Proc. Int. Cong. of Math. – 2018
Rio de Janeiro, Vol. 2 (485–504)

CHARACTERISTIC SUBSETS AND THE POLYNOMIAL METHOD

Miguel N. Walsh

Abstract

We provide an informal discussion of the polynomial method. This is a tool of general applicability that can be used to exploit the algebraic structure arising in some problems of arithmetic nature.

1 Introduction

1.1 The polynomial method. This article provides an informal discussion of the polynomial method. For us, this is the idea that when studying a problem with an underlying algebraic structure, a set S may admit a simpler "characteristic subset" $A \subseteq S$ that controls S, in the sense that a polynomial vanishing at A with sufficiently high multiplicity is forced to vanish at all or most points of S. By using dimension counting arguments in the spirit of Siegel's lemma, one may then exploit the simplicity of A to find a polynomial with suitable characteristics vanishing at most points of S.

This idea has been applied in a wide variety of contexts. Our choice of topics is largely based on personal taste, but we do try to convey the multitude of areas where it is relevant, the similarities in how the method is applied in them and some connections that exist between the different subjects. A variant of the method where the dimension counting arguments are used to find a polynomial that produces an adequate partition of the given points, instead of vanishing at them, has proven remarkably useful in recent work and is also treated in this article. We do not present proofs, but many are discussed. We refer the reader to Guth [2016c] and Tao [2014] for some further surveys on this circle of ideas.

Part of this article was written while the author was a Clay Research Fellow.
MSC2010: primary 11B30; secondary 52C10, 42B10, 11L07, 14G05, 37A45.

1.2 Notation. Before we proceed let us summarise the notation that will be used. Given two quantities X and Y, we will write either $X = O(Y)$ or $X \lesssim Y$ to mean that there exists some absolute constant C such that the inequality $X \leq CY$ holds. If this constant depends on some other parameter d, we may indicate this using a subscript and write $X = O_d(Y)$ or $X \lesssim_d Y$. If A is a finite set of points, $|A|$ will stand for its cardinality. We shall write $\mathbb{F}_q$ for the finite field with q elements, while the notation $\mathbb{F}$ alone is meant to stand for an arbitrary field. Finally, given a polynomial $P \in \mathbb{F}[x_1, \dots, x_n]$, we shall write $Z(P) = \{x \in \mathbb{F}^n : P(x) = 0\}$ for its zero set.

2 Incidence problems

2.1 Incidence geometry and its applications. We shall choose incidence geometry as our starting point and therefore spend some time motivating this subject. Some of the questions incidence geometry is concerned with rank among the simplest questions one can formulate in mathematics, but to define its problems broadly we consider the following set-up. Let V be an algebraic variety over a field $\mathbb{F}$, T a finite family of subvarieties of V and S a finite set of points inside of V. Incidence geometry is then mainly concerned with how the quantity

$$I(S,T) = |\{(s,t) \in S \times T : s \in t\}|,$$

which counts the number of incidences between S and T, relates to the sizes of S and T.

For example, when the variety V above is equal to $\mathbb{R}^n$ and T is just an arbitrary finite family of lines, we may ask for the maximal number of incidences that can occur between a set of points and a set of lines. A classical result of Szemerédi and Trotter [1983] gives in this case the sharp asymptotic bound

$$I(S,T) \lesssim |S|^{2/3}|T|^{2/3} + |S| + |T|,$$

where the implicit constant is uniform among all choices of S and T. If, more generally, we ask what happens when T is a finite family of algebraic curves of degree at most d, then a corresponding bound of the form

$$I(S,T) \lesssim_d |S|^{\frac{d^2+1}{2d^2+1}}|T|^{\frac{2d^2}{2d^2+1}} + |S| + |T|,$$

was established by Pach and Sharir [1998].

These two results constitute very simple instances of the general context described before. There is a vast literature dealing with many different cases that may arise, with T ranging from families of circles to high-dimensional varieties and with $\mathbb{F}$ ranging from a finite field to the complex numbers. While in principle there is no reason why some general unifying results could not be established, they certainly seem hard to come by. Similarly, obtaining sharp asymptotic bounds that avoid extra factors depending on $|S|$ or $|T|$ tends to be an additional challenge. Even when $V = \mathbb{R}^n$ and each element of T is a hypersurface defined by a single irreducible polynomial of bounded degree this question is not fully settled.

The simplicity of its questions is arguably one of the things that makes incidence geometry attractive and it is also this simplicity what makes its results find natural applications in different contexts. To give an example of this, let us discuss a very simple and direct connection to arithmetic combinatorics. To a finite set of points A in $\mathbb{R}^n$, say, we can associate the sets

$$A + A = \left\{a + a' : a, a' \in A\right\},$$

and

$$A \cdot A = \left\{a \cdot a' : a, a' \in A\right\}.$$

It is expected that both sets cannot be small simultaneously Erdős and Szemerédi [1983] and an estimate of this form was established by Elekes [1997] using incidence geometry. His idea was to consider the set of all lines of the form $y = (x - a)a'$, with $a, a' \in A$. Clearly, when $x = b + a$ for some $b \in A$, we get that $y = a'b \in A \cdot A$. As a consequence, we see that each of these lines touches $|A|$ points of the grid $(A+A)\times(A\cdot A)$. If both $A+A$ and $A \cdot A$ were to be small, this would then mean that these lines are highly incident to each other. So much so in fact, that they would contradict the Szemerédi-Trotter theorem. Thus we get the desired result.

Incidence bounds in the broader context we have described at the beginning of this section give rise to more general results concerning the size of

$$f(A_1, \ldots, A_m) = \{f(a_1, \ldots, a_m) : a_1 \in A_1, \ldots, a_m \in A_m\},$$

where f is a polynomial and $A_1, \ldots, A_m$ are finite sets of points (see for example Elekes and Szabó [2012]). Results of this type can in particular be applied to obtain randomness extractors, opening the door for incidence geometry to be applied in theoretical computer science Dvir [2010]. It should also be noted that the above sum-product phenomenon, as it is known, and the related concept of expansion, are pervasive throughout different parts of mathematics and have found a number of remarkable applications. See, for example, this survey by Helfgott [2015] and Green's 2014 ICM article Green [2014] for some discussion.

Sometimes problems can be encapsulated as incidence questions in more subtle ways. An example is provided by the Erdős distinct distances conjecture Erdős [1946], which asked for a bound on the minimal number of pairwise distances determined by n distinct points in the plane. Here Elekes and Sharir [2010] started with the simple observation that two pairs of points at the same distance determine two segments of the same length and so there exists some rigid motion taking one segment to the other. As it happens, given two points $x, y \in \mathbb{R}^2$, the set of rigid motions that take x to y can essentially be viewed as a line in $\mathbb{R}^3$ under an appropriate parametrisation of most of $\mathrm{SE}(2)$ (the special Euclidean group in two-dimensions). As a consequence, two pairs x_1, x_2 and y_1, y_2 at the same distance correspond to an intersection between the line of motions that send x_1 to x_2 and the line of motions that send y_1 to y_2. In paritcular, n points determining few distances lead to a set of highly incident lines in $\mathbb{R}^3$. Continuing this sort of arguments and exploiting some additional properties of the resulting set of lines, they managed to reduce Erdős' conjecture to an incidence question that was subsequently settled by Guth and Katz [2015].

