Additive Combinatorics Methods in Fractal Geometry, Lecture I

Pablo Shmerkin

Department of Mathematics
The University of British Columbia

School on Dimension Theory of Fractals, Erdős Center, Budapest, 26-30 August 2024

Plan for the course

Lecture 1: Introduction to Additive Combinatorics.

Lecture 2: The Balog-Szemerédi-Gowers Theorem.

Lecture 3: Discretized Fractal Geometry.

Lecture 4: Sum-product and applications.

Plan for the course

Lecture 1: Introduction to Additive Combinatorics.

Lecture 2: The Balog-Szemerédi-Gowers Theorem.

Lecture 3: Discretized Fractal Geometry.

Lecture 4: Sum-product and applications.

Plan for the course

Lecture 1: Introduction to Additive Combinatorics.

Lecture 2: The Balog-Szemerédi-Gowers Theorem.

Lecture 3: Discretized Fractal Geometry.

Lecture 4: Sum-product and applications.

Lecture 1: Introduction to Additive Combinatorics.

Lecture 2: The Balog-Szemerédi-Gowers Theorem.

Lecture 3: Discretized Fractal Geometry.

Lecture 4: Sum-product and applications.

Outline

What is additive combinatorics?

We will see it through a sample of some important concepts and results.

One of the main features is that is has many (bidirectional) connections:

- Fractal geometry
- Harmonic Analysis
- Ergodic Theory
- Number Theory
- Combinatorics

What is additive combinatorics?

We will see it through a sample of some important concepts and results.

One of the main features is that is has many (bidirectional) connections:

- Fractal geometry
- Harmonic Analysis
- Ergodic Theory
- Number Theory
- Combinatorics

What is additive combinatorics?

We will see it through a sample of some important concepts and results.

One of the main features is that is has many (bidirectional) connections:

- Fractal geometry
- Harmonic Analysis
- Ergodic Theory
- Number Theory
- Combinatorics

What is additive combinatorics?

We will see it through a sample of some important concepts and results.

One of the main features is that is has many (bidirectional) connections:

- Fractal geometry
- Harmonic Analysis
- Ergodic Theory
- Number Theory
- Combinatorics

We will see it through a sample of some important concepts and results.

One of the main features is that is has many (bidirectional) connections:

- Fractal geometry
- Harmonic Analysis
- Ergodic Theory
- Number Theory
- Combinatorics

What is additive combinatorics?

We will see it through a sample of some important concepts and results.

One of the main features is that is has many (bidirectional) connections:

- Fractal geometry
- Harmonic Analysis
- Ergodic Theory
- Number Theory
- Combinatorics

Additive combinatorics takes place in some ambient Abelian group Z. For the purposes of this course, you can think of:

- $\mathbb{Z}$ or $\mathbb{Z}^d$
- $\mathbb{R}$ or $\mathbb{R}^d$.
- $\mathbb{C}$ or $\mathbb{C}^d$.
- The circle $\mathbb{R}/\mathbb{Z}$ or the torus $\mathbb{R}/\mathbb{Z}^d$ (written additively as $[0, 1)^d$).
- $\mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^d$ (with p usually a prime).

Additive combinatorics takes place in some ambient Abelian group Z. For the purposes of this course, you can think of:

- $\mathbb{Z}$ or $\mathbb{Z}^d$
- $\mathbb{R}$ or $\mathbb{R}^d$.
- $\mathbb{C}$ or $\mathbb{C}^d$.
- The circle $\mathbb{R}/\mathbb{Z}$ or the torus $\mathbb{R}/\mathbb{Z}^d$ (written additively as $[0,1)^d$).
- $\mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^d$ (with p usually a prime).

Additive combinatorics takes place in some ambient Abelian group Z. For the purposes of this course, you can think of:

- $\mathbb{Z}$ or $\mathbb{Z}^d$
- $\mathbb{R}$ or $\mathbb{R}^d$.
- $\mathbb{C}$ or $\mathbb{C}^d$.
- The circle $\mathbb{R}/\mathbb{Z}$ or the torus $\mathbb{R}/\mathbb{Z}^d$ (written additively as $[0, 1)^d$).
- $\mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^d$ (with p usually a prime).

Additive combinatorics takes place in some ambient Abelian group Z. For the purposes of this course, you can think of:

- $\mathbb{Z}$ or $\mathbb{Z}^d$
- $\mathbb{R}$ or $\mathbb{R}^d$.
- $\mathbb{C}$ or $\mathbb{C}^d$.
- The circle $\mathbb{R}/\mathbb{Z}$ or the torus $\mathbb{R}/\mathbb{Z}^d$ (written additively as $[0,1)^d$).
- $\mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^d$ (with p usually a prime).

Additive combinatorics takes place in some ambient Abelian group Z. For the purposes of this course, you can think of:

- $\mathbb{Z}$ or $\mathbb{Z}^d$
- $\mathbb{R}$ or $\mathbb{R}^d$.
- $\mathbb{C}$ or $\mathbb{C}^d$.
- The circle $\mathbb{R}/\mathbb{Z}$ or the torus $\mathbb{R}/\mathbb{Z}^d$ (written additively as $[0, 1)^d$).
- $\mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^d$ (with p usually a prime).

Definition

A k-AP is

$$a, a+v, a+2v, \dots, a+(k-1)v$$

with $a, v \in Z$ and $v \neq 0$.

Question

What conditions of size and/or structure ensure that A contains (long) arithmetic progressions?

Definition

A *k-AP* is

$$a, a+v, a+2v, \ldots, a+(k-1)v$$

with $a, v \in Z$ and $v \neq 0$.

Question

What conditions of size and/or structure ensure that A contains (long) arithmetic progressions?

