THE POLYHEDRON \(\mu(m)\) AND SOME EXTREMAL PROBLEMS IN THE GEOMETRY OF NUMBERS

1970

SovietRxiv

Abstract

Full Text

UDC 511

S. S. RYSHKOV

THE POLYHEDRON $\mu(m)$ AND SOME EXTREMAL PROBLEMS IN THE GEOMETRY OF NUMBERS

(Presented by Academician I. M. Vinogradov on 10 III 1970)

§ 1. 1°. In his famous paper ((1), p. 171; see also (2,3)), G. F. Voronoi, in order to solve the question of locally densest lattice packings of n-dimensional balls, constructs in the space of coefficients of quadratic forms in n variables a certain polyhedron π and studies its properties in detail. It turned out, however, that the problem is solved much more simply (§ 3) by constructing the surface $\mu(m)$ —the surface of the constant arithmetic minimum m of positive quadratic forms. This surface turns out to be a polyhedron (§ 2), perhaps more convenient for study than the polyhedron π.

The introduction into the geometry of numbers of the idea of the polyhedron $\mu(m)$ makes it possible to view from a unified standpoint the above-mentioned problem on the locally densest lattice packing of n-dimensional balls (1,4,5), the problem of the extremal n-dimensional ζ-function (6–8), and also to solve two new extremal problems (§ 3.4° and § 7); moreover, this standpoint turns out to be the very same as that from which in the paper (9) the theory of the least dense lattice coverings of n-dimensional space by equal balls is presented.

The polyhedron $\mu(m)$ has made it possible to establish an exact connection between Voronoi' s method (1) and Minkowski' s method (4) for solving the problem on locally densest lattice packings of equal n-dimensional balls.

2°. To every quadratic form in n variables, of the form $\sum a_{ij}x^{ix^j}$ (here, as throughout the paper, summation is over all i and j from 1 to n), we put in correspondence, in the N-dimensional, where $N = n(n+1)/2$, arithmetic space E^N, a point $\{a_{ij}\}$ with coordinates $\{a_{11}, a_{22}, \dots, a_{nn}, a_{12}, a_{13}, \dots, a_{n-1\,n}\}$. It is known (2) that the set K of such points which correspond to positive definite forms is a convex conical set with vertex at the origin.

To every nonzero quadratic form in n variables, of the form $\sum a^{ij}x_{ix}j$, we shall put in correspondence the plane $\{a^{ij}\}_m$ in the space E^N with equation $\sum a^{ij}v_{ij} = m$, where by $\{v_{ij}\}$ the coordinates of points of the space E^N are denoted.

Let an arbitrary linear transformation s (with matrix $\|s\|$) of the variables x^i be given; then the transformation S of the space E^N, given by the formula $\|a'_{ij}\| = \|s\|^T \|a_{ij}\| \|s\|$, will be called the transformation generated by the transformation s. The transformation S is, obviously, linear, and its coefficients depend quadratically on the coefficients of the transformation s. We shall mainly be interested in the group $\{g\}$—the group of all integral unimodular transformations of the variables x^i, and in the group $\{G\}$ generated by it of certain (also integral and unimodular) transformations of the space E^N [7].

§ 2. **The polyhedra $M(m)$ and $\mu(m)$. Definition and properties.** Let an arbitrary system $\{q^i\} = \{q^1, q^2, \dots, q^n\}$ of integers be given, having no common divisor (a primitive system); to this system let us put in correspondence the half-space of the space E^N given by the inequality $\sum q_{ij}^{iq^{jv}} \geq m$, where $m > 0$ is an arbitrary fixed number. The intersection of such half-spaces, corresponding to all primitive systems, will be denoted by $M(m)$. Let us list the properties of the set $M(m)$.

1°. Inside the set $\overline{M}(m)$ there are points representing, up to a positive factor, every positive form. The set $\overline{M}(m)$ is nonempty.

2°. Every point of the set $\overline{M}(m)$ corresponds to a positive form. In other words, the set $\overline{M}(m)$ lies entirely inside the cone K.

