A quantified version of Bourgain's sum-product estimate in $\mathbb{F}_p$ for subsets of incomparable sizes

M. Z. Garaev

Instituto de Matemáticas,
Universidad Nacional Autónoma de México,
Campus Morelia, Apartado Postal 61-3 (Xangari),
C.P. 58089, Morelia, Michoacán, México

garaev@matmor.unam.mx

Submitted: Mar 4, 2008; Accepted: Apr 6, 2008; Published: Apr 18, 2008
Mathematics Subject Classification: 11B75, 11T23

Abstract

Let $\mathbb{F}_p$ be the field of residue classes modulo a prime number p. In this paper we prove that if $A, B \subset \mathbb{F}_p^*$, then for any fixed $\varepsilon > 0$,

$$|A+A| + |AB| \gg \Big(\min\Big\{|B|, \frac{p}{|A|}\Big\}\Big)^{1/25-\varepsilon}|A|.$$

This quantifies Bourgain's recent sum-product estimate.

1 Introduction

Let $\mathbb{F}_p$ be the field of residue classes modulo a prime number p and let A be a non-empty subset of $\mathbb{F}_p$. It is known from [4, 5] that if $|A| < p^{1-\delta}$, where $\delta > 0$, then one has the sum-product estimate

$$|A+A| + |AA| \gg |A|^{1+\varepsilon} \tag{1}$$

for some $\varepsilon = \varepsilon(\delta) > 0$. This estimate and its proof has been quantified and simplified in [3], [6]–[11]. Improving upon our earlier estimate from [6], Katz and Shen [11] have shown that in the most nontrivial range $1 < |A| < p^{1/2}$ one has

$$|A+A| + |AA| \gg |A|^{14/13}(\log|A|)^{O(1)}.$$

A version of sum-product estimates with subsequent application to exponential sum bounds is given in [3]. In particular, from [3] it follows that if $1 < |A| < p^{12/23}$, then

$$|A-A| + |AA| \gg |A|^{13/12}(\log|A|)^{O(1)}.$$

We also mention that in the case $|A| > p^{2/3}$ one has

$$\max\{|A+A|, |AA|\} \gg p^{1/2}|A|^{1/2},$$

which is optimal in general settings bound, apart from the value of the implied constant; for the details, see [7].

Sum-product estimates in $\mathbb{F}_p$ for different subsets of incomparable sizes have been obtained by Bourgain [1]. More recently, he has shown in [2] that if $A, B \subset \mathbb{F}_p^*$, then

$$|A+A| + |AB| \gg \Big(\min\Big\{|B|, \frac{p}{|A|}\Big\}\Big)^c |A| \tag{2}$$

for some absolute positive constant c. In the present paper we prove the following explicit version of this result.

Theorem 1. *For any non-empty subsets $A, B \subset \mathbb{F}_p^*$ and any $\varepsilon > 0$ we have*

$$|A+A| + |AB| \gg \Big(\min\Big\{|B|, \frac{p}{|A|}\Big\}\Big)^{1/25-\varepsilon} |A|,$$

where the implied constant may depend only on ε.

Remark. One can expect that appropriate adaptation of techniques of [3] and [11] may lead to quantitative improvement of the exponent 1/25.

2 Lemmas

Below in statements of lemmas all the subsets are assumed to be non-empty. The first two lemmas are due to Ruzsa [12, 13]. They hold for subsets of any abelian group, but here we state them only for subsets of $\mathbb{F}_p$.

Lemma 1. *For any subsets X, Y, Z of $\mathbb{F}_p$ we have*

$$|X - Z| \le \frac{|X-Y||Y-Z|}{|Y|}.$$

Lemma 2. *For any subsets $X, B_1, \ldots, B_k$ of $\mathbb{F}_p$ we have*

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

In the proof of estimate (2) (as well as in the proofs of exponential sum bounds) Bourgain used his result

$$|8XY - 8XY| \ge 0.5\{|X||Y|, p\}$$

valid for any non-empty subsets $X, Y \subset \mathbb{F}_p^*$, see [2, Lemma 2]. In the proof of our Theorem 1 we shall use the following lemma instead.

Lemma 3. *Let $X, Y \subset \mathbb{F}_p^*$, $|Y| \geq 2$. Then there are elements $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ such that either*

$$\Big|(x_1 - x_2)Y + (y_1 - y_2)X + (y_1 - y_2)X\Big| \geq \frac{0.5|X|^2|Y|}{|XY|}$$

or

$$\Big|(x_1 - x_2)Y + (y_1 - y_2)X\Big| \geq 0.5p.$$

Thus, at the cost of a slight worsening of the right hand side, we simplify the expression on the left hand side.

