Additive Combinatorics methods in Fractal Geometry III

Pablo Shmerkin

Department of Mathematics and Statistics
T. Di Tella University and CONICET

Dynamics Beyond Uniform Hyperbolicity, CIRM, May 2019

Review: L^q dimensions

Definition

Given a probability μ on $\mathbb{R}^d$ and $q \in (1, \infty)$, we let

$$S_n(\mu, q) = \sum_{I \in \mathcal{D}_n} \mu(I)^q,$$

$$\dim_q(\mu) = \liminf_{n \to \infty} \frac{\log S_n(\mu, q)}{n(1-q)} \in [0, d].$$

- $q \mapsto \dim_q(\mu)$ is non-increasing and $\dim_q(\mu) \to \dim_\infty(\mu)$ as $q \to \infty$.
- The main theorem holds not only for Frostman exponents but also for L^q dimensions.
- In the proof it is crucial that $q < \infty$.

Review: L^q dimensions

Definition

Given a probability μ on $\mathbb{R}^d$ and $q \in (1, \infty)$, we let

$$S_n(\mu, q) = \sum_{I \in \mathcal{D}_n} \mu(I)^q,$$

$$\dim_q(\mu) = \liminf_{n \to \infty} \frac{\log S_n(\mu, q)}{n(1-q)} \in [0, d].$$

- $q \mapsto \dim_q(\mu)$ is non-increasing and $\dim_q(\mu) \to \dim_\infty(\mu)$ as $q \to \infty$.
- The main theorem holds not only for Frostman exponents but also for L^q dimensions.
- In the proof it is crucial that $q < \infty$.

Review: L^q dimensions

Definition

Given a probability μ on $\mathbb{R}^d$ and $q \in (1, \infty)$, we let

$$S_n(\mu, q) = \sum_{I \in \mathcal{D}_n} \mu(I)^q,$$

$$\dim_q(\mu) = \liminf_{n \to \infty} \frac{\log S_n(\mu, q)}{n(1-q)} \in [0, d].$$

- $q \mapsto \dim_q(\mu)$ is non-increasing and $\dim_q(\mu) \to \dim_\infty(\mu)$ as $q \to \infty$.
- The main theorem holds not only for Frostman exponents but also for L^q dimensions.
- In the proof it is crucial that $q < \infty$.

Review: L^q dimensions

Definition

Given a probability μ on $\mathbb{R}^d$ and $q \in (1, \infty)$, we let

$$S_n(\mu, q) = \sum_{I \in \mathcal{D}_n} \mu(I)^q,$$

$$\dim_q(\mu) = \liminf_{n \to \infty} \frac{\log S_n(\mu, q)}{n(1-q)} \in [0, d].$$

- $q \mapsto \dim_q(\mu)$ is non-increasing and $\dim_q(\mu) \to \dim_\infty(\mu)$ as $q \to \infty$.
- The main theorem holds not only for Frostman exponents but also for L^q dimensions.
- In the proof it is crucial that $q < \infty$.

Review: Main Theorem for L^q dimensions

Theorem (P.S.)

Let (G, T, λ, Δ) be a model with exponential separation on $\mathbb{R}$. We also assume that the maps $x \mapsto \Delta(x)$ and $x \mapsto \mu_x$ are continuous a.e., and that μ_x is supported on $[0,1]$. Let

$$s(q) = \min\left(\frac{\int \log \|\Delta(x)\|_q^q \, dx}{(q-1)\log\lambda}, 1 \right),$$

where $\|\Delta\|_q^q = \sum_y \Delta(y)^q$.

Then

$$\dim_q(\mu_x) = s(q)$$

for every $x \in G$ and $q > 1$.

Tools involved in the proof

1. Additive combinatorics: an inverse theorem for the L^q norm of the convolution of two finitely supported measures(Balog-Szemerédi-Gowers Theorem, Bourgain's additive part of discretized sum-product results).
2. Ergodic theory: key role played by subadditive cocycle over a uniquely ergodic transformation (cocycle borrowed from Nazarov-Peres-S. 2012, uses the proof of the subadditive ergodic theorem given by Katznelson-Weiss).
3. Multifractal analysis (L^q spectrum, regularity at points of differentiability).
4. General scheme of proof follows Mike Hochman's strategy in his landmark paper on the dimensions of self-similar measures, but there are substantial differences.

