

An Introduction to Arithmetic Combinatorics

Chris Pryby
Georgia Institute of Technology

February 7, 2012

What is Arithmetic Combinatorics?

- Study of arithmetic structure in (finite) sets

What is Arithmetic Combinatorics?

- Study of arithmetic structure in (finite) sets
- Examples:

What is Arithmetic Combinatorics?

- Study of arithmetic structure in (finite) sets
- Examples:
 - $\{3, 6, 9, 12, 15, 18, 21, 24\}$

What is Arithmetic Combinatorics?

- Study of arithmetic structure in (finite) sets
- Examples:
 - $\{3, 6, 9, 12, 15, 18, 21, 24\}$
 - $\{2, 4, 8, 16, 32, 64, 128, 256\}$

What is Arithmetic Combinatorics?

- Study of arithmetic structure in (finite) sets
- Examples:
 - $\{3, 6, 9, 12, 15, 18, 21, 24\}$
 - $\{2, 4, 8, 16, 32, 64, 128, 256\}$
 - $\{2, 6, 7, 9, 12, 43, 51, 96, 100\}$

What is Arithmetic Combinatorics?

- Study of arithmetic structure in (finite) sets
- Examples:
 - $\{3, 6, 9, 12, 15, 18, 21, 24\}$
 - $\{2, 4, 8, 16, 32, 64, 128, 256\}$
 - $\{2, 6, 7, 9, 12, 43, 51, 96, 100\}$
 - $\{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots, 104729\}$

What is Arithmetic Combinatorics?

- Study of arithmetic structure in (finite) sets
- Examples:
 - $\{3, 6, 9, 12, 15, 18, 21, 24\}$
 - $\{2, 4, 8, 16, 32, 64, 128, 256\}$
 - $\{2, 6, 7, 9, 12, 43, 51, 96, 100\}$
 - $\{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots, 104729\}$
- What do we mean by arithmetic structure?

Defining Additive Structure

- G , an additive abelian group

Defining Additive Structure

- G , an additive abelian group
- A, B , nonempty finite subsets of G

Defining Additive Structure

- G , an additive abelian group
- A, B , nonempty finite subsets of G
- $A + B = \{a + b : a \in A, b \in B\}$, the *sumset* of A with B

Defining Additive Structure

- G , an additive abelian group
- A, B , nonempty finite subsets of G
- $A + B = \{a + b : a \in A, b \in B\}$, the *sumset* of A with B
- $A - B = \{a - b : a \in A, b \in B\}$, the *difference set*

Defining Additive Structure

- G , an additive abelian group
- A, B , nonempty finite subsets of G
- $A + B = \{a + b : a \in A, b \in B\}$, the *sumset* of A with B
- $A - B = \{a - b : a \in A, b \in B\}$, the *difference set*
- If $k \in \mathbb{N}$, then we have the iterated sumset

$$kA = \underbrace{A + A + \cdots + A}_{k \text{ times}} = \{a_1 + a_2 + \cdots + a_k : a_i \in A\}$$

Defining Additive Structure

- G , an additive abelian group
- A, B , nonempty finite subsets of G
- $A + B = \{a + b : a \in A, b \in B\}$, the *sumset* of A with B
- $A - B = \{a - b : a \in A, b \in B\}$, the *difference set*
- If $k \in \mathbb{N}$, then we have the iterated sumset

$$kA = \underbrace{A + A + \cdots + A}_{k \text{ times}} = \{a_1 + a_2 + \cdots + a_k : a_i \in A\}$$

- If $k \in \mathbb{Z}$, can also define the *dilation* of A by k :

$$k \cdot A = \{ka : a \in A\}.$$

Classifying Strength of Additive Structure

- Sets with strong additive structure

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$
 - Subgroups of G

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$
 - Subgroups of G
 - If $A \leq G$, then $A + A = A$.

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$
 - Subgroups of G
 - If $A \leq G$, then $A + A = A$.
- Sets with weak additive structure

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$
 - Subgroups of G
 - If $A \leq G$, then $A + A = A$.
- Sets with weak additive structure
 - Random sets

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$
 - Subgroups of G
 - If $A \leq G$, then $A + A = A$.
- Sets with weak additive structure
 - Random sets
 - Geometric progressions in \mathbb{Z}

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$
 - Subgroups of G
 - If $A \leq G$, then $A + A = A$.
- Sets with weak additive structure
 - Random sets
 - Geometric progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, ar, ar^2, \dots, ar^{N-1}\}$

Classifying Strength of Additive Structure

- Sets with strong additive structure
 - Arithmetic progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, a + r, a + 2r, \dots, a + (N - 1)r\}$
 - $A + A = \{a, a + r, a + 2r, \dots, a + 2(N - 1)r\}$
 - $|A + A| = 2|A| - 1$
 - Subgroups of G
 - If $A \leq G$, then $A + A = A$.
- Sets with weak additive structure
 - Random sets
 - Geometric progressions in \mathbb{Z}
 - Given $a, r \in \mathbb{Z}$, $A = \{a, ar, ar^2, \dots, ar^{N-1}\}$
 - $|A + A| = \frac{|A|(|A|+1)}{2}$

The Doubling Constant

- $\sigma[A] = \frac{|A+A|}{|A|}$

The Doubling Constant

- $\sigma[A] = \frac{|A+A|}{|A|}$
- Maximum possible: $\sigma[A] = \frac{|A|+1}{2}$

The Doubling Constant

- $\sigma[A] = \frac{|A+A|}{|A|}$
- Maximum possible: $\sigma[A] = \frac{|A|+1}{2}$
- Sets attaining this upper bound are called *Sidon sets*

The Doubling Constant

- $\sigma[A] = \frac{|A+A|}{|A|}$
- Maximum possible: $\sigma[A] = \frac{|A|+1}{2}$
- Sets attaining this upper bound are called *Sidon sets*
 - Geometric progressions in \mathbb{Z}

