The polynomial method in combinatorics

Larry Guth

AMS joint meetings

4 January 2012

Overview

In the last five years, several challenging problems in combinatorics have been solved by introducing polynomials into the problem in an unexpected way.

This approach is based on work in computer science. The main idea comes from certain algorithms for solving problems about polynomials.

The idea from these algorithms was then applied to other combinatorial problems which have no obvious connection to polynomials.

The polynomial method in outline

1. Begin with a problem about some points in a vector space.

2. Find a polynomial of lowest possible degree that vanishes on the points.

3. Use this polynomial to attack the problem.

Finding polynomials with prescribed zeroes is just linear algebra

Let $\mathbb{F}$ be a field.
Let $p_1, ..., p_s$ be points in $\mathbb{F}^n$.

Question: Is there a non-zero polynomial of degree $\leq d$ that vanishes at all the points $p_1, ..., p_s$?

This question is really just a linear algebra problem.

Finding polynomials with prescribed zeroes is just linear algebra

$\mathbb{F}$ a field. $p_1, ..., p_s \in \mathbb{F}^n$.

Let $V(d)$ be the vector space of all polynomials in n variables with degree $\leq d$.

For example, if $n = 2$, then $V(1) = \{ax_1 + bx_2 + c | a, b, c \in \mathbb{F}\}$.

Let $E : V(d) \to \mathbb{F}^s$ be the evaluation map

$$E(Q) := (Q(p_1), ..., Q(p_s)).$$

The map E is linear!

Lemma

There is a non-zero polynomial of degree $\leq d$ that vanishes at all points if and only if E has a non-trivial kernel.

Finding the lowest degree polynomial that vanishes at prescribed points

Theorem

If $p_1, ..., p_s \in \mathbb{F}^n$, we can efficiently find a lowest degree non-zero polynomial Q that vanishes at each p_j.

Proof sketch. Check if there is a degree 1 polynomial that vanishes at the points. Then check for a degree 2 polynomial... Remarks.

- The degree of Q is at most s, the number of points. But we will give a much better estimate later.
- Q will probably not be unique, but we can find one such polynomial.

Intuition: This process finds the "algebraic structure" in the given set of points.

The first problem: recovering polynomials from corrupted data

Let $\mathbb{F}$ be a finite field with q elements. (q large)
Suppose that $P(x)$ is a polynomial over $\mathbb{F}$ with degree $d \leq q^{1/3}$.
Suppose that $F(x)$ is a function that agrees with $P(x)$ for at least $(51/100)q$ values of x.

We are given the function $F(x)$.
We want an efficient algorithm to recover P.

Some basic facts about polynomials

Lemma

A non-zero polynomial of degree $\leq d$ in one variable has at most d zeroes.

Corollary

If P and Q are polynomials of degree $\leq d$ in one variable, then either

- $P(x) = Q(x)$ *for* $\leq d$ *values of* x.
- $P = Q$.

Proof.

Consider $P_1 - P_2$. Either $P_1 - P_2$ has $\leq d$ zeroes, or $P_1 - P_2 = 0$.

□

There's only one polynomial that fits the data

Review. $\mathbb{F}$ a finite field with q elements.
$P(x)$ a polynomial of degree $\leq q^{1/3}$.
$F(x) = P(x)$ for $\geq (51/100)q$ values of x.
We are given F, and we want to find P.

Lemma

If $q > 10^4$, there is only one polynomial of degree $\leq q^{1/3}$ that agrees with F for at least $(51/100)q$ values of x.

Proof.

Suppose Q has degree $\leq q^{1/3}$, $Q(x) = F(x)$ for $\geq (51/100)q$ values of x.
Then $Q(x) = P(x)$ for at least $(2/100)q$ values of x. But $(2/100)q > q^{1/3}$. So $Q = P$. □

The Berlekamp-Welch algorithm

Review. $\mathbb{F}$ a finite field with q elements.
$P(x)$ a polynomial of degree $\leq q^{1/3}$.
$F(x) = P(x)$ for $\geq (51/100)q$ values of x.
We are given F, and we want to find P.

Theorem

(Berlekamp-Welch, 1986) There is an efficient algorithm to recover P from F. (The algorithm runs in polynomial time.)

Recovering from 99 % corrupted data!

$\mathbb{F}$ is still a finite field with q elements, and $P(x)$ is still a polynomial of degree $\leq q^{1/3}$.
This time suppose $F(x) = P(x)$ for $\geq q/100$ values of x.

