Covering and expanding polynomials in finite fields

Norbert Hegyvári

Eötvös University and Rényi Institute, Budapest

Luminy, 03/02/2014

History

Starting a question in Computer Sciences – Barak, Implagliazzo, Wigderson (2004):

History

Starting a question in Computer Sciences – Barak, Implagliazzo, Wigderson (2004):

Sum-product type theorems a way of creating algebraically "pseudo-randomness" properties

History

Starting a question in Computer Sciences – Barak, Implagliazzo, Wigderson (2004):

Sum-product type theorems a way of creating algebraically "pseudo-randomness" properties

Question (B-I-W): Fix $0 < \alpha < 1$, find an explicit polynomial $f : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$, $A, B \subseteq \mathbb{F}_p$, $|B| \asymp |A| \sim p^{\alpha}$ for some $\beta = \beta(\alpha) > \alpha$

$$|f(A, B)| > p^{\beta}.$$

History

Starting a question in Computer Sciences – Barak, Implagliazzo, Wigderson (2004):

Sum-product type theorems a way of creating algebraically "pseudo-randomness" properties

Question (B-I-W): Fix $0 < \alpha < 1$, find an explicit polynomial $f : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$, $A, B \subseteq \mathbb{F}_p$, $|B| \asymp |A| \sim p^{\alpha}$ for some $\beta = \beta(\alpha) > \alpha$

$$|f(A, B)| > p^{\beta}.$$

$f = f(x, y)$ is said to be *expander polynomial*

J. Bourgain (2005):

$f = f(x, y) = x^2 + xy$ is an expander

History

Theorem: (J.B.)

For all $0 < \alpha < 1$, there exists a $\delta > 0$, s.t. $|B| \asymp |A| \sim p^{\alpha}$ the polynomial $f(x, y) = x^2 + xy$ is an expander, i.e.

$$|f(A, B)| > p^{\alpha+\delta}.$$

History

Theorem: (J.B.)

For all $0 < \alpha < 1$, there exists a $\delta > 0$, s.t. $|B| \asymp |A| \sim p^{\alpha}$ the polynomial $f(x, y) = x^2 + xy$ is an expander, i.e.

$$|f(A, B)| > p^{\alpha+\delta}.$$

Remark:

1. In his proof δ is inexplicit.

History

Theorem: (J.B.)

For all $0 < \alpha < 1$, there exists a $\delta > 0$, s.t. $|B| \asymp |A| \sim p^{\alpha}$ the polynomial $f(x, y) = x^2 + xy$ is an expander, i.e.

$$|f(A, B)| > p^{\alpha+\delta}.$$

Remark:

1. In his proof δ is inexplicit.

2. The proof based on a sum-product result in $\mathbb{F}_p$ by Bourgain-Katz-Tao.

History

Theorem: (J.B.)

For all $0 < \alpha < 1$, there exists a $\delta > 0$, s.t. $|B| \asymp |A| \sim p^{\alpha}$ the polynomial $f(x, y) = x^2 + xy$ is an expander, i.e.

$$|f(A, B)| > p^{\alpha+\delta}.$$

Remark:

1. In his proof δ is inexplicit.

2. The proof based on a sum-product result in $\mathbb{F}_p$ by Bourgain-Katz-Tao.

Theorem: (B-K-T.)

For all $0 < \alpha < 1$, there exists a $\delta > 0$, s.t. $|A| < p^{1-\alpha}$ then

$$|A + A| + |A.A| \gg p^{1+\delta}.$$

History

Expanders with more variables

History

Expanders with more variables

B-K-T theorems trivially implies

$$f(x, y, z, w) = x + y + zw$$

is an expander

History

Expanders with more variables

B-K-T theorem trivially implies

$$f(x, y, z, w) = x + y + zw$$

is an expander

+ Ruzsa's calculus

$$f(x, y, z) = x + yz$$

is an expander

Results

joint with F. Hennecart

Questions:

1. Is there an infinite family of expanding maps of two variables?

Results

joint with F. Hennecart

Questions:

1. Is there an infinite family of expanding maps of two variables?

2. What is the measure of expanding of polynomials?

Results

joint with F. Hennecart

Questions:

1. Is there an infinite family of expanding maps of two variables?

2. What is the measure of expanding of polynomials?

Theorem: (HH)

Let $k \geq 1$, $f, g \in \mathbb{Z}[x]$. Then

$$F(x, y) = f(x) + x^k g(y)$$

is an expander, provided $f(x)$ is affinely independent to x^k.

