ON THE MINKOWSKI-HLAWKA THEOREM

BY
WOLFGANG M. SCHMIDT

1. Introduction

Let S be a bounded Borel set in R_n, $n \geqq 2$, of volume $V(S)$, not containing the origin O. Then $\Delta(S)$, the *critical determinant* of S, is defined as the greatest lowes bound of the determinants $d(\Lambda)$ of lattices Λ having no point in S. The Minkowski-Hlawka Theorem [3] asserts

$$Q(S) \equiv V(S)/\Delta(S) \geqq 1. \tag{1}$$

This inequality was improved by Rogers [7], [8], and Schmidt [10], [12], [13]. The best results obtained were (i) $Q(S) > 1$ for $n = 2$ (see [13, Satz 7]), (ii) $Q(S) \geqq 2(1 + 2^{1-n})^{-1}(1 + 3^{1-n})^{-1}$ (see [10]), and (iii) $Q(S) \geqq nr - 2$ for $n \geqq n_0$, where $r \sim 0.278$ (see [13, Satz 11]).

In this note we improve (i) to

$$Q(S) \geqq \tfrac{16}{15}, \tag{2}$$

and (iii) to

$$Q(S) \geqq n \log \sqrt{2} - c_1 \quad \text{for } n \geqq c_2 \qquad (\log \sqrt{2} \sim 0.346). \tag{3}$$

Our proof of (3) will be much simpler than the proof of (iii) in [13].

Ollerenshaw [5] constructed a set S_0 in R_2 with $Q(S_0) = 1.317 \cdots$, and no set with a smaller $Q(S)$ is known. Blichfeldt [1] proved

$$\limsup_{n\to\infty} \sqrt[n]{Q(B_n)} \leqq \sqrt{2} \tag{4}$$

for the unit ball B_n in R_n centered at O; and this is the best known upper estimate[1] for large n.

2. Proof of (2)

Let p be a prime. Put $(x)_p$ for the image of the integer x under the homomorphism from the integers onto the field F_p of p elements. Put ϕ_p for the mapping

$$\phi_p : g = (g^{(1)}, \cdots, g^{(n)}) \to ((g^{(1)})_p, \cdots, (g^{(n)})_p)$$

from the fundamental lattice Λ_0 onto the vector space V_p of dimension n over F_p.

It is easy to see that ϕ_p creates a 1-1 correspondence between sublattices of Λ_0 of index p and hyperplanes of V through the origin O. Clearly, a sublattice of determinant p is mapped into a linear subspace through O. The

Received April 2, 1962.

[1] For a connected account of the subject see [2].

number of points of this subspace will be p^{n-1}; hence it will be a hyperplane. On the other hand, the set of points mapped into a given hyperplane through O will be a lattice with exactly p^{n-1} points in every cube

$$c^{(i)} \leqq g^{(i)} < c^{(i)} + p \qquad (i = 1, \cdots, n);$$

hence it will be a sublattice of index p.

We divide the lattice points of Λ_0 into three classes as follows:

$$g \in T_1 \quad \text{if} \quad g \notin 3\Lambda_0;$$

$$g \in T_2 \quad \text{if} \quad g \in 3\Lambda_0 \text{ but } g \notin 2\Lambda_0;$$

$$g \in T_3 \quad \text{if} \quad g \in 6\Lambda_0.$$

Put $\mu(g) = \frac{1}{4}, \frac{3}{4}, 1$ if g is in T_1, T_2, T_3, respectively.

In the end of this section we assume $n = 2$.

LEMMA. *Assume*

$$\sum_{g \in S \cap \Lambda_0} \mu(g) < 1.$$

Then Λ_0 has a sublattice of index 2 or 3 which has no point in S.

Proof. Every lattice point in S must be of type T_1 or T_2. Assume some $g \in T_2$ is in S. Since $\mu(g) = \frac{3}{4}$, g is the only lattice point in S. $\phi_2(g) \neq O$, and hence there is a line in V_2 through O not containing $\phi_2(g)$. Thus there is a sublattice of index 2 not containing any point of S. Assume next that no point of T_2 is in S. Assume g_1, g_2, g_3 of T_1 are in S. None of $\phi_3(g_1)$, $\phi_3(g_2)$, $\phi_3(g_3)$ are O. Applying a linear nonsingular transformation in V_3, we may assume $\phi_3(g_1) = e_1$, $\phi_3(g_2) = e_2$, and $\phi_3(g_3)$ equals one or two times $e_1 + e_2$ or $e_1 + 2e_2$, where e_1, e_2 are basis vectors in V_3. (The situation is still simpler if two of the $\phi_3(g_i)$'s are dependent.) Now the line $x_1 + x_2 = 0$ (or $x_1 + 2x_2 = 0$) meets no point $\phi_3(g_i)$ $(i = 1, 2, 3)$. Hence there is a sublattice of index 3 of Λ_0 which does not meet S.

