

The Polynomial Method

Algebraic Methods in Combinatorics, Lectures 8-10

February 25, 2011

1 Introduction

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 (these are called *algebraic varieties*). We try to understand the geometry of the objects by looking at these polynomials.

In combinatorial problems, we often have a field \mathbb{F} (usually either \mathbb{R} , or the finite field \mathbb{F}_q), and we are looking at a finite subset $S \subset \mathbb{F}^N$ with a certain property. We can often obtain combinatorial information about S by looking at multivariate polynomials over \mathbb{F} which vanish on all points of S .

What happens in the one-dimensional case, i.e. with subsets of \mathbb{F} ? If S is a finite subset of \mathbb{F} , then there is a polynomial in $\mathbb{F}[X] \setminus \{0\}$ of degree $|S|$, which vanishes on all of S , namely,

$$\prod_{s \in S} (X - s).$$

Conversely, we have the well-known

Theorem 1 (Factor theorem). *Let \mathbb{F} be a field. Any polynomial in $\mathbb{F}[X] \setminus \{0\}$ with degree d has at most d roots in \mathbb{F} .*

So if S is a finite subset of \mathbb{F} , then $|S|$ is equal to the smallest possible degree of a polynomial in $\mathbb{F}[X] \setminus \{0\}$ which vanishes on all of S .

A higher-dimensional analogue of the Factor theorem turns out to be useful in combinatorics. If \mathbb{F} is a field, and $P \in \mathbb{F}[X_1, \dots, X_N]$ is a multivariate polynomial over \mathbb{F} , the X_i -degree of P (written $\deg_{X_i}(P)$) is the highest power of X_i occurring in any monomial of P . [The *total degree* of P is the degree of the polynomial $P(X, X, \dots, X)$ in X .] The analogue is as follows:

Lemma 2 (Alon-Tarsi). *Let \mathbb{F} be a field, and let $P \in \mathbb{F}[X_1, \dots, X_N] \setminus \{0\}$ be a non-trivial polynomial. Suppose $S_1, \dots, S_N \subset \mathbb{F}$ with $|S_i| > \deg_{X_i}(P)$. Then P cannot vanish on all of $S_1 \times S_2 \times \dots \times S_k$.*

Proof. By induction on N (using the Factor theorem). For $N = 1$, the statement of the lemma is precisely the Factor theorem. Assume the lemma holds for $N - 1$; we will prove it for N . Suppose $P = P(X_1, \dots, X_N) \in \mathbb{F}[X_1, \dots, X_N]$ vanishes on all of $S_1 \times S_2 \times \dots \times S_N$, where $|S_i| > d_i := \deg_{X_i}(P)$ for each $i \in [N]$. We must show that P is the zero polynomial. Write P as a polynomial in X_1 :

$$P = \sum_{j=0}^{d_1} X_1^j P_j(X_2, \dots, X_N).$$

Observe that for any $(s_2, \dots, s_N) \in S_2 \times \dots \times S_N$, the polynomial

$$P(X_1, s_2, \dots, s_N) = \sum_{j=1}^{d_1} X_1^j P_j(s_2, \dots, s_N) \in \mathbb{F}[X_1]$$

vanishes on all of S_1 . Since it has degree $d_1 < |S_1|$, it must be the zero polynomial, by the Factor theorem. Hence, $P_j(s_2, \dots, s_N) = 0$ for all $(s_2, \dots, s_N) \in S_2 \times \dots \times S_N$. By the induction hypothesis, it follows that each P_j is the zero polynomial, so P is the zero polynomial, completing the proof. \square

Remark. *Alon's Combinatorial Nullstellensatz, which we will encounter later, obtains the same conclusion under weaker hypotheses.*

2 The Kakeya Problem

A *Besicovitch set* in \mathbb{R}^2 is a closed, bounded subset of \mathbb{R}^2 containing a unit line segment in every direction. We start with the following

Question. *What is the minimum possible Lebesgue measure of a Besicovitch set in \mathbb{R}^2 ?*

Clearly, the disc of radius $1/2$ is a Besicovitch set of area $\pi/4$. One can get a Besicovitch set of area $\pi/8$ using a *deltoid*. This is the closed curve traced out by a fixed point on the circumference of a small circle, when the small circle is rolled around the inside of the circumference of a large circle with three times the diameter, without slipping. Taking the small circle to have diameter $1/2$, the deltoid encloses an area of $\pi/8$, and the tangent to the deltoid at any point has length exactly 1 inside the deltoid.

In fact, Besicovitch proved the following:

Theorem 3 (Besicovitch). *There exists a Besicovitch set in \mathbb{R}^2 with Lebesgue measure zero.*

For a short proof of this, the reader is encouraged to consult the notes by Ben Green at

<http://www.dpmms.cam.ac.uk/~bjg23/rkp.html>

On the other hand, Davies proved that Besicovitch sets in \mathbb{R}^2 are necessarily 2-dimensional, both in the sense of Minkowski dimension and Hausdorff dimension (see Appendix).