Results

Affinely independent:

no $(u, v) \in \mathbb{Z}^2$ s.t. $f(x) = uh(x) + v$ or $h(x) = uf(x) + v$.

If $u \neq 0$, then

$$F(x, y) = (f(x) + \frac{v}{u})(1 + ug(y)) - \frac{v}{u}$$

Results

Measure of expanding:

Results

Measure of expanding:

Theorem: (HH) For any pair (A, B) of subsets of $\mathbb{F}_p$ such that $|A| \asymp |B| \asymp p^{\alpha}$, $\alpha > 1/2$

$$|F(A, B)| \gg |A|^{1+\frac{\min\{2\alpha-1;2-2\alpha\}}{2}}.$$

Results

Measure of expanding:

Theorem: (HH) For any pair (A, B) of subsets of $\mathbb{F}_p$ such that $|A| \asymp |B| \asymp p^{\alpha}$, $\alpha > 1/2$

$$|F(A, B)| \gg |A|^{1+\frac{\min\{2\alpha-1;2-2\alpha\}}{2}}.$$

We define the notations of

strong expander and complete expander

Results

Measure of expanding:

Theorem: (HH) For any pair (A, B) of subsets of $\mathbb{F}_p$ such that $|A| \asymp |B| \asymp p^{\alpha}$, $\alpha > 1/2$

$$|F(A, B)| \gg |A|^{1+\frac{\min\{2\alpha-1;2-2\alpha\}}{2}}.$$

We define the notations of

strong expander and complete expander

$F(x, y)$ is complete expander, if for

$|A| \asymp |B| = c_1 p^{\alpha}$,

Results

Measure of expanding:

Theorem: (HH) For any pair (A, B) of subsets of $\mathbb{F}_p$ such that $|A| \asymp |B| \asymp p^{\alpha}$, $\alpha > 1/2$

$$|F(A, B)| \gg |A|^{1+\frac{\min\{2\alpha-1;2-2\alpha\}}{2}}.$$

We define the notations of

strong expander and complete expander

$F(x, y)$ is complete expander, if for

$|A| \asymp |B| = c_1 p^{\alpha}$,

$$|F_p(A, B)| \geq c p^{\min\{1;2\alpha\}}.$$

Results

Measure of expanding:

Theorem: (HH) For any pair (A, B) of subsets of $\mathbb{F}_p$ such that $|A| \asymp |B| \asymp p^{\alpha}$, $\alpha > 1/2$

$$|F(A, B)| \gg |A|^{1+\frac{\min\{2\alpha-1;2-2\alpha\}}{2}}.$$

We define the notations of

strong expander and complete expander

$F(x, y)$ is complete expander, if for

$|A| \asymp |B| = c_1 p^{\alpha}$,

$$|F_p(A, B)| \geq c p^{\min\{1;2\alpha\}}.$$

(later Hart, Li and Shen did a wider classification)

Results

Measure of expanding:

For the Bourgain's map $G(x, y) = x^2 + xy$,

Theorem: (Shkredov)

$$|G(A, B)| \geq (p-1) - \frac{40p^{5/2}}{|A||B|}.$$

Results

Measure of expanding:

For the Bourgain's map $G(x, y) = x^2 + xy$,

Theorem: (Shkredov)

$$|G(A, B)| \geq (p-1) - \frac{40p^{5/2}}{|A||B|}.$$

and hence

If $|A|, |B| > p^{3/4+}$, then $G(A, B)$ covers almost everything.

Results

Measure of expanding:

For the Bourgain's map $G(x, y) = x^2 + xy$,

Theorem: (Shkredov)

$$|G(A, B)| \geq (p - 1) - \frac{40p^{5/2}}{|A||B|}.$$

and hence

If $|A|, |B| > p^{3/4+}$, then $G(A, B)$ covers almost everything.