Tools involved in the proof

1. Additive combinatorics: an inverse theorem for the L^q norm of the convolution of two finitely supported measures(Balog-Szemerédi-Gowers Theorem, Bourgain's additive part of discretized sum-product results).
2. Ergodic theory: key role played by subadditive cocycle over a uniquely ergodic transformation (cocycle borrowed from Nazarov-Peres-S. 2012, uses the proof of the subadditive ergodic theorem given by Katznelson-Weiss).
3. Multifractal analysis (L^q spectrum, regularity at points of differentiability).
4. General scheme of proof follows Mike Hochman's strategy in his landmark paper on the dimensions of self-similar measures, but there are substantial differences.

Tools involved in the proof

1. Additive combinatorics: an inverse theorem for the L^q norm of the convolution of two finitely supported measures(Balog-Szemerédi-Gowers Theorem, Bourgain's additive part of discretized sum-product results).
2. Ergodic theory: key role played by subadditive cocycle over a uniquely ergodic transformation (cocycle borrowed from Nazarov-Peres-S. 2012, uses the proof of the subadditive ergodic theorem given by Katznelson-Weiss).
3. Multifractal analysis (L^q spectrum, regularity at points of differentiability).
4. General scheme of proof follows Mike Hochman's strategy in his landmark paper on the dimensions of self-similar measures, but there are substantial differences.

Tools involved in the proof

1. Additive combinatorics: an inverse theorem for the L^q norm of the convolution of two finitely supported measures(Balog-Szemerédi-Gowers Theorem, Bourgain's additive part of discretized sum-product results).
2. Ergodic theory: key role played by subadditive cocycle over a uniquely ergodic transformation (cocycle borrowed from Nazarov-Peres-S. 2012, uses the proof of the subadditive ergodic theorem given by Katznelson-Weiss).
3. Multifractal analysis (L^q spectrum, regularity at points of differentiability).
4. General scheme of proof follows Mike Hochman's strategy in his landmark paper on the dimensions of self-similar measures, but there are substantial differences.

How much smoothing does convolution ensure?

Question

Let μ, ν be measures on $\mathbb{R}, \mathbb{R}/\mathbb{Z}$, etc.

What conditions of μ and/or ν ensure that $\mu * \nu$ is substantially smoother than μ?

- Smoothness can be measured by entropy, L^q norms, etc.
- We think in the case in which either the measures are discrete, or are discretizations of arbitrary measures at a finite resolution. So the problem is combinatorial in nature.

How much smoothing does convolution ensure?

Question

Let μ, ν be measures on $\mathbb{R}, \mathbb{R}/\mathbb{Z}$, etc.

What conditions of μ and/or ν ensure that $\mu * \nu$ is substantially smoother than μ?

- Smoothness can be measured by entropy, L^q norms, etc.
- We think in the case in which either the measures are discrete, or are discretizations of arbitrary measures at a finite resolution. So the problem is combinatorial in nature.

How much smoothing does convolution ensure?

Question

Let μ, ν be measures on $\mathbb{R}, \mathbb{R}/\mathbb{Z}$, etc.

What conditions of μ and/or ν ensure that $\mu * \nu$ is substantially smoother than μ?

- Smoothness can be measured by entropy, L^q norms, etc.
- We think in the case in which either the measures are discrete, or are discretizations of arbitrary measures at a finite resolution. So the problem is combinatorial in nature.

Size of sumsets and additive structure

- For any subset A of a group G,

$$|A| \leq |A+A| \leq \min\left(\frac{1}{2}|A|(|A|+1), |G|\right).$$

  So, to first order, $|A+A|$ varies between $|A|$ and $|A|^2$ (or $|G|$ if $|G| \leq |A|^2$).

- We think of sets A with $|A+A| \sim |A|$ as sets with additive structure or as approximate subgroups.

Size of sumsets and additive structure

- For any subset A of a group G,
$$|A| \le |A+A| \le \min\left(\frac{1}{2}|A|(|A|+1), |G|\right).$$
So, to first order, $|A+A|$ varies between $|A|$ and $|A|^2$ (or $|G|$ if $|G| \le |A|^2$).
- We think of sets A with $|A+A| \sim |A|$ as sets with additive structure or as approximate subgroups.

