum value of D given by (1.8) is attained, for all a, b, c, d , by 14 equivalent forms, one of which is

$$(2.1) \quad \begin{aligned} g_1(x_1, x_2, x_3, x_4) = & ax_1^2 + ax_1x_2 + ax_1x_4 + bx_2^2 \\ & + bx_2x_3 + bx_2x_4 + cx_3^2 + cx_3x_4 + dx_4^2. \end{aligned}$$

We begin the proof of Theorem 1 by considering quinary forms f for which g_1 is the section by $x_5 = 0$, that is (setting for convenience $f_{i5} = f_i, i = 1, \dots, 4$)

$$(2.2) \quad \begin{aligned} f(x_1, \dots, x_5) = & g_1(x_1, \dots, x_4) + f_1x_1x_5 + f_2x_2x_5 \\ & + f_3x_3x_5 + f_4x_4x_5 + ex_5^2. \end{aligned}$$

LEMMA 2.1. $f \in \mathfrak{N}^+$ if and only if the coefficients f_1, f_2, f_3, f_4 satisfy the system of linear inequalities

$$\begin{aligned}
 (2.3) \quad & |f_1| \leq a, \quad |f_2| \leq b, \quad |f_3| \leq c, \quad 0 \leq f_4 \leq d, \\
 & |f_1 - f_2| \leq b, \\
 & -f_1 + f_4 \leq d, \\
 & |f_2 - f_3| \leq c, \\
 & -f_2 + f_4 \leq d, \\
 & -f_3 + f_4 \leq d, \\
 & |f_1 - f_2 + f_3| \leq c, \\
 & |f_1 + f_3 - f_4| \leq d, \\
 & -f_1 + f_2 - f_3 + f_4 \leq -a + b + d.
 \end{aligned}$$

PROOF. Since g_1 is M -reduced, it suffices to consider only inequalities (1.1) with $x_5 \neq 0$. The inequalities (2.3) are easily found as the non-redundant inequalities derived from $x_5 = 1$ and $x_1 = 0$ or ± 1 ($i = 1, \dots, 4$), together with the assumption that $f \in \mathfrak{N}^+$, so that $f_4 = 2a_{45} \geq 0$. All other inequalities (1.1), namely those with some $x_i = 2$ and the remaining $x_j = \pm 1$, are now found to be redundant in virtue of (2.3). (For the inequalities

$$(2.4) \quad f(\pm 1, \pm 1, \pm 1, \pm 1, 2) \geq a_{44} = d$$

it is here not necessary to assume that e is large, but merely to observe that $e \geq d$. All other inequalities are independent of e .)

On solving the system (2.3), we find that there are 31 extreme solutions (where we do not distinguish between a solution and its negative), which fall into 6 equivalence classes under transformations of f which leave g_1 fixed. Evaluation of $D(f)$ now establishes that, for all a, b, \dots, e , the least determinant occurs for the 7 equivalent solutions

$$\begin{aligned}
 (2.5) \quad & (f_1, f_2, f_3, f_4) = (0, 0, c, d), (-a, -a + b, 0, -a + d), \\
 & (-a, -a + b, b - c, -a + b - c + d), \\
 & (a, b, 0, d), (a, b, b - c, b - c + d), \\
 & (0, -b, -b, -b + d), (0, -b, -c, -c + d),
 \end{aligned}$$

the value of $D(f)$ being given by the expression (1.9). Since clearly all vertices of the polytope \mathfrak{D} must arise from extreme solutions of (2.3), we have

LEMMA 2.2. If f is M -reduced and of the form (2.2), then the minimum value of $D(f)$ occurs when $f = \psi_0$, as defined in (1.10) (and by 6 other equivalent forms).

PROOF OF THEOREM 1. We write f in the form

$$(2.6) \quad \begin{aligned} f(x_1, \dots, x_5) = & g(x_1, \dots, x_4) + f_{15}x_1x_5 + f_{25}x_2x_5 \\ & + f_{35}x_3x_5 + f_{45}x_4x_5 + ex_5^2. \end{aligned}$$

Since the reduction conditions (1.1) for f include those for g (namely those with $x_5 = 0$), g is M -reduced.

We next require e to be so large that all inequalities (2.4) are redundant. Using the facts that g is positive definite and that all $|f_{i5}| \leq d$, we have crudely

$$f(\pm 1, \pm 1, \pm 1, \pm 1, 2) \geq -8d + 4e,$$

whence (2.4) is certainly satisfied if $e \geq 9d/4$.

