COVERING MINIMA AND LATTICE POINT FREE CONVEX BODIES

Ravi Kannan

Laszlo Lovasz

CS-TR-114-87

November 1987

COVERING MINIMA AND LATTICE POINT FREE CONVEX BODIES

by

Ravi Kannan [1] and László Lovász [2]

(November 2, 1987)

Abstract

The covering radius of a convex body K (with respect to a lattice L) is the least factor by which the body needs to be blown up so that its translates by lattice vectors cover the whole space. The covering radius and related quantities have been studied extensively in the Geometry of Numbers (mainly for convex bodies symmetric about the origin). In this paper, we define and study the "covering minima" of a general convex body. The covering radius will be one of these minima; the "lattice width" of the body will be the reciprocal of another. We derive various inequalities relating these minima. These imply bounds on the width of lattice point free convex bodies. We prove that every lattice-point-free body has a projection whose volume is not much larger than the determinant of the projected lattice.

[1] Department of Computer Science, Carnegie-Mellon University, Pittsburgh. Supported by NSF-Grant ECS 8418392.

[2] Department of Computer Science, Eötvös Loránd University, Budapest and Princeton University, Princeton.

Introduction

A central result in the Geometry of Numbers is Minkowski's Theorem: *if a convex body is centrally symmetric with respect to the origin and contains no point of a lattice L besides the origin, then its volume is at most* $2^n \cdot \det L$. This theorem, and its many extensions (some of which will be mentioned below) give a powerful tool to prove the existence of non-zero lattice points in 0-symmetric convex bodies.

The situation is somewhat different if we consider bodies containing no lattice point at all. Such a body may have arbitrarily large volume (even if we assume that it is centrally symmetric; this property is less relevant in the inhomogeneous case). Just think of a large flat "pancake" between two consecutive layers of lattice points. Nevertheless, the general question remains: what can be said about lattice-point-free convex bodies?

One important property of lattice-point-free convex bodies is that they are "flat": there is a lattice hyperplane such that the number of lattice hyperplanes parallel to it that intersect the body is bounded by a number $f(n)$ wich depends on the dimension only. We shall refer to this result as the *Flatness Theorem.* More formally, we define the *width* of the convex body K along a non-zero vector v as the quantity

$$\max\{v \cdot x : x \in K\} - \min\{v \cdot x : x \in K\}.$$

The *lattice width* of K is the minimum of its widths along vectors in the dual lattice. (Note that the usual geometric width of K is the minimum of its widths along vectors of unit length.) Then it is true that the lattice width of a lattice-point-free convex body in n-space is bounded by $f(n)$. The Flatness Theorem goes back to Khinchine (1948) (in a sense, in fact, to Kronecker).

Although our paper deals with the algorithmic aspects of the problems involved only marginally, we have to mention the reason for the revival of interest in the Flatness Theorem: it was exploited by H.W.Lenstra, Jr. (1983) in his celebrated algorithm, which solves the integer linear programming problem in a fixed dimension in polynomial time. The Integer Programming Problem (in its feasibility version) is the problem of determining whether a given system of linear inequalities has an integer solution. Let P be the set of all *real* solutions of the system. Using an algorithmic version of the Flatness Theorem, Lenstra either finds an integer point in P or finds a lattice hyperplane such that only $f(n)$ of the parallel lattice hyperplanes intersect K. In this latter case, we split the problem into $f(n)$ subproblems of lower dimension, and solve them recursively.

This application raises the problem of finding the best possible $f(n)$ in this theorem. As we shall see, there is a substantial difference between algorithmic and non-algorithmic results. Khinchine's work (non-algorithmic) gives about $n!$ for $f(n)$. Lenstra obtains c^{n^2}, but this result is constructive in the sense that it yields a polynomial-time algorithm for each fixed dimension to find either a lattice point in the body or a hyperplane in which direction the body is "flat". Grötschel, Lovász and Schrijver (1983) showed that this same order of magnitude can be achieved in polynomial time even for variable dimension. Babai (1985) improved the result to obtain a simply exponential function for $f(n)$, in polynomial time. Hastad (1986), based on the work of Lagarias, Lenstra and Schnorr (1987) showed that the Flatness Theorem remains valid with $f(n) = O(n^{5/2})$. One of our main results is to improve this to $O(n^2)$. We conjecture that this result is not best possible. It is easy to construct a lattice-point-free convex body with lattice width n, and it is possible that the best value of $f(n)$ is linear. Unfortunately, neither Hastad's proof nor ours yields a polynomial-time algorithm.

Minkowski also introduced the *successive minima* of a convex body. The ith successive minimum, λ_i, is the least positive real number t such that tK contains i linearly independent lattice vectors. Minkowski' Second Theorem gives an upper bound on the product of these minima; this strengthens his first theorem substantially. We remark that the lattice width of a body is just the first minimum of the polar of its difference body.

The "covering minima" introduced in this paper form another sequence of numbers associated with a body and a lattice, somewhat analogous to the successive minima. We define the jth covering minimum μ_j of the convex body K as the least positive real number t such that the translates of tK by all lattice vectors intersect each $n-j$ dimensional affine subspace.

The last of these numbers is a well-known quantity (at least for centrally symmetric bodies): it is the *covering radius* of K. Note that if K contains no lattice point then its translates by lattice vectors do not cover the origin, and hence its covering radius is more than 1. A certain converse of this observation is also true: if the covering radius of the body is more than 1, than the body can be translated to a lattice-point-free position.

The first covering minimum, on the other hand, turns out to be the reciprocal of the lattice width of K. So the sequence of covering minima "links" these two important numbers, a fact that will be exploited in our proofs. Among others, we shall prove the inequality

$$\mu_{j+1} \leq \mu_j + c \cdot j \cdot \mu_1$$

where c denotes an absolute constant. This yields by induction an inequality

$$\mu_j \leq c \cdot j^2 \cdot \mu_1.$$

Now if K is lattice-point-free then $\mu_n > 1$ and hence it follows that the lattice width of K, i.e., the reciprocal of μ_1, is $O(n^2)$.

Our results will also say something about the volume of lattice-point-free bodies. While this cannot be bounded by any function of the dimension, we shall show that for every lattice-point-free convex body there exists a projection of the space such that the projected body is "almost" disjoint from the projected lattice and the ratio of its volume to the determinant of the projected lattice is bounded by a function of the dimension. A corollary of this result yields a rather sharp "approximate min-max formula" for the covering minima.

1. Basic Definitions and Results

$\mathbf{R}^n$ and $\mathbf{Z}^n$ denote the set of column vectors of length n with real, respectively integer components. For any two vectors v, u in $\mathbf{R}^n$, $v \cdot u$

denotes the scalar product of the two vectors. For any two sets S, T in $\mathbf{R}^n$, $S + T$ denotes the set $\{s + t : s \in S, t \in T\}$. For example, $S + \mathbf{Z}^n$ is the union of copies of S translated by every integer vector. Thus, the covering radius mentioned above is the infimum over all positive reals t such that $tS + \mathbf{Z}^n = \mathbf{R}^n$. We abbreviate $S + T$ by $S + t$ if T is the singleton set $\{t\}$.

Let V be a subspace of $\mathbf{R}^n$. We denote by $V^\perp$ the orthogonal complement subspace. For any set S in $\mathbf{R}^n$, the projection of S parallel to V (denoted by S/V) is the set $\{t : t \in V^\perp; \exists s \in V \text{ such that } s + t \in S\}$. S/V may be pictured as the projection of S into $V^\perp$. For any set S, $\text{int}(S)$ denotes the interior of the set S; $\text{lin}(S)$ denotes the vector space spanned by the set S and $\text{cl}(S)$ denotes the closure of S.

We refer the reader to Cassels (1971) and Gruber and Lekkerkerker (1987) for basic definitions of a lattice, dual lattice, basis of a lattice etc. Here we give a very brief description. A *lattice* L in $\mathbf{R}^n$ is the set of integer linear combination of a finite set of linearly independent vectors which form a *basis* for the lattice. The number of vectors in a basis of the lattice is called the *dimension* of the lattice. It is an invariant of the lattice, i.e, it does not depend on the choice of the basis. If $b_1, b_2, \ldots b_m$ form a basis of the lattice L, then the *determinant* of the lattice is the $m-$dimensional volume of the parallelepiped spanned by $b_1, b_2, \ldots b_m$. It is also an invariant of the lattice. The *dual* (or *polar* or *reciprocal*) lattice of L is the set $\{x : x \in \text{lin}(L); x \cdot y \in \mathbf{Z}\ \forall y \in L\}$. It is easy to see that $(L^*)^* = L$ and that the determinant of L^* is the reciprocal of the determinant of L. The following lemma collects some well-known facts.

(1.1) Lemma *Suppose* L *is a lattice in* $\mathbf{R}^n$ *with lin*$(L) = \mathbf{R}^n$ *and* V *is any subspace of* $\mathbf{R}^n$ *. Then*

(1.1.1) V *has a linear basis containing only vectors of* L *iff* $V^\perp$ *has a basis containing only vectors of* L^*.

(1.1.2) L/V *is a lattice iff* $V^\perp$ *has a linear basis in* L^* .

∎

By a *convex body* in a linear space V, we mean a bounded, closed, convex set K such that $K - K$ spans V. We shall omit reference to V if $V = \mathbf{R}^n$. We remark that the assumption of closed does not result in any loss of generality - the covering minima we define do not change when we take the closure of the convex set and so it suffices to prove all our results for closed sets anyway. For a convex body K that contains the origin in its interior, we define its *polar* K^* by

$$K^* = \{x : x \in \mathbf{R}^n;\ x \cdot y \leq 1\ \forall y \in K\}.$$

This set is again a convex body. If K is symmetric about 0 (and hence too K^*,) their volumes are related by the following inequalities:

$$\frac{c_1^n}{n^n} \leq \mathrm{vol}(K) \cdot \mathrm{vol}(K^*) \leq \frac{c_2^n}{n^n},$$

where c_1, c_2 are absolute constants. The upper bound is due to Blaschke (1917) and Santaló (1949); the maximum is attained when K is a ball. The lower bound is due to Bourgain and Milman (1985). Mahler conjectured that the minimum is attained when K is a cube; this question is still open. The result of Bourgain and Milman will be important for us: several of our results will involve the constant $c_0 = 4/c_1$. (Clearly we may assume that $c_0 \geq 1$.)

