Character sum estimations for various problems in combinatorial number theory

Norbert Hegyvári

Budapest, Eötvös University

2016 January, 8

Content

Content

- Expander polynomials

Content

- Expander polynomials
- Covering polynomials,

Content

- Expander polynomials
- Covering polynomials,
- Product sets in Heisenberg groups

Content

- Expander polynomials
- Covering polynomials,
- Product sets in Heisenberg groups
- Character sums on Hilbert cubes

Expander polynomials

Expander polynomials

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

Expander polynomials

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

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

Expander polynomials

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 $\beta = \beta(\alpha) > \alpha$

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

Expander polynomials

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*

Expander polynomials

Expander polynomials

Theorem (J. Bourgain (2005))

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.*

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

Expander polynomials

Theorem (J. Bourgain (2005))

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.

Expander polynomials

Expander polynomials

Questions :

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

Expander polynomials

Questions :

1. IS THERE AN INFINITE FAMILY OF EXPANDING MAPS OF TWO VARIABLES ?

Theorem (H.-Hennecart)

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.

Expander polynomials

Questions :

1. IS THERE AN INFINITE FAMILY OF EXPANDING MAPS OF TWO VARIABLES ?

Theorem (H.-Hennecart)

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.

AFFINELY INDEPENDENT :

Expander polynomials

Questions :

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

Theorem (H.-Hennecart)

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.

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

Expander polynomials

Questions :

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

Theorem (H.-Hennecart)

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.

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

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

Expander polynomials

Expander polynomials

Measure of expanding :

Expander polynomials

MEASURE OF EXPANDING :

Theorem (H.-Hennecart)

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

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

Expander polynomials

MEASURE OF EXPANDING :

Theorem (H.-Hennecart)

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

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

Theorem (I. Shkredov)

For the Bourgain function $G(x, y) = x^2 + xy$,

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

Expander polynomials

Expander polynomials

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, then $G(A, B)$ covers almost all $\mathbb{F}_p$.

Expander polynomials

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, *then* $G(A, B)$ *covers almost all* $\mathbb{F}_p$.

It motivates the following

Expander polynomials

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, *then* $G(A,B)$ *covers almost all* $\mathbb{F}_p$.

It motivates the following

Definition

$F(x,y)$ *is said to be a complete expander according to* α

Expander polynomials

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, then $G(A,B)$ covers almost all $\mathbb{F}_p$.

It motivates the following

Definition

$F(x,y)$ is said to be a complete expander according to α if for any positive real numbers $L_1 \le L_2$,

Expander polynomials

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, then $G(A, B)$ covers almost all $\mathbb{F}_p$.

It motivates the following

Definition

$F(x, y)$ is said to be a complete expander according to α if for any positive real numbers $L_1 \leq L_2$, there exists a constant $c = c(F, L_1, L_2)$

Expander polynomials

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, then $G(A,B)$ covers almost all $\mathbb{F}_p$.

It motivates the following

Definition

$F(x,y)$ is said to be a complete expander according to α if for any positive real numbers $L_1 \leq L_2$, there exists a constant $c = c(F, L_1, L_2)$ such that for any prime number p and any pair (A,B) of subsets of $\mathbb{F}_p$

Expander polynomials

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, then $G(A, B)$ covers almost all $\mathbb{F}_p$.

It motivates the following

Definition

$F(x, y)$ is said to be a complete expander according to α if for any positive real numbers $L_1 \leq L_2$, there exists a constant $c = c(F, L_1, L_2)$ such that for any prime number p and any pair (A, B) of subsets of $\mathbb{F}_p$ satisfying $L_1 p^\alpha \leq |A|, |B| \leq L_2 p^\alpha$,

Corollary

If $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon > 0$, *then* $G(A, B)$ *covers almost all* $\mathbb{F}_p$.

It motivates the following

Definition

$F(x, y)$ *is said to be a complete expander according to* α *if for any positive real numbers* $L_1 \leq L_2$, *there exists a constant* $c = c(F, L_1, L_2)$ *such that for any prime number* p *and any pair* (A, B) *of subsets of* $\mathbb{F}_p$ *satisfying*
$L_1 p^\alpha \leq |A|, |B| \leq L_2 p^\alpha$,
we have

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

Expander polynomials

Expander polynomials

As a contrast

Expander polynomials

As a contrast

Theorem (H.-Hennecart)

Let $f(x)$ and $g(y)$ be non constant integral polynomials and $F(x,y) = f(x)(f(x)+g(y))$. Then F is not a complete expander according to $\alpha \leq 1/2$.

Expander polynomials

As a contrast

Theorem (H.-Hennecart)

Let $f(x)$ and $g(y)$ be non constant integral polynomials and $F(x,y) = f(x)(f(x)+g(y))$. Then F is not a complete expander according to $\alpha \le 1/2$.

For the proof we need the following :

Expander polynomials

As a contrast

Theorem (H.-Hennecart)

Let $f(x)$ and $g(y)$ be non constant integral polynomials and $F(x,y) = f(x)(f(x) + g(y))$. Then F is not a complete expander according to $\alpha \le 1/2$.

