AN ELEMENTARY PROOF OF MINKOWSKI'S SECOND INEQUALITY

I. DANICIC

(Received 22 March 1968)

1. Introduction

Let K be an open convex domain in n-dimensional Euclidean space, symmetric about the origin O, and of finite Jordan content (volume) V. With K are associated n positive constants $\lambda_1, \lambda_2, \cdots, \lambda_n$, the 'successive minima of K' and n linearly independent lattice points (points with integer coordinates) $\boldsymbol{P}_1, \boldsymbol{P}_2, \cdots, \boldsymbol{P}_n$ (not necessarily unique) such that all lattice points in the body $\lambda_j K$ are linearly dependent on $\boldsymbol{P}_1, \boldsymbol{P}_2, \cdots, \boldsymbol{P}_{j-1}$. The points $\boldsymbol{P}_1, \cdots, \boldsymbol{P}_j$ lie in λK provided that $\lambda > \lambda_j$. For $j = 1$ this means that $\lambda_1 K$ contains no lattice point other than the origin. Obviously

$$0 < \lambda_1 \leqq \lambda_2 \leqq \cdots \leqq \lambda_n.$$

The inequality of Minkowski which we are going to prove is

$$\lambda_1 \lambda_2 \cdots \lambda_n V \leqq 2^n.$$

This is best possible, e.g. when K is a parallelopiped with sides parallel to the coordinate axes. Apart from its intrinsic interest this inequality provides a powerful tool for obtaining upper bounds for the number of solutions of Diophantine inequalities (see [3]). Apart from Minkowski's difficult proof [5] there are proofs by Davenport [2] and Weyl [4] the latter being also difficult and long. Davenport's proof is very short but contains difficulties which are discussed in [6]. On the other hand Minkowski's 'first inequality' which is a special case of the second has been proved in a very simple way by Minkowski and in a particularly elegant way by Mordell [1]. We combine here the basic ideas of Davenport and Mordell to give an elementary and self-contained proof.

2. Preliminaries

For a large positive integer l let $N(l)$ denote the number of lattice points $(u_1, \cdots, u_n)$ for which the point

$$\left(\frac{2u_1}{l}, \frac{\lambda_1}{\lambda_2}\frac{2u_2}{l}, \cdots, \frac{\lambda_1}{\lambda_n}\frac{2u_n}{l}\right)$$

lies in $\lambda_1 K$. From the definition of Jordan content it follows almost at once that

$$\lim_{l\to\infty} \frac{N(l)2^n\lambda_1^{n-1}}{l^n\lambda_2\cdots\lambda_n} = \text{content of } \lambda_1 K = \lambda_1^n V$$

so that

$$\lim_{l\to\infty} \frac{N(l)}{l^n} = 2^{-n}\lambda_1\lambda_2\cdots\lambda_n V.$$

Minkowski's second inequality is therefore equivalent to the lemma proved below.

3. Lemma

$$N(l) \leqq l^n(1+o(1)) \quad as \quad l\to\infty.$$

PROOF. Since $\boldsymbol{P}_1, \cdots, \boldsymbol{P}_n$ are linearly independent lattice points there is an integral unimodular matrix A such that $A(\boldsymbol{P}_1, \cdots, \boldsymbol{P}_n)$ is an upper triangular matrix i.e. all its elements below the principal diagonal are zero. The body AK is again symmetric in the origin, convex and open. Since A transforms the integral lattice into itself, the successive minima of AK are again $\lambda_1, \cdots, \lambda_n$. By considering the number of points

$$\left(\frac{u_1}{l}, \cdots, \frac{u_n}{l}\right)$$

which lie in K or in AK it follows that K and AK have the same content and we may thus interpret $N(l)$ as being the number of points

$$\left(\frac{2u_1}{l}, \frac{\lambda_1}{\lambda_2}\frac{2u_2}{l}, \cdots\right)$$

which lie in ${}_1AK$. We therefore denote AK by K in the following. As a consequence, if $(u_1, \cdots, u_n)$ is a lattice point such that

$$(1) \qquad \begin{aligned} &(u_1, \cdots, u_n) \in \lambda_r K \qquad \text{then} \\ &u_r = u_{r+1} = \cdots = u_n = 0. \end{aligned}$$