In the range $|A|, |B| > p^{3/4+}$, the Bourgain's map is a complete expander.

Results

Measure of expanding:

On the other hand

Results

Measure of expanding:

On the other hand

Theorem: (HH)

Let $k, u \in \mathbb{Z}$, $k \geq 2$. Let

$$F(x, y) = x^{2k} + ux^k + x^k y.$$

Then for any α, $0 < \alpha \leq 1/2$, F is not a complete expander according to $\{\alpha\}$.

Results

Measure of expanding:

On the other hand

Theorem: (HH)

Let $k, u \in \mathbb{Z}$, $k \geq 2$. Let

$$F(x, y) = x^{2k} + ux^k + x^k y.$$

Then for any α, $0 < \alpha \leq 1/2$, F is not a complete expander according to $\{\alpha\}$.

(For $k = 1$ and $u = 0$ this map is Bourgain's one.)

Results

Measure of expanding:

Remark:

Many authors investigated how big is

$$A(A+1)$$

(Garaev, Jones, Roche-Newton, Shen)

Results

Measure of expanding:

Remark:

Many authors investigated how big is

$$A(A+1)$$

(Garaev, Jones, Roche-Newton, Shen)

which is related to our map

$$F(x,y) = f(x) + x^k g(y)$$

For $f(x) = x;\ k = 1;\ g(y) = y$

$$F(A,A) = A(A+1).$$

Results

Expanders with "higher degree"

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$F_1(x.y) = f(x, y) + g(x, y)$,

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$F_1(x.y) = f(x, y) + g(x, y)$,

$F_2(x.y) = g(x, f(x, y))$,

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$F_1(x.y) = f(x, y) + g(x, y)$,

$F_2(x.y) = g(x, f(x, y))$,

$F_3(x.y) = f(x, y)/g(x, y)$,

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$F_1(x.y) = f(x, y) + g(x, y)$,

$F_2(x.y) = g(x, f(x, y))$,

$F_3(x.y) = f(x, y)/g(x, y)$,

$F_4(x.y) = f(x, y) \cdot g(x, y)$.

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$F_1(x.y) = x + y + xy = (x + 1)(y + 1) - 1$

$F_2(x.y) = g(x, f(x, y)),$

$F_3(x.y) = f(x, y)/g(x, y),$

$F_4(x.y) = f(x, y) \cdot g(x, y).$

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$F_1(x.y) = x + y + xy = (x + 1)(y + 1) - 1$

$F_2(x.y) = g(x, f(x, y)) = x^2 + xy$

$F_3(x.y) = f(x, y)/g(x, y)$,

$F_4(x.y) = f(x, y) \cdot g(x, y)$.

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$F_1(x.y) = x + y + xy = (x + 1)(y + 1) - 1$

$F_2(x.y) = g(x, f(x, y)) = x^2 + xy$

$F_3(x.y) = f(x, y)/g(x, y) = \frac{1}{x} + \frac{1}{y}$

$F_4(x.y) = f(x, y) \cdot g(x, y).$

Results

Expanders with "higher degree"

By "sum-product" theorem in prime fields:

Theorem: For all $0 < \varepsilon < 1$, there is $\delta = \delta(\varepsilon) > 0$, s.t. if $|A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| \gg |A|^{1+\delta}.$$

So $f(x, y) = x + y$ or $g(x, y) = x \cdot y$ is an expander.

What about

$$F_1(x.y) = x + y + xy = (x + 1)(y + 1) - 1$$

$$F_2(x.y) = g(x, f(x, y)) = x^2 + xy$$

$$F_3(x.y) = f(x, y)/g(x, y) = \frac{1}{x} + \frac{1}{y}$$

$$F_4(x.y) = f(x, y) \cdot g(x, y) = x^2y + xy^2.$$

Results

On the map $x^2y + xy^2$

Results

On the map $x^2y + xy^2$

Sumsets in $\mathbb{R}$:

Results

On the map $x^2y + xy^2$

Sumsets in $\mathbb{R}$:

Test of Elekes and Rónyai:

Results

On the map $x^2y + xy^2$

Sumsets in $\mathbb{R}$:

Test of Elekes and Rónyai:

Let $A, B \subset \mathbb{R}$, $|A| = |B| = n$, and $q_1(x, y) := \frac{\partial T/\partial x}{\partial T/\partial y}$, and $T(x, y) \in \mathbb{R}[x, y]$. If

$$q_2(x, y) := \frac{\partial^2(\log |q_1(x, y)|)}{\partial x \partial y}$$

is not identically zero, then

$$|T(A, B)|/n \to \infty,$$

as $n \to \infty$.