Finally, the nature of incidence geometry also makes it a good source of toy models for more difficult problems. One notorious example is given by the following well-known conjecture in geometric measure theory.

Conjecture 2.1 (Kakeya problem). *A set $E \subseteq R^n$ containing a unit line segment in every direction must have Hausdorff dimension equal to n.*

A counterexample to this problem would certainly be reminiscent of the existence of a set of lines being highly incident to each other while satisfying some restricting conditions regarding their directions. This problem served as a motivation for a large body of work in incidence geometry and we will now see how it led to the introduction of the polynomial method in this area.

2.2 Enter the polynomial method.

There a number of ways of formulating toy models for the Kakeya problem in incidence geometry. A particularly straightforward way of doing so is to formulate the problem over $\mathbb{F}_q$, where the discrete nature of this space naturally turns it into a question about incidences. The resulting Kakeya problem over finite fields was answered in the affirmative by Dvir [2009]. Precisely, he established the following result.

Theorem 2.2 (Kakeya over finite fields). *Let $K \subseteq \mathbb{F}_q^n$ be a set containing a line in every direction. Then $|K| \gtrsim q^n$.*

This question was originally posed by Wolff [1999] and attracted considerable attention. Despite the large amount of work that preceded his article, Dvir's proof is extremely simple. What distinguishes it is its introduction of the polynomial method as the main tool to attack the problem. While this tool had barely been used in this or related areas before, the situation would change dramatically after this result.

The polynomial method is largely concerned with finidng a polynomial with suitable properties vanishing at most points of a set of interest. To find such a polynomial, an important role is played by the following simple observation, usually attributed to Thue and Siegel, which allows us to bound the degree of a polynomial vanishing on an arbitrary set.

Lemma 2.3 (Siegel's lemma). *For every set finite $S \subseteq \mathbb{F}^n$ there exists a non-zero polynomial $P \in \mathbb{F}[x_1, \dots, x_n]$, of degree $\lesssim_n |S|^{1/n}$, vanishing on S.*

The proof is extremely simple, consisting only of a dimension counting argument. There are so many different polynomials of degree $\lesssim_n |S|^{1/n}$ that at least two of them, say P_1 and P_2, must take the same values on S. Therefore $P = P_1 - P_2$ is of the form we want. The same kind of argument can be used to force some additional properties on the polynomial P, like having integer coefficients or vanishing to high multiplicity on our set of points.

To obtain a polynomial of low degree vanishing on a given set S, the polynomial method combines the above lemma with what might be called the idea of characteristic subsets (here we are using the notation of M. N. Walsh [2012b]). We informally define these as follows.

Definition 2.4 (Characteristic subset). A set $A \subseteq S$ is said to be a characteristic subset of S if any polynomial of low complextiy that vanishes with a certain multiplicity on A must also vanish at all or most points of S.

What exactly does it mean for a polynomial P to have low complexity depends very much on what is needed in the given problem, though it always implies that the degree of P should be small. In some cases, we may also require the coefficients to be small or restricted to the integers, or both. Clearly, if a set S admits a characteristic subset A of small size, then we can find a polynomial of low degree vanishing at all or most points of S by applying Siegel's lemma to A. As we will see during this article, this idea is a central part of the polynomial method.

Let us now see how it applies to the proof of Theorem 2.2. Dvir's crucial observation is that any set $K \subseteq \mathbb{F}_q^n$ containing a line in every direction must be a characteristic subset of $\mathbb{F}_q^n$. This is easiest to see looking at the corresponding projective space. If P is a polynomial of degree strictly less than q vanishing on an affine line in every direction, by Bezout's theorem its homogenisation must also contain the hyperplane at infinity in its zero set and this necessarily implies that P vanishes at the whole space. As a consequence, if we could find a nontrivial polynomial of degree less than q that vanishes on K, it would also have to vanish on $\mathbb{F}_q^n$, which is impossible. Comparing this observation with Siegel's lemma, we conclude that it must be $|K| \gtrsim_n q^n$.

2.3 Polynomial partitioning. The idea of characteristic subsets will also play a role in incidence geometry results over $\mathbb{R}^n$. For example, if we are given a highly incidence family of lines T, we may be able to find a subset of lines $T' \subseteq T$ such that any polynomial of low degree P vanishing on all the elements of T' must also vanish on most elements of T. The reason why this may work is that, given the highly incident nature of T, we may be able to find a small subset $T' \subseteq T$ such that most elements $t \in T$ will be incident to many lines in T'. As a consequence, a polynomial P vanishing on T' will vanish at many points of such t. If the degree of P is sufficiently small, Bezout's theorem would then force P to vanish on all of t as desired. This kind of approach is often called degree-reduction in this context.

Although arguments like this tend to be useful, it turns out that a substantial addition to the polynomial method is required in order to make progress on incidence problems taking place in $\mathbb{R}^n$. Since the original work of Szemerédi and Trotter, a central idea in incidence geometry has been to partition the space into cells in a way that limits how many of these cells the elements of T may intersect. This plays into the intuitive notion that the varieties being studied in an incidence problem should spread out across space, thus forbidding them to cluster into a highly incident configuration. As it turns out, polynomials can be used to obtain such a partition of space in an extremely structured way. Indeed, the following result was establish by Guth and Katz [2015] when trying to adapt Dvir's polynomial method to incidence questions over Euclidean space.

Theorem 2.5 (Polynomial partitioning of $\mathbb{R}^n$)**.** *For every finite set $S \in \mathbb{R}^n$ and every choice of an integer $M \geq 1$, there exists some nonzero polynomial $P \in \mathbb{R}[x_1, \dots, x_n]$ of degree $\lesssim_n M$ such that each connected component of $\mathbb{R}^n \setminus Z(P)$ contains at most $\lesssim_n \frac{|S|}{M^n}$ points of S.*

By an old result of Petrovskiĭ and Oleĭnik [1949] it is known that if P is a polynomial in n variables of degree $O(M)$, then $\mathbb{R}^n \setminus Z(P)$ can have at most $O(M^n)$ connected components. Theorem 2.5 then says that at any level M of our choice and for any set S, we can partition the points of S as efficiently as possible among the connected components of the complement of a polynomial of degree at most $O(M)$. The generality of such a statement is quite striking. There is one caveat, however, which is that the result does not rule out the possibility that some of the points of S actually lie inside of $Z(P)$. But this in itself may be an advantage, since we may be able to exploit the additional structure of having a proper subvariety covering our set of points in order to attack the problem that we are interested in.

