



ADJUSTING A CONJECTURE OF ERDŐS

WALTER CARNIELLI AND PIETRO K. CAROLINO

ABSTRACT. We investigate a conjecture of Paul Erdős, the last unsolved problem among those proposed in his landmark paper [2]. The conjecture states that there exists an absolute constant $C > 0$ such that, if v_1, \dots, v_n are unit vectors in a Hilbert space, then at least $C \frac{2^n}{n}$ of all $\epsilon \in \{-1, 1\}^n$ are such that $|\sum_{i=1}^n \epsilon_i v_i| \leq 1$.

We disprove the conjecture. For Hilbert spaces of dimension $d > 2$, the counterexample is quite strong, and implies that a substantial weakening of the conjecture is necessary. However, for $d = 2$, only a minor modification is necessary, and it seems to us that it remains a hard problem, worthy of Erdős.

We prove some weaker related results that shed some light on the hardness of the problem.

1. INTRODUCTION

In a 1945 paper [2], Paul Erdős improves on an inequality that Littlewood and Offord had formulated in order to deal with the problem of counting real roots of random real polynomials. Stripped of the details of their particular application, the inequality of Littlewood-Offord seeks to answer the following question. Given n complex numbers z_1, \dots, z_n , each of norm greater than 1, consider the 2^n possible sums $\sum_{i=1}^n \epsilon_i z_i$, where each ϵ_i is either -1 or 1 (we refer to these as \pm -sums). What is the largest number of them that can lie on a closed disk of radius 1?

The bound they obtained was of the form $O(2^n \log n / \sqrt{n})$, and it was enough for their purposes. However, the problem is combinatorially interesting in its own right, and Erdős generalized it from complex numbers to vectors in an arbitrary inner product space. His first result was an exact bound of the form $\binom{n}{\lfloor n/2 \rfloor}$ for the dimension $d = 1$ case, which he solved by applying Sperner's theorem on families of subsets of $\{1, \dots, n\}$,

Received by the editors January 11, 2010, and in revised form July 3, 2010.

2000 *Mathematics Subject Classification.* 05A16, 05D40.

Key words and phrases. Erdős conjecture, Littlewood-Offord reverse problem, counterexample.

This research was supported by FAPESP—Fundação de Amparo à Pesquisa do Estado de São Paulo, Thematic Research Project Grant 2004/14107-2. The first author has been also supported by a CNPq (Brazil) Research Grant 300702/2005-1 and the second by a FAPESP Scholarship Grant. A first version of this paper has been published in *CLE e-Prints* at <http://www.cle.unicamp.br/e-prints/>.

none of which is contained in any other. He used this result to establish an $O(2^n/\sqrt{n})$ bound in dimension two, and conjectured that this—in fact, $\binom{n}{\lfloor n/2 \rfloor}$ —is best possible in all dimensions. This conjecture initiated a series of papers by Katona, Kleitman and others; Katona settled the $d = 2$ case in [3] by an ingenious generalization of Sperner’s theorem, and Kleitman solved the general case in [4] by an inductive argument. Somewhat later, Bollobás (cf. [1]) also found a proof for general d . Both of the general proofs work for arbitrary normed spaces, not only inner product spaces.

The question of how many \pm -sums of n vectors can lie in sets of small diameter became known as the Littlewood-Offord problem. The converse question—given that many \pm -sums lie in a set of small diameter, what can be said about the original n vectors—became known as the inverse Littlewood-Offord problem. Techniques devised to deal with both problems still find major applications in combinatorics and random matrix theory (see [5]).

However, Erdős’s paper ends with a conjecture that seems to have received little attention, which we will call the reverse Littlewood-Offord problem (since the other *verse names are taken). The question is as follows. Does there exist an absolute constant $C > 0$ such that, if v_1, \dots, v_n are unit vectors in an inner product space, then at least $C \frac{2^n}{n}$ of all $\epsilon \in \{-1, 1\}^n$ are such that $|\sum_{i=1}^n \epsilon_i v_i| \leq 1$? In asymptotic notation: is the number of \pm -sums lying in the unit ball, centered at the origin, $\Omega(2^n/n)$?

We call attention to the fact that \pm -sums are counted “with multiplicity,” that is, we are interested in how many coefficient assignments $\epsilon \in \{-1, 1\}^n$ make the \pm -sums small. We do not count how many distinct vectors of small norm actually arise as \pm -sums, since it is easy to give examples where that number is just 1 or 2 (e.g. take $v_1 = \dots = v_n$). Thus, throughout the paper, expressions such as “the number of \pm -sums that lie in X ” will always refer to the number of elements $\epsilon \in \{-1, 1\}^n$ such that $\sum_{i=1}^n \epsilon_i v_i$ lies in X .