Examples of sets with/without additive structure

Examples of sets for which $|A+A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \lesssim 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \leq k_i < n_i\}.$$

- Dense subsets of a set with $|A+A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A+A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Examples of sets with/without additive structure

Examples of sets for which $|A+A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \lesssim 2|A|$.
- Proper GAPs: $|A+A| \le 2^d|A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \le k_i < n_i\}.$$

- Dense subsets of a set with $|A+A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A+A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Examples of sets with/without additive structure

Examples of sets for which $|A+A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \lesssim 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \leq k_i < n_i\}.$$

- Dense subsets of a set with $|A+A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A+A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Examples of sets with/without additive structure

Examples of sets for which $|A+A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \lesssim 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \leq k_i < n_i\}.$$

- Dense subsets of a set with $|A+A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A+A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Examples of sets with/without additive structure

Examples of sets for which $|A + A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A + A| \lesssim 2|A|$.
- Proper GAPs: $|A + A| \leq 2^d |A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \leq k_i < n_i\}.$$

- Dense subsets of a set with $|A + A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A + A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Examples of sets with/without additive structure

Examples of sets for which $|A+A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \lesssim 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \leq k_i < n_i\}.$$

- Dense subsets of a set with $|A+A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A+A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Examples of sets with/without additive structure

Examples of sets for which $|A+A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \lesssim 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \leq k_i < n_i\}.$$

- Dense subsets of a set with $|A+A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A+A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Examples of sets with/without additive structure

Examples of sets for which $|A+A| \sim |A|$:

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \lesssim 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. A GAP of rank d is a set of the form

$$\{a + k_1 v_1 + \cdots + k_d v_d : 0 \leq k_i < n_i\}.$$

- Dense subsets of a set with $|A+A| \sim |A|$ (such as a GAP).

Examples of sets for which $|A+A| \sim |A|^2$:

- Random sets (pick each element of $\mathbb{Z}/p\mathbb{Z}$ with probability $p^{-\alpha}$).
- Lacunary sets (powers of 2).
- $A \cup B$ where A, B are disjoint of the same size, A is one of the previous examples and B is arbitrary.

Freiman's Theorem

Theorem (Freiman 1966)

Given $K > 1$ there are $d(K)$ and $S(K)$ such that the following holds.

Suppose $|A + A| \leq K|A|$. Then there is a GAP *P of rank $d(K)$ such that $A \subset P$ and $|P| \leq S(K)|A|$.*

In other words, sets of small doubling are always dense subsets of GAP*s of small rank.*

Remarks on Freiman's Theorem

- Freiman's Theorem can be seen as an inverse or classification theorem: based on qualitative information about A, it returns structural information.
- In applications it is important to have quantitative estimates on $d(K)$ and $S(K)$. Good bounds were obtained by Ruzsa, Chang, Sanders and Schoen, with Schoen's current record being: $d(K) \leq K^{1+\varepsilon}$, $S(K) \leq \exp(K^{1+\varepsilon})$.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with worse quantitative bounds).
- The conjecture is that d and S can be both taken polynomial in K.
- At least with the current bounds, Freiman's Theorem says nothing if K grows with $|A|$, in particular if $K = |A|^{\delta}$. We will later see a result of Bourgain that gives structural information about A when $|A + A| \leq |A|^{1+\delta}$.

Remarks on Freiman's Theorem

- Freiman's Theorem can be seen as an inverse or classification theorem: based on qualitative information about A, it returns structural information.
- In applications it is important to have quantitative estimates on $d(K)$ and $S(K)$. Good bounds were obtained by Ruzsa, Chang, Sanders and Schoen, with Schoen's current record being: $d(K) \leq K^{1+\varepsilon}$, $S(K) \leq \exp(K^{1+\varepsilon})$.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with worse quantitative bounds).
- The conjecture is that d and S can be both taken polynomial in K.
- At least with the current bounds, Freiman's Theorem says nothing if K grows with $|A|$, in particular if $K = |A|^{\delta}$. We will later see a result of Bourgain that gives structural information about A when $|A + A| \leq |A|^{1+\delta}$.

Remarks on Freiman's Theorem

- Freiman's Theorem can be seen as an inverse or classification theorem: based on qualitative information about A, it returns structural information.
- In applications it is important to have quantitative estimates on $d(K)$ and $S(K)$. Good bounds were obtained by Ruzsa, Chang, Sanders and Schoen, with Schoen's current record being: $d(K) \leq K^{1+\varepsilon}$, $S(K) \leq \exp(K^{1+\varepsilon})$.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with worse quantitative bounds).
- The conjecture is that d and S can be both taken polynomial in K.
- At least with the current bounds, Freiman's Theorem says nothing if K grows with $|A|$, in particular if $K = |A|^{\delta}$. We will later see a result of Bourgain that gives structural information about A when $|A + A| \leq |A|^{1+\delta}$.

