An extension of
Bourgain and Garaev’s sum-product estimates

by

CHUN-YEN SHEN (Bloomington, IN)

0. Introduction. Let $\mathbb{F}_p$ be the finite field of a prime order $p$. From the work of Bourgain, Katz and Tao, with subsequent refinement by Bourgain, Glibichuk and Konyagin, it is known that one has the following sum-product result:

**Theorem [BKT, BGK].** If $A$ is a subset of $\mathbb{F}_p$ with $|A| < p^{1-\delta}$, where $\delta > 0$, then for some $\varepsilon > 0$ one has the sum-product estimate

$$|A + A| + |AA| \gtrsim |A|^{1+\varepsilon}.$$ 

Later many quantitative versions of sum-product estimates have been given ([G1]–[TV]). Garaev [G1] showed that in the most nontrivial range $|A| < p^{1/2}$, one has

$$|A + A| + |AA| \gtrsim |A|^{15/14},$$

which was slightly improved in [KS1] to

$$|A + A| + |AA| \gtrsim |A|^{14/13}.$$ 

Very recently, Bourgain and Garaev [BG] showed the following estimates:

**Theorem [BG].** For any subset $A \subset \mathbb{F}_p$,

$$E_x(A, A)^4 \lesssim \left(|A - A| + \frac{|A|^3}{p}\right)|A|^5|A - A|^4|2A - 2A|,$$

where $E_x(A, B)$ is the multiplicative energy between sets $A$ and $B$, defined as

$$E_x(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : a_1 b_1 = a_2 b_2\}|.$$

Then by adopting the arguments of Katz and Shen [KS1], they derived the following result:

---

2000 Mathematics Subject Classification: Primary 11B75; Secondary 12E20.

**Key words and phrases:** sum-product estimates, expanding maps.
Corollary [BG]. For any subset $A \subset \mathbb{F}_p$, there exists a subset $A' \subset A$ with $|A'| \gtrapprox |A|$ such that

$$E_x(A', A')^4 \lessapprox \left( |A - A| + \frac{|A|^3}{p} \right)|A|^3|A - A|^7.$$ 

Since

$$E_x(A', A') \gtrapprox \frac{|A|^4}{|AA'|},$$

the Corollary implies that if $|A| < p^{12/23}$, then

(*)

$$|A - A| + |AA| \gtrapprox |A|^{13/12}.$$ 

In this paper, we give a shorter and simpler proof of Bourgain and Garaev’s variant of sum-product estimate and extend it to a more general setting, namely:

**Theorem.** Let $F : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ be defined by $F(x, y) = x(g(x) + by)$, where $b \in \mathbb{F}_p^*$ and $g : \mathbb{F}_p \to \mathbb{F}_p$ is any function. Then for any $A \subset \mathbb{F}_p$ with $|A| < p^{1/2},$

$$|A - A| + |F(A, A)| \gtrapprox |A|^{13/12}.$$ 

Taking $g = 0$, $b = 1$ we get the result (*) of Bourgain and Garaev.

**Acknowledgements.** The author wishes to thank Nets Katz for many helpful discussions and pointing out the useful covering lemma (Lemma 1.3).

1. **Preliminaries.** For given quantities $X$ and $Y$ we use the notation

$$X \lessapprox Y \text{ to mean } X \leq CY,$$

where the constant $C$ is universal (i.e. independent of $p$ and $A$). The constant $C$ may vary from line to line. We also use

$$X \lessapprox Y \text{ to mean } X \leq C(\log |A|)^\alpha Y,$$

and $X \approx Y$ to mean $X \lessapprox Y$ and $Y \lessapprox X$, where $C$ and $\alpha$ may vary from line to line but are universal.

We present some preliminary lemmas; the first two are proved in [KS1].