2. COUNTEREXAMPLES

Our family of counterexamples is remarkably simple in construction. The idea underlying all of them is the following trivial result.

Lemma 1. *If n is odd and $\epsilon_1, \dots, \epsilon_n \in \{-1, 1\}$, then $\epsilon_1 + \dots + \epsilon_n$ is odd, and therefore $|\epsilon_1 + \dots + \epsilon_n| \geq 1$.*

For concreteness, let us work in \mathbb{R}^d with euclidean norm; the arguments are the same for any real Hilbert space of dimension d . Let $\hat{e}_1, \dots, \hat{e}_d$ be vectors in any orthonormal basis, for instance the canonical basis. Let m_1, \dots, m_d be odd numbers, and choose a set of $n = m_1 + \dots + m_d$ unit vectors v_1, \dots, v_n consisting of m_1 copies of \hat{e}_1, m_2 copies of \hat{e}_2, \dots, m_d copies of \hat{e}_d . The next lemma shows that all \pm -sums of the v_i are “far” from the origin.

Lemma 2. *If v_i, \dots, v_n are defined as above, then all their \pm -sums have norm at least \sqrt{d} .*

Proof. Consider the j -th coordinate of an arbitrary \pm -sum $s = \sum_{i=1}^n \epsilon_i v_i$. Only the m_j copies of the vector \widehat{e}_j contribute, and each adds -1 or $+1$. Since each m_j is odd, Lemma 1 says that every coordinate of s has absolute value at least 1. Therefore, the euclidean norm of s is at least \sqrt{d} . \square

From Lemma 2 it follows that, in dimensions $d > 1$, it is possible to find arbitrarily large families of vectors such that *none* of their \pm -sums lie in the unit ball centered at the origin. The counterexample motivates us to reformulate the conjecture as follows: for any n unit vectors in a d -dimensional Hilbert space, the number of their \pm -sums that lie in a ball of radius \sqrt{d} , centered at the origin, is $\Omega(2^n/n)$. However, this conjecture fails dramatically in dimensions $d > 2$, as the next proposition shows.

Proposition 3. *For each dimension $d \geq 1$, there are arbitrarily large n such that it is possible to choose unit vectors $v_1, \dots, v_n \in \mathbb{R}^d$ with the property that only $O(2^n/n^{d/2})$ of their \pm -sums have norm \sqrt{d} , and none have smaller norm.*

Proof. The argument is simply a special case of the construction in Lemma 2, and a quantitative estimate of it. Let m be an odd number, and let $n = dm$. Choose vectors v_1, \dots, v_n from an orthonormal basis as before, but now the same number m of each \widehat{e}_j ; again, no \pm -sum will have norm less than \sqrt{d} . To estimate how many have norm exactly equal to \sqrt{d} we notice that any \pm -sum s such that $|s| = \sqrt{d}$ must have all its coordinates equal to either -1 or 1 . Looking at each coordinate separately, we reduce the problem to estimating how many \pm -sums of m copies of the number 1 yield either -1 or 1 . An easy combinatorial argument shows that exactly $\binom{m}{\lfloor m/2 \rfloor} + \binom{m}{\lceil m/2 \rceil}$ of these sums lie in $\{-1, 1\}$, and Stirling's approximation of the binomial coefficients establishes that this quantity is $O(2^m/\sqrt{m})$. Multiplying this bound for all d coordinates, we obtain that $O(2^{dm}/m^{d/2})$ of the \pm sums of v_1, \dots, v_n have norm \sqrt{d} . Since $2^{dm}/m^{d/2} = d^{d/2} \cdot 2^n/n^{d/2}$ and we regard the dimension as fixed, this gives the $O(2^n/n^{d/2})$ bound claimed. \square

Hence, for $d > 2$, there are a lot less \pm -sums of norm at most \sqrt{d} than $\Omega(2^n/n)$. In fact, a straightforward extension of the quantitative estimate above shows that, for $d > 2$, there is no constant R_d independent of n (but possibly depending on d) such that $\Omega(2^n/n)$ \pm -sums have norm at most R_d . These considerations lead us to make the following adjusted conjecture.

Conjecture 4. *For each integer $d \geq 1$, there is a constant $C_d > 0$ such that, if H is a real Hilbert space of dimension d and v_1, \dots, v_n are unit vectors in H , then at least $C_d \frac{2^n}{n^{d/2}}$ of their \pm -sums have norm at most \sqrt{d} .*

The only case where the estimate $\Omega(2^n/n)$ is preserved is dimension $d = 2$, i.e. the plane. This case already seems hard enough with the new norm bound of \sqrt{d} . A small technical remark may be of interest: in dimension two, the construction in Proposition 3 forces the number n of vectors in a

counterexample to the norm bound of 1 to be even. We do not know whether the 1-bound holds if n is required to be odd.

