Recent progress in Hilbert cubes theory; combinatorial aspects of some ergodic theorems

Norbert Hegyvári
Eötvös University and Rényi Institute, Budapest

Séminaire CAESAR

2014

Introduction

In 1892 Hilbert defined an affine d-dimensional cube which is nowdays called Hilbert cube as follows : let $x_0, a_1 < a_2 < \cdots < a_d$ sequence of integers. Hilbert-cube is the set

$$H(x_0, a_1, a_2, \ldots, a_d) = \{x_0 + \sum_{1 \le i \le d} \{0, a_i\}\} = x_0 + \{0, a_1\} + \cdots + \{0, a_d\}.$$

Theorem (Hilbert 1892)

For every r and d, there exists (a least) number $h(d; r)$ so that for every colouring $\chi : [1; h(d; r)] \mapsto [1; r]$ there exists an affine d-dimensional monochromatic cube.

It is one of the first Ramsey-type result in the number theory.

Applications

Hilbert cubes have many applications. An important tool in the celebrated theorem of Szemerédi :

Theorem (Szemerédi, 1969)

For each d, if $S \subseteq [1; N]$ and

$$|S| \gg N^{1-1/2^d}$$

then S contains an affine $d-$dimensional Hilbert cube.

Corollary

If the lower density ($\liminf_{N\to\infty} |S \cap [1, N]|/N > 0$) of S is positive then S contains a Hilbert cube with dimension at least

$$d \gg \log\log N.$$

Applications

Remark

One can distinguish

• *non-degenerate Hilbert cube : when the vertices of H are all distinct (denote the dimension by* $\dim *$*)*

• *degenerate Hilbert cube : otherwise (denote the dimension by* $\dim$*)*

• Let $d(S,N) := \max\{k : S \cap [1,N] \quad \text{contains a k-cube}\}$

Theorem (H 1999)

There exists an infinite sequence of integers with $\underline{d}(S) > 0$ *s.t.*

$$d(S,N) \ll \sqrt{\log N \log\log N}.$$

(Here we allow degenerate cube as well)

Applications

Denote shortly $\Sigma(A) := H(0, a_1, a_2, \ldots, a_d)$.

The main ingredients of the probabilistic proof :

Lemma

$$|\{A \subseteq [1, n] : \ |A| = k; \ |\Sigma(A)| < k^3\}| < (kn)^{5\log_2 k} \cdot 4^{k^2}.$$

For the proof of the lemma we count the number of indices for which

$$\Sigma(a_1, \ldots, a_{j-1}) \cap \Sigma(a_1, \ldots, a_j) = \emptyset.$$

(a_j doubles the elements of $\Sigma(a_1, \ldots, a_{j-1})$)

Applications

Note that if their number could not be bigger than $[4\log_2 k]$, otherwise

$$|\Sigma(a_1,\dots,a_k)| \geq 2^{[4\log_2 k]} > k^3.$$

Secondly we pick an infinite random sequence choosing numbers with a fix probability $p > 0$ then bounding the probability that it contains a Hilbert-cube with dimension

$$> \sqrt{\log N \log\log N}$$

up to N.

Then we show that it can be bounded by $\ll \frac{1}{N^2}$.

Finally by Borel-Cantelli we obtain the result.

Applications

Conlon- Fox -Sudakov improved

Theorem (C-F-S 2013)

There exists an infinite sequence of integers with $\underline{d}(S) > 0$ s.t.

$$d(S,N) \ll \sqrt{\log N},$$

and this result is best possible (by another result of mine).

This proof is also probabilistic.

For thinner sets

In 2004 I investigate thinner sequence

Denote by $r_3(n)$ be the Roth function ; the maximal number of integers that can be selected from the interval $[1, n]$ without containing a non-trivial three-term arithmetic progression.

