Counting polynomial configurations in subsets of finite fields

Borys Kuca
University of Manchester

Standard notation

The letter p denotes a (large) prime. $\mathbb{F}_p$ is the finite field with p elements. The function e_p is the usual additive character $e_p(x) = e^{2\pi ix/p}$. The function 1_A is the indicator function of a set A.

Polynomials $P_1, ..., P_m$ are *integral* if they have integer coefficients and satisfy $P_1(0) = ... = P_m(0) = 0$.

We denote $f \ll g$ or $f = O(g)$ if there exists an absolute constant $C > 0$ such that $|f(N)| \leqslant Cg(N)$ for all sufficiently large natural numbers N. We write $f = O_m(g)$ if the absolute constant depends on parameter m. We also write $f = o(g)$ if $f(N)/g(N) \to 0$ as $N \to \infty$.

$\mathbb{E}_{x \in X} = \frac{1}{|X|} \sum_{x \in X}$ is the average over the set X.

Additive combinatorics

Additive combinatorics studies arithmetic structures in subsets of $\mathbb{N}$, $\mathbb{F}_p$, $\mathbb{F}_p[t]$, etc.

Examples of arithmetic structures:

- arithmetic progressions: $x, x+y, ..., x+(m-1)y$
- polynomial progressions: $x, x+P_1(y), ..., x+P_m(y)$
- solutions to linear equations: $a_1x_1 + ... + a_nx_n = b$
- solutions to quadratic equations: $a_1x_1^2 + ... + a_nx_n^2 = b$

Polynomial progressions

A polynomial progression is a configuration of the form

$$x,\ x+P_1(y),\ ...,\ x+P_m(y)$$

for some polynomials $P_1, ..., P_m \in \mathbb{Z}[y]$ satisfying

$$P_1(0) = ... = P_m(0) = 0.$$

Examples:

- $x,\ x+y,\ ...,\ x+(m-1)y$ (arithmetic progressions)
- $x,\ x+y,\ ...,\ x+y^{m-1}$ (geometric progressions shifted by x)
- $x,\ x+y,\ x+2y,\ x+y^2$
- $x,\ x+y,\ x+y^2,\ x+y+y^2$.

Algebraic relations in polynomial progressions

We can differentiate between various progressions based on how many algebraic relations of the form

$$Q_0(x) + Q_1(x + P_1(y)) + ... + Q_{m-1}(x + P_{m-1}(y)) = 0$$

they satisfy.

On one hand, we have arithmetic progressions which satisfy plenty of algebraic relations. For instance, $x,\ x+y,\ x+2y,\ x+3y$ satisfies

- two linear relations: $x + (x + 2y) = 2(x + y)$ and $(x + y) + (x + 3y) = 2(x + 2y)$,
- a quadratic relation: $x^2 - 3(x + y)^2 + 3(x + 2y)^2 - (x + 3y)^2 = 0$.

By contrast, the shifted geometric progression $x, x + y, x + y^2, ..., x + y^{m-1}$ satisfies no such algebraic relations.

Szemerédi theorem

Theorem (Szemerédi, 1975)

Let A be a dense subset of natural numbers, and suppose $m \geqslant 3$ is an integer. Then A contains an arithmetic progression of length m, i.e. a configuration of the form

$$x,\ x+y,\ ...,\ x+(m-1)y$$

for some $x, y \in \mathbb{N}$ with $y \neq 0$.

Note: $A \subset \mathbb{N}$ is *dense* if $\limsup_{N\to\infty} \frac{|A\cap\{1,...,N\}|}{N} > 0$ and *sparse* otherwise. For instance

- the set $2\mathbb{N} = \{2, 4, 6, ...\}$ is dense with density $\frac{1}{2}$,
- the set of primes is sparse because there are $\sim \frac{N}{\log N}$ primes in $\{1, ..., N\}$ (but primes are still known to contain arithmetic progressions of arbitrary length - see Green-Tao theorem).

Polynomial Szemerédi theorem

Szemerédi theorem has been significantly generalised.