Definition

Let $r_k(N)$ be the size of the largest subset of $\{1, \ldots, N\}$ that does not contain a k-AP.

Theorem (Szemerédi 1975)

For any $k \geq 3$,

$$\lim_{N \to \infty} \frac{r_k(N)}{N} = 0.$$

Corollary

A subset of the integers of positive upper density contains arbitrarily long arithmetic progressions.

Definition

Let $r_k(N)$ be the size of the largest subset of $\{1, \ldots, N\}$ that does not contain a k-AP.

Theorem (Szemerédi 1975)

For any $k \geq 3$,

$$\lim_{N \to \infty} \frac{r_k(N)}{N} = 0.$$

Corollary

A subset of the integers of positive upper density contains arbitrarily long arithmetic progressions.

Definition

Let $r_k(N)$ be the size of the largest subset of $\{1, \ldots, N\}$ that does not contain a k-AP.

Theorem (Szemerédi 1975)

For any $k \geq 3$,

$$\lim_{N\to\infty} \frac{r_k(N)}{N} = 0.$$

Corollary

A subset of the integers of positive upper density contains arbitrarily long arithmetic progressions.

Remarks on Szemerédi's Theorem

- The case $k = 3$ was proved by K. Roth in the 1952 using the Fourier transform. The Fourier transform does not work at all if $k \geq 4$.
- Very influential proofs of Szemerédi's Theorem were given by H. Furstenberg (Ergodic Theory), T. Gowers (Higher order Fourier analysis), T. Tao (finitary ergodic theory), and others.
- There have been many generalizations and extensions, the most famous of which is the Green-Tao Theorem extending Szemerédi's Theorem to the primes.
- An active area of research concerns Szemerédi-type phenomena in subsets of Euclidean space: Geometric Measure Theory+Harmonic Analysis.

Remarks on Szemerédi's Theorem

- The case $k = 3$ was proved by K. Roth in the 1952 using the Fourier transform. The Fourier transform does not work at all if $k \geq 4$.
- Very influential proofs of Szemerédi's Theorem were given by H. Furstenberg (Ergodic Theory), T. Gowers (Higher order Fourier analysis), T. Tao (finitary ergodic theory), and others.
- There have been many generalizations and extensions, the most famous of which is the Green-Tao Theorem extending Szemerédi's Theorem to the primes.
- An active area of research concerns Szemerédi-type phenomena in subsets of Euclidean space: Geometric Measure Theory+Harmonic Analysis.

Remarks on Szemerédi's Theorem

- The case $k = 3$ was proved by K. Roth in the 1952 using the Fourier transform. The Fourier transform does not work at all if $k \geq 4$.
- Very influential proofs of Szemerédi's Theorem were given by H. Furstenberg (Ergodic Theory), T. Gowers (Higher order Fourier analysis), T. Tao (finitary ergodic theory), and others.
- There have been many generalizations and extensions, the most famous of which is the Green-Tao Theorem extending Szemerédi's Theorem to the primes.
- An active area of research concerns Szemerédi-type phenomena in subsets of Euclidean space: Geometric Measure Theory+Harmonic Analysis.

Remarks on Szemerédi's Theorem

- The case $k = 3$ was proved by K. Roth in the 1952 using the Fourier transform. The Fourier transform does not work at all if $k \geq 4$.
- Very influential proofs of Szemerédi's Theorem were given by H. Furstenberg (Ergodic Theory), T. Gowers (Higher order Fourier analysis), T. Tao (finitary ergodic theory), and others.
- There have been many generalizations and extensions, the most famous of which is the Green-Tao Theorem extending Szemerédi's Theorem to the primes.
- An active area of research concerns Szemerédi-type phenomena in subsets of Euclidean space: Geometric Measure Theory+Harmonic Analysis.

- Recall Szemerédi's Theorem: $\lim_{N\to\infty} \frac{r_k(N)}{N} = 0$, where $r_k(N)$ is the size of the largest subset of $\{1, \ldots, N\}$ that does not contain a k-AP.
- The original proof of Szemerédi's Theorem gave extremely poor bounds on $r_k(N)$. Finding good bounds for $r_k(N)$ is a very active and important problem.
- For $k = 3$, several recent breakthroughs have been obtained by T. Bloom-O. Sisask, Z. Kelley-R. Meka and others. The current world-record is

$$r_3(N) \leq \exp(-c \log(N)^{1/9}) \cdot N.$$

- For comparison, the best lower bound dates back (essentially) to Behrend's 1946 example:

$$r_3(N) \geq \exp(-c' \log(N)^{1/2}) \cdot N.$$

- Recall Szemerédi's Theorem: $\lim_{N\to\infty} \frac{r_k(N)}{N} = 0$, where $r_k(N)$ is the size of the largest subset of $\{1, \ldots, N\}$ that does not contain a k-AP.
- The original proof of Szemerédi's Theorem gave extremely poor bounds on $r_k(N)$. Finding good bounds for $r_k(N)$ is a very active and important problem.
- For $k = 3$, several recent breakthroughs have been obtained by T. Bloom-O. Sisask, Z. Kelley-R. Meka and others. The current world-record is

$$r_3(N) \leq \exp(-c \log(N)^{1/9}) \cdot N.$$

- For comparison, the best lower bound dates back (essentially) to Behrend's 1946 example:

$$r_3(N) \geq \exp(-c' \log(N)^{1/2}) \cdot N.$$

- Recall Szemerédi's Theorem: $\lim_{N\to\infty} \frac{r_k(N)}{N} = 0$, where $r_k(N)$ is the size of the largest subset of $\{1, \ldots, N\}$ that does not contain a k-AP.
- The original proof of Szemerédi's Theorem gave extremely poor bounds on $r_k(N)$. Finding good bounds for $r_k(N)$ is a very active and important problem.
- For $k = 3$, several recent breakthroughs have been obtained by T. Bloom-O. Sisask, Z. Kelley-R. Meka and others. The current world-record is

