SUM-PRODUCT ESTIMATES IN FINITE FIELDS

M. Z. Garaev
Centro de Ciencias Matemáticas,
UNAM, campus Morelia, México

Buenos Aires, 29 July 2016

Given a finite set A we consider the sum-set

$$A + A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

Given a finite set A we consider the sum-set

$$A + A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

We are interested in lower bound estimates for $|A + A|$ or $|AA|$.

Given a finite set A we consider the sum-set

$$A + A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

We are interested in lower bound estimates for $|A + A|$ or $|AA|$.
If $A \subset \mathbb{R}$, then we order its elements $a_1 < a_2 < \ldots < a_n$ and get

$$a_1 + a_1 < a_1 + a_2 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < a_{n-1} + a_n.$$

Given a finite set A we consider the sum-set

$$A + A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

We are interested in lower bound estimates for $|A + A|$ or $|AA|$.
If $A \subset \mathbb{R}$, then we order its elements $a_1 < a_2 < \ldots < a_n$ and get

$$a_1 + a_1 < a_1 + a_2 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < a_{n-1} + a_n.$$

So we always have $|A + A| \geq 2|A| - 1$.

Given a finite set A we consider the sum-set

$$A + A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

We are interested in lower bound estimates for $|A + A|$ or $|AA|$.
If $A \subset \mathbb{R}$, then we order its elements $a_1 < a_2 < \ldots < a_n$ and get

$$a_1 + a_1 < a_1 + a_2 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < a_{n-1} + a_n.$$

So we always have $|A + A| \geq 2|A| - 1$.

If A is an arithmetic progression $\implies$ $|A + A| = 2|A| - 1$.

Given a finite set A we consider the sum-set

$$A + A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

We are interested in lower bound estimates for $|A + A|$ or $|AA|$.
If $A \subset \mathbb{R}$, then we order its elements $a_1 < a_2 < \ldots < a_n$ and get

$$a_1 + a_1 < a_1 + a_2 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < a_{n-1} + a_n.$$

So we always have $|A + A| \geq 2|A| - 1.$

If A is an arithmetic progression $\implies |A + A| = 2|A| - 1.$

If A is a geometric progression $\implies |AA| = 2|A| - 1.$

Given a finite set A we consider the sum-set

$$A+A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

We are interested in lower bound estimates for $|A+A|$ or $|AA|$.
If $A \subset \mathbb{R}$, then we order its elements $a_1 < a_2 < \ldots < a_n$ and get

$$a_1+a_1 < a_1+a_2 < \ldots < a_1+a_n < a_2+a_n < a_3+a_n < \ldots < a_{n-1}+a_n.$$

So we always have $|A+A| \geq 2|A|-1$.

If A is an arithmetic progression $\implies$ $|A+A| = 2|A|-1$.

If A is a geometric progression $\implies$ $|AA| = 2|A|-1$.
Erdős and Szemerédi (1983): if $A \subset \mathbb{Z}$, then

$$\max\{|A+A|, |AA|\} > c_1|A|^{1+c_2}; \qquad c_1, c_2 > 0.$$

Given a finite set A we consider the sum-set

$$A + A := \{a_1 + a_2; \quad a_1, a_2 \in A\}$$

and the product-set

$$AA := \{a_1 a_2; \quad a_1, a_2 \in A\}.$$

We are interested in lower bound estimates for $|A + A|$ or $|AA|$.
If $A \subset \mathbb{R}$, then we order its elements $a_1 < a_2 < \ldots < a_n$ and get

$$a_1 + a_1 < a_1 + a_2 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < a_{n-1} + a_n.$$

So we always have $|A + A| \geq 2|A| - 1$.

If A is an arithmetic progression $\implies$ $|A + A| = 2|A| - 1$.

If A is a geometric progression $\implies$ $|AA| = 2|A| - 1$.
Erdős and Szemerédi (1983): if $A \subset \mathbb{Z}$, then

$$\max\{|A + A|, |AA|\} > c_1 |A|^{1+c_2}; \qquad c_1, c_2 > 0.$$

The best known result is due to Konyagin+Shkredov (2015) improving on earlier result of Solymosi: if $A \subset \mathbb{R}$, then $\forall \varepsilon > 0$

$$\max\{|A + A|, |AA|\} > c|A|^{4/3+5/9813-\varepsilon}; \quad c = c(\varepsilon) > 0.$$

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.
Some easy variants.

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.
Some easy variants. Let $A \subset \mathbb{Z}_+$.

M. Z. Garaev
Centro de Ciencias Matemáticas, UNAM, campus Morelia, México

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.
Some easy variants. Let $A \subset \mathbb{Z}_+$. We can easily prove that

$$|A+AA| \geq |A|^2.$$

Here $A + AA := \{a_1 + a_2 a_3; \quad a_i \in A\}$.

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.
Some easy variants. Let $A \subset \mathbb{Z}_+$. We can easily prove that

$$|A + AA| \geq |A|^2.$$

Here $A + AA := \{a_1 + a_2 a_3; \quad a_i \in A\}$.
The observation is that if a_0 is the largest element of A, then all the $|A|^2$ numbers

$$x + a_0 y; \qquad x, y \in A$$

are pairwise distinct.

M. Z. Garaev
Centro de Ciencias Matemáticas, UNAM, campus Morelia, México

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.
Some easy variants. Let $A \subset \mathbb{Z}_+$. We can easily prove that

$$|A+AA| \geq |A|^2.$$

Here $A + AA := \{a_1 + a_2 a_3; \quad a_i \in A\}$.
The observation is that if a_0 is the largest element of A, then all the $|A|^2$ numbers

$$x + a_0 y; \qquad x, y \in A$$

are pairwise distinct. Indeed, if for some $x, y, x_1, y_1 \in A$

$$x + a_0 y = x_1 + a_0 y_1$$

then $y = y_1$ and $x = x_1$, as otherwise

$$a_0 = \frac{x_1 - x}{y - y_1}.$$

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.
Some easy variants. Let $A \subset \mathbb{Z}_+$. We can easily prove that

$$|A+AA| \geq |A|^2.$$

Here $A + AA := \{a_1 + a_2 a_3; \quad a_i \in A\}$.
The observation is that if a_0 is the largest element of A, then all the $|A|^2$ numbers

$$x + a_0 y; \qquad x, y \in A$$

are pairwise distinct. Indeed, if for some $x, y, x_1, y_1 \in A$

$$x + a_0 y = x_1 + a_0 y_1$$

then $y = y_1$ and $x = x_1$, as otherwise

$$a_0 = \frac{x_1 - x}{y - y_1}.$$

Impossible, because $|y - y_1| \geq 1$ and $|x_1 - x| < a_0$.

The main conjecture: for $A \subset \mathbb{R}$,

$$\max\{|A+A|, |AA|\} \gtrsim |A|^2.$$

$\forall \varepsilon > 0$, $\max\{|A+A|, |AA|\} > c_\varepsilon |A|^{2-\varepsilon}$.
Some easy variants. Let $A \subset \mathbb{Z}_+$. We can easily prove that

$$|A + AA| \geq |A|^2.$$

Here $A + AA := \{a_1 + a_2 a_3; \quad a_i \in A\}$.
The observation is that if a_0 is the largest element of A, then all the $|A|^2$ numbers

$$x + a_0 y; \qquad x, y \in A$$

are pairwise distinct. Indeed, if for some $x, y, x_1, y_1 \in A$

$$x + a_0 y = x_1 + a_0 y_1$$

then $y = y_1$ and $x = x_1$, as otherwise

$$a_0 = \frac{x_1 - x}{y - y_1}.$$

Impossible, because $|y - y_1| \geq 1$ and $|x_1 - x| < a_0$. It follows that

$$|A + AA| \geq |A|^2.$$

Another variation.

Another variation. Let $A \subset \mathbb{R}_+$.

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1 a_2 + a_3 a_4 - a_5 a_6; \quad a_i \in A\}$.

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1 a_2 + a_3 a_4 - a_5 a_6; \quad a_i \in A\}$. Take a_0 to be the largest element of A, and let a_1, a_2 be the closest pair in A, i.e. with the smallest $|a_1 - a_2| > 0$.

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1a_2 + a_3a_4 - a_5a_6; \quad a_i \in A\}$. Take a_0 to be the largest element of A, and let a_1, a_2 be the closest pair in A, i.e. with the smallest $|a_1 - a_2| > 0$. We claim that all the $|A|^2$ numbers

$$a_0x + (a_1 - a_2)y; \qquad x, y \in A$$

are distinct.