3. POSITIVE RESULTS

In this section we obtain some results on the distribution of \pm -sums in dimension two, weaker than both Erdős's original conjecture and our own. We do so mainly to illustrate where straightforward attempts fail, and why some new ideas may be needed.

Definition 5. Let H be any real vector space, and $w_1, \dots, w_N \in H$. We define the **average** of the w_i to be the vector $\mu = (w_1 + \dots + w_N)/N$. If H is also an inner product space, define their **variance** σ^2 to be the (usual) average of the numbers $|w_i - \mu|^2$.

The main point of Definition 5 is that it allows us to formulate a version of Chebyshev's inequality in general inner product spaces.

Lemma 6. If w_1, \dots, w_N are vectors in an inner product space, with average μ and variance σ^2 , then, for every $k > 0$, less than N/k^2 of the w_i are at a distance greater than $k\sigma$ from μ .

Proof. Suppose that w_1, \dots, w_M are at a distance greater than $k\sigma$ from μ , where $M \geq N/k^2$; this means that $|w_i - \mu|^2 > k^2\sigma^2$ for N/k^2 of the w_i . Therefore, the average of all $|w_i - \mu|^2$ is greater than $(N/k^2) \cdot (k^2\sigma^2)/N = \sigma^2$, a contradiction. \square

We will apply Lemma 6 to the set of all \pm -sums of n unit vectors; this will be made possible by the fact that the high symmetry of this set of sums makes its average and variance very easy to calculate.

Lemma 7. Let v_1, \dots, v_n be unit vectors in an inner product space H , put $N = 2^n$, and let w_1, \dots, w_N be all \pm -sums of the v_i . Then the average of the w_i is 0, and their variance is n .

Proof. From the definition of \pm -sums it is easy to see that, if w is a \pm -sum of some v_1, \dots, v_n , then so is $-w$. Thus the sum of all \pm -sums is 0, and so is their average.

Therefore the variance of w_1, \dots, w_N is simply the numerical average of $|w_1|^2, \dots, |w_N|^2$, which we calculate as follows:

$$\begin{aligned} \sum_{i=1}^N \langle w_i, w_i \rangle &= \sum_{\epsilon \in \{-1, 1\}^n} \left\langle \sum_{i=1}^n \epsilon_i v_i, \sum_{i=1}^n \epsilon_i v_i \right\rangle \\ &= \sum_{\epsilon \in \{-1, 1\}^n} \sum_{i=1}^n \sum_{j=1}^n \epsilon_i \epsilon_j \langle v_i, v_j \rangle = \sum_{i=1}^n \sum_{j=1}^n \left[\sum_{\epsilon \in \{-1, 1\}^n} \epsilon_i \epsilon_j \langle v_i, v_j \rangle \right]. \end{aligned}$$

Now, for each fixed pair (i, j) there are two possibilities. If $i \neq j$, then summing $\epsilon_i \epsilon_j \langle v_i, v_j \rangle$ over all $\epsilon \in \{-1, 1\}^n$ gives 0: for each i , the map

$r_i : \{-1, 1\}^n \rightarrow \{-1, 1\}^n$, which reverses the sign of the i -th coordinate and leaves the others unchanged, sends $\epsilon_i \epsilon_j \langle v_i, v_j \rangle$ to $-\epsilon_i \epsilon_j \langle v_i, v_j \rangle$, and so all these terms cancel out. If $i = j$, then $\epsilon_i \epsilon_j \langle v_i, v_j \rangle$ reduces to $\epsilon_i^2 |v_i|^2$, which is simply 1; the last sum is then $\sum_{i=1}^n \sum_{\epsilon \in \{-1, 1\}^n} 1 = nN$, and the average of $|w_1|^2, \dots, |w_N|^2$ is n . \square

Now we straightforwardly apply Lemma 6 to the \pm -sums of v_1, \dots, v_n with (say) $k = 2$, and discover that at most $2^n/4$ of these sums have norm at least $2\sqrt{n}$. In other words, at least $3 \cdot 2^n/4$ of the sums have norm less than $2\sqrt{n}$. This shows that, even though the \pm -sum of n unit vectors can in principle have norm as large as n , most of the time there is a substantial amount of “cancellation,” and the norm stays below the much smaller bound of $2\sqrt{n}$.

