The Polynomial Method

Jacob Denson

October 24, 2024

Table Of Contents

Chapter 1

Intro

The core techniques of the polynomial method are incredibly elementary, but can be used to solve questions which have stumped mathematicians for decades. The technique relies on the fact that polynomials are both a flexible family of objects, and also a very restricted family. Given any set of points, we can find a polynomial vanishing on that set. But on the other hand, the behaviour of a polynomial with low degree is very restricted. The interplay between these two properties is what makes the polynomial method click.

The first principle of the polynomial can be described using very basic ideas in linear algebra, known as *parameter counting*. Let $T : V \to W$ be a linear transformation with $\dim(W) < \dim(V)$. Then by the rank nullity theorem, the nullspace is nontrivial, so there must be $x \in V$ such that $T(x) = 0$. In particular, if V is a vector space of functions on some space X, we select some finite collection of points $x_1, \ldots, x_m \in X$, and we consider the evaluation map $T(f) = (f(x_1), \ldots, f(x_m))$, then provided $n > m$, there is a function $f \in V$ vanishing on the m points. Of course, since polynomials form an infinite dimensional vector space, this principle implies that for any finite collection of points, we can find a polynomial vanishing on them. But it is more interesting to finte a *low degree* polynomial vanishing on the set of points.

Theorem 1.1. *Given a finite set S, there is a polynomial with degree at most $n|S|^{1/n}$ vanishing on S.*

Proof. We let $\mathrm{Poly}(D, K^n)$ denote the vector space of polynomials we degree at most D defined on K^n. Now this vector space is spanned by the monomials $x_1^{m_1} \ldots x_n^{m_n}$ with $m_1 + \cdots + m_n \leqslant D$. To simplify the combinatorics, we homogenize, counting monomials $x_0^{m_0} \ldots x_n^{m_n}$ with $m_0 + \cdots + m_n = D$. But this is just the number of decompositions of D into $n+1$ equal parts, and so we conclude that

$$\dim\left(\mathrm{Poly}(D, K^n)\right) = \binom{D+n}{n} \geqslant \frac{D^n}{n!}$$

Provided that D is much greater than n, this is a good approximation to the dimension. In particular, given a finite set $S \subset K^n$, there exists a polynomial f with $\deg(f) \leqslant n|S|^{1/n}$ vanishing on S. This is tight to the bounds established above if $|S| \gg n$. □

One example of the restrictedness of polynomials is provided by the *vanishing lemma*, which implies polynomials vanishing on enough points on a line eventually lie on the entire line.

Theorem 1.2. *Let f be a polynomial vanishing on $\deg(f)+1$ points of a line. Then f vanishes on the entire line.*

Proof. Suppose $L = \{x + \lambda y : \lambda \in K\}$ is a line, for some $x, y \in K^n$. Then $f(x+\lambda y)$ is a one dimensional polynomial in λ with degree at most $\deg(f)$, with $\deg(f)+1$ zeroes. But this means that $f(x+\lambda y) = 0$ for all λ, so f vanishes on the entire line. □

We note that this remains true in the projective context. If f is a homogenous polynomial vanishing on more than $\deg(f)$ points of a projective line in $K\mathbf{P}^n$, then f vanishes on the entire projective line. This is easy to prove by reduction to the affine case using a change of coordinates.

1.1 Nikodym and Kakeya, and Joints

Despite the simplicity of the two principles we just described, they are enough to answer nontrivial questions. The statement of these theorems involves no mention of polynomials, but the proof we give uses the lemmas above. No proof without using polynomials is currently known.

A subset N of K^n is called a *Nikodym set* if, for any $x \in K$, there exists a line $L(x)$ through x such that $L(x) - \{x\} \subset N$. It is believed that any Nikodym set must be quite large. The main interest of Nikodym sets is in $\mathbf{R}^n$, where the problem becomes analytical. But as a testbed, we might want to consider the problem where K is a finite field with a large number of points, and then establishing that a Nikodym set is large becomes a purely combinatorial question.