Let now dA be the invariant measure in the space of transformations A of determinant 1, first used by Siegel, normalized so that

$$\int_F dA = 1,$$

where F is a fundamental domain with regard to the subgroup of unimodular transformations. It was shown in [14] that

$$\int_F \sum_{g \neq O} \rho(Ag)\, dA = V(S),$$

where $\rho(X)$ is the characteristic function of S.

Assume now $\Delta(S) > 3$. Let A be a linear transformation of determinant 1. Then one will have $\sum_g \mu(g) \geqq 1$, where the sum is over those $g \in \Lambda_0$ where $Ag \in S$.

Put differently, we have

$$\tfrac{1}{4}\textstyle\sum_{g\epsilon\Lambda_0}\rho(Ag) + \tfrac{1}{2}\sum_{g\epsilon 3\Lambda_0}\rho(Ag) + \tfrac{1}{4}\sum_{g\epsilon 6\Lambda_0}\rho(Ag) \geqq 1.$$

By integration over F we find

$$V(\tfrac{1}{4} + \tfrac{1}{2}\cdot\tfrac{1}{9} + \tfrac{1}{4}\cdot\tfrac{1}{36}) \geqq 1;$$

hence $V \geqq \frac{16}{5}$. Since $\Delta(S) > 3$ was our only assumption, we proved (2).

3. Proof of (3)

We may assume $V \geqq 1$. Let σ be a subset of Λ_0 whose points are linearly independent mod 2. After applying a nonsingular linear transformation in V_2, we may assume that $\phi_2(\sigma)$ consists of basis vectors $e_1, \cdots, e_k$. Now the hyperplane $x_1 + \cdots + x_k = 0$ of V_2 does not meet $\phi_2(\sigma)$, and hence there is a sublattice of Λ_0 of index 2 not meeting σ.

Assume now that S is a set with $\Delta(S) > 2$. Given any linear transformation A of determinant 1, there will be a set of lattice points $g_1, \cdots, g_d$, dependent mod 2, such that $Ag_i \epsilon S$ $(i = 1, \cdots, d)$. In fact there will be a minimal dependent set of this kind, that is, a set of points dependent mod 2 such that every subset is independent mod 2. There will be a minimal dependent set of at least three lattice points, since every minimal dependent set mod 2 of two points consists of two identical points mod 2. There will either be at least $3n/4$ lattice points g_i, $Ag_i \epsilon S$, or there will be a minimal set with $3 \leqq d \leqq 3n/4$. By integration over F we obtain

$$(4/3n)\int_F \sum_g \rho(Ag)\,dA + \sum_{d=3}^{3n/4}\frac{1}{d!}\int_F \sum_{\substack{g_1,\cdots,g_d\\ \text{min. dep. mod } 2}} \rho(Ag_1)\cdots\rho(Ag_d)\,dA \geqq 1.$$

Denote the two terms to the left by I_1, I_2. Clearly, $I_1 = (4/3n)V$. In the next section we will show

$$I_2 \leqq 2^{12-n}e^V + c_3(7/8)^{n/2}V^{c_4}. \tag{5}$$

Hence either $(4/3n)V \geqq (4/3)\log 2 = c_5$, or $c_3(7/8)^{n/2}V^{c_4} \geqq (1 - c_5)/2$, or $2^{12-n}e^V \geqq (1 - c_5)/2$. Each of these inequalities yields

$$V \geqq n\log 2 - c_6 \quad \text{for } n \geqq c_7.$$

Since this holds for any S with $\Delta(S) > 2$, (3) is proved.

4. An estimate

We start by listing some needed formulas. As mentioned by Siegel and proved explicitly by Rogers [6] and Macbeath and Rogers [4],

$$\int_F \sum_{\substack{g_1,\cdots,g_m\epsilon\Lambda_0\\ \text{lin. indep.}}} \rho(Ag_1, \cdots, Ag_m)\,dA = \int\cdots\int \rho(X_1, \cdots, X_m)\,dX_1\cdots dX_m. \tag{6}$$

Here Λ_0 is n-dimensional, $m < n$, and ρ is a Borel-measurable function in $n \times m$ variables. Next, let $k \neq 0, k_1, \cdots, k_m$ be relatively prime integers. Then for $m < n$

$$\int_F \sum_{\substack{g_1,\cdots,g_m \\ \text{indep., such that} \\ k^{-1}\Sigma k_i g_i \text{ is also in } \Lambda_0}} \rho(Ag_1, \cdots, Ag_m)\, dA = k^{-n} \int \cdots \int \rho(X_1, \cdots, X_m)\, dX_1 \cdots dX_m. \tag{7}$$

This was first shown[2] in [6].

