ACTA ARITHMETICA
147.2 (2011)

Slightly improved sum-product estimates in fields of prime order

by

Liangpan Li (Shanghai and San Marcos, TX)

1. Introduction. Let $\mathbb{F}_p$ be the field of residue classes modulo a prime number p and A, B be two nonempty subsets of $\mathbb{F}_p$. For any binary operation $\odot$ on $\mathbb{F}_p$, define $A \odot B = \{a \odot b : a \in A, b \in B\}$. From the work of Bourgain, Katz, and Tao [5] and Bourgain, Glibichuk, and Konyagin [4], we know that if $|A| \le p^{\delta}$ for some $\delta < 1$, then one has the so-called sum-product estimate

$$\max\{|A+A|, |AA|\} \gtrsim |A|^{1+\epsilon}$$

for some $\epsilon = \epsilon(\delta) > 0$. This result has found many applications in various areas of mathematics (see e.g. [1, 2, 4, 5, 14]) and it is natural to ask for quantitative relationships between δ and ϵ in certain ranges of $|A|$.

In [12] Hart, Iosevich and Solymosi (HIS) developed incidence theory between points and hyperbolas in $\mathbb{F}_p^2$ via Kloosterman sum estimates, and obtained

$$\max\{|A+A|, |AA|\} \gtrsim \min\{|A|^{2/3}p^{1/3}, |A|^{3/2}p^{-1/4}\}.$$

This led to the first concrete value of ϵ for $|A| > p^{1/2}$. In [19] Vu generalized the HIS estimate via spectral graph theory by classifying all polynomials $P(x_1, x_2)$ such that

$$\max\{|A+A|, |P(A,A)|\} \gtrsim \min\{|A|^{2/3}p^{1/3}, |A|^{3/2}p^{-1/4}\}.$$

Recently Vu's result was reproved by Hart, Shen and the author [13] via Fourier analytical methods.

In [9] Garaev improved the HIS estimate to

$$\max\{|A+A|, |AA|\} \gtrsim \min\{|A|^{1/2}p^{1/2}, |A|^2p^{-1/2}\}.$$

This is an optimal estimate up to the implied constant in the range $|A| > p^{2/3}$. In [18] Solymosi applied spectral graph theory to show among many

2010 *Mathematics Subject Classification*: Primary 11B75.
Key words and phrases: finite field, sum-product estimates.

DOI: 10.4064/aa147-2-4

others a similar bound

$$|A+f(A)| \gtrsim \min\{|A|^{1/2}p^{1/2}, |A|^2p^{-1/2}\}$$

for a class of functions f of which polynomials with integer coefficients and degrees greater than one are members. The Garaev–Solymosi type estimate was further studied in [13] via Fourier analytical methods. In particular, it was shown that for $\oplus, \otimes \in \{+, \times\}$ one has

$$\max\{|g(A)\oplus B|, |h(A)\otimes C|\} \gtrsim \min\{|A|^{1/2}p^{1/2}, |A|\,|B|^{1/2}|C|^{1/2}p^{-1/2}\}$$

for two classes of polynomials g and h depending on the choices of $\oplus$ and $\otimes$. This result is analogous to the work done by Elekes, Nathanson and Ruzsa [7] in the real numbers.

For the case $|A| \le p^{1/2}$, Garaev [8] used combinatorial methods to obtain

$$\max\{|A+A|, |AA|\} \gtrsim \frac{|A|^{15/14}}{(\log_2|A|)^{2/7}}.$$

This kind of estimate was refined several times (see e.g. [3, 15, 16, 17]), and currently the best results are due to Bourgain and Garaev [3] giving

$$\max\{|A-A|, |AA|\} \gtrsim \frac{|A|^{13/12}}{(\log_2|A|)^{4/11}}, \tag{1.1}$$

and Shen [16, 17] giving

$$\max\{|A\pm A|, |AA|\} \gtrsim \frac{|A|^{13/12}}{(\log_2|A|)^{C}} \tag{1.2}$$

for some $C > 0$. With a technique of Chang [6], we can completely drop the logarithmic terms in both (1.1) and (1.2). The main results of this paper are as follows.