For the proof we need the following :

Lemma

Let $u \in \mathbb{F}_p$, L be a positive integer less than $p/2$ and $f(x)$ be any integral polynomial of degree $k \ge 1$ (as element of $\mathbb{F}_p[x]$). Then the number $N(I)$ of residues $x \in \mathbb{F}_p$ such that $f(x)$ lies in the interval $I = (u - L, u + L)$ of $\mathbb{F}_p$ is at least $L - (k-1)\sqrt{p}$.

Proof

Proof

Let J be the indicator function of the interval $[0, L)$ of $\mathbb{F}_p$ and let

$$T := \sum_{r \in \mathbb{F}_p} \widehat{J * J}(r) S_f(-r, p) e_p(ru),$$

Proof

Let J be the indicator function of the interval $[0, L)$ of $\mathbb{F}_p$ and let

$$T := \sum_{r \in \mathbb{F}_p} \widehat{J * J}(r) S_f(-r, p) e_p(ru),$$

where $S_f(r, p) := \sum_{x \in \mathbb{F}_p} e_p(rf(x))$

Proof

Let J be the indicator function of the interval $[0, L)$ of $\mathbb{F}_p$ and let

$$T := \sum_{r \in \mathbb{F}_p} \widehat{J * J}(r) S_f(-r, p) e_p(ru),$$

where $S_f(r, p) := \sum_{x \in \mathbb{F}_p} e_p(rf(x))$

It is known $|S_f(r, p)| \leq (k-1)\sqrt{p}$ for $r \neq 0$ (p is an odd prime)

Proof

Let J be the indicator function of the interval $[0, L)$ of $\mathbb{F}_p$ and let

$$T := \sum_{r \in \mathbb{F}_p} \widehat{J * J}(r) S_f(-r, p) e_p(ru),$$

where $S_f(r, p) := \sum_{x \in \mathbb{F}_p} e_p(rf(x))$

It is known $|S_f(r, p)| \leq (k-1)\sqrt{p}$ for $r \neq 0$ (p is an odd prime)

Thus

$$T = p\widehat{J * J}(0) + \sum_{r \in \mathbb{F}_p^*} \widehat{J * J}(r) S_f(-r, p) e_p(ru) \geq$$

Proof

Let J be the indicator function of the interval $[0, L)$ of $\mathbb{F}_p$ and let

$$T := \sum_{r \in \mathbb{F}_p} \widehat{J * J}(r) S_f(-r, p) e_p(ru),$$

where $S_f(r, p) := \sum_{x \in \mathbb{F}_p} e_p(rf(x))$

It is known $|S_f(r, p)| \leq (k-1)\sqrt{p}$ for $r \neq 0$ (p is an odd prime)

Thus

$$T = p\widehat{J * J}(0) + \sum_{r \in \mathbb{F}_p^*} \widehat{J * J}(r) S_f(-r, p) e_p(ru) \geq$$

$$\geq pL^2 - k\sqrt{p} \sum_{r \in \mathbb{F}_p^*} |\widehat{J * J}(r)| \geq pL^2 - kLp^{3/2}.$$

Proof of the Lemma

Hence

Proof of the Lemma

Hence

$$T \geq pL(L - k\sqrt{p}).$$

Proof of the Lemma

Hence

$$T \geq pL(L - k\sqrt{p}).$$

On the other direction

Proof of the Lemma

Hence

$$T \geq pL(L - k\sqrt{p}).$$

On the other direction

$$T = \sum_{r \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} J(z)J(y+z)e_p(r(y+u)) \sum_{x \in \mathbb{F}_p} e_p(-rf(x)) =$$

Proof of the Lemma

Hence

$$T \geq pL(L - k\sqrt{p}).$$

On the other direction

$$T = \sum_{r\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)e_p(r(y+u))\sum_{x\in\mathbb{F}_p} e_p(-rf(x)) =$$

$$= \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)\sum_{r\in\mathbb{F}_p} e_p(r(y+u-f(x))) =$$

Proof of the Lemma

Hence

$$T \geq pL(L - k\sqrt{p}).$$

On the other direction

$$T = \sum_{r\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)e_p(r(y+u))\sum_{x\in\mathbb{F}_p} e_p(-rf(x)) =$$

$$= \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)\sum_{r\in\mathbb{F}_p} e_p(r(y+u-f(x))) =$$

$$p\sum_{x\in\mathbb{F}_p} d_L(f(x)-u),$$

Proof of the Lemma

Hence

$$T \geq pL(L - k\sqrt{p}).$$

On the other direction

$$T = \sum_{r\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)e_p(r(y+u))\sum_{x\in\mathbb{F}_p} e_p(-rf(x)) =$$

$$= \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)\sum_{r\in\mathbb{F}_p} e_p(r(y+u-f(x))) =$$

$$p\sum_{x\in\mathbb{F}_p} d_L(f(x)-u),$$

where $d_L(z)$ denotes the number of representations in $\mathbb{F}_p$ of z under the form $j - j'$, $0 \leq j, j' < L$.

Proof of the Lemma

Using

Proof of the Lemma

Using
$d_L(z) \leq L$ for each $z \in \mathbb{F}_p$,

Proof of the Lemma

Using
$d_L(z) \leq L$ for each $z \in \mathbb{F}_p$, we get

$$T \leq pLN(I).$$

Combining the two bounds one can obtain the statement.