Theorem (H)

There exists a subset A of $[1, N]$ for which $|A| \geq r_3(N)/3$, and

$$\max_{H \subseteq A \cap [1,N]} dim^*(H) \leq \frac{1}{\log 2} \log \log N.$$

For thinner sets

By Szemerédi theorem, by theorem (H) above, and a result of Behrend saying $r_3(N) > \frac{N}{e^{\sqrt{\log N}}}$,

Corollary

For every $1/2 < c < 1$ *there exists a subset* A *of* $[1, N]$ *for which*

$$|A| = \frac{N}{e^{(\log N)^c}},$$

and

$$\log\log N \ll \max_{H \subseteq A \cap [1,N]} dim^*(H) \leq \frac{1}{\log 2} \log\log N.$$

Infinite Hilbert cubes in dense sets

Infinite Hilbert-cubes are defined in a natural way : if $\{a_1 < a_2 < \cdots < a_d < \dots\}$ is a sequence of integers and $H_d = H(x_0, a_1, a_2, \dots, a_d)$, then $H := \cup_d H_d$ is an infinite Hilbert-cube.

In the end of $70'$s E.G. Strauss proved the following surprising result

Theorem (E.G. Strauss)

For every $\varepsilon > 0$, there exists a sequence of integers with density $> 1 - \varepsilon$, which does not contain an infinite Hilbert cube.

on the other hand

Theorem (M. Nathanson)

Every sequence of integers with density 1 contains an infinite Hilbert cube.

Infinite Hilbert cubes in dense sets

The proof of Nathanson's result is simple "two lines" :

Let A be a sequence of integers with density 1, and $A^c = \{x_1 < x_2 < \dots\}$ its complement.
Let

$$\Delta(A^c) =: \sup\{x_{i+1} - x_i\}.$$

Clearly $\Delta(A^c) = \infty$. Now iterating ; if $H_d = H(x_0, a_1, a_2, \dots, a_d) \cap A^c = \emptyset$, then for some i, $H_d \subseteq [1, x_{i+1} - x_i + 1]$, hence with $a_{d+1} := x_i + 1$ we have

$$H_{d+1} \cap A^c = \emptyset.$$

Infinite Hilbert cubes in dense sets

Remarks :

• For a given interval $I = [a, a + m]$ if a Hilbert-cube $H(x_0, a_1 < a_2 < \cdots < a_d)$ lies in I, then $d \leq c\sqrt{m}$.

• If for some $A \subseteq [1, N]$ we would like to avoid A by a Hilbert-cube, then statistically we have a gap with size $\frac{N}{|A|}$ and by the previous remark there is a cube with $H(N) \sim \sqrt{\frac{N}{|A|}}$.

• This argument works just in a finite case and completely false in the infinite case.

However in 2008 I proved that essentially apart from a log factor a same conclusion remains true.

Theorem (H)

Let A be a sequence of integers.
For every $\varepsilon > 0$ there exists an infinite Hilbert-cube, for which

$$\limsup_{N\to\infty} \frac{H(N)}{\sqrt{N/A(N)}} \cdot \log^{1+\varepsilon} N > 0.$$

(a little bit stronger result is proved)

Additive and multiplicative Hilbert cubes

We can define a multiplicative Hilbert cube in a similar way :

$$H_d^{\times}(a_1 < a_2 < \cdots < a_d) = \{ \prod_{1 \le i \le d} \{1, a_i\}\} = \{1, a_1\} \cdots \{1, a_d\} =$$

$$= \{a_1, \ldots, a_d, a_1 a_2, \ldots, a_1 \cdot a_2 \cdot \cdots \cdot a_d\}.$$

and for an infinite one ; $\{a_1 < a_2 < \cdots < a_d < \ldots\}$ is a sequence of integers, then

$$H^{\times} = \bigcup_d H_d^{\times}(a_1 < a_2 < \cdots < a_d).$$

Additive and multiplicative Hilbert cubes ; IP sets

IP-sets are generalization of this notion :

The subset F of integers is said to be IP-set if it contains all finite products of the form

$$\prod_i f_i^{\alpha_i} \ (\alpha_i \in \mathbb{N}) \quad f_i \neq f_j \quad \text{if and only if} \quad i \neq j.$$

Denote this set by $FPow(F)$.