Theorem 1.1. *Suppose $A \subset \mathbb{F}_p$ with $|A| \le p^{1/2}$. Then*

$$\max\{|A\pm A|, |AA|\} \gtrsim |A|^{13/12}.$$

Theorem 1.2. *Suppose $A \subset \mathbb{F}_p$ with $|A| \ge p^{1/2}$. Then*

$$\max\{|A\pm A|, |AA|\} \gtrapprox \min\{|A|^{13/12}(|A|/p^{0.5})^{1/12},\ |A|(p/|A|)^{1/11}\}.$$

From Theorems 1.1 and 1.2 we know that if $|A| \le p^{0.52}$, then

$$\max\{|A\pm A|, |AA|\} \gtrsim |A|^{13/12}.$$

Assuming this fact, it was shown in [13] that for $|A| \le p^{1/2}$ one has

$$|A+A^2| \gtrsim |A|^{147/146}, \quad \text{where} \quad A^2 \triangleq \{a^2 : a \in A\}.$$

2. Preliminaries. Throughout this paper A will denote a fixed non-empty subset of $\mathbb{F}_p$. Whenever E and F are quantities we use $E \lesssim F$ or $F \gtrsim E$ to mean $E \le CF$, and $E \lessapprox F$ or $F \gtrapprox E$ to mean $E \le \widetilde{C}(\log|A|)^{\alpha}F$, where the constants $C, \widetilde{C}$ and α are universal (i.e. independent of A and p) and may vary from line to line. Moreover, $E \sim F$ means both $E \lesssim F$ and $F \lesssim E$. Given $\odot \in \{+, \times\}$, for $Y, Z \subset \mathbb{F}_p$ we denote by $E^{\odot}(Y,Z)$ the $\odot$-energy between Y and Z, that is,

$$E^{\odot}(Y,Z) = \sum_{x \in Y} \sum_{y \in Y} |(x \odot Z) \cap (y \odot Z)|.$$

The Cauchy–Schwarz inequality implies that $E^{\odot}(Y,Z) \geq |Y|^2|Z|^2/|Y \odot Z|$.

In the following we will state some preliminary lemmas. Lemma 2.1 may be found in [16, 17], while Lemma 2.2 in [11, 15]. Lemma 2.3, following from the work of Glibichuk and Konyagin [10] on additive properties of product sets, was proved in [3, 8].

LEMMA 2.1. *Suppose $B_1, B_2 \subset \mathbb{F}_p$. Then there exist $\lesssim \min\{|B_1+B_2|/|B_2|, |B_1 - B_2|/|B_2|\}$ translates of B_2 such that the union of these copies covers (in cardinality) 99% of B_1.*

LEMMA 2.2. *Suppose $B_0, B_1, \ldots, B_k \subset \mathbb{F}_p$. Given any $\epsilon \in (0,1)$, there exist a universal constant $C_{k,\epsilon}$ and an $X \subset B_0$ with $|X| \geq (1-\epsilon)|B_0|$ such that*

$$|X + B_1 + \cdots + B_k| \leq C_{k,\epsilon} \cdot \left(\prod_{i=1}^{k} \frac{|B_0 + B_i|}{|B_0|} \right) \cdot |X|.$$

LEMMA 2.3. *Suppose $A_1 \subset \mathbb{F}_p$ with $\frac{A_1 - A_1}{A_1 - A_1} \subsetneq \mathbb{F}_p$. Then $|A_1| \leq 2p^{1/2}$ and for given $\oplus \in \{+, -\}$, there exist $a, b, c, d \in A_1$ such that for any $A' \subset A_1$ with $|A'| \geq 0.5|A_1|$,*

$$|(b-a)A' \oplus (b-a)A' + (d-c)A'| \gtrsim |A_1|^2.$$

LEMMA 2.4. *Suppose $A_1 \subset \mathbb{F}_p$ with $\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p$. Then there exist $a, b, c, d \in A_1$ such that for any $A' \subset A_1$ with $|A'| \geq 0.5|A_1|$,*

$$|(b-a)A' + (d-c)A'| \gtrsim \min\{|A_1|^2,\ p\}.$$

Proof. There exists a $\xi \in \mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$ (cf. formula (11) in [4] with $G = \mathbb{F}_p^*$) such that

$$E^+(A_1, \xi A_1) \leq |A_1|^2 + \frac{|A_1|^4}{p-1}.$$

Since $\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p$, we can write $\xi = \frac{d-c}{b-a}$ for some $a, b, c, d \in A_1$. Thus

$$|A' + \xi A'| \geq \frac{|A'|^4}{E^+(A', \xi A')} \geq \frac{|A'|^4}{E^+(A_1, \xi A_1)} \gtrsim \frac{|A_1|^4}{E^+(A_1, \xi A_1)} \gtrsim \min\{|A_1|^2, p\}.$$

