Irregularities of distribution IX* 

by

WOLFGANG M. SCHMIDT (Boulder, Colo.)

Yu. V. Linnik in memoriam

1. Introduction. Let $U^k$ be the $k$-dimensional unit cube $0 \leq x_1 \leq 1$, $\ldots$, $0 \leq x_k \leq 1$, and let $p_1, p_2, \ldots, p_N$ be points in $U^k$. There are many ways to measure the "irregularity" of the distribution of these $N$ points.

Given a Lebesgue measurable subset $A$ of $U^k$ with measure $\mu(A)$, write $\varepsilon(A)$ for the number of the given $N$ points which lie in $A$, and put

$$D(A) = \varepsilon(A) - N\mu(A).$$

If $\mathfrak{M}$ is a non-empty class of measurable sets in $U^k$, write

$$D(\mathfrak{M}) = \sup \{D(A)\},$$

where the supremum is over all $A \in \mathfrak{M}$. Further put

$$A(\mathfrak{M}) = D(\mathfrak{M})/N.$$

One could call $A(\mathfrak{M})$ the discrepancy with respect to $\mathfrak{M}$ of the given $N$ points. It is clear that $0 \leq A(\mathfrak{M}) \leq 1$.

By a box we shall understand a set of the type $a_1 \leq x_1 \leq b_1$, \ldots, $a_k \leq x_k \leq b_k$. Let $\mathfrak{B}$ be the class of boxes in $U^k$, $\mathfrak{C}$ the class of closed cubes in $U^k$ with sides parallel to the coordinate axes, $\mathfrak{G}$ the class of closed balls in $U^k$, and $\mathfrak{C}$ the class of convex subsets of $U^k$.

It is known that $A(\mathfrak{B}) \geq c_1(k)N^{-1}(\log N)^{(k-1)/2}$ (K.F. Roth [4]), that $A(\mathfrak{C}) \geq c_2N^{-1}\log N$ if $k = 2$ (W. M. Schmidt [6]), that $A(\mathfrak{C}) \geq c_2(k, e)N^{(e-1)/2(e+1)-1-e}$ for $e > 0$ (W. M. Schmidt [5], Corollary to Theorem 3A), and that $A(\mathfrak{B}) \geq c_3(k)N^{-(k+1)/2k}$ (S. K. Zaremba [9]). We shall improve the last one of these estimates:

**Theorem 1.** $A(\mathfrak{B}) \geq c_4(k)N^{-2(k+1)}$.

* Written with partial support from NSF grant NSF-6002X. The paper may be read independently of the preceding papers of this series.
Since $\mathcal{A} \subseteq \mathcal{B}'$ implies $A(\mathcal{A}) \subseteq A(\mathcal{B}')$, we have

$$A(\mathcal{B}) \subseteq A(\mathcal{A}) \subseteq A(\mathcal{B}).$$

On the other hand, according to E. Hlawka [2] (see also [1]), we have

1. $A(\mathcal{B}) \leq c(k) A(\mathcal{B})^{1/k}$,
2. $A(\mathcal{B}) \leq c(k) A(\mathcal{B})^{1/(k-1)}$,
3. $A(\mathcal{B}) \leq c(k) \log A(\mathcal{B})^{1/k}$.

A wide generalization of (1) was given by R. Mück and W. Philipp [3].

It was shown by S. K. Zaremba [9] that the exponent $1/k$ in (1) is best possible.

J. W. S. Cassels (unpublished) showed that $A(\mathcal{B}) \leq c(\mathcal{B}) A(\mathcal{B})^{1/(k+3)}$,

and C.J. Smyth [7] generalized this to

4. $A(\mathcal{B}) \leq c(k) A(\mathcal{B})^{1/(k-1)}$,

which is an improvement over (3). He also showed [8] that

$$A(\mathcal{B}) \leq c(\mathcal{B}) A(\mathcal{B})^{1/(k+3)} \left(1 + \log A(\mathcal{B})^{1/k}\right).$$

We shall improve (2) and (4). Write $\exp x = e^x$.