The Doubling Constant

- $\sigma[A] = \frac{|A+A|}{|A|}$
- Maximum possible: $\sigma[A] = \frac{|A|+1}{2}$
- Sets attaining this upper bound are called *Sidon sets*
 - Geometric progressions in \mathbb{Z}
 - Sets of N real numbers chosen uniformly at random from $[0, 1]$

The Doubling Constant

- $\sigma[A] = \frac{|A+A|}{|A|}$
- Maximum possible: $\sigma[A] = \frac{|A|+1}{2}$
- Sets attaining this upper bound are called *Sidon sets*
 - Geometric progressions in \mathbb{Z}
 - Sets of N real numbers chosen uniformly at random from $[0, 1]$
- Minimum possible: $\sigma[A] = 1$

The Doubling Constant

- $\sigma[A] = \frac{|A+A|}{|A|}$
- Maximum possible: $\sigma[A] = \frac{|A|+1}{2}$
- Sets attaining this upper bound are called *Sidon sets*
 - Geometric progressions in \mathbb{Z}
 - Sets of N real numbers chosen uniformly at random from $[0, 1]$
- Minimum possible: $\sigma[A] = 1$
 - Subgroups $A \leq G$ (and cosets of subgroups)

The Difference Constant

- $\delta[A] = \frac{|A-A|}{|A|}$

The Difference Constant

- $\delta[A] = \frac{|A-A|}{|A|}$
- $1 \leq \delta[A] \leq |A| - 1 + \frac{1}{|A|}$

The Difference Constant

- $\delta[A] = \frac{|A-A|}{|A|}$
- $1 \leq \delta[A] \leq |A| - 1 + \frac{1}{|A|}$
 - Sidon sets attain the upper bound

The Difference Constant

- $\delta[A] = \frac{|A-A|}{|A|}$
- $1 \leq \delta[A] \leq |A| - 1 + \frac{1}{|A|}$
 - Sidon sets attain the upper bound
 - Cosets of subgroups attain the lower bound

The Difference Constant

- $\delta[A] = \frac{|A-A|}{|A|}$
- $1 \leq \delta[A] \leq |A| - 1 + \frac{1}{|A|}$
 - Sidon sets attain the upper bound
 - Cosets of subgroups attain the lower bound
- Idea: sets with doubling constants near 1 behave almost like groups (up to translations)

The Difference Constant

- $\delta[A] = \frac{|A-A|}{|A|}$
- $1 \leq \delta[A] \leq |A| - 1 + \frac{1}{|A|}$
 - Sidon sets attain the upper bound
 - Cosets of subgroups attain the lower bound
- Idea: sets with doubling constants near 1 behave almost like groups (up to translations)
- Study of sets with doubling constants near $|A|$ not (presently) tractable

Ruzsa Triangle Inequality

- Fundamental result in additive combinatorics

Ruzsa Triangle Inequality

- Fundamental result in additive combinatorics

Theorem

If U, V, W are finite subsets of an additive abelian group, then

$$|U||V - W| \leq |U - V||U - W|.$$

Ruzsa Triangle Inequality

- Fundamental result in additive combinatorics

Theorem

If U, V, W are finite subsets of an additive abelian group, then

$$|U||V - W| \leq |U - V||U - W|.$$

Proof.

Define $\varphi : U \times (V - W) \rightarrow (U - V) \times (U - W)$ as follows: given $x \in V - W$, choose $v_x \in V$ and $w_x \in W$ such that $v_x - w_x = x$. Then take $\varphi(u, x) = (u - v_x, u - w_x)$. Easy to show that φ is well-defined and injective. □

Ruzsa Triangle Inequality

- Fundamental result in additive combinatorics

Theorem

If U, V, W are finite subsets of an additive abelian group, then

$$|U| |V - W| \leq |U - V| |U - W|.$$

Proof.

Define $\varphi : U \times (V - W) \rightarrow (U - V) \times (U - W)$ as follows: given $x \in V - W$, choose $v_x \in V$ and $w_x \in W$ such that $v_x - w_x = x$. Then take $\varphi(u, x) = (u - v_x, u - w_x)$. Easy to show that φ is well-defined and injective. □

- Can rewrite inequality:

$$\log \frac{|V - W|}{|V|^{1/2} |W|^{1/2}} \leq \log \frac{|U - V|}{|U|^{1/2} |V|^{1/2}} + \log \frac{|U - W|}{|U|^{1/2} |W|^{1/2}}$$

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
 - Satisfies most axioms of a true metric

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
 - Satisfies most axioms of a true metric
 - $d(A, A)$ need not be 0 (unless A is a coset of a subgroup)

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
 - Satisfies most axioms of a true metric
 - $d(A, A)$ need not be 0 (unless A is a coset of a subgroup)
- Idea: if $d(A, B)$ is small, then A and B have similar additive structure

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
 - Satisfies most axioms of a true metric
 - $d(A, A)$ need not be 0 (unless A is a coset of a subgroup)
- Idea: if $d(A, B)$ is small, then A and B have similar additive structure
- Can use Ruzsa distance to relate $\delta[A]$ and $\sigma[A]$

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
 - Satisfies most axioms of a true metric
 - $d(A, A)$ need not be 0 (unless A is a coset of a subgroup)
- Idea: if $d(A, B)$ is small, then A and B have similar additive structure
- Can use Ruzsa distance to relate $\delta[A]$ and $\sigma[A]$
 - $d(A, A) = \log \delta[A]$

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
 - Satisfies most axioms of a true metric
 - $d(A, A)$ need not be 0 (unless A is a coset of a subgroup)
- Idea: if $d(A, B)$ is small, then A and B have similar additive structure
- Can use Ruzsa distance to relate $\delta[A]$ and $\sigma[A]$
 - $d(A, A) = \log \delta[A]$
 - $d(A, -A) = \log \sigma[A]$