Proof of the Lemma

Using
$d_L(z) \leq L$ for each $z \in \mathbb{F}_p$, we get

$$T \leq pLN(I).$$

Combining the two bounds one can obtain the statement.

Furthermore we need a result of Erdős :

Proof of the Lemma

Using
$d_L(z) \leq L$ for each $z \in \mathbb{F}_p$, we get

$$T \leq pLN(I).$$

Combining the two bounds one can obtain the statement.

Furthermore we need a result of Erdős :

Lemma

There exists a positive real number δ such that the number of different integers ab where $1 \leq a, b \leq n$ is $O(n^2/(\ln n)^\delta)$.

(the best known δ is due to G. Tenenbaum)

Proof of the Theorem

Proof of the Theorem

(Let p be large enough $f(x)$ and $g(y)$ are not constant polynomials modulo p.)

Proof of the Theorem

(Let p be large enough $f(x)$ and $g(y)$ are not constant polynomials modulo p.)
Let $L = k\sqrt{p}$

Proof of the Theorem

(Let p be large enough $f(x)$ and $g(y)$ are not constant polynomials modulo p.)
Let $L = k\sqrt{p}$
Let A (resp. B) be the set of the residue classes x (resp. y) such that $f(x)$ (resp. $g(y)$) lies in the interval $(0, 2L)$.

Proof of the Theorem

(Let p be large enough $f(x)$ and $g(y)$ are not constant polynomials modulo p.)
Let $L = k\sqrt{p}$
Let A (resp. B) be the set of the residue classes x (resp. y) such that $f(x)$ (resp. $g(y)$) lies in the interval $(0, 2L)$.
By the first lemma, one has $|A|, |B| \geq \sqrt{p}$.

Proof of the Theorem

(Let p be large enough $f(x)$ and $g(y)$ are not constant polynomials modulo p.)
Let $L = k\sqrt{p}$
Let A (resp. B) be the set of the residue classes x (resp. y) such that $f(x)$ (resp. $g(y)$) lies in the interval $(0, 2L)$.
By the first lemma, one has $|A|, |B| \geq \sqrt{p}$.
Moreover for any $(x, y) \in A \times B$, we have $f(x)$ and $f(x) + g(y)$ in the interval $(0, 4L)$.

Proof of the Theorem

(Let p be large enough $f(x)$ and $g(y)$ are not constant polynomials modulo p.)
Let $L = k\sqrt{p}$
Let A (resp. B) be the set of the residue classes x (resp. y) such that $f(x)$ (resp. $g(y)$) lies in the interval $(0, 2L)$.
By the first lemma, one has $|A|, |B| \geq \sqrt{p}$.
Moreover for any $(x, y) \in A \times B$, we have $f(x)$ and $f(x) + g(y)$ in the interval $(0, 4L)$.
By Erdős Lemma, the number of residues modulo p which can be written as $F(x, y)$ with $(x, y) \in A \times B$, is at most

Proof of the Theorem

(Let p be large enough $f(x)$ and $g(y)$ are not constant polynomials modulo p.)
Let $L = k\sqrt{p}$
Let A (resp. B) be the set of the residue classes x (resp. y) such that $f(x)$ (resp. $g(y)$) lies in the interval $(0, 2L)$.
By the first lemma, one has $|A|, |B| \geq \sqrt{p}$.
Moreover for any $(x, y) \in A \times B$, we have $f(x)$ and $f(x) + g(y)$ in the interval $(0, 4L)$.
By Erdős Lemma, the number of residues modulo p which can be written as $F(x, y)$ with $(x, y) \in A \times B$, is at most

$$O(L^2/(\ln L)^{\delta}) = o(p),$$

(as p tends to infinity).

Remarks

Remarks

Remark

1. Our result ($F(x, y) = f(x) + x^k g(y)$) *covers many special cases ;*

bound on $|A(A+1)|$, $f(x) = x^k, k = 1, g(y) = y$,

or

Remarks

Remark

1. Our result $(F(x,y) = f(x) + x^k g(y))$ *covers many special cases ;*
bound on $|A(A+1)|$, $f(x) = x^k, k = 1, g(y) = y$,
or $x(x+y)$ *(Bourgain's polynomial) e.t.c.*

Remarks

Remark

1. Our result ($F(x,y) = f(x) + x^k g(y)$) *covers many special cases ;*
bound on $|A(A+1)|$, $f(x) = x^k, k = 1, g(y) = y$,
or $x(x+y)$ *(Bourgain's polynomial) e.t.c.*

2. T. Tao obtained a very deep result on expander polynomials ("expalining" the reason that a function $F(x,y)$ *is not an expander, and giving bounds for the measure of expanding on certain range)*

Covering polynomials

Covering polynomials

Definition

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

Covering polynomials

Definition

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

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

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

Covering polynomials

Definition

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

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

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

Many other problems can be performed as a covering question :

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

Many other problems can be performed as a covering question :

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

Covering polynomials

Definition

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

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

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

Many other problems can be performed as a covering question :

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

For $k \leq 8$ by Glibichuk Konyagin :

Covering polynomials

Definition

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

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

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

Many other problems can be performed as a covering question :

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

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

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

Covering polynomials

Definition

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

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

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

Many other problems can be performed as a covering question :

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

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

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

provided $|A||B| > p$.

