LATTICE POINTS ON THE BOUNDARY OF CONVEX BODIES

by

GEORGE EYRE ANDREWS

A THESIS

submitted to

OREGON STATE COLLEGE

in partial fulfillment of
the requirements for the
degree of

MASTER OF ARTS

June 1960

APPROVED

Redacted for privacy

Assistant Professor in Mathematics

in Charge of Major

Redacted for privacy

Chairman of Department of Mathematics

Redacted for privacy

Chairman of School of Science Graduate Committee

Redacted for privacy

Dean of Graduate School

Date thesis is presented May 12, 1960

Typed by Jolan Eross

TABLE OF CONTENTS

LATTICE POINTS ON THE BOUNDARY OF CONVEX BODIES

INTRODUCTION

The object of this thesis is to obtain an estimate of the number of lattice points in the interior of a strictly convex body with N lattice points on its surface.

By van der Corput's theorem (2, p. 71), if a convex body which is symmetric about the origin has content $v \geq m2^n$, then it contains at least m pairs of lattice points. Thus we are afforded two avenues of approach to this problem. We may either consider the interior lattice points directly, or we may consider the content of the convex body.

In Chapter I, we shall approach the problem directly using properties of "congruent" points to count interior lattice points. In Chapter II, we shall consider content estimations.

NOTATION

Throughout this thesis we shall follow as closely as possible the notation used in Sommerville, An Introduction to the Geometry of N Dimensions. By content, surface content, polytope, and parallelotope, we shall mean the n-dimensional generalizations of volume, surface

area, polyhedron, and parallelopiped respectively.

We shall use the following conventions:

$P, P', P'', Q, Q', Q'', X$ denote points;

s, s', s_1, s_i' denote open 2-dimensional segments;

$\underline{s}, \underline{s}', \underline{s_1}, \underline{s_i'}$ denote closed 2-dimensional segments;

$\underline{PQ} = \underline{s}$ and $\overline{PQ} = s$ provided P and Q are the end points of $\underline{s}$;

S_p, S_p', S_p'', S_p''' denote linear, p-dimensional spaces; we shall call a linear, p-dimensional space a p-flat (8, p.8); however, we shall call: 1-flats, "points"; 2-flats, "segments"; and (n-1)-flats, "hyperplanes";

$(Po)_n, (Po)_n^a, (Po)_n^b, (Po)_n^c$ denote n-dimensional, simple, convex polytopes (8, p. 99);

f_r, g_r, h_r denote r-dimensional boundary elements of an n-dimensional polytope; we shall call such elements r-boundaries;

n denotes the dimension of the space considered;

O denotes the origin;

Λ denotes the set of all points with integral coordinates in n-dimensional space; we are mainly concerned with this lattice, and when we refer to lattice points, we shall mean points of this lattice;

$P \equiv Q\ (k)$ means $p_i \equiv q_i \pmod{k}$, $i = 1, 2, \cdots, n$

with $P(p_1, p_2, \cdots, p_n)$ and $Q(q_1, q_2, \cdots, q_n)$;

$$\binom{m}{2} = \begin{cases} \frac{m!}{2!(m-2)!} & m \geq 2 \\ 0 & m < 2 \end{cases};$$

C always denotes an n-dimensional, closed, strictly convex body;

C* always denotes an n-dimensional, closed, strictly convex body symmetric about the origin.

A "regular supporting hyperplane to C" is a supporting hyperplane that contains only one point of C.

CHAPTER I

Minkowski proved that if there are more than $2^{n+1} - 2$ lattice points on the surface of C^*, then there is another lattice point in the interior of C^* besides the origin (2, p. 157). I shall generalize the method he used.

Lemma 1-1. If $P \equiv Q\ (k)$, then there are $(k-1)$ lattice points on the segment $\overline{PQ}$.

Proof: For any integer j,

$$P\left(p_1 + j\,\frac{q_1-p_1}{k}\ ,\ \cdots,\ q_n + j\,\frac{q_n-p_n}{k}\right)$$

is a lattice point. For $1 \leq j \leq k-1$, P_j is on $\overline{PQ}$. Q.E.D.

Lemma 1-2. The $(n-1)\times(n-1)$ determinant $D_n = |a_{ij}|$ (where $a_{ii} = 2$, $i \neq 1$; $a_{11} = 1$; $a_{ij} = 1$, $i \neq j$) is equal to 1.

Proof: We have

$$D_{n-1} = \begin{vmatrix} 1 & 1 & 1 & 1 & \cdots \\ 1 & 2 & 1 & 1 & \cdots \\ 1 & 1 & 2 & 1 & \cdots \\ 1 & 1 & 1 & 2 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \end{vmatrix}$$

$$= \begin{vmatrix} 0 & -1 & 0 & 0 & \cdots \\ 1 & 2 & 1 & 1 & \cdots \\ 1 & 1 & 2 & 1 & \cdots \\ 1 & 1 & 1 & 2 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \end{vmatrix}$$

$$= D_{n-2} .$$

Since $D_2 = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = 1$, we have

$$D_{n-1} = 1.$$

Q.E.D.

Lemma 1-3. The $(n-1)\times(n-1)$ determinant $F_{n-1} = |b_{ij}|$ (where $b_{ii} = 2$; $b_{ij} = 1$, $i \neq j$) is equal to n.