Question: Given F, can we recover P?

Issue: P may not be unique! There may be two polynomials of degree $\leq q^{1/3}$ that agree with F on at least $q/100$ values of x.

Theorem

(Sudan, 1997) There is a polynomial-time algorithm that lists all the polynomials of degree $\leq q^{1/3}$ which agree with F for $\geq q/100$ values of x.

The idea of the algorithm

Review. $\mathbb{F}$ a finite field with q elements.
$P(x)$ a polynomial of degree $\leq q^{1/3}$.
$F(x) = P(x)$ for $\geq (1/100)q$ values of x.
We are given F, and we want to find P.

Let $G \subset \mathbb{F}^2$ be the graph of F. $G := \{(x, F(x)) | x \in \mathbb{F}\}$.
Let $Q(x, y)$ be a non-zero polynomial that vanishes on G, of minimal degree.

As we saw above, we can find Q efficiently!

The idea of the algorithm 2

Review. $\mathbb{F}$ a finite field with q elements.
$P(x)$ a polynomial of degree $\leq q^{1/3}$.
$F(x) = P(x)$ for $\geq (1/100)q$ values of x.
We are given F, and we want to find P.
$G \subset \mathbb{F}^2$ the graph of F.
$Q(x, y)$ a non-zero polynomial that vanishes on G, of minimal degree.

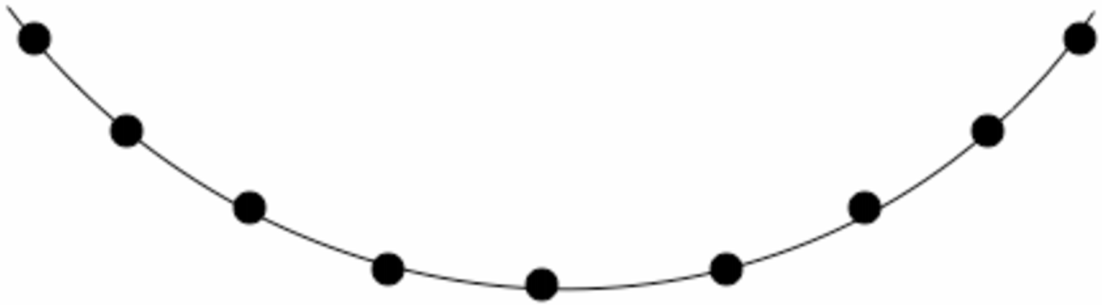
Let $P_1, ..., P_N$ be all the polynomials of degree $\leq q^{1/3}$ that agree with F for at least $q/100$ values of x. It turns out that

- The graph of each P_i is contained in the zero-set of Q.
- The polynomial $y - P_i(x)$ divides the polynomial $Q(x, y)$ (for each i).

So we can find all the P_i by factoring $Q(x, y)$ into irreducible factors.

