The polynomial method and Kakeya conjecture

Marcin Kotowski, Michał Kotowski

August 30, 2012

Contents

1 Polynomials of several variables

We will be working with polynomials of several variables, sometimes over an arbitary field $\mathbb{F}$, but usually over a finite field such as $\mathbb{Z}_p$ for prime p. For example:

$$P(x, y) = x^2 + y^2 - xy + 1$$

is a polynomial of two variables x, y and:

$$Q(x_1, x_2, \ldots, x_n) = x_1 \ldots x_n + x_1 + \ldots + x_n$$

is a polynomial of n variables.

The set of all polynomials over a field $\mathbb{F}$ in variables $x_1, \ldots, x_n$ is often denoted by $\mathbb{F}[x_1, \ldots, x_n]$.

For n variables $x_1, \ldots, x_n$ a *monomial* is a polynomial of the form $ax_1^{c_1} \ldots x_n^{c_n}$, where $c_i \geq 0$ and a is a coefficient from the field $\mathbb{F}$. The *total degree* (or simply degree) of a monomial is the sum $c_1 + \ldots + c_n$. Every polynomial can be written as a sum of monomials with nonzero coefficients and the total degree of a polynomial is the maximum degree of its monomials. For example, x^2yz has degree 4, while $x^2 + y + z$ has degree 2, since x^2 highest term.

Sometimes we will be interested in treating all variables but one as "fixed" and considering the polynomial as a polynomial of only one remaining variable, with its coefficients now being polynomials in the other variables. For example, if we treat $P(x,y) = x^2y + x^2 + xy^3$ as a polynomial of variable x only, then the coefficient of x^2 in $P(x,y)$ is $y+1$ and the coefficient of x is y^3.

A tuple $(s_1, \ldots, s_n) \in \mathbb{F}^n$ is called a *zero* of a polynomial $P(x_1, \ldots, x_n)$ of n variables if $P(s_1, \ldots, s_n)$. A familiar property of polynomials of one variable is that a polynomial of degree t can have at most t zeroes (possibly repeated). This is of course not true for polynomials of several variables - for example, $P(x,y) = xy$ as a polynomial over $\mathbb{R}$ vanishes on all pairs $(x,0), (0,y)$, $x, y \in \mathbb{R}$, so it has infinitely many zeroes. Nevertheless in a certain sense the zero set of a polynomial of low total degree cannot be too "complex", it cannot "wind" too much, in the same way as a polynomial of one variable cannot change its sign too often without having many zeroes. This observation, formulated more precisely in Combinatorial Nullstellensatz below, turns out to be surpisingly useful in solving combinatorial problems and will be the starting point of this course.

Before we get to the combinatorial meat, a few remarks about polynomials over finite fields would be in place. Every polynomial P of n variables over a field $\mathbb{F}$ can be treated as a function $P : \mathbb{F}^n \to \mathbb{F}$, simply by evaluating the polynomial on every tuple from $\mathbb{F}^n$. However, as we will see below, it is important to distinguish between the polynomial as an *algebraic expression*, involving some monomials and their coefficients, and the corresponding *function*, mapping field elements (or tuples of elements) to field elements.

For example, suppose we have a function of one variable $f(x)$ over a finite field $\mathbb{F}$ and we know its values at k distinct points $s_1, \ldots, s_k$. Then it is easy to find a polynomial $P(x)$ which agrees with f on those points by *Lagrange interpolation*:

$$P(x) = \sum_{i=1}^{d+1} f(s_i) \prod_{\substack{j=1 \\ j \neq i}}^{d+1} \frac{x - s_j}{s_i - s_j}$$

One readily checks that $P(s_i) = f(s_i)$ for all i. In particular every function can be represented by a polynomial of degree at most $|\mathbb{F}|$ simply by taking $s_1, \ldots, s_k$ to be all elements of $\mathbb{F}$. Thus over finite fields there is no difference between polynomials and arbitrary functions if we are interested only in values they take and not in their algebraic form. Note however that this representation is not unique - consider for example two polynomials:

$$P(x) = 0$$
$$Q(x) = x^p - x$$

over $\mathbb{Z}_p$. For every $y \in \mathbb{Z}_p$ we have $Q(y) = y^p - y = 0 \mod p$ by Fermat's little theorem. So although $Q(x)$ is not equal to zero as an algebraic expression, as a function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ it is equal to a constant zero function.

Since we will be interested mostly in algebraic or combinatorial properties of various objects, for us the *zero polynomial* will be a polynomial with all coefficients equal to 0 and not simply a constant zero function.

2 Combinatorial Nullstellensatz

Theorem 2.1 (Combinatorial Nullstellensatz)**.** *Let $P(x_1, \ldots, x_n)$ be a polynomial in n variables over arbitrary field $\mathbb{F}$. Suppose that P has degree d and the coefficient of $x_1^{d_1} \ldots x_n^{d_n}$, with $d_1 + \ldots + d_n = d$, is nonzero. Then for any sets $S_1, \ldots, S_n \subseteq \mathbb{F}$ such that $|S_i| > d_i$ there exist $s_1, \ldots, s_n$, with $s_i \in S_i$, such that $P(s_1, \ldots, s_n) \neq 0$.*

Proof. We use induction on n. The base case $n = 1$ is obvious, so assume $n \geq 2$ and that we have proved the theorem for $n - 1$.

Suppose by contradiction that $P(s_1, \ldots, s_n)$ for all $s_i \in S_i$. For any $s \in S_1$ we can write:

$$P(x_1, \ldots, x_n) = (x_1 - s)Q(x_1, \ldots, x_n) + R(x_1, \ldots, x_n)$$

for some polynomials Q and R. The polynomial R does not depend on x_1. By the assumption on the coefficient of $x_1^{d_1} \ldots x_n^{d_n}$ in P the polynomial Q must have nonzero coefficient of $x_1^{d_1 - 1} \ldots x_n^{d_n}$ and we have $\deg(Q) = d - 1$.

Now if we substitute any $(s, s_2, \ldots, s_n)$, $s_i \in S_i$, into the equation above, we have $P(s, s_2, \ldots, s_n) = 0$ by assumption, so $R(s, s_2, \ldots, s_n) = 0$. But R does not actually depend on the first variable, so R vanishes for any $s_2, \ldots, s_n$. Now substitute $(s', s_2, \ldots, s_n)$ into the equation for some $s' \neq s$. Then we get:

$$0 = P(s', s_2, \ldots, s_n) = (s' - s)Q(s', s_2, \ldots, s_n) + R(s', s_2, \ldots, s_n) = (s' - s)Q(s', s_2, \ldots, s_n)$$

so we must have $Q(s', s_2, \ldots, s_n) = 0$ for any $s' \neq s$ and $s_2, \ldots, s_n$. But by induction hypothesis Q cannot vanish on every point of $(S_1 \backslash \{s\}) \times S_2 \times \ldots \times S_n$, so we arrive at a contradiction.

□

Before we move to the applications of the theorem, a few words about terminology. The name "Combinatorial Nullstellensatz" comes from an analogy with the fundamental Hilbert's Nullstellensatz in algebra. In one of its variants it states that if $P, Q_1, \ldots, Q_m$ are polynomials in variables $x_1, \ldots, x_n$ over an algebraically closed field and f vanishes over all common zeroes of $g_1, \ldots, g_m$, then there exists some polynomials $H_1, \ldots, H_m$ such that:

$$P^k = H_1 G_1 + \ldots H_m G_m$$

for some integer k.

What we call Combinatorial Nullstellensatz is a consequence of a more general theorem which bears more resemblance to Hilbert's Nulstellensatz and works over an arbitrary field (although we will not need it in combinatorial applications).