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

Many other problems can be performed as a covering question :

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

For $k \leq 8$ by Glibichuk Konyagin : 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)

Covering polynomials

Definition

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

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

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

Many other problems can be performed as a covering question :

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

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

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

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

Further central notion at Heisenberg groups (see later)

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

Many other problems can be performed as a covering question :

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

For $k \leq 8$ by Glibichuk Konyagin : 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)

Further central notion at Heisenberg groups (see later)

Covering polynomials ; two examples

Covering polynomials ; two examples

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

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and $K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p, s, r, t are non-constant polynomials).

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and $K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p, s, r, t are non-constant polynomials).

Theorem (H.-Hennecart)

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and $K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p, s, r, t are non-constant polynomials).

Theorem (H.-Hennecart)

There exist real numbers $0 < \delta, \delta' < 1$ s.t.

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and $K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p, s, r, t are non-constant polynomials).

Theorem (H.-Hennecart)

There exist real numbers $0 < \delta, \delta' < 1$ *s.t. for any* p

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and $K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p, s, r, t are non-constant polynomials).

Theorem (H.-Hennecart)

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

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and
$K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p,s,r,t are non-constant polynomials).

Theorem (H.-Hennecart)

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

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and $K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p, s, r, t are non-constant polynomials).

Theorem (H.-Hennecart)

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

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

Covering polynomials ; two examples

Let $F_{p,v}(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $v \in \{0,1\}$ is fixed,
$G_u(x,y) = x^{1+u}y + x^{2-u}h(y)$ where $u \in \{0,1\}$, $h(y) \in \mathbb{Z}[y]$ is a non constant polynomial.
Write $H_{p,v}(x,y,z,w) := F_{p,v}(x,y) + p(z) + t(w)$ and $K_u(x,y,z,w) := G_u(x,y) + s(z) + r(w)$ (p, s, r, t are non-constant polynomials).

Theorem (H.-Hennecart)

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

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

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

Covering polynomials ; two examples

Covering polynomials ; two examples

Remark

Covering polynomials ; two examples

Remark

Note that for $S(x, y, z, w) := x + y + zw$,

Covering polynomials ; two examples

Remark

Note that for $S(x, y, z, w) := x + y + zw$, $S(A, B, C, D) = \mathbb{F}_p$ *provided*

Covering polynomials ; two examples

Remark

Note that for $S(x, y, z, w) := x + y + zw$, $S(A, B, C, D) = \mathbb{F}_p$ *provided* $|A||B||C||D| > p^3$ *and this bound is sharp.*

Covering polynomials ; two examples

Remark

Note that for $S(x, y, z, w) := x + y + zw$, $S(A, B, C, D) = \mathbb{F}_p$ *provided* $|A||B||C||D| > p^3$ *and this bound is sharp.*
In our functions H *and* K *we can achieve* $|A||B||C||D| > p^{3-\Delta}$.

Product sets in Heisenberg groups

Product sets in Heisenberg groups

Related to Freiman model in non-abelian groups pops up so called *Heisenberg group*

Related to Freiman model in non-abelian groups pops up so called *Heisenberg group*

$$[\underline{x}, \underline{y}, z] = \begin{pmatrix} 1 & \underline{x} & z \\ 0 & I_n & {}^t\underline{y} \\ 0 & 0 & 1 \end{pmatrix},$$

Related to Freiman model in non-abelian groups pops up so called *Heisenberg group*

$$[\underline{x}, \underline{y}, z] = \begin{pmatrix} 1 & \underline{x} & z \\ 0 & I_n & {}^t\underline{y} \\ 0 & 0 & 1 \end{pmatrix},$$

where $\underline{x} = (x_1, x_2, \ldots, x_n)$, $\underline{y} = (y_1, y_2, \ldots, y_n)$, $x_i, y_i, z \in \mathbb{F}$, $i = 1, 2, \ldots, n$, and I_n is the $n \times n$ identity matrix.

Product sets in Heisenberg groups

Related to Freiman model in non-abelian groups pops up so called *Heisenberg group*

$$[\underline{x}, \underline{y}, z] = \begin{pmatrix} 1 & \underline{x} & z \\ 0 & I_n & {}^t\underline{y} \\ 0 & 0 & 1 \end{pmatrix},$$

where $\underline{x} = (x_1, x_2, \ldots, x_n)$, $\underline{y} = (y_1, y_2, \ldots, y_n)$, $x_i, y_i, z \in \mathbb{F}$, $i = 1, 2, \ldots, n$, and I_n is the $n \times n$ identity matrix.
and operations

$$[\underline{x}, \underline{y}, z][\underline{x}', \underline{y}', z'] = [\underline{x} + \underline{x}', \underline{y} + \underline{y}', \langle \underline{x}, \underline{y}' \rangle + z + z'],$$