Let L be a lattice and K, a convex body in lin$L$, centrally symmetric with respect to the origin. The *ith successive minimum of K with respect to L*, denoted by $\lambda_i = \lambda_i(K, L)$, is the least number $t \geq 0$ such that tK contains i linearly independent lattice vectors $(1 \leq i \leq n)$.

The following Lemma will be of a particular importance.

(1.2) Lemma: *If K is a bounded 0-symmetric convex body and L is any n-dimensional lattice in $\mathbf{R}^n$, then*

$$\lambda_1(K, L)\lambda_1(K^*, L^*) \leq c_o n$$

where c_o is a constant independent of n.

Remark: Lagarias, Lenstra and Schnorr (1987) give the weaker bound of $O(n^{3/2})$. As they remark, a result of Conway and Thompson (quoted in Milnor and Husemoller (1973)) implies that $O(n)$ is the best possible upper bound in lemma (1.2). For $n = 2$, Mahler (1948) proved that $\lambda_1(K, L)\lambda_1(K^*, L^*) \leq \sqrt{2}$.

Proof: Let V and V^* denote the volumes of K, K^* respectively. Then by Minkowski's convex body theorem, we have

$$\begin{aligned}\lambda_1(K, L) &\leq 2V^{-1/n}(\det(L))^{1/n}\\ \lambda_1(K^*, L^*) &\leq 2(V^*)^{-1/n}(\det(L^*))^{1/n}\end{aligned}$$

.

Multiplying the two inequalities, the lemma follows by the theorem of Bourgain and Milman.

∎

Remark: If we apply Minkowski's theorem on successive minima, we obtain the following stronger result :

$$\sqrt[n]{\lambda_1\lambda_2\ldots\lambda_n}\ \sqrt[n]{\lambda_1^*\lambda_2^*\ldots\lambda_n^*} \leq c_o n,$$

where $\lambda_i = \lambda_i(K, L)$ and $\lambda_i^* = \lambda_i(K^*, L^*)$.

2. Covering minima

(2.1) Definition: Let L be a lattice with dimension r and K, a convex body in lin $L = V$. We define the jth *covering minimum* of K with respect to L, $\mu_j(K, L) = \mu_j$ for $j = 0, 1, 2, \ldots, r$, as follows:

$\mu_j = \inf\{t : tK + L$ meets every $(r-j)$-dimensional affine subspace of $V\}$.

It is easy to see that the infimum is, in fact, a minimum. Furthemore, for any $x_0 \in \text{lin}L$, $tK + L$ meets every $(r - j)$ dimensional affine subspace iff $t(K - x_0) + x_0 + L$ does. So the value of μ_j is invariant under translations of K.

Clearly $0 = \mu_0 \leq \mu_1 \leq \ldots \leq \mu_r$. Further, $\mu_r(K, L)$ is the usual covering radius (Cassels 1971). In what follows, we denote by λ_i the ith minimum of L with respect to $K - K$ and by λ_i^* the ith minimum of L^* with respect to $(K - K)^*$.

In the lemmas that follow, we shall assume that lin $L = \mathbf{R}^n$, unless stated otherwise.

(2.2) Lemma: *For $1 \leq j \leq n$, there exists an affine subspace T of dimension $(n - j)$ in $\mathbf{R}^n$ such that*

(i) $T \cap (\mu_j \operatorname{int}(K) + L) = \emptyset$ and

(ii) the linear subspace parallel to T has a basis in L.

Proof: Without loss of generality, we can translate K and assume that $0 \in K$. For any affine subspace T of dimension $(n - j)$, let $\mu'(T) = \inf\{t : T \text{ intersects } tK + L\}$. There is a set of $(n - j)$ orthonormal vectors $(v_1, v_2, \ldots, v_{n-j})$ and a $v \in \mathbf{R}^n$ such that $T = v + \operatorname{lin}\{v_1, \ldots, v_{n-j}\}$. Choose $v' \equiv v(\operatorname{mod} L)$, such that v' belongs to the fundamental parallelopiped corresponding to some basis of L. Clearly, $\mu'(T) = \mu'(v' + \operatorname{lin}\{v_1, \ldots, v_{n-j}\})$. Thus μ' is essentially defined on a compact set P in $\mathbf{R}^m$, where $m = (n - j + 1)n$. Suppose $\sup\{\mu'(p) : p \in P\} = \gamma$. Then there is a sequence of points $p_1, p_2, p_3, \ldots$ in P such that $\mu'(p_i) > \gamma - 1/i$. There is a convergent subsequence $q_1, q_2, \ldots,$ of the p_i, say the limit of the subsequence is q^*. Then q^* defines an $n - j$ dimensional affine subspace T^* of $\mathbf{R}^n$ because the orthonormality of the basis represented by $q_1, q_2, \ldots,$ implies the orthonormality of the basis represented by q^*. Further, $\mu'(T^*) = \gamma = \mu_j$.

Now if $T^* \cap (\mu_j \operatorname{int}(K) + L) \neq \emptyset$, then $\mu'(T^*) < \mu_j$, contradicting the definition of T^*. So T^* satisfies (i). The linear subspace parallel to T^*, however, may not have a basis in L. To ensure (ii), we proceed as follows: Let T' be an affine subspace of maximum dimension contained in $\mathbf{R}^n \setminus (\mu_j \operatorname{int}(K) + L)$. We have shown that $\dim(T') \geq n - j$. The closure of $(T' + L)$ is contained in $\mathbf{R}^n \setminus (\mu_j \operatorname{int}(K) + L)$, and so T' is a maximal affine subspace of $\operatorname{cl}(T' + L)$. Let V' be the linear space parallel to T'. If V' does not have a basis in L, then it follows from lemma (1.1) that L/V' contains a line $l = \{\lambda u : \lambda \in \mathbf{R}\}$. But then, $\mathrm{cl}(T' + L)$ contains $T' + l$, an affine subspace of dimension 1 greater than T'. This contradicts the definition of T'. So V' has basis in L. Since $\dim(V') \geq n - j$, we can choose a $(n - j)$ dimensional subspace of T' satisfying both (i) and (ii).

▮

(2.3) Lemma: $\mu_1 = 1/\lambda_1^*$.

Proof: Suppose $v \in \lambda_1^*(K - K)^* \cap L^*,\ v \neq 0$. Then $v \cdot (x - y) \leq \lambda_1^*$ for all $x, y \in K$. Let $\beta_t = \max\{v \cdot x : x \in tK\}$ and $\alpha_t = \min\{v \cdot x : x \in tK\}$. Then $\beta_1 - \alpha_1 \leq \lambda_1^*$ and since the points of L lie on hyperplanes of the form $\{x : v \cdot x = z\}$ for $z \in \mathbf{Z}$, we must have $\beta_{\mu_1} - \alpha_{\mu_1} \geq 1$, i.e., $\mu_1(\beta_1 - \alpha_1) \geq 1$, i.e., $\mu_1 \geq 1/\lambda_1^*$.

Conversely, by lemma (2.2) and lemma (1.1) $\mu_1 = \inf\{t : tK + L$ intersects every hyperplane of the form $\{x : v \cdot x = s\}$ where $v \in L^*, s \in \mathbf{R}\}$. For $v \in \mathbf{R}^n$, $v \notin \gamma((K - K)^*)$, there exist $x, y \in K$ such that $v.(x - y) > \gamma$ implying that $(1/\gamma)K + L$ intersects every hyperplane of the form $\{x : v \cdot x = s\}, s \in \mathbf{R}$. Since $\gamma(K - K)^* \cap L^* = \{\underline{0}\} \forall \gamma < \lambda_1^*$, it follows that $\mu_1 \leq 1/\gamma$ for all such γ, thus $\mu_1 \leq 1/\lambda_1^*$.

▮

It is interesting to point out that λ_1 is the least t for which the interiors of the bodies $tK + z \quad (z \in \mathbf{L})$ are disjoint. In this respect λ_1 is dual to μ_n.

The following inequalities relating the covering radius and the successive minima are proved for centrally symmetric bodies in (Cassels, 1971).

(2.4) Lemma: $\lambda_n \leq \mu_n \leq \lambda_1 + \lambda_2 + \ldots \lambda_n$.

Proof: The proof of the left hand side inequality is identical to the case of symmetric bodies; minor changes are required for the right hand side inequality, which we sketch here. First translate K so that the origin belongs to K. Suppose $v_1, v_2, \ldots v_n$ achieve the successive minima of $K - K$

and $x_1, x_2, \ldots x_n$ are points in $\mathbf{R}^n$ such that x_i and $x_i + v_i$ belong to $\lambda_i K$; so, of course, the line segment joining these two points belongs to $\lambda_i K$. Let x be $\sum_{i=1}^n x_i$. If p is any point in space, let $\alpha_1, \alpha_2, \ldots \alpha_n$ be real numbers such that $p - x = \sum_{i=1}^n \alpha_i v_i$. Suppose $\beta_i = \lfloor \alpha_i \rfloor$ and $\gamma_i = \alpha_i - \beta_i$ and $l = \sum_{i=1}^n \beta_i v_i$. Then $p = l + x + \sum_{i=1}^n \gamma_i v_i$ from which it follows that p belongs to $L + (\sum_{i=1}^n \lambda_i)K$. Since this was true of an arbitrary p, we have the required inequality.

∎

Let us remark that lemma (1.2) can now be rephrased as follows :

$$\lambda_1 \leq c_o n \mu_1$$

¿From corollary (2.8) below, it follows that $\lambda_j \leq O(n^2)\mu_j$, but we do not know the how large λ_j / μ_j can be for given j and n.