Theorem 2.2. *Let $S_1, \ldots, S_n$ be subsets of an arbitrary field $\mathbb{F}$ and let:*

$$G_i(x_i) = \prod_{s_i \in S_i} (x - s_i)$$

be polynomials over $\mathbb{F}$. *If* $P(x_1, \ldots, x_n)$ *is a polynomial such that* $P(s_1, \ldots, s_n) = 0$ *for all* $s_i \in S_i$, *then:*

$$P = H_1 G_1 + \ldots + H_n G_n$$

for some polynomials H_i *satisfying* $\deg(H_i) \leq \deg(P) - \deg(G_i)$

Combinatorial Nullstellensatz is often used to show the existence or prove lower bounds on the size of a combinatorial object. Such proofs are nonconstructive, i.e. they don't show how to construct objects that we are interested in, but nevertheless sometimes this is the easiest way to obtain the desired bound. A typical way of proving a lower bound on the size of a set with desired properties would be as follows:

- Assume by contradiction that the set we are investigating is small
- Find a polynomial which vanishes on our set
- Show that the appropriate coefficient in the polynomial is nonzero
- If our set is small, the polynomial's degree is likely to be low, so we can conclude by Combinatorial Nullstellensatz that there must exist a point in our set where the polynomial is nonzero
- The contradiction proves that our set cannot be too small

This type of argument captures the intuition that low-degree polynomials can vanish only on sets which in some sense have "low complexity". We will see different variants of such proofs in the problems.

Problem 2.1 (Cauchy-Davenport Theorem)**.** *Let* p *be a prime number and let* A, B *be nonempty subsets of* $\mathbb{Z}_p$. *Let:*

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

Prove that:

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

Proof. If $|A| + |B| > p$, then $A + B = \mathbb{Z}_p$ - for any $x \in \mathbb{Z}_p$ we have $|B| = |x - B|$, so A and $x - B$ have nonempty intersection, which implies that $a = x - b$ for some $a \in A, b \in B$, so $x = a + b$ and $x \in A + B$ as desired.

So let $|A| + |B| \leq p$ and suppose that $|A + B| \leq |A| + |B| - 2 < p$. Let C be the subset of $\mathbb{Z}_p$ such that $A + B \subseteq C$ and $|C| = |A| + |B| - 2$. Consider a polynomial:

$$P(x, y) = \prod_{c \in C} (x + y - c)$$

Its degree is equal to $|A|+|B|-2$. By definition of C we have $P(a, b) = 0$ for all $a \in A$, $b \in B$. The coefficient of $x^{|A|-1} y^{|B|-1}$ in $P(x, y)$ is $\binom{|A|+|B|-2}{|A|-1} \neq 0$ in $\mathbb{Z}_p$, since $|A| + |B| - 2 < p$. By Combinatorial Nullstellensatz applied to $S_1 = A$, $S_2 = B$ we have that there exists a pair $a' \in A$, $b' \in B$ such that $P(a', b') \neq 0$, which is a contradiction. Thus $|A + B| \geq |A| + |B| - 1$ □

Problem 2.2. *Let p be a prime number and let A, B be nonempty subsets of $\mathbb{Z}_p$ with $|A| \neq |B|$. Let:*

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

Prove that:

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

Deduce the Erdős-Heilbronn conjecture:

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

Proof. As before, we can assume that $|A|+|B|-2 \leq p$ - if not, then for any $x \in \mathbb{Z}_p$ we have $|A|+|x-B| \geq p+3$, which implies that $|A \cap (x-B)| \geq 2$. Therefore there exists elements $a, a' \in A$, $a \neq a'$, and $b, b' \in B$, $b \neq b'$, such that $a+b = a'+b' = x$. If $a \neq b$ or $a' \neq b'$, then we are done. If not then we have $2a = 2a'$ which implies $a = a'$, a contradiction, unless $p = 2$, but the theorem is trivial in the latter case. Therefore $A\widehat{+}B = \mathbb{Z}_p$.

Suppose now that $|A\widehat{+}B| \leq |A|+|B|-3$. We use the same approach as in the previous problem. Let C be such that $A\widehat{+}B \subseteq C$ and $|C| = |A|+|B|-3$. Consider a polynomial:

$$P(x,y) = (x-y)\prod_{c \in C}(x+y-c)$$

It has degree $|C|+1 = |A|+|B|-2$. Since $A\widehat{+}B \subseteq C$, we have $P(a,b) = 0$ for all $a \in A$, $b \in B$. The coefficient of $x^{|A|-1}y^{|B|-1}$ is:

$$\binom{|A|+|B|-3}{|A|-2} - \binom{|A|+|B|-3}{|A|-1} = \frac{|A|-|B|}{|B|-1}\binom{|A|+|B|-3}{|A|-2} \neq 0$$

since $|A|+|B|-3 \leq p-1$ (note that we can assume $|B| \neq 1$, since the theorem is trivial in that case). By applying Combinatorial Nullstellensatz with $S_1 = A$, $S_2 = B$ there exists a pair $a' \in A$, $b' \in B$ such that $P(a', b') \neq 0$, a contradiction. Therefore $|A\widehat{+}B| \geq |A|+|B|-2$.

To deduce the Erdős-Heilbronn conjecture, simply delete any element from A and apply the previous result to A and the obtained set. □

Erdős-Heilbronn conjecture can be thought of as a generalization of Cauchy-Davenport theorem in which we restrict the allowed values $a+b$ to those which satisfy a certain polynomial condition - for example, the condition $a \neq b$ means that the polynomial $h(x,y) = x-y$ must be nonvanishing on a, b. It turns out that the same technique as above can be used to solve restricted sumset problems for general polynomial conditions.

Problem 2.3. *Let $A_1, \ldots, A_k$ be nonempty subsets of $\mathbb{Z}_p$ and let $h(x_1, \ldots, x_k)$ be a polynomial over $\mathbb{Z}_p$. Let:*

$$A_h = \{a_1 + \ldots + a_k \,:\, a_i \in A_i,\, h(a_1, \ldots, a_k) \neq 0\}$$

and $m = (|A_1|+1)+\ldots+(|A_k|+1)-\deg(h)$. Prove that if the coefficient of $x_1^{|A_1|-1}\ldots x_k^{|A_k|-1}$ in

$$(x_1+\ldots+x_k)^m h(x_1, \ldots, x_k)$$

is nonzero, then:

$$|A_h| \geq m+1$$

Proof. Suppose by contradiction that $|A_h| \leq m$ and let B be the smallest set containing A_h such that $|B| = m$. Consider the polynomial:

$$P(x_1, \ldots, x_k) = h(x_1, \ldots, x_k) \prod_{b \in B} (x_1 + \ldots + x_k - b)$$

Note that P vanishes on all points $(a_1, \ldots, a_k) \in A_1 \times \ldots \times A_k$, since either $a_1 + \ldots + a_k \in A_h \subseteq B$ or $h(a_1, \ldots, a_k) = 0$.

Because of the assumption on the coefficient of $x_1^{|A_1|-1} \ldots x_k^{|A_k|-1}$ we have $\deg(P) = m + \deg(h)$. On other hand by definition of B we have that P vanishes on every point of $A_1 \times \ldots \times A_k$, which contradicts Combinatorial Nullstellensatz. □

Of course, the whole difficulty of using this approach to solve restricted sumset problems lies in calculating the coefficient of $x_1^{|A_1|-1} \ldots x_k^{|A_k|-1}$ in the appropriate polynomial. An example where this requires nontrivial combinatorics, but gives a nice generalization of Problem 2.2, is the following problem.