This proves the lemma. ∎

3. Proofs of the main results

Proof of Theorem 1.1. Choose arbitrarily $\oplus \in \{+,-\}$. Applying Lemma 2.2 with $B_0 = \cdots = B_3 = A$ and $\epsilon = 0.5$, one can find a subset $Z \subset A$ with $|Z| \geq 0.5|A|$ such that

$$|Z \oplus A \oplus A \oplus A| \lesssim \left(\frac{|A \oplus A|}{|A|}\right)^3 |Z| \sim \frac{|A \oplus A|^3}{|A|^2}. \tag{3.1}$$

By the pigeonhole principle there exists an element $z_0 \in Z$ so that

$$\frac{E^\times(Z,Z)}{|Z|} \leq \sum_{z \in Z} |z_0 Z \cap zZ|. \tag{3.2}$$

For each $j \leq \lceil \log_2 |Z| \rceil$, let Z_j be the set of all $z \in Z$ for which $|z_0 Z \cap zZ| \in N_j$, where $N_1 = \{1,2\}, N_2 = \{3,4\}, N_3 = \{5,6,7,8\}, N_4 = \{9,10,11,12,13,14,15,16\},\ldots$. Define $j_s = \max\{j : |Z_j| \in N_s\}$ for each $s \leq \lceil \log_2 |Z| \rceil$ (assume $\max \emptyset = 0$). Clearly,

$$\sum_{z \in Z} |z_0 Z \cap zZ| \sim \sum_{j=1}^{\lceil \log_2 |Z| \rceil} 2^j |Z_j| \sim \sum_{s:\, j_s \geq 1} 2^{j_s} 2^s. \tag{3.3}$$

Note also that

$$\begin{aligned} \sum_{s:\, j_s \geq 1} 2^{j_s} 2^s &\leq (\max_{s:\, j_s \geq 1} 2^{j_s} 2^{0.75s}) \sum_{s=1}^{\lceil \log_2 |Z| \rceil} 2^{0.25s} \\ &\lesssim (\max_j 2^j |Z_j|^{0.75}) \cdot |Z|^{0.25}. \end{aligned} \tag{3.4}$$

Combining (3.2)–(3.4) with $E^\times(Z,Z) \geq |Z|^4/|ZZ| \gtrsim |A|^4/|AA|$ we get

$$\frac{|A|^{11}}{|AA|^4} \lesssim \max_j 16^j |Z_j|^3. \tag{3.5}$$

Next choose a $j_0 \leq \lceil \log_2 |Z| \rceil$ so that

$$16^{j_0} |Z_{j_0}|^3 = \max_j 16^j |Z_j|^3. \tag{3.6}$$

According to the assumption $|A| \leq p^{1/2}$, we have $|Z_{j_0}| \leq p^{1/2}$. Hence applying either Lemma 2.3 or Lemma 2.4 one can find $a,b,c,d \in Z_{j_0}$ such that for any $E \subset Z_{j_0}$ with $|E| \geq 0.5|Z_{j_0}|$,

$$|Z_{j_0}|^2 \lesssim |(b-a)E \oplus (b-a)E + (d-c)E|. \tag{3.7}$$

By Lemma 2.1, there exist

$$\lesssim \frac{|-aZ_{j_0} \oplus (-aZ \cap z_0 Z)|}{|aZ \cap z_0 Z|} \lesssim \frac{|A \oplus A|}{2^{j_0}}$$

translates of $aZ \cap z_0 Z$ such that the union of these copies covers 99% of $-aZ_{j_0}$, say covers $-aF_1$ where $F_1 \subset Z_{j_0}$ with $|F_1| \ge 0.99|Z_{j_0}|$; there exist