What happens in higher dimensions? We define a *Besicovitch set* in \mathbb{R}^N to be a closed, bounded subset of \mathbb{R}^N containing a unit line segment in every direction. By taking the Cartesian product of $[0, 1]^{N-2}$ with a Besicovitch set in \mathbb{R}^2 with measure 0, we can obtain a Besicovitch set in \mathbb{R}^N with measure 0. It is natural to conjecture that Besicovitch sets in \mathbb{R}^N are necessarily N -dimensional, but this is open for all $N \geq 3$:

Conjecture 1 (The Kakeya conjecture). *A Besicovitch set in \mathbb{R}^N has Hausdorff dimension N , and Minkowski dimension N .*

This is one of the most famous unsolved problems in geometric measure theory. It turns out to have connections to additive combinatorics, Fourier analysis and partial differential equations; for more details, see the survey [1] by Tao.

In an effort to make headway on Conjecture 1, Wolff proposed a *finite field analogue*.

Definition. *Let F be a finite field, and let $N \in \mathbb{N}$. A Kakeya set in \mathbb{F}^N is a subset $S \subset \mathbb{F}^N$ containing a line in every direction, i.e., for every $v \in \mathbb{F}^N \setminus \{0\}$, there exists $a \in \mathbb{F}^N$ such that $a + tv \in S$ for all $t \in \mathbb{F}$.*

Conjecture 2 (Finite field Kakeya conjecture, Wolff, 1999). *Let $E \subset \mathbb{F}^N$ be a Kakeya set. Then $|E| \geq c_N |\mathbb{F}|^N$, for some $c_N > 0$ depending upon N alone.*

We think of N as being fixed and small, and $|\mathbb{F}| \rightarrow \infty$; the above conjecture says that a Kakeya set must occupy at least a constant fraction of \mathbb{F}^N .

The finite field problem avoids all the technical issues involving the Minkowski and Hausdorff dimensions, so serves as a simpler ‘model’ for the original Kakeya problem. The finite field Kakeya conjecture was proved by Dvir in 2009, using a beautifully simple application of the polynomial method.

The proof is in two steps: first, one observes that if \mathbb{F} is any field, and $S \subset \mathbb{F}^N$ is any ‘small’ set, then there exists a polynomial $P \in \mathbb{F}[X_1, \dots, X_N] \setminus \{0\}$, which has ‘low’ total degree, and vanishes on all of S . Secondly, one shows that a polynomial in $\mathbb{F}[X_1, \dots, X_N]$ which has ‘low’ total degree, and which vanishes on all of a Kakeya set, must be the zero polynomial. Combining these two facts shows that a Kakeya set cannot be ‘small’.

The first step is an easy dimension-counting argument:

Lemma 4. *Let \mathbb{F} be any field (not necessarily finite). If $S \subset \mathbb{F}^N$ is a finite set, and d is an integer such that $|S| < \binom{N+d}{N}$, then there exists a polynomial in $\mathbb{F}[X_1, \dots, X_N] \setminus \{0\}$ which has total degree at most d , and vanishes on all of S .*

Remark. *The $N = 1$ case of this lemma is simply that for any subset $S \subset \mathbb{F}$, there is a polynomial in $\mathbb{F}[X] \setminus \{0\}$ of degree at most $|S|$, which vanishes on all of S . The lemma implies that if N is fixed, then for any $S \subset \mathbb{F}^N$, there is a non-trivial polynomial of total degree at most $O_N(|S|^{1/N})$ which vanishes on all of S . In the language of algebraic geometry, any set $S \subset \mathbb{F}^N$ is contained in an algebraic variety which is the zero-set of a polynomial of total degree $O_N(|S|^{1/N})$.*

Proof. Let W denote the \mathbb{F} -vector space of all polynomials in $\mathbb{F}[X_1, \dots, X_N]$ with total degree at most d . Note that

$$\dim(W) = \binom{N+d}{N},$$

since W has a basis consisting of the set of all monomials in X_1, \dots, X_N of total degree at most d , and there are

$$\binom{N+d}{N}$$

of these. (Indeed, they are in 1-1 correspondence with sequences of d ‘dots’ and N ‘lines’, with the number of dots between the $(i-1)$ th and the i th lines being

the power of X_i in the corresponding monomial.) Consider the linear map R taking a polynomial in W to the corresponding function on S :

$$\begin{aligned} R : W &\rightarrow \mathbb{F}^S; \\ P &\mapsto (P(s))_{s \in S}. \end{aligned}$$

Since $\dim(W) > \dim(\mathbb{F}^S) = |S|$, $\ker(R) \neq \{0\}$, so there exists a polynomial in $W \setminus \{0\}$ which vanishes on all of S , as required. \square