Results

On the map $x^2y + xy^2$

Sumsets in $\mathbb{R}$:

Test of Elekes and Rónyai:

Let $A, B \subset \mathbb{R}$, $|A| = |B| = n$, and $q_1(x, y) := \frac{\partial T/\partial x}{\partial T/\partial y}$, and $T(x, y) \in \mathbb{R}[x, y]$. If

$$q_2(x, y) := \frac{\partial^2(\log |q_1(x, y)|)}{\partial x \partial y}$$

is not identically zero, then

$$|T(A, B)|/n \to \infty,$$

as $n \to \infty$.

A chance that the map $x^2y + xy^2$ to be an expander.

Results

On the map $x^2y + xy^2$

Theorem: [HH] Let $f(x, y) = xy(x+y)$ and A, B be two non empty finite sets of non zero real numbers. Then

$$|f(A, B)| \gg |A|^{2/3}|B|^{2/3}. \tag{0.1}$$

Results

On the map $x^2y + xy^2$

Theorem: [HH] Let $f(x,y) = xy(x+y)$ and A, B be two non empty finite sets of non zero real numbers. Then

$$|f(A,B)| \gg |A|^{2/3}|B|^{2/3}. \tag{0.2}$$

In finite fields just conditional results are available:

Results

On the map $x^2y + xy^2$

Theorem: [HH] Let $f(x,y) = xy(x+y)$ and A, B be two non empty finite sets of non zero real numbers. Then

$$|f(A,B)| \gg |A|^{2/3}|B|^{2/3}. \tag{0.3}$$

In finite fields just conditional results are available:

Theorem: [HH] Let $A, B \subset \mathbb{F}_p$ such that $|A|, |B| \leq p^{1/2-1/400}$ and $|A| \asymp |B|$. Let $f(x,y) = xy(x+y)$. Then

$$\max(|f(A,B)|, |A \cdot B|) \gg |A|^{1+\theta}$$

for some $\theta > 0$.

Results

On the map $x^2y + xy^2$

Furthermore

Theorem: [HH]

If $A \subset \mathbb{F}_p$ such that $|A| \leq p^{1/2-1/500}$. Let $f(x,y) = xy(x+y)$. Then

$$\max(|f(A,A)|, |A \cdot A|) \gg |A|^{1+1/800}.$$

Results

On the map $x^2y + xy^2$

Furthermore

Theorem: [HH]

If $A \subset \mathbb{F}_p$ such that $|A| \leq p^{1/2-1/500}$. Let $f(x,y) = xy(x+y)$. Then

$$\max(|f(A,A)|, |A \cdot A|) \gg |A|^{1+1/800}.$$

A more general result:

Results

On the map $x^2y + xy^2$

Furthermore

Theorem: [HH]

If $A \subset \mathbb{F}_p$ such that $|A| \leq p^{1/2-1/500}$. Let $f(x,y) = xy(x+y)$. Then

$$\max(|f(A,A)|, |A \cdot A|) \gg |A|^{1+1/800}.$$

A more general result:

Fix k and the degrees of two polynomials $g(x), h(y)$, and let $f(x,y) = g(x)h(y)(x^k + y^k)$.

Results

On the map $x^2y + xy^2$

Furthermore

Theorem: [HH]

If $A \subset \mathbb{F}_p$ such that $|A| \leq p^{1/2-1/500}$. Let $f(x,y) = xy(x+y)$. Then

$$\max(|f(A,A)|, |A \cdot A|) \gg |A|^{1+1/800}.$$

A more general result:

Fix k and the degrees of two polynomials $g(x), h(y)$, and let $f(x,y) = g(x)h(y)(x^k + y^k)$.