Remarks on Freiman's Theorem

- Freiman's Theorem can be seen as an inverse or classification theorem: based on qualitative information about A, it returns structural information.
- In applications it is important to have quantitative estimates on $d(K)$ and $S(K)$. Good bounds were obtained by Ruzsa, Chang, Sanders and Schoen, with Schoen's current record being: $d(K) \leq K^{1+\varepsilon}$, $S(K) \leq \exp(K^{1+\varepsilon})$.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with worse quantitative bounds).
- The conjecture is that d and S can be both taken polynomial in K.
- At least with the current bounds, Freiman's Theorem says nothing if K grows with $|A|$, in particular if $K = |A|^{\delta}$. We will later see a result of Bourgain that gives structural information about A when $|A + A| \leq |A|^{1+\delta}$.

Remarks on Freiman's Theorem

- Freiman's Theorem can be seen as an inverse or classification theorem: based on qualitative information about A, it returns structural information.
- In applications it is important to have quantitative estimates on $d(K)$ and $S(K)$. Good bounds were obtained by Ruzsa, Chang, Sanders and Schoen, with Schoen's current record being: $d(K) \leq K^{1+\varepsilon}$, $S(K) \leq \exp(K^{1+\varepsilon})$.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with worse quantitative bounds).
- The conjecture is that d and S can be both taken polynomial in K.
- At least with the current bounds, Freiman's Theorem says nothing if K grows with $|A|$, in particular if $K = |A|^\delta$. We will later see a result of Bourgain that gives structural information about A when $|A + A| \leq |A|^{1+\delta}$.

Additive energy

Definition

The additive energy $E(A, B)$ between two sets A, B is

$$E(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 : x_1 + y_1 = x_2 + y_2|$$

- Trivial lower bound: $|A||B| \leq E(A, B)$ since we always have the quadruples (x, x, y, y).
- Trivial upper bound: $E(A, B) \leq |A|^2|B|$, since once we have x_1, y_1, x_2, the value of y_2 is completely determined.
- In particular, $|A|^2 \leq E(A, A) \leq |A|^3$.

Additive energy

Definition

The additive energy $E(A, B)$ between two sets A, B is

$$E(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 : x_1 + y_1 = x_2 + y_2|$$

- Trivial lower bound: $|A||B| \leq E(A, B)$ since we always have the quadruples (x, x, y, y).
- Trivial upper bound: $E(A, B) \leq |A|^2|B|$, since once we have x_1, y_1, x_2, the value of y_2 is completely determined.
- In particular, $|A|^2 \leq E(A, A) \leq |A|^3$.

Additive energy

Definition

The additive energy $E(A, B)$ between two sets A, B is

$$E(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 : x_1 + y_1 = x_2 + y_2|$$

- Trivial lower bound: $|A||B| \leq E(A, B)$ since we always have the quadruples (x, x, y, y).
- Trivial upper bound: $E(A, B) \leq |A|^2|B|$, since once we have x_1, y_1, x_2, the value of y_2 is completely determined.
- In particular, $|A|^2 \leq E(A, A) \leq |A|^3$.

Additive energy

Definition

The additive energy $E(A, B)$ between two sets A, B is

$$E(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 : x_1 + y_1 = x_2 + y_2|$$

- Trivial lower bound: $|A||B| \leq E(A, B)$ since we always have the quadruples (x, x, y, y).
- Trivial upper bound: $E(A, B) \leq |A|^2|B|$, since once we have x_1, y_1, x_2, the value of y_2 is completely determined.
- In particular, $|A|^2 \leq E(A, A) \leq |A|^3$.

Additive energy as the L^2 norm of convolutions

Lemma

$$E(A,B) = \|\mathbf{1}_A * \mathbf{1}_B\|_2^2,$$

where $\mathbf{1}_A = \sum_{a\in A}\delta_a$ *(not a prob. measure).*

Proof.

Note that

$$\mathbf{1}_A * \mathbf{1}_B(z) = |\{(x,y)\in A\times B : x+y=z\}|,$$

so

$$E(A,B) = \sum_z |\{(x,y)\in A\times B : x+y\in Z\}|^2 = \|\mathbf{1}_A * \mathbf{1}_B\|_2^2.$$

□

Additive energy as the L^2 norm of convolutions

Lemma

$$E(A, B) = \|\mathbf{1}_A * \mathbf{1}_B\|_2^2,$$

where $\mathbf{1}_A = \sum_{a \in A} \delta_a$ *(not a prob. measure).*

Proof.