Additive and multiplicative Hilbert cubes ; IP sets

Theorem (Bergelson-Ruzsa 2002)

The sequence of squarefree numbers contains an infinite (additive) Hilbert-cube

Corollary

There is an infinite Hilbert-cube which avoids the sequence $Q\{= n^2 : \ n \in \mathbb{N}\}$

Additive and multiplicative Hilbert cubes ; IP sets

Theorem (H)

Let $P' = \{p_1 < p_2 < \ldots\}$ *be an infinite sequence of primes for which* $\lim_{n\to\infty} \frac{p_n}{n^\beta} = 1$, $(\beta > 1)$. *Then for all infinite Hilbert-cube which avoids* $FPow(P')$, *we have*

$$H(N) < c(\beta)\Big(\frac{\log N}{\log\log N}\Big)^{\frac{3\beta+2}{2}}.$$

Say that a subsequence $P^* = \{p_1 < p_2 < \ldots\}$ of primes is $\lambda-$lacunary, if for every n

$$\frac{p_{n+1}}{p_n} > \lambda > 1.$$

Hilbert cubes in sets of primes and squares

Theorem (H)

Let P^* be a $\lambda-$lacunary subsequence of primes. There exists an infinite (additive) Hilbert-cube H, for which $H \cap FPow(P^*) = \emptyset$, and

$$\limsup_{N\to\infty} \frac{H(N)\cdot e^{c\sqrt{\log N}}}{\sqrt{N}} > 0,$$

where $c > \pi\sqrt{\frac{2}{3\log\lambda}}$.

Hilbert cubes in sets of primes and squares

Squares :

Let $S = \{1^2, 2^2, \ldots, n^2, \ldots\}$.

Brown, Erdős and Freedman asked : Does S contain arbitrarily large Hilbert cubes ? With Sárközy we proved

Theorem (H-Sárközy)

$$d(S, N) = O(\log N^{1/3}).$$

Hilbert cubes in sets of primes and squares

Key steps of the proof :

- We take the modular version.

By exponential sums we conclude that for large primes p

Lemma

$$d'(S,p) = O(p^{1/4}),$$

where $d'(S,p)$ is the largest dimension of a Hilbert cube lies entirely in the sets of quadratic residues.

(Note that a better estimation type $d'(S,p) = O(p^{\varepsilon})$ for small $\varepsilon > 0$ would give a better estimation for the least quadratic non residues than Burgess' one)

- We use Gallagher "Larger sieve", and we argue that a Hilbert-cube of integers itself could not be "large" (larger than $O(\log N^{1/3})$.)

This result is improved in papers of Dietmann and Elsholtz (quoted the last two) :

Theorem (Dietmann and Elsholtz)

$$d(S,N) = O((\log\log N)^2)$$

$$d(S,N) = O(\log\log N)$$

Hilbert cubes in sets of primes and squares

Primes :

For primes we proved

Theorem (H-Sárközy)

$$d(P, N) = O(\log N).$$

It is also improved independently by Wood and Dietmann-Elsholtz

Theorem (W ; D-E)

$$d(P, N) = O\left(\frac{\log N}{\log\log N}\right).$$

Wood concluded from it that the number of AND and OR gates testing whether a given sequence of digits of a prime number.

Hilbert cubes and related notions

Hilbert cubes ←----→ Subsets sums ←----→ Restricted summation

(Related notion is the uniformity Gowers-norm

$$\|f\|_{U_g^d}^{2^d}\mathbb{E}_{x,h_1,h_2,\dots,h_d}\prod_{\omega_1,\dots,\omega_d\in\{0,1\}} J^{\omega_1+\dots\omega_d} f(x+\omega_1 h_1+\dots\omega_d h_d),$$

where J J denotes complex conjugation. In the argument of f there is an element of a Hilbert-cube)

In some sense a Hilbert cube controls an additive structure of a set.

Some result on restricted addition

For $h \geq 1$, hA will denote the set of sums of h not necessarily distinct elements of A,

and $h \times A$, the set of sums of h pairwise distinct elements of A.

For $X \subseteq \mathbb{N}$ let

$$\Delta(X) := \limsup_{i \to +\infty} (x_{i+1} - x_i).$$

Burr and Erdős asked (with many other related questions) what is the connection between

$$\Delta(hA) \quad \longleftarrow\!\!\!-\!-\!-\!\!\!\longrightarrow \quad \Delta(h \times A)$$

Some result on restricted addition

With F. Hennecart and A. Plagne we proved in 2007 the following

Theorem (HHP)

Let $A \subseteq \mathbb{N}$. Then there exists an increasing sequence of integers $(h_j)_{j\geq 1}$ such that $\big(\Delta(h_j \times A)\big)_{j\geq 1}$ is non-increasing.

or in a quantitative form :

Theorem (HHP)

Let $A \subseteq \mathbb{N}$, and

$$h := \min\{h : \Delta(h \times A) < \infty.$$

Then there exists an increasing sequence of integers $(h_j)_{j\geq 0}$ with $h_0 = h$ such that for any $j \geq 1$, one has $h_j + 2 \leq h_{j+1} \leq h_j + h + 1$ and $\Delta(h_{j+1} \times A) \leq \Delta(h_j \times A)$.