Let now $\rho_1, \cdots, \rho_{m+1}$ be characteristic functions of compact Borel sets in R_n, and $\rho_1^*, \cdots, \rho_{m+1}^*$ the characteristic functions of balls in R_n, centered at O, such that

$$\int \rho_i(X)\, dX = \int \rho_i^*(X)\, dX \qquad (i = 1, \cdots, m+1).$$

Then an inequality of Rogers [9] implies

$$\int \cdots \int \rho_1(X_1) \cdots \rho_m(X_m)\rho_{m+1}\left(\sum \alpha_i X_i\right) dX_1 \cdots dX_m \leqq \int \cdots \int \rho_1^*(X_1) \cdots \rho_m^*(X_m)\rho_{m+1}^*\left(\sum \alpha_i X_i\right) dX_1 \cdots dX_m. \tag{8}$$

Finally, let $\rho^*(X)$ be the characteristic function of a ball of volume V in R_n. Then it was shown in [13, Lemma 21] that for integers $k > 0$ and $k_i \neq 0$ $(i = 1, \cdots, m)$, for $\varepsilon > 0$ and $n > n(k, m, \varepsilon)$

$$\int \cdots \int \rho^*(X_1) \cdots \rho^*(X_m)\rho^*\left(k^{-1} \sum k_i x_i\right) dX_1 \cdots dX_m \leqq ((m+1)^{m-1}m^{-m}k^2 + \varepsilon)^{n/2}V^m. \tag{9}$$

We mention

$$(m+1)^{m-1}m^{-m} \leqq \tfrac{3}{4} < \tfrac{7}{8} \qquad (m \geqq 2) \tag{10}$$

and

$$(m+1)^{m-1}m^{-m} \leqq em^{-1}. \tag{11}$$

Now we are ready to estimate

$$I(d) = \frac{1}{d!}\int_F \sum_{\substack{g_1,\cdots,g_d \\ \text{min. dep. mod } 2}} \rho(Ag_1) \cdots \rho(Ag_d)\, dA.$$

At first we take the part of the sum where $g_1, \cdots, g_d$ are independent over the rationals. We have $g_d = g_1 + \cdots + g_{d-1} + 2h$, where $g_1, \cdots, g_{d-1}, h$

[2] The best way to arrive at (7) is to prove (6) as in [4], and then to apply the method at the end of [11] to derive (7) from it.

are independent over the rationals, and using (6) we obtain

$$\frac{1}{d!}\int\cdots\int\rho(X_1)\cdots\rho(X_{d-1})\rho(X_1+\cdots+X_{d-1}+2Y)\,dX_1\cdots dX_{d-1}\,dY = 2^{-n}V^d/d!\,.$$

Next, we take the part of the sum where $g_1, \cdots, g_d$ are dependent over the rationals, say,

$$k_1 g_1 + \cdots + k_d g_d = 0 \qquad (k_i \text{ integral}).$$

We may assume that at least one k_i is odd, but then this implies that all of $k_1, \cdots, k_d$ are odd, since $g_1, \cdots, g_d$ is a minimal dependent set mod 2. By multiplying our estimates by d, we may assume $k_d = \max(|k_1|, \cdots, |k_d|)$. We obtain the bound

$$\frac{d}{d!}\sum_{\substack{k>0\\ k\text{ odd}}}\sum_{\substack{k_1,\cdots,k_{d-1}\\ \text{odd, } |k_i|\leq k}}\int_F\sum_{\substack{g_1,\cdots,g_{d-1}\\ \text{such that also}\\ k^{-1}\Sigma k_i g_i\in\Lambda_0}}\rho(Ag_1)\cdots\rho(Ag_{d-1})\rho\left(Ak^{-1}\textstyle\sum_{i=1}^{d-1}k_i g_i\right)dA$$

$$= \frac{d}{d!}\sum_{\substack{k>0\\ k\text{ odd}}}\sum_{\substack{k_1,\cdots,k_{d-1}\\ \text{odd, } |k_i|\leq k}}k^{-n}\int\cdots\int\rho(X_1)\cdots\rho(X_{d-1})\cdot\rho\left(k^{-1}\textstyle\sum_{i=1}^{d-1}k_i X_i\right)dX_1\cdots dX_{d-1}.$$