Let us now briefly discuss how a partition of S of the above type can be used to tackle questions in incidence geometry. For simplicity, let us assume we are studying the incidences of S with a set of lines T and let us apply Theorem 2.5 to S for an adequate choice of M. Then we obtain a partition by the zero set of some polynomial P of degree $O(M)$ in such a way that each connected component of $\mathbb{R}^n \setminus Z(P)$ contains very few points of S. But since a line that is not properly contained in $Z(P)$ can touch this zero set in at most $\deg(P)$ places, it follows that such a line can only intersect $\deg(P) + 1 = O(M)$ of the components of $\mathbb{R}^n \setminus Z(P)$. In other words, each component contains few points and each line intersects few components. Combining this observation with a trivial incidence estimate in each component coming from the Cauhcy-Schwarz inequality, this readily provides a sharp incidence bound upon making an adequate choice of the parameter M.

It then remains to deal with the incidences occurring inside of $Z(P)$. This points out why the general context described at the beginning of this section can be relevant even if one is only interested in estimates over $\mathbb{R}^n$. To obtain sharp estimates in this case, the study of $Z(P)$ sometimes requires one to pay attention to more subtle algebraic properties of the subvarieties involved (see for example Katz's ICM 2014 article Katz [2014]), but many times even this can be avoided if one is willing to settle for slightly weaker bounds.

In any case, the fact that the problem is reduced to the study of subvarieties is not capricious. To see this, consider for example the task of estimating the number of incidences between a set of points and a set of lines in $\mathbb{R}^3$. The first part of the argument above that deals with the incidences occurring inside the cells, when applied in $\mathbb{R}^3$, leads to a bound that improves the one provided by the Szemerédi-Trotter theorem. However, the latter result is sharp in $\mathbb{R}^2$ and so it is clear that this improvement is not possible in general. Indeed, an example showing that the Szemerédi-Trotter theorem is optimal in $\mathbb{R}^2$ can obviously be replicated inside any plane of $\mathbb{R}^3$. This is a general phenomenon: incidence bounds can be worse than expected if the elements of T cluster inside lower-dimensional varieties. In their work, Guth and Katz managed to obtain an improved bound in $\mathbb{R}^3$ under the assumption that such a clustering fails to take place. Part of the remarkable effectiveness of the polynomial method as discussed above is that it provides optimal bounds outside of the zero set of a certain polynomial and thus singles out the correct obstruction, that is, the possibility that many incidences are occurring inside lower-dimensional varieties.

3 Number theory

3.1 Stepanov's method. We will now depart from the incidence geometry questions discussed in the previous section and see how the polynomial method makes an appearance throughout a range of topics in number theory. We will see how it was recently used in the study of the distribution of sets in residue classes mod p and to bound the number of rational points on curves. However, the polynomial method in this context is not new and was used by Stepanov [1969], and later Bombieri [1974], in the related topic of estimating the number of $\mathbb{F}_q$-points on a curve. Precisely, they provided an alternative proof of the following estimate, equivalent to the Riemann Hypothesis for curves over finite fields.

Theorem 3.1 (Hasse-Weil bound). *Let $\mathcal{C}$ be a nonsingular absolutely irreducible projective curve of genus g defined over $\mathbb{F}_q$. Then, writing $\mathcal{C}(q)$ for the number of $\mathbb{F}_q$-points of*

$\mathcal{C}$, *we have the estimate*

$$|\mathcal{C}(q) - (q+1)| \leq 2g\sqrt{q}.$$

The story of the Riemann Hypothesis for curves over finite fields is well-known. It was originally conjectured by Artin [1924], with the case of elliptic curves being established by Hasse [1936]. The general result was famously obtained by Weil [1949] in work that laid the foundation of modern algebraic geometry. However, an alternative proof that is more elementary was subsequently found by Stepanov in special cases using what we would now call the polynomial method. His method was subsequently used by Bombieri to produce a very simple argument that handles the result in full generality.

Let us now briefly discuss how the proof works. The lower bound on $\mathcal{C}(q)$ provided by Theorem 3.1 can be easily derived from the upper bound by means of a lifting trick, so we will just discuss how the latter is established. We are interested in an upper bound on the number of $\mathbb{F}_q$-points lying inside a curve $\mathcal{C}$, or in other words, the number of points x inside of this curve that are invariant under the Frobenius map $\mathrm{Frob}(x) = x^q$. By looking at the cartesian product $\mathcal{C} \times \mathcal{C}$, we see that it will suffice to provide an upper bound for the size of the intersection of two curves in this cartesian product: the curve $\mathcal{C}_1 = \{(x,y) \in \mathcal{C} \times \mathcal{C} : x = y\}$ and the curve $\mathcal{C}_2 = \{(x,y) \in \mathcal{C} \times \mathcal{C} : \mathrm{Frob}(x) = y\}$.

A naive application of Bezout's theorem to bound the size of this intersection would fail to produce the kind of bound we want. On the other hand, Bezout's theorem does tell us that given an irreducible curve of bounded degree, a polynomial of low degree vanishing with high multiplicity on a large subset of this curve must vanish on the whole curve. Applying this to our problem we conclude that if $\mathcal{C}_1 \cap \mathcal{C}_2$ is large, then it must be a characteristic subset of $\mathcal{C}_2$. Thus in order to prove Theorem 3.1 it would suffice to construct a polynomial of low degree vanishing with high multiplicity on $\mathcal{C}_1$, but not vanishing on $\mathcal{C}_2$. This in turn follows from a combination of the Riemann-Roch theorem and the same kind of dimension counting arguments used in the proof of Siegel's lemma.

3.2 The inverse sieve problem. One of the main topics in analytic number theory is the study of the distribution of sets in residue classes mod p. Many times, the goal is to show that a special set, like the primes, is essentially equidistributed among these classes. It is then natural to wonder what kind of structure may cause a set to be badly distributed in residue classes and in particular, whether an inverse theorem may be obtained characterising all sets exhibiting bad behaviour.

As we have just seen, algebraic curves constitute one such example and in general, so do algebraic sets of higher dimension. That abnormal behaviour should always be attributable to the presence of algebraic structure was suggested by a number of authors. The following result established a conjecture of Helfgott and Venkatesh [2009] to this effect.

Theorem 3.2 (M. N. Walsh [2014]). *Let $S \subseteq \{1, \dots, N\}^d$ occupy $\ll p^\kappa$ residue classes for every prime p and some real number $0 \le \kappa < d$. Then, for every $\varepsilon > 0$, there exists some nonzero $P \in \mathbb{Z}[x_1, \dots, x_d]$ of degree $\ll_{\kappa,d,\varepsilon} (\log N)^{\frac{\kappa}{d-\kappa}}$ vanishing on at least $(1-\varepsilon)|S|$ points of S.*

The assumption that the set occupies few classes is not prohibitive and can be replaced by an estimate on its L^2-norm mod p. Furthermore, it was shown in M. N. Walsh [2012b] that the polynomial P can be taken to have degree $O(1)$ as long as the set S satisfies some regularity assumptions. In fact, these assumptions are automatically met if the set S is not small, as conjectured in Helfgott and Venkatesh [2009].

