Characteristic subsets and the polynomial method

Miguel N. Walsh

August 6, 2018

A typical form of the polynomial method:

A typical form of the polynomial method:

Step one: Given a set of elements S, find a small 'characteristic subset' $A \subseteq S$, such that if a 'small' non-zero polynomial vanishes to sufficiently high order on A, then it must also vanish on S.

Characteristic subsets and the polynomial method

A typical form of the polynomial method:

Step one: Given a set of elements S, find a small 'characteristic subset' $A \subseteq S$, such that if a 'small' non-zero polynomial vanishes to sufficiently high order on A, then it must also vanish on S.

Step two: Use a dimension counting argument, and the small size of A, to show that there are 'small' polynomials with nice properties that vanish on A, and therefore on S.

Notation

- Given a finite set A, we write $|A|$ for its cardinality.

Notation

- Given a finite set A, we write $|A|$ for its cardinality.
- Given two quantities X, Y we write $X \lesssim Y$ if there exists an absolute constant C with $X \leq CY$.

Notation

- Given a finite set A, we write $|A|$ for its cardinality.
- Given two quantities X, Y we write $X \lesssim Y$ if there exists an absolute constant C with $X \leq CY$.
- Given a polynomial $P \in \mathbb{R}[x_1, \ldots, x_n]$, we write

$$Z(P) = \{x \in \mathbb{R}^n : P(x) = 0\}.$$

Dimension counting arguments

Siegel's lemma

For any set of points $S \subseteq \mathbb{R}^n$ there exists a non-zero polynomial P of degree $\lesssim |S|^{1/n}$ vanishing on S.

Dimension counting arguments

Siegel's lemma

For any set of points $S \subseteq \mathbb{R}^n$ there exists a non-zero polynomial P of degree $\lesssim |S|^{1/n}$ vanishing on S.

'Proof': Dimension counting argument. There are so many polynomials of at most that degree that at least two different choices P_1 and P_2 take the same values on S. Then $P = P_1 - P_2$ is a polynomial of the desired form.

Dvir's Theorem

The polynomial method was used by Dvir in 2008 to solve the Kakeya problem over finite fields, with a strikingly simple proof.

Dvir's Theorem

The polynomial method was used by Dvir in 2008 to solve the Kakeya problem over finite fields, with a strikingly simple proof.

Conj. (Original Kakeya problem)

Let $K \subseteq \mathbb{R}^n$ be a set containing a unit line segment in every direction. Then $\dim(K) = n$.

Dvir's Theorem

Dvir's Theorem (2008)

Let $\mathbb{F}$ be a finite field and $K \subseteq \mathbb{F}^n$ a set containing a line in every direction. Then $|K| \gtrsim |\mathbb{F}|^n$.

Dvir's Theorem

Dvir's Theorem (2008)

Let $\mathbb{F}$ be a finite field and $K \subseteq \mathbb{F}^n$ a set containing a line in every direction. Then $|K| \gtrsim |\mathbb{F}|^n$.

The problem had remained open for a decade, with important work on it carried out by Wolff, Bourgain, Katz and Tao among others.

Dvir's Theorem

'Proof':

- A 'small' polynomial vanishing on $K \subseteq \mathbb{F}^n$, so in particular on a line pointing in every direction of $\mathbb{F}^n$, can be shown to vanish at all of $\mathbb{F}^n$. That is, K is a characteristic subset of $\mathbb{F}^n$.

Dvir's Theorem

'Proof':

- A 'small' polynomial vanishing on $K \subseteq \mathbb{F}^n$, so in particular on a line pointing in every direction of $\mathbb{F}^n$, can be shown to vanish at all of $\mathbb{F}^n$. That is, K is a characteristic subset of $\mathbb{F}^n$.
- If K is small we can find by Siegel's lemma a nonzero polynomial of small degree (less than $|\mathbb{F}|$) that vanishes on K, and therefore also on all of $\mathbb{F}^n$, which is impossible.

Baker's Theorem

The polynomial method is old.

Baker's Theorem (1967)

Let $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}} \setminus \{0\}$. If $\log \alpha_1, \ldots, \log \alpha_r$ are linearly independent over $\mathbb{Q}$, then $\log \alpha_1, \ldots, \log \alpha_r$ are linearly independent over $\overline{\mathbb{Q}}$.

