ON A LEMMA OF LITTLEWOOD AND OFFORD

P. ERDÖS

Recently Littlewood and Offord[1] proved the following lemma: Let $x_1, x_2, \cdots, x_n$ be complex numbers with $|x_i| \geqq 1$. Consider the sums $\sum_{k=1}^{n} \epsilon_k x_k$, where the ϵ_k are ± 1. Then the number of the sums $\sum_{k=1}^{n} \epsilon_k x_k$ which fall into a circle of radius r is not greater than

$$cr2^n(\log n)n^{-1/2}.$$

In the present paper we are going to improve this to

$$cr2^n n^{-1/2}.$$

The case $x_i = 1$ shows that the result is best possible as far as the order is concerned.

First we prove the following theorem.

THEOREM 1. *Let $x_1, x_2, \cdots, x_n$ be n real numbers, $|x_i| \geqq 1$. Then the number of sums $\sum_{k=1}^{n} \epsilon_k x_k$ which fall in the interior of an arbitrary interval I of length 2 does not exceed $C_{n,m}$ where $m = [n/2]$. ($[x]$ denotes the integral part of x.)*

Remark. Choose $x_i = 1$, n even. Then the interval $(-1, +1)$ contains $C_{n,m}$ sums $\sum_{k=1}^{n} \epsilon_k x_k$, which shows that our theorem is best possible.

We clearly can assume that all the x_i are not less than 1. To every sum $\sum_{k=1}^{n} \epsilon_k x_k$ we associate a subset of the integers from 1 to n as follows: k belongs to the subset if and only if $\epsilon_k = +1$. If two sums $\sum_{k=1}^{n} \epsilon_k x_k$ and $\sum_{k=1}^{n} \epsilon_k' x_k$ are both in I, neither of the corresponding subsets can contain the other, for otherwise their difference would clearly be not less than 2. Now a theorem of Sperner[2] states that in any collection of subsets of n elements such that of every pair of subsets neither contains the other, the number of sets is not greater than $C_{n,m}$, and this completes the proof.

An analogous theorem probably holds if the x_i are complex numbers, or perhaps even vectors in Hilbert space (possibly even in a Banach space). Thus we can formulate the following conjecture.

CONJECTURE. *Let $x_1, x_2, \cdots, x_n$ be n vectors in Hilbert space $\|x_i\| \geqq 1$. Then the number of sums $\sum_{k=1}^{n} \epsilon_k x_k$ which fall in the interior of an arbitrary sphere of radius 1 does not exceed $C_{n,m}$.*

Received by the editors March 28, 1945.

[1] Rec. Math. (Mat. Sbornik) N.S. vol. 12 (1943) pp. 277–285.

[2] Math. Zeit. vol. 27 (1928) pp. 544–548.

At present we can not prove this, in fact we can not even prove that the number of sums falling in the interior of any sphere of radius 1 is $o(2^n)$.

From Theorem 1 we immediately obtain the following corollary.

COROLLARY. *Let r be any integer. Then the number of sums $\sum_{k=1}^n \epsilon_k x_k$ which fall in the interior of any interval of length $2r$ is less than $rC_{n,m}$.*

THEOREM 2. *Let the x_i be complex numbers, $|x_i| \geqq 1$. Then the number of sums $\sum_{k=1}^n \epsilon_k x_k$ which fall in the interior of an arbitrary circle of radius r (r integer) is less than*

$$crC_{n,m} < c_1 r 2^n n^{-1/2}.$$

We can clearly assume that at least half of the x_i have real parts not less than 1/2. Let us denote them by $x_1, x_2, \cdots, x_t$, $t \geqq n/2$. In the sums $\sum_{k=1}^n \epsilon_k x_k$ we fix $\epsilon_{t+1}, \cdots, \epsilon_n$. Thus we get 2^t sums. Since we fixed $\epsilon_{t+1}, \cdots, \epsilon_n$, $\sum_{k=1}^t \epsilon_k x_k$ has to fall in the interior of a circle of radius r. But then $\sum_{k=1}^t \epsilon_k R(x_k)$ has to fall in the interior of an interval of length $2r$ ($R(x)$ denotes the real part of x). But by the corollary the number of these sums is less than

$$crC_{t,[t/2]} < c_1 r 2^t / t^{1/2}.$$

Thus the total number of sums which fall in the interior of a circle of radius r is less than

$$c_2 r 2^n / n^{1/2},$$

which completes the proof.

Our corollary to Theorem 1 is not best possible. We prove:

THEOREM 3. *Let r be any integer, the x_i real, $|x_i| \geqq 1$. Then the number of sums $\sum_{k=1}^n \epsilon_k x_k$ which fall into the interior of any interval of length $2r$ is not greater than the sum of the r greatest binomial coefficients (belonging to n).*

Clearly by choosing $x_i = 1$ we see that this theorem is best possible.

The same argument as used in Theorem 1 shows that Theorem 3 will be an immediate consequence of the following theorem.