Problem 2.4. *Let $A_1, \ldots, A_k$ be nonempty subsets of $\mathbb{Z}_p$ such that $|A_i| \neq |A_j|$ for $i \neq j$ and $|A_1| + \ldots + |A_k| \leq p + \binom{k+1}{2} - 1$. For:*

$$A = \{a_1 + \ldots + a_k \,:\, a_i \in A_i,\, a_i \neq a_j \text{ for all } i \neq j\}$$

prove that:

$$|A| \geq |A_1| + \ldots + |A_k| - \binom{k+1}{2} + 1$$

Hint: show that for $m = a_1 + \ldots + a_n - \binom{n}{2}$ the coefficient of $x_1^{a_1} \ldots x_n^{a_n}$ in

$$(x_1 + \ldots + x_n)^m \prod_{i<j} (x_i - x_j)$$

is

$$\frac{m!}{a_1! a_2! \ldots a_n!} \prod_{i<j} (a_i - a_j)$$

Proof. See [ANR96]. □

Problem 2.5. *Suppose we want to find a family of hyperplanes in $\mathbb{R}^n$ such that their union covers all vertices of the unit cube $\{0,1\}^n$ but one (i.e. exactly one vertex is left uncovered). Prove that at least n hyperplanes are needed.*

Proof. We can assume that the uncovered vertex is $(0, \ldots, 0)$. Let the i-th hyperplane H_i be defined by the equation

$$H_i = \{x \in \mathbb{R}^n \,:\, a_i \cdot x = b_i\}$$

where $x = (x_1, \ldots, x_n)$, a_i are vectors in $\mathbb{R}^n$, $b_i \in \mathbb{R}$ and "$\cdot$" denotes the standard inner product. Note that $b_i \neq 0$ for all i, since we assume that $(0, \ldots, 0)$ is not covered.

Suppose that we can find a family of $m < n$ hyperplanes with the desired property. Consider the polynomial of n variables:

$$P(x_1, \ldots, x_n) = (-1)^{m+n+1}(b_1 \cdot \ldots \cdot b_m) \prod_{i=1}^{n}(x_i - 1) + \prod_{i=1}^{m}(x \cdot a_i - b_i)$$

First observe that:

$$P(0, \ldots, 0) = (-1)^{m+n+1}(b_1 \cdot \ldots \cdot b_m)(-1)^n + \prod_{i=1}^{m}(-b_i) = (-1)^{m+1}(b_1 \cdot \ldots \cdot b_m) + (-1)^m(b_1 \cdot \ldots \cdot b_m) = 0$$

The polynomial has degree n (as $m < n$, so the term involving inner products is of lower degree) and the coefficient of $x_1 \ldots x_n$ is $(-1)^{m+n+1} b_1 \cdot \ldots \cdot b_m \neq 0$. By applying Combinatorial Nullstellensatz for $S_i = \{0, 1\}$ there exists a point $s \in \{0, 1\}^n$ such that $P(s) \neq 0$. Because $P(0) = 0$, we have $s \neq 0$, so it is covered by some hyperplane H_j, which implies $s \cdot a_j - b_j = 0$. But then the second product in $P(x)$ is 0 and the first product is also 0, since $s \neq 0$ has some coordinate equal to 1. This gives $P(s) = 0$, a contradiction, so we must have $m \geq n$. □

Problem 2.6 (IMO 2006)**.** *Let:*

$$S = \{(x, y, z) \in \mathbb{R}^3 \,:\, x, y, z \in \{0, 1, \ldots, n\},\, x + y + z > 0\}$$

be a subset of $\mathbb{R}^3$*. Determine the smallest number of hyperplanes such that their union covers all elements of* S*, but* $(0, 0, 0)$ *is not covered by any hyperplane.*

Proof. It's easy to find a set of $3n$ such hyperplanes - take $\{z = 1\}, \ldots, \{z = n\}, \{x + y = 1\}, \ldots, \{x + y = 2n\}$. We now show that this is the smallest possible number.

The proof is analogous to the proof from the previous problem. Suppose that we can find a set of $m < 3n$ hyperplanes with the desired properties. Let the i-th hyperplane be defined by the equation:

$$a_i x + b_i y + c_i z + d_i = 0$$

where $(x, y, z) \in \mathbb{R}^3$. Consider the polynomial:

$$P(x, y, z) = \prod_{i=1}^{m}(a_i x + b_i y + c_i z + d_i) - \delta \left(\prod_{j=1}^{n}(x - j)\right)\left(\prod_{k=1}^{n}(y - k)\right)\left(\prod_{l=1}^{n}(z - l)\right)$$

where δ is such that $P(0, 0, 0) = 0$. We have $\delta \neq 0$, so the coefficient of $x^n y^n z^n$ is nonzero (note that the first product in $P(x, y, z)$ has degree $m < 3n$, so it doesn't contribute to this term). By Combinatorial Nullstellensatz applied to $S_1 = S_2 = S_3 = \{0, 1, \ldots, n\}$, $|S_i| > n$, we have that there exists some (x', y', z') such that $x', y', z' \in \{0, 1, \ldots, n\}$ and $P(x', y', z') \neq 0$. This implies that $(x', y', z') \neq (0, 0, 0)$, so it must be covered by some hyperplane H_i. But this implies $a_i x' + b_i y' + c_i z' + d_i = 0$, so the first product in the definition of P is 0. The second one is also 0, since at least one of x', y', z' is nonzero. This contradicts $P(x', y', z') \neq 0$, so we must have $m \geq 3n$. □

As remarked before, over a finite field the same function can be represented by different polynomials. This motivates the following definition - we will say that a polynomial over $\mathbb{Z}_p$ is *reduced* if its degree in every variable x_i is at most $p-1$. For any polynomial $P(x_1, \ldots, x_n)$ denote by $\tilde{P}(x_1, \ldots, x_n)$ the polynomial obtained from P by successively replacing every occurence of x_i^p by x_i until we get a reduced polynomial. Note that P and $\tilde{P}$ represent the same function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$,as $s_i^p = s_i$ for any value $s_i \in \mathbb{Z}_p$.

Problem 2.7. *Let $P(x_1, \ldots, x_n)$, $Q(x_1, \ldots, x_n)$ be two reduced polynomials representing the same function $f : \mathbb{Z}_p^n \to \mathbb{Z}_p$. Show that $P = Q$ as polynomials in $x_1, \ldots, x_n$.*

Proof. The polynomial $R(x_1, \ldots, x_n) = P(x_1, \ldots, x_n) - Q(x_1, \ldots, x_n)$ represents the constant 0 function. On the other hand if $P \neq Q$ as polynomials, then there exists some monomial $x_1^{a_1} \ldots x_n^{a_n}$, $a_i \leq p-1$, which has nonzero coefficient in R. By Combinatorial Nullstellensatz applied to $S_i = \mathbb{Z}_p$ we have that there exists $(s_1, \ldots, s_n)$ such that $R(s_1, \ldots, s_n) \neq 0$, a contradiction since R represents the constant 0 function. Hence $P = Q$ as polynomials. □

Problem 2.8. *Let $P(x_1, \ldots, x_n)$ be a polynomial in n variables over arbitrary field $\mathbb{F}$. Suppose that P has degree d and denote the coefficient of $x_1^{d_1} \ldots x_n^{d_n}$, with $d_1 + \ldots + d_n = d$, by $c_{d_1,\ldots,d_n}(P)$. Let $S_1, \ldots, S_n \subseteq \mathbb{F}$ be such that $|S_i| > d_i$ and let:*

$$f_i(x) = \prod_{s_i \in S_i} (x - s_i)$$

Prove that:

$$c_{d_1,\ldots,d_n}(P) = \sum_s \frac{P(s_1, \ldots, s_n)}{f_1'(s_1) \ldots f_n'(s_n)} \tag{1}$$

where the sum is over all $s = (s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ and:

$$f_i'(s_i) = \prod_{\substack{t \in S_i \\ t \neq s_i}} (s_i - t)$$

Note that the formula 1 gives another proof of Combinatorial Nullstellensatz - if $c_{d_1,\ldots,d_n}(P) \neq 0$, then in particular at least one term in the sum must be nonzero, so there exists some $(s_1, \ldots, s_n)$, $s_i \in S_i$, such that $P(s_1, \ldots, s_n) \neq 0$.