Baker's Theorem

The polynomial method is old.

Baker's Theorem (1967)

Let $\alpha_1, \dots, \alpha_r \in \overline{\mathbb{Q}} \setminus \{0\}$. If $\log \alpha_1, \dots, \log \alpha_r$ are linearly independent over $\mathbb{Q}$, then $\log \alpha_1, \dots, \log \alpha_r$ are linearly independent over $\overline{\mathbb{Q}}$.

Baker's theorems have been used to prove transcendence results, to study the class number problem, for effective bounds on Diophantine questions and recently to obtain effective bounds on Furstenberg's $2x\,3x$ problem in ergodic theory.

Baker's Theorem

'Proof': Consider the set

$$\Gamma_N = \{(\alpha_1^s, \ldots, \alpha_r^s) : s \in \{1, \ldots, N\}\},$$

with $\log \alpha_1, \ldots, \log \alpha_r$ linearly independent over $\mathbb{Q}$.

Baker's Theorem

'Proof': Consider the set

$$\Gamma_N = \{(\alpha_1^s, \ldots, \alpha_r^s) : s \in \{1, \ldots, N\}\},$$

with $\log \alpha_1, \ldots, \log \alpha_r$ linearly independent over $\mathbb{Q}$.

- It can be shown that Γ_N is a characteristic subset of Γ_M even if N is quite smaller than M.

Baker's Theorem

'Proof': Consider the set

$$\Gamma_N = \{(\alpha_1^s, \ldots, \alpha_r^s) : s \in \{1, \ldots, N\}\},$$

with $\log \alpha_1, \ldots, \log \alpha_r$ linearly independent over $\mathbb{Q}$.

- It can be shown that Γ_N is a characteristic subset of Γ_M even if N is quite smaller than M.
- A linear dependence over $\overline{\mathbb{Q}}$ between $\log \alpha_1, \ldots, \log \alpha_r$ can be used to boost Siegel's lemma over Γ_N. This produces a 'very small' polynomial vanishing on the larger set Γ_M and contradicts basic facts about Vandermonde determinants.

The inverse sieve problem

Helfgott and Venkatesh asked to classify those sets that are very badly distributed in residue class mod p, for many primes p.

The inverse sieve problem

Helfgott and Venkatesh asked to classify those sets that are very badly distributed in residue class mod p, for many primes p.

It turns out such sets admit characteristic subsets.

The inverse sieve problem

Helfgott and Venkatesh asked to classify those sets that are very badly distributed in residue class mod p, for many primes p.

It turns out such sets admit characteristic subsets.

W. (2014)

Let $S \subseteq \{1, \dots, N\}^d$ be a set occupying $\lesssim p^k$ residue classes mod p for every prime p and some $0 \leq k < d$. Then S lies in the zero set of some non-zero polynomial of degree $\lesssim (\log N)^{\frac{k}{d-k}}$.

The determinant method

The polynomial method has also been used to estimate the number of rational points in curves and varieties. In this context it has been known as the determinant method.

The determinant method

The polynomial method has also been used to estimate the number of rational points in curves and varieties. In this context it has been known as the determinant method.

It was introduced by Bombieri and Pila to study integer points on curves and subsequently extended by Heath-Brown, Ellenberg and Venkatesh, Browning and Salberger, among others, to obtain estimates for rational points on curves and varieties.

The determinant method

W. (2015)

There exists an absolute constant B such that an irreducible algebraic curve over $\mathbb{Q}$ of degree d can have at most $BN^{2/d}$ rational points of height less than N.

The determinant method

W. (2015)

There exists an absolute constant B such that an irreducible algebraic curve over $\mathbb{Q}$ of degree d can have at most $BN^{2/d}$ rational points of height less than N.

For the proof we combine an improvement of Siegel's lemma due to Bombieri and Vaaler with estimates of Salberger based on the Hasse-Weil inequality.

Stepanov's method

The Hasse-Weil inequality itself (i.e. the Riemann Hypothesis for curves over finite fields) can be established by means of the polynomial method. This was done in 1969 by Stepanov (with an extension due to Bombieri). In this context, the technique has been known as Stepanov's method.