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1a_2 + a_3a_4 - a_5a_6; \quad a_i \in A\}$. Take a_0 to be the largest element of A, and let a_1, a_2 be the closest pair in A, i.e. with the smallest $|a_1 - a_2| > 0$. We claim that all the $|A|^2$ numbers

$$a_0x + (a_1 - a_2)y; \qquad x, y \in A$$

are distinct. Indeed if

$$a_0x + (a_1 - a_2)y = a_0x_1 + (a_1 - a_2)y_1; \qquad x, y, x_1, y_1 \in A,$$

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1a_2 + a_3a_4 - a_5a_6; \quad a_i \in A\}$. Take a_0 to be the largest element of A, and let a_1, a_2 be the closest pair in A, i.e. with the smallest $|a_1 - a_2| > 0$. We claim that all the $|A|^2$ numbers

$$a_0x + (a_1 - a_2)y; \qquad x, y \in A$$

are distinct. Indeed if

$$a_0x + (a_1 - a_2)y = a_0x_1 + (a_1 - a_2)y_1; \qquad x, y, x_1, y_1 \in A,$$

then

$$\frac{x - x_1}{y_1 - y} = \frac{a_1 - a_2}{a_0}; \qquad x, y, x_1, y_1 \in A,$$

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1 a_2 + a_3 a_4 - a_5 a_6; \quad a_i \in A\}$. Take a_0 to be the largest element of A, and let a_1, a_2 be the closest pair in A, i.e. with the smallest $|a_1 - a_2| > 0$. We claim that all the $|A|^2$ numbers

$$a_0 x + (a_1 - a_2)y; \qquad x, y \in A$$

are distinct. Indeed if

$$a_0 x + (a_1 - a_2)y = a_0 x_1 + (a_1 - a_2)y_1; \qquad x, y, x_1, y_1 \in A,$$

then

$$\frac{x - x_1}{y_1 - y} = \frac{a_1 - a_2}{a_0}; \qquad x, y, x_1, y_1 \in A,$$

is impossible, because $|x - x_1| \geq |a_1 - a_2|$, $|y_1 - y| < a_0$.

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1a_2 + a_3a_4 - a_5a_6; \quad a_i \in A\}$. Take a_0 to be the largest element of A, and let a_1, a_2 be the closest pair in A, i.e. with the smallest $|a_1 - a_2| > 0$. We claim that all the $|A|^2$ numbers

$$a_0x + (a_1 - a_2)y; \qquad x, y \in A$$

are distinct. Indeed if

$$a_0x + (a_1 - a_2)y = a_0x_1 + (a_1 - a_2)y_1; \qquad x, y, x_1, y_1 \in A,$$

then

$$\frac{x - x_1}{y_1 - y} = \frac{a_1 - a_2}{a_0}; \qquad x, y, x_1, y_1 \in A,$$

is impossible, because $|x - x_1| \geq |a_1 - a_2|$, $|y_1 - y| < a_0$.
Open Problem: Prove that if $A \subset \mathbb{R}_+$, then

$$|AA + AA + AA| \geq |A|^2.$$

Another variation. Let $A \subset \mathbb{R}_+$. We shall prove that

$$|AA + AA - AA| \geq |A|^2.$$

Here $AA + AA - AA := \{a_1a_2 + a_3a_4 - a_5a_6; \quad a_i \in A\}$. Take a_0 to be the largest element of A, and let a_1, a_2 be the closest pair in A, i.e. with the smallest $|a_1 - a_2| > 0$. We claim that all the $|A|^2$ numbers

$$a_0x + (a_1 - a_2)y; \qquad x, y \in A$$

are distinct. Indeed if

$$a_0x + (a_1 - a_2)y = a_0x_1 + (a_1 - a_2)y_1; \qquad x, y, x_1, y_1 \in A,$$

then

$$\frac{x - x_1}{y_1 - y} = \frac{a_1 - a_2}{a_0}; \qquad x, y, x_1, y_1 \in A,$$

is impossible, because $|x - x_1| \geq |a_1 - a_2|$, $|y_1 - y| < a_0$.

Open Problem: Prove that if $A \subset \mathbb{R}_+$, then

$$|AA + AA + AA| \geq |A|^2.$$

In 2014 Balog and Roche-Newton:

$$|AA + AA + AA + AA| \geq |A|^2.$$

Sum-product problem in $\mathbb{F}_p$

Sum-product problem in $\mathbb{F}_p$

Let p be a prime number, $\mathbb{F}_p$ be the field of residue classes modulo p. We shall associate elements of $\mathbb{F}_p$ with $\{0, 1, 2, ..., p-1\}$.

Sum-product problem in $\mathbb{F}_p$

Let p be a prime number, $\mathbb{F}_p$ be the field of residue classes modulo p. We shall associate elements of $\mathbb{F}_p$ with $\{0, 1, 2, ..., p-1\}$. For instance, if $p = 13$ and if $A \subset \mathbb{F}_p$, say, $A = \{2, 6, 7\}$, then

$$A + A = \{4, 8, 9, 12, 13, 14\} = \{4, 8, 9, 12, 0, 1\}.$$

Let p be a prime number, $\mathbb{F}_p$ be the field of residue classes modulo p. We shall associate elements of $\mathbb{F}_p$ with $\{0, 1, 2, ..., p-1\}$. For instance, if $p = 13$ and if $A \subset \mathbb{F}_p$, say, $A = \{2, 6, 7\}$, then

$$A + A = \{4, 8, 9, 12, 13, 14\} = \{4, 8, 9, 12, 0, 1\}.$$

$$AA = \{4, 12, 14, 36, 42, 49\} = \{4, 12, 1, 10, 3, 10\} = \{4, 12, 1, 10, 3\}.$$

Let p be a prime number, $\mathbb{F}_p$ be the field of residue classes modulo p. We shall associate elements of $\mathbb{F}_p$ with $\{0, 1, 2, ..., p-1\}$. For instance, if $p = 13$ and if $A \subset \mathbb{F}_p$, say, $A = \{2, 6, 7\}$, then

$$A + A = \{4, 8, 9, 12, 13, 14\} = \{4, 8, 9, 12, 0, 1\}.$$

$$AA = \{4, 12, 14, 36, 42, 49\} = \{4, 12, 1, 10, 3, 10\} = \{4, 12, 1, 10, 3\}.$$

If $|A| \approx |\mathbb{F}_p| = p$, then

$$|A + A| \approx |A|, \quad |AA| \approx |A|.$$

Sum-product problem in $\mathbb{F}_p$

Let p be a prime number, $\mathbb{F}_p$ be the field of residue classes modulo p. We shall associate elements of $\mathbb{F}_p$ with $\{0, 1, 2, ..., p-1\}$. For instance, if $p = 13$ and if $A \subset \mathbb{F}_p$, say, $A = \{2, 6, 7\}$, then

$$A + A = \{4, 8, 9, 12, 13, 14\} = \{4, 8, 9, 12, 0, 1\}.$$

$$AA = \{4, 12, 14, 36, 42, 49\} = \{4, 12, 1, 10, 3, 10\} = \{4, 12, 1, 10, 3\}.$$

If $|A| \approx |\mathbb{F}_p| = p$, then

$$|A + A| \approx |A|, \quad |AA| \approx |A|.$$

It is reasonable to assume that

$$|A| < p^{1-\varepsilon} \quad \text{for some} \quad \varepsilon > 0.$$

Sum-product problem in $\mathbb{F}_p$

Let p be a prime number, $\mathbb{F}_p$ be the field of residue classes modulo p. We shall associate elements of $\mathbb{F}_p$ with $\{0, 1, 2, ..., p-1\}$. For instance, if $p = 13$ and if $A \subset \mathbb{F}_p$, say, $A = \{2, 6, 7\}$, then

$$A + A = \{4, 8, 9, 12, 13, 14\} = \{4, 8, 9, 12, 0, 1\}.$$

$$AA = \{4, 12, 14, 36, 42, 49\} = \{4, 12, 1, 10, 3, 10\} = \{4, 12, 1, 10, 3\}.$$

If $|A| \approx |\mathbb{F}_p| = p$, then

$$|A + A| \approx |A|, \quad |AA| \approx |A|.$$

It is reasonable to assume that

$$|A| < p^{1-\varepsilon} \quad \text{for some} \quad \varepsilon > 0.$$

Theorem. (Bourgain, Katz,Tao + Konyagin; 2003). *Let $A \subset \mathbb{F}_p$ with*

$$|A| < p^{1-\varepsilon} \quad \text{for some} \quad \varepsilon > 0.$$

Sum-product problem in $\mathbb{F}_p$

Let p be a prime number, $\mathbb{F}_p$ be the field of residue classes modulo p. We shall associate elements of $\mathbb{F}_p$ with $\{0, 1, 2, ..., p-1\}$. For instance, if $p = 13$ and if $A \subset \mathbb{F}_p$, say, $A = \{2, 6, 7\}$, then

$$A + A = \{4, 8, 9, 12, 13, 14\} = \{4, 8, 9, 12, 0, 1\}.$$

$$AA = \{4, 12, 14, 36, 42, 49\} = \{4, 12, 1, 10, 3, 10\} = \{4, 12, 1, 10, 3\}.$$

If $|A| \approx |\mathbb{F}_p| = p$, then

$$|A + A| \approx |A|, \quad |AA| \approx |A|.$$

It is reasonable to assume that

$$|A| < p^{1-\varepsilon} \quad \text{for some} \quad \varepsilon > 0.$$

Theorem. (Bourgain, Katz,Tao + Konyagin; 2003). *Let $A \subset \mathbb{F}_p$ with*

$$|A| < p^{1-\varepsilon} \quad \text{for some} \quad \varepsilon > 0.$$

Then

$$\max\{|A + A|, |AA|\} \geq |A|^{1+\delta}, \quad \delta = \delta(\varepsilon) > 0.$$