Proof. First note that it is sufficient to prove the formula for monomials with coefficient 1, since the formula is linear - for any polynomials P and Q we have:

$$c_{d_1,\ldots,d_n}(P + Q) = c_{d_1,\ldots,d_n}(P) + c_{d_1,\ldots,d_n}(Q)$$

and:

$$\sum_s \frac{(P+Q)(s_1, \ldots, s_n)}{f_1'(s_1) \ldots f_n'(s_n)} = \sum_s \frac{P(s_1, \ldots, s_n)}{f_1'(s_1) \ldots f_n'(s_n)} + \sum_s \frac{Q(s_1, \ldots, s_n)}{f_1'(s_1) \ldots f_n'(s_n)}$$

The case of $n = 1$ is simply the interpolation formula:

$$P(x) = \sum_{s_1 \in S_1} P(s_1) \frac{f_1(x)}{f_1'(s_1)(x - s_1)}$$

Now if $P(x_1, \ldots, x_n) = x_1^{c_1} \ldots x_n^{c_n}$ is a monomial, then:

$$\sum_s \frac{P(s_1, \ldots, s_n)}{f_1'(s_1) \ldots f_n'(s_n)} = \sum_s \frac{s_1^{c_1} \ldots s_n^{c_n}}{f_1'(s_1) \ldots f_n'(s_n)} = \sum_{s_1, \ldots, s_n} \frac{s_1^{c_1}}{f_1'(s_1)} \cdot \frac{s_1^{c_2}}{f_2'(s_2)} \cdot \ldots \cdot \frac{s_n^{c_n}}{f_n'(s_n)} =$$
$$= \left(\sum_{s_1} \frac{s_1^{c_1}}{f_1'(s_1)} \right) \left(\sum_{s_2} \frac{s_2^{c_2}}{f_2'(s_2)} \right) \ldots \left(\sum_{s_n} \frac{s_n^{c_n}}{f_n'(s_n)} \right) = c_{d_1}(x_1^{c_1}) c_{d_2}(x_2^{c_2}) \ldots c_{d_n}(x_n^{c_n})$$

by the 1-dimensional case and:

$$c_{d_1}(x_1^{c_1}) c_{d_2}(x_2^{c_2}) \ldots c_{d_n}(x_n^{c_n}) = c_{d_1, \ldots, d_n}(x_1^{c_1} x_2^{c_2} \ldots x_n^{c_n}) = c_{d_l, \ldots, d_n}(P)$$

which finishes the proof. □

Problem 2.9 (Dyson's conjecture)**.** *Let $a_1, \ldots, a_n$ be natural numbers and let:*

$$P(x_1, \ldots, x_n) = \prod_{i \neq j} \left(1 - \frac{x_i}{x_j}\right)^{a_i}$$

Show that the constant term in $P(x_1, \ldots, x_n)$ is equal to:

$$\frac{(a_1 + \ldots + a_n)!}{a_1! \ldots a_n!}$$

Hint: for $a = a_1 + \ldots + a_n$ the constant term of P is equal to the coefficient of $x_1^{a - a_1} \ldots x_n^{a - a_n}$ in :

$$Q(x_1, \ldots, x_n) = \prod_{i<j} (-1)^{a_j} (x_j - x_i)^{a_i + a_j}$$

Proof. Denote the coefficient we want to compute by D. We would like to use the formula 1 for $Q(x_1, \ldots, x_n)$ and suitably chosen S_i. Because we are interested only in the highest term of Q, we are free to add lower order terms to Q so that the calculation for the modified polynomial $\overline{Q}$ will be simpler. We would like to define $\overline{Q}$ so that it assumes only one nonzero value on $S_1 \times \ldots \times S_n$, so by 1 this will give us the desired coefficient.

We will replace each term $(x_j - x_i)^{a_i + a_j}$ by another polynomial which will give the same highest order term, but in such a way that only one $(s_1, \ldots, s_n)$ will give nonzero value of the whole product. For any $0 \leq s_i \leq a - a_i$ consider the interval $\Delta_i(s_i)$ of length a_i starting at s_i:

$$\Delta_i(s_i) = \{s_i, s_i + 1, \ldots, s_i + a_i - 1\}$$

For $s_1 = 0, s_2 = a_1, s_3 = a_1 + a_2, \ldots, s_n = a_1 + \ldots + a_{n-1}$ we have that $\Delta_i(s_i) \subseteq \{0, \ldots, a\}$ and intervals $\Delta_i(s_i)$ are pairwise disjoint. These are the only possible value of s_i which have this property and it can be encoded by a polynomial:

$$D_{ij}(x_1, \ldots, x_n) = \prod_{k=-a_i+1}^{a_j} (x_j - x_i + k)$$

We have $D_{ij}(s_1, \ldots, s_n)$ if and only if $\Delta_i(s_i)$ and $\Delta_j(s_j)$ are disjoint. Note also that $D_{ij}(x_1, \ldots, x_n)$ contributes the same highest order term as $(x_j - x_i)^{a_i+a_j}$. Therefore if we replace each term $(x_j - x_i)^{a_i+a_j}$ in Q by D_{ij} we will obtain:

$$\overline{Q} = \prod_{i<j} (-1)^{a_j} D_{ij}(x_1, \ldots, x_n)$$

and the whole product is nonzero only for one tuple $(s_1, \ldots, s_n)$. When we apply 1 to $\overline{Q}$ the only surviving term will be the one containing s_i as above, which gives:

$$D = \frac{\prod_{i<j} (-1)^{a_j} D_{ij}(s_1, \ldots, s_n)}{f_1'(s_1) \ldots f_n'(s_n)}$$

where f_i is the characteristic function of S_i.

We calculate easily that:

$$f_i'(s_i) = (-1)^{a_{i+1}+\ldots+a_n}(a_1 + \ldots + a_{i-1})!(a_{i+1} + \ldots + a_n)!$$

and:

$$D_{ij}(s_1, \ldots, s_n) = \frac{(a_i + \ldots a_j)!}{a_{i+1} + \ldots a_{j-1}}$$

After inserting this into the formula for C and cancelling all the necessary factorials we get the desired result. □

Problem 2.10. *Let $A = \{a_1, \ldots, a_n\}, B = \{b_1, \ldots, b_n\}$ be two nonempty subsets of $\mathbb{Z}_p$ ($p > 2$) such that $|A| = |B| = n$. Prove that there exists a permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that the sums $a_1 + b_{\sigma(1)}, a_2 + b_{\sigma(2)}, \ldots, a_n + b_{\sigma(n)}$ are all distinct.*

Proof. We can assume that $n < p$ and $A \neq B$, since the other case is trivial. Define a polynomial:

$$P(x_1, \ldots, x_n) = \prod_{i<j} (x_j - x_i)(x_j - x_i + a_j - a_i)$$

We have $\deg(P) = n(n-1)$ and the coefficient of $x_1^{n-1} \ldots x_n^{n-1}$ is, up to a sign, $n!$ (by applying Problem 2.9), which is nonzero in $\mathbb{Z}_p$. By Combinatorial Nullstellensatz applied to $S_i = B$ there exists some $b_1', \ldots, b_n' \in B$ such that $P(b_1', \ldots, b_n') \neq 0$. This means that $b_i' \neq b_j'$ for $i \neq j$ and $a_i + b_i' \neq a_j + b_j'$. By defining σ so that $b_{\sigma(i)} = b_i'$ we get the desired permutation. □