We now divide the points contributing to $N(l)$ into two types, the good and the bad points. Put

$$c_r = \left(\frac{\lambda_{r+1}}{\lambda_r} - 1\right)\frac{\lambda_r}{\lambda_1}.$$

For any r, $1 \leqq r \leqq n-1$ for which $c_r \neq 0$ and integers $v_1, \cdots, v_n$ let $s_r(v_1, \cdots, v_n)$ be the hypercube

$$\frac{2v_i}{c_r l} \leqq x_i \leqq \frac{2(v_i+1)}{c_r l} \qquad (i = 1, \cdots, n).$$

https://doi.org/10.1017/S1446788700007023 Published online by Cambridge University Press

We call this hypercube bad if it has at least one point in $\lambda_1 K$ and at least one point not in $\lambda_1 K$. From the definition of Jordan content it follows that if $M_r(l)$ is the number of bad hypercubes $s_r(v_1, \cdots v_n)$ then

$$\lim_{l\to\infty} \left(\frac{2}{c_r l}\right)^n M_r(l) = 0. \tag{2}$$

We call the point

$$\left(\frac{2u_1}{l}, \frac{\lambda_1}{\lambda_2}\frac{2u_2}{l}, \cdots, \frac{\lambda_1}{\lambda_n}\frac{2u_n}{l}\right)$$

bad if it lies in some bad hypercube s_r, for some r. The number of such points in a particular hypercube is obviously $O(1)$ and the total number of bad points is therefore

$$\sum_{r<n} O(M_r(l)) = o(l^n) \quad \text{by (2).}$$

We shall show that the number of good (= not bad) points is at most l^n, from which the lemma follows. Let

$$\boldsymbol{X}_1 = \left(\frac{2u_1}{l}, \frac{\lambda_1}{\lambda_2}\frac{2u_2}{l}, \cdots, \frac{\lambda_1}{\lambda_n}\frac{2u_n}{l}\right)$$

be any good point of $\lambda_1 K$.

The vector consisting of the last $n-r$ coordinates of $\boldsymbol{X}_1$ we denote by X^*_{r+1}. Since $\boldsymbol{X}_1$ is a good point it is contained in a good hypercube $s_r(v_1, \cdots, v_n)$ for each r for which $c_r \neq 0$. This hypercube s_r therefore lies in $\lambda_1 K$ and hence the point

$$\left(\frac{2v_1}{c_r l}, \cdots, \frac{2v_r}{c_r l}, X^*_{r+1}\right)$$

is in $\lambda_1 K$. We can therefore assign to every X^*_{r+1} an integral vector $\boldsymbol{V}_r = (V_1, \cdots, V_r)$ such that

$$\left(\frac{2\boldsymbol{V}_r}{c_r l}, X^*_{r+1}\right) \in \lambda_1 K \tag{3}$$

and if $c_r = 0$ we take $\boldsymbol{V}_r = (0, 0, \cdots 0)$. It is important to note that $\boldsymbol{V}_r$ depends only on $u_{r+1}, \cdots, u_n$. If $\boldsymbol{X}$ and $\boldsymbol{Y}$ are two points of $\lambda_r K$ $(r < n)$ then

$$\boldsymbol{X} + \left(\frac{\lambda_{r+1}}{\lambda_r} - 1\right) \boldsymbol{Y} \in \lambda_{r+1} K. \tag{4}$$

By (3)

$$\frac{\lambda_r}{\lambda_1}\left(\frac{2\boldsymbol{V}_r}{c_r l}, X^*_{r+1}\right) \in \lambda_r K.$$

https://doi.org/10.1017/S1446788700007023 Published online by Cambridge University Press