Theorem: [HH] For any $A, B, C \subset \mathbb{F}_p$, one has

$$|f(A,B)||A \cdot C||B \cdot C| \gg \min\left(\frac{|A|^2|B|^2|C|}{p}, p|A||B|\right).$$

Results

Remark:

Related results are obtained by Vu, Hart, Li, Shen, Bukh, Tsiserman

History

Covering polynomials

History

Covering polynomials

In 2005 Sárközy proved:

Theorem: (S)

For $A, B, C, D \subseteq \mathbb{F}_p$, the equation

$$a + b = cd, \ (a, b, c, d) \in A \times B \times C \times D$$

has a solution, provided

$$|A||B||C||D| > p^3.$$

History

Covering polynomials

In 2005 Sárközy proved:

Theorem: (S)

For $A, B, C, D \subseteq \mathbb{F}_p$, the equation

$$a + b = cd, \ (a, b, c, d) \in A \times B \times C \times D$$

has a solution, provided

$$|A||B||C||D| > p^3.$$

It implies if $F(x, y, z, w) = x + y + zw$, then

$$F(A, B, C, D) = \mathbb{F}_p,$$

provided $|A||B||C||D| > p^3$.

History

Covering polynomials

Definition: A map $F : {\mathbb{F}_p}^k \mapsto \mathbb{F}_p$ is said to be covering polynomial respect to β if

$$f(A_1, A_2, \ldots, A_k) = \mathbb{F}_p$$

provided $\prod_i |A_i| > p^\beta$.

History

Covering polynomials

Definition: A map $F : {\mathbb{F}_p}^k \mapsto \mathbb{F}_p$ is said to be covering polynomial respect to β if

$$f(A_1, A_2, \ldots, A_k) = \mathbb{F}_p$$

provided $\prod_i |A_i| > p^\beta$.

Sárközy's result is sharp for "balanced" cardinalities of the sets.

History

Covering polynomials

Definition: A map $F : {\mathbb{F}_p}^k \mapsto \mathbb{F}_p$ is said to be covering polynomial respect to β if

$$f(A_1, A_2, \ldots, A_k) = \mathbb{F}_p$$

provided $\prod_i |A_i| > p^\beta$.

Sárközy's result is sharp for "balanced" cardinalities of the sets.

In the "imbalanced" case Shparlinski proved that the bound p^3 can be relaxed to $\approx p^{2.5}$.

History

Covering polynomials

Definition: A map $F : {\mathbb{F}_p}^k \mapsto \mathbb{F}_p$ is said to be covering polynomial respect to β if

$$f(A_1, A_2, \ldots, A_k) = \mathbb{F}_p$$

provided $\prod_i |A_i| > p^\beta$.

Sárközy's result is sharp for "balanced" cardinalities of the sets.

In the "imbalanced" case Shparlinski proved that the bound p^3 can be relaxed to $\approx p^{2.5}$.

More precisely

History

Covering polynomials

Theorem:(Shparlinski)

For any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that if

$$|A| > p^{1/2+\varepsilon},\ |B| > p^{\varepsilon},\ |C||D| > p^{2-\delta},$$

then the equation $a + b = cd$ can be solved.

History

Covering polynomials

Theorem:(Shparlinski)

For any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that if

$$|A| > p^{1/2+\varepsilon},\ |B| > p^{\varepsilon},\ |C||D| > p^{2-\delta},$$

then the equation $a + b = cd$ can be solved.

In the opposite imbalanced case I proved

Results

Covering polynomials

Theorem:(Shparlinski)

For any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that if

$$|A| > p^{1/2+\varepsilon},\ |B| > p^{\varepsilon},\ |C||D| > p^{2-\delta},$$

then the equation $a + b = cd$ can be solved.