THEOREM 4. *Let $A_1, A_2, \cdots, A_u$ be subsets of n elements such that no two subsets A_i and A_j satisfy $A_i \supset A_j$ and $A_i - A_j$ contains more than $r-1$ elements. Then u is not greater than the sum of the r largest binomial coefficients.*

Let us assume for sake of simplicity that $n = 2m$ is even and $r = 2j+1$ is odd. Then we have to prove that

$$u \leqq \sum_{i=-j}^{+j} C_{2m,n+i}.$$

Our proof will be very similar to that of Sperner.[2] Let $A_1, A_2, \cdots, A_u$ be a set of subsets which have the required property and for which u is maximal. It will suffice to show that in every A the number of elements is between $n-j$ and $n+j$. Suppose this were not so, then by replacing if need be each A by its complement we can assume that there exist A's having less than $n-j$ elements. Consider the A's with fewest elements; let the number of their elements be $n-j-y$ and let there be x A's with this property. Denote these A's by $A_1, A_2, \cdots A_x$. To each A_i, $i=1, 2, \cdots, x$, add in all possible ways r elements from the $n+j+y$ elements not contained in A. We clearly can do this in $C_{n+j+y,r}$ ways. Thus we obtain the sets $B_1, B_2, \cdots$, each having $n+j-y+1$ elements. Clearly each set can occur at most $C_{n+j-y+1,r}$ times among the B's. Thus the number of different B's is not less than

$$xC_{n+j+y,r}(C_{n+j-y+1,r})^{-1} > x.$$

Hence if we replace $A_1, A_2, \cdots, A_x$ by the B's and leave the other A's unchanged we get a system of sets which clearly satisfies our conditions (the B's contain $n+j-y+1$ elements and all the A's now contain more than $n-j-y$ elements, thus $B-A$ can not contain more than $r-1$ elements and also $B \not\subset A$) and has more than u elements, this contradiction completes our proof.

By more complicated arguments we can prove the following theorem.

THEOREM 5. *Let $A_1, A_2, \cdots, A_u$ be subsets of n elements such that there does not exist a sequence of $r+1$ A's each containing the previous one. Then u is not greater than the sum of the r largest binomial coefficients.*

As in Theorem 4 assume that $n=2m$, $r=2j+1$, and that there are x A's with fewest elements, and the number of their elements is $n-j-y$. We now define a graph as follows: The vertices of our graph are the subsets containing z elements, $n-j-y \leqq z \leqq n+j+y$. Two vertices are connected if and only if one vertex represents a set containing z elements, the other a set containing $z+1$ elements, and the latter set contains the former. Next we prove the following lemma.

LEMMA. *There exist $C_{2n,n-j-y}$ disjoint paths connecting the vertices containing $n-j-y$ elements to the vertices containing $n+j+y$ elements.*

Our lemma will be an easy consequence of the following theorem of Menger:[8] *Let G be any graph, V_1 and V_2 two disjoint sets of its vertices. Assume that the minimum number of points needed for the separation of V_1 and V_2 is w. Then there exist w disjoint paths connecting V_1 and V_2. (A set of points w is said to separate V_1 and V_2, if any path connecting V_1 with V_2 passes through a point of w.)*

Hence the proof of our lemma will be completed if we can show that the vertices V_1 containing $n-j-y$ elements can not be separated from the vertices V_2 containing $n+j+y$ elements by less than $C_{2n,n-j-y}$ vertices. A simple computation shows that V_1 and V_2 are connected by

$$C_{2n,n-j-y}(n + j + y)(n + j + y - 1) \cdots (n - j - y + 1)$$

paths. Let z be any vertex containing $n+i$ elements, $-j-y \leq i \leq j+y$. A simple calculation shows the the number of paths connecting V_1 and V_2 which go through z equals

$$(n+i)(n+i-1) \cdots (n-j-y+1)(n-i)(n-i-1) \cdots (n-j-y+1)$$
$$\leq (n+j+y)(n+j+y-1) \cdots (n-j-y+1).$$

Thus we immediately obtain that V_1 and V_2 can not be separated by less than $C_{2n,n-j-y}$ vertices, and this completes the proof of our lemma.

Let now $A_1^{(1)}, A_2^{(1)}, \cdots, A_x^{(1)}$ be the A's containing $n-j-y$ elements. By our lemma there exist sets $A_i^{(l)}$, $i=1, 2, \cdots, x$; $l=1, 2, \cdots, 2j+2y+1$, such that $A_i^{(2j+2y+1)}$ has $n+j+y$ elements and $A_i^{(l)} \subset A_i^{(l+1)}$ and all the A's are different. Clearly not all the sets $A_i^{(l)}$, $l=1, 2, \cdots, 2j+2y+1$, can occur among the $A_1, A_2, \cdots, A_u$. Let $A_i^{(s)}$ be the first A which does not occur there. Evidently $s \leq r$. Omit $A_i^{(1)}$ and replace it by $A_i^{(s)}$. Then we get a new system of sets having also u elements which clearly satisfies our conditions, and where the sets containing fewest elements have more than $n-j-y$ elements and the sets containing most elements have not more than $n+j+y$ elements. By repeating the same process we eventually get a system of A's for which the number of elements is between $n-j$ and $n+j$. This shows that

$$u \leq \sum_{i=-j}^{+j} C_{2n,n+i},$$

which completes the proof.

One more remark about our conjecture: Perhaps it would be easier to prove it in the following stronger form: Let $|x_i| \geq 1$, then the num-

[8] See, for example, D. König, *Theorie der endlichen und unendlichen Graphen*, p. 244.

ber of sums $\sum_{k=1}^{n}\epsilon_k x_k$ which fall in the interior of a circle of radius 1 plus one half the number of sums falling on the circumference of the circle is not greater than $C_{n,m}$. If the x_i are real it is quite easy to prove this.

We state one more conjecture.

(1). Let $|x_i|=1$. Then the number of sums $\sum_{k=1}^{n}\epsilon_k x_k$ with $|\sum_{k=1}^{n}\epsilon_k x_k|\leqq 1$ is greater than $c2^n n^{-1}$, c an absolute constant.

UNIVERSITY OF MICHIGAN