Proof: We have

$$F_{n-1} = \begin{vmatrix} 2 & 1 & 1 & 1 & \cdots \\ 1 & 2 & 1 & 1 & \cdots \\ 1 & 1 & 2 & 1 & \cdots \\ 1 & 1 & 1 & 2 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \end{vmatrix}$$

$$= \begin{vmatrix} 1 & -1 & 0 & 0 & \cdots \\ 1 & 2 & 1 & 1 & \cdots \\ 1 & 1 & 2 & 1 & \cdots \\ 1 & 1 & 1 & 2 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \end{vmatrix}$$

$$= F_{n-2} + 1 \quad \text{by Lemma 1-2.}$$

Since

$$F_2 = \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} = 3, \quad \text{we have}$$

$$F_{n-1} = n.$$

Q.E.D.

Lemma 1-4. If $x_1 + x_2 + \cdots + x_n = N$ and

$$f(x_1, \cdots, x_n) = \frac{x_1(x_1-1)}{2} + \cdots + \frac{x_n(x_n-1)}{2},$$

then

$$\min f(x_1, \cdots, x_n) = \frac{N^2}{2n} - \frac{N}{2}.$$

Proof: Since $f(x_1, \cdots, x_n) \to +\infty$ as any or all of the x_i's approach infinity, we see that there will be

at least one relative minimum. Hence we need only show that there is one and only one point at which the derivatives of f all vanish. If there is only one such point, we see that it will be the absolute minimum of the function. Since

$$f(x_1,\cdots,x_n) = \frac{x_1(x_1-1)}{2} + \cdots + \frac{x_{n-1}(x_{n-1}-1)}{2} + \frac{(N-x_1-\cdots-x_{n-1})(N-x_1-\cdots-x_{n-1}-1)}{2},$$

we have

$$\frac{\partial f}{\partial x_i} = x_i - \frac{1}{2} - \frac{(N-x_1-\cdots-x_{n-1})}{2} - \frac{(N-x_1-\cdots-x_{n-1}-1)}{2}$$

$$= -N + x_1 + x_2 + \cdots + x_{i-1} + 2x_i + x_{i+1} + \cdots + x_{n-1}.$$

Setting all of the derivatives equal to zero, we obtain $(n-1)$ equations in $(n-1)$ unknowns. The determinant of the system is the F_{n-1} of Lemma 1-3. Hence the value of the determinant is $n \neq 0$. Thus there is a unique solution to this system of equations. The solution is $x_j = \frac{N}{n}$. Hence

$$\min f(x_1,\cdots,x_n) = f\left(\frac{N}{n},\ldots,\frac{N}{n}\right) = \frac{N^2}{2n} - \frac{N}{2}.$$

Q.E.D.

Lemma 1-5. We given a set, Σ, of $2M$ elements made up of M pairs, $\{a_{i1},a_{i2}\}$. We form subsets σ_i of Σ under the following two rules:

1) not both a_{i_1} and a_{i_2} are put in the same subset σ_j ; 2) if a_{ir} and a_{jt} are put in q' then a_{iu} and a_{jv} are not put in the same subset σ_w . Under these conditions the minimum number of subsets possible to form is m where

$$\binom{m}{2} \geq M > \binom{m-1}{2} .$$

Proof: We shall first show that if $M = \binom{m}{2}$ it is possible to form m sets of $(m-1)$ elements each which obey rules 1 and 2. We have

$$\sum = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{M1} \\ a_{12} & a_{22} & \cdots & a_{M2} \end{pmatrix} .$$

Take the first $(m-1)$ elements in row 1 to form σ_1. Put $a_{12}\varepsilon\sigma_2$, $a_{22}\varepsilon\sigma_3, \ldots, a_{(m-1)2}\varepsilon\sigma_m$. Take the next $(m-2)$ elements in row 1 to complete σ_2 . Put $a_{m2}\varepsilon\sigma_3$, $a_{(m+1)}\varepsilon\sigma_4, \ldots, a_{(2m-3)2}\varepsilon\sigma_m$. Following this pattern we shall in $(m-1)$ steps fill each set σ_i with $(m-1)$ elements. Hence for each integer M such that $\binom{m-1}{2} < M \leq \binom{m}{2}$, it is possible to form m subsets of Σ obeying rules 1 and 2.

We shall now show that m cannot be improved. Our proof will be by mathematical induction.

For $M = 1$, we have

$$\Sigma = \{a_{11}, a_{12}\} .$$

By rule 1, we must form two subsets. Hence

$$\binom{m}{2} = \binom{2}{2} = 1 \geq 1 = M < \binom{2-1}{2} = 0.$$

Thus the lemma is true for $M = 1$.

Assume that the lemma is true for all $M \leq M_0-1$. If $M_0-1 \neq \binom{m}{2}$, the case is trivial. If $M_0-1 = \binom{m}{2}$, we must prove that we need at least $(m+1)$ subsets to hold $2M_0$ elements. Since $M_0-1 = \binom{m}{2}$, we may divide Σ into m sets of $(m-1)$ elements each. Since m is the least number of subsets that will hold the $2M_0-2$ elements, we must show that it is impossible to add two more elements without violating the rules. Assume we add $a_{M_0 1}$ to some set. We know that the other $(m-1)$ elements in that set each have a partner in other sets. By rule 2, the partners must all lie in different sets, and there are only $(m-1)$ other sets. Hence adding $a_{M_0 2}$ to any other set will force a violation of rule 2. Thus one more set is needed.

Q.E.D.

THEOREM 1. A closed, strictly convex body symmetric about the origin with N lattice points

on its surface contains at least $1 + \sqrt{\frac{N^2}{2^n} - 2N + 1}$ lattice points in its interior if $N > 2^{n+1}$.

Proof: Let us consider congruences modulo 2 in n dimensions. We see that there are 2^n different congruence classes possible.

We may separate the N surface lattice points into two sets, A and A^*, such that neither set contains both P and the reflection of P with respect to the origin. Each of these sets has N_0 members where $N_0 = \frac{1}{2} N$.