Note that

$$\mathbf{1}_A * \mathbf{1}_B(z) = |\{(x, y) \in A \times B : x + y = z\}|,$$

so

$$E(A, B) = \sum_z |\{(x, y) \in A \times B : x + y \in Z\}|^2 = \|\mathbf{1}_A * \mathbf{1}_B\|_2^2.$$

□

Additive structure through energy

We can think of sets A with $E(A, A) \sim |A|^3$ as sets with “additive structure”. Examples:

- APs and GAPs.
- Dense subsets of APs and GAPs.
- Disjoint unions $A \cup B$ where $E(A, A) \sim |A|^3$ and B is arbitrary. If B has large sumset, then so does $A + B$!

Observation

Having small sumset and having large additive energy are indications of additive structure. These notions cannot agree because both the size of the sumset and the additive energy are increasing functions of A.

Additive structure through energy

We can think of sets A with $E(A, A) \sim |A|^3$ as sets with "additive structure". Examples:

- APs and GAPs.
- Dense subsets of APs and GAPs.
- Disjoint unions $A \cup B$ where $E(A, A) \sim |A|^3$ and B is arbitrary. If B has large sumset, then so does $A + B$!

Observation

Having small sumset and having large additive energy are indications of additive structure. These notions cannot agree because both the size of the sumset and the additive energy are increasing functions of A.

Additive structure through energy

We can think of sets A with $E(A, A) \sim |A|^3$ as sets with "additive structure". Examples:

- APs and GAPs.
- Dense subsets of APs and GAPs.
- Disjoint unions $A \cup B$ where $E(A, A) \sim |A|^3$ and B is arbitrary. If B has large sumset, then so does $A + B$!

Observation

Having small sumset and having large additive energy are indications of additive structure. These notions cannot agree because both the size of the sumset and the additive energy are increasing functions of A.

Additive structure through energy

We can think of sets A with $E(A,A) \sim |A|^3$ as sets with "additive structure". Examples:

- APs and GAPs.
- Dense subsets of APs and GAPs.
- Disjoint unions $A \cup B$ where $E(A,A) \sim |A|^3$ and B is arbitrary. If B has large sumset, then so does $A + B$!

Observation

Having small sumset and having large additive energy are indications of additive structure. These notions cannot agree because both the size of the sumset and the additive energy are increasing functions of A.

Small sumsets $\Rightarrow$ large energy

Lemma

$$E(A, A) \geq \frac{|A|^4}{|A + A|}.$$

Proof.

$$|A \times A| = \sum_{z \in A+A} |\{(x, y) : x + y = z\}| = \sum_{z \in A+A} \mathbf{1}_A * \mathbf{1}_B(z).$$

Now apply Cauchy-Schwarz. □

Small sumsets $\Rightarrow$ large energy

Lemma

$$E(A,A) \geq \frac{|A|^4}{|A+A|}.$$

Proof.

$$|A \times A| = \sum_{z \in A+A} |\{(x,y) : x+y=z\}| = \sum_{z \in A+A} \mathbf{1}_A * \mathbf{1}_B(z).$$

Now apply Cauchy-Schwarz. □

Motivation

- Additive energy is very natural for doing analysis. But it is easier to understand sets of small doubling (e.g. Freiman's Theorem).
- By Young's inequality (in this context, simply the convexity of $t \mapsto t^p$),
$$\|f * g\|_p \leq \|f\|_1 \|g\|_p.$$
Since $\|\mathbf{1}_A\|_1 = |A|$ and $\|\mathbf{1}_A\|_2 = |A|^{1/2}$, sets with $E(A, A) \sim |A|^3$ are sets for which Young's inequality applied to $\|\mathbf{1}_A * \mathbf{1}_A\|_2$ is "almost" an equality.
- The examples of sets with additive energy $\sim |A|^3$ we have seen are of the form: a set with small doubling $\cup$ an arbitrary set of similar size. Are there any other examples?