**Lemma 1.1.** Let $A_1 \subset \mathbb{F}_p$ with $1 < |A_1| < p^{1/2}$. Then for any elements $a_1, a_2, b_1, b_2$ so that

$$\frac{b_1 - b_2}{a_1 - a_2} - 1 \notin \frac{A_1 - A_1}{A_1 - A_1},$$

we have, for any $A' \subset A_1$ with $|A'| \gtrapprox |A_1|,$

$$|(a_1 - a_2)A' - (a_1 - a_2)A' + (b_1 - b_2)A'| \gtrapprox |A_1|^2.$$
In particular, such $a_1, a_2, b_1, b_2$ exist unless $(A_1 - A_1)/(A_1 - A_1) = \mathbb{F}_p$. In case $(A_1 - A_1)/(A_1 - A_1) = \mathbb{F}_p$, we may find $a_1, a_2, b_1, b_2 \in A_1$ so that

$$|(a_1 - a_2)A_1 + (b_1 - b_2)A_1| \gtrsim |A_1|^2.$$  

**Lemma 1.2.** Let $X, B_1, \ldots, B_k$ be any subsets of $\mathbb{F}_p$. Then there exists $X' \subset X$ with $|X'| > \frac{1}{2}|X|$ so that

$$|X' + B_1 + \cdots + B_k| \lesssim \frac{|X + B_1| \cdots |X + B_k|}{|X|^{k-1}}.$$  

**Lemma 1.3.** Let $C$ and $D$ be sets with $|D| \gtrsim |C|/K$ and with $|C - D| \leq K|C|$. Then there is $C' \subset C$ with $|C'| \geq \frac{9}{10}|C|$ so that $C'$ can be covered by $\sim K^2$ translates of $-D$. Similarly, there is $C'' \subset C$ with $|C''| \geq \frac{9}{10}|C|$ so that $C''$ can be covered by $\sim K^2$ translates of $D$.

**Proof.** To prove the first half of the statement, it suffices to show that we can find one translate of $-D$ whose intersection with $C$ is of size at least $|C|/K^2$. Once we find such a translate, we remove the intersection and then iterate. We stop when the size of the remaining part of $C$ is less than $|C|/10$. To prove the second half of the statement we have to show there is a translate of $D$ whose intersection with $C$ is of size at least $|C|/K^2$.

First, by the Cauchy–Schwarz inequality, we have

$$|(c, d, c', d') \in C \times D \times C \times D : c - d = c' - d'| \geq \frac{|C|^2|D|^2}{|C - D|},$$

which implies that

$$|(c, d, c', d') \in C \times D \times C \times D : c - d = c' - d'| \geq \frac{|C||D|^2}{K}.$$  

The quantity on the left hand side is equal to

$$\sum_{c \in C} \sum_{d' \in D} \sum_{d' \in D} |(c - D) \cap (C - d')|.$$  

Thus we can find $c \in C$ and $d' \in D$ so that

$$|(c - D) \cap (C - d')| \geq \frac{|D|}{K} \gtrsim \frac{|C|}{K^2}.$$  

Hence, $|(c + d' - D) \cap C| \gtrsim |C|/K^2$, which is just what we wanted to prove.

To prove the second half of the statement we start with the inequality

$$\sum_{d \in D} \sum_{c \in C} |(d + C) \cap (D + c)| \geq \frac{|C||D|^2}{K^2}.$$  

Proceeding as above, we find $c \in C$ and $d \in D$ such that

$$|(c - d + D) \cap C| \gtrsim |C|/K^2$$

and the result follows. ■
2. Proof of the Theorem. We start with $|A - A| \leq K|A|$ and $|F(A, A)| \leq K|A|$. By using Plünnecke’s inequality, we can find $A' \subset A$ with $|A'| \gtrsim |A|$ so that

$$|A' - A' - A' - A'| \lesssim K^3|A|.$$ 

First, by the Cauchy–Schwarz inequality, we have

$$\sum_{a' \in A'} \sum_{a' \in A'} |a(a(a) + bA') \cap a'(a'(a') + bA')| \gtrsim \frac{|A'|^3}{K}.$$ 

Therefore, following Garaev’s arguments [G1], we can find $A'' \subset A'$ and $a_0 \in A'$ so that

$$|A''| \gtrsim K^{-\beta}|A'|$$

for some $\beta \geq 0$, and for every $a \in A''$ we have

$$|a(a(a) + bA') \cap a_0(a_0(a) + bA')| \gtrsim K^{\beta - 1}|A|.$$ 

As in the argument of Garaev, the worst case is $\beta = 0$, so let us assume this for simplicity. Now there are two cases.