Let us choose the set A and distribute its members into the various congruence classes modulo 2. In each congruence class c_i containing e_i elements, we form all possible distinct pairs of which there are $\binom{e_i}{2}$. By Lemma 1-1, each of these pairs, P and Q, determines a lattice point at the middle of the segment $\underline{PQ}$. If P and Q are in the same congruence class, then $\frac{1}{2}(P + Q)$, $\frac{1}{2}(P - Q)$, $-\frac{1}{2}(P + Q)$, and $-\frac{1}{2}(P - Q)$ are all lattice points. For each pair, P and Q, let us consider $\frac{1}{2}(P + Q)$ and $\frac{1}{2}(P - Q)$ as being determined by P and Q.

Letting $2N_i$ denote the total number of lattice points we have determined of the form

$\frac{1}{2}(P + Q)$ and $\frac{1}{2}(P - Q)$, we obtain

$$N_i = \sum_{j=1}^{2^n} \binom{e_j}{2} \geq \frac{N_0^2}{2^{n+1}} - \frac{N_0}{2} \quad \text{by Lemma 1-4.}$$

In Lemma 1-5, we let $2N_i = 2M$ and

$$\left\{ \frac{P_i + Q_i}{2} , \frac{P_i - Q_i}{2} \right\} = \left\{ a_{i1}, a_{i2} \right\} ;$$

we shall say that a_{uv} and a_{rs} are in the same subset if and only if $a_{uv} = a_{rs}$. Rule 1 of Lemma 1-5 must be satisfied since

$$\frac{P_i + Q_i}{2} = \frac{P_i - Q_i}{2}$$

implies

$$Q_i = 0 .$$

Rule 2 of Lemma 1-5 must be satisfied since

$$\frac{P_i + Q_i}{2} = \frac{R_i + S_i}{2}$$

and

$$\frac{P_i - Q_i}{2} = \frac{R_i - S_i}{2}$$

imply $P_i = R_i$

and $Q_i = S_i$.

We thus obtain m as the least possible number of distinct lattice points (not counting reflections with

respect to the origin) that we have determined in the interior of the given body. Hence

$$\binom{m}{2} \geq \frac{N_o^2}{2^{n+1}} - \frac{N_o}{2} ,$$

or if $N_o > 2^n$

$$m \geq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{N_o^2}{2^{n-2}} - 4N_o + 1} \quad .$$

Since m does not count reflections, we see that we have determined $2m$ interior lattice points. Since $N_o = \frac{N}{2}$, we have

$$2m \geq 1 + \sqrt{\frac{N^2}{2^n} - 2N + 1} \quad , \quad \text{for} \quad N > 2^{n+1} \quad .$$

Q.E.D.

Let us check how well Theorem 1 agrees with the theorem of Minkowski mentioned in the prefacing remarks to Chapter I. Since the result of Theorem 1 counts the origin, we must demand that

$$1 + \sqrt{\frac{N^2}{2^n} - 2N + 1} \geq 2 ,$$

or

$$\frac{N^2}{2^n} - 2N + 1 \geq 1 \quad .$$

Thus

$$N \geq 2^{n+1}$$

Since we have required $N > 2^{n+1}$, the above becomes

$$N > 2^{n+1} \quad .$$

This result is very close to the estimate, $N > 2^{n+1}-2$, made by Minkowski. The reason that our estimate is not in complete agreement with Minkowski's is that we do not consider the origin in the c_i congruence classes.

CHAPTER II

In many instances of interest in the geometry of numbers, it is possible to express the content of a closed, strictly convex body as greater than or equal to some positive function of the surface content. In this chapter we shall estimate the surface content of a given, closed, strictly convex body C and in turn shall use our result to estimate the content of C. The major result of this chapter is Theorem 2.

THEOREM 2. We are given a closed strictly convex body C with N lattice points on its surface. If $S(C)$ denotes the surface content of the boundary of C, then there exists $k(n)$ such that

$$S(C) \geq k(n)\, N^{\frac{n+1}{n}} .$$

Before we prove this theorem, we shall prove eight lemmas.

Lemma 2-1. If $r_n(m)$ denotes the total number of representations of m as the sum of n squares, then

$$\frac{\pi^{\frac{n}{2}}\,(\sqrt{M}+\sqrt{n})^n}{\Gamma\left(\frac{n}{2}+1\right)} > \sum_{m=1}^{M} r_n(m) > \frac{\pi^{\frac{n}{2}}(\sqrt{M}-\sqrt{n})^n}{\Gamma\left(\frac{n}{2}+1\right)} .$$

Proof: Let us consider the geometrical meaning of the above sum. The sum,

$$\sum_{1}^{M} r_n(m),$$

denotes the number of lattice points inside or on the hypersphere

$$x_1^2 + x_2^2 + \cdots + x_n^2 = M.$$

Let us associate with each such lattice point the unit hypercube for which this lattice point would be the origin if this hypercube were translated into the first octant with one vertex in the origin. We see that the totality of such hypercubes forms a polytope whose entire boundary is within $\sqrt{n}$ of the boundary of the hypersphere. Since the volume of a hypersphere of radius r is $\frac{\pi^{\frac{n}{2}} r^n}{\Gamma(\frac{n}{2}+1)}$ (8, p. 136), we have

$$\frac{\pi^{\frac{n}{2}} (\sqrt{M}+\sqrt{n})^n}{\Gamma(\frac{n}{2}+1)} > \sum_{1}^{M} r_n(m) > \frac{\pi^{\frac{n}{2}} (\sqrt{M}-\sqrt{n})^n}{\Gamma(\frac{n}{2}+1)} .$$

Q.E.D.