**Theorem 2.**

$$A(\mathcal{B}) \leq c(k) A(\mathcal{B})^{1/k}.$$

**Theorem 3.**

$$A(\mathcal{B}) \leq c(k) A(\mathcal{B})^{1/k} \exp \left[2 \log 2 \right]^{1/k} A(\mathcal{B})^{1/k}.$$

In particular, it follows that

$$A(\mathcal{B}) \leq c(k, \varepsilon) A(\mathcal{B})^{1/k} - \varepsilon$$

for $\varepsilon > 0$.

**2. Proof of Theorem 1.** We may suppose $k > 1$. Let $B$ be the ball of radius $\frac{1}{2}$ contained in $U^k$, and let $S$ be the surface of $B$. Let $C$ be a closed spherical cap on $S$ with spherical radius $\varepsilon$. (With the radius normalized such that a half sphere has radius $\pi/2$.) The convex hull $U$ of $C$ is a solid spherical cap. For $0 < \varepsilon < \pi/2$, $\mu(C)$ is a continuous function of $\varepsilon$ with

$$\mu(C) = \frac{1}{2N}.$$

If $N$ is sufficiently large, there is a number $\varepsilon_0$ such that a cap $C$ of spherical radius $\varepsilon_0$ has

$$\mu(C) = e^{-k}.  \quad (i = 1, \ldots, k).$$

We start the numbering of constants $c_1, c_2, \ldots$ anew in each section, except in the last one. These constants may depend on the dimension $k$.  

In view of (5), $0 < \varepsilon_0 < c_N N^{-1/k}$. We now pick as many pairwise disjoint caps with radius $\varepsilon_0$ as possible; say $C_1, \ldots, C_M$. For large $N$ and hence small $\varepsilon_0$, we have $M \geq c_2 N^{1/k}$, whence

$$M \geq c_2 N^{1/k}.  \quad (6)$$

Given a sequence of numbers $\sigma_1, \ldots, \sigma_M$, with each $\sigma_i$ either $-1$ or $1$, let $B(\sigma_1, \ldots, \sigma_M)$ consist of all $x \in B$ which do not lie in a cap $C_i$ with $\sigma_i = -1$. In other words, $B(\sigma_1, \ldots, \sigma_M)$ is obtained from $B$ by removing the solid caps $C_i$ for which $\sigma_i = -1$.

Now the function $D(A)$ is additive, i.e. it satisfies

$$D(A \cup A') = D(A) + D(A').$$

If $A \cap A' = \emptyset$. It follows easily that

$$D(B(\sigma_1, \ldots, \sigma_M)) - D(B(-\sigma_1, \ldots, -\sigma_M)) = \sum_{i=1}^M \sigma_i D(C_i).$$

We have

$$D(C_i) = \varepsilon(C_i) - N_M(C_i) = \varepsilon(C_i) - 0.$$

Hence for every $i$, either $D(C_i) > 0$ or $D(C_i) < -1$. Choose $\sigma_i$ such that $\sigma_i D(C_i) > 0$ ($1 \leq i \leq M$). Then

$$D(B(\sigma_1, \ldots, \sigma_M)) = D(B(-\sigma_1, \ldots, -\sigma_M))$$

and $A = B(\sigma_1, \ldots, \sigma_M)$ or $A = B(-\sigma_1, \ldots, -\sigma_M)$ has $|D(A)| < 1/2 M$.

Thus by (6),

$$A(\mathcal{B}) \geq \frac{1}{2} M/N \geq c_2 N^{-1/k}{N^b+1}.$$
Pick as many pairwise disjoint sets \( Q(x) \) as possible; say \( Q_1, \ldots, Q_M \). Clearly \( M \geq c_1 \delta^{-\theta + 1} \), whence
\[
M \geq c_1 N^{(k-1)/2}.
\]
For any sequence \( \sigma_1, \ldots, \sigma_M \) of +1 and -1 signs, let \( Q(\sigma_1, \ldots, \sigma_M) \) be the union of \( Q \) with the "blister" \( Q_i \) for which \( \sigma_i = 1 \). The set \( Q(\sigma_1, \ldots, \sigma_M) \) belongs to \( \mathcal{D} \). We have
\[
D(Q(\sigma_1, \ldots, \sigma_M)) - D(Q(-\sigma_1, \ldots, -\sigma_M)) = \sum_{i=1}^{M} c_i D(Q_i).
\]
By an argument used in the proof of Theorem 1, we obtain a set \( A \in \mathcal{D} \) with
\[
|D(A)|/N \geq \frac{1}{2} M/N \geq c_2 N^{-1/2}.
\]

3. Proof of Theorem 2. Let \( B(\sigma, \varrho) \) be the closed ball with center \( \sigma \) and radius \( \varrho \). Given a subset \( S \) of \( U^k \), let \( S(\varrho) \) consist of points \( x \) for which \( B(x, \varrho) \subseteq S \). Let \( S' \) consist of \( x \in U^k \) which are not in \( S \).

