Publ. Mat. **54** (2010), 149–157

ON THE SUM PRODUCT ESTIMATES AND TWO VARIABLES EXPANDERS

Chun-Yen Shen

Abstract

Let $\mathbb{F}_p$ be the finite field of a prime order p. Let $F\colon \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ be a function defined by $F(x,y) = x(f(x)+by)$, where $b \in \mathbb{F}_p^*$ and $f\colon \mathbb{F}_p \to \mathbb{F}_p$ is any function. We prove that if $A \subset \mathbb{F}_p$ and $|A| < p^{1/2}$ then

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

Taking $f = 0$ and $b = 1$, we get the well-known sum-product theorem by Bourgain, Katz and Tao, and Bourgain, Glibichuk and Konyagin, and also improve the previous known exponent from $\frac{14}{13}$ to $\frac{13}{12}$.

1. Introduction

The sum product phenomenon has received a great deal of attention, since Erdös and Szemerédi made their well known conjecture that for any $\epsilon > 0$ one has

$$\max(|A+A|, |AA|) \geq C_\epsilon |A|^{2-\epsilon},$$

where A is a finite subset of integers,

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

and

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

Later, much work has been done to find the explicit exponents, and the best result to date is due to Solymosi [**11**], who showed that

$$\max(|A+A|, |AA|) \gtrapprox |A|^{\frac{4}{3}}.$$

In the finite field setting, the problem becomes more complicated and the first non-trivial sum-product estimate was obtained by Bourgain, Katz and Tao [**4**] with subsequent refinement by Bourgain, Glibichuk and

2000 *Mathematics Subject Classification.* 11B75.
Key words. Sums, products, expanders.

Konyagin [**3**]. They proved that if $A \subset \mathbb{F}_p$, p prime, and $|A| \le p^{1-\delta}$ for some $\delta > 0$, then there exists $\epsilon = \epsilon(\delta) > 0$ such that $\max(|A+A|, |AA|) \gtrsim |A|^{1+\epsilon}$. Since then there have been several generalizations and applications of this theorem (see [**1**], [**2**], [**5**]–[**10**], [**12**]). For example, it was shown by Bourgain [**1**] that if $A, B \subset \mathbb{F}_p$ and $p^\delta < |B| \le |A| < p^{1-\delta}$ for some $\delta > 0$, then the following bound holds:

$$\max(|A+B|, |AB|) \gtrsim p^\epsilon |A|,$$

for some $\epsilon > 0$. In addition, he also showed that the function $F(x,y) = x^2 + xy$ from $\mathbb{F}_p \times \mathbb{F}_p$ to $\mathbb{F}_p$ possesses an expanding property in the sense that $|F(A,B)| \gtrsim p^\epsilon$ for some $\epsilon > \delta$ whenever $|A| \sim |B| \sim p^\delta$, $0<\delta<1$. Another generalization was made by Vu [**13**] who characterized the polynomials which satisfy

$$\max(|A+A|, |P(A,A)|) \gtrsim |A| \min\left(\left(\frac{|A|^2}{k^4 p}\right)^{1/4}, \left(\frac{p}{k|A|}\right)^{1/3}\right),$$

where k is the degree of the polynomial (see, also [**6**] for some improvements in the case $P(x,y) = xy$ which corresponds to the sum-product problem). However, this result is nontrivial only when $|A| > p^{\frac{1}{2}}$. In this paper we construct a family of two variables functions of the form

$$F(x,y) = x(f(x) + y)$$

which satisfy $|F(A,A)| \gtrsim |A|^{1+\epsilon}$, and also prove a stronger sum product estimate in the most nontrivial range $|A| < p^{\frac{1}{2}}$: namely, if $A \subset \mathbb{F}_p$ with $|A| < p^{\frac{1}{2}}$ then

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

where $F\colon \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ be a function defined by $F(x,y) = x(f(x) + by)$, where $b \in \mathbb{F}_p^*$ and $f\colon \mathbb{F}_p \to \mathbb{F}_p$ is any function.

Remark 1.1. Taking $f = 0$ and $b = 1$, we get the above mentioned sum product theorem from [**3**] and [**4**] and also improve the exponent in [**9**] from $\frac{14}{13}$ to $\frac{13}{12}$. In addition, the exponent $\frac{13}{12}$ appears in the work of Bourgain and Garaev [**2**] in the form $|A-A| + |AA| \gtrapprox |A|^{13/12}$. Nevertheless, our method is different from the one of [**2**] and applies equally well to the more general case.

2. Preliminaries

Throughout this paper A will denote a nonempty subset in the prime field $\mathbb{F}_p$. If B is a set then 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. Lemma 2.1 was proven in [**8**], [**9**], Lemma 2.2 was proven in [**9**].