We have now ensured that the coefficient $a_{55} = e$ does not appear explicitly in any of the reduction conditions (1.1) for f , since these either have $x_5 = 0$ or $x_5 = \pm 1$ and $a_{ii} = a_{55} = e$. Consider now the polytope $\mathcal{D} = \mathcal{D}(a, b, c, d, e)$ for f in R^{10} ; it has a finite number of vertices v , each of which has coordinates that are linear functions of a, b, c, d only and which, by (1.2) and (1.3), all satisfy

$$|f_{ij}| \leq d \quad (1 \leq i < j \leq 5).$$

We divide these vertices into two classes: class I contains those vertices for which the corresponding form (2.6) has $g \sim g_1$ (defined in (2.1)); class II contains the remaining vertices.

Let now v be of class I. If now $g = g_1$, Lemma 2.2 shows immediately that $D(f) \geq D(\psi_0)$. The same result holds if g is one of the other 13 forms equivalent to g_1 ; for it is straightforward to verify that the equivalence transformation taking g into g_1 induces a linear transformation of $f_{11}, f_{25}, f_{35}, f_{45}$ in (2.8) which takes the defining inequalities involving these coefficients into the system (2.3); the resulting forms f are therefore equivalent to a form with $g = g_1$ and again we deduce that $D(f) \geq D(\psi_0)$.

Next let v be of class II, so that $D(g) > D(g_1)$. Since there are only finitely many such vertices, all of whose coordinates depend only on a, b, c, d , we can assert that

$$D(g) - D(g_1) \geq \mu(a, b, c, d) > 0$$

for some polynomial function μ . Expanding $D(f)$ as a bordered determinant, we have

$$D(f) = eD(g) - \frac{1}{4} \sum_1^4 B_{ij} f_{i5} f_{j5}$$

where $\sum_1^4 B_{ij}x_i x_j$ is the form adjoint to g , whence similarly

$$D(f) \geq eD(g) - \nu(a, b, c, d)$$

for some polynomial function ν . Since trivially $D(\psi_0) \leq eD(g_1)$, we deduce that

$$D(f) > D(\psi_0) \quad \text{if } e > \frac{\nu}{\mu},$$

and the proof of Theorem 1 is complete.

3. Proof of Theorem 2

The assertions of Theorem 2 are easily verified by direct computation; the condition ‘ $c \geq a + b$ ’ arises from the reduction condition

$$-a - b + c + e = \psi_1(1, 1, -1, -1, 1) \geq a_{55} = e.$$

The form ψ_1 was constructed by a method similar to that used for ψ_0 , namely by minimizing $D(f)$ over forms of the shape

$$f(x_1, \dots, x_5) = ax_1^2 + f_{12}x_1x_2 + \dots + f_{15}x_1x_5 + g_2(x_2, x_3, x_4, x_5),$$

where

$$g_2(x_2, x_3, x_4, x_5) = bx_2^2 + bx_2x_3 + bx_2x_4 + cx_3^2 + cx_3x_4 + cx_3x_5 + dx_4^2 + dx_4x_5 + ex_5^2$$

has minimum determinant for the section $f(0, x_2, \dots, x_5)$. Although, for some values of b, c, d, e , $D(f)$ is then minimized when $f = \psi_0$, Theorem 2 shows that this is not always the case. It is probable that, when $c > b$, either ψ_0 or ψ_1 has minimal determinant if a is sufficiently small compared with b, c, d, e . Two other forms with small determinant which arise from this construction are, when $c \leq a + b$, those with $(f_{12}, f_{13}, f_{14}, f_{15}) = (0, a, a, a + b - c)$ and $(a + b - c, a, a, 0)$.

We conjecture that the minimum value of $D(f)$ is always assumed at one of a finite set of forms and so is the minimum of a finite number of polynomial functions in a, b, \dots, e . However extensive computer searches have not produced any form with determinant less than those of the forms given above.

We record our thanks to Dr. B. A. Murtagh of the University of New South Wales for making available his non-linear optimization program MINOS, and to Dr. M. J. Cohn for his program which enumerates the vertices of a polytope.

References

- E. S. Barnes (1978), 'On Minkowski's fundamental inequality for reduced positive quadratic forms (I)', *J. Austral. Math. Soc. Ser. A* **26**, 46–52.
- A. Oppenheim (1946), 'A positive definite quadratic form as the sum of two positive definite quadratic forms (I)', *J. London Math. Soc.* **21**, 252–257.
- B. L. Van der Waerden (1969), 'Das Minimum von $D/f_{11}f_{22} \cdots f_{55}$ für reduzierte positive quinäre quadratische Formen', *Aequationes Math.* **2**, 233–247.

The University of Adelaide
Adelaide, 5001
Australia

The University of New South Wales
Broken Hill, 2880
Australia