CONVEX BODIES WITH FEW FACES

KEITH BALL AND ALAIN PAJOR

(Communicated by William J. Davis)

ABSTRACT. It is proved that if $u_1, \ldots, u_n$ are vectors in $\mathbb{R}^k$, $k \leq n$, $1 \leq p < \infty$ and

$$r = \left( \frac{1}{k} \sum_{i=1}^{n} |u_i|^p \right)^{1/p}$$

then the volume of the symmetric convex body whose boundary functionals are $\pm u_1, \ldots, \pm u_n$, is bounded from below as

$$\left| \{ x \in \mathbb{R}^k : \langle x, u_i \rangle \leq 1 \text{ for every } i \} \right|^k \geq 1/\sqrt{pr}.$$  

An application to number theory is stated.

0. INTRODUCTION

In [V], Vaaler proved that if $Q_n = [-\frac{1}{2}, \frac{1}{2}]^n$ is the central unit cube in $\mathbb{R}^n$ and $U$ is a subspace of $\mathbb{R}^n$ then the volume $|U \cap Q_n|$, of the section of $Q_n$ by $U$ is at least 1. This result may be reformulated as follows: if $u_1, \ldots, u_n$ are vectors in $\mathbb{R}^k$, $1 \leq k \leq n$ whose Euclidean lengths satisfy $\sum_{i=1}^{n} |u_i|^2 \leq k$ then

$$\left| \{ x \in \mathbb{R}^k : \langle x, u_i \rangle \leq 1 \text{ for every } i \} \right|^k \geq 2.$$  

A related theorem, (Theorem 1, below) in which the condition $\sum_{i} |u_i|^2 \leq k$ is replaced by $\max_i |u_i| \leq 1$ was proved by Carl and Pajor [CP] and Gluskin [G]. Gluskin’s methods enable him to obtain sharp results in limiting cases which in turn have applications in harmonic analysis. Results closely related to Theorem 1 were also obtained by Bárány and Füredi [BF] and Bourgain, Lindenstrauss and Milman [BLM].

Theorem 1. There is a constant $\delta > 0$ so that if $u_1, \ldots, u_n \in \mathbb{R}^k$, $1 \leq k \leq n$ are vectors of length at most 1 then

$$\left| \{ x \in \mathbb{R}^k : \langle x, u_i \rangle \leq 1 \text{ for every } i \} \right|^k \geq \delta/\sqrt{1 + \log(n/k)}.$$  

The estimate is best possible if $n$ is at most exponential in $k$, apart from the value of the constant $\delta$. This is demonstrated by an example which had
appeared some time earlier in a paper of Figiel and Johnson [FJ]. Theorem 1
gives a lower bound on the volume ratios of the unit balls of $k$-dimensional
subspaces of $l_\infty^n$ and hence on the distance of these subspaces from Euclidean
space.

Regarding Theorem 1 as a $p = \infty$ version of Vaaler’s $p = 2$ result, Kashin
asked whether a similar result holds for $2 < p < \infty$. This question is answered
in the affirmative by the following theorem.

**Theorem 2.** Suppose $u_1, \ldots, u_n \in \mathbb{R}^k$ with $k \leq n$, $1 \leq p < \infty$ and let

$$r = \left( \frac{1}{k} \sum_{i=1}^{n} |u_i|^p \right)^{1/p}.$$  

Then

$$|\{x \in \mathbb{R}^k: |\langle x, u_i \rangle| \leq 1 \text{ for every } i\}|^{1/k} \geq \begin{cases} 2^{2/\sqrt{p}r} & \text{if } p \geq 2 \\ 1/r & \text{if } 1 \leq p \leq 2. \end{cases}$$

The lower bound is best possible (up to a constant) provided $e^p k \leq n \leq e^k$.

**Remark.** The slightly stronger result for $p \geq 2$ is isolated since for $p = 2$ it
gives back exactly Vaaler’s result.