Next we prove a further relation between the λ's and μ's, which will play an important role later on.

(2.5) Lemma: *For each* j, $1 \leq j < n$,

$$\mu_{j+1} \leq \mu_j + \lambda_{n-j}.$$

Proof: First we prove the case $j = n - 1$. By the definition of λ_1, there exists a non–zero vector $v \in L \cap \lambda_1(K - K)$. By translating K appropriately, we may assume that $v \in \lambda_1 K$ and that $0 \in K$. Consider any point $p \in \mathbf{R}^n$, By definition, the line $\{p + tv : t \in \mathbf{R}\}$ intersects $\mu_{n-1}K + L$, and hence there exists an $s \in \mathbf{R}$ and a $u \in L$ such that $p + sv + u \in \mu_{n-1}K$. Hence $p + \lceil s \rceil v + u = (p + sv + u) + (\lceil s \rceil - s)v \in \mu_{n-1}K + (\lceil s \rceil - s)\lambda_1 K \subseteq (\mu_{n-1} + \lambda_1)K$. (because $0 \in K$). Since $\lceil s \rceil v + u \in L$, this implies that $p \in (\mu_{n-1} + \lambda_1)K + L$. Since p was arbitrary, this implies that $\mu_n \leq \mu_{n-1} + \lambda_1$.

Now we consider an arbitrary j, $1 \leq j < n$. By lemma (2.3), there exists an $(n - j - 1)$–dimensional subspace T parallel to a linear subspace

V spanned by vectors in L such that $T \cap (\mu_{j+1} \operatorname{int}(K) + L)$ is empty. Let $K' = K/V$, $L' = L/V$. Let $\mu_i^{'} = \mu_i(K', L')$, $\lambda_i^{'} = \lambda_i((K' - K'), L')$ and $\lambda_i'^{*} = \lambda_i((K' - K')^*, L'^*)$ for all relevant i. We claim that $\mu_i^{'} \leq \mu_i$ for all $i \leq j+1$. For, if S is any $(j+1-i)$–dimensional affine subspace of $\mathbf{R}^n/V$, then $S + V$ is an $(n-i)$–dimensional affine subspace of $\mathbf{R}^n$. So $\mu_i K + L$ intersects $S + V$ implying that $\mu_i K' + L'$ intersects S. Next, we claim that $\mu_{j+1}^{'} = \mu_{j+1}$. This follows from the choice of T. Further, $\lambda_i' \leq \lambda_{n-j+i-1}$ and $\lambda_i'^{*} \geq \lambda_i^{*}$. (We do not need this last fact right now). By the first part of the proof, we know that $\mu_{j+1}^{'} \leq \mu_j^{'} + \lambda_1^{'}$,. Hence, the inequality in the lemma follows.

∎

Remarks: 1. From the above proof, it is clear that $\mu_j(K, L)$ equals the maximum of $\mu_j(K/T, L/T)$ over all $n - j$ dimensional subspaces T of $\operatorname{lin}(L)$ spanned by vectors in L.

2. In the case when K is an ellipsoid, we obtain the stronger inequlity $(\mu_n)^2 \leq (\mu_{n-1}')^2 + \lambda_1^2/4$.

While the μ's and λ's are related in many ways, there is a substantial difference between them. It is easy to see that given any sequence $0 < t_1 \leq t_2 \leq t_3 \ldots \leq t_n$ of real numbers, there is always a lattice and a 0-symmetric convex body such that $\lambda_i(K, L) = t_i$. On the other hand, the sequence $\mu_1, \mu_2 \ldots \mu_n$ satisfies rather stringent conditions, as shown by the following assertions.

(2.6) Lemma: For all j, $(1 \leq j \leq n-1)$,

$$\mu_{j+1} \leq \mu_j + c_o(j+1)\mu_1.$$

Proof: Similarly as before, it suffices to prove this for $j = n-1$. Thus, by lemmas 2.5 and 2.3,

$$\mu_n \leq \mu_{n-1} + \lambda_1 \leq \mu_{n-1} + c_o n \mu_1$$

∎

By the monotonicity of the μ's, this last lemma implies that $\mu_{j+1} \leq (c_o j + c_o + 1)\mu_j$. Below, we shall improve this bound for centrally symmetric convex bodies. But first, we apply the previous lemma to obtain our main estimate on the μ's.

(2.7) Theorem: *Let K be a convex body in $\mathbf{R}^n$ and L , an $n-$dimensional lattice in $\mathbf{R}^n$. Then for all j, $1 \leq j \leq n$,*

$$\mu_j(K, L) \leq c_o \binom{j+1}{2} \mu_1(K, L).$$

Proof: We proceed by induction on j. Clearly the theorem is valid for $j = 1$. For higher j, we apply lemma (2.6):

$$\mu_j \leq \mu_{j-1} + c_o j \mu_1 \leq c_o \binom{j}{2} \mu_1 + c_o j \mu_1 = c_o \binom{j+1}{2} \mu_1.$$

∎

For the special case of 0-symmetric convex bodies, Lagarias, Lenstra and Schnorr (1986, theorem 9.2), also prove this result for $j = n$, i.e., they show that $\mu_n \lambda_1^* \leq O(n^2)$. By choosing 0 for the center of gravity of a (not necessarily 0-symmetric) convex body K, and then applying their result to $K \cap (-K)$, one obtains a similar result for general convex bodies, but with $O(n^3)$ in place of $O(n^2)$.

Remark: It is interesting to consider the following example : Let K be the simplex $\{x : \sum_{j=1}^{n} x_j \leq 1 \; ; x_j \geq 0 \forall j\}$ in $\mathbf{R}^n$ and L the standard lattice $\mathbf{Z}^n$. Then it is easy to see that $\mu_n(K, L) = n$ since for any small positive ϵ, the point $(1-\epsilon, 1-\epsilon, \ldots, 1-\epsilon)$ belongs to $tK + L$ if and only if $t \geq n(1-\epsilon)$. Further, it is easy to see that $\mu_1(K, L) = 1$. Also,

$\lambda_1(K-K,L) = \lambda_n(K-K,L) = 1$, so by lemma (2.5), we have that $\mu_j(K,L) = j$ for all j. Thus, we have a lower bound on μ_j/μ_1 of $O(j)$ and by theorem (2.7), an upper bound on this quantity of $O(j^2)$. We do not know the best possible bound. We also note that for the octahedron $\{x : \sum_{j=1}^{n} |x_j| \leq 1\}$, μ_n is $O(n)$ and μ_1 is 1. Again, it is easy to see that μ_j is $O(j)$. Thus, even for centrally symmetric bodies, we have a lower bound on μ_j/μ_1 of $O(j)$.

The next result follows immediately from Theorem 2.7 and inequality (2.4).

(2.8) Corollary:

$$\lambda_n \lambda_1^* \leq c_o \binom{n+1}{2}$$

∎

If K is lattice-point-free then $\mu_n \geq 1$ and hence $\mu_1 \geq 1/c_0 n^2$. Hence the lattice width of the body is $O(n^2)$ as claimed in the introduction.

(2.9) Lemma: *For all j, $1 \leq j \leq n$,*

$$\mu_j \leq \mu_{j-1} + c_0 \binom{j+1}{2} \frac{1}{\lambda_j^*}.$$

Proof As before, it suffices to prove for the case of $j = n$. Then the assertion follows by lemmas 2.5 and 2.8.

∎

(2.10) Corollary: *There exists an i, $1 \leq i \leq n$ such that*

$$\mu_n \lambda_i^* \leq c_o (i+1)^3 \ \log_2^2(i+1).$$

Proof It is easy to show that

$$\sum_{i=1}^{n} \frac{1}{2i\ \log_2^2(i+1)} < 1 = \frac{1}{\mu_n} \sum_{i=1}^{n} (\mu_i - \mu_{i-1}),$$

and hence there exists an $i, 1 \le i \le n$, such that $\mu_i - \mu_{i-1} > \frac{\mu_n}{2i\ log_2^2(i+1)}$. So by the previous lemma, the corollary follows.

▮

The following corollary sharpens the "Flatness Theorem": it says that a lattice-free body is either very flat or else it is flat in several directions. In the next section we will give various further extensions of this result.

(2.11) Corollary: *If a convex body* K *in* $\mathbf{R}^n$ *contains no point of a lattice* L *of dimension* n *in* $\mathbf{R}^n$*, then there exists an* i*,* $1 \le i \le n$ *and* i *linearly independent vectors* $w_1, w_2, \ldots, w_i$ *in the dual lattice* L^* *such that for each* j*,* $j = 1, 2, \ldots, i$*,*

$$\max\{w_j \cdot x : x \in K\} - \ \min\{w_j \cdot x : x \in K\} \le c_o(i+1)^3\ \log_2^2(i+1).$$

▮

Another way to formulate this result is that for every lattice-point-free body, the space $\mathbf{R}^n$ can be mapped linearly into some linear space $\mathbf{R}^i$ (by the mapping $x \mapsto (w_1 \cdot x, \ldots, w_i \cdot x)$ so that the lattice is mapped into $\mathbf{Z}^i$ and the image of K lies inside a cube in $\mathbf{R}^i$ of side $-c_o(i+1)^3 \log_2^2(i+1)$. It would be nice to achieve that the image of K be free from the image of L. We shall address this question in the next section.

It follows from the previous corollary that a lattice-point-free body either has lattice width $O(1)$ or has width $O(n^3\ \log_2^2(n+1)$ along at least two non-parallel dual lattice vectors. In fact, one can get a slightly sharper result.