Some simple observations

Some simple observations

Let $A, B \subset \mathbb{F}_p$ and J be the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1 \in A, \quad b, b_1 \in B.$$

Some simple observations

Let $A, B \subset \mathbb{F}_p$ and J be the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1 \in A, \quad b, b_1 \in B.$$

Then

$$|A + B| \geq \frac{|A|^2 |B|^2}{J}.$$

Some simple observations

Let $A, B \subset \mathbb{F}_p$ and J be the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1 \in A, \quad b, b_1 \in B.$$

Then

$$|A + B| \geq \frac{|A|^2 |B|^2}{J}.$$

Indeed, if for a given $\lambda \in A + B$ we denote by $T(\lambda)$ the number of representation

$$a + b = \lambda, \quad a \in A, \quad b \in B,$$

Some simple observations

Let $A, B \subset \mathbb{F}_p$ and J be the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1 \in A, \quad b, b_1 \in B.$$

Then

$$|A + B| \geq \frac{|A|^2|B|^2}{J}.$$

Indeed, if for a given $\lambda \in A + B$ we denote by $T(\lambda)$ the number of representation

$$a + b = \lambda, \quad a \in A, \quad b \in B,$$

then $T^2(\lambda) \Rightarrow a + b = \lambda = a_1 + b_1;\ a, a_1 \in A, b, b_1 \in B,$

$$J = \sum_{\lambda \in A+B} T^2(\lambda); \quad \sum_{\lambda \in A+B} T(\lambda) = |A||B|.$$

Some simple observations

Let $A, B \subset \mathbb{F}_p$ and J be the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1 \in A, \quad b, b_1 \in B.$$

Then

$$|A + B| \geq \frac{|A|^2|B|^2}{J}.$$

Indeed, if for a given $\lambda \in A + B$ we denote by $T(\lambda)$ the number of representation

$$a + b = \lambda, \quad a \in A, \quad b \in B,$$

then $T^2(\lambda) \Rightarrow a + b = \lambda = a_1 + b_1;\ a, a_1 \in A, b, b_1 \in B$,

$$J = \sum_{\lambda \in A+B} T^2(\lambda); \quad \sum_{\lambda \in A+B} T(\lambda) = |A||B|.$$

By Cauchy-Schwarz inequality we get

$$J = \sum_{\lambda \in A+B} T^2(\lambda) \geq \frac{1}{|A+B|}\Big(\sum_{\lambda \in A+B} T(\lambda)\Big)^2 = \frac{|A|^2|B|^2}{|A+B|}.$$

In particular, if J is the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1, b, b_1 \in A,$$

In particular, if J is the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1, b, b_1 \in A,$$

then

$$|A + A| \geq \frac{|A|^4}{J}.$$

The trivial estimate $J \leq |A|^3$, implies $|A + A| \geq |A|$.

In particular, if J is the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1, b, b_1 \in A,$$

then

$$|A + A| \geq \frac{|A|^4}{J}.$$

The trivial estimate $J \leq |A|^3$, implies $|A + A| \geq |A|$.

If $J < |A|^{3-c}$, then $|A + A| \geq |A|^{1+c}$.

In particular, if J is the number of solutions of the equation

$$a + b = a_1 + b_1, \quad a, a_1, b, b_1 \in A,$$

then

$$|A + A| \geq \frac{|A|^4}{J}.$$

The trivial estimate $J \leq |A|^3$, implies $|A + A| \geq |A|$.

If $J < |A|^{3-c}$, then $|A + A| \geq |A|^{1+c}$.

The proof of the sum-product estimate uses a number of observations and ideas.

In particular, if J is the number of solutions of the equation

$$a+b=a_1+b_1, \quad a, a_1, b, b_1 \in A,$$

then

$$|A+A| \geq \frac{|A|^4}{J}.$$

The trivial estimate $J \leq |A|^3$, implies $|A+A| \geq |A|$.

If $J < |A|^{3-c}$, then $|A+A| \geq |A|^{1+c}$.

The proof of the sum-product estimate uses a number of observations and ideas.

Let us have a bit closer look at the case $|A| < p^{1/2}$.

CASE 1. Let

$$\frac{A-A}{A-A} := \left\{ \frac{a_1 - a_2}{a_3 - a_4} : \ a_i \in A, \ a_3 \neq a_4 \right\} = \mathbb{F}_p.$$

CASE 1. Let

$$\frac{A-A}{A-A} := \left\{ \frac{a_1 - a_2}{a_3 - a_4} : \ a_i \in A, \ a_3 \neq a_4 \right\} = \mathbb{F}_p.$$

The equation

$$x + gy = u + gv; \qquad x, y, u, v \in A, \quad g \in \mathbb{F}_p^* \subset \frac{A-A}{A-A}$$

has at most $(p-1)|A|^2 + |A|^4 \leq 2(p-1)|A|^2$ solutions.

CASE 1. Let

$$\frac{A-A}{A-A} := \left\{\frac{a_1-a_2}{a_3-a_4} : a_i \in A,\ a_3 \neq a_4\right\} = \mathbb{F}_p.$$

The equation

$$x + gy = u + gv; \qquad x, y, u, v \in A, \quad g \in \mathbb{F}_p^* \subset \frac{A-A}{A-A}$$

has at most $(p-1)|A|^2 + |A|^4 \leq 2(p-1)|A|^2$ solutions. Thus, $\exists g = g_0 \in \mathbb{F}_p^*$ s.t. the equation

$$x + g_0 y = u + g_0 v; \qquad x, y, u, v \in A,$$

has at most $2|A|^2$ solutions.

CASE 1. Let

$$\frac{A-A}{A-A} := \left\{ \frac{a_1 - a_2}{a_3 - a_4} : \, a_i \in A, \, a_3 \neq a_4 \right\} = \mathbb{F}_p.$$

The equation

$$x + gy = u + gv; \qquad x, y, u, v \in A, \quad g \in \mathbb{F}_p^* \subset \frac{A-A}{A-A}$$

has at most $(p-1)|A|^2 + |A|^4 \leq 2(p-1)|A|^2$ solutions. Thus, $\exists g = g_0 \in \mathbb{F}_p^*$ s.t. the equation

$$x + g_0 y = u + g_0 v; \qquad x, y, u, v \in A,$$

has at most $2|A|^2$ solutions. Then by the previous observation

$$|A + g_0 A| \geq \frac{|A|^4}{2|A|^2} = \frac{1}{2}|A|^2.$$

CASE 1. Let

$$\frac{A-A}{A-A} := \left\{ \frac{a_1-a_2}{a_3-a_4} \,:\, a_i\in A,\ a_3\neq a_4 \right\} = \mathbb{F}_p.$$

The equation

$$x+gy=u+gv; \qquad x,y,u,v\in A, \quad g\in\mathbb{F}_p^*\subset \frac{A-A}{A-A}$$

has at most $(p-1)|A|^2+|A|^4\le 2(p-1)|A|^2$ solutions. Thus, $\exists g=g_0\in\mathbb{F}_p^*$ s.t. the equation

$$x+g_0y=u+g_0v; \qquad x,y,u,v\in A,$$

has at most $2|A|^2$ solutions. Then by the previous observation

$$|A+g_0A|\ge \frac{|A|^4}{2|A|^2}=\frac{1}{2}|A|^2.$$

Thus, there exist $a_1,a_2,a_3,a_4\in A$ such that

$$\left|A+\frac{a_1-a_2}{a_3-a_4}A\right|\ge 0.5|A|^2.$$

CASE 1. Let

$$\frac{A-A}{A-A} := \left\{ \frac{a_1-a_2}{a_3-a_4} : \ a_i \in A, \ a_3 \neq a_4 \right\} = \mathbb{F}_p.$$

The equation

$$x + gy = u + gv; \qquad x, y, u, v \in A, \quad g \in \mathbb{F}_p^* \subset \frac{A-A}{A-A}$$

has at most $(p-1)|A|^2 + |A|^4 \leq 2(p-1)|A|^2$ solutions. Thus, $\exists g = g_0 \in \mathbb{F}_p^*$ s.t. the equation

$$x + g_0 y = u + g_0 v; \qquad x, y, u, v \in A,$$

has at most $2|A|^2$ solutions. Then by the previous observation

$$|A + g_0 A| \geq \frac{|A|^4}{2|A|^2} = \frac{1}{2}|A|^2.$$

Thus, there exist $a_1, a_2, a_3, a_4 \in A$ such that

$$\left| A + \frac{a_1 - a_2}{a_3 - a_4} A \right| \geq 0.5|A|^2.$$

It follows that $|(a_1 - a_2)A + (a_3 - a_4)A| \geq 0.5|A|^2$.