$$\lesssim \frac{|bZ_{j_0} \oplus (bZ \cap z_0 Z)|}{|\oplus(bZ \cap z_0 Z)|} \lesssim \frac{|A \oplus A|}{2^{j_0}}$$

translates of $\oplus(bZ \cap z_0 Z)$ such that the union of these copies can cover 99% of bZ_{j_0}, say covers bF_2 where $F_2 \subset Z_{j_0}$ with $|F_2| \ge 0.99|Z_{j_0}|$; there exist

$$\lesssim \frac{|-cZ_{j_0} \oplus (-cZ \cap z_0 Z)|}{|\oplus(cZ \cap z_0 Z)|} \lesssim \frac{|A \oplus A|}{2^{j_0}}$$

translates of $\oplus(cZ \cap z_0 Z)$ such that the union of these copies covers 99% of $-cZ_{j_0}$, say covers $-cF_3$ where $F_3 \subset Z_{j_0}$ with $|F_3| \ge 0.99|Z_{j_0}|$; there exist

$$\lesssim \frac{|dZ_{j_0} \oplus (dZ \cap z_0 Z)|}{|\oplus(dZ \cap z_0 Z)|} \lesssim \frac{|A \oplus A|}{2^{j_0}}$$

translates of $\oplus(dZ \cap z_0 Z)$ such that the union of these copies covers 99% of dZ_{j_0}, say covers dF_4 where $F_4 \subset Z_{j_0}$ with $|F_4| \ge 0.99|Z_{j_0}|$. Letting $F = F_1 \cap F_2 \cap F_3 \cap F_4$, we have $|F| \ge 0.8|Z_{j_0}|$ and

$$(3.8) \quad |-aF + bF - cF + dF| \lesssim \left(\frac{|A \oplus A|}{2^{j_0}}\right)^4 \cdot |z_0 Z \oplus z_0 Z \oplus z_0 Z \oplus z_0 Z|.$$

By Lemma 2.2, there exists a subset $\widetilde{E} \subset F$ with $|\widetilde{E}| \ge 0.8|F| \ge 0.5|Z_{j_0}|$ such that

$$(3.9) \quad |(b-a)\widetilde{E} \oplus (b-a)F + (d-c)F| \lesssim \frac{|F \oplus F|}{|F|} \cdot |(b-a)F + (d-c)F|.$$

Combining (3.1), (3.7), (3.8), (3.9) with $|F \oplus F|/|F| \lesssim |A \oplus A|/|Z_{j_0}|$ we get

$$(3.10) \qquad 16^{j_0}|Z_{j_0}|^3 \lesssim \frac{|A \oplus A|^8}{|A|^2}.$$

Combining (3.5), (3.6) and (3.10) gives

$$|A \oplus A|^8 |AA|^4 \gtrsim |A|^{13}.$$

This concludes the proof of Theorem 1.1. ∎

Proof of Theorem 1.2. Choose arbitrarily $\oplus \in \{+,-\}$. Suppose $A \subset \mathbb{F}_p$ with $|A| \ge p^{1/2}$. Similar to the proof of Theorem 1.1, there exist a subset $Z \subset A$ with $|Z| \ge 0.5|A|$ such that

$$|Z \oplus Z \oplus Z \oplus Z| \lesssim \frac{|A \oplus A|^3}{|A|^2},$$

and a fixed element $z_0 \in Z$ so that

$$\sum_{z\in Z} |z_0 Z \cap zZ| \geq \frac{|Z|^3}{|ZZ|} \gtrsim \frac{|A|^3}{|AA|}.$$

For each $j \leq \lceil \log_2 |Z| \rceil$, let Z_j be the set of all $z \in Z$ for which $|z_0 Z \cap zZ| \in N_j$. Choose some $j_0 \leq \lceil \log_2 |Z| \rceil$ so that

$$2^{j_0}|Z_{j_0}| \gtrapprox \frac{|A|^3}{|AA|}.$$

There are two cases to consider.

