Quantitative sum product estimates on different sets

Chun-Yen Shen

Department of Mathematics
Indiana University
Bloomington, IN 47405

shenc@indiana.edu

Submitted: Apr 26, 2008; Accepted: Oct 30, 2008; Published: Nov 14, 2008
Mathematics Subject Classification: 11B75 (12E20)

Abstract

Let F_p be a finite field of p elements with p prime. In this paper we show that for $A, B \subset F_p$ with $|B| \leq |A| < p^{\frac{1}{2}}$ then

$$\max\left(|A+B|, |AB|\right) \gtrapprox \left(\frac{|B|^{14}}{|A|^{13}}\right)^{1/18} |A|.$$

This gives an explicit exponent in a sum-product estimate for different sets by Bourgain.

1 Introduction

The sum-product phenomenon has been intensively investigated, since Erdős and Szemerèdi made their well known conjecture that

$$\max(|A+A|, |AA|) \geq C_\epsilon |A|^{2-\epsilon} \quad \forall \epsilon > 0.$$

where A is a finite subset of integers and

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

and

$$AA = \{ab : a \in A, b \in A\}.$$

Much work has been done to find the explicit exponents and the best result to date is due to Solymosi [12] who showed that

$$\max(|A+A|, |AA|) \geq C_\epsilon |A|^{\frac{4}{3}-\epsilon}.$$

From the work of Bourgain, Katz and Tao [1], with subsequent refinement by Bourgain, Glibichuk and Konyagin [2], it is known that one has the following sum-product result:

Theorem 1.1 *If A is a subset of F_p, the field of p elements with p prime and if $|A| < p^{1-\delta}$, where $\delta > 0$, then one has the sum product estimate*

$$\max(|A+A|, |AA|) \geq |A|^{1+\epsilon}$$

for some $\epsilon > 0$.

Since then there are several generalizations and applications.(e.g. [1]-[4], [13]). For example, it was shown by Bourgain [3] that if $A, B \subset F_p$ and $P^{\delta} < |B| \leq |A| < p^{1-\delta}$, then for some $\epsilon > 0$, one has

$$\max(|A+B|, |AB|) \geq p^{\epsilon}|A|.$$

Nets Katz and the author [10] also obtained an analogous result in the sets of fields which are not necessarily of prime order under additional hypotheses, since it is known that the problem becomes more complicated in fields not of prime order due to the presence of non-trivial subfields or their dilates. Recently many quantitative versions of sum-product estimates in prime fields have been given (e.g. [4]-[11]). For example, in the paper [11] the author showed that if $A \subset F_p$ with $|A| < p^{\frac{1}{2}}$ then

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

where F : $F_p \times F_p$ to F_p , $(x,y) \rightarrow x(f(x)+by)$, f is any function and $b \in F_p^*$. In the paper [7] Garaev showed that if $A, B \subset F_p^*$ then

$$\max(|A+A|, |AB|) \gtrapprox \Big(\min\big\{|B|, \frac{p}{|A|}\big\}\Big)^{1/25}|A|.$$

In this paper we give an explicit exponent on Bourgain's sum-product estimate and extend the result by Garaev from comparing $|AB|$ with $|A+A|$ to $|AB|$ with $|A+B|$, namely :

Theorem 1.2 *Let F_p be a finite field of p elements with p prime. Then for $A, B \subset F_p$ with $|B| \leq |A| < p^{\frac{1}{2}}$ we have*

$$\max(|A+B|, |AB|) \gtrapprox \left(\frac{|B|^{14}}{|A|^{13}}\right)^{1/18}|A|.$$

Remark 1.3 *Taking $|B| \gtrsim |A|^{\frac{13}{14}+\delta}$ for some $\delta > 0$, we get a generalization of the result by Bourgain, Katz and Tao [1].*

2 Preliminaries

Throughout this paper A will denote a fixed set in the field F_p of p elements with p prime. For B, any set, we will denote its cardinality by $|B|$. Whenever X and Y are quantities we will use

$$X \lesssim Y,$$

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 will use

$$X \lessapprox Y,$$

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 α may vary from line to line but are universal.

We give some preliminary lemmas. The first two can be found in [9].