The above inequality may be rewritten in less precise form as

$$\sum_{1}^{M} r_n(m) = \frac{\pi^{\frac{n}{2}} M^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)} + O\left(M^{\frac{n-1}{2}}\right) .$$

Lemma 2-2. If $\sum_{1}^{a} r_n(m) \leq N < \sum_{1}^{a+1} r_n(m)$, then there exist $C_1(n)$ and $C_2(n)$ such that

$$C_2(n)\, N^{\frac{2}{n}} > a > C_1(n)\, N^{\frac{2}{n}} .$$

Proof:

Since $\sum_{1}^{a+1} r_n(m) > N$, a increases with N. Hence, if $C_1(n)$ does not exist

$$a = o\left(N^{\frac{2}{n}}\right) .$$

By Lemma 2-1,

$$N < \sum_{1}^{a+1} r_n(m) < \frac{\pi^{\frac{n}{2}} \left(\sqrt{a+1} + \sqrt{n}\right)^n}{\Gamma\left(\frac{n}{2}+1\right)} = o(N).$$

This inequality is false for sufficiently large N. Hence there exists $C_1(n)$ for all N such that

$$a > C_1(n)\, N^{\frac{2}{n}} .$$

Assume $a > \left[\frac{2\,\Gamma\left(\frac{n}{2}+1\right)}{\pi^{\frac{n}{2}}}\right]^{\frac{2}{n}} N^{\frac{2}{n}}$, then

$$N \geq \sum_{1}^{a} r_n(m) = \frac{\pi^{\frac{n}{2}} a^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)} + O\left(a^{\frac{n-1}{2}}\right) > 2N - O\left(N^{\frac{n-1}{n}}\right) .$$

This inequality is false for sufficiently large N. Hence there exists $C_2(n)$ for all N such that

$$C_2(n)\, N^{\frac{2}{n}} > a .$$

Q.E.D.

Lemma 2-3. $$\sum_{m=1}^{b}\{(\sqrt{m+1} - \sqrt{m}) \sum_{1}^{m} r_n(i)\} = \frac{\pi^{\frac{n}{2}} b^{\frac{n+1}{2}}}{(n+1)\Gamma(\frac{n}{2}+1)} + O(b^{\frac{n}{2}}).$$

Proof: Using the binomial series and Lemma 2-1, we have

$$\sum_{m=1}^{b}\{(\sqrt{m+1} - \sqrt{m}) \sum_{1}^{m} r_n(i)\} = \sum_{m=1}^{b}\{(\frac{1}{2\sqrt{m}} + O(m^{-\frac{3}{2}})) \sum_{1}^{m} r_n(i)\}$$

$$= \sum_{m=1}^{b}\{(\frac{1}{2\sqrt{m}} + O(m^{-\frac{3}{2}}))(\frac{\pi^{\frac{n}{2}} m^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)} + O(m^{\frac{n-1}{2}}))\}$$

$$= \sum_{m=1}^{b}\left\{\frac{\pi^{\frac{n}{2}} m^{\frac{n-1}{2}}}{2\Gamma(\frac{n}{2}+1)} + O\left(m^{\frac{n-2}{2}}\right)\right\} .$$

Since constants implied in the "O" functions in the

above sum are independent of the value of m, we have

$$\sum_{m=1}^{b} O(m^{\frac{n-2}{2}}) = O\left(\sum_{m=1}^{b} m^{\frac{n-2}{2}}\right) \qquad (7, \text{ p. } 94).$$

Hence by the integral test (6, p. 351),

$$\sum \frac{\pi^{\frac{n}{2}} m^{\frac{n-1}{2}}}{2\Gamma(\frac{n}{2}+1)} = -\int_{b}^{o} \frac{\pi^{\frac{n}{2}} x^{\frac{n-1}{2}}}{2\Gamma(\frac{n}{2}+1)}\, dx + O(b^{\frac{n-1}{2}})$$

$$= \frac{\pi^{\frac{n}{2}} b^{\frac{n+1}{2}}}{(n+1)\Gamma(\frac{n}{2}+1)} + O(b^{\frac{n-1}{2}}), \quad \text{and}$$

$$O\left(\sum_{m=1}^{b} m^{\frac{n-2}{2}}\right) = O\left(-\int_{b}^{o} x^{\frac{n-2}{2}}\, dx + O(b^{\frac{n-2}{2}})\right)$$

$$= O(b^{\frac{n}{2}}).$$

Thus we have

$$\sum_{m=1}^{b} \left\{(\sqrt{m+1} - \sqrt{m}) \sum_{1}^{n} r_n(i)\right\} = \frac{\pi^{\frac{n}{2}} b^{\frac{n+1}{2}}}{(n+1)\Gamma(\frac{n}{2}+1)} + O(b^{\frac{n}{2}}).$$

Q.E.D.