Ruzsa Distance

- $d(A, B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
 - Satisfies most axioms of a true metric
 - $d(A, A)$ need not be 0 (unless A is a coset of a subgroup)
- Idea: if $d(A, B)$ is small, then A and B have similar additive structure
- Can use Ruzsa distance to relate $\delta[A]$ and $\sigma[A]$
 - $d(A, A) = \log \delta[A]$
 - $d(A, -A) = \log \sigma[A]$
 - Triangle inequality: $d(A, C) \leq d(A, B) + d(B, C)$

$$d(A, A) \leq d(A, -A) + d(-A, A)$$

$$\log \delta[A] \leq 2 \log \sigma[A]$$

$$\delta[A] \leq \sigma[A]^2$$

Sumset Inequalities

- With more machinery, can establish $\sigma[A] \leq \delta[A]^2$

Sumset Inequalities

- With more machinery, can establish $\sigma[A] \leq \delta[A]^2$
- Ruzsa triple sumset inequality: If $d(U, V), d(U, W), d(V, W) \leq \log(K)$, then $|U + V + W| \leq K^C |U|^{1/3} |V|^{1/3} |W|^{1/3}$

Sumset Inequalities

- With more machinery, can establish $\sigma[A] \leq \delta[A]^2$
- Ruzsa triple sumset inequality: If $d(U, V), d(U, W), d(V, W) \leq \log(K)$, then $|U + V + W| \leq K^C |U|^{1/3} |V|^{1/3} |W|^{1/3}$
- Iterated sumset inequality: If $\sigma A \leq K$ and $k, \ell \geq 0$, then there is a constant $\gamma(k, \ell)$ such that $|kA - \ell A| \leq K^{\gamma(k, \ell)} |A|$

Sumset Inequalities

- With more machinery, can establish $\sigma[A] \leq \delta[A]^2$
- Ruzsa triple sumset inequality: If $d(U, V), d(U, W), d(V, W) \leq \log(K)$, then $|U + V + W| \leq K^C |U|^{1/3} |V|^{1/3} |W|^{1/3}$
- Iterated sumset inequality: If $\sigma A \leq K$ and $k, \ell \geq 0$, then there is a constant $\gamma(k, \ell)$ such that $|kA - \ell A| \leq K^{\gamma(k, \ell)} |A|$
- Plünnecke-Ruzsa: can take $\gamma(k, \ell) = k + \ell$

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$
- $\delta[A, B] = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$
- $\delta[A, B] = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
- Additive energy: $E(A, B) = \# \{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}$

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$
- $\delta[A, B] = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
- Additive energy: $E(A, B) = \# \{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}$
 - Number of solutions to $a + b = a' + b'$, where $a, a' \in A$ and $b, b' \in B$

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$
- $\delta[A, B] = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
- Additive energy: $E(A, B) = \# \{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}$
 - Number of solutions to $a + b = a' + b'$, where $a, a' \in A$ and $b, b' \in B$
 - High additive energy \Leftrightarrow lots of collisions when A and B are added

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$
- $\delta[A, B] = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
- Additive energy: $E(A, B) = \# \{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}$
 - Number of solutions to $a + b = a' + b'$, where $a, a' \in A$ and $b, b' \in B$
 - High additive energy \Leftrightarrow lots of collisions when A and B are added
 - $E(A, B) = \sum_{x \in A+B} r(x)^2$, where $r(x)$ is the number of representations of $x = a + b$, $a \in A, b \in B$

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$
- $\delta[A, B] = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
- Additive energy: $E(A, B) = \# \{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}$
 - Number of solutions to $a + b = a' + b'$, where $a, a' \in A$ and $b, b' \in B$
 - High additive energy \Leftrightarrow lots of collisions when A and B are added
 - $E(A, B) = \sum_{x \in A+B} r(x)^2$, where $r(x)$ is the number of representations of $x = a + b$, $a \in A, b \in B$
 - Cauchy-Schwarz inequality:
 $E(A, B) \leq E(A, A)^{1/2} E(B, B)^{1/2}$

Measuring Additive Structure Between Sets

- $\sigma[A, B] = \frac{|A+B|}{|A|^{1/2}|B|^{1/2}}$
- $\delta[A, B] = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$
- Additive energy: $E(A, B) = \#\{(a, a', b, b') \in A \times A \times B \times B : a + b = a' + b'\}$
 - Number of solutions to $a + b = a' + b'$, where $a, a' \in A$ and $b, b' \in B$
 - High additive energy \Leftrightarrow lots of collisions when A and B are added
 - $E(A, B) = \sum_{x \in A+B} r(x)^2$, where $r(x)$ is the number of representations of $x = a + b$, $a \in A, b \in B$
 - Cauchy-Schwarz inequality:
 $E(A, B) \leq E(A, A)^{1/2} E(B, B)^{1/2}$
- Some easy bounds:
 $|A| |B| \leq E(A, B) \leq |A| |B| \min(|A|, |B|)$

Additive Energy and the Doubling Constant

- If $\sigma[A, B]$ is small, then $E(A, B)$ should be large.

Additive Energy and the Doubling Constant

- If $\sigma[A, B]$ is small, then $E(A, B)$ should be large.

Lemma

If $\sigma[A, B] \leq K$, then $E(A, B) \geq \frac{|A|^{3/2}|B|^{3/2}}{K}$.

Additive Energy and the Doubling Constant

- If $\sigma[A, B]$ is small, then $E(A, B)$ should be large.

Lemma

If $\sigma[A, B] \leq K$, then $E(A, B) \geq \frac{|A|^{3/2}|B|^{3/2}}{K}$.

Proof.

$$E(A, B) = \sum_{x \in A+B} r(x)^2 \geq \frac{1}{|A+B|} \left(\sum_x r(x) \right)^2.$$

by Cauchy-Schwarz. Then use the fact that $|A| |B| = \sum_x r(x)$:

$$\frac{1}{|A+B|} \left(\sum_x r(x) \right)^2 = \frac{|A|^2 |B|^2}{|A+B|} = \frac{|A|^{3/2} |B|^{3/2}}{\sigma[A, B]}.$$



Additive Energy and the Doubling Constant

- If $\sigma[A, B]$ is small, then $E(A, B)$ should be large.

Lemma

If $\sigma[A, B] \leq K$, then $E(A, B) \geq \frac{|A|^{3/2}|B|^{3/2}}{K}$.