Lemma 1.3. *If K is finite, f vanishes on K^n, and $\deg(f) < |K|$, then $f = 0$.*

Proof. We prove this theorem by induction. For $n = 1$, if f vanishes on K, the division algorithm gives that $X^{|K|} - 1$ divides f, which implies $\deg(f) \geqslant |K|$ unless $f = 0$. For an induction, write

$$f(x_1, \ldots, x_{n+1}) = \sum_k f_k(x_1, \ldots, x_n) x_{n+1}^k$$

For each value of $x_1, \ldots, x_n \in K$, $\sum_k f_k(x_1, \ldots, x_n) x_{n+1}^k$ is a polynomial in x_{n+1} vanishing everywhere, so by the base case, we conclude $f_k(x_1, \ldots, x_n) = 0$ for all $x_1, \ldots, x_n \in K$. And then by induction, $f_k = 0$. □

Theorem 1.4. *Any Nikodym set in a finite field K^n contains $\Omega_n |K|^n$ points.*

Proof. Let N be a Nikodym set. By parameter counting, we can find a non-zero polynomial f with $\deg(f) \leqslant n|N|^{1/n}$. If $x \in K^n$, then f vanishes completely on $L(x)$, except perhaps at

the point x. Suppose $n|N|^{1/n} < |K| - 1$. Since f vanishes on at least $|K| - 1$ points of $L(x)$, this means that f vanishes at x as well. Since x was arbitrary, f vanishes on every point of K^n. The last lemma then implies $f = 0$. Thus we have a contradiction unless $n|N|^{1/n} \geqslant |K| - 1$, so it must be true that

$$|N| \geqslant \left(\frac{|K| - 1}{n}\right)^n \geqslant |K|^n n^{-n}(1 - n|K|^{-1}) = \Omega_n |K|^n \qquad \square$$

In the finite field case, a set B in K^n is called a *Kakeya*, or *Besocovitch* set if it contains a line in every direction. That is, for every $y \in K^n$, there exists x such that the line $\{x + \lambda y : \lambda \in K\}$ is a subset of B. Just like Nikodym sets, in $\mathbf{R}^n$, Kakeya sets are conjectured to be very large in size, and we can verify this in the finite field case using the polynomial method.

Theorem 1.5. *A Kakeya set has $\Omega_n |K|^n$ elements.*

Proof. Let B be a Kakeya set. Construct a homogenous polynomial f in $K[x_0, \ldots, x_n]$ with degree at most $n|B|^{1/n}$ such that $f(1, x) = 0$ all $x \in B$. Assume f has the smallest degree such that it vanishes on B. Since B contains a line in every direction, we find $f(0, x) = 0$ for all $x \in B$. If we write $f(x) = f_0(x_1, \ldots, x_n) + x_0 f_1(x)$, then $f_0(x_1, \ldots, x_n) = 0$ for all $x_1, \ldots, x_n \in K$. Since $\deg(f_0) \leqslant \deg(f) \leqslant n|B|^{1/n}$, if $n|B|^{1/n} < |K|$, then $f_0 = 0$. This implies x_0 divides f. But then $x_0^{-1} f$ vanishes on B, contradicting the fact that f was minimal. This gives a contradiction, so we must have $n|B|^{1/n} \geqslant |K|$, so $|B| \geqslant |K|^n n^{-n}$. $\square$

If $\mathcal{L}$ is a family of lines in $\mathbf{R}^3$, a joint is a point lying at the intersection of three non coplanar lines. One might consider the maximum number of joints a family of lines with a fixed cardinality L might have. If we take an $S \times S \times S$ grid, and we consider the family of axis parallel lines passing through the gridpoints. Then there are $3S^2$ points, and each grid point is a joint, giving S^3 joints. Thus the number of joints is approximately $L^{3/2}$. To do slightly better, we can consider a generic set of S planes. These intersect in S choose 2 lines, and S choose 3 joints. If we take $S = 4$, we get a slightly better constant, but still asymptotically $L^{3/2}$. And we now prove this is the maximum one can obtain, up to a constant factor.

