Proof of a conjecture of Offord

Paul Erdös

Mathematical Institute of the Hungarian Academy of Sciences, Real tanoda U. 13–15, Budapest V

(MS received 8 July 1977. Revised MS received 12 November 1979)

Synopsis

If $z_1, z_2 \ldots z_n$ are complex numbers satisfying $|z_i - z_j| \geqq 1$ for all i, j then the number of the 2^n sums $\sum_1^n \varepsilon_i z_i$, where $\varepsilon_i = \pm 1$, which lie in any circle of radius r cannot exceed $\alpha_r 2^n / n^{3/2}$ where α_r depends only on r.

Offord told me the following conjecture (for earlier references see [**1, 3, 4**]). Let $z_1, \ldots, z_n$ be n complex numbers satisfying

$$\min_{1 \leqq i < j \leqq n} |z_i - z_j| \geqq 1. \tag{1}$$

Consider the 2^n sums

$$\sum_{i=1}^{n} \varepsilon_i z_i, \quad \varepsilon_i = \pm 1.$$

But before stating our results it is convenient to define the random sums explicitly. The Radamacher functions are periodic functions of period 1 defined as follows

$$r_1(t) = \begin{cases} +1 & 0 \leqq t < \frac{1}{2} \\ -1 & \frac{1}{2} \leqq t < 1 \end{cases}$$

$$r_n(t) = r_1(2^n t).$$

So if we set $\varepsilon_n = r_n(t)$ we obtain automatically a sequence of plus and minus signs. These can equally be determined by expanding the number t in the binary scale and if the ith place is 1 we put $\varepsilon_i = 1$, if zero $\varepsilon_i = -1$. The above sum can now be written as

$$\sum_{i=1}^{n} r_i(t) z_i \tag{2}$$

Let C_r be any circle of radius r. Then the number of sums (2) which are in C_r is less than

$$\alpha_r 2^n / n^{\frac{3}{2}} \tag{3}$$

where α_r is a constant which depends only on r. We are going to prove this conjecture in a slightly sharper form. The proof will be very similar to a proof of Sárközy and Szemerédi [**5**].

I have just learnt that some time ago, Halász independently proved similar and in some sense more general results [**2**]. Put $z_i = i$, $1 \leqq i \leqq n$. It is easy to see (by the central limit theorem) that there are $c_1 2^n/n^{\frac{3}{2}}$ sums (2) which are equal, also it is easy to see that the interval of length r and centre $\frac{1}{2}\binom{n+1}{2}$, contains $c_2 r 2^n/n^{\frac{3}{2}}$ sums of the form (2) [**2**]. I conjecture that this example is essentially best possible, i.e. I conjecture $\alpha_r < c_3 r$. More precisely denote by $f(C_r; z_1, \ldots, z_n)$ the number of sums (2) which are in the interior of C_r. Define

$$F(n; r) = \max f(C_r; z_1, \ldots, z_n)$$

where the maximum is extended over all circles of radius r and all $\{z_i\}$ satisfying (1). I first of all prove the following:

THEOREM 1. *If* $r \geqq \frac{1}{2}$

$$F(n; r) < 10^5 r^2 2^n/n^{\frac{3}{2}}.$$

As stated before, I conjecture that in Theorem 1 $10^5 r^2$ can be replaced by $c_3 r$. Perhaps the maximum $R(n; r)$ is obtained if $z_i = i$ and the centre of C_r is $\frac{1}{2}\binom{n+1}{2}$ [**2**]. The constant 10^5 in our Theorem could be greatly reduced but since I cannot obtain the best possible result I do not try.

It is easy to see that every C_r can be covered by fewer than $100\, r^2$ circles of radius $\frac{1}{2}$. Thus to prove our Theorem we only have to prove

$$F(n; \tfrac{1}{2}) < 10^3 2^n/n^{\frac{3}{2}}. \tag{4}$$

We clearly can assume without loss of generality that at least half the z's are in the first quadrant. We can also assume, for convenience, and again without loss of generality, that there are an even number of these z's satisfying

$$1 \leqq |z_1| \leqq |z_2| \leqq \ldots \leqq |z_{2m}| \; m \geqq n/4. \tag{5}$$

If (4) does not hold then there is a circle $C_{\frac{1}{2}}$ so that at least

$$10^3 2^{2m}/n^{\frac{3}{2}} > 2.10^2 2^{2m}/(2m)^{\frac{3}{2}} \tag{6}$$

sums $s(t) = \sum_{i=1}^{2m} r_i(t) z_i$ are in $C_{\frac{1}{2}}$ (we of course obtain $C_{\frac{1}{2}}$ by translating out $C_{\frac{1}{2}}$ by $-\sum_{i=1}^{n-2m} r_{2m+i}\, z_{2m+i}$).