CASE 2.

$$\frac{A-A}{A-A} \neq \mathbb{F}_p.$$

CASE 2.

$$\frac{A-A}{A-A} \neq \mathbb{F}_p.$$

Then

$$\frac{A-A}{A-A} + 1 \neq \frac{A-A}{A-A}.$$

CASE 2.

$$\frac{A-A}{A-A} \neq \mathbb{F}_p.$$

Then

$$\frac{A-A}{A-A} + 1 \neq \frac{A-A}{A-A}.$$

It means that there are elements $a_1, a_2, a_3, a_4 \in A$ such that

$$\frac{a_1 - a_2}{a_3 - a_4} + 1 \notin \frac{A-A}{A-A}.$$

CASE 2.

$$\frac{A-A}{A-A} \neq \mathbb{F}_p.$$

Then

$$\frac{A-A}{A-A} + 1 \neq \frac{A-A}{A-A}.$$

It means that there are elements $a_1, a_2, a_3, a_4 \in A$ such that

$$\frac{a_1 - a_2}{a_3 - a_4} + 1 \notin \frac{A-A}{A-A}.$$

Observation: if $g \notin \frac{A-A}{A-A}$ then $|A + gA| = |A|^2$.

CASE 2.

$$\frac{A-A}{A-A} \neq \mathbb{F}_p.$$

Then

$$\frac{A-A}{A-A} + 1 \neq \frac{A-A}{A-A}.$$

It means that there are elements $a_1, a_2, a_3, a_4 \in A$ such that

$$\frac{a_1 - a_2}{a_3 - a_4} + 1 \notin \frac{A-A}{A-A}.$$

Observation: if $g \notin \frac{A-A}{A-A}$ then $|A + gA| = |A|^2$. This implies that

$$\left|A + \left(\frac{a_1 - a_2}{a_3 - a_4} + 1\right)A\right| = |A|^2.$$

CASE 2.

$$\frac{A-A}{A-A} \neq \mathbb{F}_p.$$

Then

$$\frac{A-A}{A-A} + 1 \neq \frac{A-A}{A-A}.$$

It means that there are elements $a_1, a_2, a_3, a_4 \in A$ such that

$$\frac{a_1-a_2}{a_3-a_4} + 1 \notin \frac{A-A}{A-A}.$$

Observation: if $g \notin \frac{A-A}{A-A}$ then $|A+gA| = |A|^2$. This implies that

$$\left|A + \left(\frac{a_1-a_2}{a_3-a_4} + 1\right)A\right| = |A|^2.$$

It follows that

$$|(a_3-a_4)A + (a_3-a_4)A + (a_1-a_2)A| \geq |A|^2.$$

CASE 2.

$$\frac{A-A}{A-A} \neq \mathbb{F}_p.$$

Then

$$\frac{A-A}{A-A} + 1 \neq \frac{A-A}{A-A}.$$

It means that there are elements $a_1, a_2, a_3, a_4 \in A$ such that

$$\frac{a_1 - a_2}{a_3 - a_4} + 1 \notin \frac{A-A}{A-A}.$$

Observation: if $g \notin \frac{A-A}{A-A}$ then $|A + gA| = |A|^2$. This implies that

$$\left|A + \left(\frac{a_1 - a_2}{a_3 - a_4} + 1\right)A\right| = |A|^2.$$

It follows that

$$|(a_3 - a_4)A + (a_3 - a_4)A + (a_1 - a_2)A| \geq |A|^2.$$

The rest of the proof uses known results from additive combinatorics, such as Plunnecke inequality, Ruzsa triangle inequality.

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

Bourgain, Breuillard, Chang, Gamburd, Glibichuk, Helfgott, Katz, Konyagin, Rudnev, Sarnak, Shkredov, Shparlinski, Tao,....

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

Bourgain, Breuillard, Chang, Gamburd, Glibichuk, Helfgott, Katz, Konyagin, Rudnev, Sarnak, Shkredov, Shparlinski, Tao,....

1. Bourgain, Konyagin and Glibichuk (2006): A long standing problem on estimates of Gauss trigonometric sums.

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

Bourgain, Breuillard, Chang, Gamburd, Glibichuk, Helfgott, Katz, Konyagin, Rudnev, Sarnak, Shkredov, Shparlinski, Tao,....

1. Bourgain, Konyagin and Glibichuk (2006): A long standing problem on estimates of Gauss trigonometric sums.

2. Bourgain (2005): some problems that originated from Computer Science.

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

Bourgain, Breuillard, Chang, Gamburd, Glibichuk, Helfgott, Katz, Konyagin, Rudnev, Sarnak, Shkredov, Shparlinski, Tao,....

1. Bourgain, Konyagin and Glibichuk (2006): A long standing problem on estimates of Gauss trigonometric sums.

2. Bourgain (2005): some problems that originated from Computer Science.

3. Helfgott (2008): initiation of very important works on diameters and expansion theory of Cayley graphs of finite groups.

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

Bourgain, Breuillard, Chang, Gamburd, Glibichuk, Helfgott, Katz, Konyagin, Rudnev, Sarnak, Shkredov, Shparlinski, Tao,....

1. Bourgain, Konyagin and Glibichuk (2006): A long standing problem on estimates of Gauss trigonometric sums.

2. Bourgain (2005): some problems that originated from Computer Science.

3. Helfgott (2008): initiation of very important works on diameters and expansion theory of Cayley graphs of finite groups.

4. Many new results on additive problems in finite fields.

M. Z. Garaev
Centro de Ciencias Matemáticas, UNAM, campus Morelia, México

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

Bourgain, Breuillard, Chang, Gamburd, Glibichuk, Helfgott, Katz, Konyagin, Rudnev, Sarnak, Shkredov, Shparlinski, Tao,....

1. Bourgain, Konyagin and Glibichuk (2006): A long standing problem on estimates of Gauss trigonometric sums.

2. Bourgain (2005): some problems that originated from Computer Science.

3. Helfgott (2008): initiation of very important works on diameters and expansion theory of Cayley graphs of finite groups.

4. Many new results on additive problems in finite fields.

5,6,7,....

The sum-product estimates and its versions have found a number of spectacular applications in different areas of mathematics.

Bourgain, Breuillard, Chang, Gamburd, Glibichuk, Helfgott, Katz, Konyagin, Rudnev, Sarnak, Shkredov, Shparlinski, Tao,....

1. Bourgain, Konyagin and Glibichuk (2006): A long standing problem on estimates of Gauss trigonometric sums.

2. Bourgain (2005): some problems that originated from Computer Science.

3. Helfgott (2008): initiation of very important works on diameters and expansion theory of Cayley graphs of finite groups.

4. Many new results on additive problems in finite fields.

5,6,7,....

Bourgain & G (2014). Estimates of very short Kloosterman sums.

Rational trigonometric sums

M. Z. Garaev
Centro de Ciencias Matemáticas, UNAM, campus Morelia, México

Rational trigonometric sums

Let $m \geq 2$ be an integer. Consider the trigonometric sum

$$S := \sum_{x} e^{2\pi i x/m},$$

where x runs a system of N integers.

Rational trigonometric sums

Let $m \geq 2$ be an integer. Consider the trigonometric sum

$$S := \sum_{x} e^{2\pi i x/m},$$

where x runs a system of N integers.

From $|e^{ix}| = 1$ it follows the trivial estimate

$$|S| \leq N.$$

Rational trigonometric sums

Let $m \geq 2$ be an integer. Consider the trigonometric sum

$$S := \sum_{x} e^{2\pi ix/m},$$

where x runs a system of N integers.