For each \( \varrho > 0 \), let \( \mathcal{E}(\varrho) \) be the class of subsets \( S \) of \( U^k \) having
\[
\mu(S(\varrho)) \geq \mu(S) - \varrho \sigma, \quad \mu(S'(\varrho)) \geq \mu(S') - \varrho \sigma
\]
for every \( \varrho > 0 \).

**Lemma 1.** There is a constant \( c_1 = c_1(k) \) such that
\[
\mathcal{D} \subseteq \mathcal{E}(c_1).
\]

The proof may be left to the reader. Incidentally, it may be shown that \( \mathcal{D} \subseteq \mathcal{E}(c_1) \). It is now clear that Theorem 2 is a consequence of Theorem 2a.

\[
\mathcal{D} \subseteq \mathcal{E}(c_1) \mathcal{D}(\mathbb{B})^{1/2}.
\]

Proof. Let \( S(\varrho) \) consist of points \( x \in U^k \) which have a distance \( < \varrho \) from the boundary of \( S \). Every \( x \in S(\varrho) \) is either in \( S \) but not in \( S(\varrho) \), or is in \( S \) but not in \( S'(\varrho) \). Hence for \( S \notin \mathcal{E}(\varrho) \),
\[
\mu(S(\varrho)) \leq 2\varrho \sigma.
\]

Now if \( k = 1 \) and if \( x_1, \ldots, x_M \) are on the boundary of \( S \) and in the interior of \( U \), then for small \( \varrho \), \( S(\varrho) \) contains the \( M \) open intervals with centers \( x_1, \ldots, x_M \) and of length \( \varrho \). Hence for small \( \varrho \), \( \mu(S(\varrho)) \geq 2\varrho M \), and we get \( M \leq \varrho \). Thus \( S \) has at most \( \sigma + 2 \) boundary points, and is therefore the union a bounded number of points and intervals. Hence Theorem 2a is true for \( k = 1 \).

We may henceforth assume that \( k > 1 \). Pick a point \( \sigma = (a_1, \ldots, a_k) \) such that for each of the given points \( p_i \) \( i = 1, \ldots, N \), each coordinate of \( p_i - \sigma \) is irrational. For a positive integer \( n \), let \( \mathbb{B}(n) \) be the class of cubes
\[
a_i + \frac{u_i}{n} \leq a_i \leq a_i + \frac{u_i + 1}{n} \quad (i = 1, \ldots, k)
\]
with integers \( u_1, \ldots, u_k \). Let \( \mathbb{B}(n) \) be the set of cubes of \( \mathbb{B}(n) \) which are contained in \( S \). Since a cube of \( \mathbb{B}(n) \) has diameter \( k^{1/2} \), it follows that the cubes of \( \mathbb{B}(n) \) cover \( S(k^{1/2}/n) \), and their number \( \nu(n) \) satisfies
\[
\nu(n) \geq n^k \mu(S(k^{1/2}/n)) \geq n^k \mu(S) - n^{k-1} \sigma k^{1/2}.
\]

For each positive integer \( t \), the union of the cubes of \( \mathbb{B}(n) \) contains the union of the cubes of \( \mathbb{B}(2^{t-1}) \). Put \( \mathbb{B}_t = \mathbb{B}(2^t) \), and for \( t \geq 2 \), let \( \mathbb{B}_t \) consist of the cubes of \( \mathbb{B}(2^t) \) which are not contained in a cube of \( \mathbb{B}(2^{t-1}) \).