Proof.

$$E(A, B) = \sum_{x \in A+B} r(x)^2 \geq \frac{1}{|A+B|} \left(\sum_x r(x) \right)^2.$$

by Cauchy-Schwarz. Then use the fact that $|A| |B| = \sum_x r(x)$:

$$\frac{1}{|A+B|} \left(\sum_x r(x) \right)^2 = \frac{|A|^2 |B|^2}{|A+B|} = \frac{|A|^{3/2} |B|^{3/2}}{\sigma[A, B]}.$$



- Consequence: if $\sigma[A] \leq K$, then $E(A, A) \geq \frac{|A|^3}{K}$.

Additive Energy and the Doubling Constant

- If $E(A, B)$ is large, need $\sigma[A, B]$ be small?

Additive Energy and the Doubling Constant

- If $E(A, B)$ is large, need $\sigma[A, B]$ be small?
- $A_1 = \{1, 2, \dots, n\}$

Additive Energy and the Doubling Constant

- If $E(A, B)$ is large, need $\sigma[A, B]$ be small?
- $A_1 = \{1, 2, \dots, n\}$
- $A_2 = \{2^{k+1}, \dots, 2^{k+n}\}$, $k = \lfloor \log_2(2n) \rfloor$

Additive Energy and the Doubling Constant

- If $E(A, B)$ is large, need $\sigma[A, B]$ be small?
- $A_1 = \{1, 2, \dots, n\}$
- $A_2 = \{2^{k+1}, \dots, 2^{k+n}\}$, $k = \lfloor \log_2(2n) \rfloor$
- $A = A_1 \cup A_2$

Additive Energy and the Doubling Constant

- If $E(A, B)$ is large, need $\sigma[A, B]$ be small?
- $A_1 = \{1, 2, \dots, n\}$
- $A_2 = \{2^{k+1}, \dots, 2^{k+n}\}$, $k = \lfloor \log_2(2n) \rfloor$
- $A = A_1 \cup A_2$
- $E(A, A) \approx \frac{1}{24} |A|^3$, but $\sigma[A] \approx \frac{1}{8} |A|$

Additive Energy and the Doubling Constant

- If $E(A, B)$ is large, need $\sigma[A, B]$ be small?
- $A_1 = \{1, 2, \dots, n\}$
- $A_2 = \{2^{k+1}, \dots, 2^{k+n}\}$, $k = \lfloor \log_2(2n) \rfloor$
- $A = A_1 \cup A_2$
- $E(A, A) \approx \frac{1}{24} |A|^3$, but $\sigma[A] \approx \frac{1}{8} |A|$
- Observation: most of the collisions are coming from a subset: the arithmetic progression A_1

Additive Energy and the Doubling Constant

- If $E(A, B)$ is large, need $\sigma[A, B]$ be small?
- $A_1 = \{1, 2, \dots, n\}$
- $A_2 = \{2^{k+1}, \dots, 2^{k+n}\}$, $k = \lfloor \log_2(2n) \rfloor$
- $A = A_1 \cup A_2$
- $E(A, A) \approx \frac{1}{24} |A|^3$, but $\sigma[A] \approx \frac{1}{8} |A|$
- Observation: most of the collisions are coming from a subset: the arithmetic progression A_1
- Does this always happen?

The Balog-Szemerédi-Gowers Theorem

- Answer: Yes

The Balog-Szemerédi-Gowers Theorem

- Answer: Yes

Theorem (BSG)

There are constants $c = c(K)$, $C = C(K)$ such that if

$$E(A, B) \geq \frac{|A|^{3/2} |B|^{3/2}}{K},$$

then there are sets $A' \subseteq A$ and $B' \subseteq B$ with $|A'| \geq \frac{|A|}{c}$, $|B'| \geq \frac{|B|}{c}$ such that

$$\sigma[A', B'] \leq C.$$

The Balog-Szemerédi-Gowers Theorem

- Answer: Yes

Theorem (BSG)

There are constants $c = c(K)$, $C = C(K)$ such that if

$$E(A, B) \geq \frac{|A|^{3/2} |B|^{3/2}}{K},$$

then there are sets $A' \subseteq A$ and $B' \subseteq B$ with $|A'| \geq \frac{|A|}{c}$, $|B'| \geq \frac{|B|}{c}$ such that

$$\sigma[A', B'] \leq C.$$

- If $E(A, B)$ is close to its max, then there are slightly smaller subsets of A and B where additive structure is concentrated

The Balog-Szemerédi-Gowers Theorem

- Answer: Yes

Theorem (BSG)

There are constants $c = c(K)$, $C = C(K)$ such that if

$$E(A, B) \geq \frac{|A|^{3/2} |B|^{3/2}}{K},$$

then there are sets $A' \subseteq A$ and $B' \subseteq B$ with $|A'| \geq \frac{|A|}{c}$, $|B'| \geq \frac{|B|}{c}$ such that

$$\sigma[A', B'] \leq C.$$

- If $E(A, B)$ is close to its max, then there are slightly smaller subsets of A and B where additive structure is concentrated
- Single-set version: if $E(A, A)$ is large, then there is a single subset $A' \subseteq A$ with strong additive structure

- What more can be said about sets with small doubling?

More on Small Doubling

- What more can be said about sets with small doubling?
- Small doubling is “hereditary”

- What more can be said about sets with small doubling?
- Small doubling is “hereditary”
 - If $A' \subseteq A$, $|A'| = \theta |A|$, then $\sigma[A'] \leq \sigma[A]/\theta$

- What more can be said about sets with small doubling?
- Small doubling is “hereditary”
 - If $A' \subseteq A$, $|A'| = \theta |A|$, then $\sigma[A'] \leq \sigma[A]/\theta$
- Is there a set at the top of the hierarchy?

- $\mathbb{F}_2^\infty = \{(a_n)_{n=1}^\infty : a_n \in \mathbb{F}_2\}$

- $\mathbb{F}_2^\infty = \{(a_n)_{n=1}^\infty : a_n \in \mathbb{F}_2\}$

Theorem (Rusza)

If $A \subseteq \mathbb{F}_2^\infty$ is a finite set with $\sigma[A] \leq K$, then A is contained inside some subspace H with $|H| \leq 2^C |A|$, where $C = C(K)$ is a constant dependent on K .

