TWO REMARKS ON EXTREME FORMS

MARTIN KNESER

1. Introduction. The following remarks concern two different parts of the theory of extreme quadratic forms. In §2, I shall give a new proof for the theorem of Voronoï **(4)**, which asserts that a form is extreme if and only if it is both perfect and eutactic. (For the definitions see, e.g., Coxeter **(2)** or the text below.) There is indeed a comparatively simple proof in Bachmann's *Zahlentheorie*, IV, 2. For two reasons, however, it may not be useless to communicate another proof here. First, I shall prove the necessity and the sufficiency in one step, and second, as a consequence, my proof requires a minimum of calculation. In §3, I shall add a new senary extreme form to Hofreiter's list **(3)** and Coxeter's paper **(2)**. This form was found independently by Barnes (see the succeeding paper **(1)**). I therefore restrict myself to determining its group of automorphs, which is not done in Barnes's paper.

2. Voronoï's theorem. In this section, we denote: real symmetric $(n \times n)$-matrices by capital letters $A, B, \ldots$, the $\frac{1}{2}n(n+1)$-dimensional space of these matrices by R; vectors, considered as $(n \times 1)$-matrices, by small letters $x, y, \ldots$; the transposition of a matrix by a prime, and real numbers by Greek letters. Let $x'Ax$ be a positive definite quadratic form, and $\mu(A)$ the minimum of $x'Ax$ taken over all x with integer coordinates not all 0. This minimum is attained at a finite number of vectors, called minimal vectors; for these we shall reserve the letter m. The form $x'Ax$ is called *extreme* if the quotient

$$\delta(B) = \mu(B)\det(B)^{-1/n}$$

has a local maximum at $B = A$, i.e., if $\delta(A + C) \leqslant \delta(A)$ for all matrices $C \in R$ whose elements are sufficiently small. Since $\delta(\lambda B) = \delta(B)$, we may restrict C to a hyperplane through the origin not containing A, e.g. the hyperplane H of R defined by $\operatorname{tr}(A^{-1}C) = 0$. Continuity shows that, for small C, $A + C$ is positive definite and the minimal vectors of $A + C$ are contained among those of A. Hence $\delta(A + C) \leqslant \delta(A)$ means that for at least one minimal vector m of A, the inequality

$$(1) \qquad m'(A + C)m.\det(A + C)^{-1/n} \leqslant m'Am.\det(A)^{-1/n}$$

holds; or, what is the same, the union of the regions K_m of C's such that $A + C$ is positive definite and (1) holds, contains a neighbourhood of the origin O in R; or, finally

(a) $\bigcup_m H \cap K_m$ contains a neighbourhood of O in H.

Now, the following lemma shows that K_m is convex and $H \cap K_m$ is strictly convex.

https://doi.org/10.4153/CJM-1955-018-2 Published online by Cambridge University Press

LEMMA. *Let m be a fixed vector and $\lambda > 0$. The set K of positive definite symmetric matrices C satisfying the inequality $m'Cm \leqslant \lambda \det(C)^{1/n}$ is a convex cone with its vertex at the origin O. If H is a hyperplane not containing O, $H \cap K$ is strictly convex (i.e., if C and D are in $H \cap K$ and if $0 < \tau < 1$, then $\tau C + (1 - \tau)D$ is an inner point of $H \cap K$).*

Proof. We have to show that if C and D are in K, so is $\tau C + (1 - \tau)D$, and that the latter is an inner point unless $D = \kappa C$. Since K obviously is a cone, we may replace D by a scalar multiple and so may assume

$$m'Cm = m'Dm = m'(\tau C + (1 - \tau)D)m.$$

It remains to prove that the inequalities

$$\det(C)^{1/n} \geqslant \mu = m'Cm.\lambda^{-1}, \quad \det(D)^{1/n} \geqslant \mu$$

imply $\det(\tau C + (1 - \tau)D)^{1/n} \geqslant \mu$ with equality only if $D = C$. This is well known. It is proved by transforming C and D simultaneously to diagonal form and then applying the inequality

$$\prod_{i=1}^{n} (\tau\gamma_i + (1 - \tau)\delta_i)^{1/n} \geqslant \tau \prod_{i=1}^{n} \gamma_i^{1/n} + (1 - \tau) \prod_{i=1}^{n} \delta_i^{1/n}.$$

Moreover, K_m possesses a tangent hyperplane at the origin. This will be shown by developing (1) into a power-series in the elements of C and taking the linear terms only. In point of fact, write (1) in the form

$$1 + m'Cm\,\mu(A)^{-1} \leqslant \det(E + A^{-1}C)^{1/n}.$$

For the half-space determined by the tangent hyperplane and containing K_m, we then obtain the linear inequality

$$m'Cm\,\mu(A)^{-1} \leqslant \frac{1}{n}\operatorname{tr}(A^{-1}C).$$

Restricting C to H, we obtain

$$l_m(C) = m'Cm \leqslant 0.$$

Next we show that (a) is equivalent to

(b) The half-spaces $l_m(C) < 0$ cover the whole space H except O.