For the terms where $k > 2^{11}$, say, we estimate the integral over $X_1, \cdots, X_{d-1}$ by V^{d-1}. Thus we obtain

$$dk^{-n}(k+1)^{d-1}V^{d-1}/d! \leqq d2^{d-1}k^{d-1-n}V^{d-1}/d! \leqq n2^{3n/4}k^{d-1-n}V^{d-1}/d!\,.$$

Summing over $k > 2^{11}$ we obtain

$$n2^{3n/4}2^{-11n/4}V^{d-1}/d! < 2^{-n}V^d/d!\,.$$

Next, let $k \leqq 2^{11}$, $d > 3\cdot 2^{28} = c_4$. Using (8) we obtain

$$\int\cdots\int\rho(X_1)\cdots\rho(X_{c_4})\rho\left(k^{-1}\textstyle\sum_{i=1}^{d-1}k_i X_i\right)dX_1\cdots dX_{c_4}$$
$$\leqq \int\cdots\int\rho^*(X_1)\cdots\rho^*(X_{c_4})\rho^*\left(k^{-1}\textstyle\sum_{i=1}^{c_4}k_i X_i\right)dX_1\cdots dX_{c_4}.$$

This last integral is for large n at most $V^{c_4}(3k^2c_4^{-1})^{n/2}$ by (9) and (11). Integration over $X_{c_4+1}, \cdots, X_{d-1}$ gives a factor $V^{d-1-c_4} \leqq V^{d-c_4}$. We therefore find the bound

$$n(k+1)^{d-1}(3c_4^{-1})^{n/2}V^d/d! \leqq n2^{12n}2^{-14n}V^d/d! \leqq 2^{-n}V^d/d!$$

for our part of $I(d)$, and summation over $k \leqq 2^{11}$ gives $2^{11-n}V^d/d!$.

Finally for $k \leqq 2^{11}$, $d \leqq c_4$ we use (8), (9), and (10) and find the bound

$$(d/d!)V^{c_4}2^{12c_4}\left(\tfrac{7}{8}\right)^{n/2}.$$

Putting our estimates together we see that

$$\textstyle\sum_{3\leqq d\leqq 3n/4}I(d) \leqq 2^{12-n}e^V + c_3\left(\tfrac{7}{8}\right)^{n/2}V^{c_4}.$$

References

1. H. F. Blichfeldt, *The minimum value of quadratic forms, and the closest packing of spheres*, Math. Ann., vol. 101 (1929), pp. 605–608.
2. J. W. S. Cassels, *An introduction to the geometry of numbers*, Berlin, Springer, 1959 (Grundlehren, Bd. 99).
3. E. Hlawka, *Zur Geometrie der Zahlen*, Math. Zeitschrift, vol. 49 (1943/44), pp. 285–312.
4. A. M. Macbeath and C. A. Rogers, *Siegel's mean value theorem in the geometry of numbers*, Proc. Cambridge Philos. Soc., vol. 54 (1958), pp. 139–151.
5. K. Ollerenshaw, *An irreducible non-convex region*, Proc. Cambridge Philos. Soc., vol. 49 (1953), pp. 194–200.
6. C. A. Rogers, *Mean values over the space of lattices*, Acta Math., vol. 94 (1955), pp. 249–287.
7. ———, *The number of lattice points in a set*, Proc. London Math. Soc. (3), vol. 6 (1956), pp. 305–320.
8. ———, *Lattice covering of space: the Minkowski-Hlawka theorem*, Proc. London Math. Soc. (3), vol. 8 (1958), pp. 447–465.
9. ———, *A single integral inequality*, J. London Math. Soc., vol. 32 (1957), pp. 102–108.
10. W. Schmidt, *Eine Verschärfung des Satzes von Minkowski-Hlawka*, Monatsh. Math., vol. 60 (1956), pp. 110–113.
11. ———, *Mittelwerte über Gitter*, Monatsh. Math., vol. 61 (1957), pp. 269–276.
12. ———, *The measure of the set of admissible lattices*, Proc. Amer. Math. Soc., vol. 9 (1958), pp. 390–403.
13. ———, *Masstheorie in der Geometrie der Zahlen*, Acta Math., vol. 102 (1959), pp. 159–224.
14. C. L. Siegel, *A mean value theorem in geometry of numbers*, Ann. of Math. (2), vol. 46 (1945), pp. 340–347.

Columbia University
New York, New York