If \( n = \nu(2) \), then \( n = \nu(2) \), and for \( t \geq 2 \) we have
\[
2^{-2k} \nu_t + 2^{-k-2t} \nu(2^t) \leq \mu(S),
\]
whence by (9),
\[
\nu_t \leq 2^k \mu(S) - 2^k \nu(2^t) \leq \sigma k^{1/2} 2^{(k-1)/2} n^{k-1}.
\]

Since any two distinct cubes in any of the sets \( \mathbb{B}_t \) are disjoint except possibly for their boundaries, and since by our choice of \( \sigma \) none of the given \( N \) points lie on such a boundary, we have for every positive integer \( M \),
\[
x(S) \geq M \sum_{x \in \mathbb{B}_t} \mu(W) \geq M \sum_{x \in \mathbb{B}_t} (N \mu(W) - N \Delta(W))
\geq M \left( \sum_{x \in \mathbb{B}_t} \mu(W) \right) - M \Delta(W)
\geq M \left( \mu(S) - N c_0(k, \sigma) \left( 2^k + \sigma k^{1/2} \sum_{t=1}^{M} 2^{(k-1)/2} \right) \right)
\geq M \mu(S) - N c_0(k, \sigma) \left( 2^k + \sigma k^{1/2} M^{(k-1)/2} \right),
\]
since \( k > 1 \). Now if we choose \( M \) such that \( 2^M - 1 \geq \Delta(W) \geq 2^M \), then
\[
x(S) - N \mu(S) \geq - N c_0(k, \sigma) \Delta(W) 2^M 2^{(k-1)/2} \right) = -N c_0(k, \sigma) \Delta(W) 2^M 2^{(k-1)/2}.
\]
This inequality remains true if we replace \( S \) by \( S' \). Hence
\[
x(S) - N \mu(S) \leq N c_0(k, \sigma) \Delta(W) 2^M 2^{(k-1)/2},
\]
and Theorem 2a follows.

4. Successive sweeping. Given a set \( A \), let \( rA + y \) be the set of points \( ra + y \) with \( a \in A \). Let \( \mathcal{A}(A) \) be the class of sets \( rA + y \) with \( r > 0 \) which are contained in \( U^k \). In view of Lemma 1, Theorem 3 is a consequence of
THEOREM 3a. Suppose $A \in \mathcal{S}(\tau)$ for some $\tau$, and suppose $\mu(A) > 0$. Then for every $\sigma > 0$, $A |_{\mathcal{S}(\sigma)} \leq c_1(\sigma) A \delta(\delta(A))^{\log 2} \exp \left[ 2(\log 2)^{1/2} - 1 \right] \log \delta(A)^{1/2} \right]$. Denote the distance of points $x, y$ by $|x - y|$. Now let $r_1, r_2, \ldots$ be positive real with 

$$r_{i+1} \leq \frac{1}{2} r_{i}, \quad (i = 1, 2, \ldots),$$

and set $s_i = k^i r_0$. The set $r_1 \mathcal{A}$ has diameter $\leq s_1$. For a set $S$, let $\chi(S|x)$ be the characteristic function of $S$. Let $S$ be a set belonging to $\mathcal{S}(\sigma)$. We are going to construct functions $f_i(x), g_i(x), h_i(x) (i = 0, 1, 2, \ldots).$ We begin by setting $f_0(x) = 0$. If a continuous function $f_i(x)$ is given, write

$$g_i(x) = \chi(S|x) - f_i(x),$$

$$h_i(x) = \min_{|x - y| \leq r_{i+1}} g_i(y),$$

$$f_{i+1}(x) = f_i(x) + \mu(r_{i+1} A) \cdot \frac{1}{2} \int \chi(r_{i+1} A + y|x) h_i(y) dy.$$  

LEMMA 2. We have

(i) $0 \leq f_{v+2} - \leq \chi(S|x)$

(ii) $|f_i(x) - f_i(x')| \leq c_1(\sigma) r_1 |x - x'|$;

(iii) $f_i(x) = 1$ if $x \in S(2a_i)$ ($i = 1, 2, \ldots)$;

(iv) $f_i(x) \geq 1 - 2^{-i} c_1(\sigma) (s_i/\sigma)$

Our construction may be interpreted as follows. We first sweep $S$ with a broom of the size and shape of $r_1 \mathcal{A}$. We can sweep the middle of $S$, more precisely $S(2a_1)$, very well. But we cannot sweep the border areas of $S$ very well. We then take a smaller broom of the size and shape of $r_2 \mathcal{A}$. And so on. We obtain a better and better sweeping of $S$ which is expressed by (i) and (ii). But it would have been inefficient to sweep right away with a very small broom of the size and shape of $r_1 \mathcal{A}$.