Now consider the sums

$$\sigma(t, k) = s(t) - r_k(t) z^k.$$

Each such sum is determined by a sequence $\{\eta_i\}$ where

$$\eta_i = \begin{cases} r_i(t) & i < k \\ r_{i+1}(t) & i \geqq k. \end{cases}$$

We shall show that all these sums are distinct. Let $\sigma(t_1, k_1)$ and $\sigma(t_2, k_2)$ be any two sums. First if $k_1 = k_2 = k$ and $r_k(t_1) = r_k(t_2)$, then clearly $s(t_1)$ and $s(t_2)$ must be distinct in the sense that they are derived from different sequences $\{\eta_i\}$ (although they could have the same complex values). Unless both these conditions are satisfied we show that $\sigma(t_1, k_1)$ and $\sigma(t_2, k_2)$ have different complex values and thus come from different sequences $\{\eta_i\}$. Since by hypothesis the sums $s(t_1)$ and $s(t_2)$ lie in the same $C_{\frac{1}{2}}$

$$|\sigma(t_1, k_1)-\sigma(t_2, k_2)|>|r_{k_1}(t_1)z_{k_1}-r_{k_2}(t_2)z_{k_2}|\geqslant 1.$$

Now if $k_1=k_2$ the first term in the second member is $2|z_k|\geqq 2$ since $r_k(t_1)\neq r_k(t_2)$ and if $k_1\neq k_2$ then it exceeds $|z_{k_1}-z_{k_2}|$ or $|z_{k_1}+z_{k_2}|$ as the case may be. The first is not less than 1 by (1) and the second because all the z's are in the first quadrant. This completes the proof that the two sums $\sigma(k_1, t_1)$ and $\sigma(k_2t_2)$ are distinct.

Consider the sums

$$s(t)-r_k(t)z_k=\sum_{\substack{i=1\\ i\neq k}}^{2m} r_i(t)z_i \quad k\leqq m \tag{7}$$

$$|z_1|\leqq|z_2|\leqq \dots \leqq|z_m|\leqq \dots \leqq|z_{2m}|.$$

The number of sums (7) is by (6) greater than $10^2 2^{2m}/m^{\frac{1}{2}}$. There are at least $10^2 2^m/m^{\frac{1}{2}}$ of these sums which coincide in their first m summands. If we write

$$A=\{r_i(t);\, r_i(t)=1,\, m+1\leqq i\leqq 2m\}$$

then A is a subset of a set of size m, and as we have just shown there are $10^2 2^m/m^{\frac{1}{2}}$ distinct subsets A. Now a theorem of mine states that if we are given a set S of t objects and a family of L subsets of S where L is greater than the sum of the r greatest binomial coefficients $\binom{t}{i}$ $o\leqq i\leqq t$, then there are two of these subsets such that one contains the other and their difference has at least r elements. Now by a simple computation

$$10^2 2^m/m^{\frac{1}{2}}>3\left(\begin{bmatrix} u \\ \left[\frac{u}{2}\right]\end{bmatrix}\right), \quad u=m$$

thus $10^2 2^m/m^{\frac{1}{2}}$ is certainly greater than the sum of the three largest binomial coefficients $\binom{m}{i}$. Thus there are two sums (7) $s_{j_1}-z_1$ and $s_{j_2}-z_2$ which coincide in their first m summands and one of them say $s_{j_1}-z_1$ has at least three extra summands with $\varepsilon_i=+1$. Now since $|s_{j_1}-s_{j_2}|\leqq 1\leqq|z_m|$ we have

$$|(s_{j_1}-z_1)-(s_{j_2}-z_2)|\leqq 3\,|z_m|.$$

On the other hand the extra summands with $\varepsilon_i=+1$ give $(|z_i|\leqq|z_{m/2}|$ for $m\geqq i>\left[\frac{m}{2}\right]$ and the z_i are all in the same quadrant)

$$|(s_{j_1}-z_1)-(s_{j_2}-z_2)\,|\geqq 3\sqrt{2}\,|z_m|$$

an evident contradiction, which proves our Theorem.

The same argument gives that if the z_i are vectors in k dimensional space satisfying (1) then the number of summands (2) in a sphere of radius C_r is less than $c2^k r^{2k} 2^n / m^{\frac{3}{2}}$.

It is not clear to me what happens if the vectors z_i are in Hilbert space. At the moment I cannot even prove that only $o(2^n)$ sums (2) can be in the interior of C_r.

References

1 P. Erdös, On a lemma of Littlewood and Offord, *Bull. Amer. Math. Soc.* **5** (1945), 898–902.
2 G. Halász, Estimates for the concentration function of combinatorical number theory and probability. *Period. Math. Hungar.* **8** (1977), 197–211.
3 J. H. van Lint, Representation of O as $\sum_{k=-N}^{N} \varepsilon_k k$, *Proc. Amer. Math. Soc.* **18** (1967), 182–184.
4 D. K. Kleitman, On a lemma of Littlewood and Offord on the distribution of linear combination of vectors, *Advances in Math.* **5** (1970), 115–117.
5 A. Sárközy and E. Szeméredi, Über ein Problem von Erdös und Moser, *Acta Arithmetica* **11** (1965–66), 205–208.

(*Issued* 27 *June* 1980)