Product sets in Heisenberg groups

Related to Freiman model in non-abelian groups pops up so called *Heisenberg group*

$$[\underline{x}, \underline{y}, z] = \begin{pmatrix} 1 & \underline{x} & z \\ 0 & I_n & {}^t\underline{y} \\ 0 & 0 & 1 \end{pmatrix},$$

where $\underline{x} = (x_1, x_2, \ldots, x_n)$, $\underline{y} = (y_1, y_2, \ldots, y_n)$, $x_i, y_i, z \in \mathbb{F}$, $i = 1, 2, \ldots, n$, and I_n is the $n \times n$ identity matrix.
and operations

$$[\underline{x}, \underline{y}, z][\underline{x}', \underline{y}', z'] = [\underline{x} + \underline{x}', \underline{y} + \underline{y}', \langle \underline{x}, \underline{y}' \rangle + z + z'],$$

where $\langle \cdot, \cdot \rangle$ is the inner product

Product sets in Heisenberg groups

The third coordinate

The third coordinate

$$\langle \underline{x}, \underline{y'} \rangle + z + z'$$

Product sets in Heisenberg groups

The third coordinate

$$\langle \underline{x}, \underline{y'} \rangle + z + z'$$

is a kind of "sum-product function"

The third coordinate

$$\langle \underline{x}, \underline{y'} \rangle + z + z'$$

is a kind of "sum-product function"

Definition

Product sets in Heisenberg groups

The third coordinate

$$\langle \underline{x}, \underline{y'} \rangle + z + z'$$

is a kind of "sum-product function"

Definition

A subset B of H_n is said to be a cube if

The third coordinate

$$\langle \underline{x}, \underline{y}' \rangle + z + z'$$

is a kind of "sum-product function"

Definition

A subset B of H_n is said to be a cube if

$$B = [\underline{X}, \underline{Y}, Z] := \{[\underline{x}, \underline{y}, z] \text{ such that } \underline{x} \in \underline{X},\ \underline{y} \in \underline{Y},\ z \in Z\}$$

Product sets in Heisenberg groups

The third coordinate

$$\langle \underline{x}, \underline{y'} \rangle + z + z'$$

is a kind of "sum-product function"

Definition

A subset B of H_n is said to be a cube if

$$B = [\underline{X}, \underline{Y}, Z] := \{[\underline{x}, \underline{y}, z] \text{ such that } \underline{x} \in \underline{X},\ \underline{y} \in \underline{Y},\ z \in Z\}$$

where $\underline{X} = X_1 \times \cdots \times X_n$

Product sets in Heisenberg groups

The third coordinate

$$\langle \underline{x}, \underline{y'} \rangle + z + z'$$

is a kind of "sum-product function"

Definition

A subset B of H_n is said to be a cube if

$$B = [\underline{X}, \underline{Y}, Z] := \{[\underline{x}, \underline{y}, z] \text{ such that } \underline{x} \in \underline{X},\ \ \underline{y} \in \underline{Y},\ \ z \in Z\}$$

where $\underline{X} = X_1 \times \cdots \times X_n$ and $\underline{Y} = Y_1 \times \cdots \times Y_n$ with non empty-subsets $X_i, Y_i \subset \mathbb{F}^*$.

Product sets in Heisenberg groups

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$*, there exists a positive integer* n_0

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, *there exists a positive integer* n_0 *such that if* $n \geq n_0$, $B \subseteq H_n$ *is a cube and*

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n,

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n,

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n, such that $B \cdot B$ contains a union of at least $|B|/p$ many cosets of G.

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n, such that $B \cdot B$ contains a union of at least $|B|/p$ many cosets of G.

Proposition

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n, such that $B \cdot B$ contains a union of at least $|B|/p$ many cosets of G.

Proposition

Let $n, m \in \mathbb{N}$,

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n, such that $B \cdot B$ contains a union of at least $|B|/p$ many cosets of G.

Proposition

Let $n, m \in \mathbb{N}$, $X_1, X_2, \ldots, X_n$, Y_1, $Y_2, \ldots Y_n \subseteq \mathbb{F}^* = \mathbb{F} \setminus \{0\}$, $Z \subseteq \mathbb{F}$.

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n, such that $B \cdot B$ contains a union of at least $|B|/p$ many cosets of G.

Proposition

Let $n, m \in \mathbb{N}$, $X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots Y_n \subseteq \mathbb{F}^* = \mathbb{F} \setminus \{0\}$, $Z \subseteq \mathbb{F}$. We have

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a cube and $|B| > |H_n|^{3/4+\varepsilon}$ then there exists a non trivial subgroup G of H_n, such that $B \cdot B$ contains a union of at least $|B|/p$ many cosets of G.

Proposition

Let $n, m \in \mathbb{N}$, $X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots Y_n \subseteq \mathbb{F}^* = \mathbb{F} \setminus \{0\}$, $Z \subseteq \mathbb{F}$. We have

$$mZ + \sum_{j=1}^{n} X_j \cdot Y_j := \left\{ z_1 + \cdots + z_m + \sum_{j=1}^{n} x_j y_j,\ z_i \in Z,\ x_j \in X_j,\ y_j \in Y_j \right\} = \mathbb{F},$$

Product sets in Heisenberg groups

Theorem (H.-Hennecart)

For every $\varepsilon > 0$, *there exists a positive integer* n_0 *such that if* $n \geq n_0$, $B \subseteq H_n$ *is a cube and* $|B| > |H_n|^{3/4+\varepsilon}$ *then there exists a non trivial subgroup* G *of* H_n, *such that* $B \cdot B$ *contains a union of at least* $|B|/p$ *many cosets of* G.