Lemma 2-4. If $\sum_{m=1}^{a} r_n(m) \leq N < \sum_{m=1}^{a+1} r_n(m)$, then

$$\sum_{m=1}^{a} \sqrt{m}\, r_n(m) > C_s(n)\, N^{\frac{n+1}{n}}.$$

Proof: By the first three lemmas of the chapter,

$$\sum_{m=1}^{a} \sqrt{m}\, r_n(m) = \sqrt{a} \sum_{m=1}^{a} r_n(m) - \sum_{m=1}^{a-1} \left\{ (\sqrt{m+1} - \sqrt{m}) \cdot \sum_{i=1}^{m} r_n(i) \right\}$$

$$= \sqrt{a}\, \left(\frac{\pi^{\frac{n}{2}} a^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)} + O\left(a^{\frac{n-1}{2}}\right) \right) - \frac{\pi^{\frac{n}{2}} (a-1)^{\frac{n+1}{2}}}{(n+1)\Gamma(\frac{n}{2}+1)}$$

$$- O\left(a^{\frac{n}{2}}\right)$$

$$= \frac{\pi^{\frac{n}{2}} a^{\frac{n+1}{2}}}{\Gamma(\frac{n}{2}+1)} + O(a^{\frac{n}{2}}) - \frac{\pi^{\frac{n}{2}} a^{\frac{n+1}{2}}}{(n+1)\Gamma(\frac{n}{2}+1)} - O\left(a^{\frac{n}{2}}\right)$$

$$= \frac{n\pi^{\frac{n}{2}} a^{\frac{n+1}{2}}}{(n+1)\Gamma(\frac{n}{2}+1)} + O\left(a^{\frac{n}{2}}\right)$$

$$\geq C_4(n)\, N^{\frac{n+1}{n}} + O(N) .$$

Since $\sum_{1}^{a} \sqrt{m}\, r_n(m)$ is a positive increasing function of N, we obtain

$$\sum_{1}^{a} \sqrt{m}\, r_n(m) > C_5(n)\, N^{\frac{n+1}{n}} \quad \text{for all } N.$$

Q.E.D.

In the next three lemmas we shall be dealing with many properties of n-dimensional convex sets. Eggleston's Convexity offers adequate background for the concepts dealt with here.

Lemma 2-5. All vertices of the convex cover of a set Ω consisting of a finite number of points are members of Ω.

Note: If Ω is any set of points in n-dimensional space, then by the convex cover of Ω is meant the set of points which is the intersection of all the convex sets that contain Ω (3, p. 21). A convex polytope is a set which is the convex cover of a finite number of points (3, p.29).

Proof: Assume some point $P \notin \Omega$ is a vertex of the convex cover of Ω. Pick a regular supporting hyperplane S_{n-1} at P to the convex cover of Ω. Form hyperplanes through all members of Ω parallel to S_{n-1}. Since there are only a finite number of these planes, there is one nearest to S_{n-1}, say S'_{n-1}. Since these hyperplanes are all on one side of S_{n-1}, S'_{n-1} forms the boundary of a closed half-space which contains all the members of Ω but doesn't contain P. Hence P is not in the convex cover of Ω, a contradiction. Therefore

only members of Ω are vertices of the convex cover of Ω .

Q.E.D.

The following lemmas will concern a closed, strictly convex body C. We shall be given the fact that C has N lattice points on its boundary. We shall call the set of boundary lattice points B(N) and shall assume that not all the members of B(N) are linearly dependent. If all members of B(N) were linearly dependent, we would only need to consider a space of lower dimensionality.

Lemma 2-6. The members of B(N) are the vertices of a convex polytope entirely in the interior of C.

Proof: Since a convex polytope is defined as the convex cover of a finite number of points, we see that the convex cover of B(N) is a polytope entirely in the interior of C. Call this polytope $(Po)^a_n$. By Lemma 2-5, all vertices pf $(Po)^a_n$ are members of B(N).

We need only show that all members of B(N) are vertices of $(Po)^a_n$. Let $P \varepsilon B(N)$. Choose a regular supporting hyperplane S_{n-1} to C at P. Any segment s_1 which contains P either lies in S_{n-1} or it does

not. If s_1 lies in S_{n-1}, then the only point of $(Po)^a_n$ contained by s_1 is P. Thus points of the exterior of $(Po)^a_n$ are contained by s_1. If s_1 doesn't lie on S_{n-1}, then part of s_1 lies on the opposite side of S_{n-1} from $(Po)^a_n$. Thus, again, points of the exterior of $(Po)^a_n$ are contained by s_1. Hence no segment completely on the boundary of $(Po)^a_n$ contains P. Thus P is a vertex of $(Po)^a_n$.

Q.E.D.

In the next lemma, we multiply each linear dimension of space by 3. In this way, $(Po)^a_n$ is transformed into a similar polytope $(Po)^b_n$. We shall denote the set of vertices of $(Po)^b_n$ by B'(N). Since every vertex of $(Po)^b_n$ will be congruent with all the other members of B'(N) modulo 3, the surface content of $(Po)^b_n$ will be 3^{n-1} times of $(Po)^a_n$.

Lemma 2-7. It is possible to form from $(Po)^b_n$ a convex polytope, $(Po)^c_n$, in the interior of $(Po)^b_n$ with lattice point vertices and with at least N (n-1)-boundaries where N is the number of vertices of $(Po)^b_n$.

Proof: In forming $(Po)_n^b$, we have multiplied every linear dimension by 3. Thus, by Lemma 1-1, each segment between two vertices of $(Po)_n^b$ will be divided into thirds by two lattice points. Let us form a set Σ consisting of these two lattice points taken from each segment between two vertices of $(Po)_n^b$. We define $(Po)_n^c$ as the convex cover of Σ. The polytope $(Po)_n^c$ is the interior of $(Po)_n^b$ by construction. By Lemma 2-5, we see that only members of Σ are vertices of $(Po)_n^c$.

Pick a point X in the interior of $(Po)_n^c$. Clearly $(Po)_n^c$ has an interior for no edge of $(Po)_n^b$ is completely destroyed in the formation of $(Po)_n^c$, and not all members of $B'(N)$ are linearly dependent so $(Po)_n^b$ has an interior.