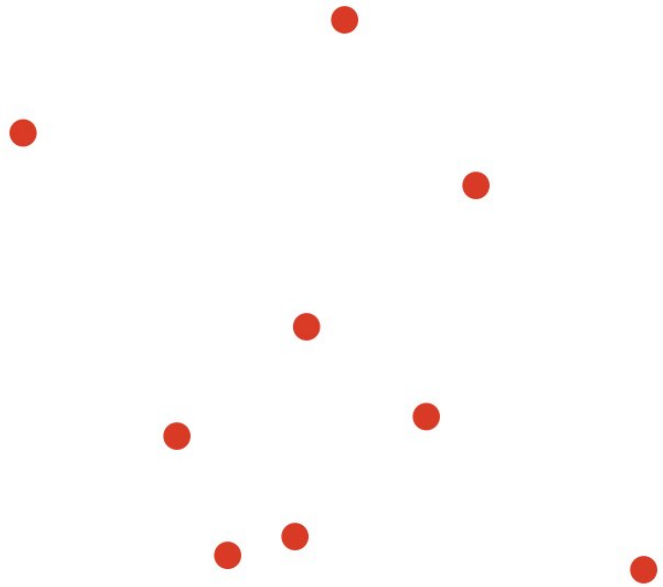
Stepanov's method

The Hasse-Weil inequality itself (i.e. the Riemann Hypothesis for curves over finite fields) can be established by means of the polynomial method. This was done in 1969 by Stepanov (with an extension due to Bombieri). In this context, the technique has been known as Stepanov's method.

A characteristic subset is found by means of Bezout's theorem, while the Riemann-Roch theorem is used to obtain an adequate version of Siegel's lemma.

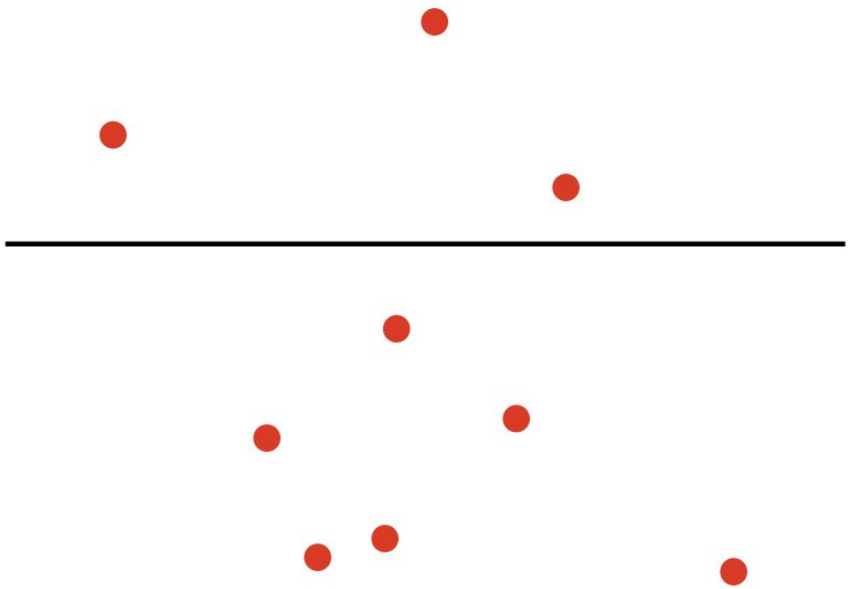
Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



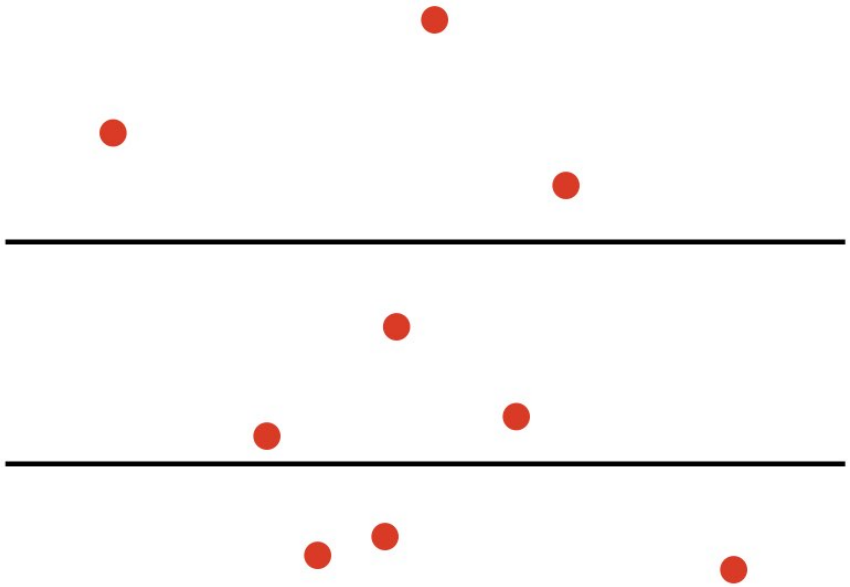
Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