3°. The set $\overline{M}(m)$ is convex and closed. The set $\overline{M}(m)$ is the closure of the open set $M(m)$, defined as the intersection of all half-spaces $\sum q^i q^j y_{ij} > m$. The boundary $\mu(m) = \overline{M}(m) \setminus M(m)$ of the set $\overline{M}(m)$ consists of points belonging to the planes $\{q^i q^j\}_m$, where the systems $\{q^i\}$ are primitive.

4°. The surface $\mu(m)$ is the locus of points corresponding to positive quadratic forms with arithmetic minimum equal to m.

5°. Both the body $M(m)$ and the surface $\mu(m)$ are invariant with respect to the transformations of the group $\{G\}$.

6°. The body $M(m)$ (the surface $\mu(m)$) is a locally finite polyhedron. All $(N-1)$-dimensional faces of the polyhedron $M(m)$ are pairwise equivalent under the group $\{G\}$.

7°. The vertices of the polyhedron $\mu(m)$ correspond to perfect forms with arithmetic minimum equal to m. To perfect forms with arithmetic minimum m there correspond vertices of the polyhedron $\mu(m)$.

8°. Any two vertices of the polyhedron $\mu(m)$ can be joined by a chain of edges consecutively having common vertices.

9°. There exists a finite algorithm—the "Voronoi algorithm" (^{1})—for finding all vertices of the polyhedron inequivalent under the group $\{G\}$. This algorithm consists in finding the vertices of the polyhedron situated on its edges issuing from an already found and studied vertex.

§ 3. We shall now indicate the various connections between the polyhedron $\mu(m)$ and the Voronoi polyhedron π (the perfect partition).

1°. Let an arbitrary point $\{a_{ij}\} \in \mu(m)$ be given; then the plane $\{a^i\}_m$, where $a^i = a_{ij}$ for all i and j, is a supporting plane of the polyhedron π.

Conversely: let the plane $\{a_{ij}\}_m$, where $m \neq 0$, be supporting for the polyhedron π; then the point a_{ij}, where $a^i = a_{ij}$ for all i and j, belongs to the polyhedron $\mu(m)$. This is proved by considering the mutually corresponding primitive systems $\{q^i\}$ and $\{q_i\}$.

2°. **Theorem 1.** *The polyhedron $\mu(m)$ is combinatorially dual to the perfect partition of the cone K (the totality of the finite faces of the polyhedron π); moreover, the infinite faces of the polyhedron $\mu(m)$ correspond to the faces of the elements of the perfect partition (of the polyhedron π) lying on the boundary of the cone K, and conversely.*

3°. As is known (2), a large part of Voronoi' s memoir (1) is devoted to the study of the properties of the polyhedron π. Therefore many properties of the polyhedra $M(m)$ and $\mu(m)$ can be obtained on the basis of our theorem from the already known properties of the polyhedron π. Examples are properties 5°, 7°, 8°, and 9° from § 2. We note, however, that property 8° is much more visual than the following dual property of the polyhedron π proved by Voronoi:

"Every two $(N-1)$-dimensional faces of the polyhedron π can be joined by a chain of its faces consecutively adjacent along $(N-2)$-dimensional faces."

§ 4. The polyhedron $\mu(m)$ and locally densest packings of n-dimensional balls.

1°. Introducing the polyhedron $\mu(m)$ into consideration makes very visual both fundamental theorems (of Korkin–Zolotarev and of Voronoi) of the theory of locally densest lattice packings of equal balls in n-dimensional space. We shall prove one of them completely, and shall only formulate the second in our terms.

2°. **Korkin-Zolotarev Theorem** (1). *A positive quadratic form is extreme if and only if it is perfect.*

We shall prove this theorem in the following, obviously equivalent, form.

A local minimum of the discriminant of a positive quadratic form with fixed arithmetic minimum can be attained only on forms corresponding to vertices of the polyhedron $\mu(m)$.

Proof. Consider an arbitrary point $\{a^0_{ij}\}$ of the polyhedron $\mu(m)$ which is not one of its vertices. Consider also the equidiscriminant surface $\det(a_{ij}) = \text{const}$ passing through this point, and an arbitrarily small segment with midpoint at this point $\{a^0_{ij}\}$ and lying entirely in the polyhedron $\mu(m)$. Since the equidiscriminant surface is strictly convex (4,3), at least one half of the segment lies from it on the same side as the origin. Consequently, all points of this half of the segment correspond to forms with the same arithmetic minimum as at the point $\{a^0_{ij}\}$, but with a smaller discriminant. The theorem is completely proved.