Remark. *More generally, if S is a finite subset of \mathbb{F}^N , and W is any subspace of $\mathbb{F}[X_1, \dots, X_N]$ with dimension $\dim(W) > |S|$, then there exists a polynomial $P \in W \setminus \{0\}$ which vanishes on all of S . This can be used to show that in \mathbb{R}^2 , any two points are contained in a unique line (take $W = \text{Span}\{1, X, Y\}$); any three points are contained in a unique line or circle (take $W = \text{Span}\{1, X, Y, X^2 + Y^2\}$), and any five points are contained in a unique conic section, possibly degenerate (take $W = \text{Span}\{1, X, Y, X^2, Y^2, XY\}$).*

The second step is as follows:

Lemma 5. *Let \mathbb{F} be a finite field, and suppose $P \in \mathbb{F}[X_1, \dots, X_N] \setminus \{0\}$ has total degree less than $|\mathbb{F}|$. Then P cannot vanish on all of a Kakeya set.*

Remark. *In the language of algebraic geometry, the algebraic variety $\{P = 0\}$ cannot contain a Kakeya set, intuitively because it does not bend back and forth enough times.*

Proof. Let $E \subset \mathbb{F}^N$ be a Kakeya set. Suppose $P \in \mathbb{F}[X_1, \dots, X_N]$ has total degree less than $|\mathbb{F}|$, and vanishes on all of E . We must show that P is the zero polynomial.

Suppose otherwise. Write $P = \sum_{i=0}^d P_i$, where P_i is the i th homogeneous component¹ of P , and d is the total degree of P . By assumption, $1 \leq d < |\mathbb{F}|$. Let $v \in \mathbb{F}^N \setminus \{0\}$ be an arbitrary direction. Since E is a Kakeya set, there exists $a \in \mathbb{F}^N$ such that $a + tv \in E$ for all $t \in \mathbb{F}$. Hence, $P(a + tv) = 0$ for all $t \in \mathbb{F}$. Consider the polynomial

$$q(T) := P(a + Tv) = p(a_1 + Tv_1, a_2 + Tv_2, \dots, a_N + Tv_N) \in \mathbb{F}[T];$$

note that q has degree $d < |\mathbb{F}|$. But q vanishes on all of $|\mathbb{F}|$, so it must be the zero polynomial, by the Factor theorem. In particular, its T^d -coefficient, which is precisely $P_d(v)$, must be zero. Hence, $P_d(v) = 0$ for all $v \in \mathbb{F}^N \setminus \{0\}$.

Since $d \geq 1$, and P_d is homogeneous of degree d , we obviously have $P_d(0) = 0$ as well, so P_d vanishes on all of \mathbb{F}^N . By the Alon-Tarsi lemma, it follows that P_d is the zero polynomial, a contradiction. \square

It does not seem possible to use the polynomial method in the original ‘Euclidean’ Kakeya problem, which remains open for $N \geq 3$. However, the polynomial method was used in a similar way to tackle the *lines/joints problem* in \mathbb{R}^k .

¹Recall that a polynomial is said to be *i-homogeneous* if all its monomials have total degree i .

3 The lines/joints problem

This is a problem from combinatorial geometry. Let L be a set of lines in \mathbb{R}^3 . A *joint* of L is a point $x \in \mathbb{R}^3$ such that the lines of L going through x do not all lie in a single plane — in other words, we can find three lines in L that go through x , and whose unit direction-vectors span \mathbb{R}^3 . Chazelle et al asked for a determination of the maximum possible number of joints of a set of n lines in \mathbb{R}^3 .

The problem has an obvious generalization to higher dimensions. If L is a set of lines in \mathbb{R}^k , a *joint* of L is defined to be a point $x \in \mathbb{R}^k$ such that the lines of L going through x do not all lie in some $(k-1)$ -dimensional hyperplane — i.e., we can find k lines in L that go through x , and whose unit direction vectors span \mathbb{R}^k . We are interested in the following

Question. *What is the maximum possible number of joints of a set of n lines in \mathbb{R}^k ?*

(We write $f_k(n)$ for this maximum.) Note that the question is uninteresting for $k=2$: by taking a set of n lines such that each pair of lines meet at a different point, we see that $f_2(n) = \binom{n}{2}$ for all n . For $k=3$, however, the problem is already non-trivial.

The ‘grid’ supplies us with a lower bound on $f_k(n)$. Take an $a \times a \times \dots \times a$ grid in \mathbb{R}^k , and let L be the set of all ka^{k-1} axis-parallel lines. The joints of L are precisely the a^k points of the grid. Therefore, if $n = ka^{k-1}$, we have

$$f_k(n) \geq (n/k)^{k/(k-1)},$$

so

$$f_k(n) \geq \Omega_k(n^{k/(k-1)}).$$

In the other direction, we have the following

Theorem 6 (Kaplan-Sharir-Shustin / Quilodrán, 2009).

$$f_k(n) \leq 4^{k/(k-1)} (k!)^{1/(k-1)} n^{k/(k-1)}.$$

Hence, $f_k(n) = \Theta_k(n^{k/(k-1)})$. It would be interesting to determine whether the grid is asymptotically best possible.