Lemma 2.1 *Let $A_1 \subset F_p$ with $1 < |A_1| < p^{\frac{1}{2}}$. 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 that 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 $\frac{A_1 - A_1}{A_1 - A_1} = F_p$. In case $\frac{A_1 - A_1}{A_1 - A_1} = F_p$, we may find $a_1, a_2, b_1, b_2 \in A_1$ so that

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

Lemma 2.2 *Let $X, B_1, \ldots, B_k$ be any subsets of F_p.Then there is $X' \subset X$ with $|X'| > \frac{1}{2}|X|$ so that*

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

Lemma 2.3 *Let C and D be sets with $|D| \gtrapprox \frac{|C|}{K_1}$ and with $|C+D| \leq K_2|C|$. Then there is $C' \subset C$ with $|C'| \geq \frac{9}{10}|C|$ so that C' can be covered by $\sim K_1K_2$ translates of D. Similarly there is $C'' \subset C$ of the same size so that $-C''$ can be covered by $\sim K_1K_2$ 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 at least $|C|/K_1K_2$. 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 at least $|C|/K_1K_2$. First, by Cauchy-Schwarz inequality, we have that

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

which implies that

$$|(c,d,c',d')\in C\times D\times C\times D : c+d=c'+d'| \geq \frac{|C||D|^2}{K_2}.$$

The quantity on the left hand side is equal to

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

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

$$|(c+D)\cap(C+d')| \geq \frac{|D|}{K_2} \gtrsim \frac{|C|}{K_1K_2}.$$

Hence, $|(c-d'+D)\cap C| \gtrsim |C|/K_1K_2$ which is just what we wanted to prove. To prove the second half of the statement we start with the inequality

$$\sum_{d\in D}\sum_{c\in C}|(C-d)\cap(c-D)| \geq \frac{|C||D|^2}{K_2}.$$

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

$$|(c+d-D)\cap C| \gtrsim \frac{|C|}{K_1K_2}$$

and the result follows.

3 Proof of Main Theorem

Proof. We start with $|A+B|\leq K|A|$ and $|AB|\leq K|A|$. Then by using Plünnecke's inequality (see Ch 6, [14]), we have $|B+B+B+B|\leq K^4|A|$ and $|B+B+B+B+B+B|\leq K^6|A|$. First, by Cauchy-Schwarz inequality, we have that

$$\sum_{a\in A}\sum_{a'\in A}|aB\cap a'B| \geq \frac{|A||B|^2}{K}.$$

Therefore, following Garaev's arguments [5], we can find $A'\subset A$, $a_0\in A$ so that

$$|A'| \gtrapprox K^{-\beta}|B|$$

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

$$|aB\cap a_0B| \gtrapprox K^{\beta-1}\frac{|B|^2}{|A|}.$$

In the argument as in Garaev [5], the worst case is $\beta = 0$, so let us assume that for simplicity. Now there are two cases. In the first case, we have

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

If so, applying Lemma 2.1, we can find $a_1, a_2, b_1, b_2 \in A'$ so that

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

Now we apply Lemma 2.3 to find A'' whose size is at least $6/10$ of A' so that each of a_1A'', $-a_2A''$, b_1A'' and $-b_2A''$ can be covered by $\sim K^2\frac{|A|^2}{|B|^2}$ translates of $a_1B \cap a_0B$, $a_2B \cap a_0B$, $b_1B \cap a_0B$ and $b_2B \cap a_0B$ respectively. Therefore $a_1A'' - a_2A'' + b_1A'' - b_2A''$ can be covered by $\sim K^8(\frac{|A|^2}{|B|^2})^4$ translates of $a_1B \cap a_0B + a_2B \cap a_0B + b_1B \cap a_0B + b_2B \cap a_0B$. Hence we have

$$|A'|^2 \lesssim K^8(\frac{|A|^2}{|B|^2})^4|B + B + B + B| \leq K^{12}\frac{|A|^9}{|B|^8}$$

which gives that

$$K \gtrapprox \left(\frac{|B|^{10}}{|A|^9}\right)^{\frac{1}{12}}.$$

So that we have more than we need in this case. Now we are left with the case that

$$\frac{A' - A'}{A' - A'} \neq F_p.$$

Applying Lemma 2.1, we can find $a_1, a_2, a_3, a_4 \in A'$ such that

$$|A'|^2 \lesssim |(a_1 - a_2)A' + (a_1 - a_2)A' + (a_3 - a_4)A'|$$

We apply Lemma 2.2 with $X = (a_1 - a_2)A'$ and proceed as above, we get

$$|A'|^2 \lesssim K^{12}(\frac{|A|^2}{|B|^2})^6|B + B + B + B + B + B| \lesssim K^{18}\frac{|A|^{13}}{|B|^{12}}$$

which implies

$$K \gtrapprox \left(\frac{|B|^{14}}{|A|^{13}}\right)^{\frac{1}{18}}$$

and this completes the proof.

We note that from the result in [11] and Plünnecke sumset inequality (see Ch 6, [14]), we have that if $|B| \sim |A| < p^{1/2}$ then

$$\max(|A + B|, |AB|) \gtrapprox |A|^{25/24}.$$

Here we show that by using Lemma 2.3 we can get a better exponent.