Lemma 1.6. *If $\mathcal{L}$ is a set of lines in $\mathbf{R}^3$ determining J joints, then one line contains fewer than $3J^{1/3}$ joints.*

Proof. Let f be a polynomial vanishing at every joint of $\mathcal{L}$, with degree at most $3J^{1/3}$. If every line contains more than $3J^{1/3}$ joints, then f vanishes on all of the lines. But then ∇f vanishes on all of the joints as wells. If we choose f to have minimal degree vanishing on the joints, this is impossible. $\square$

Theorem 1.7. *L lines determine at most $O(L^{3/2})$ joints.*

Proof. Let $J(L)$ denote the maximum joints from a set of L lines. If $\mathcal{L}$ is a set of L lines determining $J(L)$ joints, then one line contains fewer than $3J^{1/3}$ joints. If we remove this line, the remaining joints are formed by $L - 1$ lines, and so we obtain that $J(L) \leqslant 3J(L)^{1/3} + J(L - 1)$. Thus we obtain that $J(L) \leqslant 3LJ(L)^{1/3}$, and so $J(L) = O(L^{3/2})$. $\square$

This theorem easily generalizes to high dimensions. The analogy of Lemma 1.6 is that if lines in $\mathbf{R}^n$ determine J joints, then one line must have fewer than $nJ^{1/n}$ joints. This gives $J(L) \leqslant nJ(L)^{1/n} + J(L-1)$, and so $J(L) = O(nL^{1+1/n})$.

1.2 Exercises

Theorem 1.8. *Given a set of L m-planes in $\mathbf{R}^n$, we can find a polynomial with degree at most $2n^{n/(n-m)}L^{1/(n-m)}$ vanishing on the planes.*

Proof. Fix K, and form an orthogonal grid of K^m points on each plane. Then we can find a polynomial with degree at most $n(K^m L)^{1/n}$ vanishing on this grid. Provided that $n(K^m L)^{1/n} < K$, this polynomial must also vanish on all of the planes. It is possible to do this with $K \leqslant 2n^{n/(n-m)}L^{1/(n-m)}$, which gives a polynomial with degree at most $2n^{n/(n-m)}L^{1/(n-m)}$ vanishing on the set of planes. □

Theorem 1.9 (Schwarz-Zippel Lemma)**.** *Suppose $A_1, \ldots, A_n$ are finite subsets with $|A_k| \leqslant N$ for each k, and f is a polynomial with degree at most D. Then the number of zeroes of f in $A_1 \times \cdots \times A_n$ is at most DN^{n-1}.*

Proof. We prove by induction. For $n = 1$, the theorem is elementary. In general, if f has most that DN^{n-1} zeroes on $A_1 \times \cdots \times A_n$, then by pidgeonholing it must have more than DN^{n-2} zeroes on some line parallel to the n'th axis. But this is impossible by induction. □

Corollary 1.10. *In $\mathbf{R}^n$, $V(f)$ always has zero Lebesgue measure.*

Proof. We prove this by Riemann integration. Note that

$$|V(f) \cap [0,1]^n| = \int_{[0,1]^n} \mathbf{I}(f(x) = 0)\, dx$$

Now by the Schwarz-Zippel lemma,

$$\frac{1}{N^n} \sum_{m_1,\ldots,m_n=1}^{N} \mathbf{I}(f(m_1,\ldots,m_n) = 0) \leqslant \frac{DN^{n-1}}{N^n} = D/N$$

Thus, taking $N \to \infty$, we conclude that $|V(f) \cap [0,1]^n| = 0$. □

Chapter 2

Lecture

Given an irreducible polynomial f over an algebraically closed field, it is useful to find a large vector space containing functions not vanishing identically on $Z(f)$. Any polynomial which vanishes identically on $Z(f)$ is divisible by f. Furthermore, the dimension of the set of polynomials with degree at msot D which are divisible by f is $\binom{D-\deg f+n}{n}$, if $\deg f \leqslant D$. By linear algebra, given any linear map $L : V \to W$, we can decompose V as the direct sum of the kernel of L and a complementary subspace. Here, we can take $L(g) = g|_{Z(f)}$. Thus we get a space with dimension $\binom{D+n}{n} - \binom{D-\deg f+n}{n}$. Since $\binom{D+n}{n} \gtrsim_n D^n$, we find that we can find a space with dimension $\gtrsim (\deg f)D^{n-1}$.