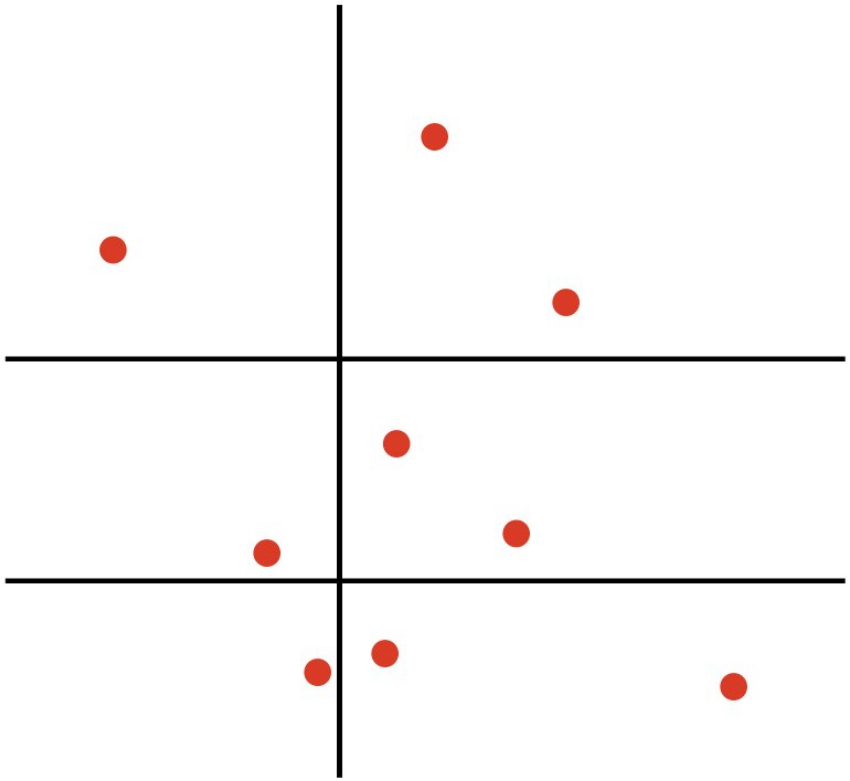
Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



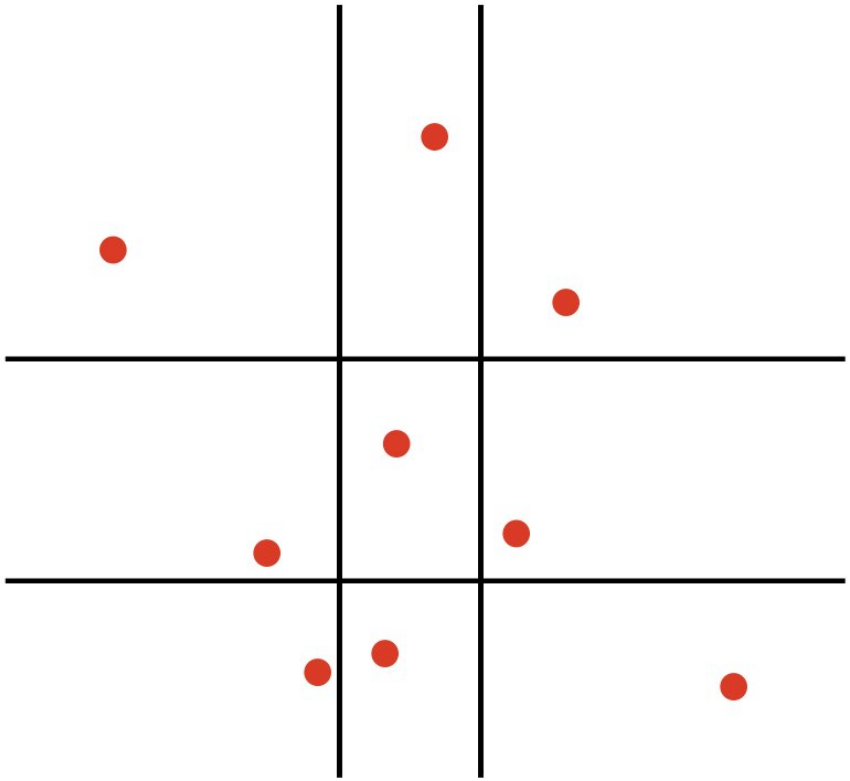
Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