3°. **Voronoi's theorem** (^{1}) **in our formulation, equivalent to the classical one.** *A vertex of the polyhedron $\mu(m)$ corresponds to an extreme form if and only if the plane tangent to the surface of equal discriminant passing through this point has, in its neighborhood, no more than one common point with the polyhedron $\mu(m)$.*

The proof is practically obvious.

4°. With the aid of a certain modification of the polyhedron $\mu(m)$ one can solve the problem of the densest lattice packings of equal spheres, namely prove the following theorem:

Theorem 2. *To find all locally densest lattice packings of equal n-dimensional spheres it is sufficient to consider only a finite number of quadratic forms. The algorithm for finding such forms is connected with the investigation of the polyhedron $\mu(m)$, the determination of the domains of types of n-dimensional lattices* ((^{1}), p. 239) *and the solution of algebraic equations of degree $n+1$.*

We shall return to a more detailed study of lattice packings in one of the subsequent publications.

§ 5. **The polyhedron $\mu(m)$ and the reduction of positive quadratic forms according to Hermite-Minkowski.** Consider in the space E^N the domain $\mathfrak{M}$ of reduction of quadratic forms in the sense of Minkowski (^{4,10}) and the domains $\mathfrak{M}_i$—its images under all transformations g_i. Obviously, the totality of the domains $\mathfrak{M}_i$ forms a decomposition of the cone K, which we shall denote by $\{\mathfrak{M}\}$. Consider also in the space E^N the totality of infinite pyramids constructed on the (closed) faces of the polyhedron $\mu(m)$, with common vertex at the origin. This totality $\{M_i\}$ also forms a decomposition of the cone K.

Theorem 3. *The decomposition $\{\mathfrak{M}\}$ is an (infinite) subdivision of the decomposition $\{M_i\}$.*

It follows from Theorem 3 that every perfect form is a "generic" form of the Minkowski domain $\mathfrak{M}$. Previously (^{4,11}) this was known only for extreme forms.

§ 6. **The polyhedron $\mu(m)$ and the problem of an extremal n-dimensional ζ-function.**

1°. Important problems of applied analysis lead to the question of finding lattices which, among lattices with the same determinant, give a local minimum of the function $\zeta(a_{ij}, m)$ for a fixed value of the parameter m. Some results on this question were obtained in works ($^{6-8}$); the necessary definitions and some further references are also given there. In this paragraph we study the surface $\zeta(a_{ij}, m) = C$ lying in the cone K. The study of such surfaces is important because every point of tangency of the surface $\zeta(a_{ij}, m) = C$ with the surface $\det(a_{ij}) = \text{const}$ is a critical point of our extremal problem, and every such point $\{a_{ij}^0\}$ of tangency of these surfaces, in a sufficiently small neighborhood of which the surface $\zeta(a_{ij}, m) = \zeta(a_{ij}^0, m)$ lies inside the body $\det(a_{ij}) = \det(a_{ij}^0)$, is the desired local minimum.

For each fixed value of the parameter $m > n/2$, the surfaces $\zeta(a_{ij}, m) = t_1$ and $\zeta(a_{ij}, m) = t_2$ are homothetic with respect to the origin; therefore we fix the number t equal to 2 and shall consider only the surface $\zeta(a_{ij}, m) = 2$, which we denote by ζ_m.

2°. **Theorem 4.** *For any $\varepsilon > 0$ there exists an m_0 such that, for all $m > m_0$, the surface ζ_m is contained between the surfaces $\mu(1+\varepsilon)$ and $\mu(1)$.*

Theorem 4 makes more transparent many results cited above, especially the results of paper (^{7}).

§ 7. The polyhedron $M(m)$ and the (r, R)-problem.