(2.12) Corollary: *If a convex body K in $\mathbf{R}^n$ contains no point of a lattice L of dimension n in $\mathbf{R}^n$, then either its lattice width is less than 2 or else there exists an i, $2 \le i \le n$ and i linearly independent vectors $w_1, w_2, \ldots, w_i$ in the dual lattice L^* such that for each j, $j = 1, 2, \ldots, i$,*

$$\max\{w_j \cdot x : x \in K\} - \min\{w_j \cdot x : x \in K\} \le 2c_o(i+1)^3 \log_2^2(i+1).$$

Proof: By the hypothesis, we have $\mu_n > 1$. We replace K by the body $\mu_n K$ and prove the conclusion for this which clearly suffices. Now we have $\mu_n = 1$. If the lattice width of K is at least 2 then $\mu_1 \le 1/2$ and hence

$$\sum_{i=2}^{n}(\mu_i - \mu_{i-1}) = 1 - \mu_1 \ge 1/2.$$

Hence the assertion follows by the same argumment as above.

∎

Let us return to inequalities relating various covering minima. We do not know how far the estimate $\mu_{j+1} \le \mu_j + c_o(j+1)\mu_1$ can be improved. For $j = 1$, we can apply the result of Mahler (1948) mentioned above to obtain $\mu_2 \le (1+\sqrt{2})\mu_1$. Hurkens (1987) has shown that in the plane, the maximum value of μ_2/μ_1 is exactly $1 + (2/\sqrt{3})$. From this it follows (by remark 1 following lemma 2.5) that in general, we have

$$\mu_2 \le (1 + (2/\sqrt{3}))\mu_1.$$

For centrally symmetric bodies, perhaps $\mu_{j+1} \le \mu_j + \mu_1$ is valid. We can only prove the following result (which does not remain valid for general convex bodies).

(2.13) Theorem: *If K is a centrally symmetric convex body then for all k, $\mu_{k+1} \le 2\mu_k$.*

Proof: Again it suffices to consider the case when $k = n - 1$. We may also assume that K is 0-symmetric since the covering minima are translation invariant. For this proof, let $\lambda_1 = \lambda_1(K, L)$. Suppose v is nonzero and $v \in \lambda_1 K \cap L$. Let $V = \text{lin}\{v\}$ and let superscript $'$ denote projection parallel to V. Let $p \in \mathbf{R}^n$ be an arbitrary point. We will show that $p \in 2\mu_{n-1}K + L$. First we consider the case when $p' \notin L'$. $p' \in \mu_{n-1}K' + l_1' = S(\text{say})$ for some $l_1 \in L$ by the definition of μ_{n-1}. Let w be the point on the boundary of S such that l_1', p', w are colinear (in that order). Since $\mu_{n-1}K' + L'$ covers $\mathbf{R}^n/V$, there is some $l_2 \in L$, $l_2' \neq l_1'$ such that $w \in \mu_{n-1}K' + l_2'$. Let s_1, s_2, s be the straight lines parallel to v through l_1, l_2, p respectively. Then there are points e, f on s_1, s_2 respectively such that $g(pe) + g(pf) \leq 2\mu_{n-1}$ where g is the distance function corresponding to K. Let a, b be the two lattice points nearest to e on s_1 and c, d be the lattice points nearest to f on s_2. We will show that one of a, b, c, d is at distance (with respect to K) at most $2\mu_{n-1}$ from p. Let $g(pe) = \alpha$ and $g(pf) = \beta$. Then it is easy to see that there must be two adjacent lattice points A, B on s_2 such that $g(aA) + g(aB) \leq 2(\alpha + \beta) + \lambda_1$; but $g(aA), g(aB) \geq \lambda_1$ by definition of λ_1, so $\lambda_1 \leq 2(\alpha + \beta) \leq 4\mu_{n-1}$. Now the sum of distances (corresponding to K) from p to a, b, c, d is at most $2(\alpha + \beta + \lambda_1) \leq 4(\alpha + \beta)$, so one of these 4 distances must be at most $\alpha + \beta$ which is at most $2\mu_{n-1}$ which finishes the proof of the lemma in this case.

In the case that $p' \in L'$, there is a lattice point on the line s at distance at most $\lambda_1/2$ from p, and again it is true that $4\mu_{n-1} \geq \lambda_1$, so we have the required result.

∎

Remark: This inequality is tight. For example, if we take $L = \{x : x \in \mathbf{Z}^n, \sum x_i \text{ is even}\}$ and $K =$ the unit cube, then $\mu_n(K, L) = 2$ whereas $\mu_i(K, L) = 1$ for $i < n$.

3. The volume of lattice-point-free convex bodies

Recall Minkowski's fundamental theorem: If L is an n-dimensional lattice and K is a 0-symmetric convex body in lin (L) , containing no points of L other than 0, then the volume of K is at most $2^n\times$ the determinant of the lattice L. In this section, we address the question of what can be said about the volume of convex bodies that do not contain any lattice points at all. It is trivial to see that we cannot assert anything as strong as an upper bound on the volume — for example in $\mathbf{R}^n$, the convex body $K = \{x : 0.1 \leq x_1 \leq 0.9\}$ has no point of the lattice $L = \mathbf{Z}^n$ and has infinite volume. In this example, however, if we let V to be the subspace $\{x : x_1 = 0\}$, then we see that K/V has the following two nice properties :

(1) $K/V \cap L/V = \emptyset$;

(2) $\text{vol}(K/V) \leq 1$.

The first condition obviously implies that $K \cap L = \emptyset$. Further, the second condition is a Minkowski like upper bound on the volume. This leads us to ask whether there exists a fixed function $f(\cdot)$ such that whenever $K \cap L = \emptyset$, then we can find a subspace V spanned by vectors in L such that $K/V \cap L/V = \emptyset$ and $\text{vol}(K/V) \leq f(i) \cdot \det(L/V)$ where i is the codimension of V. Unfortunately, this is false as we show by a simple two-dimensional example.

Example: Let M be a large positive real. Consider the triangle T in the plane with vertices $(-\frac{1}{2M}, 0), (\frac{1}{2}, M+1), (1+\frac{1}{2M}, 0)$. It is easy to see that the only integer points of T are on its boundary, so the set $S =$ int (T) has no integer points. It is not difficult to see that when M is large enough, for any subspace V of $\mathbf{R}^2$ spanned by integer vectors, S/V contains integer points except when $V = \{0\}$. But of course the volume of S can be increased without bound by increasing M. So we cannot simultaneously satisfy conditions 1 and 2.

But, fortunately, a slight weakening of this is true and this will be the main theorem of this section: instead of requiring that the $K/V \cap L/V = \emptyset$ we can only require that if x belongs to $K/V \cap L/V$, then x is not very "centrally" located in K.

Definition: Suppose δ is a nonnegative real number. A point x in a convex set K is $\delta-$ central for K if for any $y \in K$, there exists $z \in K$ such that $z - x = \delta(z - y)$.

(3.1) Remark: It is clear that every point is 0-central and no point is ϵ-central for any ϵ greater than 1/2.

If the convex set K in $\mathbf{R}^n$ has a center of gravity $c(K)$, then the contraction of K about $c(K)$ by a factor of $(1 - \delta)$ contains only $\frac{\delta}{n+1}-$ central points of K. Conversely, if a point x is δ-central for a convex body K in $\mathbf{R}^n$ with center of gravity y, then there is a z in K such that $z - x = \delta(z - y)$, thus x belongs to a contraction of K by a factor of $1 - \delta$ about y. In the special case when K has a center of symmetry, the contraction of K by a factor of $1 - \delta$ about this center is precisely the set of $\delta/2$-central points. This remark is not used in what follows; it shows, however, that the notion of centrality we use here ties in with another notion in which a point x may be defined to be central if it lies in the body obtained from K by shrinking it by a factor of $1 - \delta$ from its center of gravity.

We associate a series of numbers with a convex body and a given basis of a lattice. Suppose K is a convex body in $\text{lin}(L)$ where L is a lattice described by a basis $b_1, b_2, \ldots b_n$ of it. Let $V_i = \text{lin}\{b_1, b_2, \ldots b_n\}$ for $i = 1, 2, \ldots n$ and $V_0 = \{0\}$. Let $\hat{b}_i = b_i/V_{i-1}$ for $i = 1, 2, \ldots n$. Let $f_i(\cdot)$ be the distance function on V_n/V_{i-1} whose unit ball is $(K - K)/V_{i-1}$ for $i = 1, 2, \ldots n$. We define the series of numbers $\tau_1, \tau_2, \ldots \tau_n$ as follows :

$$\tau_i(K; b_1, b_2, \ldots b_n) = f_i(\hat{b}_i).$$

(3.2) Lemma: For any lattice L, any basis $b_1, b_2, \ldots b_n$ of it and any convex body K in $\text{lin}(L)$, we have

$$\mu_n(K, L) \leq \sum_{j=1}^{n} \tau_j(K; b_1, b_2, \ldots b_n).$$

Proof: The proof follows the lines of the proof of lemma (2.5). Let $\tau_i = \tau_i(K; b_1, b_2, \ldots b_n)$. Since $b_1 \in \tau_1 \cdot (K - K)$, we can assume (after a suitable translation of K) that 0 and b_1/τ_1 both belong to K. (Note that translation of K leaves all quantities in the lemma invariant.) Arguing as in lemma (2.5), we have then that $\mu_n(K,L) \le \tau_1 + \mu_{n-1}(K/V_1, L/V_1)$. But $\{b_2/V_1, b_3/V_1, \dots b_n/V_1\}$ forms a basis of L/V_1. Hence the lemma follows by induction.

∎

We now define a notion of "reduced basis". This notion was introduced for the case when the 0-symmetric convex body in the definition is a sphere by Korkine and Zolatarev (1873).

(3.3) Definition: Let $b_1, b_2, \dots, b_n$ be a basis of the lattice L. For $i = 2, 3, \dots n$, let $\hat{b}_i = b_i/\text{lin}\{b_1, b_2, \dots b_{i-1}\}$ and let $\hat{b}_1 = b_1$. The basis $b_1, b_2, \dots b_n$ is said to be a reduced basis for the lattice L with respect to a 0-symmetric convex body P if

(3.3.1) b_1 achieves the first (Minkowski) minimum of L with respect to P.