Proposition

Let $n, m \in \mathbb{N}$, $X_1, X_2, \dots, X_n, Y_1, Y_2, \dots Y_n \subseteq \mathbb{F}^* = \mathbb{F} \setminus \{0\}$, $Z \subseteq \mathbb{F}$. *We have*

$$mZ + \sum_{j=1}^{n} X_j \cdot Y_j := \left\{ z_1 + \cdots + z_m + \sum_{j=1}^{n} x_j y_j,\ z_i \in Z,\ x_j \in X_j,\ y_j \in Y_j \right\} = \mathbb{F},$$

provided $|Z|^2 \prod_{i=1}^{n} |X_i|^n \prod_{i=1}^{n} |Y_i|^n > p^{n(n+1)+2}$.

Two other results

Two other results

Definition

Two other results

Definition

A set A is said to be semi-cube of H

Two other results

Definition

A set A is said to be semi-cube of H if

$$A = \{[x, y, z] \text{ such that } (x, y) \in U, \ z \in Z\}.$$

Two other results

Definition

A set A is said to be semi-cube of H if

$$A = \{[x,y,z] \text{ such that } (x,y) \in U,\ z \in Z\}.$$

Theorem (H.-Hennecart)

Let $A = U \rtimes Z$ be a semi-cube in H. If $|A| \geq 2^{-1/3}p^{8/3}$ then the four-fold product set $A \cdot A \cdot A \cdot A$ contains at least $|U|\left(1 - \frac{p^4}{\sqrt{2}|A|^{3/2}}\right)$ cosets of the type $[x, y, \mathbb{F}]$.

Two other results

Definition

A set A is said to be semi-cube of H if

$$A = \{[x, y, z] \text{ such that } (x, y) \in U,\ z \in Z\}.$$

Theorem (H.-Hennecart)

Let $A = U \rtimes Z$ be a semi-cube in H. If $|A| \geq 2^{-1/3}p^{8/3}$ then the four-fold product set $A \cdot A \cdot A \cdot A$ contains at least $|U|\left(1 - \frac{p^4}{\sqrt{2}|A|^{3/2}}\right)$ cosets of the type $[x, y, \mathbb{F}]$.

We considered the question of counting the subsets X of H such that $X = [A, B, C]^2$ is a square of a 3-cubes.

Two other results

Definition

A set A is said to be semi-cube of H if

$$A = \{[x, y, z] \text{ such that } (x, y) \in U,\ z \in Z\}.$$

Theorem (H.-Hennecart)

Let $A = U \rtimes Z$ be a semi-cube in H. If $|A| \geq 2^{-1/3} p^{8/3}$ then the four-fold product set $A \cdot A \cdot A \cdot A$ contains at least $|U| \left(1 - \frac{p^4}{\sqrt{2}|A|^{3/2}}\right)$ cosets of the type $[x, y, \mathbb{F}]$.

We considered the question of counting the subsets X of H such that $X = [A, B, C]^2$ is a square of a 3-cubes.

Two other results

Two other results

Theorem (H.-Hennecart)

The number of subsets $X \subset H$ *satisfying* $X = [A, B, C]^2$ *with* $A, B, C \subset \mathbf{F}_p$

Two other results

Theorem (H.-Hennecart)

The number of subsets $X \subset H$ satisfying $X = [A, B, C]^2$ with $A, B, C \subset \mathbf{F}_p$ is a $O(2^{2p+p^{3/4}})$.

Two other results

Theorem (H.-Hennecart)

The number of subsets $X \subset H$ satisfying $X = [A, B, C]^2$ with $A, B, C \subset \mathbf{F}_p$ is a $O(2^{2p+p^{3/4}})$.

Since the total number of arbitrary 3-cubes is $\mathcal{K} := 2^{3p}$, the above upper bound is a $O\left(\mathcal{K}^{2/3+o(1)}\right)$.

Hilbert cubes

Hilbert cubes

In 1892 Hilbert defined an affine d-dimensional cube

Hilbert cubes

In 1892 Hilbert defined an affine *d*-dimensional cube

$H(x_0, a_1, a_2, \ldots, a_d) = \left\{ x_0 + \sum_{1 \le i \le d} \varepsilon_i a_i \right\} \quad \varepsilon_i \in \{0, 1\}.$

Hilbert cubes

In 1892 Hilbert defined an affine d-dimensional cube

$$H(x_0, a_1, a_2, \dots, a_d) = \left\{x_0 + \sum_{1\le i\le d} \varepsilon_i a_i\right\} \quad \varepsilon_i \in \{0, 1\}.$$

or d-dimensional cube of order $r \ge 1$

$$H_r(x_0, a_1, a_2, \dots, a_d) = \left\{x_0 + \sum_{1\le i\le d} \varepsilon_i a_i\right\} \quad \varepsilon_i \in \{0, 1, \dots, r\}.$$

Hilbert cubes

In 1892 Hilbert defined an affine d-dimensional cube

$$H(x_0, a_1, a_2, \dots, a_d) = \left\{x_0 + \sum_{1\le i\le d} \varepsilon_i a_i\right\} \quad \varepsilon_i \in \{0,1\}.$$

or d-dimensional cube of order $r \ge 1$

$$H_r(x_0, a_1, a_2, \dots, a_d) = \left\{x_0 + \sum_{1\le i\le d} \varepsilon_i a_i\right\} \quad \varepsilon_i \in \{0,1,\dots,r\}.$$

