Combinatorics: Projects

October 20, 2009

Most of this course has been (or will be) about "pure" combinatorics, except for the last section on Roth's theorem and harmonic analysis. For the sake of contrast, I've chosen these projects to emphasize links between combinatorics and other branches of mathematics, specifically: geometry, topology, functional analysis, coding theory, probability theory and graph theory. I find these connections beautiful and surprising, and I hope you will enjoy thinking about them.

Choose a project you like. I will find some way of dealing with conflicts, should they arise. The aim is to have 2 people to each project: you are both required to read and understand the proof(s), and either one or both of you can present it in class.

Borsuk's conjecture

In 1933, Borsuk raised the following question:

Can every set of diameter 1 in $\mathbb{R}^d$ be partitioned into $d+1$ pieces of diameter less than 1?

Here, the diameter $\mathrm{diam}(A)$ of a set $A \subset \mathbb{R}^d$ is defined as

$$\mathrm{diam}(A) = \sup\{||x-y|| : x, y \in A\}.$$

The example of the unit simplex shows that we need at least $d+1$ pieces. After the conjecture was proved in dimensions 2 and 3, and in all dimensions for centrally symmetric convex bodies and smooth convex bodies, many people believed that it was true.

It therefore came as a big surprise when Kahn and Kalai proved in 1993 that Borsuk's conjecture fails for *a finite set of points* in sufficiently high dimension d. Their proof used a combinatorial result of Frankl and Wilson. The second reference below gives a short self-contained proof.

[1] J. Kahn and G. Kalai, A counterexample to Borsuk's conjecture, *Bull. Amer. Math. Soc.* **29** (1993), 60–62.

[2] A. Nilli, On Borsuk's problem, in "Jerusalem Combinatorics '93" (H. Barcelo and G. Kalai, eds.), Contemporary Mathematics **178**, Amer. Math. Soc. 1994, 209–210.

Kneser's conjecture

Let $X = \{1, 2, \ldots, 2n + k\}$ and let $\mathcal{A} = X^{(n)}$. In 1955, Kneser considered the problem of partitioning $\mathcal{A}$ into subsets $\mathcal{A}_1, \ldots, \mathcal{A}_m$ such that each $\mathcal{A}_i$ is an intersecting family. How small can m be so that this is possible? It is not too hard to see that such a partition exists with $m = k + 2$, so the question is whether we can take $m < k + 2$. Kneser conjectured "no", i.e. that $m = k + 2$ is best possible, but it was 20 years before Lovász proved this using *algebraic topology.* Since then, simpler proofs have appeared, and the shortest seems to be the one in the paper below, which was written by an undergraduate.

[1] J.E. Greene, A new short proof of Kneser's conjecture, *Amer. Math. Monthly* **109** (2002), 918–920.

The Littlewood-Offord problem

Let $x_1, \ldots, x_n \in \mathbb{R}$ with $|x_i| \geq 1$ for all i. One of the homework exercises was to show that at most $\binom{n}{\lfloor n/2 \rfloor}$ of the 2^n sums $s(A) = \sum_{i \in A} x_i$ can lie within any fixed interval $[t, t + 1) \subset \mathbb{R}$. (By convention $s(\emptyset) = 0$.) What if the x_i are *complex* numbers? Then the question would be: how many of the 2^n sums can lie in any fixed open disc

$$\{z : |z - z_0| < 1/2\}.$$

This problem first arose in work of Littlewood and Offord on the number of real zeros of random polynomials, and, shortly afterwards, Erdős conjectured that the answer is again $\binom{n}{\lfloor n/2 \rfloor}$. Erdős' conjecture was proved 20 years later by Katona and Kleitman independently. In 1970, Kleitman generalized the result to vectors in an arbitrary normed space. The goal of the project is to understand and present Kleitman's proof, which is described in Chapter 4 of the set text by Bollobás.

Shannon's theorem

Suppose I am transmitting data bits (i.e. 0s and 1s) over a *noisy channel*, where each data bit has probability $p \ll 1$ of being sent incorrectly (a 0 could become a 1, and a 1 could become a 0 – both these events have probability p). How can I reduce the error probability p? I can certainly do it at the cost of also reducing the *data rate*: for instance I can send each bit 3 times, reducing the error probability from p to $p' = p^3 + 3p^2(1-p)$, but bringing the data rate down from 1 to 1/3. What if I want the error probability to be *really small*? Suppose, for instance, that $p = 0.1$, but I want the new error probability p' (of my modified scheme) to be 10^{-100}. Surely the data rate will now be incredibly poor (i.e. small)? Not necessarily. Shannon proved that in fact, for $0 < p < 1/2$ and all $\varepsilon > 0$,

- There exists a code of rate greater than $1 - H(p) - \varepsilon$ and error probability less than ε.

Here, $H(p)$ is the *entropy function*

$$H(p) = -p \log_2 p - (1-p) \log_2 (1-p),$$

and a *code* is simply a rule telling us how to convert our data (blocks of 0s and 1s) into a form suitable for transmission. The above code could be summarized as $0 \to 000$ and $1 \to 111$, and we need to supplement this with a *decoding rule*: in this case we decode 000, 001, 010 and 100 as 0, and 111, 110, 101 and 011 as 1. In general, we will allow ourselves to use codes of the form $f : \{0,1\}^m \to \{0,1\}^n$, which have rate m/n.

This major insight of Shannon is now an instinct of many communications engineers. The essence of it is that the optimum rate $1 - H(p)$ of a code is a function only of p. Moreover, the essence of Shannon's *proof*, namely that a *random* map $f : \{0,1\}^m \to \{0,1\}^n$ does the job, is now an instinct of many mathematicians. A modern version of Shannon's proof is explained in *The Probabilistic Method* by Alon and Spencer (pages 255–257 in the third edition), but you should contrast this with Shannon's own account in his 1948 paper, which is reprinted in *The Mathematical Theory of Communication* by Shannon and Weaver.

Sidon's problem

In the 1930s, Sidon posed the following problem to Erdős. Let $0 < a_1 < a_2 < \cdots$ be an infinite sequence of positive integers, and let $f(n)$ be the number of solutions of $n = a_i + a_j$. Is there a sequence (a_i) with $f(n) > 0$ for all $n > 1$ and $\lim f(n)/n^\varepsilon = 0$ for all $\varepsilon > 0$? Loosely speaking, is there a sequence which *represents* every positive integer (greater than one), but which does not *over-represent* an increasing sequence of integers? 20 years later, Erdős proved that such a sequence does indeed exist. A modern version of the proof is on page 131 of Alon and Spencer's book mentioned above – it may also be necessary to read some of the references contained therein.

This project requires some familiarity with probability theory, although the basic method is strikingly simple (but, needless to say, unexpected).

The triangle removal lemma

This project requires some familiarity with graph theory. The triangle removal lemma states that for all $\varepsilon > 0$, there exists a $\delta > 0$ such that given any graph on n vertices with less than δn^3 triangles, we can destroy all the triangles by removing at most εn^2 edges. This turns out to imply Roth's theorem. The aim of the project is to understand why.

[1] I. Ruzsa and E. Szemerédi, Triple systems with no six points carrying three triangles, *Colloq. Math. Soc. J. Bolyai* 18 (1978), 939–945.