$$r_3(N) \leq \exp(-c \log(N)^{1/9}) \cdot N.$$

- For comparison, the best lower bound dates back (essentially) to Behrend's 1946 example:

$$r_3(N) \geq \exp(-c' \log(N)^{1/2}) \cdot N.$$

- Recall Szemerédi's Theorem: $\lim_{N\to\infty} \frac{r_k(N)}{N} = 0$, where $r_k(N)$ is the size of the largest subset of $\{1, \ldots, N\}$ that does not contain a k-AP.
- The original proof of Szemerédi's Theorem gave extremely poor bounds on $r_k(N)$. Finding good bounds for $r_k(N)$ is a very active and important problem.
- For $k = 3$, several recent breakthroughs have been obtained by T. Bloom-O. Sisask, Z. Kelley-R. Meka and others. The current world-record is

$$r_3(N) \leq \exp(-c \log(N)^{1/9}) \cdot N.$$

- For comparison, the best lower bound dates back (essentially) to Behrend's 1946 example:

$$r_3(N) \geq \exp(-c' \log(N)^{1/2}) \cdot N.$$

Outline

Definition

If $A, B \subset \mathbb{Z}$ we define their sumset and difference set as

$$\begin{aligned} A + B &= \{x + y : x \in A, y \in B\}, \\ A - B &= \{x - y : x \in A, y \in B\}, \\ nA &= \underbrace{A + \cdots + A}_{n \text{ times}}. \end{aligned}$$

Remark

One of the most fundamental problems of additive combinatorics is to understand the relationship between the sizes (and the structure) of A, B and sets obtained from them via sums and differences.

When the ambient group is a ring (e.g. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}/p/\mathbb{Z}$), one is also interested in product sets $A.B$.

Definition

If $A, B \subset \mathbb{Z}$ we define their sumset and difference set as

$$A + B = \{x + y : x \in A, y \in B\},$$
$$A - B = \{x - y : x \in A, y \in B\},$$
$$nA = \underbrace{A + \cdots + A}_{n \text{ times}}.$$

Remark

One of the most fundamental problems of additive combinatorics is to understand the relationship between the sizes (and the structure) of A, B and sets obtained from them via sums and differences.

When the ambient group is a ring (e.g. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}/p/\mathbb{Z}$), one is also interested in product sets $A.B$.

Definition

If $A, B \subset \mathbb{Z}$ we define their sumset and difference set as

$$A + B = \{x + y : x \in A, y \in B\},$$
$$A - B = \{x - y : x \in A, y \in B\},$$
$$nA = \underbrace{A + \cdots + A}_{n \text{ times}}.$$

Remark

One of the most fundamental problems of additive combinatorics is to understand the relationship between the sizes (and the structure) of A, B and sets obtained from them via sums and differences.

When the ambient group is a ring (e.g. $\mathbb{Z}, \mathbb{R}, \mathbb{Z}/p/\mathbb{Z}$), one is also interested in product sets $A.B$.

Definition

If $A, B \subset \mathbb{Z}$ we define their sumset and difference set as

$$\begin{aligned} A+B &= \{x+y : x \in A, y \in B\}, \\ A-B &= \{x-y : x \in A, y \in B\}, \\ nA &= \underbrace{A+\cdots+A}_{n \text{ times}}. \end{aligned}$$

Remark

One of the most fundamental problems of additive combinatorics is to understand the relationship between the sizes (and the structure) of A, B and sets obtained from them via sums and differences.

When the ambient group is a ring (e.g. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}/p/\mathbb{Z}$), one is also interested in product sets $A.B$.

Size of sumsets and additive structure

- For any set A,

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

So, up to multiplicative constants, $|A+A|$ varies between $|A|$ and $|A|^2$ (or $|Z|$ if $|Z| \leq |A|^2$).

- The first inequality follows since $A + A \supset A + a$ for a fixed $a \in A$. The second inequality follows from the fact that there are $|A|(|A+1)/2$ possible non-ordered pairs $\{a, a'\}$ with $a, a' \in A$.
- 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 set A,

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

  So, up to multiplicative constants, $|A+A|$ varies between $|A|$ and $|A|^2$ (or $|Z|$ if $|Z| \leq |A|^2$).
- The first inequality follows since $A + A \supset A + a$ for a fixed $a \in A$. The second inequality follows from the fact that there are $|A|(|A+1)/2$ possible non-ordered pairs $\{a, a'\}$ with $a, a' \in A$.
- 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 set A,

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

  So, up to multiplicative constants, $|A+A|$ varies between $|A|$ and $|A|^2$ (or $|Z|$ if $|Z| \leq |A|^2$).

- The first inequality follows since $A+A \supset A+a$ for a fixed $a \in A$. The second inequality follows from the fact that there are $|A|(|A+1)/2$ possible non-ordered pairs $\{a, a'\}$ with $a, a' \in A$.
- We think of sets A with $|A+A| \sim |A|$ as sets with additive structure or as approximate subgroups.

Definition

A GAP is a set of the form

$$\{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \leq i_j < k_i\} = a + [\mathbf{k}].\mathbf{v},$$

where $\mathbf{k} = (k_1, \ldots, k_d) \subset \mathbb{N}^d$, $a \in Z$, $\mathbf{v} = (v_1, \ldots, v_d) \in Z^d$, $v_i \neq 0$.

A GAP A is proper if

$$|A| = k_1 \cdots k_d,$$

i.e. all the sums $a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d$ are different.