These results are essentially sharp and their proof employs the polynomial method. The argument goes more or less as follows. If S occupies few residue classes mod p for many primes p, it should be possible to find a very small set $A \subseteq S$ that, for many primes p, contains a representative of many of the classes occupied by S mod p. We claim that A is then a characteristic subset of S. Indeed, suppose P is a polynomial with small coefficients and small degree that vanishes on A. By construction of A, we find that to most elements $s \in S$ we can associate many primes p_i such that $s \equiv x_i \pmod{p_i}$ for some $x_i \in A$ and so, in particular, $P(s) \equiv P(x_i) \pmod{p_i}$. The fact that P vanishes on A then implies that every such p_i must divide $P(s)$. But since P has small coefficients and small degree, $|P(s)|$ is small, and so the only way this can happen is if $P(s) = 0$. We have thus shown that A is indeed a characteristic subset of S. The result then follows from applying Siegel's lemma to find a polynomial of low degree vanishing on A.

There is an interesting question that remains when considering one dimensional sets $S \subseteq \{1, \dots, N\}$. We know by the large sieve inequality that a set occupying approximately half of the residue classes mod p, for all primes p, can have size at most $O(N^{1/2})$. On the other hand, the squares in $\{1, \dots, N\}$ show that this estimate is sharp. The question arises whether every set of comparable size occupying at most half the residue classes mod p, for every prime p, must be correlated to the set of squares. This question can be generalised a bit further (see M. N. Walsh [2012b]). Given the arguments described above, one would expect that the polynomial method should be useful to make progress on this problem, although this has not been achieved so far (but see Green and Harper [2014] and Hanson [2017] for some partial progress by means of different tools).

3.3 The determinant method. The polynomial method has also been used effectively to bound the number of points S of bounded height that an algebraic variety can have over $\mathbb{Z}$ or $\mathbb{Q}$. As in Stepanov's method, the problem does not lie in finding an adequate characteristic subset A for S, since in this context this is generally accomplished by simply picking a maximal algebraically independent subset of S. The actual difficulty lies instead in finding an appropriate polynomial vanishing on A. This gives rise to the study of a certain system of linear equations and in particular, to estimates on the size of the determinants associated with this system. As a consequence, this form of the polynomial method has been known as the determinant method in this context. It dates back to the work of Bombieri and Pila [1989], with subsequent improvements of this method being obtained by Heath-Brown [2002] and Salberger [2010], among others.

For the rest of this discussion let us assume for simplicity that A lies inside a plane curve $\mathcal{C}$ defined by an irreducible polynomial f. The task of finding a polynomial vanishing on A may seem circular, since after all, we already know that f vanishes on A. The idea is instead to show that the dimension of the space of polynomials of small degree vanishing on A is big. Big enough, in fact, as to guarantee the existence of at least one polynomial g in this space that is not divisible by f. Since S must then lie in $\mathcal{C} \cap Z(g)$, a bound for its size readily follows from Bezout's theorem.

While the Stepanov-Bombieri argument required us at this stage to improve on Siegel's lemma by means of a dimension counting argument relying on the Riemann-Roch theorem, the improvement of Siegel's lemma needed here can be obtained through the following estimate of Bombieri and Vaaler on the space of solutions of a system of linear equations over the integers.

Theorem 3.3. *Bombieri and Vaaler [1983] Let $\sum_{k=1}^{r} b_{mk} x_k = 0$, $m = 1, \dots, s$, be a system of s linearly independent equations in $r > s$ unknowns, with integer coefficients b_{mk}. Then, there exists a nontrivial integer solution $(x_1, \dots, x_r)$ satisfying the bound*

$$\max_{1 \le i \le r} |x_i| \le \left(D^{-1} \sqrt{\left|\det\left(BB^T\right)\right|} \right)^{\frac{1}{r-s}}. \tag{3-1}$$

Here $B = (b_{mk})$ is the $s \times r$ matrix of coefficients, B^T its transpose, and D is the greatest common divisor of the determinants of the $s \times s$ minors of B.

When trying to find a polynomial of small degree that vanishes on A, the system of equations we are interested in is the one where the coefficients b_{mk} are given by the values taken by the monomials of small degree when evaluated at the elements of A. It is the presence of the factor D^{-1} in the above statement what provides an improvement over the classical form of Siegel's lemma.

We already know that as a consequence of the Hasse-Weil bound, the rows of the resulting matrix of coefficients B will occupy few residue classes mod p for many primes p, exceptions occurring only when $\mathcal{C}$ has a singular reduction mod p. On the other hand, the discussion of the previous subsection would suggest that a system of linear equations whose coefficients occupy few residue classes mod p, for many primes p, should be easier to solve. In a sense, Theorem 3.3 formalises this idea. Indeed, if the rows of B occupy few classes mod p then we would expect its minors to be divisible by a high power of p. A concrete estimate of this form is established in Salberger's work, giving rise to a strong lower bound on the size of D. This lower bound, when combined with Theorem 3.3, forces A to be small and as a consequence, the dimension of the space of polynomials vanishing on A to be large, as desired.

Let us finally remark that it is an interesting feature of the polynomial method that when the points being studied are already known to lie in the zero set of a polynomial with either large coefficients or large degree, this can usually be used to obtain stronger estimates. As noted by Ellenberg and Venkatesh [2005], something like this holds true in this context. In particular, it can be used to produce an improved lower bound for the left-hand side of (3-1), by assuming for the sake of contradiction that all solutions are multiples of f. This in turn gives rise to improved bounds for S when f has a large coefficient and in particular, manages to compensate a loss that appears in Salberger's bound in this case. Combining the ideas we have discussed, a uniform bound of the form $O_d(N^{2/d})$ was obtained in M. N. Walsh [2015] for the number of rational points of height at most N that an irreducible curve of degree d can have. It is easy to see that this bound is asymptotically sharp upon consideration of the equation $y = x^d$.

3.4 Exponential sums and Montgomery's conjecture. We finish this section with a brief discussion of some connections between the topics studied so far. On the one hand, the problems treated in the previous section are naturally related with each other, with such incidence problems ultimately leading to the Kakeya problem over $\mathbb{R}^n$ and the more general Stein's restriction conjecture in harmonic analysis. As we shall see in Section 4.4, the polynomial method can be extended to make progress on these problems as well.

