Unic 2025-1

2025年6月11日 22:37

# Additive combinatorics

(Meng Wu)

(meng.wu@oulu.fi)

23/June

Introduction to additive combinatorics (basic notion, problems, ideas)
applications to fractal geometry (selfsimilar sets, fractal dimensions...)

fractal dimension of selfsimilar sets

Measure theory / additive combinatorics

Some references:

T. Tao & V. Vu Additive combinatorics, Cambridge studies in advanced math vol 105, 2006

B. Green Additive comb, lecture notes (online)

M. Hochman. Selfsimilar sets, entropy and add comb, exposition article arXiv 1307.6399

Today: Basic objects in AC

Next week: introduction. selfsimilar sets, fractal dimension, entropy.

## Additive combinatorics

# Size of sumsets and the inverse problem

The sumset of $A, B \subset \mathbb{R}^d$, $A, B \neq \phi$, is defined by

$$A+B := \{a+b : a \in A,\ b \in B\}$$

main topic in AC.

Inverse problem: If $A+B$ is 'small' (in cardinality, volume, dimension) compared to $A$ and $B$, then what kind of structures the sets $A$ & $B$ must have?

$$|A+B| \leq \overset{100000}{C}|A|,\ C|B|,$$

$|\cdot| \to$ cardinality, volume

We shall see: If $A+B$ is 'small' compared to $A$ and $B$, then $A$ and $B$ must have some form of algebraic/arithmetic features

$A, B \subset \mathbb{R}^d$, finite sets

$$A+B = \left\{a+b : \begin{matrix} a \in A \\ b \in B \end{matrix}\right\} = \bigcup_{b \in B}(A+b)$$

Lemma: If $A, B \subset \mathbb{R}^d$ are finite and non-empty, then

$$\max\{|A|, |B|\} \leq |A+B| \leq |A||B|$$

$$|A+b| = |A| \quad \forall b \in B$$

$$|A+B| = \left|\bigcup_{b \in B}(A+b)\right| \leq \sum_{b \in B}|A+b| = |B| \times |A|$$

Remark: (1) $|A+B| = |A|$ or $|B| \iff A$ or $B$ is a singleton

(2) $|A+B| = |A||B| \iff$ every element in $A+B$ is uniquely represented

$\iff$ if $a+b = a'+b'$ for $a', a \in A$, $b', b \in B$, then $\begin{matrix} a = a' \\ b = b' \end{matrix}$

$\Leftrightarrow$ if $a+b = a'+b'$ for $a', a \in A$, $b', b \in B$, then $a = a'$, $b = b'$

$A = \{0, q, q^2, \dots, q^n\}$ and $B = \{0, 1, 2, \dots, q-1\}$ $q, n \in \mathbb{N}$

$|A+B| = |A||B|$ (Exercise)

$|A+B| \leq \Theta |A|$

If we consider "random" subsets of $\mathbb{Z}^d$, then one would expect

$$|A+B| \approx |A||B| \qquad |A+B| \leq c|A|, \ c|B|$$

Example: If $n$ is fixed, $A, B \subset \{1, \dots, n\}$ and choose randomly such that each index $j \in \{1, \dots, n\}$ is chosen with probability $0<p<1$, then the event

$$|A+B| \geq c|A||B|$$

for some constant $c>0$ occurs with high probability

$$\mathbb{P}\left( \omega : |A_\omega + B_\omega| \geq \varepsilon |A_\omega||B_\omega| \right\} \geq 1 - o_\varepsilon(1)$$

$\varepsilon = \frac{1}{1000}$ $\quad$ $\varepsilon \perp\!\!\!\perp n$

What happens when $|A+B| << |A||B|$ ?

$|A+B| \leq c|A|, c|B|$ ?

Minimal growth: Arithmetic progression and Cauchy–Davenport inequality

Classical result: Brunn–Minkowski inequality

...