The rank of the GAP is d (a GAP of rank 1 is an AP).

Definition

A GAP is a set of the form

$$\{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \le i_j < k_i\} = a + [\mathbf{k}].\mathbf{v},$$

where $\mathbf{k} = (k_1, \ldots, k_d) \subset \mathbb{N}^d$, $a \in Z$, $\mathbf{v} = (v_1, \ldots, v_d) \in Z^d$, $v_i \neq 0$.

A GAP A is proper if

$$|A| = k_1 \cdots k_d,$$

i.e. all the sums $a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d$ are different.

The rank of the GAP is d (a GAP of rank 1 is an AP).

Definition

A GAP is a set of the form

$$\{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \leq i_j < k_i\} = a + [\mathbf{k}].\mathbf{v},$$

where $\mathbf{k} = (k_1, \ldots, k_d) \subset \mathbb{N}^d$, $a \in Z$, $\mathbf{v} = (v_1, \ldots, v_d) \in Z^d$, $v_i \neq 0$.

A GAP A is proper if

$$|A| = k_1 \cdots k_d,$$

i.e. all the sums $a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d$ are different.

The rank of the GAP is d (a GAP of rank 1 is an AP).

Definition

A GAP is a set of the form

$$\{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \le i_j < k_i\} = a + [\mathbf{k}].\mathbf{v},$$

where $\mathbf{k} = (k_1, \ldots, k_d) \subset \mathbb{N}^d$, $a \in Z$, $\mathbf{v} = (v_1, \ldots, v_d) \in Z^d$, $v_i \neq 0$.

A GAP A is proper if

$$|A| = k_1 \cdots k_d,$$

i.e. all the sums $a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d$ are different.

The rank of the GAP is d (a GAP of rank 1 is an AP).

Examples of sets with additive structure

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

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \leq 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. Indeed, let

$$A = a + [\mathbf{k}].\mathbf{v} = \{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \leq i_\ell < k_\ell\}.$$

Then

$$A+A = \{2a + j_1 v_1 + j_2 v_2 + \ldots + j_d v_d : 0 \leq j_\ell < 2k_\ell\} = a + [2\mathbf{k}].\mathbf{v},$$

so

$$|A+A| \leq (2k_1)\cdots(2k_\ell) = 2^d(k_1 \cdots k_\ell) = 2^d|A|.$$

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

Examples of sets with additive structure

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

- Subgroups (if they exist).
- Arithmetic progressions: $|A + A| \leq 2|A|$.
- Proper GAPs: $|A + A| \leq 2^d|A|$ where d is the rank. Indeed, let

  $$A = a + [\mathbf{k}].\mathbf{v} = \{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \leq i_\ell < k_\ell\}.$$

  Then

  $$A+A = \{2a+j_1 v_1+j_2 v_2+\ldots+j_d v_d : 0 \leq j_\ell < 2k_\ell\} = a+[2\mathbf{k}].\mathbf{v},$$

  so

  $$|A + A| \leq (2k_1)\cdots(2k_\ell) = 2^d(k_1 \cdots k_\ell) = 2^d|A|.$$

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

Examples of sets with additive structure

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

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \leq 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. Indeed, let

  $$A = a + [\mathbf{k}].\mathbf{v} = \{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \leq i_\ell < k_\ell\}.$$

  Then

  $$A+A = \{2a+j_1 v_1+j_2 v_2+\ldots+j_d v_d : 0 \leq j_\ell < 2k_\ell\} = a+[2\mathbf{k}].\mathbf{v},$$

  so

  $$|A+A| \leq (2k_1)\cdots(2k_\ell) = 2^d(k_1\cdots k_\ell) = 2^d|A|.$$

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

Examples of sets with additive structure

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

- Subgroups (if they exist).
- Arithmetic progressions: $|A+A| \leq 2|A|$.
- Proper GAPs: $|A+A| \leq 2^d|A|$ where d is the rank. Indeed, let

$$A = a + [\mathbf{k}].\mathbf{v} = \{a + i_1 v_1 + i_2 v_2 + \ldots + i_d v_d : 0 \leq i_\ell < k_\ell\}.$$

Then

$$A+A = \{2a+j_1 v_1+j_2 v_2+\ldots+j_d v_d : 0 \leq j_\ell < 2k_\ell\} = a+[2\mathbf{k}].\mathbf{v},$$

so

$$|A+A| \leq (2k_1)\cdots(2k_\ell) = 2^d(k_1\cdots k_\ell) = 2^d|A|.$$

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

Examples of sets without additive structure

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 (e.g. 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 without additive structure

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 (e.g. 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 without additive structure

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 (e.g. 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.

A set with intermediate additive structure

- Let A be the set of all numbers in $[1, N]$ with $N = 4^k$ whose base 4 expansion has only digits 0 and 1.
- This is an integer analog of a self-similar set.
- We have $|A| \sim 2^k = N^{1/2}$.
- Then $A + A$ is the set of all numbers in $[2, 2N]$ whose base 4 expansion has only digits 0, 1, 2.
- We have $|A + A| \sim 3^k = N^{3/4} \sim |A|^{3/2}$.
- So $|A| \ll |A + A| \ll |A|^2$.

A set with intermediate additive structure

- Let A be the set of all numbers in $[1, N]$ with $N = 4^k$ whose base 4 expansion has only digits 0 and 1.
- This is an integer analog of a self-similar set.
- We have $|A| \sim 2^k = N^{1/2}$.
- Then $A + A$ is the set of all numbers in $[2, 2N]$ whose base 4 expansion has only digits 0, 1, 2.
- We have $|A + A| \sim 3^k = N^{3/4} \sim |A|^{3/2}$.
- So $|A| \ll |A + A| \ll |A|^2$.