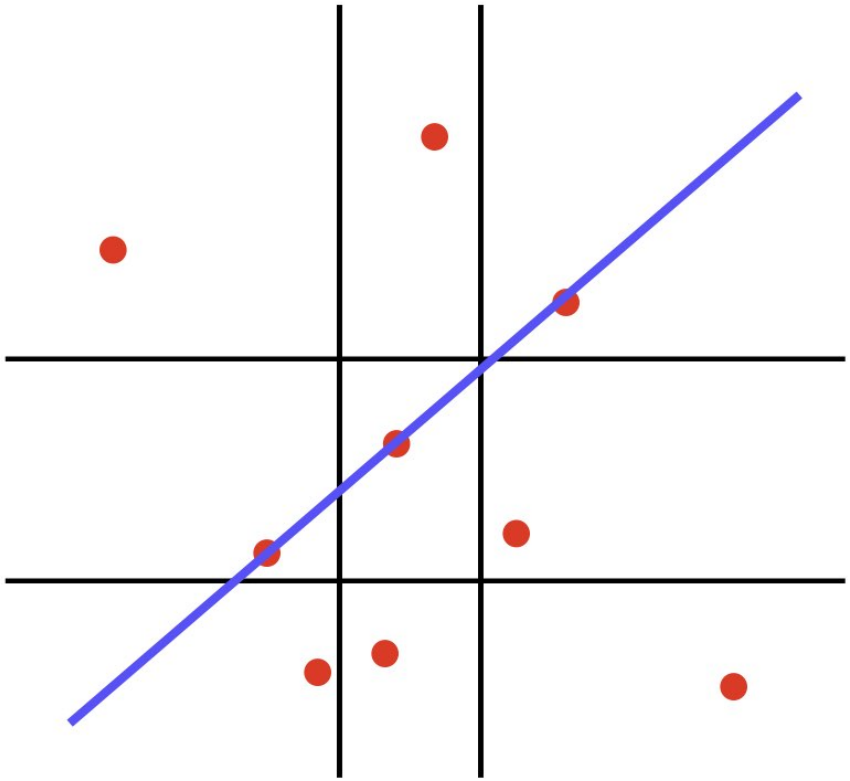
Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



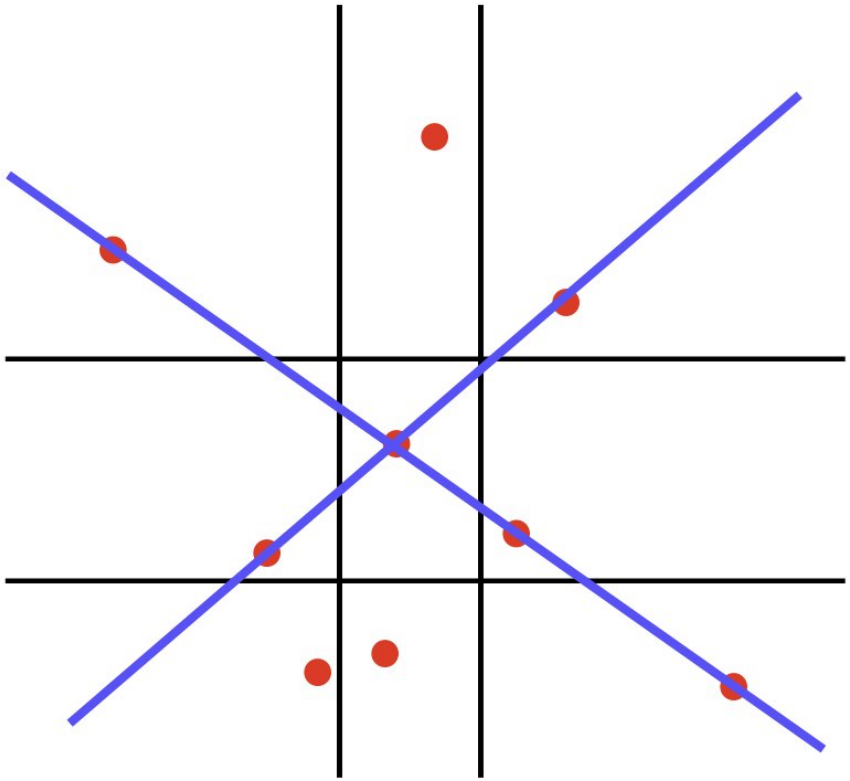
Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