(3.3.2) For $i \ge 2$, $\hat{b}_i$ achieves the first minimum of $L/$ lin $\{b_1, b_2, \dots, b_{i-1}\}$ with respect to $P/$ lin $\{b_1, b_2, \dots, b_{i-1}\}$.

(3.3.3) For j, i such that $n \ge j > i \ge 1$, $|b_j \cdot \hat{b}_i| \le |\hat{b}_i \cdot \hat{b}_i|/2$.

Our definition makes it clear that such a reduced basis always exists. Note that the value of the first minimum attained in (3.3.2) is exactly $\tau_i(\frac{1}{2}P; b_1, b_2, \dots b_n)$.

(3.4) Theorem: *Suppose L is an $n-$dimensional lattice and K is a convex body in $lin(L)$ with $K \cap L = \emptyset$. Let $b_1, b_2, \dots b_n$ be a reduced basis of L with respect to $K - K$. Let $V_i = lin(b_1, b_2, \dots b_i)$ and $\tau_i = \tau_i(K; b_1, b_2, \dots b_n)$ for $i = 1, 2, \dots n$. Then for each i, $1 \le i \le n-1$, the projection parallel to V_i has the following properties.*

(3.4.1) L/V_i contains no $(\tau_1 + \dots + \tau_i)$-central point K/V_i.

(3.4.2) There exist $n - i$ linearly independent vectors $w_1, w_2, \dots, w_{n-i}$ in $(L/V_i)^*$ so that for $j = 1, 2, \dots n - i$,

$$\max\{w_j \cdot x : x \in K/V_i\} - \min\{w_j \cdot x : x \in K/V_i\} \leq \frac{c_o(n-i)^2}{\tau_{i+1}}$$

(3.4.3) The volume of K/V_i is at most $\det(L/V_i)/(\tau_{i+1})^{n-i}$.

(3.5) Remark: We have

$$\begin{aligned} &\max\ \{w_j \cdot x : x \in K/V_i\} - \min\ \{w_j \cdot x : x \in K/V_i\} \\ &= \max\ \ \{w_j \cdot x : x \in K\} - \ \min\ \ \{w_j \cdot x) : x \in K\}, \end{aligned}$$

since $w_j \in \text{lin}(L)/V_i$. Also observe that $w_1, \ldots, w_{n-i}$ are vectors in L^*. So (3.4.2) implies that K has "small" width along these $n-i$ dual lattice vectors. In words, the theorem states that if K is free of lattice points, there is an $n-i$ dimensional projection of it that is free of "central" lattice points of the projected lattice and has "small" width in $n-i$ independent directions - the maximum number possible.

Proof: I. Suppose (3.4.1) fails. Then there is a $(\tau_1 + \ldots + \tau_i)$-central point of K/V_i which belongs to L/V_i. Of course, we have $\tau_1 + \tau_2 + \ldots \tau_i \leq 1/2$. Without loss of generality, we may assume that this point is 0. For the rest of the proof, we use the following notation: $K' = K \cap V_i$ and $L' = L \cap V_i$.

(3.6) Claim: $K' - K' \supseteq (\tau_1 + \ldots + \tau_i)((K-K) \cap V_i)$.

(Note that $(K-K)/V_i = K/V_i - K/V_i$ but in general $(K-K) \cap V_i \neq (K \cap V_i) - (K \cap V_i)$.)

Proof: Suppose $v \in (K-K) \cap V_i$. We wish to show that $(\tau_1 + \ldots + \tau_i)v \in (K' - K')$. There exists $p \in K$ so that $p + v \in K$. Since 0 is $(\tau_1 + \ldots + \tau_i)$ central in K/V_i, there exists $s \in K$ so that $s/V_i = (\tau_1 + \ldots + \tau_i)(s/V_i - p/V_i)$. Now the vectors $(\tau_1 + \ldots + \tau_i)p + (1 - (\tau_1 + \ldots + \tau_i))s$ and $(\tau_1 + \ldots + \tau_i)(p + v) + (1 - (\tau_1 + \ldots + \tau_i))s$ are in K', since $\tau_1 + \tau_2 + \ldots \tau_i \leq 1$, which proves the claim.

∎

(3.7) Claim: $\mu_i(K', L') \leq 1$.

Proof: $b_1, b_2, \dots b_i$ is a basis of the lattice L'. By claim (3.6), we have $\tau_j(K'; b_1, b_2, \dots b_i) \leq \frac{\tau_j(K; b_1, b_2, \dots b_n)}{\tau_1 + \tau_2 + \dots \tau_i}$ for $j = 1, 2, \dots i$. So the claim follows by lemma (3.2).

∎

Thus, we have that $K' \cap L' \neq \emptyset$ which implies that $K \cap L \neq \emptyset$, a contradiction that establishes (3.4.1).

II. Since $\tau_{i+1} = \lambda_1((K-K)/V_i, L/V_i)$, we have by lemma (2.8),

$$\lambda_{n-i}(((K-K)/V_i)^*, (L/V_i)^*) \leq c_o \binom{n-i+1}{2} / \tau_{i+1}$$

which implies (3.4.2).

III. Finally,$\tau_{i+1} = \lambda_1((K-K)/V_i, L/V_i)$ also implies that

$$\text{vol}((K-K)/V_i) < \frac{2^{n-i} \text{ det } (L/V_i)}{\tau_{i+1}^{n-i}}$$

by Minkowski's convex body theorem. Since

$$\begin{aligned} \text{vol}((K-K)/V_i) &= \text{vol}(K/V_i - K/V_i) = 2^{n-i}\text{vol}(\tfrac{1}{2} \cdot K/V_i - \tfrac{1}{2} \cdot K/V_i) \\ &\geq \text{vol}(K/V_i) \end{aligned}$$

by the Brunn-Minkowski Theorem, (3.4.3) follows.

∎

(3.8) Corollary: *Suppose L is an $n-$dimensional lattice and K is a convex body in lin(L) with $K \cap L = \emptyset$. Let $\Delta_1, \Delta_2, \ldots \Delta_n$ be real numbers satisfying $0 = \Delta_0 < \Delta_1 < \Delta_2 < \Delta_3 \ldots < \Delta_n \leq 1$. Then there is an i, $0 \leq i \leq n-1$ and an i dimensional subspace T of lin(L) spanned by vectors in L such that*

(3.8.1) K/T contains no Δ_i - central point which belongs to L/T.

(3.8.2) There exist $n-i$ linearly independent vectors $w_1, w_2, \ldots w_{n-i}$ in $(L/T)^*$ so that for $j = 1, 2, \ldots n-i$,

$$max\ \{w_j \cdot x : x \in K/T\} - \ min\ \{w_j \cdot x : x \in K/T\} \leq \frac{c_o(n-i)^2}{\Delta_{i+1} - \Delta_i}$$

(3.8.3) The volume of K/T is at most $det\ (L/T)/(\Delta_{i+1} - \Delta_i)^{n-i}$.

Proof: Let $b_1, b_2, \ldots, b_n$ be a reduced basis of L with respect to $K - K$ and let $\tau_i = \tau_i(K; b_1, b_2, \ldots b_n)$ for $i = 1, 2, \ldots n$. Note that $\tau_1 + \tau_2 + \ldots \tau_n \geq \mu_n(K, L) > \Delta_n$. Let k be the minimum value of j such that $\tau_1 + \tau_2 + \ldots \tau_j \geq \Delta_j$. We will prove that the corallory holds with $i = k-1$.We consider two cases :

Case 1: $k = 1$. Then we choose $T = \emptyset$. (3.8.1) is obviously true. We have $\lambda_1((K-K), L) = \tau_1 \geq \Delta_1$. So, (3.8.2) follows by corallory (2.8). (3.8.3) follows from Minkowski's convex body theorem ; the proof is very similar to the proof of (3.4.3) and we omit it.

Case 2: $k \geq 2$. Then we take $T = \text{lin}(b_1, b_2, \ldots b_i)$. Then $\tau_1 + \tau_2 + \ldots \tau_i < \Delta_i$ and $\tau_{i+1} \geq \Delta_{i+1} - \Delta_i$, so the corallory follows from theorem 3.4.

∎

By choosing different sequences for the Δ's we can get different applications of the corallory. One natural choice is $\Delta_i = \sum_{j=1}^{i} 1/(2j \log_2^2(j+1))$. For this choice, (3.4.1) will be rather weak whereas (3.4.2) will be strong :

$$\max\{w_j \cdot x : x \in K/T\} - \min\{w_j \cdot x : x \in K/T\} \leq 2c_o i^3 \log_2^2(i+1).$$

Thus we obtain corallory (2.11) as a special case. Another sequence $\Delta_i = i/n$ for $i = 0, 1, 2, \dots n$ yields some interesting results. With this sequence, we immediately get the following corallory.

(3.9) Corollary: *If L is an n-dimensional lattice and K is a convex body in lin(L) with $K \cap L = \emptyset$ then there exists an $j, 1 \leq j \leq n$ and an $(n-j)$-dimensional subspace T spanned by vectors in L such that the volume of K/T is at most $n^j \det(L/T)$.*

∎

We can re-formulate this result to give upper and lower bounds on the covering radius μ_n in terms of volumes of projections. Assuming that we can compute volumes efficiently (which in fact we can not), these bounds give an "approximate good characterization" of the covering radius in the following sense: they provide a necessary condition and a (different but close) sufficient condition for the *existence* of a lattice point in every translation of a body in terms of the *non-existence* of a projection with small volume.

(3.9) Definition: Let L be a lattice and K a convex body in the linear span of L. We define $\rho(K, L)$ to the infimum over all subspaces V of $\text{lin}(L)$ spanned by vectors in L of the quantity $(\text{vol}(K/V) \ / \det(L/V))^{1/k}$ where k is the dimension of $\text{lin}(L)/V$.