Pictures of reconstructing polynomials from corrupted data

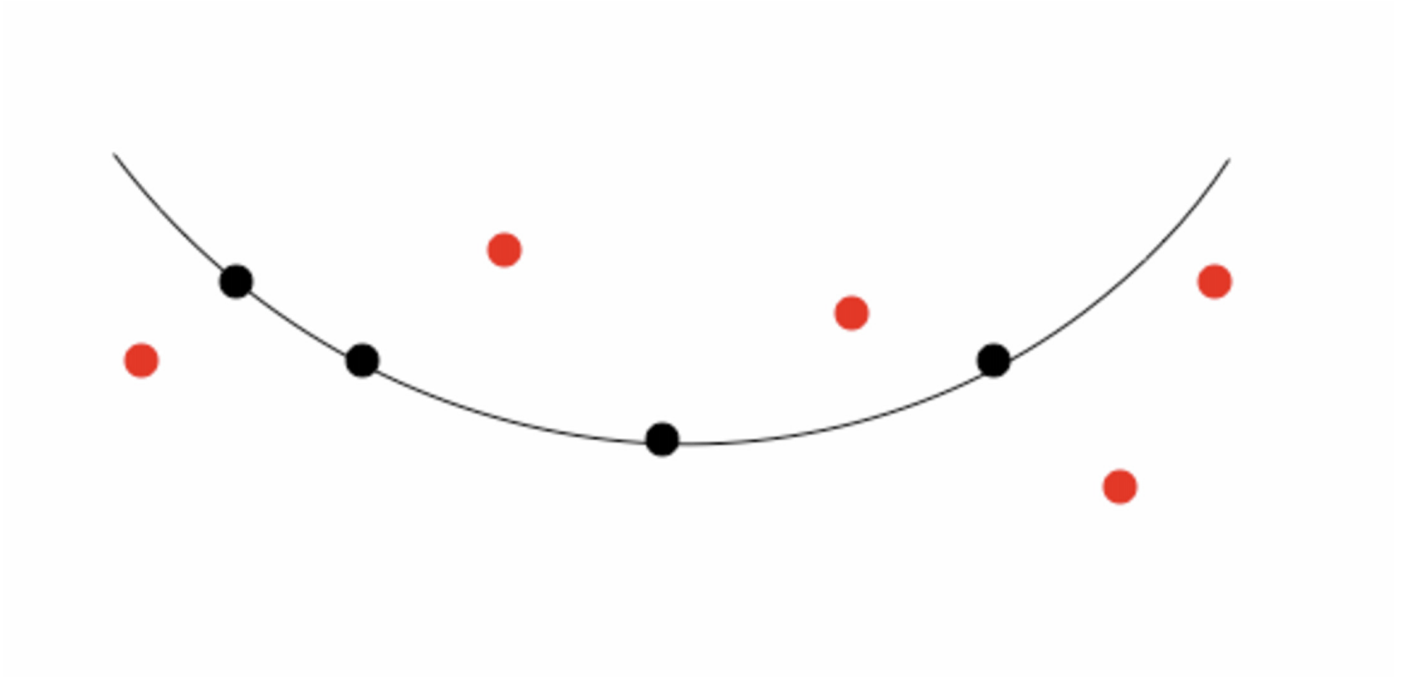
We begin with a low-degree polynomial P.



Here is the graph of P. Next the data will be corrupted.

Pictures of reconstructing polynomials from corrupted data

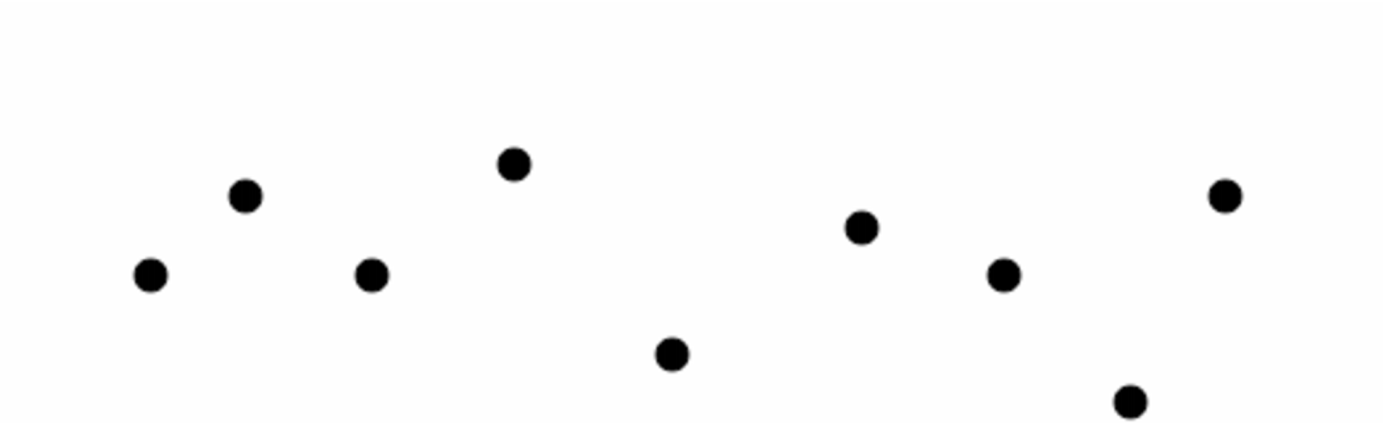
Then the polynomial P gets corrupted. Some of the values are changed, and the resulting function is called F.



Here is the graph of F. We don't know which values of F are right and which are wrong.