Problem 2.11 (Chevalley-Warning theorem)**.** *Let $P_i(x_1, \ldots, x_n)$, $i = 1, \ldots, k$, be polynomials over $\mathbb{Z}_p$ such that P_i has degree d_i. Prove that if $d_1 + \cdots + d_k < n$, then the set of common zeros of all P_i's has size divisible by p.*

Proof. Let $Z = \{(x_1, \ldots, x_n) : P_1(x_1, \ldots, x_n) = \ldots = P_k(x_1, \ldots, x_n) = 0\}$ be the set of common zeroes of P_i's. We want to show that $|Z| = 0 \mod p$. Consider the polynomial $P(x_1, \ldots, x_n)$ representing the characteristic function of Z:

$$P(x_1, \ldots, x_n) = \prod_{i=1}^{k} (1 - P_i(x_1, \ldots, x_n)^{p-1})$$

that is, $P(x_1, \ldots, x_n) = 1$ if and only if $(x_1, \ldots, x_n)$ is a common zero of all P_i's. P has total degree $(p-1)(d_1 + \ldots + d_n) < (p-1)n$, so the reduced polynomial $\tilde{P}$ has also degree $< (p-1)n$.

On the other hand the characteristic function of Z can also be written as:

$$Q(x_1, \ldots, x_n) = \sum_{c \in Z} \prod_{i=1}^{k} (1 - (x_i - c_i)^{p-1})$$

where the sum is over all $c = (c_1, \ldots, c_n) \in Z$. If $|Z| \neq 0 \mod p$, then the coefficient of $x_1^{p-1} \ldots x_n^{p-1}$ in Q is equal to $(-1)^n |Z| \neq 0 \mod p$. Thus Q has degree $(p-1)n$ and is clearly a reduced polynomial. But then we have $\deg(\tilde{P}) < \deg(Q)$ and $\tilde{P}$, Q are reduced polynomials representing the same function, which is impossible. Hence we must have $|Z| = 0 \mod p$. □

Problem 2.12 (Erdős-Ginzburg-Ziv theorem)**.** *Let $a_1, \ldots, a_{2p-1}$ be elements of $\mathbb{Z}_p$. Prove that there exist a set of indices $I \subseteq \{1, \ldots, 2p-1\}$ of size p such that:*

$$\sum_{i \in I} a_i = 0 \mod p$$

Proof. Consider polynomials:

$$P(x_1, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i^{p-1}$$

$$Q(x_1, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} x_i^{p-1}$$

Since $P(0, \ldots, 0) = Q(0, \ldots, 0) = 0$ and $\deg(P) + \deg(Q) \leq 2p - 2 < 2p - 1$, by Chevalley-Warning theorem there exists $(c_1, \ldots, c_{2p-1}) \neq (0, \ldots, 0)$ such that:

$$P(c_1, \ldots, c_{2p-1}) = Q(c_1, \ldots, c_{2p-1}) = 0$$

so:

$$\sum_{i=1}^{2p-1} a_i c_i^{p-1} = 0$$
$$\sum_{i=1}^{2p-1} c_i^{p-1} = 0$$

Let I be the set of those indices i for which $c_i \neq 0$. Since c_i^{p-1} is equal to 1 if $c_i \neq 0$ and 0 otherwise, we have:

$$\sum_{i \in I} a_i = 0$$
$$\sum_{i \in I} 1 = 0$$

The second equation implies $|I| = 0 \bmod p$, but $|I| \leq 2p-1$, so $|I| = p$, which finishes the proof. □

Problem 2.13. *Let $v_1 = (a_1, b_1), \ldots, v_{2p-1} = (a_{2p-1}, b_{2p-1})$ be elements of $\mathbb{Z}_p \times \mathbb{Z}_p$. Prove that there exist a set of indices $I \subseteq \{1, \ldots, 2p-1\}$ such that:*

$$\sum_{i \in I} v_i = 0 \quad \text{in } \mathbb{Z}_p \times \mathbb{Z}_p$$

Proof. Consider polynomials:

$$P(x_1, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i$$
$$Q(x_1, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} b_i x_i$$

and

$$R(x_1, \ldots, x_{2p-1}) = \left(1 - P(x_1, \ldots, x_{2p-1})^{p-1}\right)\left(1 - Q(x_1, \ldots, x_{2p-1})^{p-1}\right) - \prod_{i=1}^{2p-1}(1 - x_i)$$

R has total degree $2p-1$ and the coefficient of $x_1 \ldots x_{2p-1}$ is 1. By Combinatorial Nullstellensatz applied to $S_i = \{0, 1\}$ there exists $(c_1, \ldots, c_{2p-1}) \in \{0,1\}^{2p-1}$ such that $R(c_1, \ldots, c_{2p-1}) \neq 0$. Now take I to be the set of indices i such that $c_i = 1$. By the same argument as in the previous problem we see that $\sum_{i \in I} v_i = 0$. □

Problem 2.14. *Let p be a prime number and let $G = (V, E)$ be a graph with average degree bigger than $2p-2$ and maximum degree at most $2p-1$. Prove that G contains a p-regular subgraph.*

Proof. Associate a variable x_e to each edge e and consider the polynomial:

$$F = \prod_{v \in V} \left(1 - \left(\sum_{v \in e} x_e\right)^{p-1}\right) - \prod_{e \in E}(1 - x_e)$$

F has degree $|E|$, since the degree of the first product is at most $(p-1)|V| < |E|$ by the assumption on the average degree. The coefficient of $\prod_{e \in E} x_e$ is nonzero, so by applying Combinatorial Nullstellensatz to $S_e = \{0, 1\}$ we deduce that there are values $x_e \in \{0, 1\}$ such that $F \neq 0$. Moreover not all values of x_e are 0, since F vanishes for the zero vector. It follows that for every v we must have;

$$1 - \left(\sum_{e \ni v} x_e\right)^{p-1} \neq 0 \mod p$$

which is possible only $\sum_{e \ni v} x_e$ is 0 mod p. This means that if we take edges e such that $x_e = 1$, then each vertex in the corresponding subgraph will have degree divisible by p. By the assumption that the maximal degree is at most $2p - 1$ we have that every degree is exactly p, which gives us the desired p-regular subgraph. □

Problem 2.15. *A king invites n couples to sit around a round table with $2n + 1$ seats. For each couple, the king decides a prescribed distance $d_i \in \{1, \ldots, n\}$ so that the spouses in the i-th couple are separated by exactly $d_i - 1$ chairs. Prove that if $2n + 1$ is a prime number, then it is always possible to seat the couples so that these constraints are satsfied. Provide a counterexample showing that this is not always possible in the case where $2n+1$ is composite.*

Proof. Let $p = 2n + 1$ be a prime number. The solution to the seating problem consists of a tuple $(x_1, \ldots, x_n)$, $x_i \in \mathbb{Z}_p$ such that the $2n$ numbers $x_1, \ldots, x_n, x_1 + d_1, \ldots, x_n + d_n$ are pairwise distinct mod p. Consider a polynomial:

$$P(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)(x_i + d_i - x_j)(x_i - x_j - d_j)(x_i + d_i - x_j - d_j)$$

We have $P(c_1, \ldots, c_n) \neq 0$ if and only if $(c_1, \ldots, c_n)$ is a solution to the seating problem, so we want to show tht P is not 0 everywhere. We have $\deg(P) = n(2n-2)$ and $x_1^{2n-2} \ldots x_n^{2n-2}$ is a monomial of degree $\deg(P)$. To find its coefficient in P note that we only need to consider the highest order terms, which are equal to a polynomial:

$$\prod_{i<j}(x_i - x_j)^4 = x_1^{2n-2} \ldots x_n^{2n-2} \prod_{i \neq j}\left(1 - \frac{x_i}{x_j}\right)^2$$

So we only need to show that the constant term of

$$\prod_{i \neq j}\left(1 - \frac{x_i}{x_j}\right)^2$$

is nonzero. But by Problem 2.9 the constant term equals $\frac{(2n)!}{2^n} \neq 0 \bmod p$ (as $(2n)! = (p-1)!$).