Theorem 1 follows immediately from Theorem 2 by a standard optimization
argument. If $(u_i)_{i=1}^n$ in $\mathbb{R}^k$ all have norm at most 1 then for any $p \in [1, \infty),$  

$$\left( \frac{1}{k} \sum_{i=1}^{n} |u_i|^p \right)^{1/p} \leq \left( \frac{n}{k} \right)^{1/p}$$

so that

$$|\{x: |\langle x, u_i \rangle| \leq 1 \text{ for every } i\}|^{1/k} \geq 2^{2/\sqrt{p}r} \left( \frac{n}{k} \right)^{1/p}$$

(for $p \geq 2$) and the latter is at least $2/\sqrt{e} \sqrt{1 + \log(n/k)}$ when $p = 2(1 + \log(n/k))$.

With the careful use of well-known methods for estimating the entropy of
convex bodies it is possible to obtain more general (but less precise) estimates
than that provided by Theorem 2; (see [BP]). The purpose of this paper is to
provide a very short proof of Theorem 2, and a fortiori, Theorem 1.

Vaaler originally proved his theorem because of its applications to the ge-
ometry of numbers. The last section of this paper includes a statement of the
generalization of Siegel’s lemma which follows from Theorem 2.

1. THE LOWER BOUND

The proof of Theorem 2 makes use of the following result from [MeP] which
was designed to extend Vaaler’s theorem in a different direction: it estimates
the volumes of sections of the unit balls of the spaces \( l_p^n \), \( 1 \leq p \leq \infty \). For \( 1 \leq p \leq \infty \), \( n \in \mathbb{N} \) let

\[
  B_p^n = \left\{ x \in \mathbb{R}^n : \sum_{i=1}^n |x_i|^p \leq 1 \right\}
\]

be the unit ball of \( l_p^n \).

**Theorem 3.** Let \( U \) be a \( k \)-dimensional subspace of \( \mathbb{R}^n \); if \( 1 \leq p < q < \infty \) then

\[
  \frac{|B_p^n \cap U|}{|B_p^n|} \leq \frac{|B_q^n \cap U|}{|B_q^n|}. \quad \square
\]

**Remark.** The case \( p = 2 \), \( q = \infty \) is Vaaler’s theorem since then, the left side is 1 and the inequality states that

\[
  |B_\infty^n \cap U| \geq |B_\infty^k| \geq 2^k.
\]

For notational convenience, the proof of Theorem 2 is divided into several short lemmas. The first is no more than a convenient form of Hölder's inequality. For \( k \in \mathbb{N} \), \( S^{k-1} \) will denote the Euclidean sphere in \( \mathbb{R}^k \) and \( \sigma = \sigma_{k-1} \), the rotationally invariant probability measure on \( S^{k-1} \). Also let \( v_k \) be the volume of the Euclidean unit ball in \( \mathbb{R}^k \).

**Lemma 4.** Let \( C \) and \( B \) be symmetric convex bodies in \( \mathbb{R}^k \) with Minkowski gauges \( \| \cdot \|_C \) and \( \| \cdot \|_B \), respectively. Then for \( p > 0 \)

\[
  \left( \frac{|C|}{|B|} \right)^{1/k} \geq \left( \frac{k + p}{k|B|} \int_B \|x\|_C^p \, dx \right)^{-1/p}.
\]

**Proof.**

\[
  \left( \frac{|C|}{|B|} \right)^{1/k} = \left( \frac{v_k}{|B|} \int_{S^{k-1}} \|\theta\|_C^{-k} \, d\sigma(\theta) \right)^{1/k} \\
  = \left( \frac{k v_k}{|B|} \int_{S^{k-1}} \left( \frac{\|\theta\|_B}{\|\theta\|_C} \right)^k \int_0^{\|\theta\|_B^{-1}} r^{k-1} \, dr \, d\sigma(\theta) \right)^{1/k} \\
  = \left( \frac{1}{|B|} \int_B \left( \frac{\|x\|_B}{\|x\|_C} \right)^k \, dx \right)^{1/k} \\
  \geq \left( \frac{1}{|B|} \int_B \left( \frac{\|x\|_B}{\|x\|_C} \right)^{-p} \, dx \right)^{-1/p} \\
  = \left( \frac{k + p}{k|B|} \int_B \|x\|_C^p \, dx \right)^{-1/p}. \quad \square
\]

