

Algebraic Methods in Combinatorics

David Ellis

Lent 2011

Introduction

In the last fifty years, algebraic methods have been used with striking success in combinatorics. This course looks at some of the most important of these methods, and some of the most beautiful results obtained using them. We will also explore connections with combinatorial geometry, probability theory and theoretical computer science.

Many questions in extremal combinatorics have the following general form. We have a universe of objects U , and we are interested in subsets S of the universe U which have a certain property P . We ask: what is the maximum (or minimum) possible size of a subset S of U which has the property P ? What exactly are the maximum-sized subsets of U with property P ? (We call these the *extremal subsets of U with the property P* .)

For example:

Definition. We say that a family \mathcal{A} of r -element subsets of $\{1, 2, \dots, n\} =: [n]$ is intersecting if $x \cap y \neq \emptyset$ for all $x, y \in \mathcal{A}$.

Question. What is the maximum possible size of an intersecting family of r -element subsets of $[n]$?

Theorem 1 (Erdős-Ko-Rado, 1961). Let $r < n/2$, and let \mathcal{A} be an intersecting family of r -subsets of $[n]$. Then

$$|\mathcal{A}| \leq \binom{n-1}{r-1}.$$

Equality holds if and only if \mathcal{A} consists of all r -subsets containing some fixed $i \in [n]$.

‘Purely’ combinatorial techniques for tackling this sort of question include:

Induction on n (where n is some parameter of the universe U). For example, Erdős, Ko and Rado’s original proof of their theorem above was by induction on n .

Averaging: Find a family \mathcal{C} of subsets of U , such that \mathcal{C} is a k -cover of U for some $k \in \mathbb{N}$ (meaning that each element of U is contained in at least k sets in \mathcal{C}), and such that for any subset $S \subset U$ with the property P , $|S \cap \mathcal{C}|$ is

small for each $C \in \mathcal{C}$. If $|S \cap C| \leq t_C$ for all $C \in \mathcal{C}$, then we can ‘average’ over all $C \in \mathcal{C}$ in order to obtain an upper bound on $|S|$:

$$m|S| \leq \sum_{x \in S} |\{C \in \mathcal{C} : x \in C\}| = \sum_{C \in \mathcal{C}} |S \cap C| \leq \sum_{C \in \mathcal{C}} t_C.$$

Often, all the sets in \mathcal{C} have the same size, and \mathcal{C} is a *uniform* cover (every element of U is contained in exactly k sets in \mathcal{C}). In this case, if $|S \cap C|/|C| \leq \gamma$ for all $C \in \mathcal{C}$, we then have $|S|/|U| \leq \gamma$.

The classic example is Katona’s proof of the Erdős-Ko-Rado theorem; indeed, these arguments are often referred to as ‘Katona-type’ arguments.

Shifting: Suppose we want to show any subset $S \subset U$ with the property P has size at most $|E|$ for some $E \in \mathcal{E}$ (think of \mathcal{E} as a family of ‘candidate extremal sets’). Starting with any subset $S \subset U$ with the property P , perform a suitable sequence of simple ‘shift’ operations (C_i) which

- make subsets ‘more like’ some $E \in \mathcal{E}$, or more like a subset of some $E \in \mathcal{E}$;
- preserve the property P ;
- preserve $|S|$ (or, at any rate, don’t reduce $|S|$).

Show that at the end of the process, we end up with a subset of some $E \in \mathcal{E}$ (or something no larger). This approach was one ingredient in the proof of the t -intersecting analogue of the Erdős-Ko-Rado theorem, by Ahlswede and Khachatrian [1].

However, if our universe U has a ‘complicated’ structure, these techniques may fail. Instead, we can try using algebraic techniques, which may actually utilize the additional structure.

The linear independence method

Our first important algebraic method is the *linear independence* method. In its simplest form, the method is as follows. In order to show that a set S with a certain property has size at most m , we construct a linearly independent set of size $|S|$ in a vector-space of dimension at most m .

Simple though it sounds, this method has produced surprisingly strong results in many problems that make no explicit mention of vectors. These problems often seem intractable by ‘purely’ combinatorial methods. Sometimes, the linear independence method gives a sharp bound when there are many non-isomorphic sets attaining this bound. (A purely combinatorial method is unlikely to give a sharp bound in this case, as a combinatorial proof can typically be examined to give a simple characterization of the extremal sets.)