A set with intermediate additive structure

- Let A be the set of all numbers in $[1, N]$ with $N = 4^k$ whose base 4 expansion has only digits 0 and 1.
- This is an integer analog of a self-similar set.
- We have $|A| \sim 2^k = N^{1/2}$.
- Then $A + A$ is the set of all numbers in $[2, 2N]$ whose base 4 expansion has only digits 0, 1, 2.
- We have $|A + A| \sim 3^k = N^{3/4} \sim |A|^{3/2}$.
- So $|A| \ll |A + A| \ll |A|^2$.

A set with intermediate additive structure

- Let A be the set of all numbers in $[1, N]$ with $N = 4^k$ whose base 4 expansion has only digits 0 and 1.
- This is an integer analog of a self-similar set.
- We have $|A| \sim 2^k = N^{1/2}$.
- Then $A + A$ is the set of all numbers in $[2, 2N]$ whose base 4 expansion has only digits 0, 1, 2.
- We have $|A + A| \sim 3^k = N^{3/4} \sim |A|^{3/2}$.
- So $|A| \ll |A + A| \ll |A|^2$.

A set with intermediate additive structure

- Let A be the set of all numbers in $[1, N]$ with $N = 4^k$ whose base 4 expansion has only digits 0 and 1.
- This is an integer analog of a self-similar set.
- We have $|A| \sim 2^k = N^{1/2}$.
- Then $A + A$ is the set of all numbers in $[2, 2N]$ whose base 4 expansion has only digits 0, 1, 2.
- We have $|A + A| \sim 3^k = N^{3/4} \sim |A|^{3/2}$.
- So $|A| \ll |A + A| \ll |A|^2$.

A set with intermediate additive structure

- Let A be the set of all numbers in $[1, N]$ with $N = 4^k$ whose base 4 expansion has only digits 0 and 1.
- This is an integer analog of a self-similar set.
- We have $|A| \sim 2^k = N^{1/2}$.
- Then $A + A$ is the set of all numbers in $[2, 2N]$ whose base 4 expansion has only digits 0, 1, 2.
- We have $|A + A| \sim 3^k = N^{3/4} \sim |A|^{3/2}$.
- So $|A| \ll |A + A| \ll |A|^2$.

Recall: If A is a dense subset of a proper GAP, then $|A + A| \sim |A|$.

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.*

Theorem (Ruzsa, Chang, Sanders, Schoen)

Suppose $|A+A| \leq K|A|$. *Then there is a* GAP P *with*

$$rank(P) \leq K^{1+C\log(K)^{-1/2}} \leq K^{1+\varepsilon}$$

and such that $A \subset P$ *and*

$$|P| \leq \exp(1 + C\log(K)^{-1/2})|A| \leq \exp(K^{1+\varepsilon}).$$

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, the quantitative estimates on $d(K)$ and $S(K)$ are crucial.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with slightly worse quantitative bounds).
- At least with the current bounds, Freiman's Theorem says nothing if K grows like $K = |A|^{\delta}$.

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, the quantitative estimates on $d(K)$ and $S(K)$ are crucial.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with slightly worse quantitative bounds).
- At least with the current bounds, Freiman's Theorem says nothing if K grows like $K = |A|^{\delta}$.

- Freiman's Theorem can be seen as an inverse or classification theorem: based on qualitative information about A, it returns structural information.
- In applications, the quantitative estimates on $d(K)$ and $S(K)$ are crucial.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with slightly worse quantitative bounds).
- At least with the current bounds, Freiman's Theorem says nothing if K grows like $K = |A|^{\delta}$.

- Freiman's Theorem can be seen as an inverse or classification theorem: based on qualitative information about A, it returns structural information.
- In applications, the quantitative estimates on $d(K)$ and $S(K)$ are crucial.
- The theorem does not guarantee that P is proper. But it can be taken to be proper (with slightly worse quantitative bounds).
- At least with the current bounds, Freiman's Theorem says nothing if K grows like $K = |A|^{\delta}$.

Outline

Motivation

Freiman's Theorem says that if $|A + A| \leq K|A|$ then A is a dense subset of a low-rank GAP*.*

Using this it is easy to show that $|A + A + A| \leq f(K)|A|$ and so on. In other words, having a small sumset implies having a small n-sumset nA.

But can we do better than Freiman's Theorem in this direction?

Theorem (Plünnecke Inequalities, 1969)

Suppose $|A + A| \leq K|A|$. Then $|nA| \leq K^n|A|$.

More generally, if $|A + B| \leq K|A|$, then $|nB| \leq K^n|A|$.

Motivation

Freiman's Theorem says that if $|A + A| \leq K|A|$ *then* A *is a dense subset of a low-rank* GAP*.*

Using this it is easy to show that $|A + A + A| \leq f(K)|A|$ *and so on. In other words, having a small sumset implies having a small n-sumset nA.*

But can we do better than Freiman's Theorem in this direction?