Proof. If $|XY| = |X||Y|$ then we are done. Let $|XY| < |X||Y|$. Since

$$\sum_{x\in X}\sum_{y\in Y} |xY \cap yX| \geq \frac{|X|^2|Y|^2}{|XY|},$$

there are elements $x_0 \in X$, $y_0 \in Y$ such that

$$|x_0Y \cap y_0X| \geq \frac{|X||Y|}{|XY|}.$$

Let $x_0Y_1 = x_0Y \cap y_0X$. Then,

$$Y_1 \subset Y, \qquad \frac{x_0}{y_0}Y_1 \subset X, \qquad |Y_1| \geq \frac{|X||Y|}{|XY|} > 1.$$

If

$$\frac{X - X}{Y_1 - Y_1} \neq \mathbb{F}_p,$$

then

$$\frac{X - X}{Y_1 - Y_1} + \frac{x_0}{y_0} \neq \frac{X - X}{Y_1 - Y_1}.$$

Thus, for some $(x_1, x_2, y_1, y_2) \in X^2 \times Y_1^2$,

$$\frac{x_1 - x_2}{y_1 - y_2} + \frac{x_0}{y_0} \notin \frac{X - X}{Y_1 - Y_1}.$$

Hence,

$$\Big|\Big(\frac{x_1 - x_2}{y_1 - y_2} + \frac{x_0}{y_0}\Big)Y_1 + X\Big| = |X||Y_1|.$$

Since

$$\frac{x_0}{y_0}Y_1 \subset X,$$

we conclude that

$$\Big|(x_1 - x_2)Y_1 + (y_1 - y_2)X + (y_1 - y_2)X\Big| \geq |X||Y_1| \geq \frac{|X|^2|Y|}{|XY|}.$$

If

$$\frac{X-X}{Y_1-Y_1}=\mathbb{F}_p,$$

then we use the well-known fact that for some $z\in\mathbb{F}_p$ we have

$$|X+zY_1|\ge 0.5\min\{|X||Y_1|,p\}.$$

This implies that for some $(x_1,x_2,y_1,y_2)\in X^2\times Y_1^2$,

$$|(x_1-x_2)Y_1+(y_1-y_2)X|\ge 0.5\min\{|X||Y_1|,\,p\}.$$

□

The following statement follows from the aforementioned work [7]. We shall only use it in order to avoid a minor inconvenience that may arise when $p/|A|$ is as small as a fixed power of $\log|B|$.

Lemma 4. *Let $A,B,C\subset\mathbb{F}_p^*$. Then*

$$|A+C||AB|\gg\min\Big\{p|A|,\frac{|A|^2|B||C|}{p}\Big\}.$$

3 Proof of Theorem 1

If $G\subset X\times Y$ then for a given $x\in X$ we denote by $G(x)$ the set of all elements $y\in Y$ for which $(x,y)\in G$. The notation $E_+(X,Y)$ is used to denote the additive energy between X and Y, that is the number of solutions of the equation

$$x_1+y_1=x_2+y_2,\qquad (x_1,x_2,y_1,y_2)\in X^2\times Y^2.$$

We can assume that $|A|>10$, $|B|>10$. In view of Lemma 4, we can also assume that $p/|A|>(\log|B|)^{100}$.

Let

$$|A+A|+|AB|=|A|\Delta.$$

Then,

$$\sum_{b\in B}\sum_{b'\in B}|bA\cap b'A|\ge\frac{|A|^2|B|^2}{|AB|}\ge\frac{|A||B|^2}{\Delta}.$$

Hence, for some fixed $b_0\in B$,

$$\sum_{b\in B}|bA\cap b_0A|\ge\frac{|A||B|}{\Delta}. \tag{3}$$

Define

$$B_1=\Big\{b\in B:\ |bA\cap b_0A|\ge\frac{|A|}{2\Delta}\Big\}. \tag{4}$$

From Ruzsa's triangle inequalities (Lemma 1 and Lemma 2 with $k=2$),

$$|bA \pm b_0A| \le \frac{|bA + (bA \cap b_0A)| \cdot |(bA \cap b_0A) + b_0A|}{|bA \cap b_0A|} \le \frac{|A+A|^2}{|bA \cap b_0A|},$$

which, in view of (4), implies that

$$|bA \pm b_0A| \le \frac{2|A+A|^2\Delta}{|A|} \le 2|A|\Delta^3 \quad \text{for} \quad \text{any} \quad b \in B_1. \tag{5}$$

For a given $a \in A$ let $aB_1(a) = aB_1 \cap b_0A$. From (3) and (4) it follows that

$$\sum_{a\in A} |B_1(a)| = \sum_{a \in A} |aB_1 \cap b_0A| = \sum_{b \in B_1} |bA \cap b_0A| \ge \frac{|A||B|}{2\Delta}.$$