Starting with X_1 we define a point X_r of $\lambda_r K$ inductively by the formula

$$(5)\quad \begin{aligned} X_{r+1} &= X_r + \left(\frac{\lambda_{r+1}}{\lambda_r} - 1\right)\frac{\lambda_r}{\lambda_1}\left(\frac{2V_r}{c_r l}, X^*_{r+1}\right) \\ \text{i.e.}\quad X_{r+1} &= X_r + \left(\frac{2V_r}{l}, c_r X^*_{r+1}\right) \end{aligned}$$

which by (4) lies in $\lambda_{r+1}K$, even if $c_r = 0$. Since

$$c_r = \frac{\lambda_{r+1} - \lambda_r}{\lambda_1}$$

it follows by induction from (5) that

$$(6)\quad X_r = \left(\frac{2u_1}{l}, \cdots, \frac{2u_r}{l}, \frac{\lambda_r}{\lambda_{r+1}}\frac{2u_{r+1}}{l}, \cdots, \frac{\lambda_r}{\lambda_n}\frac{2u_n}{l}\right) + \sum_{j=1}^{r-1}\frac{2}{l}(V_j, O)$$

from which it can be seen that

$$(7)\quad X_r = \left(\cdots, \frac{2u_r}{l}, \frac{\lambda_r}{\lambda_{r+1}}\frac{2u_{r+1}}{l}, \cdots, \frac{\lambda_r}{\lambda_n}\frac{2u_n}{l}\right).$$

For given integers $k_1, \cdots, k_n$ satisfying $0 \leqq k_i < l$ we consider those good points X_1 which satisfy

$$\frac{l}{2}X_n \equiv (k_1, k_2, \cdots, k_n) \pmod{l}.$$

This has a meaning since $(l/2)X_n$ is a lattice point and every point X_n satisfies such a congruence. We shall show that there is at most one such point X_1. If

$$X'_1 = \left(\frac{2u'_1}{l}, \cdots, \frac{\lambda_1}{\lambda_n}\frac{2u'_n}{l}\right)$$

is another such point, then denoting corresponding quantities by using accents, we have

$$(8)\quad \frac{l}{2}X_n \equiv \frac{l}{2}X'_n \pmod{l}.$$

Putting

$$X = \frac{X_n - X'_n}{2}$$

we have that $X \in \lambda_n K$, by the convexity and symmetry of $\lambda_n K$, and by (8) X is a lattice point. Since the n'th coordinate of X is $(u_n - u'_n)/l$ and all coordinates are integers it follows from (1) that $u_n = u'_n$. Since V_{n-1} depends only on u_n it follows that $V_{n-1} = V'_{n-1}$. Suppose we have already proved that $u_j = u'_j$ for $j = n, \cdots, r+1$. This implies $V_j = V'_j$ for $j = n-1, \cdots, r$. Hence, by (6),

$$X = \tfrac{1}{2}(X_r - X'_r) \in \lambda_r K$$

which by (7) and (1) implies $u_r = u'_r$. Thus corresponding to given $k_1, \cdots, k_n$ there is at most one point X_1 and since there are l^n sets $(k_1, \cdots, k_n)$ there are at most l^n points X_1, and the lemma follcws.

References

[1] Mordell, L. J., 'On some arithmetical results in the Geometry of Numbers', *Compositio Math.* 1 (1934).

[2] Davenport, H., Minkowski's inequality for the minima associated with a convex body', *Quarterly J. of Math.* (10) 38 (1939), 119–121.

[3] Davenport, H., 'Indefinite quadratic forms in many variables (II)', *Proc. Lond. Math. Soc.* (3) 8 (1958), 109–126.

[4] Weyl, H., 'On Geometry of Numbers', *Proc. Lond. Math. Soc.* (2) 47 (1942), 268–289.

[5] Minkowski, H., *Geometrie der Zahlen* (Teubner 1896) chapter 5.

[6] Bambah, R. P., Woods, A. C. and Zassenhaus, H., 'Three proofs of Minkowski's second inequality in the geometry of numbers', *J. Aust. Math. Soc.* 5 (1965), 453–462.

University College of Wales
Aberystwyth
Gt. Britain