On the other hand, we have seen that the number-theoretic topics discussed in this section are also quite interconnected. Furthermore, estimates like the large sieve inequality and the Riemann Hypothesis for curves over finite fields lead into the general area of exponential sums, where some of the most far-reaching conjectures in analytic number theory have been formulated. An outstanding example is the exponent pairs conjecture Iwaniec and Kowalski [2004], an open problem that has among its consequences the Lindelöf Hypothesis. This part of mathematics gives us an excuse to join the two lines of enquiry we have covered so far in this article. In particular, not only the density hypothesis for the zeros of the Riemann zeta function but also the Kakeya problem would follow from a positive answer to the following conjecture about exponential sums.

Conjecture 3.4 (Montgomery's Conjecture Montgomery [1971]). *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 $\varepsilon > 0$.

That this implies the Kakeya problem can be seen upon rephrasing the latter as a question about the existence of small subsets of $\mathbb{F}_p$ containing large arithmetic progressions with each possible common difference Bourgain [1991]. There is indeed a good amount of work making progress on the Kakeya problem employing tools from arithmetic combinatorics.

While this shows that analytic number theory could be used to make progress on problems related to the Kakeya problem, the opposite is also true, with progress on questions related to restriction theory being used recently to yield results in analytic number theory. Indeed, the l^2-decoupling theory started by Bourgain and Demeter [2015], a family of results in the spirit of the restriction conjecture whose proof relies on the multilinear Kakeya inequality among other things, has been used to establish Vinogradov's main conjecture in analytic number theory Bourgain, Demeter, and Guth [2016]. Previous to this work, the best result on this problem had been obtained by Wooley [2012] by means of his efficient congruencing mod p method. Finally, the set of ideas surrounding the decoupling theory was also used by Bourgain to improve the best-known exponent towards the Lindelöf Hypothesis Bourgain [2017].

It is then fair to ask to what extent the polynomial method is a tool that finds applications on a wide variety of contexts and to what extent it reflects underlying phenomenona in somewhat interconnected families of results.

4 Further topics

4.1 Baker's theorem. In order to emphasise the recurring features of the polynomial method, let us briefly discuss one last example of an application that would seem to have little connection to the topics discussed in the rest of this article, besides its link to arithmetic. Our choice is Baker's classical result in transcendental number theory regarding linear forms in logarithms Baker [1968]. For simplicity, let us discuss the integer case, where we are seeking uniform lower bounds over expressions of the form $\sum_{i=1}^{m} b_i \log a_i$, where the a_i are multiplicatively independent integers and the b_i are integers not all equal to zero.

To attack this problem, we will consider the curve $\mathcal{C} = (a_1^t, \dots, a_m^t)$, and more generally, subsets of this curve of the form

$$\mathcal{C}_N = \{(a_1^n, \dots, a_m^n) : n = 1, \dots, N\},$$

for positive integers N. Looking at the corresponding Vandermonde matrix of coefficients, the fact that the a_i are multiplicatively independent easily implies that no polynomial P of small degree, relative to N, can vanish at all points of $\mathcal{C}_N$.

A polynomial P evaluated at the curve $\mathcal{C} = (a_1^t, \ldots, a_m^t)$ may be seen as a function of the parameter t. With this point of view, we claim that we can find some value N_0, relatively small with respect to N, such that $\mathcal{C}_{N_0}$ is a characteristic subset of $\mathcal{C}_N$. Indeed, suppose we are given some polynomial P with integer coefficients and low degree that vanishes at $\mathcal{C}_{N_0}$ with some large multiplicity J with respect to the variable t. Then, $\mathcal{C}$ being an analytic curve, this will force $\frac{d^j}{dt^j}P$ to take small values in a neighbourhood of $\mathcal{C}_{N_0}$, as long as j is at least slightly smaller than J. In particular, this will happen at all points of $\mathcal{C}_{N_1}$, provided N_1 is an integer not much larger than N_0. If J is sufficiently large, we can then iterate this argument enough times as to guarantee that P itself takes small values at all points of $\mathcal{C}_N$. But since P takes integer values, the only way this can happen is if P is in fact zero at all points of $\mathcal{C}_N$.

Since $\mathcal{C}_{N_0}$ is a characteristic subset of $\mathcal{C}_N$, we know, by our observation regarding the Vandermonde matrix, that no polynomial with integer coefficients and low degree can vanish with high multiplicity at $\mathcal{C}_{N_0}$. On the other hand, if $\sum_{i=1}^m b_i \log a_i$ were to be small, an argument like in the proof of Siegel's lemma can be used to contradict this fact. Indeed, for any polynomial P with integer coefficients, a relation of this kind between the $\log a_i$ significantly restricts the range of values that the derivatives of P with respect to t can take at any given point of $\mathcal{C}_{N_0}$. In particular, this allows us to find two polynomials P_1, P_2 with integer coefficients and abnormally low degree such that, with respect to t, their first J derivatives take the same values at $\mathcal{C}_{N_0}$, for some large value of J. The polynomial $P = P_1 - P_2$ then gives us the desired contradiction.

The generality of Baker's result makes it applicable in a number of different contexts, thus implicitly extending the range of problems where the polynomial method may have some relevance. As a curious example, the integer version just discussed was used by Bourgain, Lindenstrauss, Michel, and Venkatesh [2009] to provide effective proofs of a family of results relating to Furstenberg's ×2 × 3 conjecture in ergodic theory Furstenberg [1967]. These include the well-known Rudolph-Johnson theorem Rudolph [1990] and Johnson [1992], establishing the conjecture in the positive entropy case, and Furstenberg's topological result, showing that $\mathbb{R}/\mathbb{Z}$ has no infinite closed subset other than itself that is invariant under multiplication by a pair of multiplicatively independent integers Furstenberg [1967]. One may wonder whether proofs that use the polynomial method in an explicit way may contribute to understand better such applications of Baker's theorem.

4.2 Structure and randomness. It may be worthwhile to give some brief consideration to how the polynomial method fits with the general phenomenon of structure-randomness decompositions that is pervasive throughout analysis. The idea of the latter is that it tends to be possible to decompose an object of interest into a part that detects the structure of the problem being studied and a random part that is, in a sense, completely independent from this information. In the context of Hilbert spaces, this observation can be formalised by noting that given a distinguished set Σ of bounded functions, any bounded element of the Hilbert space may be written in the form $\sum_j \lambda_j \sigma_j + g$, where the sum of the coefficients λ_j is uniformly bounded, $\sigma_j \in \Sigma$ for every j, and g is essentially orthogonal to Σ, in the sense that $\langle g, \sigma \rangle$ is small for every $\sigma \in \Sigma$. We refer the reader to this article Gowers [2010] of Gowers for an elegant discussion of this and more general decompositions.

The polynomial method may be considered a useful complement to the structure-randomness approach when the arithmetic of the problem gives rise to an underlying algebraic structure. The characteristic subsets notation used in M. N. Walsh [2012b, 2014] and in the present article is, in fact, inspired by the concept of characteristic factors that plays the role of the structured part in several problems in ergodic theory Furstenberg [1967], Furstenberg and Weiss [1996], and Host and Kra [2005]. In the same way that information about the behaviour of a polynomial on a set can be deduced from what happens in a characteristic subset, the behaviour of nonconventional ergodic averages over a set of functions can be deduced from what happens in the corresponding characteristic factors. This is exactly what these decompositions seek to accomplish.