Pictures of reconstructing polynomials from corrupted data

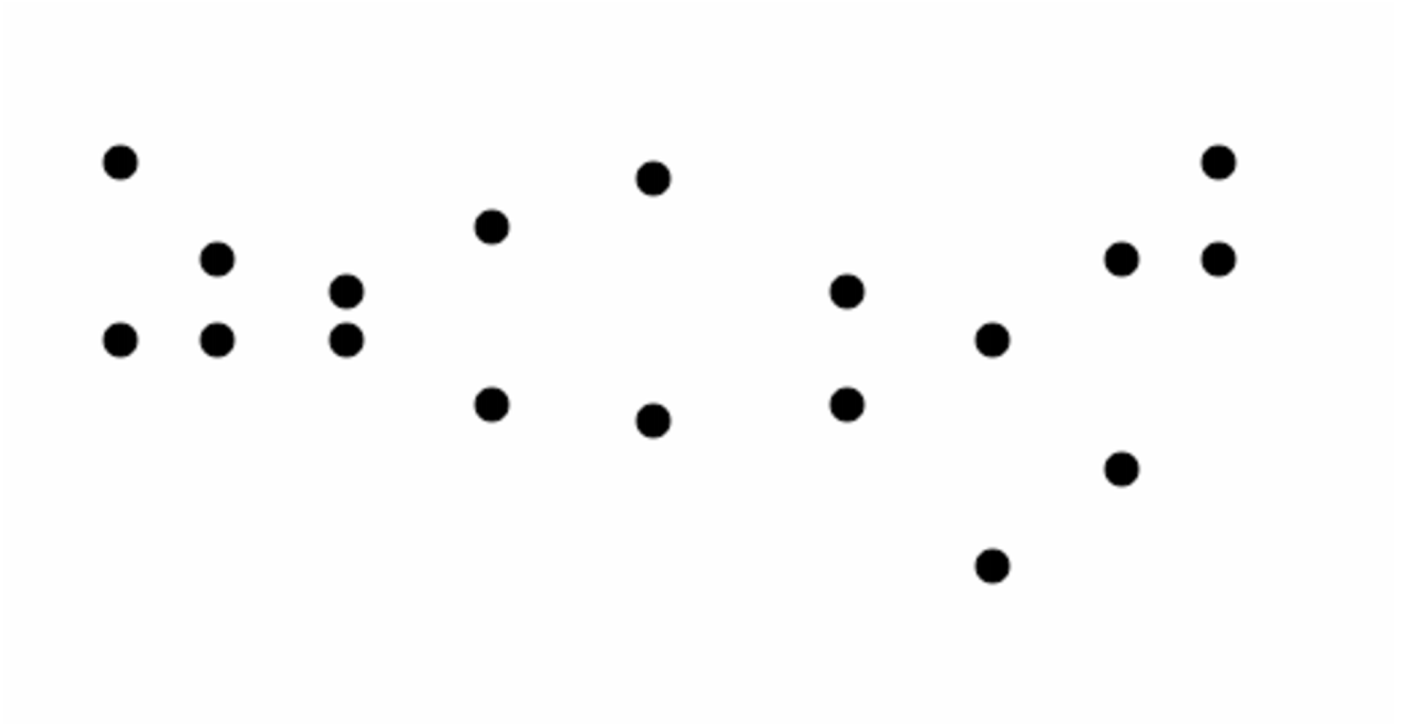
We don't know which values of P were changed and which remain the same. This is the information we are given.



We want to recover the polynomial P from this graph.
We start by finding a lowest-degree polynomial $Q(x, y)$ that vanishes on the graph.