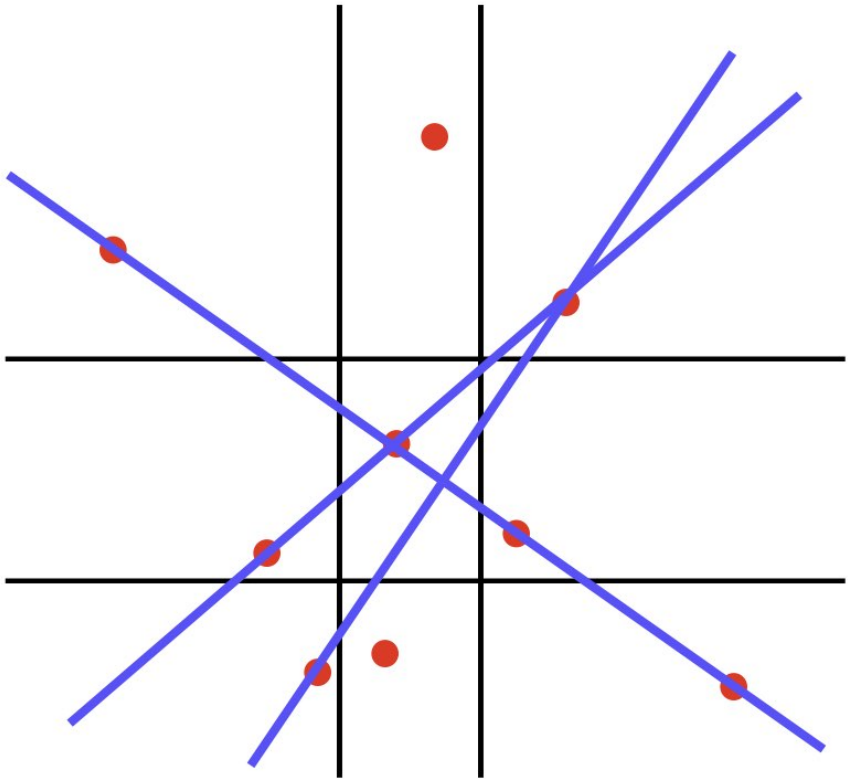
Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



Polynomial partitioning

Guth and Katz introduced an extension of the polynomial method to study incidences between points and lines in $\mathbb{R}^n$.



Polynomial partitioning

- Given a set of points $S \subseteq \mathbb{R}^n$ and a positive integer M, there exists a polynomial P of degree at most M such that each component of $\mathbb{R}^n \setminus Z(P)$ contains $\lesssim |S| M^{-n}$ points of S.

Polynomial partitioning

- Given a set of points $S \subseteq \mathbb{R}^n$ and a positive integer M, there exists a polynomial P of degree at most M such that each component of $\mathbb{R}^n \setminus Z(P)$ contains $\lesssim |S|M^{-n}$ points of S.
- A line can intersect at most $M+1$ of these components.

Polynomial partitioning

- Given a set of points $S \subseteq \mathbb{R}^n$ and a positive integer M, there exists a polynomial P of degree at most M such that each component of $\mathbb{R}^n \setminus Z(P)$ contains $\lesssim |S| M^{-n}$ points of S.
- A line can intersect at most $M+1$ of these components.
- Therefore, each component of $\mathbb{R}^n / Z(P)$ contains few points and each line touches few components. Summing a trivial bound among each component we get a good global bound.