Hilbert cubes play an important role in the proof of Szemerédi's celebrated theorem, and many authors investigated in different context

Hilbert cubes

In 1892 Hilbert defined an affine d-dimensional cube

$$H(x_0, a_1, a_2, \ldots, a_d) = \left\{x_0 + \sum_{1 \le i \le d} \varepsilon_i a_i\right\} \quad \varepsilon_i \in \{0, 1\}.$$

or d-dimensional cube of order $r \ge 1$

$$H_r(x_0, a_1, a_2, \ldots, a_d) = \left\{x_0 + \sum_{1 \le i \le d} \varepsilon_i a_i\right\} \quad \varepsilon_i \in \{0, 1, \ldots, r\}.$$

Hilbert cubes play an important role in the proof of Szemerédi's celebrated theorem, and many authors investigated in different context (Elsholtz, Dietmann and C. Elsholtz, Conlon-Fox-Sudakov e.t.c.)

Character Sums on Hilbert Cubes

An observation of Montgomery :

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$

Character Sums on Hilbert Cubes

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p, \ B > 0$.

Character Sums on Hilbert Cubes

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p,\ B > 0$. Let $A(x)$ be its characteristic function, An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p, \;\; B > 0$. Let $A(x)$ be its characteristic function,

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases},$$

Character Sums on Hilbert Cubes

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p, \ B > 0$. Let $A(x)$ be its characteristic function,

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases},$$

then for some $c = c(B)$, $\max_{r \neq 0} |\widehat{A}(r)| \geq c|A|$.

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p, \;\; B > 0$. Let $A(x)$ be its characteristic function,

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases},$$

then for some $c = c(B)$, $\max_{r \neq 0} |\widehat{A}(r)| \geq c|A|$. As a contrast

Character Sums on Hilbert Cubes

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p, \ B > 0$. Let $A(x)$ be its characteristic function,

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases},$$

then for some $c = c(B)$, $\max_{r \neq 0} |\widehat{A}(r)| \geq c|A|$. As a contrast Ajtai, Iwaniec, Komlós, Pintz, and E. Szemerédi construct a set $T \subseteq \mathbb{Z}_m$

Character Sums on Hilbert Cubes

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p, \ B > 0$. Let $A(x)$ be its characteristic function,

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases},$$

then for some $c = c(B)$, $\max_{r \neq 0} |\widehat{A}(r)| \geq c|A|$. As a contrast Ajtai, Iwaniec, Komlós, Pintz, and E. Szemerédi construct a set $T \subseteq \mathbb{Z}_m$ for which

$$|T| = O(\log m (\log^* m)^{c' \log^* m}) \ c' > 0,$$

Character Sums on Hilbert Cubes

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p, \; B > 0$. Let $A(x)$ be its characteristic function,

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases},$$

then for some $c = c(B)$, $\max_{r \neq 0} |\widehat{A}(r)| \geq c|A|$. As a contrast Ajtai, Iwaniec, Komlós, Pintz, and E. Szemerédi construct a set $T \subseteq \mathbb{Z}_m$ for which

$$|T| = O(\log m (\log^* m)^{c' \log^* m}) \; c' > 0,$$

and $\max_{r \neq 0} |\widetilde{T}(r)| \leq O(|T| / \log^* m)$

An observation of Montgomery : Let $U \subseteq \mathbb{F}_p$ $A \subseteq U$ for which $|A| < B \log p,\ B > 0$. Let $A(x)$ be its characteristic function,

$$A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases},$$

then for some $c = c(B)$, $\max_{r \neq 0} |\widehat{A}(r)| \geq c|A|$. As a contrast Ajtai, Iwaniec, Komlós, Pintz, and E. Szemerédi construct a set $T \subseteq \mathbb{Z}_m$ for which

$$|T| = O(\log m (\log^* m)^{c' \log^* m})\ c' > 0,$$

and $\max_{r \neq 0} |\widetilde{T}(r)| \leq O(|T|/\log^* m)$
(where $\log^* m$ is the multi-iterated logarithm) hold.

Character Sums on Hilbert Cubes

Character Sums on Hilbert Cubes

A related result on Hilbert cubes :

Character Sums on Hilbert Cubes

A related result on Hilbert cubes :

Theorem (H.)

Let $H(x_0, a_1 < a_2 < \cdots < a_d)$ be an arbitrary non-degenerate Hilbert cube. For every $\xi \in \mathbb{F}_p^*$ there is a subset $H' \subseteq H$ with $|H'| \gg e^{c\sqrt{\log |H|}}$, such that

$$|\widehat{H'}(\xi)| \gg |H'|.$$

(H is non-degenerate, if $|H(x_0, a_1 < a_2 < \cdots < a_d)| = 2^d$)

Character Sums on Hilbert Cubes

A related result on Hilbert cubes :

Theorem (H.)

Let $H(x_0, a_1 < a_2 < \cdots < a_d)$ be an arbitrary non-degenerate Hilbert cube. For every $\xi \in \mathbb{F}_p^*$ there is a subset $H' \subseteq H$ with $|H'| \gg e^{c\sqrt{\log |H|}}$, such that

$$|\widehat{H'}(\xi)| \gg |H'|.$$

(H is non-degenerate, if $|H(x_0, a_1 < a_2 < \cdots < a_d)| = 2^d$)

For the proofs we need some bound on energy of H ;

Let $A \subseteq \mathbb{F}_p$. Its *additive* energy is defined by

$$E_+(A) := \{(a_1, a_2, a_3, a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\}$$

Character Sums on Hilbert Cubes

A related result on Hilbert cubes :

Theorem (H.)