(Lemma 4 appears in [MiP] as Corollary 2.2.)
Lemma 5. Suppose \( u_1, \ldots, u_n \in \mathbb{R}^k \) with \( k \leq n \) and \( 1 \leq p < \infty \). Then

\[
\left| \{ x \in \mathbb{R}^k : |\langle x, u_i \rangle| \leq 1 \text{ for every } i \} \right|^{1/k} \geq 2 \left( \frac{k + p}{k} \sum_{i=1}^{n} \frac{1}{|B^k_p|} \int_{B^k_p} |\langle x, u_i \rangle|^p \, dx \right)^{-1/p}.
\]

Proof. Define \( T : \mathbb{R}^k \to \mathbb{R}^n \) by \( (Tx)_i = \langle x, u_i \rangle, \ 1 \leq i \leq n \) and let \( U = T(\mathbb{R}^k) \). The problem is to estimate from below

\[
|T^{-1}(B^n_\infty)|^{1/k} = |T^{-1}(U \cap B^n_\infty)|^{1/k}.
\]

By Theorem 3,

\[
|U \cap B^n_\infty|^{1/k} \geq 2 \left( \frac{|U \cap B^n_\infty|}{|B^n_\infty|} \right)^{1/k}
\]

and so

\[
|T^{-1}(B^n_\infty)|^{1/k} \geq 2 \left( \frac{|T^{-1}(B^n_\infty)|}{|B^n_\infty|} \right)^{1/k}.
\]

Regard \( T \) as an operator: \( l^k_p \to l^n_p \). Then by Lemma 4,

\[
2 \left( \frac{|T^{-1}(B^n_\infty)|}{|B^n_\infty|} \right)^{1/k} \geq 2 \left( \frac{k + p}{k} \sum_{i=1}^{n} \frac{1}{|B^k_p|} \int_{B^k_p} \|Tx\|^p \, dx \right)^{-1/p}
\]

\[
= 2 \left( \frac{k + p}{k} \sum_{i=1}^{n} \frac{1}{|B^k_p|} \int_{B^k_p} |\langle x, u_i \rangle|^p \, dx \right)^{-1/p}.
\]

Proofof Theorem 2. Let \( (u_i)_1^n \) and \( p \) be as above. For each \( i \) let \( v_i \) be the unit vector in the direction of \( u_i \). By Lemma 5,

\[
\left| \{ x \in \mathbb{R}^k : |\langle x, u_i \rangle| \leq 1 \text{ for every } i \} \right|^{1/k} \geq 2 \left( \frac{k + p}{k} \sum_{i=1}^{n} \frac{1}{|B^k_p|} \int_{B^k_p} |\langle x, u_i \rangle|^p \, dx \right)^{-1/p}
\]

\[
= 2 \left( \frac{k + p}{k} \sum_{i=1}^{n} |u_i|^p \cdot \frac{1}{|B^k_p|} \int_{B^k_p} |\langle x, v_i \rangle|^p \, dx \right)^{-1/p}
\]

\[
\geq 2 \left( \frac{1}{k} \sum_{i=1}^{n} |u_i|^p \right)^{-1/p} \min \left( \frac{k + p}{|B^k_p|} \int_{B^k_p} |\langle x, v \rangle|^p \, dx \right)^{-1/p}
\]

where the minimum is taken over all vectors \( v \) of Euclidean length 1. So to complete the proof it suffices to show that for such a vector \( v \),