Some result on restricted addition

At the proof of the theorem we used the so called "SUNFLOWER LEMMA" of Erdős and Rado.

We conjectured that

Conjecture

Let A be a set of positive integers, then the sequence $\big(\Delta(h \times A)\big)_{h\geq 1}$ is non-increasing.

Recently Yong-Gao Chen and Jin-Hui Fang extend this type of questions to subsets of integers.

Some ergodic result via combinatorial way

In 1985 Bergelson investigated the additive structure of difference sets.

Theorem (Bergelson)

There exists an infinite set B of integers for which

$$A - A \supseteq B + B + \cdots + B = B \cdot k,$$

provided A has positive upper density

In 2002 I observed a pure combinatorial proof.
Recently with Ruzsa we give a third proof for a little bit more general result

Some ergodic result via combinatorial way

Let $f : \mathbb{N}_+ \mapsto \mathbb{N}_+$ be any function.
Let

$$FS(C)_f := \Big\{ \sum_{c_i \in X} w(i) c_i : X \subseteq C,\ |X| < \infty;\ 1 \le w(i) \le f(i) \Big\}.$$

and

$$FP(C) := \Big\{ \prod_{c_i \in X} c_i : X \subseteq C;\ |X| < \infty \Big\}.$$

Theorem (H-Ruzsa)

Let A be a set of integers, $\overline{d}(A) > 0$. Let $f : \mathbb{N}_+ \mapsto \mathbb{N}_+$ be any function. There exists an infinite set C of integers, such that

$$A - A \supseteq FS(C)_f \cup FP(C).$$

Proof

Lemma (Følner)

Assume $A \subseteq \mathbb{N}$, with $\overline{d}(A) > 0$. Then there is a Bohr set $B(S,\varepsilon) := \{m \in \mathbb{Z} : \max_{s\in S} \|sm\| < \varepsilon\}$ for which the set

$$E := B(S,\varepsilon) \setminus (A - A)$$

has zero density.

Some properties of a Bohr-sets :

for every pair of sets S, S' and for every k, $0 < k \cdot \varepsilon' \leq \varepsilon$, we have

- $k \cdot B(S,\varepsilon') \subseteq B(S,\varepsilon)$,
- $B(S \cup S',\varepsilon) = B(S,\varepsilon) \cap B(S',\varepsilon)$.

Proof

The existence of the infinite set C inductively :

Let $K_1 := f(1)$, then there is an element c_1 from $B(S, \varepsilon/K_1)$ such that $ic_1 \notin E$, for $i = 1, 2, \dots K_1$.
Hence

$$FS(\{c_1\})_f \cup FP(\{c_1\}) = \{0, c_1, \dots, K_1 c_1\} \subseteq B \setminus E \subseteq A - A.$$

Assume the elements $c_1 < c_2 < \dots < c_n$ have been defined and

$$\mathcal{F}_n := FS(\{c_1, c_2, \dots c_n\})_f \cup FP(\{c_1, c_2, \dots c_n\}) \subseteq B \setminus E \subseteq A - A.$$

Write $FP(\{c_1, c_2, \dots c_n\}) = \{p_1 < p_2 < \dots < p_m\}$, and let $K := \max\{f(n+1), p_m\}$. Define

$$\varepsilon_1 = \frac{1}{2K} \min\{\varepsilon - \|xs\| : x \in \mathcal{F}_n; s \in S\},$$

Proof

Let $B_1 := B(S, \varepsilon_1)$.
Note that

$$B(S, \varepsilon_1) \subseteq B(S, \varepsilon).$$

Observe that for every $i \leq K;\ i \in \mathbb{N}$ and every $u \in FS_f(\{c_1, c_2, \dots c_n\})$, and $c \in B_1, s \in S$ we have $\|s(u + ic)\| < \varepsilon$, hence

$$FS_f(\{c_1, c_2, \dots c_n\}) + \{0, c, 2c, \dots K \cdot c\} \subseteq B.$$

E has zero density, so there exists a $B_1' \subseteq B_1$, $d(B_1') = d(B_1)$ and for every $c \in B_1'$,

$$FS_f(\{c_1, c_2, \dots c_n\}) + \{0, c, 2c, \dots K \cdot c\} \subseteq B \setminus E \subseteq A - A$$

also holds.