Motivation

- Additive energy is very natural for doing analysis. But it is easier to understand sets of small doubling (e.g. Freiman's Theorem).
- By Young's inequality (in this context, simply the convexity of $t \mapsto t^p$),
$$\|f * g\|_p \leq \|f\|_1 \|g\|_p.$$
Since $\|\mathbf{1}_A\|_1 = |A|$ and $\|\mathbf{1}_A\|_2 = |A|^{1/2}$, sets with $E(A, A) \sim |A|^3$ are sets for which Young's inequality applied to $\|\mathbf{1}_A * \mathbf{1}_A\|_2$ is "almost" an equality.
- The examples of sets with additive energy $\sim |A|^3$ we have seen are of the form: a set with small doubling $\cup$ an arbitrary set of similar size. Are there any other examples?

Motivation

- Additive energy is very natural for doing analysis. But it is easier to understand sets of small doubling (e.g. Freiman's Theorem).
- By Young's inequality (in this context, simply the convexity of $t \mapsto t^p$),

$$\|f * g\|_p \leq \|f\|_1 \|g\|_p.$$

  Since $\|\mathbf{1}_A\|_1 = |A|$ and $\|\mathbf{1}_A\|_2 = |A|^{1/2}$, sets with $E(A, A) \sim |A|^3$ are sets for which Young's inequality applied to $\|\mathbf{1}_A * \mathbf{1}_A\|_2$ is "almost" an equality.
- The examples of sets with additive energy $\sim |A|^3$ we have seen are of the form: a set with small doubling $\cup$ an arbitrary set of similar size. Are there any other examples?

The Balog-Szemerédi-Gowers Theorem

Theorem (Balog-Szemerédi (1994), Gowers (1998), Schoen (2014))

There are constants $c, C > 0$ such that the following holds. Suppose

$$E(A, A) \geq |A|^3/K.$$

Then there exists $A' \subset A$ such that

$$|A'| \geq c|A|/K$$

and

$$|A' + A'| \leq CK^4|A'|.$$

Remarks on BSG

- The proof is an elementary count of paths on bi-partite graphs.
- Gowers (1998) obtained polynomial bounds in K in his proof of a quantitative version of Szemerédi's Theorem for progressions of length 4.
- There is a very similar statement for two different sets A, B of similar size (for example, $B = -A$), but the bounds become meaningless if one set is much larger than the other. There is an asymmetric version of BSG that gives information if $\log|A|$ and $\log|B|$ are comparable.

Remarks on BSG

- The proof is an elementary count of paths on bi-partite graphs.
- Gowers (1998) obtained polynomial bounds in K in his proof of a quantitative version of Szemerédi's Theorem for progressions of length 4.
- There is a very similar statement for two different sets A, B of similar size (for example, $B = -A$), but the bounds become meaningless if one set is much larger than the other. There is an asymmetric version of BSG that gives information if $\log|A|$ and $\log|B|$ are comparable.

Remarks on BSG

- The proof is an elementary count of paths on bi-partite graphs.
- Gowers (1998) obtained polynomial bounds in K in his proof of a quantitative version of Szemerédi's Theorem for progressions of length 4.
- There is a very similar statement for two different sets A, B of similar size (for example, $B = -A$), but the bounds become meaningless if one set is much larger than the other. There is an asymmetric version of BSG that gives information if $\log |A|$ and $\log |B|$ are comparable.

Small sumset in an exponential sense

Question

Suppose $A \subset \mathbb{Z}/2^m\mathbb{Z}$ satisfies

$$|A + A| \leq 2^{\varepsilon m}|A|$$

for ε small but independent of A. What can we say about A?

- In this regime Freiman's Theorem gives no information.
- Trivial cases are $|A| \leq 2^{\varepsilon m}$ or $|A| \geq 2^{(1-\varepsilon)m}$.

Small sumset in an exponential sense

Question

Suppose $A \subset \mathbb{Z}/2^m\mathbb{Z}$ satisfies

$$|A + A| \leq 2^{\varepsilon m}|A|$$

for ε small but independent of A. What can we say about A?

- In this regime Freiman's Theorem gives no information.
- Trivial cases are $|A| \leq 2^{\varepsilon m}$ or $|A| \geq 2^{(1-\varepsilon)m}$.

Small sumset in an exponential sense

Question

Suppose $A \subset \mathbb{Z}/2^m\mathbb{Z}$ satisfies

$$|A + A| \leq 2^{\varepsilon m}|A|$$

for ε small but independent of A. What can we say about A?

- In this regime Freiman's Theorem gives no information.
- Trivial cases are $|A| \leq 2^{\varepsilon m}$ or $|A| \geq 2^{(1-\varepsilon)m}$.