Thm If $A, B \subset \mathbb{R}^d$ are convex, then

$$\mathrm{Vol}(A+B) \geq \left(\mathrm{Vol}(A)^{\frac{1}{d}} + \mathrm{Vol}(B)^{\frac{1}{d}}\right)^d$$

Moreover, this is an equality $\iff$ $A$ and $B$ are homothetic

$\mathrm{Vol}(A+B)$ is minimal $\Rightarrow$ $A$ and $B$ are similar

Discrete analogue of a convex set is an arithmetic progression

Def: Any set $P \subset \mathbb{R}$ of the form

$$P = \{a, a+p, a+2p, \dots, a+(k-1)p\}$$

for some $p \in \mathbb{R}$ and $k \in \mathbb{N}$ is called an arithmetic progression (AP) of gap $p$ and length $k$. Moreover, an AP in $\mathbb{R}^d$ is any product of $d$ AP in $\mathbb{R}$

AP in $\mathbb{R}^d$: $P = \{a, a+p, \dots, a+(k-1)p\}$ $\quad p \in \mathbb{R}^d$, $a \in \mathbb{R}^d$

Cauchy–Davenport inequality

Thm If $A, B \subset \mathbb{R}$ are finite with $|A|, |B| \geq 2$, then

$$|A+B| \geq |A| + |B| - 1$$

Exercise

Moreover, this is an equality if and only if $A$ and $B$ are APs of the same gap

Linear growth: Generalised APs and Freiman's thm

## Linear growth: Generalized APs and Freiman's thm

Let's first $A=B$, $|A+A| \le c|A| \Rightarrow ?$

**Def** We say a finite set $A \subset \mathbb{R}^d$ is small doubling with a constant $c>0$ if

$$|A+A| \le c|A|$$

$A+A$

**Note** . $C = |A|$ $\quad |A+A| \le |A|^2 = c|A|$

$C = 10000$
$|A| \longrightarrow \infty$

**Example**: If $A$ is an AP, then by Cauchy-Davenport

$$|A+A| = 2|A|-1 \le 2|A|$$

So $A$ is small doubling with $c=2$
Moreover, in higher dimension if $A \subset \mathbb{R}^d$ is AP, then

$$|A+A| \le 2^d|A| \quad (\text{Exercise})$$

Eg: if $A = \{1, \dots, n\}^d \subset \mathbb{R}^d$ then $|A+A| = |\{2, 3, \dots, 2n\}^d|$

$$\le 2^d |A|$$

Sometimes, we do not have a set $A$, which is AP, but still satisfies $|A+A| \le 2^k|A|$ for some $k>d$. $\longrightarrow$ generalized AP

**Def** (generalized AP)

A finite set $A \subset \mathbb{R}$ is a generalized AP (GAP) of rank $k \in \mathbb{N}$ if

A finite set $A \subset \mathbb{R}$ is a generalized AP (GAP) of rank $k \in \mathbb{N}$ if

$$A = \left\{ a + \sum_{i=1}^{k} k_i p_i : k_i = 0, 1, \dots, n \right\}$$

for some gaps $p_i > 0$ and $N_i \in \mathbb{N}$, $v \in \mathbb{N}$

$$|A+A| \leq 2^k |A|$$

Fact: If $A$ is a GAP of rank $k$, then

$$|A+A| \leq 2^k |A| \quad (\text{Exercise})$$

Example: If $A$ is small doubling with $C > 0$ and $A' \subset A$ satisfying $|A'| \geq \rho |A|$ for some $0 < \rho \leq 1$. Then $A'$ is small doubling with constant $C/\rho$:

$$|A'+A'| \leq |A+A| \leq C|A| \leq \frac{C}{\rho}|A'|$$

Theorem (Freiman) If $A \subset \mathbb{R}^d$ is finite and small doubling with doubling constant $C > 0$, then $A \subset P$ for GAP of rank $k$ and cardinality $|P| \leq C' |A|$ for some $k \in \mathbb{N}$ and $C'$ that only depend on $C$

$\left( k = O(\log_2 C (1 + \log C)),\ C' = O(C^{O(1)}) \right)$

Proof (Tao-Vu)

$$|A+A| \leq |A|^{1+o(1)} \qquad C|A| \qquad |A||A|^{o(1)}$$