Obviously, we can assume that $|B_1| \ge 2$, since otherwise the statement is trivial from $2|B_1|\Delta \ge |B|$. We allot the values of $|B_1(a)|$ into duadic intervals and derive that for some subset $A_0 \subset A$ and for some number $N \ge 1$,

$$N|A_0| \ge \frac{|A||B|}{8\Delta \log|B|} \tag{6}$$

and

$$N \le |B_1(a)| \le 2N \quad \text{for} \quad \text{any} \quad a \in A_0. \tag{7}$$

In what follows, up to the inequality (10), is based on Bourgain's idea from [2]. We have

$$\sum_{(a,a')\in A_0^2} |B_1(a) \cap B_1(a')| \ge \frac{1}{|B_1|}\Big(\sum_{a\in A_0} |B_1(a)|\Big)^2 \ge \frac{N^2|A_0|^2}{|B_1|}.$$

We allot the values of $|B_1(a) \cap B_1(a')|$ into duadic intervals and get that for some $G \subset A_0 \times A_0$ and some number $M \ge 1$,

$$M \le |B_1(a) \cap B_1(a')| \le 2M \quad \text{for} \quad \text{any} \quad (a,a') \in G$$

and

$$M|G| \ge \frac{N^2|A_0|^2}{10|B_1| \cdot \log|B|}.$$

In particular,

$$M \ge \frac{N^2}{10|B_1| \cdot \log|B|}. \tag{8}$$

Let

$$A_1 = \Big\{ a \in A_0 : \, |G(a)| \ge \frac{N^2|A_0|}{20M|B_1| \cdot \log|B|} \Big\}.$$

From

$$\sum_{a \in A_0} |G(a)| = |G| \ge \frac{N^2|A_0|^2}{10M|B_1| \cdot \log|B|}$$

it follows

$$|A_1| \geq \frac{N^2|A_0|}{20M|B_1| \cdot \log|B|}. \tag{9}$$

For a given $a_1 \in A_1$ we shall estimate $|a_1B_1 \pm b_0G(a_1)|$ for any choice of the symbol "$\pm$". Let $\delta \in \{-1, 1\}$. To each element $x \in a_1B_1 + \delta b_0G(a_1)$ we assign one representation

$$x = a_1b + \delta b_0a_1', \qquad b \in B_1, \quad a_1' \in G(a_1)$$

and define $B_{11}(x) = B_1(a_1) \cap B_1(a_1')$. Then

$$\delta b_0^2A + xB_{11}(x) \subset \delta b_0^2A + ba_1B_1(a_1) + \delta b_0a_1'B_1(a') \subset b_0(bA + \delta b_0A + \delta b_0A),$$

whence, by Lemma 2 with $k = 3$ and estimate (5),

$$|\delta b_0^2A + xB_{11}(x)| \leq \frac{|bA + \delta b_0A| \cdot |A + A|^2}{|A|^2} \leq 2|A|\Delta^5.$$

Hence, for a given $x \in a_1B_1 + \delta b_0G(a_1)$, we have

$$E_+(b_0^2A, xB_1(a_1)) \geq E_+(b_0^2A, xB_{11}(x)) \geq \frac{|A|^2M^2}{2|A|\Delta^5} = \frac{|A|M^2}{2\Delta^5}.$$

Summing up this inequality over $x \in a_1B_1 + \delta b_0G(a_1)$ and observing that the number of solutions of the equation

$$b_0^2a' + xb' = b_0^2a'' + xb'', \quad a', a'' \in A;\ b', b'' \in B_1(a_1);\ x \in a_1B_1 + \delta b_0G(a_1)$$

is not greater than $2N|A| \cdot |a_1B_1 + \delta b_0G(a_1)| + 4N^2|A|^2$, we get

$$\frac{|A|M^2}{2\Delta^5}|a_1B_1 + \delta b_0G(a_1)| \leq 2N|A| \cdot |a_1B_1 + \delta b_0G(a_1)| + 4N^2|A|^2.$$

If $|A|M^2 \leq 10|A|N\Delta^5$, then we are done in view of (8) and (6). Therefore, we can assume that

$$|a_1B_1 \pm b_0G(a_1)| \ll \frac{|A|N^2\Delta^5}{M^2} \quad \text{for} \quad \text{any} \quad a_1 \in A_1. \tag{10}$$