If for a positive real number t, $tK + L$ covers $\text{lin}(L)$, then clearly, $t\,K/V + L/V$ covers $\text{lin}(L)/V$ for all subspaces V spanned by vectors in L, so we must have $\text{vol}(t\,K/V)/\det(L/V)$ must be at least 1. Thus it is clear that $\mu_n(K, L) \geq 1/\rho(K, L)$. Together with Corollary (3.8), this yields the following:

(3.10) Corollary: *For any lattice L and convex body K in the span of L, $1/\rho(K, L) \leq \mu_n(K, L) \leq n/\rho(K, L)$.*

∎

Remark : In the case when K is an ellipsoid, the upper bound can be improved to $O(\sqrt{n})/\rho(K,L)$, along the lines mentioned after Lemma (2.5).

The question arises as to how much we can improve the upper bound on the product $\mu\rho$ in Corollary (3.10). We will show below that it cannot be improved below $O(\log n)$. To this end, consider the simplex

$$S = \{x : x \in \mathbf{R}^n \ ; \ \sum_{i=1}^{n} a_i x_i \leq 1 \ ; \ x_i \geq 0 \forall i\}$$

where the a_i are as yet unspecified reals satisfying $1 = a_1 \geq a_2 \geq a_3 \ldots \geq a_n > 0$. Let L be $\mathbf{Z}^n$. We claim that

$$\mu_n(S,L) = \sum_{i=1}^{n} a_i.$$

In fact, for any positive ϵ, it is easy to see that the point $(1-\epsilon, 1-\epsilon, \ldots, 1-\epsilon)$ belongs to $tS+L$ iff $t \geq \sum a_i(1-\epsilon)$, so we have $\mu_n(S,L) \geq \sum a_i$. The reverse inequality is also obvious.

We now wish to compute $\rho(S,L)$. To this end, we argue that the infimum in the definition of ρ is achieved for a subspace V spanned by a subset of $\{e_1, \ldots, e_n\}$. For, given any subspace V of dimension i, choose subspace U spanned by $n-i$ unit vectors such that $V \cap U = \{0\}$ .Let W be the orthogonal complement of U. Let S' and L' denote the projection of S and L parallel to V on the space U. Then it is clear that $\text{vol}(S/V)/\det(L/V) = \text{vol}(S')/\det(L')$. Furthermore, $\text{vol}(S') \geq \text{vol}(S/W)$ and $\det(L') \leq \det(L/W)$. So W is "better" than V.

Now if V is spanned by the unit vectors $\{e_{k_1}, \ldots, e_{k_i}\}$ then

$$\text{vol}(S/V) = \frac{1}{i!a_{k_1} \ldots a_{k_i}} \geq \frac{1}{i!a_1 \ldots a_i},$$

and

$$\det(L/V) = 1.$$

Let $g(i) = \left(\frac{1}{i!a_1 a_2 \ldots a_i}\right)^{1/i}$ for $i = 1, 2, \ldots n$. Then, we have $\rho(S, L) \geq \min_i g(i)$. Choosing $V = \text{lin}(e_{i+1}, e_{i+2}, \ldots e_n)$, we see that equality is acheived, so we in fact have

$$\rho(S, L) = \min_i g(i).$$

Now putting $a_i = 1/i$ for $i = 1, 2, \ldots n$, we have $\rho(S, L) = 1$ and $\mu_n(S, L) = \sum_{i=1}^{n} 1/i = O(\log n)$, thus establishing a lower bound of $O(\log n)$ on the product $\mu\rho$. It is not diffucult to see that for any $a_1, a_2, \ldots a_n$ satisfying $1 = a_1 \geq a_2 \geq a_3 \ldots a_n \geq 0$, we have $\min_i g(i) \leq O(\log n)/\sum a_i$, so we have $\mu_n(S, \mathbf{Z}^n)\rho(S, \mathbf{Z}^n) \leq O(\log n)$ for any simplex S with one vertex at the origin and the others along the coordinate axes.

4. Convex bodies with few lattice points

In this section, we extend our results on lattice-point-free convex bodies in terms of the number of lattice points in the body.

(4.1) Theorem: *If L is a n dimensional lattice and K a convex body in lin(L), with $s = |K \cap L|$, then there exists a nonzero element u of L^* such that* $\max\{u \cdot x : x \in K\} - \min\{u \cdot x : x \in K\} \leq c_o\lceil (s+1)^{1/n} \rceil n^2$.

Proof: For any convex body S in the linear span of an m dimensional lattice P and any natural number k, define $\mu_m(S, P, k)$ to be the infimum over positive reals t such that for each $x \in$ lin (P), there exist k distinct elements $y_1, y_2, \ldots y_k$ in P such that x belongs to $y_i + tS$ for $i = 1, 2, \ldots k$. Note that this quantity is also invariant under translations of S. We will show that for any natural number k, the following holds.

$$\mu_n(K, L, k)\lambda_1((K-K)^*, L^*) \leq c_o\lceil k^{1/n} \rceil n^2 \qquad (4.2)$$

For the rest of the proof, let us abbreviate $\mu_n(K, L, k)$ by $\mu(k)$; $\lambda_1(K - K, L)$ by λ_1 and $\lambda_1((K-K)^*, L^*)$ by λ_1^*. Note that $|K \cap L| = s$ implies that $\mu(s+1) \geq 1$. This together with the inequality (4.2) obviously gives us the theorem.

Let v be a nonzero element of $L \cap \lambda_1(K-K)$. We first translate K so that $0, v$ belong to $\lambda_1 K$. Let $V =$ lin (v) and let $K' = K/V; L' = L/V$ and for each natural number k, denote by $\mu'(k)$ the quantity $\mu_{n-1}(K', L', k)$. We claim that for any natural numbers k, l

$$\mu(kl) \leq \mu'(k) + l\lambda_1$$

For any p in lin (L), there exist k distinct points $y_1, y_2, \ldots y_k$ in L' such that $y_i + \mu'(k)K'$ intersects the line through p parallel to v. There are clearly l distinct points of L (say $v_{i1}, v_{i2}, \ldots, v_{il}$) on the line $y_i + V$ such that $v_{ij} + \mu'(k)K$ intersects $p+V$ at a point q_{ij} with $p - q_{ij} = \alpha_{ij} v$ where $0 \leq \alpha_{ij} \leq l$. Clearly all the v_{ij} are distinct and p belongs to $v_{ij} + (\mu'(k) + l\lambda_1)K$ for all i, j proving the claim.

Using this, we prove the inequality (4.2) by induction on n. First observe that it is obvious for $n = 1$. Let $l = \lceil k^{1/n} \rceil$ and $r = \lceil k^{\frac{n-1}{n}} \rceil$. Since $lr \geq k$, we have that $\mu(k) \leq l\lambda_1 + \mu'(r)$. By induction, we have that $\mu'(r)\lambda_1((K/V - K/V)^*, (L/V)^*) \leq c_o \lceil r^{\frac{1}{n-1}} \rceil (n-1)^2 \leq c_o l(n-1)^2$ which gives that $\mu'(r)\lambda_1^* \leq c_o l(n-1)^2$. This combined with the inequality $\lambda_1 \lambda_1^* \leq c_o n$ finishes the proof.

∎

Remark: The bound in the theorem cannot be improved below $O(n(s+1)^{1/n})$ as the following examples show : Let K be the the simplex in $\mathbf{R}^n$ with vertices $(0,0,\ldots 0), (M,0,0,\ldots 0), (0,M,0,0\ldots 0), \ldots (0,0,\ldots 0,M)$ for an arbitrary (large) positive M. Then for suitably large M, K has roughly as many points of $\mathbf{Z}^n$ as the volume of K which is $M^n/n!$ and the width of K is $O(M)$.

In the case that K is centrally symmetric (i.e., there exists a point c in K such that for all x, whenever $c+x$ belongs to K, so does $c-x$), the upper bound in the theorem can be improved by a factor of $O(n)$ as follows:

(4.3) Claim: *For any positive real number* α, $\frac{\alpha}{\lambda_1^*}(K-K)$ *contains at least* $\lfloor \left(\frac{\alpha}{c_o n}\right)^n \rfloor$ *distinct points of* L.

Proof: The volume of $\lambda_1^*(K-K)^*$ is at most 2^n det (L^*) and hence the volume of the dual object $\frac{1}{\lambda_1^*}(K-K)$ is at least $\frac{(4/c_o n)^n}{2^n \text{ det } (L^*)} = \frac{2^n \text{ det } (L)}{c_o^n n^n}$ (by the result of Bourgain and Milman). Thus the volume of $\frac{\alpha}{\lambda_1^*}(K-K)$ is at least $\frac{(2\alpha)^n \text{ det } (L)}{c_o^n n^n}$ whence the claim follows by Mordell's theorem (Theorem 1, §7.2 of Lekkekerker (1969)).

∎

Let $f(\cdot)$ be the distance function defined by $K-K$. Now for any point p in space, there is a point x of L such that $\mu_n(K,L)K + x$ contains p. Let k be any natural number. By the above claim, there are at least k distinct points y in L, such that $f(y-x) \leq c_o n k^{1/n}/\lambda_1^*$. All these points y satisfy $f(y-p) \leq \mu_n(K,L) + c_o n k^{1/n}/\lambda_1^*$, thus we have the following theorem.

(4.4) Theorem: *If* L *is an* n *diemnsional lattice and* K *is a centrally symmetric convex body in lin*(L), *with* $s = |K \cap L|$, *then there exists a nonzero element* u *of* L^* *such that* $\max\{u \cdot x : x \in K\} - \min\{u \cdot x : x \in K\} \leq c_o n^2 + c_o n s^{1/n}$.

∎

5. Some Applications

In this section, we give some applications of the methods and results of this paper in number theory. The first concerns the residue classes of a linear form modulo a prime and the second concerns inhomogeneous simultaneous diophantine approximation.

Suppose p is a prime number and $a_1, a_2, \ldots a_n$ are any natural numbers. For any natural number b, define $\alpha(b)$ as follows :

$$\alpha(b) = \min\{x_1 + x_2 + \ldots + x_n \ : \ x_i \geq 0, \text{ integers } , \sum_{i=1}^{n} a_i x_i \equiv b \pmod{p}\}.$$

Let

$$\mu(a_1, a_2, \ldots, a_n; p) = \max\{\alpha(b) : 0 \leq b < p\}.$$

(In words, μ is the least integer such that every residue class modulo p can be represented as the sum of at most μ — not necessarily distinct — numbers a_i.)