First suppose (a) holds. Let $C \neq O$ be any point of H. It follows from (a) that there exist an m and a $\lambda > 0$ such that λC is in $L_m = H \cap K_m$. Since L_m is strictly convex, μC is an inner point of L_m if $0 < \mu < \lambda$, and thus

$$l_m(C) = \mu^{-1} l_m(\mu C) < 0,$$

which proves (b). Conversely, suppose (b) holds. Let S be the unit sphere in H. For every $C \in S$ there is an m with $l_m(C) < 0$. Since $l_m = 0$ is the tangent hyperplane of L_m at O, there exists a $\lambda > 0$ such that λC is an inner point of

L_m. Then there is a neighbourhood U of C on S such that $\mu D \in L_m$ for every $D \in U$ and $0 < \mu \leqslant \lambda$. As S is compact, it is covered by a finite number of U's. Denote by λ_0 the minimum of the corresponding λ's. Then the solid sphere of radius λ_0 is contained in $\bigcup_m L_m$, which proves (a). Transforming (b) into a statement about the complementary half-spaces $l_m(C) \geqslant 0$, we get

(c) O is the only point of H common to all the half-spaces $l_m(C) \geqslant 0$.

Now, let H' be the space of linear forms on H, and $M \subset H'$ the convex set generated by O and the l_m. Since the elements l of any hyperplane in H' passing through the origin satisfy an equation $l(C) = 0$ with some fixed $C \neq O$, the statement (c) means that there is no hyperplane through O in H' leaving M on one side. Since M is convex, a neighbourhood of O in H' is contained in M. This assertion can be divided into two parts. First, H' is the linear space generated by M, i.e., M is not contained in any hyperplane in H'. This means that there is no hyperplane passing through O and the l_m. Second, O is an inner point of M relative to the linear space generated by M, i.e., there are numbers ρ_0, $\rho_m > 0$ with sum 1, such that $O = \rho_0 . O + \sum_m \rho_m l_m$. We may multiply this equation by an arbitrary positive number, and so the condition that the sum of the coefficients is 1 may be dropped. We have the following two statements which, together, are equivalent to (c).

(d) The equations $l_m(C) = 0$ have no common solution $C \neq O$ in H.

(e) There exist positive numbers ρ_m such that $\sum_m \rho_m l_m(C) = 0$ for all C in H.

Since H is defined by $\mathrm{tr}(A^{-1}C) = 0$, (e) is equivalent to

$$\sum_m \rho_m \, m'Cm = \sigma \, \mathrm{tr}(A^{-1}C) \qquad \text{for all } C \text{ in } R, \tag{2}$$

with some constant σ. Putting $C = A$ we get $\sigma > 0$. If $C = x.x'$ we obtain

$$\sum_m \rho_m (m'x)^2 = \sigma \, \mathrm{tr}(A^{-1}xx') = \sigma \, \mathrm{tr}(x'A^{-1}x) = \sigma \, x'A^{-1}x. \tag{3}$$

This means that A is eutactic. Conversely (2) follows from (3), since every symmetric matrix C is a linear combination of matrices of the type xx' (this is nothing else than the well-known theorem that every quadratic form is a linear combination of squares of linear forms). Finally, (d) and (e) also imply that the equations $m'Cm = 0$ have no common solution in R, except $C = O$. For, if C is a solution, (2) implies $C \in H$ and then $C = O$ according to (d). This means that A is perfect and so we have proved

VORONOI'S THEOREM. *A positive definite quadratic form is extreme if and only if it is both perfect and eutactic.*

