

# The Littlewood-Offord problem

notes by

MARCEL K. GOH

20 NOVEMBER 2020

Let  $x_1, x_2, \dots, x_n$  be vectors in some normed space  $B$  of norm at least 1. There are  $2^n$  ways to form sums out of these vectors (where the empty sum is taken to be 0) and the Littlewood-Offord problem asks how many of these sums differ by less than 1. In its original 1943 formulation by J. E. Littlewood and A. C. Offord, the normed space in question was the complex plane  $\mathbf{C}$ .

Before we get started, let us recall the properties of a *normed space*. It is a vector space  $B$  over a field  $F$  along with a function  $\|\cdot\| : B \rightarrow \mathbf{R}$  such that

- i)  $\|x\| \geq 0$  for all  $x \in B$ ;
- ii)  $\|x\| = 0$  if and only if  $x = 0$ ;
- iii) for every  $\lambda \in F$ ,  $\|\lambda x\| = |\lambda| \|x\|$ ;
- iv) the triangle inequality  $\|x + y\| \leq \|x\| + \|y\|$  for all  $x, y \in B$ .

Note that in (iii), we have assumed some kind of norm on the field  $F$ . In the case that  $F = \mathbf{R}$ , this is the ordinary absolute value function, and in the case that  $F = \mathbf{C}$ , we can take the modulus. The *distance* between two vectors  $x$  and  $y$  is the norm of the difference  $x - y$ .

On a completely different note, we will also need some notions regarding families of subsets of a finite set. If  $X = \{1, 2, \dots, n\}$ , then the power set  $2^X$  has a natural partial order given by inclusion. A *chain* is a set of subsets  $\{A_1, A_2, \dots, A_k\}$  of  $X$  such that  $A_1 \subseteq A_2 \subseteq \dots \subseteq A_k$ , while an *antichain* or *Sperner family* is a family of subsets  $\{A_1, A_2, \dots, A_k\}$  such that if  $i \neq j$  then  $A_i \not\subseteq A_j$ , for any  $1 \leq i, j \leq k$ . A chain is *maximal* if one cannot add any set to the family without violating the chain property. A chain can be as large as  $|X| + 1$ , since for example, we have the maximal chain

$$\emptyset \subseteq \{1\} \subseteq \{1, 2\} \subseteq \dots \subseteq X.$$

How big can an antichain be? Well, we could take every set to be of the same size  $i$ , and this would certainly form an antichain. Since  $\binom{n}{i}$  is maximised, when  $i = \lfloor n/2 \rfloor$ , we see that the maximum size of an antichain must be at least  $\binom{n}{\lfloor n/2 \rfloor}$ . The following famous theorem shows that we can do no better.

**Theorem S** (*Sperner*, 1928). *Let  $X = \{1, 2, \dots, n\}$  and let  $\mathcal{F} \subseteq 2^X$  be an antichain. Then  $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$ .*

*Proof.* We will double count the number of pairs  $(\mathcal{C}, A)$  where  $\mathcal{C}$  is a maximal chain and  $A \in \mathcal{F} \cap \mathcal{C}$ . Observe that any permutation  $\sigma_1, \sigma_2, \dots, \sigma_n$  of  $\{1, 2, \dots, n\}$  defines a unique maximal chain

$$\emptyset \subseteq \{\sigma_1\} \subseteq \{\sigma_1, \sigma_2\} \subseteq \dots \subseteq \{\sigma_1, \sigma_2, \dots, \sigma_n\}.$$

Since the intersection of a chain with the antichain  $\mathcal{F}$  consists of at most one set  $A$ , the number of pairs  $(\mathcal{C}, A)$  is at most  $n!$ .

On the other hand, for a fixed set  $A = \{x_1, x_2, \dots, x_k\} \in \mathcal{F}$ , we must ask how many chains actually contain  $A$ . Note that a maximal chain  $\mathcal{C}$  contains  $A$  if and only if the first  $k$  nonempty sets in the chain introduce the elements  $x_1, x_2, \dots, x_k$  in some order. After that, the elements of  $X \setminus A$  can be introduced in any order. So for a fixed  $A$ , there are  $|A|!(n - |A|)!$  pairs  $(\mathcal{C}, A)$ . We have deduced that

$$\sum_{A \in \mathcal{F}} |A|!(n - |A|)! \leq n!,$$

and dividing both sides by  $n!$ , we have

$$\sum_{A \in \mathcal{F}} \binom{n}{|A|}^{-1} \leq 1.$$

Note that  $\binom{n}{|A|} \leq \binom{n}{\lfloor n/2 \rfloor}$  for all  $A$ , so we find that

$$\frac{|\mathcal{F}|}{\binom{n}{\lfloor n/2 \rfloor}} \leq \sum_{A \in \mathcal{F}} \binom{n}{|A|}^{-1} \leq 1,$$

which allows us to conclude that  $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$ . ■

**Lemma R** (Erdős, 1945). *Let  $x_1, x_2, \dots, x_n$  be real numbers with absolute value at least 1. At most  $\binom{n}{\lfloor n/2 \rfloor}$  of their sums differ by less than 1 from each other.*

*Proof.* For  $A \subseteq \{1, 2, \dots, n\}$ , let

$$x_A = \sum_{i \in A} x_i.$$

Without loss of generality, we may assume that all the  $x_i$  are positive. This is because replacing  $x_i$  with  $-x_i$  and  $A$  with  $A \triangle \{i\}$  does not change the relative differences between the sums; this operation causes the  $x_A$  to permute amongst themselves and increase by  $x_i$ .

Let  $\mathcal{F}$  be a family of subsets of  $\{1, 2, \dots, n\}$  such that  $|x_A - x_B| < 1$  for every pair of distinct  $A, B \in \mathcal{F}$ . It is an antichain because if  $A \subseteq B$  then  $x_B > x_A$  and in particular,

$$|x_B - x_A| = \sum_{x \in B} x_i - \sum_{x \in A} x_i = \sum_{x \in B \setminus A} x_i = x_{B \setminus A} \geq 1.$$

So at most one of  $A$  and  $B$  can be in  $\mathcal{F}$ . Applying Theorem S,  $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$ . ■

Note that Lemma R gives the best possible bound, because if  $x_1 = x_2 = \dots = x_n = c$  for some positive constant  $c$ , then  $\binom{n}{\lfloor n/2 \rfloor}$  of the sums are equal to  $c \lfloor n/2 \rfloor$ . With a bit of extra work, we can derive the following statement (and in fact, it is more than a corollary, because it is equivalent to Lemma R).

**Corollary T.** *Let  $x_1, x_2, \dots, x_n$  be real numbers, all with absolute value at least 1 and consider the  $2^n$  different sums  $\sum_{i=1}^n \epsilon_i x_i$ , where  $\epsilon_i$  is either  $-1$  or  $1$ . For any  $x \in \mathbf{R}$  with  $|x| \geq 1$ , at most  $\binom{n}{\lfloor n/2 \rfloor}$  of them are at distance less than 1 from  $x$ . ■*

## References

Béla Bollobás, *Combinatorics* (Cambridge: Cambridge University Press, 1986).

John Edensor Littlewood and Albert Cyril Offord, “On the number of real roots of a random algebraic equation (III),” *Matematicheskii Sbornik* **12** (1943), 277–286.

Paul Erdős, “On a lemma of Littlewood and Offord,” *Bulletin of the American Mathematical Society* **51** (1945), 898–902.