1°. Consider an arbitrary (r, R)-system $\mathcal{E} \in E^n$ (^{5}), and find the numbers r^* and R^*, which are respectively the upper and lower bounds of such numbers r' and R' for which the system $\mathcal{E}$ is also an (r', R')-system. Denote by $\varkappa(n)$ the lower bound of the ratio R^*/r^* over all (r, R)-systems of the space E^n. Denote by $\varkappa_\Gamma(n)$ the lower bound of the ratio R^*/r^* over all lattice (r, R)-systems, i.e. over all lattices of the space E^n.

Theorem 5. *The inequalities*

$$1 \geq \varkappa(n) \geq \sqrt{n/2(n+1)}$$

hold.

The upper estimate can be obtained by a known simple inductive construction, the lower one by considering the upper bound of the ratio of the length of the smallest edge of an inscribed polyhedron (the polyhedron L from the decomposition $\{L\}$ corresponding to the (r, R)-system $\mathcal{E}$) to the radius of the sphere circumscribed about it. This upper bound is equal to $\sqrt{2(n+1)/n}$ and is attained on a regular simplex.

2°. Denote by Δ an arbitrary domain of the type of n-dimensional lattices ((^{1}), p. 239), and by $\{G^*\}$ the subgroup of those transformations $G^* \in \{G\}$ with respect to which the domain Δ is invariant.

Theorem 6. *The set of points $\{a_{ij}\} \in \Delta$ corresponding to lattices giving a local minimum of the ratio R^*/r^* among lattices of type Δ is a convex cone $Q \in \Delta$ with vertex at the origin. The cone Q is invariant with respect to the group $\{G^*\}$.*

The theorem is proved by comparing the body $M(m)$ and the convex bounded body $\widetilde{W}(\Delta)$ constructed in (^{3})–the set of those points $\{a_{ij}\} \in \Delta$ to which lattices with covering radius not exceeding one correspond.

We note that in this analogue of the Barnes-Dickson theorem (11) we cannot assert a pure uniqueness theorem, since the surface $\mu(m)$, unlike the equidiscriminant surface, is not strictly convex.

3°. **Theorem 7.** *Among the points of the cone Q there are points invariant with respect to the group $\{G^*\}$.*

Theorem 7 gives us the possibility of indicating the "best" ratio R^*/r^* for lattices of the first type; this ratio is equal to $\sqrt{(n+2)/12}$ and is attained on the lattice Γ_1^n—the principal lattice of the first type ((1), p. 239).

4°. From our theorems it follows: A. $\varkappa(2) = \sqrt{1/3}$, since this value is attained on the lattice Γ_1^2, constructed on a regular triangle. B. The lattice Γ_1^2 gives a strict and moreover unique local minimum of our problem. C. $\varkappa_\Gamma(3) = \sqrt{5/12}$, since all three-dimensional lattices have one and the same type. D. For $n < 10$ we have

$$\varkappa(n) \leq \varkappa_\Gamma(n) \leq \sqrt{(n+2)/12} < 1.$$

Steklov Mathematical Institute
Academy of Sciences of the USSR
Moscow

Received
19 II 1970

Cited Literature

[1] G. F. Voronoi, *Collected Works*, 2, Kiev, 1952.
[2] B. A. Venkov, in the book: G. F. Voronoi, *Collected Works*, 2, Kiev, 1952, p. 379.
[3] B. A. Venkov, *Izv. AN SSSR, Ser. Mat.*, 4, No. 1 (1940).
[4] H. Minkowski, *Ges. Abh.*, 2, Leipzig—Berlin, 1911, S. 53.
[5] B. N. Delone, *UMN*, 3 (1937).
[6] B. N. Delone, N. N. Sandakova, S. S. Ryshkov, *DAN*, 162, No. 6 (1965).
[7] B. N. Delone, S. S. Ryshkov, *DAN*, 173, No. 5 (1967).
[8] S. S. Ryshkov, *DAN*, 184, No. 2 (1969).
[9] B. N. Delone, N. P. Dolbilin, S. S. Ryshkov, M. I. Shtogrin, *Izv. AN SSSR, Ser. Mat.*, 30, No. 2 (1970).
[10] B. L. van der Waerden, *Acta Math.*, 96, No. 3-4 (1956).
[11] E. S. Barnes, T. J. Dickson, *J. Austral. Math. Soc.*, 7, 1 (1967).

Note: Figure translations are in progress. See original paper for figures.