Theorem (Bergelson & Leibman, 1996)

Let $P_1, ..., P_m$ be integral polynomials, i.e. polynomials with integer coefficients and $P_1(0) = ... = P_m(0) = 0$. Then each dense subset of natural numbers contains a polynomial progression of the form

$$x,\ x + P_1(y),\ ...,\ x + P_m(y)$$

for $x, y \in \mathbb{N}$ with $y \neq 0$.

The theorem need not be true if the condition

$$P_1(0) = ... = P_m(0) = 0$$

is not satisfied. Let $P(y) = y^2 + 1$. Then $P(y) \neq 0 \mod 3$ for $y \in \mathbb{Z}$. Hence $3\mathbb{N}$ does not contain $x,\ x + P(y)$.

Polynomial Szemerédi theorem in finite fields

Theorem (Polynomial Szemerédi theorem, finitary version)

Let $P_1, ..., P_m$ be integral polynomials and $0 < \alpha < 1$. There exists $N_0 = N_0(\alpha) \in \mathbb{N}$ such that for all $N > N_0$, each subset of $\{1, ..., N\}$ of size at least αN contains

$$x,\ x + P_1(y),\ ...,\ x + P_m(y)$$

for $y \neq 0$.

Theorem (Polynomial Szemerédi theorem in finite fields)

Let $P_1, ..., P_m$ be integral polynomials and $0 < \alpha < 1$. There exists $p_0 = p_0(\alpha) \in \mathbb{N}$ such that for all primes $p > p_0$, each subset of $\mathbb{F}_p$ of size at least αp contains

$$x,\ x + P_1(y),\ ...,\ x + P_m(y)$$

for $y \neq 0$.

Theorem (Polynomial Szemerédi theorem in finite fields)

Let $P_1, ..., P_m$ be integral polynomials and $0 < \alpha < 1$. There exists $p_0 = p_0(\alpha) \in \mathbb{N}$ such that for all primes $p > p_0$, each subset of $\mathbb{F}_p$ of size at least αp contains

$$x,\ x + P_1(y),\ ...,\ x + P_m(y)$$

for $y \neq 0$.

Once we fix polynomials $P_1, ..., P_m$, can we say anything about the *number* of polynomial progressions of the form

$$x,\ x + P_1(y),\ ...,\ x + P_m(y)$$

in a subset $A \subseteq \mathbb{F}_p$?

This is our big question.

Counting arithmetic progressions in subsets of finite fields

One of the corollaries of Szeméredi theorem is the following statement.

Theorem (Varnavides, 1959)

Let $\alpha > 0$ and $m \geqslant 3$. Then there exist $c_{\alpha,m} > 0$ such that for all primes p, each subset $A \subseteq \mathbb{F}_p$ of size αp contains at least $c_{\alpha,m} p^2$ arithmetic progressions of length m.

We have lower bounds on $c_{\alpha,m}$. For instance, we can take

$$c_{\alpha,3} = \exp(-C\alpha^{-(1-c)})$$

for some $c, C > 0$ by (Bloom & Sisask, 2020).

Counting linearly independent configurations

How about other polynomial progressions?

Theorem (Peluse, 2019)

Let $m \geqslant 3$ and $A \subseteq \mathbb{F}_p$ have size $|A| = \alpha p$. There exists $c_m > 0$ such that

$$|\{(x,\ x+y,\ ...,\ x+y^{m-1}) \in A^m\}| = \alpha^m p^2 + O_m(p^{2-c_m}).$$

More generally, the result holds if we replace $y, ..., y^{m-1}$ by any $m-1$ linearly independent integral polynomials (the absolute constants in the error term depend on the choice of polynomials).

In particular, Peluse's theorem imply that all subsets of $\mathbb{F}_p$ of size at least $C_m p^{1-c'_m}$ for some $c'_m, C_m > 0$ contain

$$x,\ x+y,\ ...,\ x+y^{m-1}$$

with $y \neq 0$.

Arithmetic progressions with higher-power differences

Theorem (K., 2020)

Let $m \geqslant 3, k \geqslant 2$ and $A \subseteq \mathbb{F}_p$. There exists $c_{m,k} > 0$ such that

$$|\{(x,\ x+y^k,\ ...,\ x+(m-1)y^k) \in A^m\}|$$
$$= \frac{1}{k}|\{(x,\ x+y,\ ...,\ x+(m-1)y) \in A^m\}| + O_{m,k}(p^{2-c_{m,k}}).$$

Hence the number of arithmetic progressions with, say, square or cubic differences in subsets of finite fields is of the same order of magnitude as the number of all arithmetic progressions.