By Lemma 3, for some $a_1, a_{11} \in A_1$ and $b_1, b_{11} \in B_1$, either

$$\Big|(a_1 - a_{11})B_1 + (b_1 - b_{11})A + (b_1 - b_{11})A\Big| \gg \frac{|A_1|^2|B_1|}{|A_1B_1|} \gg \frac{|A_1|^2|B_1|}{\Delta|A|}$$

or

$$\Big|(a_1 - a_{11})B_1 + (b_1 - b_{11})A\Big| \gg p.$$

In the first case, by Lemma 2 with $k = 3$ and $X = (b_1 - b_{11})A$,

$$\Big|(a_1 - a_{11})B_1 + (b_1 - b_{11})A\Big||A|\Delta^3 \gg |A_1|^2|B_1|.$$

Again by Lemma 2 with $k=4$ and $X=b_0A$, and by (5),

$$|a_1B_1+b_0A|\cdot|a_{11}B_1-b_0A|\Delta^9\gg|A_1|^2|B_1|.$$

To each of the cardinalities on the left hand side we again apply Lemma 2, with $k=2$ and $X=b_0G(a_1)$ or $X=-b_0G(a_{11})$, and recalling the lower bound for $|G(a)|$ when $a\in A_1$, we deduce

$$|a_1B_1+b_0G(a_1)|\cdot|a_{11}B_1-b_0G(a_{11})|\cdot|A|^2\Delta^{11}\gg|A_1|^2|B_1|\Big(\frac{N^2|A_0|}{M|B_1|\cdot\log|B|}\Big)^2.$$

Combining this with (10), we get

$$|A|^4\Delta^{21}\gg\frac{M^2|A_1|^2|A_0|^2}{|B_1|\cdot\log^2|B|}.$$

Using (9) to substitute $M|A_1|$, and then (6) to substitute $N|A_0|$, we obtain

$$|A|^4\Delta^{21}\gg\frac{|A|^4|B|^4}{\Delta^4|B_1|^3\log^8|B|}\gg\frac{|A|^4|B|}{\Delta^4\log^8|B|}.$$

This proves our assertion in the first case.

In the second case we have

$$\Big|(a_1-a_{11})B_1+(b_1-b_{11})A\Big|\gg p,$$

which implies

$$|a_1B_1+b_0A|\cdot|a_{11}B_1-b_0A|\Delta^6\gg p|A|.$$

Then as in the first case,

$$|A|^2\Delta^{18}\gg\frac{p|A_0|^2M^2}{|A||B_1|^2\log^2|B|}.$$

Using (8) and then (6), we get

$$\Delta^{22}\gg\frac{p}{|A|\log^8|B|}$$

and the result follows in view of the assumption $p/|A|>(\log|B|)^{100}$.

Acknowledgements. The author is thankful to A. A. Glibichuk, S. V. Konyagin and the referee for useful remarks. The author was partially supported by Project PAPIIT IN 100307 from UNAM.

References

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

[2] J. Bourgain, *Multilinear exponential sum bounds with optimal entropy assignments,* Geom. Funct. Anal. (to appear).

[3] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields,* Math. Proc. Cambridge Philos. Soc. (to appear).

[4] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order,* J. London Math. Soc. (2) **73** (2006), 380–398.

[5] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields and their applications,* Geom. Func. Anal. **14** (2004), 27–57.

[6] M. Z. Garaev, *An explicit sum-product estimate in F_p,* Int. Math. Res. Notices 2007, no. 11, Art. ID rnm035, 11 pp.

[7] M. Z. Garaev, *The sum-product estimate for large subsets of prime fields,* Proc. Amer. Math. Soc. (to appear).

[8] A. A. Glibichuk and S. V. Konyagin, *Additive properties of product sets in fields of prime order,* Centre de Recherches Mathématiques, CRM Proceedings and Lecture Notes, 43, 279–286 (2007).

[9] D. Hart, A. Iosevich and J. Solymosi, *Sum product estimates in finite fields via Kloosterman sums,* Int. Math. Res. Notices 2007, no. 5, Art. ID rnm007, 14pp.

[10] N. H. Katz and Ch.-Y. Shen, *Garaev's inequality in finite fields not of prime order,* Online Journal of Analytic Combinatorics, Issue 3 (2008), #3.

[11] N. H. Katz and Ch.-Y. Shen, *A slight improvement to Garaev's sum product estimate,* Proc. Amer. Math. Soc. (to appear).

[12] I. Z. Ruzsa, *An application of graph theory to additive number theory,* Scientia, Ser. A **3** (1989), 97–109.

[13] I. Z. Ruzsa, *Sums of finite sets,* Number theory (New York, 1991–1995), 281–293, Springer, New York, 1996.

[14] T. Tao and V. Vu, 'Additive combinatorics', Cambridge Univ. Press, Cambridge, 2006.