From $|e^{ix}| = 1$ it follows the trivial estimate

$$|S| \leq N.$$

The central problem is to obtain a nontrivial estimate of the form

$$|S| \leq \Delta N$$

with $\Delta = \Delta(N)$ as small as possible.

Rational trigonometric sums

Let $m \geq 2$ be an integer. Consider the trigonometric sum

$$S := \sum_{x} e^{2\pi i x/m},$$

where x runs a system of N integers.

From $|e^{ix}| = 1$ it follows the trivial estimate

$$|S| \leq N.$$

The central problem is to obtain a nontrivial estimate of the form

$$|S| \leq \Delta N$$

with $\Delta = \Delta(N)$ as small as possible. Especially are interesting estimates with

$$\Delta = \Delta(N) \to 0 \quad \text{as} \quad N \to \infty.$$

There are relations between trigonometric sums and additive congruences observed by Vinogradov in 1926.

There are relations between trigonometric sums and additive congruences observed by Vinogradov in 1926.

LEMMA. *Let $m \geq 2$ be an integer, u, v run system of integers*

$$u = u_1, u_2, \ldots, u_L; \qquad v = v_1, v_2, \ldots, v_M.$$

There are relations between trigonometric sums and additive congruences observed by Vinogradov in 1926.

LEMMA. *Let $m \geq 2$ be an integer, u, v run system of integers*

$$u = u_1, u_2, \ldots, u_L; \qquad v = v_1, v_2, \ldots, v_M.$$

Assume that

$$\max_{1 \leq a \leq m-1} \left| \sum_{u} e^{2\pi i a u/m} \right| \leq R; \qquad \sum_{a=1}^{m-1} \left| \sum_{v} e^{2\pi i a v/m} \right| \leq D.$$

There are relations between trigonometric sums and additive congruences observed by Vinogradov in 1926.

Lemma. *Let $m \geq 2$ be an integer, u, v run system of integers*

$$u = u_1, u_2, \ldots, u_L; \qquad v = v_1, v_2, \ldots, v_M.$$

Assume that

$$\max_{1 \leq a \leq m-1} \left| \sum_u e^{2\pi i a u/m} \right| \leq R; \qquad \sum_{a=1}^{m-1} \left| \sum_v e^{2\pi i a v/m} \right| \leq D.$$

Then for any integer λ the number T of solutions of the congruence

$$u + v \equiv \lambda \pmod{m}$$

can be represented in the form

$$T = \frac{LM}{m}\left(1 + \theta \frac{RD}{LM}\right); \qquad |\theta| \leq 1.$$

The starting point:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi i a x/m} = \begin{cases} 1, & \text{if } x \equiv 0 \pmod{m}, \\ 0, & \text{if } x \not\equiv 0 \pmod{m}. \end{cases}$$

The starting point:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi iax/m} = \begin{cases} 1, & \text{if } x \equiv 0 \pmod{m}, \\ 0, & \text{if } x \not\equiv 0 \pmod{m}. \end{cases}$$

For $x \not\equiv 0 \pmod{m}$ take $z = e^{2\pi ix/m}$ and use

$$1 + z + z^2 + \ldots + z^{m-1} = (z^m - 1)/(z - 1) = 0.$$

The starting point:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi iax/m} = \begin{cases} 1, & \text{if } x \equiv 0 \pmod{m}, \\ 0, & \text{if } x \not\equiv 0 \pmod{m}. \end{cases}$$

For $x \not\equiv 0 \pmod{m}$ take $z = e^{2\pi ix/m}$ and use

$$1 + z + z^2 + \ldots + z^{m-1} = (z^m - 1)/(z-1) = 0.$$

Substitute $x = u + v - \lambda$:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi ia(u+v-\lambda)/m} = \begin{cases} 1, & \text{if } u + v \equiv \lambda \pmod{m}, \\ 0, & \text{if } u + v \not\equiv \lambda \pmod{m}. \end{cases}$$

The starting point:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi iax/m} = \begin{cases} 1, & \text{if } x \equiv 0 \pmod{m}, \\ 0, & \text{if } x \not\equiv 0 \pmod{m}. \end{cases}$$

For $x \not\equiv 0 \pmod{m}$ take $z = e^{2\pi ix/m}$ and use

$$1 + z + z^2 + \ldots + z^{m-1} = (z^m - 1)/(z-1) = 0.$$

Substitute $x = u + v - \lambda$:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi ia(u+v-\lambda)/m} = \begin{cases} 1, & \text{if } u+v \equiv \lambda \pmod{m}, \\ 0, & \text{if } u+v \not\equiv \lambda \pmod{m}. \end{cases}$$

We sum over $u = u_1, u_2, \ldots, u_L$ and $v = v_1, v_2, \ldots, v_M$;

$$T = \sum_u \sum_v \frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi ia(u+v-\lambda)/m} = \frac{1}{m}\sum_{a=0}^{m-1}\sum_u \sum_v e^{2\pi ia(u+v-\lambda)/m}.$$

The starting point:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi iax/m} = \begin{cases} 1, & \text{if } x \equiv 0 \pmod{m}, \\ 0, & \text{if } x \not\equiv 0 \pmod{m}. \end{cases}$$

For $x \not\equiv 0 \pmod{m}$ take $z = e^{2\pi ix/m}$ and use

$$1 + z + z^2 + \ldots + z^{m-1} = (z^m - 1)/(z-1) = 0.$$

Substitute $x = u + v - \lambda$:

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi ia(u+v-\lambda)/m} = \begin{cases} 1, & \text{if } u+v \equiv \lambda \pmod{m}, \\ 0, & \text{if } u+v \not\equiv \lambda \pmod{m}. \end{cases}$$

We sum over $u = u_1, u_2, \ldots, u_L$ and $v = v_1, v_2, \ldots, v_M$;

$$T = \sum_u \sum_v \frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi ia(u+v-\lambda)/m} = \frac{1}{m}\sum_{a=0}^{m-1}\sum_u\sum_v e^{2\pi ia(u+v-\lambda)/m}.$$

Separate $a = 0$ and obtain

$$T = \frac{LM}{m} + Error,$$

where

$$Error = \frac{1}{m}\sum_{a=1}^{m-1}\left(\sum_{u} e^{2\pi iau/m}\right)\left(\sum_{v} e^{2\pi iav/m}\right) e^{-2\pi ia\lambda/m}.$$

where

$$Error = \frac{1}{m}\sum_{a=1}^{m-1}\left(\sum_{u} e^{2\pi iau/m}\right)\left(\sum_{v} e^{2\pi iav/m}\right)e^{-2\pi ia\lambda/m}.$$

The conditions of the Lemma imply

$$|Error| \le \frac{1}{m}\sum_{a=1}^{m-1}\left|\sum_{u} e^{2\pi iu/m}\right|\left|\sum_{v} e^{2\pi iav/m}\right| \le \frac{RD}{m},$$

and the claim follows.

LEMMA. *Let* U, $V \subset \{1, 2, \ldots, p\}$. *Then for any* $a \in \{1, 2, \ldots, p-1\}$ *the following holds:*

$$\left|\sum_{u\in U}\sum_{v\in V} e^{2\pi i auv/p}\right| \leq \sqrt{p|U||V|},$$

Lemma. *Let U, $V \subset \{1, 2, \ldots, p\}$. Then for any $a \in \{1, 2, \ldots, p-1\}$ the following holds:*

$$\left| \sum_{u \in U} \sum_{v \in V} e^{2\pi i auv/p} \right| \le \sqrt{p|U||V|},$$

If, say, $|U||V| > p^{1+\varepsilon}$, then

$$\left| \sum_{u \in U} \sum_{v \in V} e^{2\pi i auv/p} \right| \le |U||V|p^{-\varepsilon/2}.$$

Lemma. *Let U, $V \subset \{1, 2, \dots, p\}$. Then for any $a \in \{1, 2, \dots, p-1\}$ the following holds:*

$$\left| \sum_{u \in U} \sum_{v \in V} e^{2\pi i a u v / p} \right| \leq \sqrt{p|U||V|},$$

If, say, $|U||V| > p^{1+\varepsilon}$, then

$$\left| \sum_{u \in U} \sum_{v \in V} e^{2\pi i a u v / p} \right| \leq |U||V| p^{-\varepsilon/2}.$$

The proof of the Lemma follows from the Cauchy-Schwarz inequality + Trigonometric identity.

Gauss sums

The Gauss sum:

$$S_n(a,p)=\sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a,p)=1.$$

Gauss sums

The Gauss sum:

$$S_n(a, p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n / p}, \qquad (a, p) = 1.$$

Gauss proved that $|S_2(a, p)| = \sqrt{p}$.