Proof. We proceed by induction on $v$. Assume that either $v = 0$ or that the lemma is true for a particular value of $v > 0$. We have $0 \leq f_v(x) \leq \chi(S|x)$, whence $0 \leq g_v(x) \leq \chi(S|x)$. Now if $x \in r_{v+1} A + y$, then

$$d(x) = \sum_{i=1}^{v} d_i(x) \leq s_{v+1},$$

whence $h_v(x) = g_v(x)$. We obtain

$$0 \leq \int \chi(r_{v+1} A + y|x) h_v(y) dy \leq g_v(x) \int \chi(r_{v+1} A + y|x) dy = g_v(x) \mu(r_{v+1} A),$$

and

$$f_v(x) \leq f_{v+2}(x) \leq f_v(x) + g_v(x) = \chi(S|x).$$

Hence (i) is true for $v = 1$. Now it is clear that $L_0(\mathcal{A}) = f_1(x) \leq f_v(x)$ has

$$L_0(x) - L_0(x') = (\mu(r_{v+1} A))^{-1} \int \chi(r_{v+1} A + y|x) - \chi(r_{v+1} A + y|x') h_v(y) dy.$$}

Since $0 \leq h_v(y) \leq 1$, we obtain

$$L_0(x) - L_0(x') \leq (\mu(r_{v+1} A))^{-1} \mu(C_1),$$

where $C_1$ consists of $y$ for which $-y$ lies in $r_{v+1} A - x$ but not in $r_{v+1} A - x'$. Now

$$\mu(C_1) \leq r_{v+1}(\mu(C_1),$$

where $C_2$ consists of $y$ which are in $A - r_{v+1} (x - x')$ but not in $A$. Now if $y \in C_2$ lies in $A - r_{v+1} (x - x')$, then $y \in A'$ and $y \in A' (r_{v+1} A - x - x')$. Hence by virtue of $A \in \mathcal{S}(\tau)$, the intersection $C_2 \cap U_k$ has volume $\leq r_{v+1} (x - x')$. On the other hand if $y \in C_2$ lies outside of $U_k$, then it has distance $\leq r_{v+1} (x - x')$ from $U_k$, and if $r_{v+1} (x - x') \leq 1$, then the part of $C_2$ outside $U_k$ has volume $\leq r_{v+1} (x - x')$. Thus if $|x - x'|$ is small, then $\mu(C_2) \leq (\tau + 3\delta) r_{v+1} (x - x')$, and therefore

$$L_0(x) - L_0(x') \leq \frac{2}{c_1(\sigma)} r_{v+1} (x - x'),$$

with $c_2(\sigma) = 2 \mu(\mathcal{A}) \tau (\tau + 3\delta)^2$. It follows that for every $x, x'$,

$$L_0(x) - L_0(x') \leq \frac{2}{c_1(\sigma)} r_{v+1} (x - x').$$

Now if $v = 0$, we have $f_0(x) = f_1(x) = l_0(x)$, and the case $v = 1$ of (iia) follows. If $v > 0$, we use our inductive assumption, (10), (11) and the relation $f_{v+1}(x) = f_v(x) + l_{v+1}(x)$ to obtain

$$|f_{v+1}(x) - f_v(x)| \leq \frac{c_1(\sigma) r_{v+1} + c_1(\sigma) r_{v+1}^a |x - x'|}{c_1(\sigma) r_{v+1}^a |x - x'|} \leq c_1(\sigma) r_{v+1}^a |x - x'|.$$

Thus (iia) is true for $v = 1$. Therefore
Before taking up the proof of (ib) we observe the following. Suppose that either
\[ i = r \quad \text{and} \quad x, x' \in S(s_{i+1}), \]

or that
\[ 1 \leq i \leq r - 1, \quad |x - x'| \leq s_i, \quad \text{and} \quad x, x' \in S(3s_{i+1} + \ldots + s_i + s_{i+1}). \]