Theorem 3.1 *Let $A, B \subset F_p$ with $|B| \sim |A| < p^{\frac{1}{2}}$ then*

$$\max(|A+B|, |AB|) \gtrapprox |A|^{\frac{15}{14}}.$$

Remark 3.2 *Taking $A = B$, it corresponds to the result by Garaev [5] who showed that*

$$\max(|A+A|, |AA|) \gtrapprox |A|^{\frac{15}{14}}.$$

Proof. We start with $|A+B| \leq K|A|$ and $|AB| \leq K|A|$. By using Plünnecke's inequality (see Ch 6, [14]), we have $|A+A| \leq K^2|A|$ and $|B+B+B+B| \leq K^4|A|$. First, by Cauchy-Schwarz inequality, we have that

$$\sum_{a\in A}\sum_{a'\in A} |aB \cap a'B| \geq \frac{|A|^3}{K}.$$

Therefore, following the same arguments as Garaev's [5], we can find $A' \subset A$ and $a_0 \in A$ and a number $N \gtrapprox \frac{|A|}{K}$ so that

$$|A'| \gtrapprox |A|$$

and for every $a \in A'$ we have

$$|aB \cap a_0B| \sim N.$$

Now there are two cases. In the first case, we have

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

If so, applying Lemma 2.1, we can find $a_1, a_2, b_1, b_2 \in A'$ so that

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

Now we apply Lemma 2.3 to find A'' whose size is at least $6/10$ of A' so that each of a_1A'', $-a_2A''$, b_1A'' and $-b_2A''$ can be covered by $\sim K^2$ translates of $a_1B \cap a_0B$, $a_2B \cap a_0B$, $b_1B \cap a_0B$ and $b_2B \cap a_0B$ respectively. Then $a_1A'' - a_2A'' + b_1A'' - b_2A''$ can be covered by $\sim K^8$ translates of $a_0B + a_0B + a_0B + a_0B$. Since $|4a_0B| = |B+B+B+B| \lessapprox K^4|A|$. Thus we get $K \gtrapprox |A|^{1/12} \gtrsim |A|^{1/14}$, so that we have more than we need in this case. Now we are left with the case that

$$\frac{A'-A'}{A'-A'} \neq F_p.$$

Applying Lemma 2.1, we can find $a_1, a_2, a_3, a_4 \in A'$ such that

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

Now we apply Lemma 2.2 with $X = (a_1-a_2)A'$ to get

$$|A'|^2 \lessapprox \frac{|A+A|}{|A'|}|(a_1-a_2)A' + (a_3-a_4)A'|.$$

Proceeding as above, we get

$$|A'|^2 \lessapprox K^{14}|A|$$

which implies that $K \gtrapprox |A|^{1/14}$.

References

[1] J. Bourgain, N. Katz and T. Tao, A sum product estimate in finite fields and applications, *GAFA* **14** (2004), 27-57

[2] J. Bourgain, A. Glibichuk and S. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, *J. London Math. Soc.* **63** (2006) , 380-398

[3] J. Bourgain, More on the sum-product phenomenon in prime fields and its applications, *Int. J. Number Theory* **1** (2005), 1-32

[4] J. Bourgain and M. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields, *Math. Proc. Cambridge Philos. Soc.* 2008

[5] M. Garaev, An explicit sum-product estimate in $\mathbb{F}_p$, *Int. Math. Res. Notices* **2007** (2007)

[6] M. Garaev, The sum-product estimates for large subsets of prime fields, *Proc. Amer. Math. Soc.* **137** (2008), 2735–2739

[7] M. Garaev, A quantified version of Bourgain's sum-product estimate in F_p for subsets of incomparable sizes, *The Electronic Journal of Combinatorics* **15** (2008)

[8] D. Hart, A. Iosevich and J. Solymosi, Sum product estimates in finite fields via Kloosterman sums, *Int. Math. Res. Notices* **5** (2007)

[9] N. Katz and C-Y Shen, A slight improvement to Garaev's sum product estimate, *Proc. Amer. Math. Soc.* **136** (2008) , 2499-2504

[10] N. Katz and C-Y Shen, Garaev's inequality in finite fields not of prime order , *Online J. Anal. Comb.* **2008**

[11] C-Y Shen, On the sum product estimates and two variables expanders, *submitted.*

[12] J. Solymosi, An upper bound on the multiplicative energy, *preprint.*

[13] T. Tao and V. Vu, Additive Combinatorics, *Cambridge Univ. Press* (2006)