The proof of Theorem 6 is one of the most beautiful applications of the polynomial method in combinatorial geometry. Again, it proceeds in two steps. Suppose L is a set of n lines in \mathbb{R}^k , and J is the set of its joints; write $|J| = m$. Firstly, we will observe from Lemma 4 that if J is *any* set of m points in \mathbb{R}^k , then there exists a polynomial $P \in \mathbb{R}[X_1, \dots, X_k] \setminus \{0\}$ which vanishes on all of J , and has total degree at most $d(m) = O_k(m^{1/k})$. Secondly, we will prove that no polynomial in $\mathbb{R}[X_1, \dots, X_k] \setminus \{0\}$ with total degree at most $m/(2n)$ can vanish on all the joints of a set of n lines. It will follow immediately that $m/(2n) < O_k(m^{1/k})$, and therefore $m < O_k(n^{k/(k-1)})$.

Proof. Let J be any set of m points in \mathbb{R}^k . By Lemma 4, provided $d \in \mathbb{N}$ is such that

$$\binom{k+d}{k} > m,$$

there exists $P \in \mathbb{R}[X_1, \dots, X_k] \setminus \{0\}$ with total degree most d , and which vanishes on all of J . Note that

$$\binom{k+d}{k} > m \Leftrightarrow d^k/k! \geq m \Leftrightarrow d \geq \lceil (mk!)^{1/k} \rceil,$$

so we may take $d \leq 2(mk!)^{1/k}$.

Now let L be a set of n lines in \mathbb{R}^k , and let J be the set of its joints; write $|J| = m$. We first produce a subset $L' \subset L$ and a subset $J' \subset J$ such that any line in L' contains more than $m/(2n)$ points of J' , and each point of J' is a joint of L' . To do this, we perform the following iterative process. Let $L_0 = L$, and let $J_0 = J$. At stage i , if there exists a line $\ell \in L_i$ which is incident with at most $m/(2n)$ points of J_i , delete ℓ from L_i , producing L_{i+1} , and delete all the points of J_i which are incident with ℓ , producing J_{i+1} . Repeat this process as long as there exists a line in L_i incident with at most $m/(2n)$ points in J_i . When the process stops (at stage N , say), we have deleted at most $m/2$ points from J , so some lines remain. Let $L = L_N$, the set of remaining lines, and let $J' = J_N$, the set of remaining points. Each point of J' is then a joint of L' , and each line in L' is incident with more than $m/(2n)$ points of J' , as desired.

Now let $P \in \mathbb{R}[X_1, \dots, X_k]$ be a polynomial of total degree at most $m/(2n)$ which vanishes on all of J' . We must show that P is the zero polynomial. First, we claim that P must vanish on all of each line in L' . Indeed, let $\ell \in L'$, and parameterize ℓ by

$$\{a + tv : t \in \mathbb{R}\},$$

where v is the unit direction vector of ℓ , and a is any point on ℓ . Since ℓ is incident with more than $m/(2n)$ points of J' , the polynomial

$$q(T) := P(a + Tv) = P(a_1 + Tv_1, a_2 + Tv_2, \dots, a_k + Tv_k) \in \mathbb{R}[T]$$

has more than $m/(2n)$ roots. But it has degree at most $m/(2n)$, so by the Factor theorem, it must be the zero polynomial. Hence, P vanishes on all of ℓ , as claimed.

Next, we use this to show that each of the first-order partial derivatives of P must also vanish on all of J' . Indeed, take any $a \in J'$. Let ℓ_1, \dots, ℓ_k be k lines of L' going through a , not all lying in any $(k-1)$ -dimensional hyperplane. Take one of these lines, ℓ_1 say, and parameterize it by

$$\{a + tv : t \in \mathbb{R}\},$$

as before. Observe that

$$P(a + tv) = P(a) + t\langle(\nabla P)(a), v\rangle + O(t^2),$$

where

$$\nabla P := \left(\frac{\partial P}{\partial x_i} \right)_{1 \leq i \leq k}.$$

Since P vanishes on all of ℓ_1 , we have $P(a + tv) = 0$ for every $t \in \mathbb{R}$, so

$$t\langle(\nabla P)(a), v\rangle + O(t^2) = 0 \quad \forall t \in \mathbb{R}.$$

Taking t to be sufficiently small, it follows that $\langle(\nabla P)(a), v\rangle = 0$, i.e. the vector of first-order partial derivatives at a is orthogonal to v . Repeating this argument

for each of the lines ℓ_1, \dots, ℓ_k (whose unit direction-vectors span \mathbb{R}^k), we see that $(\nabla P)(a) = 0$. This holds for every $a \in J'$, so ∇P vanishes on all of J' . Hence, for each $i \in [k]$, $\frac{\partial P}{\partial x_i}$ vanishes on all of J' , as claimed.

Like P , $\frac{\partial P}{\partial x_i}$ is a polynomial in $\mathbb{R}[X_1, \dots, X_k]$ of total degree at most $m/(2n)$. Clearly, we can repeat the above argument for all the higher-order partial derivatives of P , showing that they all vanish on all of J' . This implies that P must be the zero-polynomial: otherwise, the partial derivative corresponding to a monomial of maximum total degree would be a non-zero constant.