Pictures of reconstructing polynomials from corrupted data

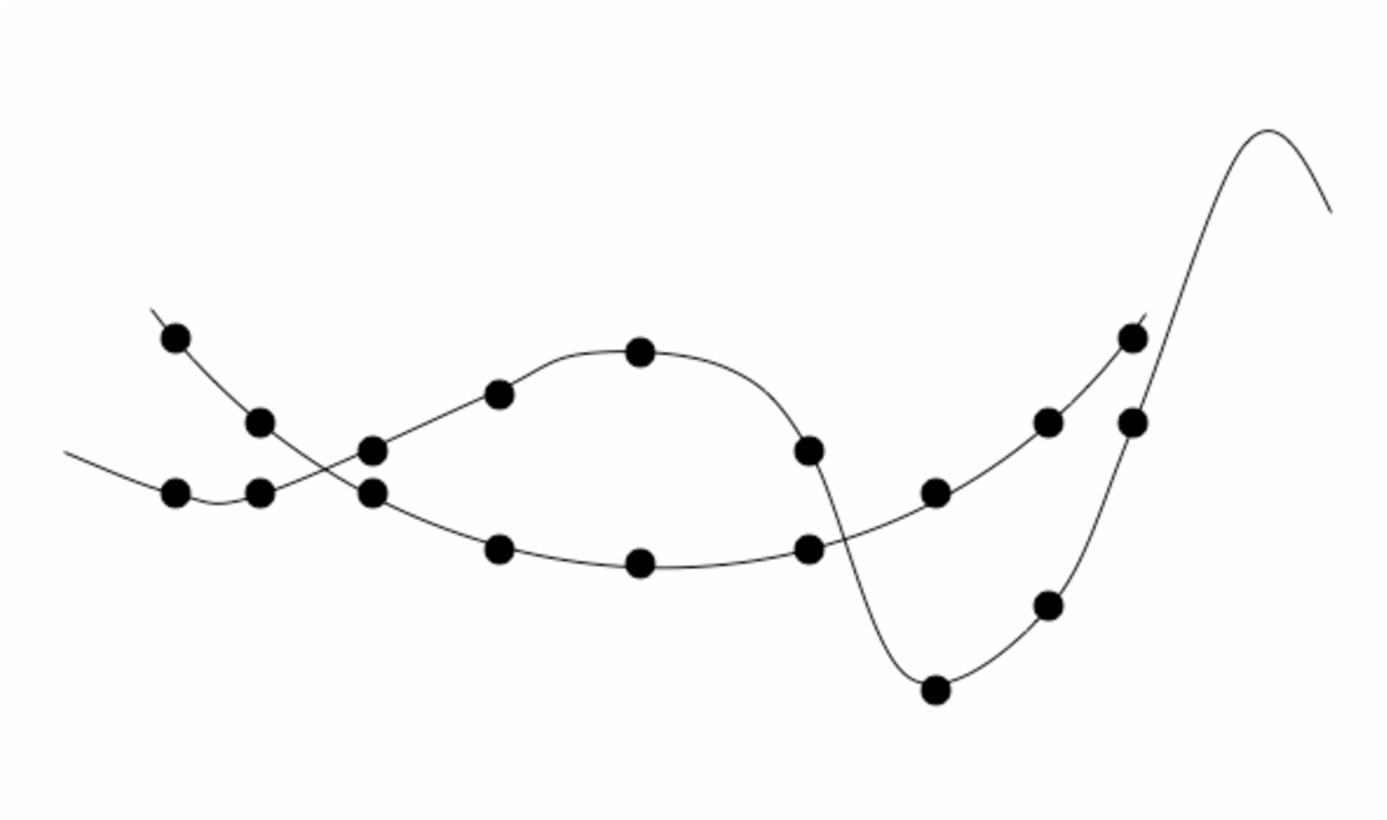
We find the lowest degree polynomial $Q(x, y)$ that vanishes on the graph of F. Here is the zero set of Q.



Of course, it contains the graph of F. But it also contains the graph of P!

Pictures of reconstructing polynomials from corrupted data

Finally, we factor Q into irreducible factors. The zero-set of Q gets divided into irreducible varieties, one for each factor.



One of the irreducible pieces is the graph of P.

The polynomial method in outline: recovering polynomials from corrupted data

1. Begin with a problem about some points in a vector space.

Given F which agrees with P for at least 51 % (or 1 %) of values of x. We want to find P.
We consider the graph of F, $G \subset \mathbb{F}^2$.

2. Find a polynomial of low degree that vanishes on the points.

Let $Q(x, y)$ be a non-zero polynomial of lowest degree that vanishes on G.

3. Use this polynomial to attack the problem.

The zero set of Q contains the graph of P.
Moreover, $y - P(x)$ divides $Q(x, y)$.

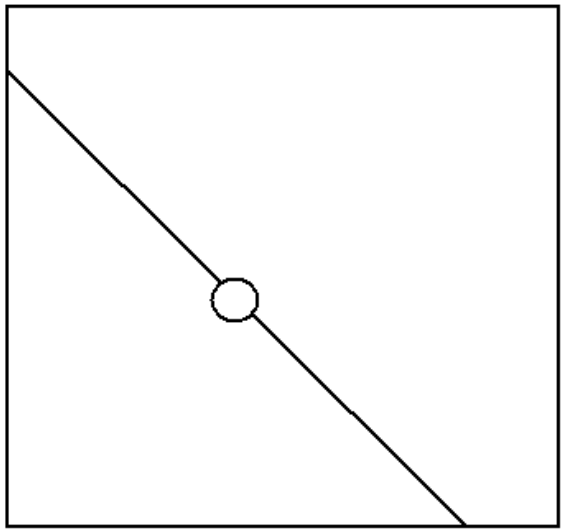
Other kinds of problems

Next we will turn to a problem coming from geometry.
The problem is about points and lines. It does not have any obvious connection to polynomials.
Nevertheless, we will attack it with the polynomial method.