The polynomial method

The *polynomial method* is a relatively recent innovation in combinatorics. It borrows some of the philosophy of algebraic geometry. In algebraic geometry, we are often interested in geometrical objects which are the vanishing sets of a

collection of one or more polynomials. (Or we may try to approximate geometrical objects by the vanishing sets of polynomials.) We try to understand the geometry of the objects by looking at these polynomials.

In combinatorial problems, we often have a field \mathbb{F} , and we are looking at a subset $S \subset \mathbb{F}^n$ with a certain property, P . We can often obtain combinatorial information about S by looking at multivariate polynomials over \mathbb{F} which vanish on all points of S .

This is the idea behind Alon's Combinatorial Nullstellensatz, which has several applications in extremal combinatorics and combinatorial geometry. The polynomial method was also a crucial ingredient in the stunning recent result of Guth and Katz on Erdős' 'distinct distances problem' in the plane. Erdős asked the following

Question. *If we have N points in the plane, what is the minimum number of distinct distances that can occur between them?*

We write $f(N)$ for this minimum. The points of the $\sqrt{N} \times \sqrt{N}$ grid determine $\Theta(N/\sqrt{\log N})$ distinct distances, so $f(N) = O(N/\sqrt{\log N})$.

In the other direction, Erdős showed that $f(N) \geq (1 - o(1))\sqrt{N}$ (this is a nice exercise), but he was unable to improve on this. Over the next 60 years, the problem attracted the efforts of many researchers, but until recently, the best known lower bound was only $f(N) \geq N^\alpha$, where $\alpha \approx 0.8641$.

In November 2010, Guth and Katz proved that $f(N) = \Omega(N/\log N)$, determining the order of magnitude of $f(N)$ up to a factor of $\sqrt{\log N}$. Their proof uses an elegant geometrical reformulation of the problem due to Elekes and Sharir, the polynomial method, and the method of cell decompositions. We won't give their proof in this course, but we will prove some easier results which use the polynomial method in a similar way.

The eigenvalue method

Often, we can reformulate a problem in extremal combinatorics in terms of finding the maximum size of an independent set (or clique) in a certain graph. We can then tackle this problem by looking at the *eigenvalues* of certain linear operators associated with our graph, such as the *adjacency matrix*. Sometimes, we have to construct a linear operator with the eigenvalues we want.

There is also an intimate connection between the *expansion* properties of a graph, and the eigenvalues of its Laplacian matrix. If $c > 0$, we call a graph $G = (V, E)$ a *c-edge-expander* if any subset $S \subset V(G)$ with size $|S| \leq |V(G)|/2$ has

$$e(S, S^c) \geq c|S|.$$

In other words, the vertices in S have average out-degree at least c . The largest such c is called the *edge-expansion ratio* of G . It is (relatively) easy to see that if $d \geq 3$ is fixed, then almost every d -regular graph is a c_d -edge expander, for some $c_d > 0$ depending on d .¹ However, for a long time, no explicit constructions of arbitrarily large d -regular c -expander graphs (for fixed $d \in \mathbb{N}$ and $c > 0$) were known. (Such graphs have many applications in computer science, for

¹Formally, if we choose G uniformly at random from the set of all d -regular graphs on n vertices, then the probability that G is a c_d -edge-expander tends to 1 as $n \rightarrow \infty$.

example in the construction of sparse networks where there are ‘many’ vertex-disjoint paths between two given sets of vertices. We will cover some of these applications in the course; others can be found in the excellent survey article [3].)

It turns out that a bounded-degree graph is a good edge-expander if and only if its Laplacian matrix has a large ‘eigenvalue gap’. In 1973, Margulis used this connection between edge-expansion and eigenvalues, together with results from the representation theory of infinite groups, to give an explicit construction of arbitrarily large 8-regular graphs with edge-expansion ratio bounded away from zero. We will sketch his argument later on in the course.

There is also a close connection between graph eigenvalues and ‘discrepancy.’ Informally, a graph has small discrepancy if the density of edges between any two reasonably large subsets of its vertex-set is close to the expected number in a random graph of the same edge-density. Dense graphs with low discrepancy are known as ‘quasirandom graphs’; eigenvalue methods can be used to show that certain algebraically constructed graphs (e.g. Paley graphs) are ‘quasirandom’. For G a bounded-degree graph, it turns out that there is a rough equivalence between small discrepancy, a certain eigenvalue property, and the rapid convergence of the random walk on G . Graphs with these properties (in particular, the so-called ‘Ramanujan graphs’) have further applications in computer science: they can be used, for example, to reduce the number of random bits required to solve a decision problem using a randomized algorithm.