Now \( h_i(x) \) equals \( g_i(x) \) for some \( w \) with \( |w - z| \leq s_{i+1} \). Since \( h_i(x') \) is defined as the minimum of \( g_i(x') \) for \( |w - z| \leq s_{i+1} \), and since \( w = w' + z - z \) has \( |w - z'| \leq s_{i+1} \), we get \( h_i(x') \leq g_i(x') \), whence
\[ h_i(x') - h_i(x) \leq g_i(x') - g_i(x). \]

Our hypotheses on \( x, x' \) imply that \( w, w' \in S \), whence \( \chi(S | w') = \chi(S | w) = 1 \) and
\[ g_i(x') - g_i(x) = f_i(x') - f_i(x). \]

Now if (12) holds, apply (iia) to \( w, w' \). On the other hand, if (13) holds, then \( |w - w'| = |z - z'| \leq s_i \), and \( w, w' \in S(3s_{i+1} + \ldots + s_i) \). In this case we apply (iiib) to \( w, w' \). We may do so, since (ib) is true for our particular value of \( \nu \) by induction. In either case, we get
\[ |f_i(x') - f_i(x)| \leq 2^{i-1} c_i(A) r_i^{-1} |x - x'|. \]

Combining this with (14) and (15), we may conclude that both (12) or (13) implies
\[ |h_i(x') - h_i(x)| \leq 2^{i-1} c_i(A) r_i^{-1} |x - x'|. \]

Now suppose that \( 1 \leq i \leq r \), that \( |x - x'| \leq s_{i+1} \) and that \( x, x' \in S(3s_{i+1} + \ldots + s_{r+1}) \). We have
\[ l_{i+1}(x) - l_{i+1}(x') = (u(r_{i+1}A) - 1) \int \chi(r_{i+1}A + y | x') h_i(y + x - x') dy. \]

The integrand is zero unless \( |y - x'| \leq s_{i+1} \), hence is zero unless \( y \in S(3s_{i+1} + \ldots + s_{r+1}) \). But then \( y + x - x' \in S(3s_{i+1} + \ldots + s_{i} + s_{i+1}) \). We apply the remark made above above \( z = y, x' = y + x - x' \), and we obtain
\[ |h_i(y + x - x') - h_i(y)| \leq 2^{i-1} c_i(A) r_i^{-1} |x - x'|. \]

Hence
\[ |l_{i+1}(x) - l_{i+1}(x')| \leq 2^{i-1} c_i(A) r_i^{-1} |x - x'|. \]

Since \( f_{i+1}(x) = f_i(x) + l_{i+1}(x) \) and since
\[ |f_{i}(x) - f_{i}(x')| \leq 2^{i-1} c_i(A) r_i^{-1} |x - x'| \]

by induction, we obtain
\[ |f_{i+1}(x) - f_{i+1}(x')| \leq 2^{i-1} c_i(A) r_i^{-1} |x - x'|. \]

Thus (ib) is true for \( r + 1 \).

We have
\[ f_i(x) = \mu(r_iA)^{-1} \int \chi(r_iA + y | x) h_i(y) dy. \]

If \( x \in S(2s_i) \) and if \( x \in r_iA + y \), then \( |y - x| \leq s_i \) and \( y \in S(s_i) \). Since \( g_i \) is the characteristic function of \( S \), the definition of \( h_i(y) \) implies that \( h_i(y) = 1 \) for \( y \in S(s_i) \). Therefore \( x \in S(2s_i) \) implies that \( f_i(x) = 1 \). Since \( f_i(x) \leq f_i(x') \leq 1 \) by (i), we obtain (iia).

There remains (iiib). Suppose \( 1 \leq i \leq r \) and \( x \in S(3s_{i+1} + \ldots + s_{i+1}) \).