Arithmetic progressions with higher-power differences

Theorem (K., 2020)

Let $m \geqslant 3, k \geqslant 2$ and $A \subseteq \mathbb{F}_p$. There exists $c_{m,k} > 0$ such that

$$|\{(x,\ x+y^k,\ ...,\ x+(m-1)y^k) \in A^m\}|$$
$$= \frac{1}{k}|\{(x,\ x+y,\ ...,\ x+(m-1)y) \in A^m\}| + O_{m,k}(p^{2-c_{m,k}}).$$

We remarked before that a set $A \subset \mathbb{F}_p$ of size αp would contain at least $c'_{m,k}p^2$ m-term arithmetic progressions for some $c'_{m,k} > 0$, hence the result above implies a special case of the polynomial Szemerédi theorem in finite fields.

Counting other polynomial progressions

Theorem (K., 2020)

Suppose $A \subseteq \mathbb{F}_p$. There exists $c > 0$ such that

$$|\{(x,\ x+y,\ x+2y,\ x+y^3) \in A^4\}|$$
$$= \{(x,\ x+y,\ x+2y) \in A^3\}| \cdot \frac{|A|}{p} + O(p^{2-c}).$$

The same result (with different values of absolute constants) holds if we replace y^3 in the last term by any polynomial of degree at least 3, but not if we replace it by y^2 or another quadratic. We will explain this later.

Counting other polynomial progressions

And one more.

Theorem (K., 2020)

Suppose $A \subseteq \mathbb{F}_p$. Then

$$|\{(x,\ x+y,\ x+y^2,\ x+y+y^2) \in A^4\}|$$
$$= \{(x,\ x+y,\ x+z,\ x+y+z) \in A^4\}|/p + o(p^2).$$

How to prove an asymptotic count?

How would we prove a result like this?

Theorem (K., 2020)

Suppose $A \subseteq \mathbb{F}_p$. There exists $c > 0$ such that

$$|\{(x,\ x+y,\ x+2y,\ x+y^3) \in A^4\}|$$
$$= \{(x,\ x+y,\ x+2y) \in A^3\}| \cdot \frac{|A|}{p} + O(p^{2-c}).$$

A functional version of the problem

Instead of working with

$$|\{(x,y) \in \mathbb{F}_p^2 : (x,\ x+y,\ x+2y,\ x+y^3) \in A^4\}|$$

we look at

$$\mathbb{E}_{x,y\in\mathbb{F}_p} 1_A(x)1_A(x+y)1_A(x+2y)1_A(x+y^3).$$

More generally, we need to analyse

$$\mathbb{E}_{x,y\in\mathbb{F}_p} f_1(x)f_2(x+y)f_3(x+2y)f_4(x+y^3)$$

for $f_1, f_2, f_3, f_4 : \mathbb{F}_p \to \mathbb{C}$ that are 1-bounded (i.e. $|f_i(x)| \leqslant 1$).

A functional version of the counting theorem

The estimate

$$|\{(x,y) \in \mathbb{F}_p^2 : (x,\ x+y,\ x+2y,\ x+y^3) \in A^4\}|$$
$$= |\{(x,y) \in \mathbb{F}_p^2 : (x,\ x+y,\ x+2y) \in A^3\}| \cdot |A|/p + O(p^{2-c})$$

follows from the following.

Theorem (K., 2019)

For any 1-bounded functions $f_1, f_2, f_3, f_4 : \mathbb{F}_p \to \mathbb{C}$, we have

$$\mathbb{E}_{x,y \in \mathbb{F}_p} f_1(x) f_2(x+y) f_3(x+2y) f_4(x+y^3)$$
$$= \mathbb{E}_{x,y \in \mathbb{F}_p} f_1(x) f_2(x+y) f_3(x+2y) \cdot \mathbb{E}_{z \in \mathbb{F}_p} f_4(z) + O(p^{-c}),$$

where the error term does not depend on the choice of functions f_1, f_2, f_3, f_4.