We can use this concentration effect in a weak version of Conjecture 4.

Proposition 8. *For each integer $d \geq 1$ there exists a constant $C_d > 0$ with the following property. If v_1, \dots, v_n are unit vectors in an inner product space H of dimension d , then there exists a ball of radius \sqrt{d} and center no farther than $2\sqrt{n}$ from the origin, such that at least $C_d \frac{2^n}{n^{d/2}}$ of the \pm -sums of v_1, \dots, v_n lie in it.*

Proof. Let v_1, \dots, v_n be unit vectors in the space H , pick any $\epsilon > 0$, and let B, B_ϵ be balls centered at the origin, with radii $2\sqrt{n}$ and $(2 - \epsilon)\sqrt{n}$, respectively. Another application of Lemma 6 shows that at most $2^n/(2 - \epsilon)^2$ of the \pm -sums of v_1, \dots, v_n lie outside B_ϵ , thus at least $2^n(1 - 1/(2 - \epsilon)^2)$ of them lie in B_ϵ . Divide B into disjoint cubes, with sides of length 2 parallel to the coordinate axes. Since the volume of B is $K_d(2\sqrt{n})^d$ for some constant K_d (depending only on the dimension) and each cube has volume 2^d , then there are at most $K_d(2\sqrt{n})^d/2^d = K_d n^{d/2}$ cubes entirely inside B . For fixed and large enough n , the cubes entirely contained in B will cover B_ϵ , and hence also the \pm -sums that lie in it. It follows that at least one of the cubes, Q , contains at least $C_d \frac{2^n}{n^{d/2}}$ of the sums, for $C_d = (1 - 1/(2 - \epsilon)^2)/K_d$. Now we take the ball of radius \sqrt{d} centered at the same point as Q . It properly contains Q , so we are done. \square

Thus, we can find a small ball, relatively close to the origin, with many sums in it. The full conjecture states that such a ball can be taken *at* the origin. The proof of Proposition 8 is a simple volume argument.

4. CONCLUSIONS

Roughly speaking, the main challenge in Erdős’s conjecture is to establish fine grained control over some random distribution. Most of the techniques used today in Probabilistic Combinatorics—a field founded by Erdős himself—are only able to yield information about facts that occur “a constant fraction” of the time, and do not adapt well to situations where this

fraction depends on the instance of the problem (unless specific probability distributions are assumed).

Let us give a concrete example, focusing on dimension two. Lemma 6, applied to the ensemble of \pm -sums, says that at least $2^n(1 - 1/k^2)$ of all sums have norm less than $k\sqrt{n}$; this is only useful information if $k > 1$, otherwise it would be the trivial statement that less than at least 0 of the sums have norm less than \sqrt{n} . Taking $k > 1$ independent of n , as we did in Proposition 8, we managed to get some not entirely obvious bounds, but always with “rough” control on the position of the sums, at scales around \sqrt{n} . If we attempt to improve this by letting k depend on n , so as to obtain control at scales around 1, we are forced to make $k \approx 2/\sqrt{n}$, and we get the nonsensical statement that at least $2^n(1 - n/2)$ —a negative number—of the sums have norm less than 2.

This is a recurring theme in combinatorics. Some standard probabilistic inequalities can be used to show that, beyond $2\sqrt{n}$, the density of the sums decreases square-exponentially (i.e. like a Gaussian distribution), but are powerless to examine the fine-scale behavior near the peak of the distribution (the origin). It seems likely that more sophisticated methods are necessary to completely solve Erdős’s problem.

REFERENCES

1. B. Bollobás, *Combinatorics: Set systems, hypergraphs, families of vectors and combinatorial probability (Chapter 4)*, Cambridge University Press, 1986.
2. P. Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902, available at http://www.renyi.hu/~p_erdos/1945-04.pdf.
3. G. Katona, *On a conjecture of Erdős and a stronger form of Sperner’s theorem*, Studia Sci. Math. Hungar. **1** (1966), 59–63.
4. D. Kleitman, *On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors*, Advances in Math. **5** (1970), 155–157.
5. T. Tao and V. Vu, *From the Littlewood-Offord problem to the Circular Law: Universality of the spectral distribution of random matrices*, to appear, available at <http://arxiv.org/abs/0810.2994>.

CENTRE FOR LOGIC, EPISTEMOLOGY AND THE HISTORY OF SCIENCE
AND DEPARTMENT OF PHILOSOPHY, STATE UNIVERSITY OF CAMPINAS - UNICAMP

E-mail address: walter.carnielli@cle.unicamp.br

E-mail address: pietro.kc@gmail.com