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$
 - $|A| = 4(n + 1)$

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$
 - $|A| = 4(n + 1)$
 - $|A + A| = 7(2n + 1), \sigma[A] \approx 3.5$

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$
 - $|A| = 4(n + 1)$
 - $|A + A| = 7(2n + 1), \sigma[A] \approx 3.5$
- Generalized arithmetic progression (GAP):
 $A = \{x_0 + l_1x_1 + l_2x_2 + \dots + l_dx_d : 0 \leq l_i < L_i\}$

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$
 - $|A| = 4(n + 1)$
 - $|A + A| = 7(2n + 1), \sigma[A] \approx 3.5$
- Generalized arithmetic progression (GAP):
 $A = \{x_0 + l_1x_1 + l_2x_2 + \dots + l_dx_d : 0 \leq l_i < L_i\}$
 - The *dimension* of A is d

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$
 - $|A| = 4(n + 1)$
 - $|A + A| = 7(2n + 1), \sigma[A] \approx 3.5$
- Generalized arithmetic progression (GAP):
 $A = \{x_0 + l_1x_1 + l_2x_2 + \dots + l_dx_d : 0 \leq l_i < L_i\}$
 - The *dimension* of A is d
 - A is *proper* if $|A| = L_1L_2 \dots L_d$

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$
 - $|A| = 4(n + 1)$
 - $|A + A| = 7(2n + 1), \sigma[A] \approx 3.5$
- Generalized arithmetic progression (GAP):
 $A = \{x_0 + \ell_1 x_1 + \ell_2 x_2 + \dots + \ell_d x_d : 0 \leq \ell_i < L_i\}$
 - The *dimension* of A is d
 - A is *proper* if $|A| = L_1 L_2 \dots L_d$
 - $A + A = \{2x_0 + \ell_1 x_1 + \ell_2 x_2 + \dots + \ell_d x_d : 0 \leq \ell_i < 2L_i - 1\}$

Small Doubling in \mathbb{Z}

- Already saw that arithmetic progressions have doubling constant ≈ 2
- $A = \{0, 1, 2, 3, 10, 11, 12, 13, \dots, 10n, 10n + 1, 10n + 2, 10n + 3\}$
 - $|A| = 4(n + 1)$
 - $|A + A| = 7(2n + 1), \sigma[A] \approx 3.5$
- Generalized arithmetic progression (GAP):
 $A = \{x_0 + \ell_1 x_1 + \ell_2 x_2 + \dots + \ell_d x_d : 0 \leq \ell_i < L_i\}$
 - The *dimension* of A is d
 - A is *proper* if $|A| = L_1 L_2 \dots L_d$
 - $A + A = \{2x_0 + \ell_1 x_1 + \ell_2 x_2 + \dots + \ell_d x_d : 0 \leq \ell_i < 2L_i - 1\}$
 - $\sigma[A] \leq 2^d$ if A is proper

Small Doubling in \mathbb{Z}

- Are there other sets in \mathbb{Z} with small doubling?

Small Doubling in \mathbb{Z}

- Are there other sets in \mathbb{Z} with small doubling?
- Answer: No

Small Doubling in \mathbb{Z}

- Are there other sets in \mathbb{Z} with small doubling?
- Answer: No

Theorem (Freiman-Ruzsa-Chang)

If $A \subseteq \mathbb{Z}$ is a finite set with $\sigma A \leq K$, then there is a GAP P containing A such that $\dim(P) \leq CK^C$ and $|P| \leq e^{CK^c} |A|$.

Small Doubling in \mathbb{Z}

- Are there other sets in \mathbb{Z} with small doubling?
- Answer: No

Theorem (Freiman-Ruzsa-Chang)

If $A \subseteq \mathbb{Z}$ is a finite set with $\sigma A \leq K$, then there is a GAP P containing A such that $\dim(P) \leq CK^C$ and $|P| \leq e^{CK^c} |A|$.

- Novel idea: Freiman (1966) treated sets of integers as intrinsic objects (not embedded in \mathbb{Z})

Small Doubling in \mathbb{Z}

- Are there other sets in \mathbb{Z} with small doubling?
- Answer: No

Theorem (Freiman-Ruzsa-Chang)

If $A \subseteq \mathbb{Z}$ is a finite set with $\sigma A \leq K$, then there is a GAP P containing A such that $\dim(P) \leq CK^C$ and $|P| \leq e^{CK^c} |A|$.

- Novel idea: Freiman (1966) treated sets of integers as intrinsic objects (not embedded in \mathbb{Z})
- Generalized the notion of group homomorphism and isomorphism

Small Doubling in \mathbb{Z}

- Are there other sets in \mathbb{Z} with small doubling?
- Answer: No

Theorem (Freiman-Ruzsa-Chang)

If $A \subseteq \mathbb{Z}$ is a finite set with $\sigma A \leq K$, then there is a GAP P containing A such that $\dim(P) \leq CK^C$ and $|P| \leq e^{CK^c} |A|$.

- Novel idea: Freiman (1966) treated sets of integers as intrinsic objects (not embedded in \mathbb{Z})
- Generalized the notion of group homomorphism and isomorphism
- Ruzsa: a subset of \mathbb{Z} with small doubling is Freiman-isomorphic to a dense subset of $\mathbb{Z}/p\mathbb{Z}$

Small Doubling in \mathbb{Z}

- Are there other sets in \mathbb{Z} with small doubling?
- Answer: No

Theorem (Freiman-Ruzsa-Chang)

If $A \subseteq \mathbb{Z}$ is a finite set with $\sigma A \leq K$, then there is a GAP P containing A such that $\dim(P) \leq CK^C$ and $|P| \leq e^{CK^c} |A|$.