Unfortunately, this doesn't work so well over the real numbers, so we have to look a little harder. If R is a commutative ring, and I is an idea, we say it is **real** if for every sequence $r_1, \ldots, r_n \in R$ for which $r_1^2 + \cdots + r_n^2 \in R$, $r_1, \ldots, r_n \in R$. A real ideal is radical, because if $n = 1$, and $r^{2N} \in R$, $r^N \in R$. Eventually we obtain that $r \in R$. Given an ideal I, the real radical of I is the set of all r such that there is $s_1, \ldots, s_n \in R$ such that $r^n + s_1^2 + \cdots + s_k^2 \in I$. The real nullstellensatz says that I is a real ideal if and only if $I(Z(I)) = \sqrt[R]{I}$.

There is a nice classification of irreducible polynomials which generate real ideals. One condition is that there exists $x \in Z(f)$ such that $\nabla f = 0$, and another is that f changes sign somewhere on $\mathbf{R}^n$.

Lemma 2.1. *Let f be a polynomial. Then there exists f' with degree smaller than f, $Z(f') \supset Z(f)$, and each irreducible component of f' generates a real ideal.*

Proof. We prove by induction on $\deg f$. Then we may assume f is irreducible. PROVE LATER. □

Chapter 3

Sphere

Spheres of arbitrary radius:

Forbidden configurations help. But not really many forbidden configurations here.

Thus number of spheres times number of points is sharp for incidences of points and spheres.

However, if no four points are co-circular, then there can be no four points incidents to two spheres simultaneously. Running the partitioning machine, we can guess that the polynomial partitioning result will give us the right result.

More generally, if we take a family of varieties and points, and assume there is no particular graph lying in the incidence graph of the situation. Then we can try and bound the number of incidences.

Unit distances in four dimensions:

Idea of Solymozi and Tao: Looks like problem one dimension lower than the one we started with.

Chapter 4

Distinct Distances

Distinct Distances

Erdos conjectured

d(P) ¿¿ N / (log N)$^{1/2}$

based on the integer lattice.

Sackely 97 shows d(P) ¿¿ N$^{0.8}$

Katz, Tardos 2004 shows d(P) ¿¿ N$^{0.864}$

Guth, Katz showed d(P) ¿¿ N / log N

r-rich partial symmetry of a set S is a rigid motion g such that —g(S) n S— ¿= r

Elekes, Sharir —$G_3(S)$| << $N^3 Guth, Katz |G_r(P)| << N^3/r^2$

How does the proof work

Define Q(P) = (p,q,p',q') : —p - q— = —p' - q'—

Then

—d(P)— —Q(P)— ¿¿ N^4

and

—Q(P)— sum r —$G_r(P)$|

Also

—$G_r(P)$| << N^3/r^2

so

—Q(P)— ¡¡ N$^3 logN$

so —d(P)— ¿¿ N / log(N)

NOOOOW how do we prove —$G_r(P)$| << N^3/r^2

For each $p_1, p_2, the collection S_{p1,p2} of rigid motions moving p_1 to p_2 is diffeomorphic to the unit circle.$

If g is in $G_r(P), then g is contained in >= r curves S_{p1,p2}, for p1, p2 in P$

Chapter 5

Restriction Problem

To prove a bound of the form $\|Ef\|_p \lesssim_p \|f\|_\infty$, it suffices to prove estimates of the form $\|Ef\|_{L^p(B_R)} \lesssim_{\varepsilon,p} R^\varepsilon \|F\|_\infty$ for a slightly small value of p.

Parabolic rescaling tells us that if $\|Ef\|_{L^p(B_R)} \leqslant A\|f\|_{L^\infty(S)}$, then $\|Ef\|_{L^p(B_R)} \leqslant Ar^{2-4/p}\|f\|_{L^\infty(S_r)}$, where f is supported on a cap of radius r.