Lemma 2.1. *Let $A_1 \subset \mathbb{F}_p$ 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 $|A'| \gtrsim |A_1|$

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

In particular such a_1, a_2, b_1, b_2 exist unless $\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p$. In case $\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p$, 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 2.2. *Let $X, B_1, \ldots, B_k$ be any subsets of $\mathbb{F}_p$. Then there is $X' \subset X$ with $|X'| > \frac{1}{2}|X|$ so that*

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

Lemma 2.3. *Let C and D be sets with $|D| \gtrsim \frac{|C|}{K}$ and with $|C + D| \leq K|C|$. Then there is a $C' \subset C$ with $|C'| \geq \frac{9}{10}|C|$ so that C' can be covered by $\sim K^2$ translates of D. Similarly, there is a $C'' \subset C$ 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 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 at least $|C|/K^2$. First, by the Cauchy-Schwartz 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

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

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

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

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

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

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. □

3. Explicit two variables expanding maps

Theorem 3.1. *Let $A \subset \mathbb{F}_p$ with $|A| < p^{1-\delta}$ for some $\delta > 0$. Then for any nonconstant polynomial f, we have*

$$|\{x(f(x)+y) : x, y \in A\}| \gtrsim |A|^{1+\epsilon}$$

for some $\epsilon > 0$ that depends only on δ and on the degree of the polynomial f.

The key ingredient is the Szemerédi-Trotter incidence theorem in the affine plane $\mathbb{F}_p^2$ which was proven in [**3**], [**4**].

Theorem 3.2. *Let P and L be the points and lines in $\mathbb{F}_p^2$ and $|P|, |L| \leq N < p^\alpha$ for some $0 < \alpha < 2$. Then*

$$|\{(p,\ell) \in P \times L : p \in \ell\}| \lesssim N^{\frac{3}{2}-\gamma}$$

for some $\gamma > 0$.

Proof: We proceed by contradiction. Suppose it is not true. Then we have

$$|\{x(f(x)+y) : x, y \in A\}| \lesssim |A|^{1+\epsilon}$$

for some small ϵ. Let k be the degree of f and denote $C = \{x(f(x)+y) : x, y \in A\}$. By the Cauchy-Schwartz inequality, we have

$$\sum_{x \in A} \sum_{x' \in A} |x(f(x)+A) \cap x'(f(x')+A)| \gtrsim |A|^{3-\epsilon}.$$

Therefore, we can find $a_0 \in A$ and $A_1 \subset A$ such that

$$|A_1| \gtrapprox |A|^{1-\epsilon}$$

and

$$|(x'(f(x')+A) \cap (a_0(f(a_0)+A)| \gtrsim |A|^{1-\epsilon}, \quad \forall\, x' \in A_1.$$

Thus, for any $x_1 \in A_1$, there is a subset $A_{x_1} \subset A$ with $|A_{x_1}| > |A|^{1-\epsilon}$ and

$$x_1(f(x_1)+A_{x_1}) \subset a_0(f(a_0)+A).$$

Hence, for any $x \in A$ we have

$$x\left(f(x) + \frac{x_1(f(x_1)+A_{x_1})}{a_0} - f(a_0)\right) \subset C.$$

Now, given $x \in A$, $x' \in A_1$, let $\ell_{x,x'}$ be the line

$$\mu = \frac{xx'}{a_0}\nu + \frac{xx'f(x')}{a_0} + xf(x) - xf(a_0)$$

and $L = \{\ell_{x,x'} : x \in A, x' \in A_1\}$. Then it is easy to verify that $|A|^{2-\epsilon}\frac{1}{k} \lesssim |L| \le |A||A_1| < |A|^2$. If we let $P = A \times C$ then $|P| = |A| \times |C| \lesssim |A|^{2+\epsilon}$. Therefore we have $|\ell_{x,x'} \cap P| > |A|^{1-\epsilon}$, and the total number of incidences between L and P is at least $|L||A|^{1-\epsilon} \gtrsim \frac{1}{k}|A|^{3-\epsilon}$. By applying Theorem 3.2, it follows that if ϵ is too small, it leads a contradiction and this completes the proof. □

Remark 3.3. In Theorem 3.1 we assume that f is a nonconstant polynomial. If f is a constant, then we mention the recent preprint [**7**], where explicit bounds have been obtained for this case.

4. Stronger sum product estimates

Theorem 4.1. *Let $A \subset \mathbb{F}_p$ with $|A| < p^{\frac{1}{2}}$. Then*

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

where $F(x,y) = x(f(x)+by)$, f is any function from $\mathbb{F}_p$ to $\mathbb{F}_p$, and $b \in \mathbb{F}_p^*$.