Proof

Since $K \geq p_m$ and $0 \in FS_f(\{c_1, c_2, \dots c_n\})$ we also have

$$c \cdot \{p_1 < p_2 < \cdots < p_m\} = c \cdot FP(\{c_1, c_2, \dots c_n\}) \subseteq$$

$$\subseteq \{0, c, 2c, \dots K \cdot c\} \subseteq B \setminus E \subseteq A - A.$$

Pick an arbitrary element $c_{n+1} := c \in B_1'$. For this element we obtain that

$$FS_f(\{c_1, c_2, \dots c_n, c_{n+1}\}) \subseteq$$

$$\subseteq FS_f(\{c_1, c_2, \dots c_n\}) + \{0, c, 2c, \dots K \cdot c\} \subseteq B \setminus E \subseteq A - A,$$

and

$$FP(\{c_1, c_2, \dots c_n\}) \cup c_{n+1} \cdot FP(\{c_1, c_2, \dots c_n\}) \subseteq B \setminus E \subseteq A - A$$

simultaneously holds.

Proof

Thus we have that

$$\mathcal{F}_{n+1} \subseteq B \setminus E \subseteq A - A,$$

as we want.

Character sums

Let f be an arbitrary function from $\mathbb{F}_p$ to $\mathbb{C}$. Denote the Fourier transform (respect to a multiplicative character) of it by

$$\widehat{f(u)} := \sum_{x \in \mathbb{F}_p} f(x)\chi_u(x),$$

where $\chi_u(x)$ is the multiplicative (Dirichlet) character ; $\chi_u(x) = e^{\frac{2\pi i ind x \cdot u}{p-1}}$. When $\chi \neq \chi_0$ is not the principle character, then let $\chi(0) = 0$.

Let $g : \mathbb{F}_p \to \mathbb{C}$ and $x \in \mathbb{F}_p$. Denote the Fourier transform (respect to an additive character) of it by

$$\widetilde{g}(x) := \sum_{y \in \mathbb{F}_p} g(y)e_p(yx),$$

where $e_p(t) := \exp(2i\pi t/p)$.

Character sums

An observation of H. Montgomery : if

$$A \subseteq \mathbb{F}_p, \quad |A| < B \log p, \; B > 0,$$

$A(x)$ is its characteristic function, then for some $c = c(B)$,

$$\max_{r \neq 0} |\widetilde{A}(r)| \geq c|A|.$$

We can define an $r-$Hilbert-cube extending the definition :

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

When $r = 1$ we write shortly $H(x_0, a_1, a_2, \ldots, a_d) = H_1(x_0, a_1, a_2, \ldots, a_d)$.

We say that $\dim(H) := d$ is the dimension of the Hilbert-cube and $|H(x_0, a_1, a_2, \ldots, a_d)|$ is the size of it.

Let $\Delta, 0 < \Delta \leq 1$ be a real parameter, and we say that a cube $H =: H_r(x_0, a_1, a_2, \ldots, a_d)$ is $\Delta-$degenerate, if

$$\frac{\log_{r+1} |H|}{d} = \Delta.$$

(Here $\log_{r+1} x$ means $\ln x / \ln(r+1)$.)

When $\Delta = 1$ then $|H| = (r+1)^d$, and so all sums are different and then we say that H is non-degenerate.

Character sums ; some unpublished result

I proved

Theorem (H)

Let $\Delta \in (0.1]$, $r > 1; r \in \mathbb{N}$, *and let* $H_r(x_0, a_1 < a_2 < \cdots < a_d)$ *be an arbitrary* Δ*-degenerate Hilbert cube. Assume that the size of* H

$$|H| \geq p^{\frac{2}{3}}.$$

Then

$$\max_{\chi \neq \chi_0} \left| \sum_{h \in H} \chi(h) \right| \gg \frac{\sqrt{p}}{|H|^{\gamma_r/2}},$$

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

Furthermore a related result of Montgomery :

Theorem (H)

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

$$|\widetilde{H'}(r)| \gg |H'|.$$