It follows that $m/(2n) < d(m) \leq 2(mk!)^{1/k}$. Rearranging, we obtain

$$m \leq 4^{k/(k-1)}(k!)^{1/(k-1)}n^{k/(k-1)},$$

proving the theorem. \square

4 Alon's Combinatorial Nullstellensatz

It turns out that the conclusion of the Alon-Tarsi lemma holds under a weaker hypothesis. This is the content of Alon's Combinatorial Nullstellensatz, which is useful in a variety of applications in combinatorics.

Theorem 7 (Combinatorial Nullstellensatz). *Let \mathbb{F} be a field, let $S_1, S_2, \dots, S_N \subset \mathbb{F}$, and let $P \in \mathbb{F}[X_1, \dots, X_N]$ be a polynomial. Suppose there exist integers $t_1, \dots, t_N \geq 0$ such that the coefficient of $X_1^{t_1} \dots X_N^{t_N}$ in P is non-zero, P has total degree $\sum_{i=1}^N t_i$, and $|S_i| > t_i$ for each $i \in [N]$. Then P cannot vanish on all of $S_1 \times S_2 \times \dots \times S_N$, i.e. there exist $s_i \in S_i$ such that*

$$P(s_1, \dots, s_n) \neq 0.$$

Proof. We prove this by induction on $\sum_{i=1}^N t_i$. It is clearly true when $\sum_{i=1}^N t_i = 0$, as then P is a non-zero constant. Let P , (S_i) , and (t_i) be as above, and suppose that the theorem holds for all smaller values of $\sum_{i=1}^N t_i$. Suppose for a contradiction that P vanishes on all of $S_1 \times \dots \times S_N$.

Without loss of generality, we may assume that $t_1 > 0$. Take any $a \in S_1$. It is easy to see that we may write

$$P = (X_1 - a)Q + R,$$

where $Q \in \mathbb{F}[X_1, X_2, \dots, X_n]$, and $R \in \mathbb{F}[X_2, \dots, X_N]$. Since P vanishes on all of $\{a\} \times S_2 \times S_3 \times \dots \times S_N$, R vanishes on all of $S_2 \times S_3 \times \dots \times S_N$. Since P and R both vanish on all of $(S_1 \setminus \{a\}) \times S_2 \times S_3 \times \dots \times S_n$, so does Q .

Note that the coefficient of $X_1^{t_1-1} X_2^{t_2} \dots X_n^{t_n}$ in Q is non-zero, and Q has total degree $(\sum_{i=1}^n t_i) - 1$. Hence, we may apply the induction hypothesis to Q with $t_1 - 1, t_2, \dots, t_N$. It follows that there exists $(s_1, s_2, \dots, s_N) \in (S_1 \setminus \{a\}) \times S_2 \times \dots \times S_N$ such that $Q(s_1, s_2, \dots, s_N) \neq 0$. But then

$$P(s_1, \dots, s_N) = (s_1 - a)Q(s_1, \dots, s_N) + R(s_1, \dots, s_N) \neq 0,$$

a contradiction. This proves the theorem. \square

The Combinatorial Nullstellensatz is usually applied in the following way. To obtain combinatorial information about sets with a certain property, we take

an arbitrary set with this property, and use it to build a polynomial P which vanishes on some Cartesian product $S_1 \times S_2 \times \dots \times S_N$. The fact that the polynomial P and the sets (S_i) cannot satisfy the hypotheses of the Nullstellensatz yields combinatorial information about the original set.

For example, Alon and Füredi applied the Combinatorial Nullstellensatz to answer the following

Question (Komjáth). *What is the minimum number of hyperplanes in \mathbb{R}^n needed to cover all points of the unit cube $\{0, 1\}^n$ except one (which must be uncovered)?*

Without loss of generality, we may assume that 0 is the uncovered point. Clearly, n hyperplanes suffice: we may take $\{x : x_i = 1\}$ ($1 \leq i \leq n$). Alon and Füredi proved that this is best possible:

Theorem 8 (Alon-Füredi, 1993). *Let H_1, \dots, H_m be a family of hyperplanes in \mathbb{R}^n that cover all vertices of $\{0, 1\}^n$ except for one (which is uncovered). Then $m \geq n$.*

Proof. Let H_1, \dots, H_m be as in the statement of the theorem. We may assume that 0 is the uncovered point. Let $\langle \cdot, \cdot \rangle$ denote the usual inner product on \mathbb{R}^n . Let $\langle x, a^{(j)} \rangle = b^{(j)}$ be the equation defining the hyperplane H_j . Then $b^{(j)} \neq 0$ for each j , since 0 is uncovered. Consider

$$P(x) = \prod_{j=1}^m (\langle x, a^{(j)} \rangle - b^{(j)}) - (-1)^m \left(\prod_{j=1}^m b^{(j)} \right) \left(\prod_{i=1}^n (1 - x_i) \right),$$

which we think of as a polynomial in x_1, \dots, x_n . Observe that P vanishes on all of $\{0, 1\}^n$. Indeed, since H_1, \dots, H_m cover $\{0, 1\}^n \setminus \{0\}$, we also have $P(x) = 0$ for all $x \in \{0, 1\}^n \setminus \{0\}$, and by the choice of the second term, we also have $P(0) = 0$.