We have
\[ f_{i+1}(x) = (u(r_{i+1}A) - 1) \int \chi(r_{i+1}A + y | x) f_i(x) + h_i(y) dy. \]

Here \( h_i(y) = g_i(y) \) for some \( w \) with \( |w - y| \leq s_{i+1} \). In particular, if \( x \in r_{i+1}A + y \), we have \( |y - x| \leq s_{i+1} \), whence \( |x - w| \leq 2s_{i+1} \). In particular \( w \in S \), so that \( g_i(w) = 1 - f_i(w) \) and
\[ f_i(x) + h_i(y) = 1 + f_i(x) - f_i(w). \]

Now either \( i = r \); then we estimate \( f_i(x) - f_i(w) \) by (iia). Or \( i \leq r - 1 \), \( |w - x| \leq 2s_{i+1} \leq s_i \), and both \( x, w \in S(3s_{i+1} + \ldots + s_i) \). Then we estimate \( f_i(x) - f_i(w) \) by (iib). In either case we get
\[ |f_i(x) - f_i(w)| \leq 2^{i-1} c_i(A) r_i^{-1} |x - w| \leq 2^{i-1} c_i(A) (2s_{i+1} r_i) \]
\[ = 2^{i-1} c_i(A) (s_{i+1} r_i), \]
say. Thus every \( y \) with \( x \in r_{i+1}A + y \) has
\[ f_i(x) + h_i(y) \geq 1 - 2^{i-1} c_i(A) (s_{i+1} r_i), \]
and (16) yields
\[ f_{i+1}(x) \geq 1 - 2^{i-1} c_i(A) (s_{i+1} r_i). \]

Since \( S(3s_{i+1}) \subseteq S(3s_{i+1} + \ldots + s_{i+1}) \) by (10), the lemma is proved.

5. A measure on the space \( \mathfrak{Q}(A) \). Let \( r_1, r_2, \ldots, s_1, s_2, \ldots \) be as in § 4. Let \( M \) be an integer greater than 1.

The space \( \Omega = \mathfrak{Q}(A) \) of sets \( rA + y \) in \( V^k \) may be parametrized by the pair \( (r, y) \). We introduce a measure \( \omega \) on \( \Omega \) by the formula
\[ \int \omega(r, y) d\omega = \sum_{i=0}^{M-1} \chi(r, y) h_i(y) dy. \]

This formula is valid for functions \( \omega(r, y) \) on \( \Omega \) for which the integrals on the right are defined.
Lemma 3. We have

(i) \[ \int_B \chi(rA + y|x) \, d\omega \leq \chi(S|x), \]

(ii) \[ \int_B d\omega \leq c(A, \sigma)(r_1^{-2} + 2r_2^{-2}r_1 + \ldots + 2^{M-1}r_M^{-2}r_{M-1}), \]

(iii) \[ \int_B \mu(rA) \, d\omega \geq \mu(S) - 2^M c(A, \sigma) r_M. \]

Proof. We begin by observing that

\[ \int_B \chi(rA + y|x) \, d\omega = \sum_{r_{1,1}} (\mu(r_{1,1}A))^{-1} \int_{r_{1,1}A + y|x} \chi(y) \, dy \]

\[ = \sum_{r_{1,1}} \int_{r_{1,1}A} f_M(x) \leq \chi(S|x). \]

Next,

\[ \int_B d\omega = \sum_{r_{1,1}} (\mu(r_{1,1}A))^{-1} \int_{r_{1,1}A} g_s(y) \, dy \]

We have

\[ \int g_s(y) \, dy = \int \chi(S|y) \, dy = \mu(S). \]

For \( v \geq 1 \) we write

\[ \int g_s(y) \, dy = \int_{S_1} + \int_{S_2} + \ldots + \int_{S_v} + \int_{S_v^c}, \]

where \( S_1 = S(6s^v) \), where \( S_j \) is the complement of \( S(6s^j) \) in \( S(6s^j) \) (\( j = 2, 3, \ldots \)), and where \( S_v^c \) is the complement of \( S(6s^v) \) in \( S \). By (iia) of Lemma 2, \( g_s(y) = 0 \) for \( x \notin S_j \), so that the integral over \( S_v^c \) is zero. By (iiib) of Lemma 2 we have

\[ g_s(y) \leq 2^{v-1} \, c(A)(s/v), \]

if \( y \in S_j \), with \( 2 \leq j \leq v \). On the other hand we have \( \mu(S_j) \leq 6s_{j-1} \sigma \), because \( S_j \in \mathcal{S} \). Thus for \( 2 \leq j \leq v \),

\[ g_s(y) \, dy \leq 6c(A)(s/v) \, 2^{v-1} \, dy. \]

On \( S_v^c \), we have \( g_s(y) \leq 1 \), and since \( \mu(S_v^c) \leq 6s_v \sigma \), the integral over \( S_v^c \) is \( \leq 6s_v \sigma \). Combining our estimates, we obtain

\[ \int g_s(y) \, dy \leq \sigma (1 + c(A))s_v(2^{v-1} + 2^{v-2} + \ldots + 1) \leq c(A, \sigma) 2^v r_v. \]

In view of (17) and (18) we obtain part (ii) of the lemma.