We shall now show that any member of $B'(N)$ is in the exterior of $(Po)_n^c$. Choose $P' \varepsilon B'(N)$. Choose a regular supporting hyperplane, S_{n-1}, to $(Po)_n^b$ at P'. Since all members of Σ are on one side of S_{n-1} and none are on S_{n-1}, we may apply the same argument used in Lemma 2-5. Thus P' is in the exterior of $(Po)_n^c$.

Thus we see that the segment $\underline{P'X}$ intersects the

boundary of $(Po)_n^c$ in a single point for each $P'\varepsilon B'(N)$.

Assume $P'\varepsilon B'(N)$ and $Q'\varepsilon B'(N)$. We shall now show that the segments $\underline{P'X}$ and $\underline{Q'X}$ do not intersect the same $(n-1)$-boundary of $(Po)_n^c$. Assume that $\underline{P'X}$ and $\underline{Q'X}$ intersect the same $(n-1)$-boundary f'_{n-1} of $(Po)_n^c$. Let us consider the hyperplane S'_{n-1} containing f'_{n-1}. The segment $\underline{P'Q'}$ contains two members of Σ by definition. However, the convex cover of Σ is either on S'_{n-1} or on the opposite side of S'_{n-1} from P' and Q', a contradiction. Hence to each segment $\underline{PX}$ for $P\varepsilon B'(N)$ corresponds a single $(n-1)$- boundary of $(Po)_n^c$.

Thus $(Po)_n^c$ satisfies all the conditions of the lemma.

Q.E.D.

Lemma 2-8. We are given an $(n-1)$-dimensional simplex with lattice point vertices. This simplex lies in the hyperplane S_{n-1} defined by

$$A_1(x_1-p_1) + A_2(x_2-p_2) +\cdots+ (A_n(x_n-p_n) = 0$$

where all the A's are integers, $P(p_1,p_2,\cdots,p_n)$ is a vertex of the simplex, and $(A_1,A_2, \quad ,A_n)=1$. Then the content of the above simplex is at least

$$\frac{1}{(n-1)!}\sqrt{A_1^2 + A_2^2 + \cdots + A_n^2}\ .$$

Proof: Let us assume that P is the origin. If this is not so, we merely translate P into the origin. The equation of S_{n-1} is now

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = 0.$$

Since such a translation transforms lattice points into lattice points, we see that all the vertices of the considered simplex are still lattice points. Let us consider the $(n-1)$ edges of this simplex emanating from the origin as fixed position vectors of the form $(a_{i1}, a_{i2}, \cdots, a_{in})$. The end points of these vectors lie on the hyperplane

$$\begin{vmatrix} x_1 & x_2 & \cdots & x_n \\ a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{(n-1)1} & a_{(n-1)2} & & a_{(n-1)n} \end{vmatrix} = 0\ .$$

But this hyperplane is merely S_{n-1}. Hence the above determinant must expand into

$$k(A_1x_1 + A_2x_2 + \cdots + A_nx_n) = 0$$

Since the components of all the vectors considered are

integers and since $(A_1, A_2, \cdots, A_n) = 1$, we have $k \geq 1$.

Let us consider the content of a parallelotope defined by the unit normal vector to S_{n-1} and the $(n-1)$ vectors of the form $(a_{i1}, a_{i2}, \cdots, a_{in})$. The content of this parallelotope will be numerically equal to the $(n-1)$ dimensional content of its base (8, p.118). Thus if $(b_1, \cdots, b_n)$ denotes the unit normal vector, we have

$$\frac{1}{(n-1)!}\begin{vmatrix} b_1 & b_2 \cdots & b_n \\ a_{11} & a_{12} \cdots & a_{1n} \\ a_{21} & a_{22} \cdots & a_{2n} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_{(n-1)1} & a_{(n-1)2} & a_{(n-1)n} \end{vmatrix} = V_{n-1}$$

where V_{n-1} is the content of the simplex under consideration. However,

$$(b_1, b_2, \cdots, b_n) = \frac{1}{\sqrt{A_1^2+A_2^2+\cdots+A_n^2}}(A_1, A_2, \cdots, A_n).$$

Thus

$$V_{n-1} = \frac{1}{(n-1)!\sqrt{A_1^2+\cdots+A_n^2}}\begin{vmatrix} A_1 & A_2 & A_n \\ a_{11} & a_{12} & a_{12} \\ a_{21} & a_{22} & a_{2n} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_{(n-1)1} & a_{(n-1)2} & a_{(n-1)n} \end{vmatrix}$$

$$= \frac{k(A_1^2 + A_2^2 + \cdots + A_n^2)}{(n-1)!\sqrt{A_1^2 + A_2^2 + \cdots + A_n^2}}$$

$$\geq \frac{1}{(n-1)!}\sqrt{A_1^2 + A_2^2 + \cdots + A_n^2} \quad .$$

Q.E.D.

We are now in a position to prove Theorem 2. We shall restate it here for convenience.

THEOREM 2. We are given a closed, strictly convex body C with N lattice points on its surface. If S(C) denotes the surface content of the boundary of C, then there exists k(n) such that

$$S(C) \geq k(n)\, N^{\frac{n+1}{n}} \quad .$$

Note: In this proof we shall use the fact that if one convex body is contained in another, then the first has smaller surface area than the second (2,p.47). We shall start the proof assuming that from C we have constructed $(Po)_n^a$, $(Po)_n^b$, and $(Po)_n^c$.