3. The new senary extreme form. The senary form

$$x'Ax = \sum_{i=1}^{3} (x_i^2 - x_i x_{i+3} + x_{i+3}^2) + \left(\sum_{i=1}^{6} x_i\right)^2$$

https://doi.org/10.4153/CJM-1955-018-2 Published online by Cambridge University Press

with the matrix

$$A = \begin{pmatrix} 2 & 1 & 1 & \frac{1}{2} & 1 & 1 \\ 1 & 2 & 1 & 1 & \frac{1}{2} & 1 \\ 1 & 1 & 2 & 1 & 1 & \frac{1}{2} \\ \frac{1}{2} & 1 & 1 & 2 & 1 & 1 \\ 1 & \frac{1}{2} & 1 & 1 & 2 & 1 \\ 1 & 1 & \frac{1}{2} & 1 & 1 & 2 \end{pmatrix}$$

has determinant $2^{-6}.3^3.13$ and minimum 2. There are 21 pairs $\pm m_i$ of minimal vectors. First, the pairs $\pm m_i$ $(i = 1, \ldots, 6)$ of unit vectors with ith coordinate ± 1, all others 0; second, 12 pairs $\pm m_i$ $(i = 7, \ldots, 18)$ with $x_k = 1$, $x_l = -1$ $(k \equiv l \bmod 3)$ and $x_j = 0$ if $j \neq k, l$; third, three pairs $\pm m_i$ $(i = 19, 20, 21)$ with coordinates obtained from $x_1 = x_4 = 1$, $x_2 = x_5 = -1$, $x_3 = x_6 = 0$ by permuting the values $1, -1, 0$. That A is perfect is seen by an easy calculation. That it is eutactic follows from the identity

$$(4) \qquad 39\, y'Ay = 6\sum_{i=1}^{6} (m_i'Ay)^2 + 5\sum_{i=7}^{18} (m_i'Ay)^2 + 7\sum_{i=19}^{21} (m_i'Ay)^2$$

which, by the substitution $y = A^{-1}x$, yields a formula of type (3). The representation (4) of $y'Ay$ as a linear combination of the squares of the linear forms $m_i'Ay$ is unique. This fact is important for the determination of the group of automorphs of A, i.e., of those unimodular matrices U which transform A into itself: $U'AU = A$. At the first glance there is a group G of 48 automorphs, namely those permutations of the variables x_i, which change each pair (x_i, x_{i+3}) into a pair of the same kind. We shall show that G combined with $\pm E$ is the whole group of automorphs of A. Obviously every U permutes the minimal vectors and preserves the scalar products $m_i'Am_k$. Now U transforms the representation (4) into another of the same kind, with Um_i instead of m_i. Since (4) is unique and the first coefficient, 6, is different from the two others, 5 and 7, U permutes the pairs $\pm m_i$ $(i = 1, \ldots, 6)$ amongst each other. This permutation is such that any quadruple $\pm m_i$, $\pm m_{i+3}$ changes into one of the same kind, because $m_i'Am_k = 1$ or $\neq 1$ according as $i \not\equiv k$ or $i \equiv k \bmod 3$. Hence we can write every automorph as a product of an element of G by an automorph V with $Vm_i = \pm m_i$ $(i = 1, \ldots, 6)$. As $m_i'Am_k \neq 0$, the sign must be the same for all i and so $V = \pm E$. Therefore the total group of automorphs is the direct product of G and the cyclic group $\pm E$ of order two.

As we have seen, the group of automorphs is not transitive on the minimal vectors, contrary to most other known extreme forms **(2)**, nor is it irreducible. The irreducible subspaces are: One of dimension one, generated by

$$\sum_{i=1}^{6} m_i;$$

one of dimension two, generated by m_{19}, m_{20}, m_{21}; one of dimension three, generated by $n_1 = m_1 - m_4$, $n_2 = m_2 - m_5$, $n_3 = m_3 - m_6$. The representation

https://doi.org/10.4153/CJM-1955-018-2 Published online by Cambridge University Press

of G in the third subspace is isomorphic. G induces all transformations of the form $n_i \to \pm n_k$, $i \to k$ being any permutation and $\pm$ any combination of signs. So G is isomorphic to the extended octahedral group. This completes the determination of the structure of the group of automorphs.

References

1. E. S. Barnes, *Note on extreme forms*, Can. J. Math. *7* (1955), 150–154.
2. H. S. M. Coxeter, *Extreme forms*, Can. J. Math. *3* (1951), 391–441.
3. N. Hofreiter, *Ueber Extremformen*, Monatsh. Math. Phys. *40* (1933), 129–152.
4. G. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques*, J. reine angew. Math. *133* (1908), 97–178.

Universität Heidelberg

https://doi.org/10.4153/CJM-1955-018-2 Published online by Cambridge University Press