Finally,

\[ \int h_s(y) \, dy = (\mu(r_{1,1}A))^{-1} \int \chi(r_{1,1}A + y|x) h_s(y) \, dx \, dy = \int l_{r_{1,1}}(x) \, dx. \]

Thus

\[ \int \mu(rA) \, d\omega = \int \int h_s(y) \, dy = \sum_{r_{1,1}} \int l_{r_{1,1}}(x) \, dx \]

\[ = \int f_M(x) \, dx = \mu(S) - \int g_M(x) \, dx \geq \mu(S) - 2^M c(A, \sigma) r_M \]

by (19).

6. Proof of Theorem 3a. We may assume that \( A = A(\mathcal{S}(A)) \) is so small that

\[ |\log \mathcal{A}|(\log 2) \geq 9k^3. \]

Repeated application of Lemma 3 yields

\[ \int \mu(rA) \, d\omega = \int_{\mathcal{S}(A)} \chi(S|\mathcal{S}(A)) \, d\omega \geq \int (\sum_{r_{1,1}} \chi(r_{1,1}A + y|\mathcal{S}(A))) \, d\omega \]

\[ \geq \int (N \mu(rA) - N A(\mathcal{S}(A))) \, d\omega = N \int (\mu(rA) \, d\omega - A \, d\omega) \]

\[ \geq N(\mu(S) - 2^M c(A, \sigma) r_M - A(\mathcal{S}(A)) R_M) \]

with

\[ R_M = r_1^{-2} + 2r_2^{-2}r_1 + \ldots + 2^{M-1}r_M^{-2}r_{M-1}. \]

Choose the integer \( M \) with

\[ M - 1 \geq |\log A(\mathcal{S}(A))|/\log 2 \geq 9k^3. \]

Then \( M \geq 3 \) by (20). Let \( d \) be the number with

\[ \log d = |\log A(\mathcal{S}(A))|. \]

Now by (20), (22),

\[ |\log A(\mathcal{S}(A))| = |\log A(\mathcal{S}(A))|/|\log 2| \geq |\log A(\mathcal{S}(A))|/|\log 2| \geq 9k^3. \]

so that \( d \geq 2. \)

Put \( r_{i} = d^{-i} \) (\( i = 1, 2, \ldots \)). Then

\[ R_M = d^2 - 2d^{2-1} + \ldots + 2^{M-1}d^{2(M-1)} \leq 2M d^{M(k+1)}, \]

so that

\[ 2^M r_M + M R_M \leq (2/d)M(1 + A d^{M(k+1)}) = 2(2/d)^M. \]
by our choice of \( \delta \). We have
\[
M(\log d - \log 2) = \frac{M}{(Mk+1)} \log d - M \log 2 \\
\geq \log d/[\log(1/k) - (1/k^2M)] - M \log 2 \\
\geq (1/k) \log d - (2/k) \log d^{1/k} (\log d)^{1/k} - \log 2
\]
by (22), so that by (23),
\[
2^M \tau_d \leq d^{1/k} \exp\left(2(\log 2)^{1/k} - \log d^{1/k}\right).
\]
This in conjunction with (21) gives
\[
2^S \geq N_{[0]}(S) - \tau(S, A, c) d^{1/k} \exp\left(2(\log 2)^{1/k} - \log d^{1/k}\right).
\]
The same inequality holds with \( S \) replaced by \( S' \). Both inequalities together yield
\[
2^S \leq N_{[0]}(S) \leq N_{[0]}(S, A, c) d^{1/k} \exp\left(2(\log 2)^{1/k} - \log d^{1/k}\right).
\]
Since this holds for every \( S \in \mathbb{S}(\sigma) \), Theorem 3 is proved.

References


UNIVERSITY OF COLORADO

Received on 6.12.1973 (601)