ON A LEMMA OF LITTLEWOOD AND OFFORD

PETER PHELAN

1. Introduction

The study of algebraic equations and their roots is a matter that has permeated mathematics since the earliest civilisations, yet still remains an active area of interest today. As a testament to this, we shall discuss here what is often referred to as the Littlewood-Offord problem, an inequality proven by Littlewood and Offord in 1943. This result first appeared as a lemma in [2], which as its title suggests was concerned with the number of real roots of random algebraic equations. Some years later a sharper inequality was found by Paul Erdős, and by 1970, it had been proven by Daniel Kleitman that Erdős's result was a special case of a more general inequality which holds for Hilbert spaces. Here we discuss these improvements following their presentation in Daniel Matthews talk given on 21/11/2018 and in Chapter 22 of [1].

2. Erdős's Improvement

The original lemma as proven by Littlewood and Offord can be stated as follows:

Theorem 2.1. *Let $a_1, \ldots, a_n \in \mathbb{C}$ such that $|a_i| \geq 1$ for all i and let $\varepsilon_i = \pm 1$ for all i. From this we have 2^n linear combinations of the form*

$$\sum_{i=1}^{n} \varepsilon_i a_i$$

Then the number of these sums which lie in the interior of any circle radius 1 cannot be greater than

$$c \frac{2^n}{\sqrt{n}} \log n$$

for some constant $c > 0$.

What Erdős had contributed to this result was that the $\log n$ term is unnecessary when the a_i are real. Furthermore he conjectured that this would also be true for a_i complex, as was later proven by Gyula Katona and Daniel Kleitman. What follows is Erdős's proof.

Let $a_1, \ldots, a_n \in \mathbb{R}$ such that $a_i \geq 1$ for all i, $\varepsilon_i = \pm 1$ for all i and let $N = \{1, 2, \ldots, n\}$ be the index set. We can say that all $a_i > 0$ by changing a_i to $-a_i$ and ε_i to $-\varepsilon_i$ when it is less than 0. Suppose a collection of linear combinations of the form $\sum_{i=1}^{n} \varepsilon_i a_i$ all lie in the interior of an interval of length 2.

Date: 21/11/2018.

For every such linear combination consider the set $I = \{i \in N \mid \varepsilon_i = 1\}$. For any two of these sets I, I' such that $I \subsetneq I'$ we know that

$$\sum_{i \in I'} \varepsilon_i a_i - \sum_{i \in I} \varepsilon_i a_i = 2 \sum_{i \in I' \setminus I} a_i \geq 2$$

which is a contradiction. Therefore for any two such sets I, I' that are not equal, I cannot contain I' and vice versa.

Recall from the talk "Three famous theorems on finite sets" [1, Chapter 27] given by Alden Mathieu on the 31st of October, that a family $\mathcal{F}$ of subsets of N is called an antichain if no set in $\mathcal{F}$ contains any other set of $\mathcal{F}$, thus the above sets I form an antichain. Furthermore we recall Sperner's theorem from the same talk, which states that the size of a largest antichain of N is $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. Therefore we have at most $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ linear combinations in our chosen interval, since each linear combination corresponds to some I. Finally, Stirling's formula [1, Chapter 2] tells us that

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} \leq c \frac{2^n}{\sqrt{n}}$$

for some $c > 0$, which proves the result.

We can in fact obtain an exact bound in this case if we let n be even and $a_i = 1$ for all i on the interval $(-1, 1)$, which follows from the fact that we will have $\binom{n}{\frac{n}{2}}$ linear combinations sum to 0.

3. Kleitman's Improvement

Theorem 3.1. *Let $\mathbf{a_1}, \ldots, \mathbf{a_n} \in \mathbb{R}^d$ with $|\mathbf{a_i}| \geq 1$ for all i and $\varepsilon_i = \pm 1$ for all i. Let $R_1, \ldots, R_k$ be k open regions in $\mathbb{R}^d$ such that for any two points x, y in the same region, $|x - y| < 2$. Then the number of linear combinations of the form*

$$\sum_{i=1}^{n} \varepsilon_i \mathbf{a_i}$$

that lie in the union of the k regions $\cup_{i=1}^{k} R_i$ is at most the sum of the k largest binomial coefficients $\binom{n}{j}$.