Discorrelation

One can think of the equality

$$\begin{aligned}&\mathbb{E}_{x,y\in\mathbb{F}_p} f_1(x)f_2(x+y)f_3(x+2y)f_4(x+y^3)\\&= \mathbb{E}_{x,y\in\mathbb{F}_p} f_1(x)f_2(x+y)f_3(x+2y)\cdot \mathbb{E}_{z\in\mathbb{F}_p} f_4(z) + O(p^{-c}),\end{aligned}$$

as a "discorrelation": up to the error term $O(p^{-c})$, the term $x+y^3$ is "independent" from the arithmetic progression $x,\ x+y,\ x+2y$.

The result above (with different absolute constants) remains true if we replace y^3 by any polynomial of degree at least 3. But it fails for y^2 or other quadratic polynomials. Why?

Why does $x,\ x+y,\ x+2y,\ x+y^2$ not work?

Given a polynomial progression

$$x,\ x+P_1(y),\ \ldots,\ x+P_{m-1}(y),$$

one has to understand algebraic relations of the form

$$Q_0(x)+Q_1(x+P_1(y))+\ldots+Q_{m-1}(x+P_{m-1}(y))=0$$

for polynomials $Q_0,\ldots,Q_{m-1}$.

For instance, the terms of $x,\ x+y,\ x+2y,\ x+y^3$ only satisfy

$$x-2(x+y)+(x+2y)=0,$$

and similarly if we replace y^3 by any $P\in\mathbb{Z}[y]$ with $\deg P\geqslant 3$.

However, the progression $x,\ x+y,\ x+2y,\ x+y^2$ also satisfies

$$(x^2+2x)-2(x+y)^2+(x+2y)^2-2(x+y^2)=0.$$

Why does $x,\ x+y,\ x+2y,\ x+y^2$ not work?

Let's see why we care about the algebraic relation

$$(x^2+2x)-2(x+y)^2+(x+2y)^2-2(x+y^2)=0.$$

Taking

$$f_0(t)=e_p(t^2+2t),\ f_1(t)=e_p(-2t^2),\ f_3(t)=e_p(t^2),\ f_4(t)=e_p(-2t),$$

and observing that

$$\begin{aligned} &f_0(x)f_1(x+y)f_2(x+2y)f_3(x+y^2)\\ &=e_p((x^2+2x)-2(x+y)^2+(x+2y)^2-2(x+y^2))=1, \end{aligned}$$

we deduce that

$$\mathbb{E}_{x,y\in\mathbb{F}_p}f_1(x)f_2(x+y)f_3(x+2y)f_4(x+y^3)=1$$

but

$$\mathbb{E}_{x,y\in\mathbb{F}_p}f_1(x)f_2(x+y)f_3(x+2y)\mathbb{E}_{z\in\mathbb{F}_p}f_4(z)=0.$$

Algebraic relations as obstruction

Hence discorrelation fails for $x,\ x+y,\ x+2y,\ x+y^2$.

The example of f_1, f_2, f_3, f_4 in the previous slide shows how we can use algebraic relations like

$$(x^2+2x)-2(x+y)^2+(x+2y)^2-2(x+y^2)=0.$$

to construct counterexamples to discorrelation.

These algebraic relations are the only obstructions.

How general is the discorrelation equality?

A discorrelation equality

$$\mathbb{E}_{x,y\in\mathbb{F}_p}\prod_{j=0}^{m-1} f_j(x+jy)\prod_{j=m}^{m+k-1} f_j(x+P_j(y))$$

$$=\mathbb{E}_{x,y\in\mathbb{F}_p}\prod_{j=0}^{m-1} f_j(x+jy)\left(\prod_{j=m}^{m+k-1}\mathbb{E}_{x\in\mathbb{F}_p} f_j(x)\right)+O(p^{-c})$$

holds for any polynomial progression

$$x,\ x+y,\ \ldots,\ x+(m-1)y,\ x+P_m(y),\ \ldots,\ x+P_{m+k}(y),$$

such that

$$a_m P_m+\ldots+a_{m+k}P_{m+k}$$

has degree at least m unless $a_m=\ldots=a_{m+k}=0$.