Proof: We start with $|A+A| \le K|A|$ and $|F(A,A)| \le K|A|$. By using Plünnecke's inequality, we can find $A' \subset A$ with $|A'| \gtrsim |A|$ so that

$$|A'+A'+A'| \lesssim K^2|A|$$

and

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

First, by the Cauchy-Schwartz inequality, we have that

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

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

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

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

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

As in the argument of Garaev, the worst case is $\beta = 0$, so let's assume that for simplicity. There are two cases. In the first case, we have

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

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

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

$$=|a_1f(a_1)+a_1bA''-a_2f(a_2)-a_2bA''+b_1f(b_1)+b_1bA''-b_2f(b_2)-b_2bA''|$$

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

Now we apply Lemma 2.3 to find a A''' whose size is at least $6/10$ of A'' so that each of $a_1(f(a_1)+bA''')$, $-a_2(f(a_2)+bA''')$, $b_1(f(b_1)+bA''')$, and $-b_2(f(b_2)+bA''')$ can be covered by $\sim K^2$ translates of $a_0(f(a_0)+bA')$. However, then $a_1(f(a_1)+bA''')-a_2(f(a_2)+bA''')+b_1(f(b_1)+bA''')-b_2(f(b_2)+bA''')$ can be covered by $\sim K^8$ translates of $a_0(f(a_0)+bA')+a_0(f(a_0)+bA')+a_0(f(a_0)+bA')+a_0(f(a_0)+bA')$. Since $|a_0(f(a_0)+bA')+a_0(f(a_0)+bA')+a_0(f(a_0)+bA')+a_0(f(a_0)+bA')| = |A'+A'+A'+A'| \lesssim K^3|A|$, by the definition of A'. Thus we get

$$|a_1A'''-a_2A'''+b_1A'''-b_2A'''| \lesssim K^{11}|A|.$$

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

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

Applying Lemma 2.1, 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 2.2, 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, we get

$$|A'|^2 \lesssim K^{12}|A|,$$

which implies that $K \gtrapprox |A|^{1/12}$. □

Theorem 4.2. *Let $A, B \subset \mathbb{F}_p$ with $|B| \sim |A| < p^{\frac{1}{2}}$ then*

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

where $F(x, y) \to x(f(x)+by)$, f is any function from $\mathbb{F}_p$ to $\mathbb{F}_p$ and $b \in \mathbb{F}_p^*$.

Remark 4.3. Taking $f = 0$, $b = 1$ and $A = B$, it corresponds to the result by Garaev [**5**] who showed that

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

Proof: The proof is completely the same as the proof in Theorem 4.1. We start with $|A+B| \leq K|A|$ and $|F(A, B)| \leq K|A|$. By using Plünnecke's inequality, we have $|A + A| \leq K^2|A|$ and $|B + B + B + B| \leq K^4|A|$. Therefore, following the same arguments in the proof of Theorem 4.1, we can find $A' \subset A$ with $|A'| \gtrapprox |A|$ such that either we have

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

or

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

for some elements $a_1, a_2, b_1, b_2 \in A'$. The worst case is the second one, let us just deal with this case for simplicity. Therefore, by the same argument in the proof of Theorem 4.1, we get

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

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

Acknowledgements. The author wishes to thank Nets Katz for helpful discussions and the referee for her/his valued comments in developing the final version of this article.

References

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

[2] 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.* **146(1)** (2009), 1–21.

[3] 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(2)** (2006), 380–398.

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

[5] M. Z. Garaev, An explicit sum-product estimate in $\mathbb{F}_p$, *Int. Math. Res. Not. IMRN* **11** (2007), Art. ID rnm035, 11 pp.

[6] M. Z. Garaev, The sum-product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* **136(8)** (2008), 2735–2739.

[7] M. Z. Garaev and C.-Y. Shen, On the size of the set $A(A+1)$, *Math. Z.* (2009), in press.

[8] A. A. Glibichuk and S. V. Konyagin, Additive properties of product sets in fields of prime order, in: *"Additive combinatorics"*, CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007, pp. 279–286.

[9] N. H. Katz and C.-Y. Shen, A slight improvement to Garaev's sum product estimate, *Proc. Amer. Math. Soc.* **136(7)** (2008), 2499–2504.

[10] N. H. Katz and C.-Y. Shen, Garaev's inequality in finite fields not of prime order, *Online J. Anal. Comb.* **3** (2008), 6 pp.

[11] J. Solymosi, An upper bound on the multiplicative energy, Preprint.

[12] T. Tao and V. Vu, *"Additive combinatorics"*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, Cambridge, 2006.

[13] V. H. Vu, Sum-product estimates via directed expanders, *Math. Res. Lett.* **15(2)** (2008), 375–388.

Department of Mathematics
Indiana University
Bloomington, IN 47405
USA
E-mail address: shenc@indiana.edu

Primera versió rebuda el 25 de setembre de 2008,
darrera versió rebuda el 20 de febrer de 2009.