In the opposite imbalanced case I proved

Theorem:(H)

Let $A, B \subseteq \mathbb{F}_p$, $H < \mathbb{F}_p^*$. Write $|A||B| = p^{2-2\alpha}$ and $|H| = p^{\beta}$. Then the equation

$$a + b = h;\ (a, b, h) \in A \times B \times H$$

is solvable, provided

$$\beta > \frac{8\alpha + 1}{3}.$$

History

Covering polynomials

Remark:

Many other problems can be performed as a covering question:

History

Covering polynomials

Remark:

Many other problems can be performed as a covering question:

An nice and old problem:

History

Covering polynomials

Remark:

Many other problems can be performed as a covering question:

An nice and old problem:

If $H < \mathbb{F}_p^*$, $|H| > \sqrt{p}$, then what is the $\min\{k : kH = \mathbb{F}_p\}$?

History

Covering polynomials

Remark:

Many other problems can be performed as a covering question:

An nice and old problem:

If $H < \mathbb{F}_p^*$, $|H| > \sqrt{p}$, then what is the $\min\{k : kH = \mathbb{F}_p\}$?

$k \leq 8$ by Glibichuk Konyagin. Follows from: For $f(x_1, \ldots, x_{16} := \sum_{i=1}^{8} x_i x_{i+1}$,

$$f(A, B, \ldots, A, B) = \mathbb{F}_p,$$

provided $|A||B| > p$. (reduced to $k \leq 6$, by Shkredov)

Results

Covering polynomials

Define the following four maps:

Results

Covering polynomials

Define the following four maps:

$G_u(x, y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0, 1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.

Results

Covering polynomials

Define the following four maps:

$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.

$F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed.

Results

Covering polynomials

Define the following four maps:

$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.

$F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed.

With Hennecart we observed:

Results

Covering polynomials

Theorem: [HH] There exist real numbers $0 < \delta, \delta' < 1$ s.t. for any p and for any sets $A, B, C, D \subseteq \mathbb{F}_p$ with

$$|C| > p^{1/2-\delta}, \quad |D| > p^{1/2-\delta} \quad |A||B| > p^{2-\delta'},$$

there exist $a \in A, b \in B, c \in C, d \in D$ solving the equation

$$a + b = F_{p,v}(c, d)$$

and

$$a + b = G_u(x, y)$$

Results

Covering polynomials

Corollary :

The maps $F_{p,v}(x,y)+u+v$ and $G_u(x,y)+u+v$ are covering polynomials on the range of sets above.

Results

Covering polynomials

Corollary :

The maps $F_{p,v}(x,y)+u+v$ and $G_u(x,y)+u+v$ are covering polynomials on the range of sets above.

Covering polynomials pop up many other places.

Results

Covering polynomials

Corollary :

The maps $F_{p,v}(x,y)+u+v$ and $G_u(x,y)+u+v$ are covering polynomials on the range of sets above.

Covering polynomials pop up many other places.

Mentioned a non-abelian group called Heisenberg group over primefield, with elements

Results

Covering polynomials

Corollary :

The maps $F_{p,v}(x,y)+u+v$ and $G_u(x,y)+u+v$ are covering polynomials on the range of sets above.

Covering polynomials pop up many other places.

Mentioned a non-abelian group called Heisenberg group over primefield, with elements

$$[x,y,z]=\begin{pmatrix}1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix}, \quad x,y,z\in\mathbb{F}$$

Results

Covering polynomials

Corollary :

The maps $F_{p,v}(x,y)+u+v$ and $G_u(x,y)+u+v$ are covering polynomials on the range of sets above.

Covering polynomials pop up many other places.

Mentioned a non-abelian group called Heisenberg group over primefield, with elements

$$[x,y,z] = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, \quad x,y,z \in \mathbb{F}$$

$$[x,y,z]\cdot[x',y',z'] = [x+x', y+y', xy'+z+z'].$$

Covering polynomials

The third coordinate

Results

Covering polynomials

The third coordinate

$$f(x, y', z, z') = xy' + z + z'$$

Results

Covering polynomials

The third coordinate

$$f(x, y', z, z') = xy' + z + z'$$

is also a sum-product type map

Results

Covering polynomials

The third coordinate

$$f(x, y', z, z') = xy' + z + z'$$

is also a sum-product type map

which is related some structure result can be followed a forthcoming talk of F. Hennecart.

Thank you