- Novel idea: Freiman (1966) treated sets of integers as intrinsic objects (not embedded in \mathbb{Z})
- Generalized the notion of group homomorphism and isomorphism
- Ruzsa: a subset of \mathbb{Z} with small doubling is Freiman-isomorphic to a dense subset of $\mathbb{Z}/p\mathbb{Z}$
- Using harmonic analysis, can establish that $2A - 2A$ contains a large GAP

Introducing Multiplicative Structure

- R , a commutative ring

Introducing Multiplicative Structure

- R , a commutative ring
- A, B , nonempty finite subsets of R

Introducing Multiplicative Structure

- R , a commutative ring
- A, B , nonempty finite subsets of R
- $A.B = \{ab : a \in A, b \in B\}$, the *product set* of A with B

Introducing Multiplicative Structure

- R , a commutative ring
- A, B , nonempty finite subsets of R
- $A.B = \{ab : a \in A, b \in B\}$, the *product set* of A with B
- $A/B = \{ab^{-1} : a \in A, b \in B\}$, the *ratio set*

Introducing Multiplicative Structure

- R , a commutative ring
- A, B , nonempty finite subsets of R
- $A.B = \{ab : a \in A, b \in B\}$, the *product set* of A with B
- $A/B = \{ab^{-1} : a \in A, b \in B\}$, the *ratio set*
- If $k \in \mathbb{N}$, then we have the iterated product set

$$A^{\cdot k} = \underbrace{A.A.\dots.A}_{k \text{ times}} = \{a_1 a_2 \cdots a_k : a_i \in A\}$$

Introducing Multiplicative Structure

- R , a commutative ring
- A, B , nonempty finite subsets of R
- $A.B = \{ab : a \in A, b \in B\}$, the *product set* of A with B
- $A/B = \{ab^{-1} : a \in A, b \in B\}$, the *ratio set*
- If $k \in \mathbb{N}$, then we have the iterated product set

$$A^{\cdot k} = \underbrace{A.A.\dots.A}_{k \text{ times}} = \{a_1 a_2 \cdots a_k : a_i \in A\}$$

- If $k \in \mathbb{Z}$, then the analogous set to the dilation of A is the set of k th powers:

$$\{a^k : a \in A\}$$

Introducing Multiplicative Structure

- R , a commutative ring
- A, B , nonempty finite subsets of R
- $A \cdot B = \{ab : a \in A, b \in B\}$, the *product set* of A with B
- $A/B = \{ab^{-1} : a \in A, b \in B\}$, the *ratio set*
- If $k \in \mathbb{N}$, then we have the iterated product set

$$A^{\cdot k} = \underbrace{A \cdot A \cdots A}_{k \text{ times}} = \{a_1 a_2 \cdots a_k : a_i \in A\}$$

- If $k \in \mathbb{Z}$, then the analogous set to the dilation of A is the set of k th powers:

$$\{a^k : a \in A\}$$

- Can also extend previous notion of dilation using ring structure: if $r \in R$,

$$r \cdot A = \{ra : a \in A\}$$

Sumsets and Product Sets

- Our previous work can tell us much about $|A \cdot A|$ and $|A/A|$ compared to $|A|$

Sumsets and Product Sets

- Our previous work can tell us much about $|A.A|$ and $|A/A|$ compared to $|A|$
 - E.g. if $A \subseteq F \setminus \{0\}$, a multiplicative group

Sumsets and Product Sets

- Our previous work can tell us much about $|A \cdot A|$ and $|A/A|$ compared to $|A|$
 - E.g. if $A \subseteq F \setminus \{0\}$, a multiplicative group
 - More complicated if R is not a field

Sumsets and Product Sets

- Our previous work can tell us much about $|A.A|$ and $|A/A|$ compared to $|A|$
 - E.g. if $A \subseteq F \setminus \{0\}$, a multiplicative group
 - More complicated if R is not a field
- Historically, addition and multiplication don't mix well

Sumsets and Product Sets

- Our previous work can tell us much about $|A.A|$ and $|A/A|$ compared to $|A|$
 - E.g. if $A \subseteq F \setminus \{0\}$, a multiplicative group
 - More complicated if R is not a field
- Historically, addition and multiplication don't mix well
- Can we relate $|A + A|$ and $|A.A|$?

Sumsets and Product Sets

- If $A = \{1, 2, \dots, n\}$ then $|A + A| = 2|A| - 1$, but $|A.A| \gg \frac{n^2}{\log^2(n)}$

Sumsets and Product Sets

- If $A = \{1, 2, \dots, n\}$ then $|A + A| = 2|A| - 1$, but $|A.A| \gg \frac{n^2}{\log^2(n)}$
- If $A = \{2^1, 2^2, \dots, 2^n\}$, then $|A.A| = 2|A| - 1$, but $|A + A| \gg n^2$

Sumsets and Product Sets

- If $A = \{1, 2, \dots, n\}$ then $|A + A| = 2|A| - 1$, but $|A.A| \gg \frac{n^2}{\log^2(n)}$
- If $A = \{2^1, 2^2, \dots, 2^n\}$, then $|A.A| = 2|A| - 1$, but $|A + A| \gg n^2$
- Arithmetic progressions and geometric progressions are the extremes

Sumsets and Product Sets

- If $A = \{1, 2, \dots, n\}$ then $|A + A| = 2|A| - 1$, but $|A.A| \gg \frac{n^2}{\log^2(n)}$
- If $A = \{2^1, 2^2, \dots, 2^n\}$, then $|A.A| = 2|A| - 1$, but $|A + A| \gg n^2$
- Arithmetic progressions and geometric progressions are the extremes
- Can we mix additive and multiplicative structure to have small doubling in both senses?

