Product and quotient sets of the finite subsets of rationals and integers.

Yurii Shteinikov

Steklov Mathematical Institute.

Pecs, 2017
Start

1. \( Q \) is large positive integer.
2. All logarithms are on base \( e \).

Plan of the talk

1. Product sets of rationals
2. Product and quotient sets of integers
Definitions

1. Let $A, B$ be the sets rational numbers:

   $$A, B \subseteq F_Q = \{r/s, 1 \leq r, s \leq Q\}$$

2. The set $AB$ and is called the product set of $A \cap B$, which is defined as

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

3. I will talk about some results for the lower bound of $|AB|$. 
Some history

J. Bourgain, S. Konyagin and I. Shparlinski proved the following Theorem.

**THEOREM 1**  [2008]

Let $A, B \subseteq F_Q$, then we have the following estimate

$$|AB| \geq |A||B|\exp\left\{(-9 + o(1)) \frac{\log Q}{\sqrt{\log \log Q}} \right\}, Q \to \infty, \quad (1)$$

J. Cilleruelo obtained a slightly better result using a different method.

**THEOREM 2**  [2016]

Let $A, B \subseteq F_Q$, then we have the following estimate

$$|AB| \geq |A||B|\exp\left\{(-4\sqrt{\log 2} + o(1)) \frac{\log Q}{\sqrt{\log \log Q}} \right\}, Q \to \infty, \quad (2)$$
**Some history**

J. Bourgain, S. Konyagin and I. Shparlinski proved the following Theorem.

**THEOREM 1** [2008]

Let $A, B \subseteq F_Q$, then we have the following estimate

$$|AB| \geq |A||B|\exp\left\{(-9 + o(1))\frac{\log Q}{\sqrt{\log \log Q}}\right\}, Q \to \infty, \quad (1)$$

J. Cilleruelo obtained a slightly better result using a different method.

**THEOREM 2** [2016]

Let $A, B \subseteq F_Q$, then we have the following estimate

$$|AB| \geq |A||B|\exp\left\{(-4\sqrt{\log 2} + o(1))\frac{\log Q}{\sqrt{\log \log Q}}\right\}, Q \to \infty, \quad (2)$$
Applications

1. Distribution of elements of cosets of multiplicative subgroups

2. Fixed points of discrete logarithm

Suppose that $A, B \in [1, Q]$.

It is easy to see that

$$|AB| \geq |A||B| \exp \left\{ (-2\log 2 + o(1)) \frac{\log Q}{\log \log Q} \right\}, \quad Q \to \infty.$$ 

Proof:

1. The number $r_{A,B}(n)$ of pairs $(a, b)$ such that $n = ab$ is less or equal to $\tau(n)$.
2. $n \leq Q^2$ and we are using well-known upper bound for $\tau(n)$,

$$\tau(n) < \exp \left\{ (\log 2 + o(1)) \frac{\log n}{\log \log n} \right\}, \quad n \to \infty.$$ 

Suppose $A, B \in F_Q$. Then the proof does not work, – the problem is in the first step.
Applications

1. Distribution of elements of cosets of multiplicative subgroups

2. Fixed points of discrete logarithm

Suppose that $A, B \in [1, Q]$.

It is easy to see that

$$|AB| \geq |A||B| \exp\left\{(-2\log 2 + o(1)) \frac{\log Q}{\log \log Q}\right\}, Q \to \infty.$$

Proof:

1. The number $r_{A,B}(n)$ of pairs $(a, b)$ such that $n = ab$ is less or equal to $\tau(n)$.

2. $n \leq Q^2$ and we are using well-known upper bound for $\tau(n)$,

$$\tau(n) < \exp\left\{(\log 2 + o(1)) \frac{\log n}{\log \log n}\right\}, n \to \infty.$$

Suppose $A, B \in F_Q$. Then the proof does not work, – the problem is in the first step.
Applications

1. Distribution of elements of cosets of multiplicative subgroups

2. Fixed points of discrete logarithm

Suppose that $A, B \in [1, Q]$.

It is easy to see that

$$|AB| \geq |A||B| \exp\left\{(-2\log 2 + o(1)) \frac{\log Q}{\log \log Q}\right\}, \ Q \to \infty.$$

Proof:

1. The number $r_{A,B}(n)$ of pairs $(a, b)$ such that $n = ab$ is less or equal to $\tau(n)$.
2. $n \leq Q^2$ and we are using well-known upper bound for $\tau(n)$,

$$\tau(n) < \exp\left\{(\log 2 + o(1)) \frac{\log n}{\log \log n}\right\}, \ n \to \infty.$$

Suppose $A, B \in F_Q$. Then the proof does not work, – the problem is in the first step.
Main result

**THEOREM 1** [Y.S.] There is an absolute constant $C > 0$ such that if $A, B \subseteq F_Q$, then we have the following estimate

$$|AB| \geq |A||B|\exp\left\{(-C + o(1))\frac{\log Q}{\log \log Q}\right\}, \quad Q \to \infty, \quad (3)$$

The constant $C$ can be taken $8 \log 2$. In the case $A = B$ one can take $C = 6 \log 2$ and $C$ cannot be taken smaller than $4 \log 2$. 
Elements of the proof

Consider the case $A = B$.