Assume for a contradiction that $m < n$. Then P has total degree n , and the coefficient of $\prod_{i=1}^n x_i$ is

$$(-1)^{n+m+1} \prod_{j=1}^m b^{(j)} \neq 0.$$

Hence, applying the Combinatorial Nullstellensatz with $t_i = 1$ and $S_i = \{0, 1\}$ for each $i \in [n]$, we see that there exists $y \in \{0, 1\}^n$ such that $P(y) \neq 0$, a contradiction. \square

Sumsets in \mathbb{Z}_p

In additive combinatorics, we are interested in the combinatorial properties of finite subsets of Abelian groups. A basic problem is to find lower bounds on the size of *sumsets* in Abelian groups. If Z is an Abelian group, and $A, B \subset Z$, we define the sumset

$$A + B = \{a + b : a \in A, b \in B\}.$$

Given two finite sets $A, B \subset Z$, how small can $A + B$ be?

One of the oldest results in this direction is the Cauchy-Davenport theorem, which gives a sharp lower bound on the size of sumsets in \mathbb{Z}_p , where p is a prime:

Theorem 9 (Cauchy-Davenport). *If p is prime, and $A, B \subset \mathbb{Z}_p$, then*

$$|A + B| \geq \min\{|A| + |B| - 1, p\}.$$

Remark. *When $|A| + |B| > p$, the theorem is trivial: in this case, for any $x \in \mathbb{Z}_p$, the sets A and $x - B$ intersect, so $A + B = \mathbb{Z}_p$. It is sharp for all values of $|A|$ and $|B|$. Indeed, if $|A| + |B| \leq p$, taking $A = \{0, 1, 2, \dots, |A| - 1\}$ and $B = \{0, 1, 2, \dots, |B| - 1\}$ gives $A + B = \{0, 1, 2, \dots, |A| + |B| - 2\}$.*

Davenport rediscovered this theorem 122 years after Cauchy had first proved it. They gave essentially the same proof, by induction on $|B|$. Alon, Nathanson and Ruzsa gave an entirely different, algebraic proof, using the Combinatorial Nullstellensatz.

Proof. Let $A, B \subset \mathbb{Z}_p$. By the remark above, we may assume that $|A| + |B| \leq p$. Suppose for a contradiction that $|A + B| \leq |A| + |B| - 2$. Let $E \subset \mathbb{Z}_p$ such that $A + B \subset E$ and $|E| = |A| + |B| - 2$. Consider the polynomial:

$$P(X, Y) = \prod_{e \in E} (X + Y - e) \in \mathbb{Z}_p[X, Y].$$

By construction, $P(a, b) = 0$ for all $a \in A$, $b \in B$. Put $t_1 = |A| - 1$, $t_2 = |B| - 1$. Observe that P has total degree $t_1 + t_2$, and that the coefficient of $X^{t_1}Y^{t_2}$ in P is

$$\binom{|A| + |B| - 2}{|A| - 1},$$

which is $\neq 0 \pmod{p}$, since $|A| + |B| - 2 \leq p - 2 < p$. Therefore, applying the Combinatorial Nullstellensatz with $n = 2$, $S_1 = A$ and $S_2 = B$, we see that there exists $a \in A$, $b \in B$ such that $P(a, b) \neq 0$, a contradiction. \square

What happens if we consider *restricted* sumsets? If Z is an Abelian group, and $A, B \subset Z$, we define the *restricted sumset*

$$A \dot{+} B = \{a + b : a \in A, b \in B, a \neq b\},$$

i.e. we are only allowed to sum distinct elements. Erdős and Heilbronn made the following

Conjecture 3 (Erdős-Heilbronn, 1964). *If $A \subset \mathbb{Z}_p$, then*

$$|A \dot{+} A| \geq \min\{2|A| - 3, p\}.$$

In other words, when we restrict to summing distinct elements, the Cauchy-Davenport bound changes by at most 2.

Remark. *Conjecture 3 is trivial when $p = 2$, and also when $2|A| - 3 \geq p$. Indeed, if $p > 2$ and $2|A| - 3 \geq p$, then $A \dot{+} A = \mathbb{Z}_p$, since*

$$(x - A) \cap (A \setminus \{2^{-1}x\}) \neq \emptyset \quad \forall x \in \mathbb{Z}_p.$$

Note that Conjecture 3 is sharp for all values of $|A|$ and $|B|$. Indeed, if $2|A| + 3 \leq p$, taking $A = \{0, 1, \dots, |A| - 1\}$ gives $A \dot{+} A = \{1, 2, \dots, 2|A| - 3\}$.