Using group structure

Many combinatorial problems are explicitly set up on groups, or can be moved into the setting of a group. For example, the power-set $\mathcal{P}(X)$ of a set X is an Abelian group under the symmetric difference operation. In such cases, *Fourier analysis* is often very useful. Why? The main reason is that the Fourier transform behaves very nicely with respect to *convolution*.

If G is a finite group, and S is a subset of G , the *characteristic function* of S is the Boolean function on G defined by:

$$1_S : G \rightarrow \{0, 1\}; \quad 1_S(x) = \begin{cases} 1 & \text{if } x \in S; \\ 0 & \text{if } x \notin S. \end{cases}$$

We can often gain useful information about a set S by analysing how various linear operators act on its characteristic function, 1_S . Similarly, we can gain useful information about the relationship between sets by looking at relations between their characteristic functions.

Given two functions $u, v : G \rightarrow \mathbb{C}$, we define their *convolution* $u * v$ by

$$u * v(x) = \sum_{y \in G} u(xy^{-1})v(y).$$

Taking the convolution of two functions on a group corresponds to thinking of the functions as linear combinations of group elements, and multiplying them together using the multiplication inherited from the group. Explicitly,

$$u * v = \left(\sum_{x \in G} u_x x \right) \left(\sum_{y \in G} v_y y \right) = \sum_{x, y \in G} u_x v_y (xy) = \sum_{x \in G} \left(\sum_{y \in G} u_{xy^{-1}} v_y \right) x.$$

As we will see, many combinatorial problems are closely related to the convolution of functions on a group G . For example:

- If $A, B \subset G$, then the set

$$AB := \{ab : a \in A, b \in B\}$$

is precisely the support of the convolution of the indicator functions of A and B :

$$AB = \{x \in G : (1_A * 1_B)(x) \neq 0\} =: \text{supp}(1_A * 1_B).$$

- The adjacency matrix of a Cayley graph on G acts on functions on G by convolving them with the characteristic function of the generating-set of the Cayley graph.

It turns out that the Fourier transform of the convolution of two functions is $|G|$ times the pointwise-product of their Fourier transforms. In other words, convolution in the original ('physical') space means pointwise-product in 'Fourier' space, so it is often easier to work in Fourier space.

Working with the Fourier transforms of functions which arise in combinatorial problems about sets often reveals useful information, which, when translated back into physical space, yields bounds on the sizes of the original sets.

One of the first applications of Fourier analysis was Roth's proof in 1956 that a subset of $\{1, 2, \dots, n\}$ containing no 3-term arithmetic progression has size $O(n/\log \log n)$. This is an example of a problem which can be 'moved' into the setting of the Abelian group \mathbb{Z}_N , where N is prime; one can then use Fourier analysis on \mathbb{Z}_N .

Sometimes, Fourier analysis fails to properly capture the 'structure' of a combinatorial problem. This is the case with Szemerédi's Theorem for arithmetic progressions of length 4 and higher:

Theorem 2 (Szemerédi's Theorem). *Let $k \in \mathbb{N}$ and let $\delta > 0$. If n is sufficiently large depending on k and δ , then any subset $S \subset \{1, 2, \dots, n\}$ with $|S| \geq \delta n$ contains an arithmetic progression of length k .*

The $n = 3$ case is implied by Roth's Theorem, but for $k \geq 4$, Fourier analysis fails to capture the structure associated with k -term progressions. Gowers developed a higher-order analogue of Fourier analysis in order to give a proof of Szemerédi's Theorem for $k \geq 4$. We will not cover higher-order Fourier analysis in this course, but the interested reader is referred to the paper of Gowers [2].

References

- [1] R. Ahlswede, L. H. Khachatrian, The complete intersection theorem for systems of finite sets, *European Journal of Combinatorics* Volume 18 (1997), pp. 125-136.
- [2] Gowers, W.T., A new proof of Szemerédi's theorem, *Geometric and Functional Analysis*, Volume 11, Issue 3 (2001), pp. 465-588.
- [3] Hoory, S., Linial, N., Wigderson, A., Expander graphs and their applications, *Bulletin of the American Mathematical Society*, Volume 43, Number 4, October 2006, pp. 439-561.