A problem from geometry

A set $N \subset [0,1]^n$ is called a Nikodym set if, for each $x \in [0,1]^n$, there is a line segment L_x with boundary points on the edge of the cube so that

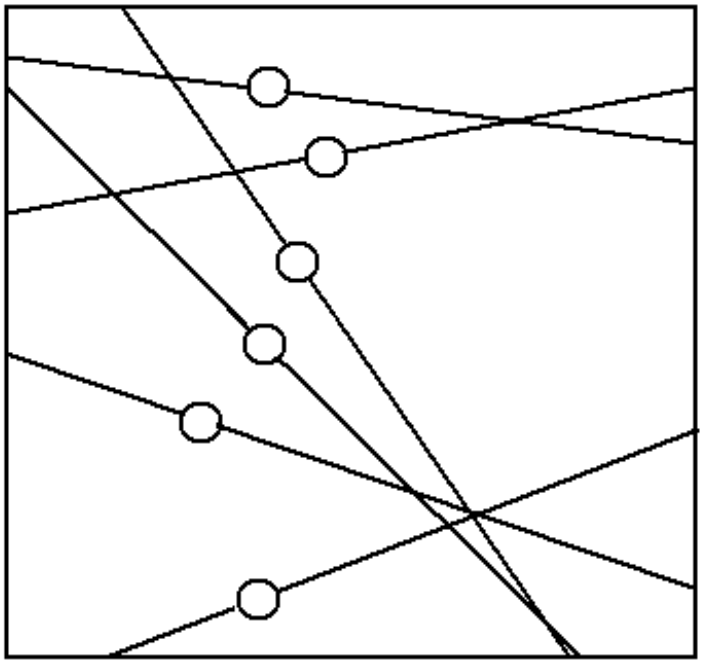
- L_x contains x
- $L_x \setminus \{x\} \subset N$.



In the figure, the circle denotes x and the line denotes L_x.

Nikodym sets

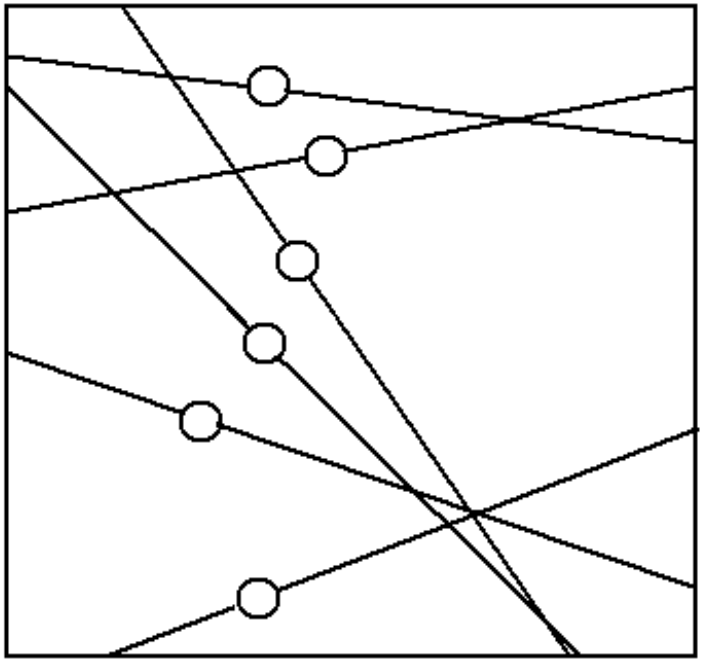
Review. A set $N \subset [0,1]^n$ is called a Nikodym set if, for each $x \in [0,1]^n$, there is a line segment L_x with boundary points on the edge of the cube so that L_x contains x and $L_x \setminus \{x\} \subset N$.



It may seem intuitive that a Nikodym set should fill up most of the cube.

The strange example of Besicovitch and Nikodym

Review. A set $N \subset [0,1]^n$ is called a Nikodym set if, for each $x \in [0,1]^n$, there is a line segment L_x with boundary points on the edge of the cube so that L_x contains x and $L_x \setminus \{x\} \subset N$.



