Fourier proof of the classical Littlewood-Offord inequality

Ernie Croot

April 18, 2011

1 Introduction

We saw in class the standard combinatorial Littlewood-Offord inequality, and here we will consider the discrete version:

Theorem 1 *Suppose $x_1, ..., x_k$ are non-zero real numbers. Then, for any $x \in \mathbb{R}$ we have that there are $O(2^k/\sqrt{k})$ choices for $(\varepsilon_1, ..., \varepsilon_k) \in \{+1, -1\}^k$ such that*

$$\varepsilon_1 x_1 + \cdots + \varepsilon_k x_k \ = \ x.$$

Our proof will make use of Fourier analysis, together with a basic fact from elementary Diophantine approximation.

2 Proof of the theorem

We begin with the following lemma that we will apply to transfer our problem to $\mathbb{Z}_N$ where the Fourier analysis is easier (this lemma is due to Dirichlet):

Lemma 1 *Given $y_1, ..., y_k \in \mathbb{R}$ and $Q \in \mathbb{Z}_+$, there exists an integer $1 \leq D \leq Q$ and integers $N_1, ..., N_k$ such that*

$$|y_i - N_i/D| \ \leq \ 1/DQ^{1/k}.$$

Proof. The proof is just via some pigeonholing: consider the set of mod 1 vectors

$$\{(jy_1, ..., jy_k) \pmod 1 \ : \ 0 \le j \le Q\}.$$

For each of these points, draw a box around them of radius $1/2Q^{1/k}$ using the ℓ^∞ norm. Each such box has volume $1/Q$; and so thinking of these boxes as subsets of the torus $[0,1]^k$ we have that since there are $Q+1$ of them, their total volume exceeds the volume of the torus, implying that two of these boxes must intersect. Say the boxes correspoinding to this intersection are associated with $j = j_1$ and j_2, where $j_1 > j_2$. It is easy to see that this means that for all $i = 1, ..., k$,

$$\|(j_1 - j_2)y_i\| \ = \ \|j_1 y_i - j_2 y_i\| \ \le \ 1/Q^{1/k}.$$

(Here, $\|y\|$ denotes the distance from y to the nearest integer.) Letting $D = j_1 - j_2$ we then have that for $i = 1, ..., k$,

$$Dy_i \ = \ I_i + \delta_i, \text{ where } |\delta_i| \ \le \ 1/Q^{1/k}, \text{ and } I_i \in \mathbb{Z}.$$

Dividing through by D the lemma now follows. ■

We now resume the proof of Littlewood-Offord: given $x_1, ..., x_k$, consider the set

$$S \ := \ \{\gamma_1 x_1 + \cdots + \gamma_k x_k \ : \ \gamma_i = 0, \pm 2\}.$$

(This set contains all the differences of two sums of the form $\varepsilon_1 x_1 + \cdots + \varepsilon_k x_k$.) Let $E \ge 1$ be any integer such that for every non-zero $s \in S$ we have that $|Es| \ \ge \ 1$, and set $y_i = Ex_i$, $i = 1, ..., k$.

Next, we apply the above lemma, choosing $Q \ge 1$ as needed later in the proof. Let $z_i = Dy_i = DEx_i$, and note that $z_i = I_i + \delta_i$, where $|\delta_i| \le 1/Q^{1/k}$. The point of choosing D and E will now be made clear by the following claim, which basically says we can transfer our problem to $\mathbb{Z}$:

Claim. For Q sufficiently large we will have that for any sequence $\varepsilon_1, ..., \varepsilon_k, \varepsilon'_1, ..., \varepsilon'_k = \pm 1$,

$$\varepsilon_1 x_1 + \cdots + \varepsilon_k x_k \ = \ \varepsilon'_1 x_1 + \cdots + \varepsilon'_k x_k \qquad (1)$$

if and only if

$$\varepsilon_1 I_1 + \cdots + \varepsilon_k I_k \ = \ \varepsilon'_1 I_1 + \cdots + \varepsilon'_k I_k. \qquad (2)$$

First let us suppose that (1) holds. Then, multiplying through by DE and rearranging terms, we find that

$$(\varepsilon_1 - \varepsilon_1')z_1 + \cdots + (\varepsilon_k - \varepsilon_k')z_k \ = \ 0.$$

Writing the z_i's in terms of the I_i's then gives

$$(\varepsilon_1 - \varepsilon_1')I_1 + \cdots + (\varepsilon_k - \varepsilon_k')I_k \ = \ O(k/Q^{1/k}).$$

If Q is large enough the RHS will be smaller than $1/2$; and so, the LHS, being an integer, must therefore be 0. This then establishes (2).