Conjecture 3 remained open for thirty years. It was first proved by Dias da Silva and Hamidoune in 1994, using an exterior algebra method, together with results from the representation theory of the symmetric group. Alon, Nathanson and Ruzsa found a much simpler proof, using the Combinatorial Nullstellensatz. They deduced it from the following

Theorem 10. *Let $A, B \subset \mathbb{Z}_p$ with $|A| \neq |B|$. Then*

$$|A \dot{+} B| \geq \min\{|A| + |B| - 2, p\}.$$

This immediately implies a strengthening of Conjecture 3:

Corollary 11. *Let $A, B \subset \mathbb{Z}_p$. Then*

$$|A \dot{+} B| \geq \min\{|A| + |B| - 3, p\}.$$

Proof. If $|A| = |B|$, delete any element from B and apply Theorem 10. \square

Proof of Theorem 10: By a similar argument to that above, we may assume that $|A| + |B| \leq p + 2$. If $|B| \leq 1$, then the theorem is trivial, so we may assume that $|B| \geq 2$.

Suppose for a contradiction that $|A \dot{+} B| \leq |A| + |B| - 3$. Let $E \subset \mathbb{Z}_p$ such that $A \dot{+} B \subset E$ and $|E| = |A| + |B| - 3$. Consider the polynomial:

$$P(X, Y) = (X - Y) \prod_{e \in E} (X + Y - e) \in \mathbb{Z}_p[X, Y].$$

By construction, $P(a, b) = 0$ for all $a \in A$, $b \in B$. Put $t_1 = |A| - 1$, $t_2 = |B| - 1$. Observe that P has total degree $t_1 + t_2$, and that the coefficient of $X^{t_1} Y^{t_2}$ in P is

$$\binom{|A| + |B| - 3}{|A| - 2} - \binom{|A| + |B| - 3}{|A| - 1} = \frac{|A| - |B|}{|B| - 1} \binom{|A| + |B| - 3}{|A| - 1},$$

which is $\neq 0 \pmod{p}$, since $|A| + |B| - 3 \leq p - 1$. Therefore, applying the Combinatorial Nullstellensatz with $n = 2$, $S_1 = A$ and $S_2 = B$, we see that there exists $a \in A$, $b \in B$ such that $P(a, b) \neq 0$, a contradiction. \square

Appendix: A brief discussion of the Minkowski and Hausdorff dimensions

The Minkowski dimension

The Minkowski dimension measures the dimension of a bounded subset $S \subset \mathbb{R}^N$ by looking at how many boxes of small side-length are needed to cover S .

If $\delta > 0$, and $S = [-r, r]^d$, then the number of boxes of side-length δ required to cover S is $(2r)^d / \delta^d$, which grows like $(1/\delta)^d$. Note that

$$\frac{\log((2r)^d / \delta^d)}{\log(1/\delta)} \rightarrow d \quad \text{as } \delta \rightarrow 0.$$

This motivates the definition of Minkowski dimension. If $S \subset \mathbb{R}^N$ is bounded, and $\delta > 0$, let $N_\delta(S)$ be the number of boxes of side-length δ in \mathbb{R}^N which are needed to cover S . Now define

$$\dim_M(S) = \lim_{\delta \rightarrow 0} \frac{\log(N_\delta(S))}{\log(1/\delta)},$$

if this limit exists. This is called the *Minkowski dimension* of S ; it is a real number between 0 and N .

The limit above does not always exist, even for compact subsets of \mathbb{R} . If it does not, we define the *upper* and *lower Minkowski dimensions* of S to be

$$\overline{\dim}_M(S) = \limsup_{\delta \rightarrow 0} \frac{\log(N_\delta(S))}{\log(1/\delta)},$$

and

$$\underline{\dim}_M(S) = \liminf_{\delta \rightarrow 0} \frac{\log(N_\delta(S))}{\log(1/\delta)},$$

respectively.

If $S \subset \mathbb{R}^N$ is unbounded, and the Minkowski dimension is defined for all bounded subsets of S , then we define

$$\dim_M(S) = \max\{\dim_M(S') : S' \subset S, S' \text{ is bounded}\}.$$

Observe that the Minkowski dimension of \mathbb{R}^d is d . Indeed, let S' be a bounded subset of \mathbb{R}^d ; then S' is contained within $[-r, r]^d$, for some $r > 0$, and therefore

$$N_\delta(S') \leq (2r)^d (1/\delta)^d.$$

Hence,

$$\frac{\log(N_\delta(S'))}{\log(1/\delta)} \leq \frac{d \log(2r) + d \log(1/\delta)}{\log(1/\delta)} \rightarrow d \quad \text{as } \delta \rightarrow 0,$$

and therefore $\dim_M(S') \leq d$ for any bounded subset $S' \subset S$. On the other hand, $\dim_M([0, 1]^d) = d$, and therefore $\dim_M(\mathbb{R}^d) = d$.