Proof. We shall assume that all k regions are disjoint. If we set $r = \lfloor \frac{n-k+1}{2} \rfloor$ and $s = \lfloor \frac{n+k-1}{2} \rfloor$, then from [1, Chapter 2], we know that the k largest binomial coefficients are

$$\binom{n}{r}, \binom{n}{r+1}, \ldots, \binom{n}{s}$$

Moreover we have the following formula

$$\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$$

To see why this is true we recall the well-known result that the entries of Pascal's triangle correspond to binomial coefficients, and that the sum of any two adjacent entries in a row is equal to the entry directly beneath them, as we can see below.

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

Therefore we have that

$$\begin{aligned}
\sum_{i=r}^{s}\binom{n}{i} &= \sum_{i=r}^{s}\binom{n-1}{i} + \sum_{i=r}^{s}\binom{n-1}{i-1} \\
&= \sum_{i=r}^{s}\binom{n-1}{i} + \sum_{i=r-1}^{s-1}\binom{n-1}{i} \\
&= \sum_{i=r-1}^{s}\binom{n-1}{i} + \sum_{i=r}^{s-1}\binom{n-1}{i} \qquad (1)
\end{aligned}$$

Where the first sum adds the $k+1$ largest, and the second sum the $k-1$ largest binomial coefficients of the form $\binom{n-1}{i}$.

From here we will prove the theorem by induction on n, where for $n = 1$ it follows trivially. Let us assume that the theorem is true for $n-1$. To prove that its true for n, we will show that the linear combinations of $\mathbf{a_1}, \ldots, \mathbf{a_n}$ that lie in the k disjoint regions can be bijectively mapped onto combinations of $\mathbf{a_1}, \ldots, \mathbf{a_{n-1}}$ that lie in $k+1$ or $k-1$ regions.

To do this, we begin with the claim that at least one of the translated regions $R_j - \mathbf{a_n}$ is disjoint from all other translated regions $R_1 + \mathbf{a_n}, \ldots, R_k + \mathbf{a_n}$. First let us consider the hyperplane $H = \{x \in \mathbb{R}^d \mid \langle \mathbf{a_n}, x\rangle = c\}$ for some particular c. H is orthogonal to $\mathbf{a_n}$ and has each translated region of the form $R_i + \mathbf{a_n}$ in the region $\langle \mathbf{a_n}, x\rangle \geq c$. Moreover c is chosen so that the hyperplane touches the closure of some region $R_j + \mathbf{a_n}$. H exists since the regions are by definition bounded. Since R_j is an open region, for any $x \in R_j$ and $y \in \bar{R}_j$ the closure of R_j, we have $|x - y| < 2$ by construction. We claim that that $R_j - \mathbf{a_n}$ lies in the region $\langle \mathbf{a_n}, x\rangle < c$. So assume that it doesn't, then for some $x \in R_j$

$$\begin{aligned}
\langle \mathbf{a_n}, x - \mathbf{a_n}\rangle &\geq c \\
\langle \mathbf{a_n}, x\rangle - \langle \mathbf{a_n}, \mathbf{a_n}\rangle &\geq c \\
\langle \mathbf{a_n}, x\rangle &\geq |\mathbf{a_n}|^2 + c
\end{aligned}$$

Let y be the point in the closure of R_j that touches the hyperplane, then

$$\begin{aligned}\langle \mathbf{a_n}, y + \mathbf{a_n}\rangle &= c \\ \langle \mathbf{a_n}, y\rangle + \langle \mathbf{a_n}, \mathbf{a_n}\rangle &= c \\ -\langle \mathbf{a_n}, y\rangle &= |\mathbf{a_n}|^2 - c \\ \langle \mathbf{a_n}, -y\rangle &= |\mathbf{a_n}|^2 - c \\ \langle \mathbf{a_n}, x - y\rangle &\geq 2|\mathbf{a_n}|^2\end{aligned}$$