5.1 Broad vs. Narrow Points

Let $f : S \to \mathbf{C}$, with $|f(\omega)| \leqslant 1$ for all $\omega \in S$. We want $\|Ef\|_{L^p(B_R)} \lesssim_\varepsilon R^\varepsilon \|f\|_\infty$. Let $K > 1$ be a large number, and divide S into caps of diameter $1/K$. We call a point $x \in B_R$ *narrow* if the wave packets passing through x come from the same $1/K$ cap.

Suppose all of B_R is narrow for a given function f. Suppose we have already established for some fixed ε, C_ε for all balls of radius $\leqslant R/2$. Let $N = \{x \in B_2 : \text{no wave packets through } x\}$, so $Ef(x) = 0$ on N. For each $1/K$ cap τ, elt X_τ be the set of points passing through the x cone from the cap τ. If $x \in X_\tau$, then $Ef(x) = Ef_\tau(x)$, so

$$\int_{X_\tau} |Ef(x)|^p = \int_{X_\tau} |Ef_\tau(x)|^p \leqslant \int_{B_R} |Ef_\tau(x)|^p$$

Thus Thus we have found $\|Ef\|_{L^p(B_R)} \lesssim K^{6/p-2}C_\varepsilon R^\varepsilon \|f\|_{L^\infty}$.

Now let's imagine every point in B_R is broad. We will prove instead that if $p = 13/4 + \varepsilon$, then

$$\|Ef\|^p_{L^p(B_R)} \lesssim_\varepsilon R^p_\varepsilon \|f\|^{3+\varepsilon}_{L^2(S)} \|f\|^{1/4}_{L^\infty(S)} \leqslant R^p_\varepsilon \|f\|^{3+\varepsilon}_{L^2(S)} \max_\Theta \|f\|^{1/4}_{L^2(\Theta)}$$

TODO: EXPAND

We want to understand $\int_{B_R} |Ef|^p$. Let $D > 1$ be a large integer. Let P be a polynomial breaking up $\mathbf{R}^3$ into a union of $O(D^3)$ cells. The mass of $|Ef|^p$ is roughly the same in each one of the cells (examine the proof of polynomial partitioning but rather than taking points take equidistributed mass). Thus on each cell Ω,

$$\int_\Omega |Ef|^p = D^{-3} \int_{B(R)} |Ef|^p$$

Unfortunately, a wave packet is a thickened line, so even though the line might not enter a cell, the wave packet might still enter a cell.

Define $W = N_{R^{1/2}}(Z(p))$. For each cell Ω, let $\Omega' = \Omega - W$. If a wave packet supported on a tube T intersects Ω', then the line coaxial with T intersects Ω, then on average each smaller cell Ω' only intersects $|T|/D^2$ wave packets. For each cell Ω, let $f_\Omega : S \to \mathbf{C}$ be the function whose extension Ef_Ω consists of the wave packets that intersect Ω'.

Chapter 6

The Cap Set Problem

The cap set problem comes out of additive combinatorics, whose goal is to understand additive structure in some abelian group, typically the integers. For instance, we can think of a set A as being roughly closed under addition if $|A + A| = O(|A|)$. Over rings, we can study the interplay between additive and multiplicative structure. For instance, one conjecture of Erdös and Szemerédi says that if A is a finite subset of real numbers, then $\max(|A + A|, |A \cdot A|) \gtrsim |A|^{1+c}$ for some positive $c \in (0, 1)$. The best known c so far is $c \sim 1/3$, though it is conjectured that we can take c arbitrarily close to 1. This can be seen as a discrete version of the results of Bourgain and Edgar-Miller on the Hausdorff dimensions of Borel subrings.

Theorem 6.1 (Van Der Waerden - 1927)**.** *For any positive integes r and k, there is N such that if the integers in* $[1, N]$ *are given an r coloring, then there is a monochromatic k term arithmetic progression.*

The coloring itself is not so important, more just the partitioning. We just pidgeonhole, using the density of k term arithmetic progressions. This problem suggests the Ramsey type problem of determining the largest set A of the integers $[1, N]$ which does not contain k term arithmetic progressions. Behrend's theorem says we can choose A to be on the order of $N \exp(-c\sqrt{\log N})$.