Therefore by applying Combinatorial Nullstellensatz to $S_i = \mathbb{Z}_p$ we get that there exists a solution to the seating problem.

In the case of $2n+1$ being a composite number, let k be a nontrivial divisor of $2n+1$ and take $d_i = k$ for all i. For any j let $C_j = \{j, j+k, j+3k, \ldots\}$. Then each couple must belong to the same set C_j, but each C_j has an odd number of elements, so at least one set in each C_j must be empty. But there are at least two disjoint sets C_j, $C_{j'}$ in $\mathbb{Z}_p$, since $k > 1$ divides $2n+1$ and on the other hand there can be at most one empty seat, so we have a contradiction. □

Problem 2.16. *Let $M_3(n)$ denote the smallest number of queens that can be placed on an $n \times n$ chessboard so that no three queens are in the same line (where line is a column, a row or a diagonal), but it is impossible to put any additional queens on the board without violating this condition. Show that $M_3(n) \geq n$.*

Proof. We cover only the case of $n = 4k+1$ for some integer k (the other three cases can be handled along the same lines). We will treat the $n \times n$ board as a subset of the plane, where the square in the i-th row and j-th column corresponds to the point $(i, j) \in \mathbb{R}^2$.

Suppose it is possible to place $q \leq n-1 = 4k$ queens so that this configuration is maximal (i.e. there are no three queens in the same line and it is impossible to add any queensso that this condition is still satisfied). We will construct a polynomial $P(x, y)$ of two variables of degree $8k$ which vanishes on every point of the board and reach contradiction by Combinatorial Nullstellensatz.

If two queens lie in the same line, we can treat this line L_i as a subset of $\mathbb{R}^2$ described by one of the equations (depending on whether the line is vertical, horizontal or diagonal):

$$\begin{aligned} x - a_i &= 0 \\ y - b_i &= 0 \\ x - y - c_i &= 0 \\ x + y - d_i &= 0 \end{aligned}$$

for some constants a_i, b_i, c_i, d_i.

By the assumption of maximality each unoccupied square of the board lies in at least one line L_i (otherwise we could put a queen on that square without creating three in a line).

Some of the queens may not be colinear to any other queen. Suppose there are q' such queens and for each of them define K_i to be a line passing through the square occupied by the queen, having arbitrary of the above four types. For the sake of simplicity it is convenient to choose the types as evenly as possible, so that there are at most $\lceil \frac{q'}{4} \rceil$ lines K_i of given type.

For any given type of a line there are at most $\lceil \frac{4k-q'}{2} \rceil$ lines L_i of that type and at most $\lceil \frac{q'}{4} \rceil$ lines K_i of that type, so the total number is at most $2k$. If it is strictly less than $2k$, we add some "fake" lines of that type so that the total number is $2k$ (their form is unimportant). Thus the total number of lines is $8k$.

If $P_i(x, y)$ is the polynomial defining the i-th line, then let:

$$P(x, y) = \prod_{i=1}^{8k} P_i(x, y)$$

By the assumption that there are exactly $2k$ lines of each type we get:

$$P(x, y) = \prod_{i=1}^{2k} (x - a_i)(y - b_i)(x - y - c_i)(x + y - d_i)$$

for some constants a_i, b_i, c_i, d_i. By definition if (x, y) is contained in one of the $8k$ lines, then $P(x, y) = 0$.

The polynomial has degree $8k$ and the coefficient of $x^{4k}y^{4k}$ is $\pm\binom{2k}{k} \neq 0$. By Combinatorial Nullstellensatz applied to $S_1 = S_2 = \{1, \ldots, 4k + 1\}$ there exists a point (x_0, y_0) such that $P(x_0, y_0) \neq 0$. But then (x_0, y_0) does not lie in any line, so it is an unoccupied square with no other queen in the same row, column or diagonal and we can put a new queen on (x_0, y_0), violating the maximality assumption. Thus $M_3(n) \geq n$. □

3 Finite field Kakeya conjecture

One of the outstanding open problems, with connections to harmonic analysis and partial differential equations, is the Euclidean **Kakeya conjecture**, concerning the dimension (more precisely, Minkowski or Hausdorff dimension) of Kakeya sets in $\mathbb{R}^n$. A **Kakeya set** $S \subseteq \mathbb{R}^n$ is a set that contains a unit interval in every direction. A good introduction to the Kakeya problem can be found here: `http://en.wikipedia.org/wiki/Kakeya_set`. The conjecture, which states that Kakeya sets always have Hausdorff dimension n, has only been solved for $n = 2$ and is open for $n \geq 3$.

As an attempt to attack the conjecture, a variant has been proposed where the Euclidean space $\mathbb{R}^n$ is replaced by a vector space over a finite field $\mathbb{F}_q^n$, where $|\mathbb{F}_q| = q$. This leads to a simplified problem, since finite fields are more amenable to combinatorial or algebraic techniques than the Euclidean space. An analogue of a set containing a unit interval in every direction is defined in a natural way:

Definition 3.1. A set $K \subseteq \mathbb{F}_q^n$ is a **Kakeya set** if it contains a line in every direction, i.e. for every $x \in \mathbb{F}_q^n$ there exists $y \in \mathbb{F}_q^n$ such that for all $t \in \mathbb{F}_q$ $y + tx \in K$.

What is the right analogue of dimension? Recall that the notion of dimension is closely connected to scaling - intuitively, a set S has dimension d if scaling the set by a factor of c changes its volume by a factor c^d. In a finite field setting there is no concept of scaling, but we can change the size of the base field $\mathbb{F}_q$ instead. This leads to the following conjecture, which states that Kakeya sets over finitie fields have "dimension" n:

Theorem 3.2 (Finite field Kakeya conjecture)**.** *For every $n \geq 1$ there exists a constant c_n such that for any Kakeya set $K \subseteq \mathbb{F}_q^n$ we have:*

$$|K| \geq c_n \cdot q^n$$

The conjecture has attracted the attention of many brilliant mathematicians, including Fields medalists - however, up till 2008 the best bound on the exponent was only $\frac{4}{7}n$. In 2008, Zeev Dvir ([Dvi09b]) provided a "proof from the Book" for the conjecture, which essentially fits in one paragraph. We present that proof below. Before we proceed we need two lemmas concerning finite field polynomials in several variables.