Theorem (Plünnecke Inequalities, 1969)

Suppose $|A + A| \leq K|A|$*. Then* $|nA| \leq K^n|A|$*.*

More generally, if $|A + B| \leq K|A|$*, then* $|nB| \leq K^n|A|$*.*

G. Petridis' proof of Plünnecke's inequalities

- Suppose $|A + B| \leq K|A|$. We want to show $|nB| \leq K^n|A|$.
- Choose a subset A' of A which minimizes the ratio

$$\frac{|A' + B|}{|A'|},$$

  let K' be the ratio.
- Then $K' \leq K$ (since A' is a subset of A).
- By definition we have:

$$|A' + B| = K'|A'|,$$
$$|Z + B| \geq K'|Z| \quad (Z \subset A).$$

G. Petridis' proof of Plünnecke's inequalities

- Suppose $|A+B| \leq K|A|$. We want to show $|nB| \leq K^n|A|$.
- Choose a subset A' of A which minimizes the ratio

$$\frac{|A'+B|}{|A'|},$$

let K' be the ratio.
- Then $K' \leq K$ (since A' is a subset of A).
- By definition we have:

$$|A'+B| = K'|A'|,$$
$$|Z+B| \geq K'|Z| \quad (Z \subset A).$$

G. Petridis' proof of Plünnecke's inequalities

- Suppose $|A + B| \leq K|A|$. We want to show $|nB| \leq K^n|A|$.
- Choose a subset A' of A which minimizes the ratio

$$\frac{|A' + B|}{|A'|},$$

  let K' be the ratio.
- Then $K' \leq K$ (since A' is a subset of A).
- By definition we have:

$$|A' + B| = K'|A'|,$$
$$|Z + B| \geq K'|Z| \quad (Z \subset A).$$

G. Petridis' proof of Plünnecke's inequalities

- Suppose $|A + B| \leq K|A|$. We want to show $|nB| \leq K^n|A|$.
- Choose a subset A' of A which minimizes the ratio

$$\frac{|A' + B|}{|A'|},$$

  let K' be the ratio.
- Then $K' \leq K$ (since A' is a subset of A).
- By definition we have:

$$|A' + B| = K'|A'|,$$
$$|Z + B| \geq K'|Z| \quad (Z \subset A).$$

Lemma (Petridis 2011)

For every set $C \subset Z$,

$$|A' + B + C| \leq K'|A' + C|.$$

Proof of Plünnecke's inequalities, assuming lemma.

We prove by induction that

$$|nB| \leq |A' + nB| \leq (K')^n|A'| \leq K^n|A|$$

For $n = 1$, this is the definition of K'.

For the induction step, apply the lemma to $C = (n-1)B$. □

Plünnecke's inequality: main lemma

Lemma (Petridis 2011)

For every set $C \subset Z$,

$$|A' + B + C| \leq K'|A' + C|.$$

Proof of Plünnecke's inequalities, assuming lemma.

We prove by induction that

$$|nB| \leq |A' + nB| \leq (K')^n|A'| \leq K^n|A|$$

For $n = 1$, this is the definition of K'.

For the induction step, apply the lemma to $C = (n-1)B$. $\square$

Plünnecke inequalities: proof of main lemma I

Lemma (Petridis)

$$|A' + B + C| \leq K'|A' + C|,$$

where

$$K' = \frac{|A' + B|}{|A'|} = \min_{X \subset A} \frac{|X + B|}{|X|}.$$

- Induction in $|C|$.
- The case $|C| = \{x\}$ is true since $|A' + B + x| = |A' + B|$ and $|A' + x| = |A'|$.
- Assume true for C, and let $C' = C \cup \{x\}$.

Plünnecke inequalities: proof of main lemma I

Lemma (Petridis)

$$|A' + B + C| \leq K'|A' + C|,$$

where

$$K' = \frac{|A' + B|}{|A'|} = \min_{X \subset A} \frac{|X + B|}{|X|}.$$

- Induction in $|C|$.
- The case $|C| = \{x\}$ is true since $|A' + B + x| = |A' + B|$ and $|A' + x| = |A'|$.
- Assume true for C, and let $C' = C \cup \{x\}$.

Plünnecke inequalities: proof of main lemma I

Lemma (Petridis)

$$|A' + B + C| \leq K'|A' + C|,$$

where

$$K' = \frac{|A' + B|}{|A'|} = \min_{X \subset A} \frac{|X + B|}{|X|}.$$

- Induction in $|C|$.
- The case $|C| = \{x\}$ is true since $|A' + B + x| = |A' + B|$ and $|A' + x| = |A'|$.
- Assume true for C, and let $C' = C \cup \{x\}$.

Plünnecke inequalities: proof of main lemma I

Lemma (Petridis)

$$|A' + B + C| \leq K'|A' + C|,$$

where

$$K' = \frac{|A' + B|}{|A'|} = \min_{X \subset A} \frac{|X + B|}{|X|}.$$

- Induction in $|C|$.
- The case $|C| = \{x\}$ is true since $|A' + B + x| = |A' + B|$ and $|A' + x| = |A'|$.
- Assume true for C, and let $C' = C \cup \{x\}$.

Plünnecke inequalities: proof of main lemma II

Lemma (Petridis)

$$|A' + B + C| \le K'|A' + C|, \quad \textit{where } \frac{|A' + B|}{|A'|} = K', \ K' \textit{ minimal.}$$

- $A' + B + C' = (A' + B + C) \cup \left((A' + B + x) \setminus (Z + B + x)\right)$, where

$$Z = \{a \in A' : a + B + x \subset A + B + C\}.$$

- $|Z + B| \ge K'|Z|$ by minimality of K'.
- By the inductive hypothesis,

$$\begin{aligned} |A' + B + C'| &\le |A' + B + C| + \left(|A' + B + x| - |Z + B + x|\right) \\ &\le K'|A' + C| + K'|A'| - K'|Z|. \end{aligned}$$

- It remains to show that

$$|A' + C| + |A'| - |Z| \le |A' + C'|.$$

Plünnecke inequalities: proof of main lemma II

Lemma (Petridis)

$$|A' + B + C| \le K'|A' + C|, \quad \textit{where } \frac{|A' + B|}{|A'|} = K', \ K' \textit{ minimal.}$$