Structure-randomness decompositions are a flexible tool that can be substantially refined when a small error term is allowed in the decompositions. This played an important role in the convergence result of M. N. Walsh [2012a] and we refer again to Gowers' article Gowers [2010] for a general discussion. As noted by Lovász and Szegedy [2007], these more general decompositions can be seen as versions of the Szemerédi regularity lemma Szemerédi [1978]. The regularity lemma was itself the key tool used to obtain the cell-decomposition in the original proof of the Szemerédi-Trotter theorem and, in this sense, the polynomial partitioning method of Guth an Katz may be seen as an instance of these general decomposition results where the algebraic nature of the decomposition is made more explicit.

4.3 Polynomial partitioning over varieties. In order to apply the polynomial method efficiently over general varieties some further improvements may be needed. During the discussion of the determinant method, we observed how the polynomial method could be made more effective when the points being studied lie in the zero set of some polynomial with large coefficients. One may similarly wonder whether knowing that the points lie inside of an algebraic variety of high degree may also lead to improved estimates. Since it is known that the dimension of the polynomial ring associated with a variety increases in proportion with its degree Nesterenko [1984], it is logical to suspect that a corresponding improvement may be achieved on the kind of dimension counting arguments that are ubiquitous in the polynomial method. Indeed, combining this kind of observations with the type of tools used to prove Theorem 2.5, we can obtain the following result.

Theorem 4.1 (Polynomial partitioning over varieties M. Walsh [n.d.]). *Given any real algebraic variety $V \subseteq \mathbb{R}^n$ of dimension d, any set of points $S \subseteq V$ and any integer $M \geq 1$, there exists some polynomial $P \in \mathbb{R}[x_1, \ldots, x_n]$ of degree $\lesssim_{d,n} M$, not vanishing identically on V, such that each connected component of $V \setminus Z(P)$ contains at most $\lesssim_{d,n} \frac{|S|}{M^d \deg(V)}$ points of S.*

That this should hold was already conjectured in Basu and Sombra [2016]. A more general sharp estimate was obtained in M. Walsh [n.d.] by including an additional explicit dependence on the degrees of the various individual polynomials defining the variety V. Notice that a particular case of the above result is a version of Siegel's lemma that allows us to find a polynomial of degree $\lesssim_{d,n} \frac{|S|^{1/d}}{\deg(V)^{1/d}}$ that vanishes on S without vanishing identically on V.

As we saw in Section 2.3, both the nature of incidence geometry and of polynomial partitioning techniques lead to the consideration of lower-dimensional algebraic varieties, even for problems that originally take place over $\mathbb{R}^n$. Without proper tools to handle varieties of high degree, the polynomial partitioning needs to be truncated as to produce only varieties of low degree, leading to suboptimal bounds. Estimates like Theorem 4.1 may prove useful in providing a unified approach to manage these problems and produce sharp bounds.

Nevertheless, to make this work, we saw that a second result that is needed is a bound on how many of the components produced by the above partitioning result can be touched by a given algebraic variety W. In general, by work of Milnor [1964] and Thom [1965], we have bounds that give a good dependence in terms of the degree of the partitioning polynomial, but not in terms of W. Some progress on this issue has been made by Barone and Basu [2012], who were able to obtain an estimate with a good dependence on the product of the degrees of the polynomials defining W, with this result being subsequently applied in incidence geometry Basu and Sombra [2016].

Since in general estimates like Theorem 4.1 can only be expected to yield a saving proportional to the degree of the variety V itself, it may be necessary to obtain a version of the result of Barone and Basu that depends only on the degree of W, instead of depending on the product of the degrees of the polynomials defining it. A step in this direction was taken in M. Walsh [n.d.] where a bound with a main term of the desired form was obtained. Nevertheless, the error term in this estimate is not optimal and it remains an interesting problem to improve it. In fact, it is shown in M. Walsh [ibid.] that a suitable refinement can indeed be combined with Theorem 4.1 to attain sharp incidence bounds that currently remain out of reach.

4.4 Restriction estimates. The proof of Theorem 4.1 combines algebraic estimates for the size of ideals with tools like the polynomial ham-sandwich theorem, the latter being a result that lies at the heart of polynomial partitioning results since the original work of Guth and Katz. The classical ham-sandwich theorem states that given n open sets in $\mathbb{R}^n$, they can always be simultaneously bisected by a suitable hyperplane. The polynomial ham-sandwich theorem extends this claim to show that we can always bisect a larger number of open sets as long as, instead of restricting to hyperplanes, we allow the bisection to be performed by hypersurfaces of a correspondingly large degree.

This bisecting result can be further put to use to extend the scope of the polynomial method to the Kakeya conjecture in Euclidean space. This conjecture can be sen as a question about estimating the minimal possible volume that can be attained by a collection of tubes pointing in a large number of quantitatively distinct directions. Covering this union by a family of small cubes and replacing the notion of a polynomial vanishing at a point by that of a polynomial bisecting a cube, the ideas surrounding the polynomial method can be extended from the discrete case to this continuous setting.

Recall that to find characteristic subsets we have relied heavily on estimates on the intersection of algebraic sets. For example, that given a polynomial P not vanishing identically on a given line, this line can only intersect $Z(P)$ in at most $\deg(P)$ points. In order to carry the polynomial method to this new context, we need to find analogues of these estimates that hold true for tubes. For example, we may observe that if a polynomial P takes small values at more than $C\deg(P)$ points along a fixed tube, for some sufficiently large constant C, then it must also take small values at most places that lie between these points. Similarly, another alternative is to consider the directed volume of a surface, allowing one more or less to conclude that a polynomial P can cut a tube transversally in at most $O(\deg(P))$ places.

By introducing these ideas, Guth essentially showed in Guth [2016b] that a counterexample to the Kakeya problem in $\mathbb{R}^3$ can be approximated by a polynomial of the smallest possible degree allowed by the Crofton formula, and used this to obtain graininess estimates in the spirit of Katz, Łaba, and Tao [2000]. He also combined these ideas with slightly more sophisticated tools from algebraic topology, involving cohomology classes and Lusternik-Schnirelmann theory, to obtain the first proof Guth [2010] of the endpoint case of the multilinear Kakeya inequality of Bennett, Carbery, and Tao [2006].

It is even possible to extend the polynomial method further to make progress on the more general restriction conjecture of Stein [1979]. Here, by applying a decomposition into wave packets, we can translate the problem into a question about overlapping patterns of tubes and this can be treated in a similar spirit as the incidence geometry questions that we discussed in Section 2.3. Indeed, the polynomial partitioning method works in a very similar way, as long as we replace the zero set of the partitioning polynomial by its neighbourhood, as to be able to bound the number of cells of the resulting partition that a tube can intersect Guth [2016a]. It should be remarked that this approach helps to highlight the role played by low degree varieties in hypothetical counterexamples to this conjecture. Whether this kind of ideas based on the polynomial method will lead to further progress on this sort of problems remains an interesting question.