Lemma 3.3 (Schwartz-Zippel lemma, simple version)**.** *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a nonzero polynomial of degree d. Then:*

$$\text{zero}(f) = |\{x \in \mathbb{F}_q^n | f(x) = 0\}| \leq d \cdot q^{n-1}$$

Proof. Proof is by induction on n. For $n = 1$ this is simply the fact that a nonzero polynomial of degree d can have at most d zeroes. For any $a_1, \ldots, a_{n-1} \in \mathbb{F}_q$ let $f_{a_1,\ldots,a_{n-1}} \in \mathbb{F}_q[t]$ be defined as:

$$f_{a_1,\ldots,a_{n-1}}(t) = f(a_1, \ldots, a_{n-1}, t)$$

Notice that:

$$|\text{zero}(f)| \leq \sum_{a_1,\ldots,a_{n-1} \in \mathbb{F}_q} |\text{zero}(f_{a_1,\ldots,a_{n-1}})|$$

since if $(x_1, \ldots, x_{n-1}, x_n) \in \text{zero}(f)$, then $x_n \in \text{zero}(f_{x_1,\ldots,x_{n-1}})$. From this it follows that:

$$|\text{zero}(f)| \leq q^{n-1} \cdot \max_{a_1,\ldots,a_{n-1} \in \mathbb{F}_q} |\text{zero}(f_{a_1,\ldots,a_{n-1}})| \leq d \cdot q^{n-1}$$

□

Problem 3.1. *Let $S(d, n) \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ be the subspace spanned by all monomials of degree $\leq d$. What is the dimension of $S(d, n)$?*

Proof. Counting monomials of degree $\leq d$ is equivalent to counting ways of putting d indistinguishable balls into $n + 1$ distinguishable boxes - we first put $k \leq d$ balls into first n boxes, corresponding to variables $x_1, \ldots, x_n$, and discard the remaining $d - k$ balls into the last box. Elementary combinatorics shows that this can be achieved in $\binom{n+d}{n}$ ways. □

Proof of finite field Kakeya conjecture. Let K be a Kakeya set. Suppose that $|K| < \binom{q+n-1}{n}$ (note that essentially $\binom{q+n-1}{n} \approx c_n \cdot q^n$ for some $c_n \approx \frac{1}{n!}$). Since $\binom{q+n-1}{n}$ is the dimension of $S(q-1, n)$, the space of polynomials of degree $\leq q - 1$, there exists a nonzero polynomial $p \in S(q-1, n)$ such that $p(x) = 0$ for all $x \in K$.

Now, for any $x \in \mathbb{F}_q^n$ consider h_x, the polynomial of one variable defined as restriction of p to a line in direction x lying in K - $h_x(t) = p(y + tx)$. The degree of h_x is at most $q - 1$ and h_x vanishes for all t, so it must be identically zero.

Let $s = \deg(p)$ and:

$$p = \sum_{i=0}^{s} p_i$$

where p_i is homogenous of degree i. Notice that:

$$h_x(t) = p(y + tx) = t^s p_s(x) + \sum_{i=0}^{s-1} t^i p'_i(x)$$

where $p'_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a polynomial of degree i (note that for $i < s$ we may have $p_i \neq p'_i$ - however, these polynomials agree for the leading term of degree s). Since $h_x \equiv 0$, in particular $p_s(x) = 0$ for all x. However, by definition $\deg p_s = s \leq q-1$, so, unless $p_s \equiv 0$, from Schwartz-Zippel lemma p_s can have at most $q^{n-1}(q-1) < q^n$ zeroes - a contradiction. If $p_s \equiv 0$, we apply the same reasoning to all p_i and conclude that $p_i \equiv 0$ for all i, which contradicts the fact that p is not identically zero. □

We have obtained a bound with the constant $c_n \approx \frac{1}{n!}$. On the other hand, there exist Kakeya sets with size $|K| \approx \frac{1}{2^{n-1}} q^n$, which we construct below for odd q (the case of even q can be handled in a similar fashion). The constant in Kakeya conjecture can be improved to almost optimal using an extension of the polynomial method called "the method of multiplicities" (see [DKSS09]).

Problem 3.2. *For q odd, prove that there exists a Kakeya set K of size:*

$$|K| \leq \frac{q^n}{2^{n-1}} + O(q^{n-1})$$

Proof. We will construct a set K which contains lines in all direction of the form $b = (b_1, \ldots, b_{n-1}, 1)$ - directions with $b_n = 0$ can be added "by hand" into the $O(q^{n-1})$ remainder term. Consider the following set:

$$K = \left\{ \left(\frac{v_1^2}{4} + v_1 t, \ldots, \frac{v_{n-1}^2}{4} + v_{n-1} t, t \right) | v_1, \ldots, v_{n-1}, t \in \mathbb{F} \right\}$$

K contains lines in all required directions - a line in direction $b = (b_1, \ldots, b_{n-1}, 1)$ passes through $(\frac{1}{4}b_1^2, \ldots, \frac{1}{4}b_{n-1}^2, 0) \in K$. It remains to count how many distinct points there are in K.

Let $x = (\frac{x_1^2}{4} + x_1 t, \ldots, \frac{x_{n-1}^2}{4} + x_{n-1} t, t)$, $y = (\frac{y_1^2}{4} + y_1 t', \ldots, \frac{y_{n-1}^2}{4} + y_{n-1} t', t')$ and suppose that $x = y$. This implies $t = t'$ and, for $i = 1, \ldots, n-1$:

$$\frac{x_y^2}{4} + x_i t = \frac{y_i^2}{4} + y_i t$$

which gives:

$$(x_i - y_i)(x_i + y_i + 4t) = 0$$

For each fixed x_i, this gives 2 choices for y_i unless $x_i = -2t$. Therefore, for each fixed t the number of distinct points equals:

$$\sum_{k=0}^{n-1} \binom{n-1}{k} \left(\frac{q-1}{2} \right)^{n-1-k} = \left(\frac{q+1}{2} \right)^{n-1} = \frac{q^{n-1}}{2^{n-1}} + O(q^{n-2})$$

which upon multiplying by q possible values of t gives the desired answer. □

4 Lines and joints

Another interesting problem with a geometric flavor where the polynomial method yields a simple and elegant solution is the *lines and joints problem*. Consider a set of lines in $\mathbb{R}^k$. A *joint* is a point such that the lines intersecting at it do not all lie in a $(k-1)$-dimensional hyperplane. In other words, direction vectors of lines intersecting at a joint span all $\mathbb{R}^k$. What is the largest number of joints that can be created using n lines in $\mathbb{R}^k$?

Throughout this section the set of lines will be denoted by L and the set of their joints by J. We take $n = |L|$ and $m = |J|$. Let $f_k(n)$ denote the maximal m as a function of n. It is easy to give a lower bound on $f_k(n)$ - consider a k-dimensional cube $\{1, \ldots, a\}^k$ and take L to be the set of all lines parallel to the axes in $\mathbb{R}^k$ and intersecting the cube. It is easy to prove by induction that there are $n = ka^{k-1}$ such lines and their intersection points are vertices of the cube. Each such intersection point is a joint, so we have $m = a^k$. This gives us:

$$m = \left(\frac{n}{k}\right)^{\frac{k}{k-1}}$$

so:

$$f_k(n) \geq c_k n^{\frac{k}{k-1}}$$

where $c_k = (1/k)^{\frac{k}{k-1}}$ is a constant depending only on k. It turns out that this simple construction is optimal up to a constant - there exists $C_k > 0$ such that:

$$f_k(n) \leq C_k n^{\frac{k}{k-1}}$$

This bound is proved using the polynomial method (which also gives the value of C_k).

The first step of the proof is a direct application of Problem 3.1.

Lemma 4.1. *For any set of m points in $\mathbb{R}^k$ there exists a nonzero polynomial $P(x_1, \ldots, x_k)$ such that P vanishes on this set and its degree is at most $d_k m^{1/k}$ for some constant $d_k > 0$.*

The next step will be proving that no nontrivial polynomial of low degree can vanish on the set of joints for a given set of lines.