Proof

1. Let $\nu = \{\nu_p\}, p \leq Q$ be vector where each coordinate is $+1$ or $-1$.
2. Define the set $A_\nu \subseteq A$ as is written below

$$A_\nu = \left\{ a \in A : \forall p \left\{ \begin{array}{l} \nu(p) = 1 \Rightarrow \nu_p(a) \geq 0; \\
\nu(p) = -1 \Rightarrow \nu_p(a) \leq 0. \end{array} \right. \right\}$$

3. Consider random set $A_\nu$, where vector $\nu = \{\nu(p)_{p \leq Q}\}$ is a random variable (vector), where each coordinate $\nu(p)$ is $\pm 1$ with probability $\frac{1}{2}$ and $\nu(p)$ are independent for different $p$.
4. It is easy to estimate mean value (expectation) of $|A_\nu|$.
5. if $r/s$ and $r'/s' \in A_\nu$, then $\text{gcd}(r, s') = \text{gcd}(r', s) = 1$ and the result easily follows.
The result about the energy of the sets $A, B$

The multiplicative energy $E(A, B)$ of two sets $A, B$ is

$$E(A, B) = |\{a_1b_1 = a_2b_2 : a_1, a_2 \in A; b_1, b_2 \in B\}|.$$

It is easy to show that $|AB| \geq \frac{|A|^2|B|^2}{E(A,B)}$.

We note that using good estimates of $E(A, B)$ one can deduce non-trivial estimates of the size of $AB$ but not vice versa.

**THEOREM** [Y.S.] *There is an absolute constant $C > 0$ such that if $A, B \subseteq F_Q$ then we have*

$$E(A, B) \leq |A||B| \exp\left\{(C + o(1))\frac{\log Q}{\log \log Q}\right\}, \; Q \to \infty, \; (4)$$

*and $C$ can be taken $8 \log 2$.*

This Theorem generalize the previous result.
The result about the energy of the sets $A, B$

The multiplicative energy $E(A, B)$ of two sets $A, B$ is

$$E(A, B) = |\{a_1 b_1 = a_2 b_2 : a_1, a_2 \in A; b_1, b_2 \in B\}|.$$

It is easy to show that $|AB| \geq \frac{|A|^2 |B|^2}{E(A, B)}$.

We note that using good estimates of $E(A, B)$ one can deduce non-trivial estimates of the size of $AB$ but not vice versa.

**THEOREM** [Y.S.] *There is an absolute constant $C > 0$ such that if $A, B \subseteq \mathbb{F}_Q$ then we have*

$$E(A, B) \leq |A||B| \exp\left((C + o(1)) \frac{\log Q}{\log \log Q}\right), \; Q \to \infty, \quad (4)$$

*and $C$ can be taken $8 \log 2$. This Theorem generalize the previous result.*
The result about the energy of the sets $A, B$

The multiplicative energy $E(A, B)$ of two sets $A, B$ is

$$E(A, B) = |\{a_1b_1 = a_2b_2 : a_1, a_2 \in A; b_1, b_2 \in B\}|.$$ 

It is easy to show that $|AB| \geq \frac{|A|^2|B|^2}{E(A, B)}$. We note that using good estimates of $E(A, B)$ one can deduce non-trivial estimates of the size of $AB$ but not vice versa.

**Theorem** [Y.S.] There is an absolute constant $C > 0$ such that if $A, B \subseteq F\mathbb{Q}$ then we have

$$E(A, B) \leq |A||B| \exp\left\{(C + o(1))\frac{\log Q}{\log \log Q}\right\}, \quad Q \to \infty, \quad (4)$$

and $C$ can be taken $8\log 2$.

This Theorem generalize the previous result.
The result about the energy of the sets $A, B$

The multiplicative energy $E(A, B)$ of two sets $A, B$ is

$$E(A, B) = |\{a_1b_1 = a_2b_2 : a_1, a_2 \in A; b_1, b_2 \in B\}|.$$

It is easy to show that $|AB| \geq \frac{|A|^2|B|^2}{E(A,B)}$.

We note that using good estimates of $E(A, B)$ one can deduce non-trivial estimates of the size of $AB$ but not vice versa.

**THEOREM** [Y.S.] *There is an absolute constant $C > 0$ such that if $A, B \subseteq \mathbb{F}_Q$ then we have*

$$E(A, B) \leq |A||B| \exp\left\{(C + o(1))\frac{\log Q}{\log \log Q}\right\}, \quad Q \to \infty, \quad (4)$$

*and $C$ can be taken $8 \log 2$.*

This Theorem generalize the previous result.
Quotient sets of integers

One can easily obtain the following proposition:

*If* $A, B \subseteq [1, Q]$ *then we have the following estimate*

$$|AB|, |A/B| \geq |A||B| \exp\left\{(-2 \log 2 + o(1)) \frac{\log Q}{\log \log Q}\right\}, \quad Q \to \infty.$$  

(5)

For the case $|A/B|$ this estimate cannot be improved very much in general except for the constant $-2 \log 2$. But still the following Theorem takes place.

**Theorem**

*There is an absolute constant* $c > 0$, *such that if* $A, B \subseteq [1, Q]$ *then we have the following estimate*

$$|A/B| \geq |A||B| \exp\left\{(-2 \log 2 + c + o(1)) \frac{\log Q}{\log \log Q}\right\}, \quad Q \to \infty.$$  

(6)

One can take $c = 0.1$
Questions

1) Is it possible to improve the coefficients $6 \log 2$ and $8 \log 2$ in the Theorem concerning product sets of rationals?
References


Thank you for your attention