Adventures in additive combinatorics

by

Marcel K. Goh

18 December 2020

1. Introduction

This set of notes will contain neat theorems and problems that are (at least a little bit) related to additive combinatorics. The individual sections are intended to be largely self-contained, and will not delve too much into theory, but focus on famous problems and their solutions, especially if the proofs are rather elegant (particular preference has been given to probabilistic proofs). None of these proofs are new in any way; they all appear in one of the references listed at the end of the document.

Notation and terminology. The notation $[a, b]$ always denotes the *discrete interval* $\{n \in \mathbf{Z} : a \leq n \leq b\}$. For a set X, we let 2^X denote the set of all subsets of X (the *power set*) and the notation $X^{(r)}$ indicates the collection of all subsets of X with cardinality r.

A *graph* G is a pair (V, E) where $E \subseteq V^{(2)}$. If, for $u, v \in V$, we have $\{u, v\} \in E$, then we write $u \text{ — } v$ and say that u and v are *adjacent*. The *neighbourhood* of a node $u \in V$ is the set $N(u) = \{v \in V : u \text{ — } v\}$, that is, the set of nodes adjacent to u, and the *degree* of u, denoted $d(u)$, is the cardinality of this set.

2. The Littlewood-Offord problem

We begin with a simple problem, which J. E. Littlewood and A. C. Offord came across in 1943 while studying the zeroes of random polynomials. Let $z_1, z_2, \ldots, z_n$ be complex numbers of modulus at least 1 and form all 2^n possible sums. How many of these sums can differ by less than 1? To attack this problem, we will need a couple of definitions and inequalities. Given a ground set X, an *antichain* or *Sperner system* is a collection of subsets $\mathcal{F}$ such that for any $A \subseteq B \in 2^X$, either $A \notin \mathcal{F}$ or $B \notin F$. In other words, if all the elements of 2^X are ordered by inclusion, then no two elements of $\mathcal{F}$ are comparable. On the other hand, a *chain* is a collection $\mathcal{C} = \{C_1, C_2, \ldots, C_k\}$ of subsets of X such that $C_1 \subset C_2 \subset \cdots \subset C_k$.

The following inequality was proved independently by D. Lubell, K. Yamamoto, and L. D. Meshalkin, and has thus become known as the LYM inequality. However, it also follows from an earlier result of B. Bollobás, and in fact, the probabilistic proof we present is due to Bollobás.

Lemma B (*LYM inequality*). *Let X be a finite set of size n; for simplicity, we assume that $X = [1, n]$. Let $\mathcal{F} \subseteq 2^X$ be an antichain; then*

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

Proof. Let $\sigma : X \to X$ be a permutation chosen uniformly from all $n!$ such permutations. For $A \subseteq X$, $\sigma(A)$ denote the set $\{\sigma(x) : x \in A\}$ and consider the probability that $\sigma(A) = [1, |A|]$. Note that $\sigma(A)$ is uniformly distributed over the $\binom{n}{|A|}$ members of $X^{(|A|)}$, so the probability that it equals $[1, |A|]$ is $\binom{n}{|A|}^{-1}$. Note that for two sets $A, B \in 2^X$, if $\sigma(A) = [1, |A|]$ and $\sigma(B) = [1, |B|]$ for the same fixed σ, then either $A \subseteq B$ or $B \subseteq A$. Since $\mathcal{F}$ is an antichain, the events $\sigma(A) = [1, |A|]$ must then be disjoint and the sum of their probabilities is at most 1. This proves the inequality. ∎

Because $\binom{n}{k}$ is maximal when $k = \lfloor n/2 \rfloor$, we can derive the following theorem of E. Sperner as a corollary.

Corollary S (*Sperner,* 1928). *Let X be a finite set and let $\mathcal{F} \subseteq 2^X$ be an antichain. Then $\mathcal{F}$ has size at most $\binom{n}{\lfloor n/2 \rfloor}$.*

Proof. We have, by Lemma B,

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

Multiplying on both sides by $\binom{n}{\lfloor n/2 \rfloor}$ yields the result. ∎

With this theorem in hand, we can already solve the Littlewood-Offord problem in the special case when all the z_i are real. The following construction is due to P. Erdős (1945). Let $x_1, x_2, \ldots, x_n$ be real numbers with absolute value at least 1. For $A \subseteq [1, n]$, let $x_A = \sum_{i \in A} x_i$. We may assume all of the x_i are positive, because replacing x_i with $-x_i$ and A with $A \cup \{i\} \setminus \big(A \cap \{i\}\big)$ does not change the relative differences between the 2^n sums. This operation simply causes all the x_A to permute amongst themselves and shift by $-x_i$. Now let $\mathcal{F}$ be a family of subsets of $[1, n]$ such that $|x_A - x_B| < 1$ for every distinct pair of $A, B \in \mathcal{F}$. It is an antichain because if A is a proper subset of B then $x_B > x_A$ and we have

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

and this is at least 1 since $B \setminus A$ is nonempty. Hence at most one of A and B belongs to $\mathcal{F}$. By Corollary S, $|\mathcal{F}| \le \binom{n}{n/2}$.

3. Independent sets

For a graph $G = (V, E)$, an *independent set* is a subset $S \subseteq V$ of vertices such that no two elements of S are adjacent. The largest independent set in G is denoted $\alpha(G)$. In this section, we present two beautiful probabilistic proofs that give lower bounds for $\alpha(G)$. The first is due to Turán; sometimes this theorem is called Turán's theorem, but more often, that name is reserved for a somewhat dual statement about the maximum number of edges in a graph that has no complete graph on $r + 1$ vertices as a subgraph.

Theorem T. *Let $G = (V, E)$ be a graph. The size $\alpha(G)$ of the largest independent set in G satisfies the inequality*

$$\alpha(G) \ge \sum_{u \in V} \frac{1}{d(u) + 1}.$$

Proof. Suppose V has size n and let $\sigma : V \to [1, n]$ be a bijection, chosen uniformly at random from all $n!$ such bijections. Regarding this as an ordering of the vertices, consider the set

$$S = \{u \in V : \sigma(u) < \sigma(v) \text{ for all } v \in N(u)\},$$

which consist of vertices that come before all of their neighbours in the ordering. For any ordering, the set S that it induces must be an independent set, for if two vertices $u, v \in V$ are adjacent then the vertex which was assigned a larger value in the ordering cannot be in S. Fixing a node $u \in V$, the probability that it is the first among all of its neighbours is $1/\big(d(u) + 1\big)$, and by linearity of expectation, we have

$$\mathbf{E}\{|S|\} = \mathbf{E}\Big\{ \sum_{u \in V} \mathbf{1}_{[u \in S]} \Big\} = \sum_{u \in V} \frac{1}{d(u) + 1}.$$

So there exists an independent set S with size at least the value of this sum, which was what we wanted. ∎

In particular, if maximal degree over all vertices in G is d, then there is an independent set of size at least $n/(d + 1)$.

References

Noga Alon and Joel Harold Spencer, *The Probabilistic Method*, (New York: Wiley-Interscience, 2000).

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

Terence Tao and Van Ha Vu, *Additive Combinatorics* (Cambridge: Cambridge University Press, 2006).