Sum-Product Inequality

- Answer: No

Sum-Product Inequality

- Answer: No
- First known result: $|A + A| + |A \cdot A| \gg |A|^{1+\varepsilon}$ for an explicit constant $\varepsilon > 0$

Sum-Product Inequality

- Answer: No
- First known result: $|A + A| + |A \cdot A| \gg |A|^{1+\varepsilon}$ for an explicit constant $\varepsilon > 0$
- First obtained for $F = \mathbb{R}$ by Erdős and Szemerédi in 1983

Sum-Product Inequality

- Answer: No
- First known result: $|A + A| + |A \cdot A| \gg |A|^{1+\varepsilon}$ for an explicit constant $\varepsilon > 0$
- First obtained for $F = \mathbb{R}$ by Erdős and Szemerédi in 1983
- Obtained for finite fields by Bourgain, Katz, and Tao in 2004

Sum-Product Inequality

- Answer: No
- First known result: $|A + A| + |A \cdot A| \gg |A|^{1+\varepsilon}$ for an explicit constant $\varepsilon > 0$
- First obtained for $F = \mathbb{R}$ by Erdős and Szemerédi in 1983
- Obtained for finite fields by Bourgain, Katz, and Tao in 2004
- Can be shown for all fields F with no finite subfields

Sum-Product Inequality in \mathbb{R}

- Conjectured by Erdős and Szemerédi that $|A + A| + |A.A| \gg |A|^{1+\varepsilon}$ for all $0 < \varepsilon < 1$

Sum-Product Inequality in \mathbb{R}

- Conjectured by Erdős and Szemerédi that $|A + A| + |A.A| \gg |A|^{1+\varepsilon}$ for all $0 < \varepsilon < 1$
- M. Nathanson (1997): $\varepsilon = \frac{1}{31}$

Sum-Product Inequality in \mathbb{R}

- Conjectured by Erdős and Szemerédi that $|A + A| + |A.A| \gg |A|^{1+\varepsilon}$ for all $0 < \varepsilon < 1$
- M. Nathanson (1997): $\varepsilon = \frac{1}{31}$
- K. Ford (1998): $\varepsilon = \frac{1}{15}$

Sum-Product Inequality in \mathbb{R}

- Conjectured by Erdős and Szemerédi that $|A + A| + |A.A| \gg |A|^{1+\varepsilon}$ for all $0 < \varepsilon < 1$
- M. Nathanson (1997): $\varepsilon = \frac{1}{31}$
- K. Ford (1998): $\varepsilon = \frac{1}{15}$
- Proofs utilize properties of factorizations

Improvement by Elekes

- Gy. Elekes (1997): $\varepsilon = \frac{1}{4}$

Improvement by Elekes

- Gy. Elekes (1997): $\varepsilon = \frac{1}{4}$
- Uses techniques from incidence geometry

Improvement by Elekes

- Gy. Elekes (1997): $\varepsilon = \frac{1}{4}$
- Uses techniques from incidence geometry

Theorem (Szemerédi-Trotter)

Let P be a finite set of points in \mathbb{R}^2 , let L be a finite set of lines in \mathbb{R}^2 , and let $I(P, L)$ be the number of incidences between points in P and lines in L . Then

$$I(P, L) \leq 4 |P|^{2/3} |L|^{2/3} + 4 |P| + |L|.$$

Improvement by Elekes

- Gy. Elekes (1997): $\varepsilon = \frac{1}{4}$
- Uses techniques from incidence geometry

Theorem (Szemerédi-Trotter)

Let P be a finite set of points in \mathbb{R}^2 , let L be a finite set of lines in \mathbb{R}^2 , and let $I(P, L)$ be the number of incidences between points in P and lines in L . Then

$$I(P, L) \leq 4 |P|^{2/3} |L|^{2/3} + 4 |P| + |L|.$$

- Theorem is sharp up to constants

Improvement by Elekes

- Gy. Elekes (1997): $\varepsilon = \frac{1}{4}$
- Uses techniques from incidence geometry

Theorem (Szemerédi-Trotter)

Let P be a finite set of points in \mathbb{R}^2 , let L be a finite set of lines in \mathbb{R}^2 , and let $I(P, L)$ be the number of incidences between points in P and lines in L . Then

$$I(P, L) \leq 4 |P|^{2/3} |L|^{2/3} + 4 |P| + |L|.$$

- Theorem is sharp up to constants
- Can be proved using graph theoretical arguments

- To show: $|A + A||A.A| \gg n^{5/2}$

- To show: $|A + A||A.A| \gg n^{5/2}$
 - Either $|A + A|$ or $|A.A| \gg n^{5/4}$, so $|A + A| + |A.A| \gg n^{5/4}$

- To show: $|A + A||A.A| \gg n^{5/2}$
 - Either $|A + A|$ or $|A.A| \gg n^{5/4}$, so $|A + A| + |A.A| \gg n^{5/4}$
- For $1 \leq i, j \leq n$, let $\ell_{i,j}(x) := a_i x - a_i a_j = a_i(x - a_j)$

- To show: $|A + A||A.A| \gg n^{5/2}$
 - Either $|A + A|$ or $|A.A| \gg n^{5/4}$, so $|A + A| + |A.A| \gg n^{5/4}$
- For $1 \leq i, j \leq n$, let $\ell_{i,j}(x) := a_i x - a_i a_j = a_i(x - a_j)$
- Observe: $\ell_{i,j}(a_k + a_j) = a_i(a_k + a_j - a_j) = a_i a_k$

- To show: $|A + A||A.A| \gg n^{5/2}$
 - Either $|A + A|$ or $|A.A| \gg n^{5/4}$, so $|A + A| + |A.A| \gg n^{5/4}$
- For $1 \leq i, j \leq n$, let $l_{i,j}(x) := a_i x - a_i a_j = a_i(x - a_j)$
- Observe: $l_{i,j}(a_k + a_j) = a_i(a_k + a_j - a_j) = a_i a_k$
- $l_{i,j}$ intersects $(a_k + a_j, a_i a_j)$ for each $k = 1, \dots, n$

- To show: $|A + A||A.A| \gg n^{5/2}$
 - Either $|A + A|$ or $|A.A| \gg n^{5/4}$, so $|A + A| + |A.A| \gg n^{5/4}$
- For $1 \leq i, j \leq n$, let $\ell_{i,j}(x) := a_i x - a_i a_j = a_i(x - a_j)$
- Observe: $\ell_{i,j}(a_k + a_j) = a_i(a_k + a_j - a_j) = a_i a_k$
- $\ell_{i,j}$ intersects $(a_k + a_j, a_i a_j)$ for each $k = 1, \dots, n$
- So we have n^2 lines, each intersecting n points in the grid $(A + A) \times (A.A)$

Corollary (Szemerédi-Trotter)

Given a set of N points in \mathbb{R}^2 , there are at most

$$O\left(\frac{N^2}{k^3} + \frac{N}{k}\right)$$

lines intersecting (at least) k points each.