Polynomial partitioning

- Given a set of points $S \subseteq \mathbb{R}^n$ and a positive integer M, there exists a polynomial P of degree at most M such that each component of $\mathbb{R}^n \setminus Z(P)$ contains $\lesssim |S| M^{-n}$ points of S.
- A line can intersect at most $M+1$ of these components.
- Therefore, each component of $\mathbb{R}^n / Z(P)$ contains few points and each line touches few components. Summing a trivial bound among each component we get a good global bound.
- We then deal with the points inside of $Z(P)$.

Polynomial partitioning

They used it among other things to establish Erdös's distinct distances conjecture.

Guth-Katz (2010)

Between N points in the plane there are at least $\gtrsim \frac{N}{\log N}$ distinct distances.

Polynomial partitioning

They used it among other things to establish Erdös's distinct distances conjecture.

Guth-Katz (2010)

Between N points in the plane there are at least $\gtrsim \frac{N}{\log N}$ distinct distances.

By work of Elekes and Sharir, this can be reduced to an incidence question between points and lines in $\mathbb{R}^3$. The latter estimate was then established by Guth and Katz by means of their extension of the polynomial method.

The Kakeya problem

Back to the Kakeya problem.

Conj. (Kakeya problem)

Let $K \subseteq \mathbb{R}^n$ be a set containing a unit line segment in every direction. Then $\dim(K) = n$.

The Kakeya problem

Back to the Kakeya problem.

Conj. (Kakeya problem)

Let $K \subseteq \mathbb{R}^n$ be a set containing a unit line segment in every direction. Then $\dim(K) = n$.

The polynomial method can be extended to continuous settings by considering the neighbourhood of algebraic varieties (e.g. replacing lines by tubes). Using this, Guth was able to obtain progress both on the Kakeya problem and the more general restriction conjecture of Stein in harmonic analysis.

The polynomial method over varieties

W. (2015-2018)

Let $V \subseteq \mathbb{R}^n$ be an algebraic variety. It is possible to establish improved versions of the components of the polynomial method.

The polynomial method over varieties

W. (2015-2018)

Let $V \subseteq \mathbb{R}^n$ be an algebraic variety. It is possible to establish improved versions of the components of the polynomial method.

1. We can find a polynomial of optimal degree vanishing on any set of algebraic subvarieties of V of given dimension and degree. The bound improves with the degree of V.

The polynomial method over varieties

W. (2015-2018)

Let $V \subseteq \mathbb{R}^n$ be an algebraic variety. It is possible to establish improved versions of the components of the polynomial method.

1. We can find a polynomial of optimal degree vanishing on any set of algebraic subvarieties of V of given dimension and degree. The bound improves with the degree of V.
2. We can find a polynomial partition of optimal degree for any set of points in V. The bound improves with the degree of V.

The polynomial method over varieties

W. (2015-2018)

Let $V \subseteq \mathbb{R}^n$ be an algebraic variety. It is possible to establish improved versions of the components of the polynomial method.

3. We can establish a sharp bound for the number of connected components of a 'cover' of any subvariety.

The polynomial method over varieties

W. (2015-2018)

Let $V \subseteq \mathbb{R}^n$ be an algebraic variety. It is possible to establish improved versions of the components of the polynomial method.

3. We can establish a sharp bound for the number of connected components of a 'cover' of any subvariety.
4. As an application, we can establish a general incidence estimate over V for subvarieties of arbitrary degree and dimension.

Some further remarks

Conj. (Montgomery's Conjecture)

For any real number $r \geq 1$ and any sequence of complex numbers $(a_n)_{n=1}^N$ with $|a_n| \leq 1$, the estimate

$$\frac{1}{T} \int_0^T \left| \sum_{n=1}^N a_n n^{is} \right|^{2r} ds \lesssim_\varepsilon N^{r+\varepsilon},$$

holds for all $T \geq N^r$ and all $\varepsilon > 0$.

Some further remarks

Montgomery's conjecture implies the Kakeya problem.

Some further remarks

Montgomery's conjecture implies the Kakeya problem.

The connection also works the other way, with the decoupling theory developed by Bourgain and Demeter to study restriction problems leading to applications in analytic number theory.

Some further remarks

Montgomery's conjecture implies the Kakeya problem.

The connection also works the other way, with the decoupling theory developed by Bourgain and Demeter to study restriction problems leading to applications in analytic number theory.

These include a proof of Vinogradov's main conjecture and the best known exponents on the Lindelöf Hypothesis.