\[
\left( \frac{k + p}{|B^k_p|} \int_{B^k_p} |\langle x, v \rangle|^p \, dx \right)^{1/p} \leq \left\{ \begin{array}{ll}
\sqrt{p/2} & \text{if } p \geq 2 \\
2 & \text{if } 1 \leq p < 2
\end{array} \right.
\]
Let $(x^{(j)})_{j=1}^k$ and $(v^{(j)})_{j=1}^k$ be the coordinates of the vectors $x$ and $v$ in $\mathbb{R}^k$. For $p \geq 2$, observe that the functions $(x^{(j)} v^{(j)})$ on $B_p^k$ form a conditionally symmetric sequence, so by Khintchine's inequality and Hölder's inequality (for $\sum_1^n v^{(j)} = 1$),

\[
\left( \frac{k + p}{|B_p^k|} \int_{B_p^k} \left| \sum_{j=1}^k x^{(j)} v^{(j)} \right|^p \, dx \right)^{1/p} \\
\leq \sqrt{\frac{p}{2}} \left( \frac{k + p}{|B_p^k|} \int_{B_p^k} \left( \sum_{j=1}^k x^{(j)2} v^{(j)2} \right)^{p/2} \, dx \right)^{1/p} \\
\leq \sqrt{\frac{p}{2}} \left( \frac{k + p}{|B_p^k|} \int_{B_p^k} \sum_{j=1}^n |x^{(j)}|^p v^{(j)2} \, dx \right)^{1/p} \\
= \sqrt{\frac{p}{2}} \left( \frac{k + p}{|B_p^k|} \int_{B_p^k} |x^{(1)}|^p \, dx \right)^{1/p} \\
= \sqrt{\frac{p}{2}}.
\]

For $1 \leq p < 2$ it is easily checked that

\[
\left( \frac{k + p}{|B_p^k|} \int_{B_p^k} |\langle x, v \rangle|^p \, dx \right)^{1/p} \\
\leq (k + p)^{1/p} \left( \frac{1}{|B_p^k|} \int_{B_p^k} |x, v|^2 \, dx \right)^{1/2} \\
= (k + p)^{1/p} \left( \frac{1}{|B_p^k|} \int_{B_p^k} |x^{(1)}|^2 \, dx \right)^{1/2}
\]

and the last expression can be (rather roughly) estimated by 2 using standard inequalities involving logarithmically concave functions. \(\square\)

**Remark.** The proof of Theorem 2 can be simplified even further if the integration over $B_p^k$ is replaced by integration over $S^{k-1}$ (and Hölder's inequality applied here). The proof was presented as above because Lemma 5 has some intrinsic interest: for example it may be used to recover Gluskin's precise estimate as follows. Suppose $m \in \mathbb{N}$ and the vectors $(z_i)_{i=1}^m \in \mathbb{R}^k$ satisfy

\[
|z_i| \leq (\log(1 + m/k))^{-1/2}, \quad 1 \leq i \leq m.
\]

For $\varepsilon > 0$, let $W(\varepsilon)$ be the set

\[
\left\{ x \in \mathbb{R}^k : \max_j |x^{(j)}| \leq 1, \max_i |\langle x, z_i \rangle| \leq \frac{1}{\varepsilon} \right\}.
\]
that is, \( W(\varepsilon) \) is the intersection of the cube \( B^k_\infty \) with \( m \) “bands” of width at most \((2/\varepsilon)\sqrt{\log(1 + m/k)}\). Then \( |W(\varepsilon)|^{1/k} \to 2 \) as \( \varepsilon \to 0 \), uniformly in \( k \) and \( m \). To see this, apply Lemma 5 with \( n = k + m \), the first \( k \), \( u_i \)'s being the standard basis vectors \( \mathbf{R}^k \) and the remaining \( m \) being the vectors \((\varepsilon z_i)_1^m\).