Gauss sums

The Gauss sum:

$$S_n(a,p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a,p)=1.$$

Gauss proved that $|S_2(a,p)| = \sqrt{p}$.

Iff $d=(n,p-1)$, then $S_n(a,p)=S_d(a,p)$. We assume that n divides $p-1$.

Gauss sums

The Gauss sum:

$$S_n(a,p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a,p)=1.$$

Gauss proved that $|S_2(a,p)| = \sqrt{p}$.

Iff $d=(n,p-1)$, then $S_n(a,p)=S_d(a,p)$. We assume that n divides $p-1$.

Hardy-Littlewood 1917:

$$|S_n(a,p)| \le (n-1)p^{1/2}.$$

Is nontrivial when $n < p^{1/2}$.

$$S_n(a,p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a,p) = 1.$$

The problem of obtaining nontrivial estimates for larger values of n was a topic of investigation of many mathematicians.

$$S_n(a,p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a,p) = 1.$$

The problem of obtaining nontrivial estimates for larger values of n was a topic of investigation of many mathematicians.

1991: Shparlinski using a result of Garcia and Voloch (1988) obtained a nontrivial estimate for $n < p^{4/7-\varepsilon}$

$$S_n(a,p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a,p)=1.$$

The problem of obtaining nontrivial estimates for larger values of n was a topic of investigation of many mathematicians.

1991: Shparlinski using a result of Garcia and Voloch (1988) obtained a nontrivial estimate for $n < p^{4/7-\varepsilon}$

Heath-Brown and Konyagin (2000) extended the range to $n < p^{2/3-\varepsilon}$

$$S_n(a,p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a,p) = 1.$$

The problem of obtaining nontrivial estimates for larger values of n was a topic of investigation of many mathematicians.

1991: Shparlinski using a result of Garcia and Voloch (1988) obtained a nontrivial estimate for $n < p^{4/7-\varepsilon}$

Heath-Brown and Konyagin (2000) extended the range to $n < p^{2/3-\varepsilon}$

Konyagin (2003): obtained nontrivial estimate for $n \le p^{3/4-\varepsilon}$.

Another view to Gauss sum

$$S_n(a,p) = 1 + \sum_{x=1}^{p-1} e^{2\pi i a x^n / p}.$$

Another view to Gauss sum

$$S_n(a,p) = 1 + \sum_{x=1}^{p-1} e^{2\pi i a x^n/p}.$$

The set

$$H := \{x^n \pmod p : 1 \le x \le p-1\}$$

is a multiplicative subgroup of $\mathbb{F}_p^*$ of the order $(p-1)/n$.

Another view to Gauss sum

$$S_n(a,p) = 1 + \sum_{x=1}^{p-1} e^{2\pi i a x^n/p}.$$

The set

$$H := \{x^n \pmod{p} : 1 \le x \le p-1\}$$

is a multiplicative subgroup of $\mathbb{F}_p^*$ of the order $(p-1)/n$. Each element $h \in H$ has exactly n representation in the form

$$h \equiv x^n \pmod{p}; \quad 1 \le x \le p-1.$$

Another view to Gauss sum

$$S_n(a,p) = 1 + \sum_{x=1}^{p-1} e^{2\pi i a x^n/p}.$$

The set

$$H := \{x^n \pmod{p} : 1 \le x \le p-1\}$$

is a multiplicative subgroup of $\mathbb{F}_p^*$ of the order $(p-1)/n$. Each element $h \in H$ has exactly n representation in the form

$$h \equiv x^n \pmod{p}; \quad 1 \le x \le p-1.$$

For this reason one has

$$S_n(a,p) = 1 + n\sum_{h\in H} e^{2\pi i a h/p}.$$

Another view to Gauss sum

$$S_n(a,p) = 1 + \sum_{x=1}^{p-1} e^{2\pi i a x^n/p}.$$

The set

$$H := \{x^n \pmod p : 1 \le x \le p-1\}$$

is a multiplicative subgroup of $\mathbb{F}_p^*$ of the order $(p-1)/n$. Each element $h \in H$ has exactly n representation in the form

$$h \equiv x^n \pmod p; \quad 1 \le x \le p-1.$$

For this reason one has

$$S_n(a,p) = 1 + n \sum_{h \in H} e^{2\pi i a h/p}.$$

Thus, the problem is equivalent to the problem of estimating the sum

$$\sum_{x \in H} e^{2\pi i a x/p}.$$

Another view to Gauss sum

$$S_n(a,p) = 1 + \sum_{x=1}^{p-1} e^{2\pi i a x^n/p}.$$

The set

$$H := \{x^n \pmod p : \; 1 \le x \le p-1\}$$

is a multiplicative subgroup of $\mathbb{F}_p^*$ of the order $(p-1)/n$. Each element $h \in H$ has exactly n representation in the form

$$h \equiv x^n \pmod p; \quad 1 \le x \le p-1.$$

For this reason one has

$$S_n(a,p) = 1 + n\sum_{h\in H} e^{2\pi i a h/p}.$$

Thus, the problem is equivalent to the problem of estimating the sum

$$\sum_{x\in H} e^{2\pi i a x/p}.$$

The result of Konyagin applies to the case $|H| > p^{1/4+\varepsilon}$.

We have the representation

$$\sum_{x\in H} e^{2\pi i a x/p} = \frac{1}{|H|^{k-1}} \sum_{x_1\in H} \cdots \sum_{x_k\in H} e^{2\pi i a x_1\ldots x_k/p}.$$

We have the representation

$$\sum_{x\in H} e^{2\pi i a x/p} = \frac{1}{|H|^{k-1}} \sum_{x_1\in H} \dots \sum_{x_k\in H} e^{2\pi i a x_1 \dots x_k/p}.$$

If we take $k=2$, then we can estimate it using Vinogradov's bound:

$$|\sum_{x\in H} e^{2\pi i a x/p}| = \frac{1}{|H|} \Big|\sum_{x_1\in H}\sum_{x_2\in H} e^{2\pi i a x_1 x_2/p}\Big| \le p^{1/2}.$$

We have the representation

$$\sum_{x\in H} e^{2\pi i a x/p} = \frac{1}{|H|^{k-1}} \sum_{x_1\in H} \dots \sum_{x_k\in H} e^{2\pi i a x_1 \dots x_k/p}.$$

If we take $k = 2$, then we can estimate it using Vinogradov's bound:

$$|\sum_{x\in H} e^{2\pi i a x/p}| = \frac{1}{|H|}\Big|\sum_{x_1\in H}\sum_{x_2\in H} e^{2\pi i a x_1 x_2/p}\Big| \le p^{1/2}.$$

But this estimate is nontrivial only in the case $|H| > p^{1/2}$.

We have the representation

$$\sum_{x\in H} e^{2\pi i a x/p} = \frac{1}{|H|^{k-1}} \sum_{x_1\in H} \dots \sum_{x_k\in H} e^{2\pi i a x_1 \dots x_k/p}.$$

If we take $k = 2$, then we can estimate it using Vinogradov's bound:

$$|\sum_{x\in H} e^{2\pi i a x/p}| = \frac{1}{|H|}\Big|\sum_{x_1\in H}\sum_{x_2\in H} e^{2\pi i a x_1 x_2/p}\Big| \le p^{1/2}.$$

But this estimate is nontrivial only in the case $|H| > p^{1/2}$.

Using the sum-product estimate Bourgain, Glibichuk and Konyagin proved the following result.

We have the representation

$$\sum_{x\in H} e^{2\pi i a x/p} = \frac{1}{|H|^{k-1}} \sum_{x_1\in H} \ldots \sum_{x_k\in H} e^{2\pi i a x_1 \ldots x_k/p}.$$

If we take $k = 2$, then we can estimate it using Vinogradov's bound:

$$|\sum_{x\in H} e^{2\pi i a x/p}| = \frac{1}{|H|}\Big|\sum_{x_1\in H}\sum_{x_2\in H} e^{2\pi i a x_1 x_2/p}\Big| \le p^{1/2}.$$

But this estimate is nontrivial only in the case $|H| > p^{1/2}$.

Using the sum-product estimate Bourgain, Glibichuk and Konyagin proved the following result.