A less trivial example

Example

Fix $T \gg 1$, let $m = m'T$ and let $S \subset \{0, 1, \ldots, m'\}$.

Let A be the numbers in $[0, 1] \cap 2^{-m}\mathbb{Z}$ whose 2^T-adic expansion has a digit zero in position s for all $s \notin S$, and has no restriction on the digit for $s \in S$.

Other than the carries, $A + A$ has the same structure, so one indeed has

$$|A + A| \leq 2^{|S|}|A| \leq 2^{m/T}|A|.$$

The set A is in fact a GAP.

Multiscale decompositions

$$m = Tm', \quad T \gg 1, m' \gg T.$$

Given $A \subset 2^{-m}\mathbb{Z} \cap [0,1)$, we associate to it the 2^T-adic expansion tree $\mathcal{T}_A$: the level s vertices are the 2^{-sT}-dyadic intervals meeting A.

Definition

A is $(R_1, \ldots, R_{m'})$-regular if in $\mathcal{T}_A$ each level $(s-1)$-vertex has R_s offspring.

Bourgain's sumset theorem

Theorem (Bourgain 2010)

Given $\varepsilon > 0$ *there are* $\delta > 0$ *and* $T \in \mathbb{N}$ *such that the following holds for large enough* m'.

Let $m = m'T$. *Suppose* $A \subset [0,1] \cap 2^{-m}\mathbb{Z}$ *satisfies*

$$|A + A| \leq 2^{\varepsilon m}|A|.$$

Then A *contains a subset* A' *with* $|A'| \geq 2^{-\delta m}|A|$. *Moreover,* A' *is* $(R_1, \ldots, R_{m'})$*-regular and for each* s

either $R_s = 1$ *(no branching) or* $R_s \geq 2^{(1-\delta)m}$ *(full branching)*

A combined asymmetric version

Theorem (P.S.)

Given $\delta > 0$, $q \in (1, \infty)$ there is $\varepsilon > 0$ such that the following holds for large $m = m'T$. Suppose μ, ν are prob. measures on $\mathbb{Z}/2^m\mathbb{Z}$ such that

$$\|\mu * \nu\|_q \geq 2^{-\varepsilon m}\|\mu\|_q$$

Then there exist sets $A \subset \text{supp}\mu$, $B \subset \text{supp}\nu$ such that:

1. $\|\mu|_A\|_q \geq m^{-\delta}\|\mu|_A\|$, $\nu(B) \geq m^{-\delta}$.
2. μ, ν *are constant on* A, B *(up to a constant factor).*
3. *The set* A *is* $(R_1, \ldots, R_{m'})$*-regular and the set* B *is* $(R'_1, \ldots, R'_{m'})$*-regular.*
4. *For each* s,

$$\text{either } R_s \geq 2^{(1-\delta)T} \text{ or } R'_s = 1$$

A combined asymmetric version

Theorem (P.S.)

Given $\delta > 0$, $q \in (1,\infty)$ there is $\varepsilon > 0$ such that the following holds for large $m = m'T$. Suppose μ, ν are prob. measures on $\mathbb{Z}/2^m\mathbb{Z}$ such that

$$\|\mu * \nu\|_q \geq 2^{-\varepsilon m}\|\mu\|_q$$

Then there exist sets $A \subset \text{supp}\mu$, $B \subset \text{supp}\nu$ such that:

1. $\|\mu|_A\|_q \geq m^{-\delta}\|\mu|_A\|$, $\nu(B) \geq m^{-\delta}$.
2. *μ, ν are constant on A, B (up to a constant factor).*
3. *The set A is $(R_1, \ldots, R_{m'})$-regular and the set B is $(R'_1, \ldots, R'_{m'})$-regular.*
4. *For each s,*

$$\text{either } R_s \geq 2^{(1-\delta)T} \text{ or } R'_s = 1$$

A combined asymmetric version

Theorem (P.S.)

Given $\delta > 0$, $q \in (1, \infty)$ there is $\varepsilon > 0$ such that the following holds for large $m = m'T$. Suppose μ, ν are prob. measures on $\mathbb{Z}/2^m\mathbb{Z}$ such that

$$\|\mu * \nu\|_q \geq 2^{-\varepsilon m}\|\mu\|_q$$

Then there exist sets $A \subset \text{supp}\mu$, $B \subset \text{supp}\nu$ such that:

1. $\|\mu|_A\|_q \geq m^{-\delta}\|\mu|_A\|$, $\nu(B) \geq m^{-\delta}$.
2. μ, ν *are constant on* A, B *(up to a constant factor).*
3. *The set A is $(R_1, \ldots, R_{m'})$-regular and the set B is $(R'_1, \ldots, R'_{m'})$-regular.*
4. *For each s,*

$$\text{either } R_s \geq 2^{(1-\delta)T} \text{ or } R'_s = 1$$

A combined asymmetric version

Theorem (P.S.)