References

E. Artin (1924). "Quadratische Körper im Gebiete der höheren Kongruenzen. II". *Math. Z.* 19.1, pp. 207–246. MR: 1544652 (cit. on p. 492).

A. Baker (1968). "Linear forms in the logarithms of algebraic numbers. IV". *Mathematika* 15, pp. 204–216. MR: 0258756 (cit. on p. 496).

Sal Barone and Saugata Basu (2012). "Refined bounds on the number of connected components of sign conditions on a variety". *Discrete Comput. Geom.* 47.3, pp. 577–597. MR: 2891249 (cit. on p. 499).

Saugata Basu and Martín Sombra (2016). "Polynomial partitioning on varieties of codimension two and point-hypersurface incidences in four dimensions". *Discrete Comput. Geom.* 55.1, pp. 158–184. MR: 3439263 (cit. on p. 499).

Jonathan Bennett, Anthony Carbery, and Terence Tao (2006). "On the multilinear restriction and Kakeya conjectures". *Acta Math.* 196.2, pp. 261–302. MR: 2275834 (cit. on p. 500).

E. Bombieri and J. Pila (1989). "The number of integral points on arcs and ovals". *Duke Math. J.* 59.2, pp. 337–357. MR: 1016893 (cit. on p. 494).

E. Bombieri and J. Vaaler (1983). "On Siegel's lemma". *Invent. Math.* 73.1, pp. 11–32. MR: 707346 (cit. on p. 494).

Enrico Bombieri (1974). "Counting points on curves over finite fields (d'après S. A. Stepanov)", 234–241. Lecture Notes in Math., Vol. 383. MR: 0429903 (cit. on p. 491).

J. Bourgain (1991). "Remarks on Montgomery's conjectures on Dirichlet sums". In: *Geometric aspects of functional analysis (1989–90)*. Vol. 1469. Lecture Notes in Math. Springer, Berlin, pp. 153–165. MR: 1122620 (cit. on p. 496).

– (2017). "Decoupling, exponential sums and the Riemann zeta function". *J. Amer. Math. Soc.* 30.1, pp. 205–224. MR: 3556291 (cit. on p. 496).

Jean Bourgain and Ciprian Demeter (2015). "The proof of the l^2 decoupling conjecture". *Ann. of Math. (2)* 182.1, pp. 351–389. MR: 3374964 (cit. on p. 496).

Jean Bourgain, Ciprian Demeter, and Larry Guth (2016). "Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three". *Ann. of Math. (2)* 184.2, pp. 633–682. MR: 3548534 (cit. on p. 496).

Jean Bourgain, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh (2009). "Some effective results for $\times a \times b$". *Ergodic Theory Dynam. Systems* 29.6, pp. 1705–1722. MR: 2563089 (cit. on p. 497).

Zeev Dvir (2009). "On the size of Kakeya sets in finite fields". *J. Amer. Math. Soc.* 22.4, pp. 1093–1097. MR: 2525780 (cit. on p. 488).

– (2010). "Incidence theorems and their applications". *Found. Trends Theor. Comput. Sci.* 6.4, 257–393 (2012). MR: 3004132 (cit. on p. 487).

György Elekes (1997). "On the number of sums and products". *Acta Arith.* 81.4, pp. 365–367. MR: 1472816 (cit. on p. 487).

György Elekes and Micha Sharir (2010). "Incidences in three dimensions and distinct distances in the plane [extended abstract]". In: *Computational geometry (SCG'10)*. ACM, New York, pp. 413–422. MR: 2742978 (cit. on p. 487).

György Elekes and Endre Szabó (2012). "How to find groups? (and how to use them in Erdős geometry?)" *Combinatorica* 32.5, pp. 537–571. MR: 3004808 (cit. on p. 487).

J. Ellenberg and A. Venkatesh (2005). "On uniform bounds for rational points on nonrational curves". *Int. Math. Res. Not.* 35, pp. 2163–2181. MR: 2181791 (cit. on p. 495).

P. Erdős (1946). "On sets of distances of n points". *Amer. Math. Monthly* 53, pp. 248–250. MR: 0015796 (cit. on p. 487).

P. Erdős and E. Szemerédi (1983). "On sums and products of integers". In: *Studies in pure mathematics*. Birkhäuser, Basel, pp. 213–218. MR: 820223 (cit. on p. 487).

Harry Furstenberg (1967). "Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation". *Math. Systems Theory* 1, pp. 1–49. MR: 0213508 (cit. on pp. 497, 498).

– (1977). "Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions". *J. Analyse Math.* 31, pp. 204–256. MR: 0498471.

Hillel Furstenberg and Benjamin Weiss (1996). "A mean ergodic theorem for $(1/N)\sum_{n=1}^{N} f(T^n x)g(T^{n^2}x)$". In: *Convergence in ergodic theory and probability (Columbus, OH, 1993)*. Vol. 5. Ohio State Univ. Math. Res. Inst. Publ. de Gruyter, Berlin, pp. 193–227. MR: 1412607 (cit. on p. 498).

W. T. Gowers (2010). "Decompositions, approximate structure, transference, and the Hahn-Banach theorem". *Bull. Lond. Math. Soc.* 42.4, pp. 573–606. MR: 2669681 (cit. on p. 498).

Ben Green (2014). "Approximate algebraic structure". In: *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. 1*. Kyung Moon Sa, Seoul, pp. 341–367. MR: 3728475 (cit. on p. 487).

Ben Green and Adam J. Harper (2014). "Inverse questions for the large sieve". *Geom. Funct. Anal.* 24.4, pp. 1167–1203. MR: 3248483 (cit. on p. 493).

Larry Guth (2010). "The endpoint case of the Bennett-Carbery-Tao multilinear Kakeya conjecture". *Acta Math.* 205.2, pp. 263–286. MR: 2746348 (cit. on p. 500).

– (2016a). "A restriction estimate using polynomial partitioning". *J. Amer. Math. Soc.* 29.2, pp. 371–413. MR: 3454378 (cit. on p. 500).

– (2016b). "Degree reduction and graininess for Kakeya-type sets in $\mathbb{R}^3$". *Rev. Mat. Iberoam.* 32.2, pp. 447–494. MR: 3512423 (cit. on p. 500).

– (2016c). *Polynomial methods in combinatorics*. Vol. 64. University Lecture Series. American Mathematical Society, Providence, RI, pp. ix+273. MR: 3495952 (cit. on p. 485).

Larry Guth and Nets Hawk Katz (2015). "On the Erdős distinct distances problem in the plane". *Ann. of Math. (2)* 181.1, pp. 155–190. MR: 3272924 (cit. on pp. 488, 490).