(i) Suppose $|Z_{j_0}| \leq 2p^{0.5}$. Similar to the proof of Theorem 1.1 one can establish

$$16^{j_0}|Z_{j_0}|^3 \lesssim \frac{|A \oplus A|^8}{|A|^2}.$$

Consequently,

$$\frac{|A|^{12}}{|AA|^4} \lessapprox 16^{j_0}|Z_{j_0}|^4 \lesssim \frac{|A \oplus A|^8}{|A|^2} \cdot p^{0.5},$$

which yields

$$|A \oplus A|^8 |AA|^4 \gtrapprox \frac{|A|^{14}}{p^{0.5}}. \tag{3.11}$$

(ii) Suppose $|Z_{j_0}| > 2p^{0.5}$. By Lemma 2.3 we have $\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p$. By Lemma 2.4 one can find $a, b, c, d \in Z_{j_0}$ such that for any $E \subset Z_{j_0}$ with $|E| \geq 0.5|Z_{j_0}|$,

$$p \lesssim |(b-a)E + (d-c)E|.$$

Similar to the proof of Theorem 1.1 one can find a subset $\widetilde{E} \subset Z_{j_0}$ with $|\widetilde{E}| \geq 0.5|Z_{j_0}|$ such that

$$|(b-a)\widetilde{E} + (d-c)\widetilde{E}| \lesssim \left(\frac{|A \oplus A|}{2^{j_0}}\right)^4 \cdot \frac{|A \oplus A|^3}{|A|^2}.$$

Consequently,

$$p \lesssim \left(\frac{|A \oplus A|}{2^{j_0}}\right)^4 \cdot \frac{|A \oplus A|^3}{|A|^2}.$$

Thus

$$\frac{|A|^8}{|AA|^4} \leq \frac{|A|^{12}}{|AA|^4 |Z_{j_0}|^4} \lessapprox 16^{j_0} \lesssim \frac{|A \oplus A|^7}{p|A|^2},$$

which yields

$$|A \oplus A|^7 |AA|^4 \gtrapprox |A|^{10} p. \tag{3.12}$$

Thus Theorem 1.2 follows from (3.11) and (3.12). ∎

Acknowledgments. The author would like to thank Chun-Yen Shen, Jian Shen and Yaokun Wu for helpful discussions. He also thanks the anonymous referee for carefully reading the manuscript. This work was supported by the Mathematical Tianyuan Foundation of China (No. 10826088) and Texas Higher Education Coordinating Board (ARP 003615-0039-2007).

References

[1] J. Bourgain, *The sum-product phenomenon and some of its applications*, in: Analytic Number Theory, Cambridge Univ. Press, Cambridge, 2009, 62–74.

[2] J. Bourgain, A. Gamburd and P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. 179 (2010), 559–644.

[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. 146 (2009), 1–21.

[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. 73 (2006), 380–398.

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

[6] M.-C. Chang, *On product sets in fields of prime order and an application of Burgess' inequality*, preprint, 2007.

[7] Gy. Elekes, M. B. Nathanson and I. Z. Ruzsa, *Convexity and sumsets*, J. Number Theory 83 (2000), 194–201.

[8] M. Z. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$, Int. Math. Res. Notices 2007, no. 11, art. ID rnm035, 11 pp.

[9] —, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc. 136 (2008), 2735–2739.

[10] 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., 2007, 279–286.

[11] K. Gyarmati, M. Matolcsi and I. Z. Ruzsa, *Plünnecke's inequality for different summands*, in: Building Bridges, Bolyai Soc. Math. Stud. 19, Springer, Berlin, 2008, 309–320.

[12] 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.

[13] D. Hart, L. P. Li and C.-Y. Shen, *Fourier analysis and expanding phenomena in finite fields*, preprint, 2009.

[14] H. A. Helfgott, *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) 167 (2008), 601–623.

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

[16] C.-Y. Shen, *An extension of Bourgain and Garaev's sum-product estimates*, Acta Arith. 135 (2008), 351–356.

[17] —, *On the sum product estimates and two variables expanders*, Publ. Mat. 54 (2010), 149–157.

[18] J. Solymosi, *Incidences and the spectra of graphs*, in: Building Bridges, Bolyai Soc. Math. Stud. 19, Springer, Berlin, 2008, 499–513.

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

Liangpan Li
Department of Mathematics
Shanghai Jiao Tong University
Shanghai 200240, China
and
Department of Mathematics
Texas State University
San Marcos, TX 78666, U.S.A.
E-mail: liliangpan@yahoo.com.cn

Received on 11.7.2009
and in revised form on 24.5.2010 (6084)