Proof: By Lemma 2-6, $(Po)_n^a$ is in the interior of C. Thus

$$S(C) \geq S\,[(Po)_n^a] \quad .$$

From the remarks prefacing Lemma 2-7, we have

$$S\,[(Po)_n^a] = 3^{-(n-1)}\,S\,[(Po)_n^b]\ .$$

From Lemma 2-7, we have

$$S\,[(Po)_n^b] \geq S\,[(Po)_n^c]$$

Hence

$$S(C) \geq 3^{-(n-1)}\,S[(Po)_n^c]\ .$$

Let us pick one (n-1)-dimensional simplex from each (n-1)-boundary of $(Po)_n^c$. By Lemma 2-7, $(Po)_n^c$ has at least N (n-1)-boundries. Hence if S(m) denotes the (n-1)-dimensional content of the m^{th} simplex chosen, then

$$S\,[(Po)_n^c] \geq \sum_{m=1}^{N} S\,(m)\ .$$

However, no three (n-1)-boundaries of $(Po)_n^c$ may have the same direction numbers. If three (n-1)-boundaries of $(Po)_n^c$ had the same director numbers, then two of these (n-1)-boundaries would be on opposite sides of the hyperplane containing the third. By Lemma 2-8, we know that any simplex on a hyperplane of direction numbers $(A_1 : A_2 : \cdots : A_n)$ has content not less than

$$\frac{1}{(n-1)!}\sqrt{A_1^2 + A_2^2 + \cdots + A_n^2}\ .$$

Thus by Lemma 2-8, there will be no more than $r_n(1)$

simplexes among those chosen of content $\frac{1}{(n-)!}$; there will be no more than $r_n(2)$ simplexes among those chosen of content $\frac{\sqrt{2}}{(n-1)!}$, etc. Thus, if

$$\sum_{m=1}^{a} r_n(m) \leq N < \sum_{m=1}^{a+1} r_n(m), \quad \text{then}$$

$$\sum_{m=1}^{N} S(m) \geq \frac{1}{(n-1)!} \sum_{1}^{a} \sqrt{m}\, r_n(m) .$$

Hence by Lemma 2-4,

$$\sum_{1}^{N} S(m) \geq \frac{C_s(n)}{(n-1)!} N^{\frac{n+1}{n}} .$$

Thus combining the above results, we obtain

$$S(C) \geq k(n)\, N^{\frac{n+1}{n}} .$$

Q.E.D.

We may generalize Theorem 2 to certain non-convex bodies. When we speak of a strictly convex surface we mean a surface which is part of the boundary of a strictly convex body.

Corollary 2-1. Let $\bar{C}$ be a surface which is made up of M strictly convex surfaces. Let $t\bar{C}$ be the set of all points $t \cdot P$ where $P \epsilon \bar{C}$. If there are N lattice points on the boundary of $t\bar{C}$,

we have

$$N < k'(\bar{C})t^{\frac{n(n-1)}{n+1}}$$

where $k'(\bar{C})$ is dependent upon certain properties of $\bar{C}$ but not on t.

Proof: We have

$$S(\bar{C}) = \sum_{1}^{M} S(c_i)$$

where $\sum_{1}^{M} S(c_i)$ denotes the sum of the surface content of the M surfaces making up $\bar{C}$. Assuming there are N lattice points on the boundary of $t\bar{C}$, we have that there are at least $\frac{N}{M}$ lattice points on at least one boundary element tc_j. Let tC be a strictly convex body containing tc_j. We define a number θ by

$$\frac{S(c_j)}{S(C)} = \frac{t^{n-1}\,S(c_j)}{t^{n-1}S(C)} = \frac{S(tc_j)}{S(tC)} = \theta .$$

We see that θ is constant for all t and $0 < \theta < 1$. By Theorem 2,

$$S(tc_j) = \theta S(tC) > \theta k(n)\,(\tfrac{N}{M})^{\frac{n+1}{n}} .$$

Hence

$$t^{n-1}S(\bar{C}) = S(t\bar{C}) = \sum_{1}^{M} S(tc_i) \geq S(tc_j) > k''(\bar{C})N^{\frac{n+1}{n}},$$

or

$$N < k'(\bar{C})t^{\frac{n(n-1)}{n+1}} .$$

Q.E.D.

APPLICATIONS

We shall now apply Theorem 2 to two problems in number theory. We first consider hyperspheres. For $n = 2, 4, 6, 8, 10$, $r_n(m)$ is known for all m. Hence we shall have the opportunity to compare the estimates of Theorem 2 with the actual content of the hyperspheres considered.

In n-dimensional space, the content, V, and the surface content, S, of the hypersphere are given by

$$V = \frac{\pi^{\frac{n}{2}} r^n}{\Gamma(\frac{n}{2} + 1)} \qquad \text{(8, p. 136), and}$$

$$S = \frac{2\pi^{\frac{n}{2}} r^{n-1}}{\Gamma(\frac{n}{2})}$$

$$= \frac{n\pi^{\frac{n}{2}} r^{n-1}}{\Gamma(\frac{n}{2} + 1)} \qquad \text{(8, p. 136)} .$$

Hence, $V = C_s(n)\, S^{\frac{n}{n-1}}$ where $C_s(n)$

$$= \pi^{-\frac{n}{2(n-1)}}\, n^{\frac{-n}{n-1}} \left(\Gamma(\tfrac{n}{2} + 1)\right)^{\frac{1}{n-1}} .$$

For $n=2$, $r_2(m) = 4\tau(m')$ (6, p.241). The symbol $\tau(m')$ denotes the number of divisors of m of the form $4k + 1$.

For $n = 4$, $r_4(m) = 8 \sum_{\substack{d|m \\ 4\nmid d}} d$ (6, p. 314).

For $n = 6$, $r_6(m) = 16 \sum_{d|n} x(d')d^2 - 4 \sum_{d|n} x(d)d^2$, where

$$dd' = n \qquad x(d) = \begin{cases} 1 & d=4k+1 \\ -1 & d=4k-1 \\ 0 & d=2k \end{cases}$$ (6, p. 314).