Given $\delta > 0$, $q \in (1, \infty)$ there is $\varepsilon > 0$ such that the following holds for large $m = m'T$. Suppose μ, ν are prob. measures on $\mathbb{Z}/2^m\mathbb{Z}$ such that

$$\|\mu * \nu\|_q \geq 2^{-\varepsilon m}\|\mu\|_q$$

Then there exist sets $A \subset \mathrm{supp}\mu$, $B \subset \mathrm{supp}\nu$ such that:

1. $\|\mu|_A\|_q \geq m^{-\delta}\|\mu|_A\|$, $\nu(B) \geq m^{-\delta}$.
2. μ, ν *are constant on* A, B *(up to a constant factor).*
3. *The set* A *is* $(R_1, \ldots, R_{m'})$*-regular and the set* B *is* $(R'_1, \ldots, R'_{m'})$*-regular.*
4. *For each* s,

$$\text{either } R_s \geq 2^{(1-\delta)T} \text{ or } R'_s = 1$$

A combined asymmetric version

Theorem (P.S.)

Given $\delta > 0$, $q \in (1,\infty)$ there is $\varepsilon > 0$ such that the following holds for large $m = m'T$. Suppose μ, ν are prob. measures on $\mathbb{Z}/2^m\mathbb{Z}$ such that

$$\|\mu * \nu\|_q \geq 2^{-\varepsilon m}\|\mu\|_q$$

Then there exist sets $A \subset \mathrm{supp}\mu$, $B \subset \mathrm{supp}\nu$ such that:

1. $\|\mu|_A\|_q \geq m^{-\delta}\|\mu|_A\|$, $\nu(B) \geq m^{-\delta}$.
2. *μ, ν are constant on A, B (up to a constant factor).*
3. *The set A is $(R_1, \ldots, R_{m'})$-regular and the set B is $(R'_1, \ldots, R'_{m'})$-regular.*
4. *For each s,*

$$\text{either } R_s \geq 2^{(1-\delta)T} \text{ or } R'_s = 1$$

Back to self-similar measures

The following is a key step in the proof of the main result. It is proved using the inverse theorem from the previous slide.

Definition

$$\nu^{(m)}(j2^{-m}) = \nu([j2^{-m}, (j+1)2^{-m}))$$

Theorem

Let $(\mu_x)_{x\in g}$ be a family of DSSM, and suppose $q > 1$, $D(q) < 1$ and D is differentiable at q, there $D(q)$ is the almost sure value of $\dim_q(\mu_x)$.

Then for every $\sigma > 0$ there is $\varepsilon = \varepsilon(\sigma, q) > 0$ such that the following holds for all large enough m and all x: if ρ is an arbitrary 2^{-m}-measure such that $\|\rho\|_q^{q'} \leq 2^{-\sigma m}$, then

$$\|\rho * \mu_x^{(m)}\|_q^q \leq 2^{-\varepsilon m}\|\mu_x^{(m)}\|_q^q.$$

Back to self-similar measures

The following is a key step in the proof of the main result. It is proved using the inverse theorem from the previous slide.

Definition

$$\nu^{(m)}(j2^{-m}) = \nu([j2^{-m}, (j+1)2^{-m}))$$

Theorem

Let $(\mu_x)_{x\in g}$ be a family of DSSM, and suppose $q > 1$, $D(q) < 1$ and D is differentiable at q, there $D(q)$ is the almost sure value of $\dim_q(\mu_x)$.

Then for every $\sigma > 0$ there is $\varepsilon = \varepsilon(\sigma, q) > 0$ such that the following holds for all large enough m and all x: if ρ is an arbitrary 2^{-m}-measure such that $\|\rho\|_q^{q'} \leq 2^{-\sigma m}$, then

$$\|\rho * \mu_x^{(m)}\|_q^q \leq 2^{-\varepsilon m}\|\mu_x^{(m)}\|_q^q.$$

End of part III

Merci beaucoup!