- $A' + B + C' = (A' + B + C) \cup \big((A' + B + x) \setminus (Z + B + x)\big)$, where

$$Z = \{a \in A' : a + B + x \subset A + B + C\}.$$

- $|Z + B| \ge K'|Z|$ by minimality of K'.
- By the inductive hypothesis,

$$\begin{aligned} |A' + B + C'| &\le |A' + B + C| + \big(|A' + B + x| - |Z + B + x|\big) \\ &\le K'|A' + C| + K'|A'| - K'|Z|. \end{aligned}$$

- It remains to show that

$$|A' + C| + |A'| - |Z| \le |A' + C'|.$$

Plünnecke inequalities: proof of main lemma II

Lemma (Petridis)

$$|A' + B + C| \leq K'|A' + C|, \quad \textit{where } \frac{|A' + B|}{|A'|} = K', \ K' \textit{ minimal.}$$

- $A' + B + C' = (A' + B + C) \cup \big((A' + B + x) \setminus (Z + B + x)\big)$, where

$$Z = \{a \in A' : a + B + x \subset A + B + C\}.$$

- $|Z + B| \geq K'|Z|$ by minimality of K'.
- By the inductive hypothesis,

$$\begin{aligned}|A' + B + C'| &\leq |A' + B + C| + \big(|A' + B + x| - |Z + B + x|\big)\\ &\leq K'|A' + C| + K'|A'| - K'|Z|.\end{aligned}$$

- It remains to show that

$$|A' + C| + |A'| - |Z| \leq |A' + C'|.$$

Plünnecke inequalities: proof of main lemma II

Lemma (Petridis)

$|A' + B + C| \leq K'|A' + C|$, *where* $\frac{|A' + B|}{|A'|} = K'$, K' *minimal.*

- $A' + B + C' = (A' + B + C) \cup \big((A' + B + x) \setminus (Z + B + x)\big)$, where

$$Z = \{a \in A' : a + B + x \subset A + B + C\}.$$

- $|Z + B| \geq K'|Z|$ by minimality of K'.
- By the inductive hypothesis,

$$|A' + B + C'| \leq |A' + B + C| + \big(|A' + B + x| - |Z + B + x|\big)$$
$$\leq K'|A' + C| + K'|A'| - K'|Z|.$$

- It remains to show that

$$|A' + C| + |A'| - |Z| \leq |A' + C'|.$$

Plünnecke inequalities: proof of main lemma II

Lemma (Petridis)

$$|A' + B + C| \leq K'|A' + C|, \quad \textit{where } \frac{|A' + B|}{|A'|} = K', \ K' \textit{ minimal.}$$

- $A' + B + C' = (A' + B + C) \cup \big((A' + B + x) \setminus (Z + B + x)\big)$, where
$$Z = \{a \in A' : a + B + x \subset A + B + C\}.$$
- $|Z + B| \geq K'|Z|$ by minimality of K'.
- By the inductive hypothesis,
$$\begin{aligned} |A' + B + C'| &\leq |A' + B + C| + \big(|A' + B + x| - |Z + B + x|\big) \\ &\leq K'|A' + C| + K'|A'| - K'|Z|. \end{aligned}$$
- It remains to show that
$$|A' + C| + |A'| - |Z| \leq |A' + C'|.$$

Plünnecke inequalities: proof of main lemma III

Lemma

$$|A' + C| + |A'| - |Z| \leq |A' + C'|,$$

where $Z = \{a \in A' : a + B + x \subset A + B + C\}$.

Proof.

- $$A' + C' = A + C \cup (A + x \setminus W + x),$$

  where $W = \{a \in A' : a + x \in A' + C\}$.

- Since the union is disjoint and $W + x \subset A + x$,

  $$|A' + C'| = |A' + C| + |A'| - |W|.$$

- But $W \subset Z$ since $a + x \in A' + C \Rightarrow a + B + x \subset A + B + C$. So

  $$|A' + C'| \geq |A' + C| + |A'| - |Z|.$$

Plünnecke inequalities: proof of main lemma III

Lemma

$$|A' + C| + |A'| - |Z| \le |A' + C'|,$$

where $Z = \{a \in A' : a + B + x \subset A + B + C\}$.

Proof.

- $$A' + C' = A + C \cup (A + x \setminus W + x),$$

  where $W = \{a \in A' : a + x \in A' + C\}$.
- Since the union is disjoint and $W + x \subset A + x$,

  $$|A' + C'| = |A' + C| + |A'| - |W|.$$

- But $W \subset Z$ since $a + x \in A' + C \Rightarrow a + B + x \subset A + B + C$. So

  $$|A' + C'| \ge |A' + C| + |A'| - |Z|.$$

Plünnecke inequalities: proof of main lemma III

Lemma

$$|A' + C| + |A'| - |Z| \leq |A' + C'|,$$

where $Z = \{a \in A' : a + B + x \subset A + B + C\}$.

Proof.

- $$A' + C' = A + C \cup (A + x \setminus W + x),$$

  where $W = \{a \in A' : a + x \in A' + C\}$.
- Since the union is disjoint and $W + x \subset A + x$,

  $$|A' + C'| = |A' + C| + |A'| - |W|.$$
- But $W \subset Z$ since $a + x \in A' + C \Rightarrow a + B + x \subset A + B + C$. So

  $$|A' + C'| \geq |A' + C| + |A'| - |Z|.$$

Plünnecke inequalities: proof of main lemma III

Lemma

$$|A' + C| + |A'| - |Z| \leq |A' + C'|,$$

where $Z = \{a \in A' : a + B + x \subset A + B + C\}$.

Proof.