So by the Cauchy-Schwarz inequality we have that

$$2|\mathbf{a_n}|^2 \leq \langle \mathbf{a_n}, x - y\rangle \leq |\mathbf{a_n}||x - y|$$

Since $|\mathbf{a_i}| \geq 1$ for all i, we obtain that

$$2 \leq 2|\mathbf{a_n}| \leq |x - y|$$

which is a contradiction. Therefore at least one region $R_j - \mathbf{a_n}$ is disjoint from the other translated regions $R_1 + \mathbf{a_n}, \ldots, R_k + \mathbf{a_n}$ as required.

To complete the proof, we consider two classes of linear combinations that lie in the union of open regions as described above. In class 1 we have all the linear combinations $\sum_{i=1}^{n} \varepsilon_i \mathbf{a_i}$ such that either $\varepsilon_n = -1$ or $\varepsilon_n = 1$ and the sum lies in R_j. Let the remaining sums be in class 2, so those with $\varepsilon_n = 1$ such that the sum does not lie in R_j. From this it is clear that the linear combinations $\sum_{i=1}^{n-1} \varepsilon_i a_i$ in class 1 correspond to the $k+1$ disjoint regions $R_1 + \mathbf{a_n}, \ldots, R_k + \mathbf{a_n}, R_j - \mathbf{a_n}$, whereas the linear combinations $\sum_{i=1}^{n-1} \varepsilon_i a_i$ in class 2 correspond to the $k - 1$ disjoint regions $R_1 - \mathbf{a_n}, \ldots, R_k - \mathbf{a_n}$.

So by induction class 1 contains at most $\sum_{i=r-1}^{s} \binom{n-1}{i}$ linear combinations and class 2 contains at most $\sum_{i=r}^{s-1} \binom{n-1}{i}$ linear combination. Therefore by the above sum (1), the proof is true for all n and we have the desired inequality. □

We now conclude with some interesting observations. Recall again that the largest binomial coefficient of a given binomial power $(x + 1)^n$ is $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. So for $k = 1$ we get $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ as the upper bound. Again since Stirling's formula tells us that

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} \leq c\frac{2^n}{\sqrt{n}}$$

for some $c > 0$, so we have reduced the original lemma to a corollary of Kleitman's result.

We should also note that for $\mathbf{a_1} = \ldots, = \mathbf{a_n} = \mathbf{a} = (1, 0, \ldots, 0)^T$ we get an exact bound. To see this first we let n be even, then we have $\binom{n}{\frac{n}{2}}$ sums equal to 0, $\binom{n}{\frac{n}{2}-1}$ sums equal to $-2\mathbf{a}$ and $\binom{n}{\frac{n}{2}+1}$ sums equal to $2\mathbf{a}$, and so on. So if we choose open balls of radius 1 about each of the points

$$\{-2\lfloor \frac{k-1}{2} \rfloor \mathbf{a}, \ldots, -2\mathbf{a}, 0, 2\mathbf{a}, \ldots, 2\lfloor \frac{k-1}{2} \rfloor \mathbf{a}\}$$

then we obtain the sum

$$\binom{n}{\lfloor\frac{n-k+1}{2}\rfloor}+\cdots+\binom{n}{\lfloor\frac{n-2}{2}\rfloor}+\binom{n}{\lfloor\frac{n}{2}\rfloor}+\binom{n}{\lfloor\frac{n+2}{2}\rfloor}+\cdots+\binom{n}{\lfloor\frac{n+k-1}{2}\rfloor}$$

which is the exact bound, since the largest terms in a binomial expansion are those closest to the centre. The argument is the same for odd n.

References

[1] Martin Aigner and Günter M. Ziegler. *Proofs from The Book*. Springer-Verlag, Berlin, fifth edition, 2014. Including illustrations by Karl H. Hofmann.

[2] J. E. Littlewood and A. C. Offord. On the number of real roots of a random algebraic equation. *Rec. Math.[Mat. Sbornik] N.S.*, 54:277–286, 1943.