In the 20's, Besicovitch and Nikodym gave a surprising construction of a Nikodym set in $[0,1]^2$ with measure 0!

The Nikodym conjecture

Although Nikodym sets can have measure 0, they still seem to be pretty large. Each known example has full Hausdorff dimension.

The Nikodym conjecture

Each Nikodym set in $[0,1]^n$ *has Hausdorff dimension* n.

The Nikodym conjecture is true if $n = 2$.
For $n \geq 3$, the Nikodym conjecture is a major open problem in geometry and harmonic analysis.
Best current estimate: a Nikodym set in $[0,1]^3$ has dimension $\geq 5/2$.

Nikodym sets in finite fields

There is an analogous problem in finite fields, first posed by Wolff in the mid-90's.

Let $\mathbb{F}$ be a finite field with q elements.
A set $N \subset \mathbb{F}^n$ is called a Nikodym set if for each $x \in \mathbb{F}^n$, there is an (affine) line L_x so that

- The line L_x contains x.
- $L_x \setminus \{x\} \subset N$.

Question: What is the smallest possible number of elements of a Nikodym set $N \subset \mathbb{F}^n$?

The finite-field Nikodym conjecture

Review. $\mathbb{F}$ a finite field with q elements.
A set $N \subset \mathbb{F}^n$ is called a Nikodym set if for each $x \in \mathbb{F}^n$, there is a line L_x so that L_x contains x and $L_x \setminus \{x\} \subset N$.

Theorem

(Dvir 2007) Each Nikodym set $N \subset \mathbb{F}^n$ has at least $c_n q^n$ elements.

Theorem

(special case) Each Nikodym set $N \subset \mathbb{F}^3$ has at least $(1/30)q^3$ elements.

Morally, Nikodym sets in finite fields have full dimension!

Although the result was expected to be true, many harmonic analysts were shocked by the short proof.

Polynomials that vanish on the Nikodym set

Theorem

(special case) Each Nikodym set $N \subset \mathbb{F}^3$ has at least $(1/30)q^3$ elements.

Review. $\mathbb{F}$ a finite field with q elements.
A set $N \subset \mathbb{F}^n$ is called a Nikodym set if for each $x \in \mathbb{F}^n$, there is a line L_x so that L_x contains x and $L_x \setminus \{x\} \subset N$.

In the proof, we're going to look at a lowest degree polynomial that vanishes on N.

Question: How big is the degree of this polynomial?

Tool 1. The polynomial existence lemma

Polynomial existence lemma

If $p_1, ..., p_s \in \mathbb{F}^3$, then there is a non-zero polynomial Q of degree $\leq 2s^{1/3}$ that vanishes on all the points p_j.

Proof. Let $V(d)$ be the vector space of polynomials in three variables of degree at most d.
Let $E : V(d) \to \mathbb{F}^s$ be the evaluation map:

$$E(Q) := (Q(p_1), ..., Q(p_s)) .$$

The map E is linear. If the dimension of the domain is larger than the dimension of the range, then E has a non-trivial kernel.
The dimension of $V(d)$ is $\binom{d+3}{3} \geq d^3/6$. If d is close to $2s^{1/3}$, $\dim V(d) \sim (8/6)s > s$.

Comparison with a naive construction

Suppose $p_1, ..., p_s \in \mathbb{F}^3$.
Our method gives the following:

Polynomial existence lemma

There is a non-zero polynomial Q that vanishes at each p_j with degree $\leq 2s^{1/3}$.

Here is a naive method.
Let L_j be a linear polynomial that vanishes at p_j. Then $\prod_{j=1}^{s} L_j$ vanishes at each p_j. It has degree s.

Tool 2: vanishing on a line

Let $L \subset \mathbb{F}^n$ be a line, parametrized by $\gamma(t) = at + b$.
(Here, $t \in \mathbb{F}$ and $a, b \in \mathbb{F}^n$, $a \neq 0$.)

Vanishing Lemma

If P is a polynomial of degree $\leq d$ that vanishes at $d+1$ points of L, then P vanishes on L.

Proof.

Let $R(t) := P(\gamma(t))$. R is a polynomial of degree $\leq d$ with $d+1$ zeroes. So R is identically zero. Hence P vanishes on L. $\square$

Proof of the finite-field Nikodym theorem in 3 dimensions

$\mathbb{F}$ a finite field with q elements.