Lemma 4.2. *If $P(x_1, \ldots, x_k)$ is a polynomial of degree at most $m/2n$ vanishing on the set J of m joints, then P must be identically zero.*

By combining Lemma 4.1 and 4.2 we get that:

$$m/2n \leq d_k m^{1/k}$$

which after rearranging gives us:

$$m \leq (2d_k n)^{\frac{k}{k-1}}$$

and finishes the proof of our bound.

Proof of Lemma 4.2. The first step is to restrict our attention to lines which intersect many joints - given L and J we construct sets $L' \subseteq L$ and $J' \subseteq G$ such that:

- each line L' contains more than $m/2n$ points of J'
- every point of J' is a joint of L'

This is done by a simple iterative procedure. Start with $L_0 = L$ and $J_0 = J$. At the i-th step remove all the lines from L_i which intersect at most $m/2n$ points from J_i and then remove the points from J_i which lay on those lines. Take L_{i+1} to be the set of remaining lines and J_{i+1} to be the set of remaining points. Since at each step we are removing at most $m/2n$ points and we started with n lines and m points, this procedure will eventually halt with at least $m/2$ points left. In particular, the set of lines will be nonempty, so we obtain L' and J' satisfying the above two properties.

Now let P be a polynomial of degree at most $m/2n$ vanishing on J'. We will show that P is identically zero. First we claim that P vanishes on each line from L'. To see this, let l' be a line from L' and parametrize it by;

$$l' = \{a + tv \,:\, t \in \mathbb{R}\}$$

where $v = (v_1, \ldots, v_k) \in \mathbb{R}^k$ is the direction vector of l' and $a = (a_1, \ldots, a_k) \in \mathbb{R}^k$ is any point on l'. Since l' intersects more than $m/2n$ points from J', the polynomial:

$$Q(t) = P(a_1 + tv_1, \ldots, a_k + tv_k)$$

has more than $m/2n$ roots. However, its degree can be at most $m/2n$, since P had total degree at most $m/2n$, so Q must be identically zero. Therefore P vanishes on each point of l'.

To show that P is identically zero we will show that all its partial derivatives vanish. Take any $a \in J'$ and let $l'_1, \ldots, l'_k$ be a set of k lines passing through a and not lying in a $(k-1)$-dimensional hyperplane (note that a is a joint, so we can always find such lines). Take one of these lines, say l'_1, and parametrize it as before:

$$l'_1 = \{a + tv_1 \,:\, t \in \mathbb{R}\}$$

where $v_1 \in \mathbb{R}^k$.

We will need to do some differentiation here. Recall that for a differentiable function $f : \mathbb{R} \to \mathbb{R}$ of one variable we have for any $x \in \mathbb{R}$:

$$f(x + t) = f(x) + tf'(x) + O(t^2)$$

where f' is the derivative of f and $O(t^2)$ denotes the terms that go to 0 as $t \to 0$ faster than linearly. An analogous formula holds for functions of many variables - for any sufficiently nice function $f : \mathbb{R}^k \to \mathbb{R}$ (for example a polynomial) and any $a \in \mathbb{R}^k$, $v \in \mathbb{R}^{\urcorner}$, we have:

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

where $\nabla f = \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_k}\right)$ is the vector of partial derivatives of f and $\langle \cdot, \cdot \rangle$ denotes the inner product in $\mathbb{R}^k$.

Now let us apply this formula to P. We have:

$$P(a + tv_1) = P(a) + t \langle (\nabla P)(a), v_1 \rangle + O(t^2)$$

Since P vanishes on each line from L', we have $P(a + tv) = P(a) = 0$, so;

$$t \langle (\nabla P)(a), v_1 \rangle = O(t^2)$$

which, by taking t small enough, implies that $\langle (\nabla P)(a), v_1 \rangle = 0$. This means that $(\nabla P)(a)$ is orthogonal to v_1. But we can repeat the same argument for any l'_i instead of l'_1 and we will get that $(\nabla P)(a)$ is orthogonal to all direction vectors of $l'_1, \ldots, l'_k$. Since a is a joint, the direction vectors span all $\mathbb{R}^k$, so each coordinate of $(\nabla P)(a)$ must be 0.

Therefore we have obtained that each partial derivative $\frac{\partial P}{\partial x_i}$ vanishes on points from J'. Since this derivative still has degree at most $m/2n$, we can apply to it the same argument as to P to show that it vanishes on each line from L' and prove that second partial derivatives of P vanish on points from J'. By continuing this argument we get that all derivatives of P vanish on all lines from L', but this is possible only if P is identically zero, which finishes the proof. □

5 Further reading

We have presented here only a few applications of the polynomial method and there are many topics that we haven't touched upon at all. Below are some references to papers dealing with the material in more depth.

The paper which first proved Combinatorial Nullstellensatz and where many more applications can be found is [Alo99]. Another paper featuring applications of Combinatorial Nullstellensatz to restricted sumset problems is [ANR96]. A good source on additive combinatorics (a rich subfield of mathematics to which sumset problems belong) is the book [TV06] (see especially Chapter 9).

More about Kakeya problem, apart from the Wikipedia article, can be found in Terence Tao's survey [Tao00] and Zeev Dvir's survey [Dvi09a]. Finite field Kakeya conjecture was proved in [Dvi09b] (the paper is only 5 pages long!). Improvements using "the method of multiplicities" come from [DKSS09]. Other applications, including randomness extractors (an interesting topic in theoretical computer science we haven't mentioned at all), are discussed in [DKSS09] and [DW11].

Problems for Combinatorial Nullstellensatz section were taken from various sources, mostly research papers, including [Alo99], [ANR96], [TV06], [KP12], [CPSW12].

The application of the polynomial method to lines and joints problems comes from [Qui10] and [KSS10].

References

[Alo99] Noga Alon, *Combinatorial nullstellensatz*, Combinatorics, Probability and Computing **8** (1999).

[ANR96] Noga Alon, Melvyn B. Nathanson, and Imre Ruzsa, *The polynomial method and restricted sums of congruence classes*, Journal of Number Theory **56** (1996), no. 2, 404 – 417.

[CPSW12] Alec S. Cooper, Oleg Pikhurko, John R. Schmitt, and Gregory S. Warrington, *Martin gardner's minimum no-3-in-a-line problem*, `http://arxiv.org/abs/1206.5350`, 2012.

[DKSS09] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan, *Extensions to the method of multiplicities, with applications to Kakeya sets and mergers*, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS) (Washington, DC, USA), IEEE Computer Society, 2009, pp. 181–190.

[Dvi09a] Zeev Dvir, *From randomness extraction to rotating needles*, SIGACT News **40** (2009), no. 4, 46–61.

[Dvi09b] Zeev Dvir, *On the size of Kakeya sets in finite fields.*, J. Amer. Math. Soc. **22** (2009), 1093–1097.

[DW11] Zeev Dvir and Avi Wigderson, *Kakeya sets, new mergers, and old extractors*, SIAM J. on Computing **40** (2011), no. 3, 778–792, (Extended abstract appeared in FOCS 2008).

[KP12] R.N. Karasev and F.V. Petrov, *Partitions of nonzero elements of a finite field into pairs*, Israel Journal of Mathematics (2012), 1–14.

[KSS10] Haim Kaplan, Micha Sharir, and Eugenii Shustin, *On lines and joints*, Discrete & Computational Geometry (2010), 838–843.

[Qui10] Rene Quilodrán, *The joints problem in* $\mathbb{R}^n$, SIAM Journal on Discrete Mathematics **23** (2010), no. 4, 2211–2213.

[Tao00] Terence Tao, *From rotating needles to stability of waves: emerging connections between combinatorics, analysis, and PDE*, Notices Amer. Math. Soc **48** (2000), 294–303.

[TV06] Terence Tao and Van Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., vol. 105, Cambridge Univ. Press, Cambridge, 2006.