How general is the discorrelation equality?

For instance, the discorrelation equality holds for

$$x,\ x+y,\ x+2y,\ x+y^3,\ x+y^4+y^2,$$

but it fails for

$$x,\ x+y,\ x+2y,\ x+y^3,\ x+y^3+y^2$$

because

$$(x+y^3+y^2)-(x+y^3)=y^2$$

has degree 2, and so the algebraic relation

$$(x^2+2x)-2(x+y)^2+(x+2y)^2+2(x+y^3)-2(x+y^3+y^2)=0$$

prevents discorrelation from happening.

The asymptotic for $x,\ x+y,\ x+y^2,\ x+y+y^2$

At the end, we shall briefly explain the following equality

$$\begin{aligned}&|\{(x,\ x+y,\ x+y^2,\ x+y+y^2)\in A^4\}|\\&=\{(x,\ x+y,\ x+z,\ x+y+z)\in A^4\}|/p+o(p^2).\end{aligned}$$

The heuristic here is that y^2 acts like a separate variable, hence these two counts are related.

The crucial part is that these two progressions satisfy essentially the same linear relation

$$\begin{aligned}x-(x+y)-(x+y^2)+(x+y+y^2)&=0\\\text{and}\quad x-(x+y)-(x+z)+(x+y+z)&=0,\end{aligned}$$

and nothing else.

The asymptotic for $x,\ x+y,\ x+y^2,\ x+y+y^2$

You may also wonder why we divide the second expression by p

$$|\{(x,\ x+y,\ x+y^2,\ x+y+y^2) \in A^4\}|$$
$$= |\{(x,\ x+y,\ x+z,\ x+y+z) \in A^4\}|/p + o(p^2).$$

The first expression is of order $O(p^2)$ (because there are two parameters x and y) while the second is of order $O(p^3)$ (because there is an additional parameter z), therefore the second expression is normalized by dividing by p.

Questions

I will finish by answering some of the questions that you might have.

Why do we care?

Question

Why do we care at all about counting such configurations?

First, I think that polynomial progressions are fairly intuitive objects to study, and understanding how often they appear in subsets of integers or finite fields seems a natural thing that we may want to know about them. Second, we can use these counts to deduce upper bounds for the size of subsets of $\mathbb{F}_p$ lacking the configurations in question.

Can p be a prime power?

Question

Do the results generalize to $\mathbb{F}_q$, where q is a prime power?

The results for

1. $x,\ x+y,\ x+y^2$
2. $x,\ x+y^2,\ x+2y^2$
3. $x,\ x+y,\ x+2y,\ x+y^3$

hold for any prime power q.

The method that I have used for $x,\ x+y,\ x+y^2,\ x+y+y^2$ has only allowed me to prove the results for this configuration over $\mathbb{F}_p$ with p prime. Nevertheless, I do not see an obvious reason for analogous results to fail over $\mathbb{F}_q$ with a prime power q.

Proving a discorrelation equality

Question

How do you prove a discorrelation equality for $x,\ x+y,\ x+2y,\ x+y^3$ and similar progressions?

It is a mix of discrete Fourier analysis, the Cauchy-Schwarz inequality, popularity principle and a basic theory of Gowers norms.

Error terms

Question

Why do you have an $O(p^{2-c})$ error term for some configurations but $o(p^2)$ for another?

The method that I use to prove the result for $x,\ x+y,\ x+y^2,\ x+y+y^2$ relies on nilsequences from so-called higher order Fourier analysis. Results concerning nilsequences that I am quoting don't have reasonable quantitative bounds, hence the error term is purely qualitative.

Thank you!

Thank you for your attention! Feel free to contact me with any questions over email: borys.kuca@manchester.ac.uk

References


B. Kuca *Further bounds in the polynomial Szemerédi theorem over finite fields*, arXiv:1907.08446, Acta Arithmetica, accepted.


B. Kuca *True complexity of polynomial progressions in finite fields*, arXiv:2001.05220.


S. Peluse *On the polynomial Szemerédi theorem in finite fields*, Duke Mathematical Journal, 168 (2019), no. 5, 749-774.