The Minkowski dimension respects finite unions, meaning that for any $S_1, \dots, S_l \subset \mathbb{R}^N$,

$$\dim_M \left(\bigcup_{i=1}^l S_i \right) = \max\{\dim_M(S_i) : i \in [l]\},$$

whenever these exist. However, it does not respect countable unions: for example, the rationals have Minkowski dimension 1. The Hausdorff measure *is* countably additive, however...

The Hausdorff dimension

The Hausdorff dimension measures the dimension of a subset $S \subset \mathbb{R}^N$ by looking at the smallest possible total ' d -dimensional measure' of a collection of small balls in \mathbb{R}^N which cover the set. To avoid minor technicalities, we will restrict our attention to Borel sets in \mathbb{R}^N .

To start off with, suppose we have a bounded, simple, closed curve $\gamma : [0, 1] \rightarrow \mathbb{R}^3$, and we want to estimate its length by looking at how easy it is to cover it with balls in \mathbb{R}^3 . We might try defining its length to be

$$\inf \left\{ \sum_{i=1}^l (2r_i) : \exists \text{ open balls of radii } r_1, r_2, \dots, r_l \text{ covering } \gamma \right\}.$$

But if the curve was tightly coiled, this would not work: we might be able to cover it with a single ball of diameter 1, and yet it could be very ‘long’. It could even be differentiable, with length

$$\int_0^1 \|\gamma'(t)\|_2 dt = 100. \quad (1)$$

We can get around this by restricting ourselves to using small balls. For any $\delta > 0$, define

$$L_\delta(\gamma) = \inf \left\{ \sum_{i=1}^l (2r_i) : r_i \leq \delta \forall i, \exists \text{ open balls of radii } r_1, r_2, \dots, r_l \text{ covering } \gamma \right\}.$$

Now define

$$L(\gamma) = \lim_{\delta \rightarrow 0} L_\delta(\gamma).$$

(Note that this may be infinite, even if γ is differentiable.) If γ is differentiable, we have

$$L(\gamma) = \int_0^1 \|\gamma'(t)\|_2 dt,$$

Now suppose that we have a compact surface $S \subset \mathbb{R}^3$. It is intuitively clear that its ‘length’, as defined above, will be infinite. Indeed, $\Omega(1/\delta^2)$ balls of radius δ are needed to cover S ; each has diameter 2δ , giving a total length of $\Omega(1/\delta)$. But if instead, we sum the *squares* of the diameters of a collection of balls of radii at most δ , covering S , we get a finite limit. For any $\delta > 0$, define

$$A_\delta(S) = \inf \left\{ \sum_{i=1}^l (2r_i)^2 : r_i \leq \delta \forall i, \exists \text{ open balls of radii } r_1, r_2, \dots, r_l \text{ covering } S \right\}.$$

Now define

$$A(S) = \lim_{\delta \rightarrow 0} A_\delta(S).$$

Of course, to get the genuine area, we would need to multiply $A(S)$ by $\pi/4$, but then we would get a definition that does not generalize as easily.

In general, we can define the ‘ d -dimensional measure’ of more complicated sets. If $S \subset \mathbb{R}^N$ is a Borel set, and d is any real number between 0 and N , we define

$$C_{d,\delta}(S) = \inf \left\{ \sum_{i=1}^{\infty} (2r_i)^d : r_i \leq \delta \forall i, \exists \text{ open balls of radii } r_1, r_2, \dots \text{ covering } S \right\}.$$

The above sum can be seen as the (scaled) total d -dimensional measure of the open balls. We define the *d -dimensional Hausdorff content* of S to be

$$C_d(S) = \lim_{\delta \rightarrow 0} C_{d,\delta}(S).$$

It can be proved that for any Borel set $S \subset \mathbb{R}^N$, there is a unique real number $x \in [0, N]$ such that

$$C_d(S) = \begin{cases} \infty & \text{if } d < x; \\ 0 & \text{if } d > x. \end{cases}$$

We define the *Hausdorff dimension* of S , $\dim_H(S)$, to be this real number x . It may not be an integer — for example, the Hausdorff dimension of the Cantor set is $(\log 3)/(\log 2)$.

It turns out that the Hausdorff dimension has many useful properties, and is particularly useful for studying fractals. Unlike the Minkowski dimension, it respects countable unions: for any Borel sets $S_1, S_2, \dots \subset \mathbb{R}^N$, we have

$$\dim_H \left(\bigcup_{i=1}^{\infty} S_i \right) = \sup \{ \dim_H(S_i) : i \in \mathbb{N} \}.$$

For an illuminating discussion, see the chapter on dimension in *The Princeton Companion to Mathematics*. For a more in-depth discussion of the Minkowski and Hausdorff dimensions, the reader may also visit Terence Tao's blog,

<http://terrytao.wordpress.com/2009/05/19/245c-notes-5-hausdorff-dimension-optional/>.

References

- [1] Tao, T., From Rotating Needles to Stability of Waves: Emerging Connections between Combinatorics, Analysis and PDE, *Notices of the American Mathematical Society*, Volume 48, Number 3 (March 2001), pp. 294-303.