Conversely, suppose that (2) holds. Then, it follows that

$$E \cdot ((\varepsilon_1 - \varepsilon_1')x_1 + \cdots + (\varepsilon_k - \varepsilon_k')x_k) \ = \ O(k/DQ^{1/k}).$$

Again, if Q is large enough then the RHS will be less than $1/2$ in magnitude; yet, the LHS is of the form Es, where $s \in S$. Since E was chosen to make any such non-zero product exceed 1 in magnitude, we are forced to have that the LHS equals 0. The claim now follows.

Lastly, we choose N to be a very large prime number – so large that it does not divide any non-zero integer of the form

$$\gamma_1 I_1 + \cdots + \gamma_k I_k, \text{ where } \gamma_i = 0, \pm 2.$$

It is easy to see, then, that for such N we will have that

$$\varepsilon_1 x_1 + \cdots + \varepsilon_k x_k \ = \ \varepsilon_1' x_1 + \cdots + \varepsilon_k' x_k$$

if and only if

$$\varepsilon_1 I_1 + \cdots + \varepsilon_k I_k \ \equiv \ \varepsilon_1' I_1 + \cdots + \varepsilon_k' I_k \pmod{N}.$$

That is to say, we have now reduced ourselves to a Littlewood-Offord problem for $\mathbb{Z}_N$... one that is amenable to the methods of discrete Fourier analysis.

Let now $r(x)$ denote the number of representations

$$x \ \equiv \ \varepsilon_1 I_1 + \cdots + \varepsilon_k I_k \pmod{N}, \text{ where } \varepsilon_i = \pm 1.$$

We have that

$$r(x) \ = \ 1_{\{I_1, -I_1\}} * \cdots * 1_{\{I_k, -I_k\}}(x).$$

By Fourier inversion, then, we deduce that

$$\begin{aligned} r(x) &= N^{-1}\sum_{a=0}^{N-1} e^{2\pi i a x/N}\hat{r}(a) \\ &= N^{-1}\sum_{a=0}^{N-1} e^{2\pi i a x/N}\hat{1}_{\{I_1,-I_1\}}(a)\cdots\hat{1}_{\{I_k,-I_k\}}(a) \\ &= N^{-1}\sum_{a=0}^{N-1} e^{2\pi i a x/N}\prod_{j=1}^{k}(e^{2\pi i a I_j/N}+e^{-2\pi i a I_j/N}) \\ &= 2^k N^{-1}\sum_{a=0}^{N-1} e^{2\pi i a x/N}\prod_{j=1}^{k}\cos(2\pi a I_j/N). \end{aligned}$$

Since all we need is an upper bound, we just need to work with

$$r(x) \ \le\ 2^k N^{-1}\sum_{a=0}^{N-1}\left|\prod_{j=1}^{k}\cos(2\pi a I_j/N)\right|.$$

Using Hölder, we deduce that

$$r(x) \ \le\ 2^k N^{-1}\prod_{j=1}^{k}\left(\sum_{a=0}^{N-1}|\cos(2\pi a I_j/N)|^k\right)^{1/k}.$$

Now, all the factors in this product are equal since the I_j's are non-zero, and since

$$\{aI_i\ :\ a=0,...,N-1\}\ \equiv\ \{aI_j\ :\ a=0,...,N-1\}\pmod N.$$

So,

$$r(x)\ \le\ 2^k N^{-1}\sum_{|a|<N/2}|\cos(2\pi a/N)|^k.$$

To bound this sum from above, we only consider those a satisfying $|a| < N/4$, since the total sum is at most double this. For such a we have that

$$\cos(2\pi a/N)\ =\ 1-(2\pi a/N)^2/2+O((a/N)^4)\ <\ 1-c(a/N)^2,$$

for some $c > 0$ (we won't even bother to work it out). Now suppose a satisfies

$$|a|\ \in\ [hN/\sqrt{k},\ (h+1)N/\sqrt{k}],\ \text{where } 0\le h\le\sqrt{k}/4.$$

It follows that for such a we will have

$$|\cos(2\pi a/N)|^k \ \le\ (1 - c(a/N)^2)^k \ \le\ (1 - cj^2/k)^k \ \le\ e^{-cj^2}.$$

So,

$$r(x) \ \ll\ 2^k N^{-1} \sum_{h=0}^{\sqrt{k}/4} (N/\sqrt{k}) e^{-cj^2} \ \ll\ 2^k/\sqrt{k},$$

thus completing the proof of Littlewood-Offord.