- $$A' + C' = A + C \cup \left(A + x \setminus W + x\right),$$

  where $W = \{a \in A' : a + x \in A' + C\}$.
- Since the union is disjoint and $W + x \subset A + x$,

  $$|A' + C'| = |A' + C| + |A'| - |W|.$$

- But $W \subset Z$ since $a + x \in A' + C \Rightarrow a + B + x \subset A + B + C$. So

  $$|A' + C'| \geq |A' + C| + |A'| - |Z|.$$

Plünnecke inequalities: proof of main lemma III

Lemma

$$|A' + C| + |A'| - |Z| \leq |A' + C'|,$$

where $Z = \{a \in A' : a + B + x \subset A + B + C\}$.

Proof.

- $$A' + C' = A + C \cup \left(A + x \setminus W + x\right),$$
  where $W = \{a \in A' : a + x \in A' + C\}$.
- Since the union is disjoint and $W + x \subset A + x$,
  $$|A' + C'| = |A' + C| + |A'| - |W|.$$
- But $W \subset Z$ since $a + x \in A' + C \Rightarrow a + B + x \subset A + B + C$. So
  $$|A' + C'| \geq |A' + C| + |A'| - |Z|.$$

Plünnecke inequalities: connections

- The Plünnecke inequalities are a key component of all the quantitative proofs of Freiman's Theorem.
- Usually one uses the contrapositive: in order to prove that

$$|A + A| \gg |A|,$$

it is enough to prove that

$$|A + A + \cdots + A| \gg |A|,$$

which is easier since repeated sumsets have far more structure/smoothness.
- There is a useful version of Plünnecke's inequalities (due to Kaimanovich-Vershik) for entropy, with convolutions of measures in place of sumsets.

Plünnecke inequalities: connections

- The Plünnecke inequalities are a key component of all the quantitative proofs of Freiman's Theorem.
- Usually one uses the contrapositive: in order to prove that

$$|A+A| \gg |A|,$$

it is enough to prove that

$$|A+A+\cdots+A| \gg |A|,$$

which is easier since repeated sumsets have far more structure/smoothness.
- There is a useful version of Plünnecke's inequalities (due to Kaimanovich-Vershik) for entropy, with convolutions of measures in place of sumsets.

Plünnecke inequalities: connections

- The Plünnecke inequalities are a key component of all the quantitative proofs of Freiman's Theorem.
- Usually one uses the contrapositive: in order to prove that

$$|A+A| \gg |A|,$$

it is enough to prove that

$$|A+A+\cdots+A| \gg |A|,$$

which is easier since repeated sumsets have far more structure/smoothness.
- There is a useful version of Plünnecke's inequalities (due to Kaimanovich-Vershik) for entropy, with convolutions of measures in place of sumsets.

No Plünnecke inequalities for Hausdorff dimension

Theorem (T. Körner 2010, J. Schmeling-P.S. 2012)

For any non-decreasing sequence α_n of numbers in $[0,1]$ there exists a compact set A such that

$$\dim_H \left(\underbrace{A + \cdots + A}_{n \text{ times}} \right) = \alpha_n.$$

Remark

- *Körner proved the result first but we were not aware of it; the constructions are different.*
- *We also show that there are no Plünnecke inequalities for upper box dimension, but they do hold for lower box dimension.*

No Plünnecke inequalities for Hausdorff dimension

Theorem (T. Körner 2010, J. Schmeling-P.S. 2012)

For any non-decreasing sequence α_n *of numbers in* $[0,1]$ *there exists a compact set A such that*

$$\dim_H \left(\underbrace{A + \cdots + A}_{n \text{ times}} \right) = \alpha_n.$$

Remark

- *Körner proved the result first but we were not aware of it; the constructions are different.*
- *We also show that there are no Plünnecke inequalities for upper box dimension, but they do hold for lower box dimension.*

No Plünnecke inequalities for Hausdorff dimension

Theorem (T. Körner 2010, J. Schmeling-P.S. 2012)

For any non-decreasing sequence α_n of numbers in $[0,1]$ there exists a compact set A such that

$$\dim_H \left(\underbrace{A + \cdots + A}_{n \text{ times}} \right) = \alpha_n.$$

Remark

- *Körner proved the result first but we were not aware of it; the constructions are different.*
- *We also show that there are no Plünnecke inequalities for upper box dimension, but they do hold for lower box dimension.*

No Plünnecke inequalities for Hausdorff dimension

Theorem (T. Körner 2010, J. Schmeling-P.S. 2012)

For any non-decreasing sequence α_n of numbers in $[0,1]$ there exists a compact set A such that

$$\dim_H \left(\underbrace{A + \cdots + A}_{n \text{ times}} \right) = \alpha_n.$$

Remark

- *Körner proved the result first but we were not aware of it; the constructions are different.*
- *We also show that there are no Plünnecke inequalities for upper box dimension, but they do hold for lower box dimension.*

Outline

Some jewels of additive combinatorics

Szemerédi's Theorem: Dense subsets of $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}$ contain arbitrarily long arithmetic progressions.

Freiman's Theorem: Sets with $|A+A| \le K|A|$ can be densely embedded in a GAP.

Plünnecke's Inequalities: If $A+A$ is small, so are $A+A+A$ and nA for all n.

Szemerédi's Theorem: Dense subsets of $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}$ contain arbitrarily long arithmetic progressions.

Freiman's Theorem: Sets with $|A+A| \leq K|A|$ can be densely embedded in a GAP.

Plünnecke's Inequalities: If $A+A$ is small, so are $A+A+A$ and nA for all n.

Szemerédi's Theorem: Dense subsets of $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}$ contain arbitrarily long arithmetic progressions.

Freiman's Theorem: Sets with $|A + A| \leq K|A|$ can be densely embedded in a GAP.

Plünnecke's Inequalities: If $A + A$ is small, so are $A + A + A$ and nA for all n.