To see what makes μ large, suppose that there exists a natural number t and integers s_i such that $s_i \equiv ta_i \pmod{p}$ and $|s_i| \leq \phi$ for all i. Let $b \equiv t^{-1}(p-1)/2 \pmod{p}$. Then for any natural numbers $x_1, x_2, \ldots x_n$ with $\sum_{i=1}^{n} a_i x_i \equiv b \pmod{p}$, we have $\sum_{i=1}^{n} s_i x_i \equiv \frac{p-1}{2} \pmod{p}$, whence $\sum_{i=1}^{n} |s_i| x_i \geq \frac{p-1}{2}$ and hence $\sum_{i=1}^{n} x_i \geq (p-1)/2\phi$. We show that this is, in a sense, the only reason for μ to be large.

Let $\phi(a_1, a_2, \ldots, a_n; p)$ denote the least ϕ in the above argument. More formally, let $|x \pmod{p}|$ be the minimum absolute value of an integer y such that $y \equiv x \pmod{p}$ (thus $|x \pmod{p}|$ is always in the range $[0 \ \frac{p-1}{2}]$) and $\phi = \phi(a_1, a_2, \ldots, a_n; p)$, the minimum over all integers $t, 1 \leq t \leq p-1$, of the maximum of $\{|ta_1 \pmod{p}|, |ta_2 \pmod{p}|, \ldots, |ta_n \pmod{p}|\}$.

Theorem (5.1): *Let p be a prime number and $a_1, a_2, \ldots a_n$ any n natural numbers and let $\mu(a_1, a_2, \ldots a_n; p) = \mu$ and $\phi(a_1, a_2, \ldots a_n; p) = \phi$ be the quantities defined above. With c_o as in lemma (1.2), we have*

$$(p-1)/2\phi \leq \mu \leq c_o n^2 p/\phi.$$

Proof: We already proved the left hand side inequality. To prove the right hand side inequality, we will use theorem (2.7). First observe that we can assume that the greatest common divisor of $a_1, a_2, \ldots a_n$ is 1 — if not we can divide all of them by their g.c.d., which leaves the two quantities in the theorem unchanged. Let $S \subseteq \mathbf{R}^n$ be the simplex $\{x : \sum_{i=1}^n x_i \leq 1; x_i \geq 0 \text{ for } i = 1, 2 \dots n\}$ and let L be the lattice $\{x : x \in \mathbf{Z}^n; \sum_{i=1}^n a_i x_i \equiv 0 \pmod p\}$. Let $\mu_n(S, L)$ be the covering minimum defined in section 2. Let a be the vector $(a_1, a_2, \dots a_n)$ and for any x in $\mathbf{R}^n$, we will denote $\sum_{i=1}^n a_i x_i$ by $a \cdot x$.

Claim (5.2): $\mu \leq \mu_n(S, L)$.

Proof: Let b be an arbitrary natural number. Consider any $x \in \mathbf{Z}^n$ such that $a \cdot x \equiv b \pmod p$. There exists a $y \in L$ such that $y + \mu_n(S, L)S$ contains x. Then $x - y$ is in $\mu_n(S, L)S$ and $a \cdot (x - y) \equiv b \pmod p$ thus proving the claim.

∎

It is easy to see a converse to the inequality :

$$\mu \geq \mu_n(S, L) - n.$$

In fact, for any point x in $\mathbf{Z}^n$, there is an integer point z in μS such that $a \cdot z \equiv a \cdot x \pmod p$ by the definition of μ. Then $x - z$ belongs to L, thus $L + \mu S$ contains $\mathbf{Z}^n$. Further, $\mathbf{Z}^n + nS$ contains $\mathbf{R}^n$ proving the ineqality. We will not use this ineqality in what follows.

Claim (5.3): $\phi \leq p\lambda_1((S - S)^*, L^*) \leq 2\phi$.

Proof: First, we assert that L^* is the set of all integer linear combinations of the n unit vectors plus the vector $(\frac{a_1}{p}, \frac{a_2}{p}, \dots \frac{a_n}{p})$. (This is not a basis because it is a dependent set.) To see this, first observe that there is a unimodular $n \times n$ matrix B whose first row is $a_1, a_2, \dots a_n$ since the a_i are relatively prime. It is easy to see that the rows of B with the first row multiplied by $1/p$ form a basis of L^*. Then the assertion follows since all the unit vectors and $(\frac{a_1}{p}, \frac{a_2}{p}, \dots \frac{a_n}{p})$ are all integer combinations of this basis of L^* and conversely. So,

$$L^* = \{\sum_{i=1}^{n} \beta_i e_i + tv : \beta_i, t \in \mathbf{Z}\}$$

where, e_i are the unit vectors and $v = (a_1/p, a_2/p, \ldots a_n/p)$. Thus the minimum l_∞ norm of a nonzero vector in L^* is the minimum over all nonzero integers t of the value max $\{\lceil ta_1/p \rfloor, \lceil ta_2/p \rfloor, \ldots, \lceil ta_n/p \rfloor\}$ where for a real number r, $\lceil r \rfloor$ denotes the distance from r to the nearest integer. Thus the first minimum of L^* with respect to $C = \{x : |x_i| \leq 1\}$ equals ϕ/p.

Next, we assert that $\frac{1}{2}C \subseteq (S - S)^* \subseteq C$. If $a \in (S - S)^*$, then $-1 \leq a \cdot e_i \leq 1$ for all the unit vectors e_i (since all e_i belong to S), so $|a|_\infty \leq 1$, thus $(S - S)^* \subseteq C$. If $a \in \frac{1}{2}C$, then for all $x, y \in S$, we have $|a \cdot (x - y)| \leq \sum_{i=1}^{n} |a_i| \, |x_i - y_i| \leq \frac{1}{2} \sum_{i=1}^{n} |x_i| + |y_i| \leq 1$, so we have $\frac{1}{2}C \subseteq (S - S)^*$. Now the claim follows from the last paragraph.

$\blacksquare$

Now theorem (5.1) follows from claims (5.2) and (5.3) and theorem (2.7).

$\blacksquare$

Remark (5.4): The lower bound in theorem (5.1) is tight as seen by the following example : $a_1 = -1$, $a_2 = a_3 = \ldots = a_n = 1$ whence it is easy to see that $\phi = 1$ and $\mu = (p-1)/2$. We do not know if the upper bound is tight. But it can be shown that the upper bound cannot be improved by more than a factor of $O(n)$ as follows. (We only sketch the argument.) Suppose p is fixed and much larger than n. We give a counting argument that for most $a_1, a_2, \ldots a_n$, we have $\alpha(0) \geq cnp^{1/n}$ for some numerical constant c. Let S be the simplex defined above. Then for positive reals M such that $M >> n$, the number of integer points in $M \cdot S$ is roughly the volume of $M \cdot S$ which equals $M^n/n!$. Each point x in $M \cdot S$ satisfies $a \cdot x \equiv 0 \pmod{p}$ for p^{n-1} of the possible p^n vectors a. Thus there exists a constant c such that if $M < cnp^{1/n}$, then for 3/4 of all possible a's

, there is no x in $M \cdot S$ such that $a \cdot x \equiv 0 \pmod{p}$. This proves our claim from which it obviously follows that for at least 3/4 of the a's, μ exceeds $cnp^{1/n}$. We will also show that there is a numerical constant d such that for at least 3/4 ths of the a's, $\phi \geq dp^{\frac{n-1}{n}}$. Let M be any positive real. Then the number of vectors with n integer components each at most M in absolute value is at most $(2M+1)^n$, each such vector can be multiplied by any integer t modulo p to produce an a with $\phi \leq M$. Thus there are at most $O(pM^n)$ vectors a for which ϕ is less than or equal to M. Since the total number of a's is p^n, our claim is proved. The two claims together show that for a positive fraction of the a's , the product $\mu\phi$ exceeds c_1pn for some numerical constant c_1.

The methods above can be extended to several congruences (instead of one) and to non-prime modulii. Also, α and μ can be defined with respect to convex bodies other than the simplex S.

Our second aplication concerns inhomogenoeus simultaneous diophantine approximation. Suppose $\alpha_1, \alpha_2, \ldots \alpha_n$ are arbitrary reals. The general problem of approximating them by rationals with the same denominator is called simulataneous homogeneous diophantine approximation. In the inhomogeneous case, we have also n other reals $\beta_1, \beta_2, \ldots \beta_n$ and we wish to approximate $\alpha_1, \alpha_2, \ldots \alpha_n$ by reals $(p_1+\beta_1)/q, (p_2+\beta_2)/q, (p_3+\beta_3)/q \ldots, (p_n+\beta_n)/q$ (respectively) where $p_1, p_2, \ldots p_n$ and q are integers. Cassels (1957) is a general reference on the topic. For the next theorem, we remind the reader of the notation that for a real number r, we denote by $\lceil r \rfloor$ the distance of r to the nearest integer.