THEOREM (BGK). *For any* $\varepsilon > 0$ *there exists a positive integer* $k = k(\varepsilon)$ *such that if* $X \subset \mathbb{F}_p$ *and* $|X| > p^{\varepsilon}$, *then*

$$\Big|\sum_{x_1\in X} \ldots \sum_{x_k\in X} e^{2\pi i a x_1 \ldots x_k/p}\Big| < |X|^k p^{-\delta}, \quad \delta = \delta(\varepsilon) > 0.$$

As a corollary it follows that if H is a subgroup of $\mathbb{F}_p^*$ with $|H| > p^{\varepsilon}$, then for $(a, p) = 1$ we have

$$|\sum_{x\in H} e^{2\pi iax/p}| < |H|^{1-\delta}; \qquad \delta = \delta(\varepsilon) > 0.$$

As a corollary it follows that if H is a subgroup of $\mathbb{F}_p^*$ with $|H| > p^{\varepsilon}$, then for $(a, p) = 1$ we have

$$|\sum_{x\in H} e^{2\pi i a x/p}| < |H|^{1-\delta}; \qquad \delta = \delta(\varepsilon) > 0.$$

In other words, the Gauss sum

$$S_n(a, p) = \sum_{x=0}^{p-1} e^{2\pi i a x^n/p}, \qquad (a, p) = 1.$$

admits a nontrivial estimate for $n < p^{1-\varepsilon}$, with any small fixed constant $\varepsilon > 0$.

We know that if $|X| > p^{1/2+\varepsilon}$ then

$$\left|\sum_{x\in X}\sum_{y\in X} e^{2\pi i axy/p}\right| \le |X|^2 p^{-\varepsilon}.$$

We know that if $|X| > p^{1/2+\varepsilon}$ then

$$\left|\sum_{x\in X}\sum_{y\in X} e^{2\pi i axy/p}\right| \le |X|^2 p^{-\varepsilon}.$$

If $|X| \sim p^{1/2}$, then there is no nontrivial estimate of this bilinear sum.

We know that if $|X| > p^{1/2+\varepsilon}$ then

$$\left|\sum_{x\in X}\sum_{y\in X} e^{2\pi iaxy/p}\right| \le |X|^2 p^{-\varepsilon}.$$

If $|X| \sim p^{1/2}$, then there is no nontrivial estimate of this bilinear sum. Let us consider the trilinear sum

$$S = \sum_{x\in X}\sum_{y\in X}\sum_{z\in X} e^{2\pi iaxyz/p}$$

We know that if $|X| > p^{1/2+\varepsilon}$ then

$$\left|\sum_{x\in X}\sum_{y\in X} e^{2\pi i axy/p}\right| \le |X|^2 p^{-\varepsilon}.$$

If $|X| \sim p^{1/2}$, then there is no nontrivial estimate of this bilinear sum. Let us consider the trilinear sum

$$S = \sum_{x\in X}\sum_{y\in X}\sum_{z\in X} e^{2\pi i axyz/p}$$

The idea is to use the sum-product estimate and try to substitute this sum with a double sum over sets with larger cardinalities.

We know that if $|X| > p^{1/2+\varepsilon}$ then

$$\left|\sum_{x\in X}\sum_{y\in X} e^{2\pi i axy/p}\right| \le |X|^2 p^{-\varepsilon}.$$

If $|X| \sim p^{1/2}$, then there is no nontrivial estimate of this bilinear sum. Let us consider the trilinear sum

$$S = \sum_{x\in X}\sum_{y\in X}\sum_{z\in X} e^{2\pi i axyz/p}$$

The idea is to use the sum-product estimate and try to substitute this sum with a double sum over sets with larger cardinalities. This trilinear sum already contains product-set:

$$\{xy;\, x \in X, y \in X\} = XX.$$

We know that if $|X| > p^{1/2+\varepsilon}$ then

$$\left|\sum_{x\in X}\sum_{y\in X} e^{2\pi iaxy/p}\right| \le |X|^2 p^{-\varepsilon}.$$

If $|X| \sim p^{1/2}$, then there is no nontrivial estimate of this bilinear sum. Let us consider the trilinear sum

$$S = \sum_{x\in X}\sum_{y\in X}\sum_{z\in X} e^{2\pi iaxyz/p}$$

The idea is to use the sum-product estimate and try to substitute this sum with a double sum over sets with larger cardinalities. This trilinear sum already contains product-set:

$$\{xy;\, x\in X, y\in X\} = XX.$$

Furthermore,

$$|S|^2 \le |X|^2 \sum_{y\in X}\sum_{z\in X}\left|\sum_{x_1\in X}\sum_{x_2\in X} e^{2\pi i(x_1+x_2)yz/p}\right|.$$

We know that if $|X| > p^{1/2+\varepsilon}$ then

$$\left|\sum_{x\in X}\sum_{y\in X} e^{2\pi iaxy/p}\right| \le |X|^2 p^{-\varepsilon}.$$

If $|X| \sim p^{1/2}$, then there is no nontrivial estimate of this bilinear sum. Let us consider the trilinear sum

$$S = \sum_{x\in X}\sum_{y\in X}\sum_{z\in X} e^{2\pi iaxyz/p}$$

The idea is to use the sum-product estimate and try to substitute this sum with a double sum over sets with larger cardinalities. This trilinear sum already contains product-set:

$$\{xy;\, x\in X, y\in X\} = XX.$$

Furthermore,

$$|S|^2 \le |X|^2 \sum_{y\in X}\sum_{z\in X}\left|\sum_{x_1\in X}\sum_{x_2\in X} e^{2\pi i(x_1+x_2)yz/p}\right|.$$

And here we have the sum-set

$$X+X = \{x_1+x_2;\, x_1\in X, x_2\in X\}.$$

In general, the sum-product estimate eventually reduces the problem of estimating $2k$-linear sum

$$\sum_{x_1\in X_1}\sum_{x_2\in X_2}\ldots\sum_{x_{2k}\in X_{2k}} e^{2\pi i x_1 x_2 \ldots x_{2k}/p}$$

In general, the sum-product estimate eventually reduces the problem of estimating $2k$-linear sum

$$\sum_{x_1\in X_1}\sum_{x_2\in X_2}\ldots\sum_{x_{2k}\in X_{2k}} e^{2\pi i x_1 x_2\ldots x_{2k}/p}$$

to the problem of estimating k-linear sum:

$$\sum_{y_1\in Y_1}\ldots\sum_{y_k\in Y_k} e^{2\pi i y_1\ldots y_k/p}$$

In general, the sum-product estimate eventually reduces the problem of estimating $2k$-linear sum

$$\sum_{x_1\in X_1}\sum_{x_2\in X_2}\cdots\sum_{x_{2k}\in X_{2k}} e^{2\pi i x_1x_2\ldots x_{2k}/p}$$

to the problem of estimating k-linear sum:

$$\sum_{y_1\in Y_1}\cdots\sum_{y_k\in Y_k} e^{2\pi i y_1\ldots y_k/p}$$

but now the cardinalities of Y_i are much larger than of X_i (say, $|Y_i|\geq|X_i|^{1.0001}$).

In general, the sum-product estimate eventually reduces the problem of estimating $2k$-linear sum

$$\sum_{x_1\in X_1}\sum_{x_2\in X_2}\cdots\sum_{x_{2k}\in X_{2k}} e^{2\pi i x_1 x_2\ldots x_{2k}/p}$$

to the problem of estimating k-linear sum:

$$\sum_{y_1\in Y_1}\cdots\sum_{y_k\in Y_k} e^{2\pi i y_1\ldots y_k/p}$$

but now the cardinalities of Y_i are much larger than of X_i (say, $|Y_i|\ge|X_i|^{1.0001}$). Take k to be a big power of 2 and iterate it until we arrive at bilinear sum

$$\sum_{u\in U}\sum_{v\in V} e^{2\pi i uv/p}$$

with $|U||V|>p^{1+c}$.

In general, the sum-product estimate eventually reduces the problem of estimating $2k$-linear sum

$$\sum_{x_1\in X_1}\sum_{x_2\in X_2}\cdots\sum_{x_{2k}\in X_{2k}} e^{2\pi i x_1x_2\ldots x_{2k}/p}$$

to the problem of estimating k-linear sum:

$$\sum_{y_1\in Y_1}\cdots\sum_{y_k\in Y_k} e^{2\pi i y_1\ldots y_k/p}$$

but now the cardinalities of Y_i are much larger than of X_i (say, $|Y_i|\geq |X_i|^{1.0001}$). Take k to be a big power of 2 and iterate it until we arrive at bilinear sum

$$\sum_{u\in U}\sum_{v\in V} e^{2\pi i uv/p}$$

with $|U||V|>p^{1+c}$. Then apply Vinogradov's bilinear sum estimate.