For $n = 8$, $r_8(m) = 16(-1)^n \sum_{d|n} (-1)^d d^3$ (6,p.314).

For $n = 10$, $r_{10}(m) = \frac{4}{5}\left\{ 16^{a+1} + (-1)^{\frac{1}{2}(\ell-1)} \right\}\lambda + \frac{8}{5}m^2\mu - \frac{64}{5}\zeta$.

In this formula, $m = 2^a\ell$; λ is the excess (taken positively) of the sum of the fourth powers of the divisors of m of the form $4k + 1$ over the sum of the fourth powers of the divisors of n of the form $4k + 3$; μ is the number of solutions of the equation $n = s^2 + s'^2$, and ζ is the sum of the products $s^2 . s'^2$ for all the solutions (4, p. 483-484).

Hence,

$$r_2(5^\ell) = 4(\ell + 1) ;$$

$$r_4(2\cdot 3^{\ell}) = 8\left(\sum_{0}^{\ell} 2\cdot 3^i + \sum_{0}^{\ell} 3^i\right) = 24(3^{\ell+1} - 1) ;$$

$$r_6(5^{\ell}) = 12\sum_{1}^{\ell} 5^{2i} = \tfrac{1}{2}(5^{2\ell+2} - 1) ;$$

$$r_8(2^{\ell}) = 16\sum_{0}^{\ell} 2^{3i} = \tfrac{1}{7}(2^{3\ell+7} - 16), \quad \ell \geq 1 ;$$

$$r_{10}(2^{2\ell}) = \tfrac{4}{5}(16^{2\ell+1} + 1) + \tfrac{8}{5}(2^{2\ell})^2\cdot 4 = \tfrac{4}{5}(2^{8\ell+4} + 2^{4\ell+3} + 1) ;$$

$$r_{10}(2^{2\ell+1}) = \tfrac{4}{5}(16^{2\ell+2} + 1) + \tfrac{8}{5}(2^{2\ell+1})^2\cdot 4 - \tfrac{64}{5}\cdot 4\cdot 2^{4\ell}$$

$$= \tfrac{4}{5}(2^{8\ell+8} + 2^{4\ell+5} - 2^{4\ell+6} + 1) .$$

By Theorem 2, we predict the volume of a hypersphere of radius $\sqrt{m}$ to be

$$V \geq k'(n)[r_n(m)]^{\frac{n+1}{n-1}} .$$

If $n = 2$ and $m = 5^{\ell}$, $V = \pi 5^{\ell}$. We predicted

$$V \geq k'(2)\ell^3 .$$

If $n = 4$ and $m = 2\cdot 3^{\ell}$, $V = (\pi^2 4)\cdot 3^{2\ell}$. We predicted

$$V \geq k'(4)3^{\frac{5\ell}{3}}$$

If $n = 6$ and $m = 5^{\ell}$, $V = (\frac{\pi^3}{6}) \cdot 5^{3\ell}$. We predicted

$$V \geq k'(6) \cdot 5^{\frac{14\ell}{5}} .$$

If $n = 8$ and $m = 2^{\ell}$, $V = (\frac{\pi^4}{24}) \cdot 2^{4\ell}$. We predicted

$$V \geq k'(8) \cdot 2^{\frac{27\ell}{7}}$$

If $n = 10$ and $m = 2^{\ell}$, $V \geq (\frac{\pi^5}{120}) \cdot 2^{5\ell}$. We predicted

$$V \geq k'(10) 2^{\frac{44\ell}{9}} .$$

Thus, we see that Theorem 2 is a very good asymptotic estimate in the case of a hypersphere.

We now consider a more general problem.

$$|x_1|^p + |x_2|^p + \cdots + |x_n|^p = R, \quad p > 1.$$

By Minkowski's inequality (5, p.490), the closed region defined by this function is strictly convex, and since the equation is homogeneous, the content V and the surface content S satisfy the inequality $V \geq C(n) S^{\frac{n}{n-1}}$.

Hence, if the above equation has N solutions in lattice points, then by Theorem 2 and van der Corput's theorem (2:71),

$$|x_1|^p + |x_2|^p + \cdots + |x_n|^p < R$$

has $c'(n) N^{\frac{n+1}{n-1}}$ solutions in lattice points.

BIBLIOGRAPHY

1. Bonnesen, T. and W. Fenchel. Theorie der Konvexen Körper. New York, Chelsea, 1948. 164 p.

2. Cassels, J. W. S. An introduction to the geometry of numbers. Berlin, Springer-Verlag, 1959. 344 p. (Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen. Band 99.)

3. Eggleston, H. G. Convexity. Cambridge, Cambridge University Press, 1958. 136 p. (Cambridge Tracts in Mathematics and Mathematical Physics. No. 47)

4. Glaisher, J. W. L. On the number of representations of a number as a sum of 2r squares, where 2r does not exceed eighteen. Proceedings of the London Mathematical Society, 2d ser., 5:479-490. 1907.

5. Hardy, G. H. A course of pure mathematics. 10th ed. Cambridge, Cambridge University Press, 1955. 509 p.

6. Hardy, G. H. and E. M. Wright. An introduction to the theory of numbers. 3d ed. Oxford, Oxford University Press, 1954. 419 p.

7. LeVegue, William Judson. Topics in number theory. Vol. 1. Reading, Addison-Wesley, 1956. 198 p. (Addison Wesley Mathematics Series).

8. Sommerville, D. M. Y. An introduction to the geometry of N dimensions. New York, E. P. Dutton and Company, 1929, 196 p.