Theorem

(Dvir 2007) Each Nikodym set in $\mathbb{F}^3$ has at least $(1/30)q^3$ elements.

Suppose that N is a Nikodym set with $< (1/30)q^3$ elements. By the polynomial existence lemma, we can find a non-zero polynomial P so that

- P vanishes on N
- Degree of P is $\leq (2/3)q$.

Let x be any point of $\mathbb{F}^3$. We know that P has $q-1$ zeroes on L_x. Hence P vanishes on L_x. So P vanishes at x. So P vanishes at every point. But P was non-zero and has degree $\leq (2/3)q$. Contradiction.

Technical detail. Polynomials that vanish at every point

$\mathbb{F}$ a finite field with q elements.
Is it true that a polynomial that vanishes at each point of $\mathbb{F}^n$ is the zero polynomial? Not necessarily. For example, $x_1^q - x_1$ vanishes at every point.

Lemma

Let P be a polynomial in n variables which vanishes at each point of $\mathbb{F}^n$. If the degree of P is $< q$, then P is the zero polynomial.

Proof by induction. Base case is $n = 1$: a non-zero polynomial of degree $\leq q - 1$ has $\leq q - 1$ zeroes.
Induction. Write $P = \sum_{j=0}^{q-1} P_j(x_1, ..., x_{n-1}) x_n^j$.
Fix $x_1, ..., x_{n-1}$. We have a polynomial in x_n of degree $\leq q - 1$ with q zeroes. So every coefficient is zero.
Hence $P_j(x_1, ..., x_{n-1})$ vanishes at each value of $x_1, ..., x_{n-1}$. P_j has degree $\leq q - 1$. By induction, each P_j vanishes identically. So then P is zero.

The polynomial method in outline: the finite field Nikodym problem

1. Begin with a problem about some points in a vector space.

$N \subset \mathbb{F}^3$. For each $x \in \mathbb{F}^3$, there is a line L_x containing x with $L_x \setminus \{x\} \subset N$. How big does N have to be?

2. Find a non-zero polynomial of low degree that vanishes on N.

If N were small, then the degree of the polynomial would be $\leq (2/3)q$.

3. Use this polynomial to attack the problem.

But that can't be. If the degree were $\leq (2/3)q$, we could show the polynomial would vanish on the whole space $\mathbb{F}^3$.
$L_x \setminus \{x\} \subset N$, so the polynomial vanishes there. But then it vanishes at x also by the vanishing lemma.

Influence of the finite-field Nikodym theorem

After Dvir's paper, many harmonic analysts began to look at the polynomial method.

Question: Will the polynomial method help us to make progress on the Nikodym problem?

Nobody knows.

But the polynomial method has helped to solve a number of longstanding problems in combinatorics.

Applications of the polynomial method in combinatorics

- Joints problem (posed in 1991, proven in 2008, Katz, G.)
- Distinct distance problem in the plane (posed in 1946, proven in 2010, Katz, G.)
- New proof of Szemeredi-Trotter theorem and other important known results in combinatorics/computer science. (2010, Kaplan, Matousek, Sharir)
- Generalizations of Szemeredi-Trotter theorem (posed in early 2000's, proven in 2010, Solymosi, Tao)
- Sum-product estimates in combinatorial number theory (a variant of a problem posed in early 80's, proven in 2010, Iosevich, Roche-Newton, Rudnev)

Why polynomials?

These problems are mostly about sets of lines in $\mathbb{R}^n$.
(In some cases, the problem can be connected to lines in $\mathbb{R}^n$ by a clever argument.)

Why do polynomials play a useful role?
They aren't mentioned in the statements of the problems, and they don't even seem to be connected to the problem.

Will we find proofs of the finite field Nikodym theorem and other results without using the polynomial trick?

Isolate the key facts about polynomials

1. The space of polynomials is large. In 3 dimensions, $V(d)$ has dimension $\sim d^3$.

Polynomial existence lemma

If $p_1, ..., p_s \in \mathbb{F}^3$, then there is a non-zero polynomial that vanishes on all the points p_j with degree $\lesssim s^{1/3}$.

2. The behavior of polynomials along a line is rather restricted.

Vanishing Lemma

If P is a polynomial of degree $\leq d$ that vanishes at $d+1$ points of a line L, then P vanishes on L.

If we restrict the polynomials in $V(d)$ to a line L, we get a vector space of dimension $d+1$.