If \( e_j \) is a standard basis vector,

\[
\frac{k + p}{|B^k_p|} \int_{B^k_p} |(x, e_j)|^p \, dx = 1
\]

and so Lemma 5 (and the proof of Theorem 2) show that for each \( p \geq 2 \),

\[
|W(\varepsilon)|^{1/k} \geq 2(1 + m/k(p/2)^{p/2} \varepsilon^p (\log(1 + m/k))^{-p/2})^{-1/p}
\]

and the latter is at least \( 2/(1 + \sqrt{2} \cdot \varepsilon) \) if \( p = \max(2, 2\log(1 + m/k)) \). \( \square \)

As was briefly mentioned earlier, more general estimates than that of Theorem 2 are obtained in [BP] (for entropy numbers instead of volumes). It is worth noting however that even the argument of Theorem 2 can be used to give the following: there is a constant \( c \) so that if \( u_1, \ldots, u_n \in \mathbf{R}^k \), \( k \leq n \) and \( T: l^k_2 \to l^n_\infty \) is given by \((Tx)_i = (u_i, x)\), \( 1 \leq i \leq n \), then the \( k \)th entropy number of \( T \) satisfies

\[
e_k(T) \leq \frac{c\sqrt[p]{p}}{\sqrt[k]{k}} \left( \frac{1}{k} \sum_{i=1}^n |u_i|^p \right)^{1/p} \left( 1 + \log \frac{n}{k} \right)^{1/p}
\]

and hence

\[
e_k(T) \leq \frac{cc}{\sqrt[k]{k}} \sqrt{1 + \log \frac{n}{k}} \cdot ||T||
\]

(taking \( p = 2(1 + \log(n/k)) \)). To obtain this, one uses Schütt’s estimates [S] for the entropy numbers of the formal identity from \( l^n_p \) to \( l^n_\infty \) in place of the result of Meyer and Pajor, an the dual Sudakov inequality of Pajor and Tomczak, [PT] in place of the application of Hölder’s inequality.

2. AN APPLICATION TO LINEAR FORMS

As stated in the Introduction, Vaaler’s original result has applications to the geometry of numbers. One such, a sharpened form of Siegel’s lemma, is given in [BV]. Using the arguments of Bombieri and Vaaler and Theorem 2, one can obtain the generalization of their result, contained in Theorem 6, below. Some notation is needed. If \( A \) is a \( k \times n \) matrix of reals with independent rows \( (1 \leq k \leq n) \), denote by \( v_j = v_j(A) \), \( 1 \leq j \leq k \), the rows of \( A \). Let \( (e_i)_1^n \) be the standard basis of \( \mathbf{R}^n \) and denote by \( c_i \), the distance (in the Euclidean norm) of \( e_i \) from the span of the \( v_j \)'s in \( \mathbf{R}^n \). (So if \( A_i \) is the matrix with \( k + 1 \) rows, \( v_1, \ldots, v_n, e_i \), then

\[
c_i^2 = \frac{\det(A_i A_i^*)}{\det(A A^*)} \text{ for } 1 \leq i \leq n.
\]
Theorem 6. Let $A$ be a $k \times n$ matrix with rank $k$ and integral entries. With the notation above, the system $Ax = 0$ admits $n - k$ linearly independent solutions

$$z^{(r)} = (z_1^{(r)}, \ldots, z_n^{(r)}) \in \mathbb{Z}^n, \quad 1 \leq r \leq n - k$$

so that for every $p \geq 2$,

$$\prod_{1 \leq r \leq n-k} \max_i |z_i^{(r)}| \leq D^{-1} \sqrt{\frac{p}{2}} \left( \frac{1}{n-k} \sum_{i=1}^{n} c_i^p \right)^{1/p} \sqrt{\det AA^T}$$

where $D$ denotes the $G-C-D$ of all $k \times k$ determinants extracted from $A$.

Remark. The principal importance of such a generalization of Bombieri and Vaaler’s result is that it takes into account, more strongly, the form of the matrix $A$. If the $c_i$’s are all about the same size, then for $p > 2$, the expression

$$\left( \frac{1}{n-k} \sum c_i^p \right)^{1/p}$$

is small compared with the corresponding expression in which $p$ is replaced by 2.

References


DEPARTMENT OF MATHEMATICS, TEXAS A & M UNIVERSITY, COLLEGE STATION, TEXAS 77843

U. E. R. DE MATHEMATIQUES, UNIVERSITÉ DE PARIS VII, 2 PLACE JUSSIEU, 75251 PARIS CEDEX 05, FRANCE