Let $H(x_0, a_1 < a_2 < \cdots < a_d)$ be an arbitrary non-degenerate Hilbert cube. For every $\xi \in \mathbb{F}_p^*$ there is a subset $H' \subseteq H$ with $|H'| \gg e^{c\sqrt{\log |H|}}$, such that

$$|\widehat{H'}(\xi)| \gg |H'|.$$

(H is non-degenerate, if $|H(x_0, a_1 < a_2 < \cdots < a_d)| = 2^d$)

For the proofs we need some bound on energy of H ;

Let $A \subseteq \mathbb{F}_p$. Its *additive* energy is defined by

$$E_+(A) := \{(a_1, a_2, a_3, a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\}$$

and its *multiplicative* energy is defined by

$$E_\times(A) := \{(a_1, a_2, a_3, a_4) \in A^4 : a_1 \cdot a_2 = a_3 \cdot a_4\}.$$

Character Sums on Hilbert Cubes

A related result on Hilbert cubes :

Theorem (H.)

Let $H(x_0, a_1 < a_2 < \cdots < a_d)$ be an arbitrary non-degenerate Hilbert cube. For every $\xi \in \mathbb{F}_p^*$ there is a subset $H' \subseteq H$ with $|H'| \gg e^{c\sqrt{\log |H|}}$, such that

$$|\widehat{H'}(\xi)| \gg |H'|.$$

(H is non-degenerate, if $|H(x_0, a_1 < a_2 < \cdots < a_d)| = 2^d$)

For the proofs we need some bound on energy of H ;

Let $A \subseteq \mathbb{F}_p$. Its *additive* energy is defined by

$$E_+(A) := \{(a_1, a_2, a_3, a_4) \in A^4 : a_1 + a_2 = a_3 + a_4\}$$

and its *multiplicative* energy is defined by

$$E_\times(A) := \{(a_1, a_2, a_3, a_4) \in A^4 : a_1 \cdot a_2 = a_3 \cdot a_4\}.$$

Character Sums on Hilbert Cubes

Character Sums on Hilbert Cubes

Theorem

Let $r > 1, \; r \in \mathbb{N}$ *and let* $H = H_r(x_0, a_1 < a_2 < \cdots < a_d)$ *be an arbitrary non-degenerate Hilbert cube.*

Character Sums on Hilbert Cubes

Theorem

Let $r > 1,\ r \in \mathbb{N}$ and let $H = H_r(x_0, a_1 < a_2 < \cdots < a_d)$ be an arbitrary non-degenerate Hilbert cube. We have

$$E_\times(H) \ll \begin{cases} |H|^{\gamma_r} p & |H| < p^{2/3} \\ \frac{|H|^{3+\gamma_r}}{p} & |H| \geq p^{2/3} \end{cases}$$

Character Sums on Hilbert Cubes

Theorem

Let $r > 1,\ r \in \mathbb{N}$ *and let* $H = H_r(x_0, a_1 < a_2 < \cdots < a_d)$ *be an arbitrary non-degenerate Hilbert cube. We have*

$$E_\times(H) \ll \begin{cases} |H|^{\gamma_r} p & |H| < p^{2/3} \\ \frac{|H|^{3+\gamma_r}}{p} & |H| \geq p^{2/3} \end{cases}$$

where $\gamma_r = \log_{r+1}(2r+1)$.

Character Sums on Hilbert Cubes

Theorem

Let $r > 1,\ r \in \mathbb{N}$ and let $H = H_r(x_0, a_1 < a_2 < \cdots < a_d)$ be an arbitrary non-degenerate Hilbert cube. We have

$$E_\times(H) \ll \begin{cases} |H|^{\gamma_r} p & |H| < p^{2/3} \\ \frac{|H|^{3+\gamma_r}}{p} & |H| \geq p^{2/3} \end{cases}$$

where $\gamma_r = \log_{r+1}(2r+1)$.

Remark

Note that the estimations above are nontrivial; for example let $|H| \asymp p^{2/3}$ r is "big",then $|H|^{\gamma_r} p$ is close to $|H|^{5/2}$, which is better than the trivial bound $|H|^3$.

Character Sums on Hilbert Cubes

Theorem

Let $r > 1,\ r \in \mathbb{N}$ and let $H = H_r(x_0, a_1 < a_2 < \cdots < a_d)$ be an arbitrary non-degenerate Hilbert cube. We have

$$E_\times(H) \ll \begin{cases} |H|^{\gamma_r} p & |H| < p^{2/3} \\ \frac{|H|^{3+\gamma_r}}{p} & |H| \geq p^{2/3} \end{cases}$$

where $\gamma_r = \log_{r+1}(2r+1)$.

Remark

Note that the estimations above are nontrivial; for example let $|H| \asymp p^{2/3}$ r is "big",then $|H|^{\gamma_r} p$ is close to $|H|^{5/2}$, which is better than the trivial bound $|H|^3$.

The proof based on a Gowers version of Balog-Szemerédi theorem