Corollary (Szemerédi-Trotter)

Given a set of N points in \mathbb{R}^2 , there are at most

$$O\left(\frac{N^2}{k^3} + \frac{N}{k}\right)$$

lines intersecting (at least) k points each.

- $N = |A + A| |A \cdot A|$

Corollary (Szemerédi-Trotter)

Given a set of N points in \mathbb{R}^2 , there are at most

$$O\left(\frac{N^2}{k^3} + \frac{N}{k}\right)$$

lines intersecting (at least) k points each.

- $N = |A + A| |A \cdot A|$
- $k = n$

Corollary (Szemerédi-Trotter)

Given a set of N points in \mathbb{R}^2 , there are at most

$$O\left(\frac{N^2}{k^3} + \frac{N}{k}\right)$$

lines intersecting (at least) k points each.

- $N = |A + A| |A.A|$
- $k = n$
- Thus, $n^2 \ll |A + A|^2 |A.A|^2 n^{-3} + |A + A| |A.A| n^{-1}$

Corollary (Szemerédi-Trotter)

Given a set of N points in \mathbb{R}^2 , there are at most

$$O\left(\frac{N^2}{k^3} + \frac{N}{k}\right)$$

lines intersecting (at least) k points each.

- $N = |A + A| |A.A|$
- $k = n$
- Thus, $n^2 \ll |A + A|^2 |A.A|^2 n^{-3} + |A + A| |A.A| n^{-1}$
- $n^{5/2} \ll |A + A| |A.A|$

- J. Solymosi (2005): $\varepsilon = \frac{3}{11}$

More Results

- J. Solymosi (2005): $\varepsilon = \frac{3}{11}$
- Elekes and Ruzsa: If $|A + A| = O(|A|)$, then
$$|A + A| \gg \frac{|A|^2}{\log|A|}$$

- J. Solymosi (2005): $\varepsilon = \frac{3}{11}$
- Elekes and Ruzsa: If $|A + A| = O(|A|)$, then
$$|A + A| \gg \frac{|A|^2}{\log|A|}$$
 - Also use techniques from combinatorial geometry

- J. Solymosi (2005): $\varepsilon = \frac{3}{11}$
- Elekes and Ruzsa: If $|A + A| = O(|A|)$, then
$$|A + A| \gg \frac{|A|^2}{\log|A|}$$
 - Also use techniques from combinatorial geometry
- Chang: If $|A \cdot A| \leq K |A|$, then $|A + A| \geq \frac{|A|^2}{36^K}$

- J. Solymosi (2005): $\varepsilon = \frac{3}{11}$
- Elekes and Ruzsa: If $|A + A| = O(|A|)$, then
$$|A + A| \gg \frac{|A|^2}{\log|A|}$$
 - Also use techniques from combinatorial geometry
- Chang: If $|A \cdot A| \leq K |A|$, then $|A + A| \geq \frac{|A|^2}{36^K}$
 - Uses Freiman-type arguments

Another Flavor of Arithmetic Combinatorics

- Determine whether a given set A contains arithmetic progressions of a given length

Another Flavor of Arithmetic Combinatorics

- Determine whether a given set A contains arithmetic progressions of a given length
- Theorem: (Szemerédi) If $A \subseteq \mathbb{N}$ has positive upper density, then A contains arbitrarily long APs

Another Flavor of Arithmetic Combinatorics

- Determine whether a given set A contains arithmetic progressions of a given length
- Theorem: (Szemerédi) If $A \subseteq \mathbb{N}$ has positive upper density, then A contains arbitrarily long APs
- Conjecture: (Erdős-Turán) If $A \subseteq \mathbb{N}$ satisfies $\sum_{n \in A} \frac{1}{n} = +\infty$, then A contains arbitrarily long APs

Another Flavor of Arithmetic Combinatorics

- Determine whether a given set A contains arithmetic progressions of a given length
- Theorem: (Szemerédi) If $A \subseteq \mathbb{N}$ has positive upper density, then A contains arbitrarily long APs
- Conjecture: (Erdős-Turán) If $A \subseteq \mathbb{N}$ satisfies $\sum_{n \in A} \frac{1}{n} = +\infty$, then A contains arbitrarily long APs
- Theorem: (Green-Tao) The primes contain arbitrarily long APs

Another Flavor of Arithmetic Combinatorics

- Determine whether a given set A contains arithmetic progressions of a given length
- Theorem: (Szemerédi) If $A \subseteq \mathbb{N}$ has positive upper density, then A contains arbitrarily long APs
- Conjecture: (Erdős-Turán) If $A \subseteq \mathbb{N}$ satisfies $\sum_{n \in A} \frac{1}{n} = +\infty$, then A contains arbitrarily long APs
- Theorem: (Green-Tao) The primes contain arbitrarily long APs
- Theorem: If $A \subseteq \mathbb{N}$ has positive upper density, then A contains infinitely many length-3 APs

Another Flavor of Arithmetic Combinatorics

- Determine whether a given set A contains arithmetic progressions of a given length
- Theorem: (Szemerédi) If $A \subseteq \mathbb{N}$ has positive upper density, then A contains arbitrarily long APs
- Conjecture: (Erdős-Turán) If $A \subseteq \mathbb{N}$ satisfies $\sum_{n \in A} \frac{1}{n} = +\infty$, then A contains arbitrarily long APs
- Theorem: (Green-Tao) The primes contain arbitrarily long APs
- Theorem: If $A \subseteq \mathbb{N}$ has positive upper density, then A contains infinitely many length-3 APs
- Strong diversity in proof strategies: Fourier analysis, graph theory, Ramsey theory, ergodic theory, etc.