Theorem 6.2 (Roth - 1956)**.** *If A is a set of integers in* $[1, N]$ *which is free of three term arithmetic progressions, then* $|A| = O(N/\log\log N)$.

Szemerédi proved that if A is free of k term arithmetic progressions, $|A| = o(N)$. If Erdös Turan, if $\sum_{x \in X} 1/x$ diverges, then X contains arbitrarily long arithmetic progressions. For now, we'll restrict our attention to three term arithmetic progressions. Heath and Brown showed that three term arithmetic progresisons are $O(N/(\log N)^c)$ for some constant c. In 2016, the best known bound was given by Bloom, given $O(N(\log\log N)^4/\log N)$.

One way we can simplify our problem is to note that avoiding three term arithmetic progressions is a local issue, so we can embed $[1, N]$ in $\mathbf{Z}/M\mathbf{Z}$ for suitably large M, and we lose none of the problems we had over the integers. A heuristic is that it is easier to solve

these kind of problems in $\mathbf{F}_p^n$, where p is small and n is large, which should behave like $\{1,\dots,p^n\}$. This leads naturally to the cap set problem.

Theorem 6.3 (Cap Set Problem)**.** *What is the largest subset of* $\mathbf{F}_3^n$ *containing no three term arithmetic progressions?*

We look at $\mathbf{F}_3$ because it is the smallest case where three term arithmetic progressions become important.

Theorem 6.4 (Meschulam - 1995)**.** *Let* $A \subset \mathbf{F}_3^n$ *be a cap set. Then* $|A| = O(3^n/n)$*. This is analogous to a* $N/\log N$ *case over the integers, giving evidence that the finite field case is easier.*

In 2012, Bateman and Katz showed $|A| = O(3^n/n^{1+\varepsilon})$ for some $c > 0$. This was a difficult proof. In 2016, there was a more significant breakthrough, which gave an easy proof using the polynomial method of an exponentially small bound of c^n, where $c < 4$, over $\mathbf{Z}/4\mathbf{Z}$, and a week later Ellenberg-Gijswijt used this argument in the $\mathbf{F}_3$ case to prove that if A is a capset in $\mathbf{F}_3$,then $|A| = O(c^n)$, for $c = 2.7551\dots$.

The idea of the polynomial method is to take combinatorial information about some set, encode it as some algebraic structura information, and then apply the theory of polynomials to encode this algebraic information and use it to limit and enable certain properties to occur.

If V is the space of polynomials of degree d vanishing on a set A, then we know $\dim V \geqslant \dim \mathcal{P}_d - |A|$. This gives a lower bound on the size of A, whereas we want a lower bound. To get an upper bound, we take $|A|^c$ instead, which shows

$$\dim V \geqslant \dim \mathcal{P}_d + |A| - 3^n$$

whichs gives $|A| \leqslant 3^n + \dim V - \dim \mathcal{P}_d$. Now using linear algebra, we can find a polynomial P vanishing on A^c with support of cardinality greater than or equal to $\dim V$, hence

$$|A| \leqslant 3^n - \dim \mathcal{P}_d + \max |\mathrm{supp}(P)|$$

It follows that A is a cap set if and only if $x + y = 2z$, or $x + y + z = 0$ holds if and only if $x = y = z$. This is an algebraic property which says directly that A has no nontrivial three term arithmetic progressions. Thus for any $a_1,\dots,a_m \in A$, $P(-a_i - a_j) = 0$ when $i \neq j$. Equivalently, this means $P(-a_i - a_j) \neq 0$ when $i = j$. This suggests we consider the $|A|$ by $|A|$ matrix M with $M_{ij} = P(-a_i - a_j)$. This is a diagonal matrix, with $M_{ii} = P(a_i)$. Thus the rank of this matrix is the dimension of the support of P, so it suffices to upper bound the rank of M. The key observation, where we now explicitly employ the fact that P is a polynomial, is that $P(-x - y)$ is a polynomial in $2n$ variables $x, y \in \mathbf{F}_3^n$,

Bibliography