In general, the sum-product estimate eventually reduces the problem of estimating $2k$-linear sum

$$\sum_{x_1\in X_1}\sum_{x_2\in X_2}\cdots\sum_{x_{2k}\in X_{2k}} e^{2\pi i x_1 x_2\ldots x_{2k}/p}$$

to the problem of estimating k-linear sum:

$$\sum_{y_1\in Y_1}\cdots\sum_{y_k\in Y_k} e^{2\pi i y_1\ldots y_k/p}$$

but now the cardinalities of Y_i are much larger than of X_i (say, $|Y_i|\geq|X_i|^{1.0001}$). Take k to be a big power of 2 and iterate it until we arrive at bilinear sum

$$\sum_{u\in U}\sum_{v\in V} e^{2\pi i uv/p}$$

with $|U||V|>p^{1+c}$. Then apply Vinogradov's bilinear sum estimate.

To implement into reality one more tool is needed, Balog-Szemeredi-Gowers type estimates.

One recent application, in 2014.

M. Z. Garaev
Centro de Ciencias Matemáticas, UNAM, campus Morelia, México

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \cdots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \ldots x_n)^*/p}; \qquad (a, p) = 1$$

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \dots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \dots x_n)^*/p}; \qquad (a,p)=1$$

The trivial bound is $\leq N_1 N_2 \cdots N_n$.

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \ldots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \ldots x_n)^*/p}; \qquad (a,p)=1$$

The trivial bound is $\leq N_1 N_2 \cdots N_n$. The problem is to obtain a nontrivial bound. Consider the case $N_1 = \ldots = N_n = N$.

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \dots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \dots x_n)^*/p}; \qquad (a,p)=1$$

The trivial bound is $\le N_1 N_2 \cdots N_n$. The problem is to obtain a nontrivial bound. Consider the case $N_1 = \ldots = N_n = N$.
Luo in 1999

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \cdots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \ldots x_n)^* / p}; \qquad (a, p) = 1$$

The trivial bound is $\leq N_1 N_2 \cdots N_n$. The problem is to obtain a nontrivial bound. Consider the case $N_1 = \ldots = N_n = N$.
Luo in 1999 and Shparlinski in 2007:

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \cdots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \ldots x_n)^*/p}; \qquad (a,p)=1$$

The trivial bound is $\leq N_1 N_2 \cdots N_n$. The problem is to obtain a nontrivial bound. Consider the case $N_1 = \ldots = N_n = N$.
Luo in 1999 and Shparlinski in 2007: for large values of n one has a nontrivial bound in the range

$$N^n > p^{n/4+\sqrt{n/2}+\ldots}.$$

M. Z. Garaev
Centro de Ciencias Matemáticas, UNAM, campus Morelia, México

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \dots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \dots x_n)^*/p}; \qquad (a,p)=1$$

The trivial bound is $\leq N_1 N_2 \cdots N_n$. The problem is to obtain a nontrivial bound. Consider the case $N_1 = \ldots = N_n = N$.
Luo in 1999 and Shparlinski in 2007: for large values of n one has a nontrivial bound in the range

$$N^n > p^{n/4+\sqrt{n/2}+\dots}.$$

Now the sum-product estimates eventually leads to the following result

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \cdots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \ldots x_n)^*/p}; \qquad (a,p)=1$$

The trivial bound is $\leq N_1 N_2 \cdots N_n$. The problem is to obtain a nontrivial bound. Consider the case $N_1 = \ldots = N_n = N$.
Luo in 1999 and Shparlinski in 2007: for large values of n one has a nontrivial bound in the range

$$N^n > p^{n/4+\sqrt{n/2}+\ldots}.$$

Now the sum-product estimates eventually leads to the following result
Theorem. (Bourgain & G., 2014). *For $N > p^{4/n^2}$, we have*

$$\Big| \sum_{x_1=M_1+1}^{M_1+N} \cdots \sum_{x_n=M_n+1}^{M_n+N} e^{2\pi i a (x_1 \ldots x_n)^*/p} \Big| < N^n p^{-\delta}$$

for some $\delta = \delta(n) > 0$.

One recent application, in 2014.
The incomplete n-linear Kloosterman sums

$$\sum_{x_1=M_1+1}^{M_1+N_1} \cdots \sum_{x_n=M_n+1}^{M_n+N_n} e^{2\pi i a (x_1 \ldots x_n)^*/p}; \qquad (a, p) = 1$$

The trivial bound is $\leq N_1 N_2 \cdots N_n$. The problem is to obtain a nontrivial bound. Consider the case $N_1 = \ldots = N_n = N$.
Luo in 1999 and Shparlinski in 2007: for large values of n one has a nontrivial bound in the range

$$N^n > p^{n/4 + \sqrt{n/2} + \ldots}.$$

Now the sum-product estimates eventually leads to the following result
THEOREM. (Bourgain & G., 2014). *For $N > p^{4/n^2}$, we have*

$$\Big| \sum_{x_1=M_1+1}^{M_1+N} \cdots \sum_{x_n=M_n+1}^{M_n+N} e^{2\pi i a (x_1 \ldots x_n)^*/p} \Big| < N^n p^{-\delta}$$

for some $\delta = \delta(n) > 0$.
Suffices $N^n > p^{4/n}$.

Investigations on very short Kloosterman sums started with works of Karatsuba continued by Korolev.

THEOREM. (Bourgain & G., 2014). *The following bound holds:*

$$\max_{(a,p)=1}\left|\sum_{n\le N} e_p(an^*)\right| \ll \frac{(\log\log p)^3\log p}{(\log N)^{3/2}}\,N,$$

where the implied constant is absolute.

Investigations on very short Kloosterman sums started with works of Karatsuba continued by Korolev.

Theorem. (Bourgain & G., 2014). *The following bound holds:*

$$\max_{(a,p)=1}\left|\sum_{n\le N} e_p(an^*)\right| \ll \frac{(\log\log p)^3 \log p}{(\log N)^{3/2}}\, N,$$

where the implied constant is absolute.

It follows that if $N = p^{\varepsilon}$ with $\varepsilon > 0$ fixed, the saving is $O((\log\log p)^3/(\log p)^{1/2})$ and the estimate is nontrivial if $N > \exp((\log p)^{\frac{2}{3}}(\log\log p)^3)$.

Problem

Problem

Let $A \subset \mathbb{F}_p$. Obtain optimal sum-product estimate.

What is a conjectured bound?

Problem

Let $A \subset \mathbb{F}_p$. Obtain optimal sum-product estimate.

What is a conjectured bound? One should be careful.

The seemingly reasonable conjecture

$$\max\{|A+A|, |AA|\} \gtrsim \min\{p, |A|^2\}$$

is false.

Problem

Let $A \subset \mathbb{F}_p$. Obtain optimal sum-product estimate.

What is a conjectured bound? One should be careful.

The seemingly reasonable conjecture

$$\max\{|A+A|, |AA|\} \gtrsim \min\{p, |A|^2\}$$

is false.

For any $N \in [1, p]$ one can construct a subset $A \subset \mathbb{F}_p$ with $|A| = N$ such that

$$\max\{|A+A|, |AA|\} \leq c_1 \sqrt{p|A|}.$$

Problem

Let $A \subset \mathbb{F}_p$. Obtain optimal sum-product estimate.

What is a conjectured bound? One should be careful.

The seemingly reasonable conjecture

$$\max\{|A+A|, |AA|\} \gtrsim \min\{p, |A|^2\}$$

is false.

For any $N \in [1, p]$ one can construct a subset $A \subset \mathbb{F}_p$ with $|A| = N$ such that

$$\max\{|A+A|, |AA|\} \le c_1\sqrt{p|A|}.$$

For instance, if $|A| \approx p^{1/2}$ then

$$\max\{|A+A|, |AA|\} \le c_1|A|^{3/2} \approx p^{3/4}.$$

Conjecture.

$$\max\{|A+A|, |AA|\} \gtrsim \min\{|A|^2, \sqrt{p|A|}\}.$$

Conjecture.

$$\max\{|A+A|, |AA|\} \gtrsim \min\{|A|^2, \sqrt{p|A|}\}.$$

THEOREM. (G., 2008). *If $|A| > p^{2/3}$, then the conjecture is true:*

$$\max\{|A+A|, |AA|\} \geq c\sqrt{p|A|}, \quad c > 0.$$

Conjecture.

$$\max\{|A+A|, |AA|\} \gtrsim \min\{|A|^2, \sqrt{p|A|}\}.$$

THEOREM. (G., 2008). *If $|A| > p^{2/3}$, then the conjecture is true:*

$$\max\{|A+A|, |AA|\} \geq c\sqrt{p|A|}, \quad c > 0.$$

THEOREM. (Roche-Newton, Rudnev, Shkredov, 2016). *If $|A| < p^{5/8}$, then*

$$\max\{|A+A|, |AA|\} \geq c|A|^{6/5}, \quad c > 0.$$