In the first case, we have

$$\frac{A'' - A''}{A'' - A''} = F.$$ 

If so, applying Lemma 1.1, we can find $a_1, a_2, b_1, b_2 \in A''$ so that

$$|A''|^2 \lesssim |(a_1 - a_2)A'' + (b_1 - b_2)A''| \lesssim |a_1A'' - a_2A'' + b_1A'' - b_2A''|$$

$$= |a_1g(a_1) + a_1bA'' - a_2g(a_2) - a_2bA'' + b_1g(b_1) + b_1bA'' - b_2g(b_2) - b_2bA''|$$

$$= |a_1(g(a_1) + bA'') - a_2(g(a_2) + bA'') + b_1(g(b_1) + bA'') - b_2(g(b_2) + bA'')|. $$

Now we apply Lemma 1.3 to find $A'''$ whose size is at least $6/10$ that of $A''$ so $a_1(g(a_1) + bA'''), a_2(g(a_2) + bA'''), b_1(g(b_1) + bA'''),$ and $b_2(g(b_2) + bA''')$ can be covered by $\sim K^2$ translates of $a_0(g(a_0) + bA'), a_0(g(a_0) + bA'''), a_0(g(a_0) + bA'''), a_0(g(a_0) + bA''')$ and $a_0(g(a_0) + bA''')$ respectively. But then

$$a_1(g(a_1) + bA''') - a_2(g(a_2) + bA''') + b_1(g(b_1) + bA''') - b_2(g(b_2) + bA''')$$

can be covered by $\sim K^3$ translates of

$$a_0(g(a_0) + bA') - a_0(g(a_0) + bA') - a_0(g(a_0) + bA') - a_0(g(a_0) + bA').$$

Since

$$|a_0(g(a_0) + bA') - a_0(g(a_0) + bA') - a_0(g(a_0) + bA') - a_0(g(a_0) + bA')|$$

$$= |A' - A' - A' - A'| \lesssim K^3|A|$$

by the definition of $A'$, we thus get

$$|a_1A''' - a_2A''' + a_3A''' - a_4A'''| \lesssim K^{11}|A|.$$
Therefore
\[ |A'|^2 \lesssim K^{11}|A|, \]
which implies that \( K \gtrapprox |A|^{1/11} \gtrapprox |A|^{1/12} \), so that we have more than we need in this case.

Thus we are left with the case that
\[ \frac{A'' - A''}{A'' - A''} \notin \mathbb{F}_p. \]

Applying Lemma 1.1, we can find \( a_1, a_2, b_1, b_2 \in A'' \) such that
\[ \frac{b_1 - b_2}{a_1 - a_2} - 1 \notin \frac{A'' - A''}{A'' - A''}. \]

Then we have
\[ |A''|^2 \lesssim |(a_1 - a_2)A'' - (a_1 - a_2)A'' + (b_1 - b_2)A''|. \]

Now by applying Lemma 1.2, we get
\[ |A''|^2 \lesssim \frac{|A - A|}{|A|} |(a_1 - a_2)A'' + (b_1 - b_2)A''|. \]

Applying the same argument as above leads to
\[ |A'|^2 \lesssim K^{12}|A|, \]
which implies that \( K \gtrapprox |A|^{1/12} \). ■

**Remark.** Based on the same arguments, in the paper [S] the author also showed that if \( |A| < p^{1/2} \), then one has
\[ |A + A| + |AA| \gtrapprox |A|^{13/12}. \]

**References**


Department of Mathematics  
Indiana University  
Rawles Hall  
831 East Third St.  
Bloomington, IN 47405, U.S.A.  
E-mail: shenc@indiana.edu

Received on 29.4.2008  
and in revised form on 23.7.2008