Brandon Hanson (2017). "Additive Correlation and the Inverse Problem for the Large Sieve". arXiv: 1706.06958 (cit. on p. 493).

Helmut Hasse (1936). "Zur Theorie der abstrakten elliptischen Funktionenkörper III". *Crelle's Journal* 175, pp. 193–208 (cit. on p. 492).

D. R. Heath-Brown (2002). "The density of rational points on curves and surfaces". *Ann. of Math. (2)* 155.2, pp. 553–595. MR: 1906595 (cit. on p. 494).

H. A. Helfgott and A. Venkatesh (2009). "How small must ill-distributed sets be?" In: *Analytic number theory*. Cambridge Univ. Press, Cambridge, pp. 224–234. MR: 2508647 (cit. on pp. 492, 493).

Harald A. Helfgott (2015). "Growth in groups: ideas and perspectives". *Bull. Amer. Math. Soc. (N.S.)* 52.3, pp. 357–413. MR: 3348442 (cit. on p. 487).

Bernard Host and Bryna Kra (2005). "Nonconventional ergodic averages and nilmanifolds". *Ann. of Math. (2)* 161.1, pp. 397–488. MR: 2150389 (cit. on p. 498).

Henryk Iwaniec and Emmanuel Kowalski (2004). *Analytic number theory*. Vol. 53. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, pp. xii+615. MR: 2061214 (cit. on p. 495).

Aimee S. A. Johnson (1992). "Measures on the circle invariant under multiplication by a nonlacunary subsemigroup of the integers". *Israel J. Math.* 77.1-2, pp. 211–240. MR: 1194793 (cit. on p. 497).

Nets Hawk Katz (2014). "The flecnode polynomial: a central object in incidence geometry". In: *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. III*. Kyung Moon Sa, Seoul, pp. 303–314. MR: 3729029 (cit. on p. 491).

Nets Hawk Katz, Izabella Łaba, and Terence Tao (2000). "An improved bound on the Minkowski dimension of Besicovitch sets in $\mathbf{R}^3$". *Ann. of Math. (2)* 152.2, pp. 383–446. MR: 1804528 (cit. on p. 500).

László Lovász and Balázs Szegedy (2007). "Szemerédi's lemma for the analyst". *Geom. Funct. Anal.* 17.1, pp. 252–270. MR: 2306658 (cit. on p. 498).

J. Milnor (1964). "On the Betti numbers of real varieties". *Proc. Amer. Math. Soc.* 15, pp. 275–280. MR: 0161339 (cit. on p. 499).

Hugh L. Montgomery (1971). *Topics in multiplicative number theory*. Lecture Notes in Mathematics, Vol. 227. Springer-Verlag, Berlin-New York, pp. ix+178. MR: 0337847 (cit. on p. 495).

Yu. V. Nesterenko (1984). “Estimates for the characteristic function of a prime ideal”. *Mat. Sb. (N.S.)* 123(165).1, pp. 11–34. MR: 728927 (cit. on p. 498).

János Pach and Micha Sharir (1998). “On the number of incidences between points and curves”. *Combin. Probab. Comput.* 7.1, pp. 121–127. MR: 1611057 (cit. on p. 486).

I. G. Petrovskiĭ and O. A. Oleĭnik (1949). “On the topology of real algebraic surfaces”. *Izvestiya Akad. Nauk SSSR. Ser. Mat.* 13, pp. 389–402. MR: 0034600 (cit. on p. 490).

Daniel J. Rudolph (1990). “×2 and ×3 invariant measures and entropy”. *Ergodic Theory Dynam. Systems* 10.2, pp. 395–406. MR: 1062766 (cit. on p. 497).

Per Salberger (2010). “Counting rational points on projective varieties”. preprint (cit. on p. 494).

E. M. Stein (1979). “Some problems in harmonic analysis”. In: *Harmonic analysis in Euclidean spaces (Proc. Sympos. Pure Math., Williams Coll., Williamstown, Mass., 1978), Part 1*. Proc. Sympos. Pure Math., XXXV, Part. Amer. Math. Soc., Providence, R.I., pp. 3–20. MR: 545235 (cit. on p. 500).

S. A. Stepanov (1969). “The number of points of a hyperelliptic curve over a finite prime field”. *Izv. Akad. Nauk SSSR Ser. Mat.* 33, pp. 1171–1181. MR: 0252400 (cit. on p. 491).

Endre Szemerédi (1978). “Regular partitions of graphs”. In: *Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976)*. Vol. 260. Colloq. Internat. CNRS. CNRS, Paris, pp. 399–401. MR: 540024 (cit. on p. 498).

Endre Szemerédi and William T. Trotter Jr. (1983). “Extremal problems in discrete geometry”. *Combinatorica* 3.3-4, pp. 381–392. MR: 729791 (cit. on p. 486).

Terence Tao (2014). “Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory”. *EMS Surv. Math. Sci.* 1.1, pp. 1–46. MR: 3200226 (cit. on p. 485).

René Thom (1965). “Sur l’homologie des variétés algébriques réelles”. In: *Differential and Combinatorial Topology (A Symposium in Honor of Marston Morse)*. Princeton Univ. Press, Princeton, N.J., pp. 255–265. MR: 0200942 (cit. on p. 499).

M. Walsh (n.d.). *Polynomial partitioning over varieties*. Preprint (cit. on p. 499).

Miguel N. Walsh (2012a). “Norm convergence of nilpotent ergodic averages”. *Ann. of Math. (2)* 175.3, pp. 1667–1688. MR: 2912715 (cit. on p. 498).

– (2012b). “The inverse sieve problem in high dimensions”. *Duke Math. J.* 161.10, pp. 2001–2022. MR: 2954623 (cit. on pp. 489, 493, 498).

– (2014). “The algebraicity of ill-distributed sets”. *Geom. Funct. Anal.* 24.3, pp. 959–967. MR: 3213836 (cit. on pp. 493, 498).

– (2015). “Bounded rational points on curves”. *Int. Math. Res. Not. IMRN* 14, pp. 5644–5658. MR: 3384452 (cit. on p. 495).

André Weil (1949). “Numbers of solutions of equations in finite fields”. *Bull. Amer. Math. Soc.* 55, pp. 497–508. MR: 0029393 (cit. on p. 492).

Thomas Wolff (1999). “Recent work connected with the Kakeya problem”. In: *Prospects in mathematics (Princeton, NJ, 1996)*. Amer. Math. Soc., Providence, RI, pp. 129–162. MR: 1660476 (cit. on p. 488).

Trevor D. Wooley (2012). “Vinogradov’s mean value theorem via efficient congruencing”. *Ann. of Math. (2)* 175.3, pp. 1575–1627. MR: 2912712 (cit. on p. 496).

Received 2017-12-03.

Miguel N. Walsh
Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
1428 Buenos Aires
Argentina
walsh@maths.ox.ac.uk
mwalsh@dm.uba.ar