Theorem (5.5): *Suppose $\alpha_1, \alpha_2, \ldots \alpha_n$ are any reals and let Q, ϵ be positive reals such that for all integers $a_1, a_2, \ldots a_n$, not all zero,*

$$Q\lceil a_1\alpha_1 + a_2\alpha_2 + \ldots a_n\alpha_n \rfloor + \epsilon \sum_{i=1}^{n} |a_i| \geq c_o n^2 \qquad (5.6).$$

Then for all reals $\beta_1, \beta_2, \ldots \beta_n$, there exist integers $p_1, p_2, \ldots p_n, q$ with $|q| \leq Q$ such that for all i,

$$|q\alpha_i - p_i - \beta_i| \leq \epsilon. \qquad (5.7)$$

Conversely, if for all reals $\beta_1, \beta_2, \ldots \beta_n$, there exist integers $p_1, p_2, \ldots p_n$, and q with $|q| \leq Q$ such that (5.7) is satisfied, then for all integers $a_1, a_2, \ldots a_n$, not all zero, we have

$$Q\lceil a_1\alpha_1 + a_2\alpha_2 + \ldots a_n\alpha_n\rfloor + \epsilon\sum_{i=1}^{n}|a_i| \geq 1/2.$$

Proof: We first prove the second statement in the theorem. Suppose $a_1, a_2, \ldots a_n$ is any set of integers not all zero. Choose $\beta_1, \beta_2, \ldots \beta_n$ so that $\sum_{i=1}^{n} a_i\beta_i = 1/2$. For these β's there exist integers $q, p_1, p_2, \ldots p_n$ by hypothesis so that (5.7) is satisfied. So we have $a_ip_i + a_i\beta_i - \epsilon|a_i| \leq qa_i\alpha_i \leq a_ip_i + a_i\beta_i + \epsilon|a_i| \quad \forall i$. Summing these and noting the definition of β, we have $\lceil q\sum a_i\alpha_i\rfloor \geq \frac{1}{2} - \epsilon\sum|a_i|$ whence of course $|q|\lceil\sum a_i\alpha_i\rfloor \geq \frac{1}{2} - \epsilon\sum|a_i|$, completing the proof of the second part of the theorem.

The first part of the theorem is proved by appealing to theorem (2.7). To this end, let L be the lattice generted by the rows of the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & & & & . \\ . & . & & . & & & . \\ . & . & & & . & & . \\ 0 & 0 & . & . & 0 & 1 & 0 \\ \alpha_1 & \alpha_2 & . & . & . & \alpha_n & \epsilon/Q \end{pmatrix}$$

Let K be the unit "cube" $= \{x : x \in \mathbf{R}^{n+1}; |x_i| \leq 1\}$. Then it is easy to see that the conclusion of the first part of the theorem is true (i.e., for all reals $\beta_1, \beta_2, \ldots \beta_n$ there exist integers $p_1, p_2, \ldots p_n, q$ with $|q| \leq Q$ satisfying (5.7)) if and only if $\mu_{n+1}(K, L) \leq \epsilon$. So it suffices to prove that under the hypothesis, $\mu_{n+1}(K, L) \leq \epsilon$. But, the dual lattice L^* is generated by the rows of the following matrix :

$$\begin{pmatrix} 1 & 0 & 0 & . & . & . & (-Q\alpha_1)/\epsilon \\ 0 & 1 & 0 & . & . & . & (-Q\alpha_2)/\epsilon \\ . & . & . & & & & . \\ . & . & & . & & & . \\ . & . & & & . & & . \\ 0 & 0 & . & . & 0 & 1 & (-Q\alpha_n)/\epsilon \\ 0 & 0 & . & . & . & 0 & Q/\epsilon \end{pmatrix}$$

$(K-K)^*$ is the octahedron $\{x : x \in \mathbf{R}^{n+1}; \sum |x_i| \leq 1/2\}$ and it is easy to check that the hypothesis in the theorem implies that $\lambda_1((K-K)^*, L^*) \geq c_o n^2/\epsilon$; this together with theorem (2.7) yields the current theorem.

∎

We formulate another version of this last result, which shows that it can be viewed as a strong quantitative version of a theorem of Kronecker (cf Lovász 1986, Theorems (1.1.9) and (1.3.4)). Another quantitative version was proved by Khinchine (1946); his result implies the version of ours in which the factor n^2 below is replaced by an exponentially large factor. Note, however, that ours is in a sense weaker than Kronecker's and Khinchine's result, because the latter say something about each particular choice of the β_i. We could use the results of Hastad (1987) instead, and obtain a version which would assert a similar "pseudo-equivalence" for each particular choice of the β_i, but would give a worse value (n^3 instead of n^2) on the right hand side.

(5.8) Theorem: *Suppose p is a prime number and n is a natural number greater than 1. Suppose $\alpha_1, \alpha_2, \ldots \alpha_n$ are integers not all divisible by p and ϵ is a positive real such that*

$$\min\{\sum_{i=1}^{n} |a_i| : \sum_{i=1}^{n} a_i\alpha_i \equiv 0 \pmod{p} \text{ ; } a_i \in \mathbf{Z}\forall i \text{ ; not all } a_i = 0\} \geq c_o n^2/\epsilon \tag*{(5.9).}$$

Then, for all integers $\beta_1, \beta_2, \dots \beta_n$, there exists an integer t such that

$$|t\alpha_i - \beta_i \pmod{p}| \leq \epsilon p \text{ for } i = 1, 2, \dots n \tag{5.10}$$

Conversely, if for all integers $\beta_1, \beta_2, \dots \beta_n$, there exists an integer t satisfying (5.10), then

$$\min\{\sum_{i=1}^{n} |a_i| : \sum_{i=1}^{n} a_i\alpha_i \equiv 0 \pmod{p} \ ; \ a_i \in \mathbf{Z} \forall i \ ; \text{ not all } a_i = 0\} \geq \frac{1}{4\epsilon}.$$

Proof: The first part of the theorem is proved using theorem (5.5). To this end, let $\alpha'_i = \alpha_i/p$ for $i = 1, 2, \dots, n$. We wish to apply the first part of theorem (5.5) with the α' s , ϵ and $Q = c_o n^2 p$. Note that $|\sum_{i=1}^{n} a_i\alpha_i \pmod{p}| = p\lceil \sum_{i=1}^{n} a_i\alpha'_i \rfloor$, so if $\sum a_i\alpha_i$is not equal to $0 \pmod{p}$, then $\lceil \sum_{i=1}^{n} a_i\alpha'_i \rfloor \geq 1/p$, so (5.6) is satisfied ; so we have by theorem (5.5), that for all integers $\beta_1, \beta_2, \dots \beta_n$, there exist integers $t, p_1, p_2, \dots p_n$ so that $|t\alpha'_i - p_i - \beta_i/p| \leq \epsilon$ which implies that $|t\alpha_i - \beta_i \pmod{p}| \leq \epsilon p$ completing the proof. If $\sum a_i\alpha_i \equiv 0 \pmod{p}$, then, we have by the hypothesis of the current theorem, $\epsilon \sum |a_i| \geq c_o n^2$ whence again (5.6) is satisfied and hence its conclusion which implies the conclusion of the current theorem.

To prove the second part of the theorem, assume that for all integers $\beta_1, \beta_2, \dots \beta_n$, there exists an integer t satisfying (5.10). Let $a_1, a_2, \dots a_n$ be arbitrary integers not all zero such that $\sum a_i\alpha_i \equiv 0 \pmod{p}$ and choose β 's so that $\sum a_i\beta_i \equiv (p-1)/2 \pmod{p}$. Let t satisfy (5.10). Then, we have $(p-1)/2 = |-\sum a_i\beta_i \pmod{p}| = |(\sum a_i t\alpha_i - \sum a_i\beta_i) \pmod{p}| \leq p\epsilon \sum |a_i|$ from which the theorem follows.

∎

Acknowledgments: This research was done while both authors were visiting the Institut für Operations Research, Universität Bonn, School of Operations Research, Cornell University and the Mathematical Sciences

Institute, University of California, Berkeley. We thank the institutions for their hospitality. We thank Herb Scarf, Éva Tardos and Bill Cook for helpful discussions.

References

W.Blaschke, *Über Affine Geometrie VII: Neue Extremeigenschaften von Ellipse und Ellipsoid*, Leipziger Ber. 69, pp 306-318 (1917).

J.Bourgain and V.D.Milman, *Sections euclidiennes et volume des corps symetriques convexes dans* $\mathbf{R}^n$, C.R.Acad. Sc. Paris, t. 300, Série I,n 13, pp 435-438 (1985).

J.W.S.Cassels, *An introduction to the geometry of numbers* Springer Verlag (1971).

J.W.S.Cassels, *An introduction to diophantine approximation*, Cambridge University Press, Cambridge Tracts in Mathematics and Mathematical Physics , No.45, (1957).

P.M.Gruber and C.G.Lekkerkerker, *Geometry of Numbers*, 2nd edition, North Holland , Amsterdam–New York (1987).

J.Hastad, *A good dual vector*, to appear in Combinatorica (1987).

J.Hastad, private communication (1986).

R.Kannan, *Minkowski's Convex body theorem and integer programming*, Mathematics of Operations Research, Volume 12, Number 3, (1987) pp415-440

C.J.Hurkens, *Blowing up a convex body in two dimensions*, manuscript (1987)

N.Karmarkar, *A new polynomial time algorithm for linear programming*, Combinatorica 4, pp 373-396 (1984).

A. Khintchine, *A quantitative formulation of Kronecker's theory of approximation*, Izv. Akad. Nauk. SSSR, Ser. Mat. 12, pp 113-122 (1948) (In Russian).

A.Korkine and G.Zolotarev, *Sur les formes quadratiques*, Math. Annalen 6, pp 366-389 (1873).

J.Lagarias, H.W.Lenstra and C.P.Schnorr, *Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal lattice*, to appear in Combinatorica (1987).

A.K.Lenstra, H.W.Lenstra and L.Lovász, *Factoring polynomials with rational coefficients* Mathematische Annalen 261, pp 513-534 (1982).

H.W.Lenstra, *Integer programming with a fixed number of variables*, Mathematics of Operations research, Volume 8, pp 538-548 (1983).

L.Lovász, *An algorithmic theory of numbers, graphs and convexity*, NSF-CBMS Regional Conference Series 50, SIAM (1986).

K.Mahler, *On lattice points in polar reciprocal domains*, Proc. Kon. Ned. Wet. 51 pp 482-485 (=Indag. Math. 10, pp 176-179) (1948).

J.Milnor and D.Husemoller, *Symmetric bilinear forms* Springer-Verlag, Berlin (1973).

L.A.Santaló, *Un invariente afin para los cuerpos convexos de espacios de n dimensiones* , Portugal Math. 8 (1949) pp 155-161.