Bull. Aust. Math. Soc. **100** (2019), 268–280
doi:10.1017/S0004972719000303

A NEW SUM–PRODUCT ESTIMATE IN PRIME FIELDS

CHANGHAO CHEN, BRYCE KERR✉ and ALI MOHAMMADI

(Received 11 December 2018; accepted 10 January 2019; first published online 24 May 2019)

Abstract

We obtain a new sum–product estimate in prime fields for sets of large cardinality. In particular, we show that if $A \subseteq \mathbb{F}_p$ satisfies $|A| \leqslant p^{64/117}$ then $\max\{|A \pm A|, |AA|\} \gtrsim |A|^{39/32}$. Our argument builds on and improves some recent results of Shakan and Shkredov ['Breaking the 6/5 threshold for sums and products modulo a prime', Preprint, 2018, arXiv:1806.07091v1] which use the eigenvalue method to reduce to estimating a fourth moment energy and the additive energy $E^+(P)$ of some subset $P \subseteq A + A$. Our main novelty comes from reducing the estimation of $E^+(P)$ to a point–plane incidence bound of Rudnev ['On the number of incidences between points and planes in three dimensions', *Combinatorica* **38**(1) (2017), 219–254] rather than a point–line incidence bound used by Shakan and Shkredov.

2010 *Mathematics subject classification*: primary 11T99; secondary 05B10.

Keywords and phrases: sum–product estimate, additive combinatorics.

1. Introduction

Let p be a prime number and $\mathbb{F}_p$ the finite field of order p. Given a subset $A \subseteq \mathbb{F}_p$, define the sum set and product set of A respectively by $A + A = \{a + b : a, b \in A\}$ and $AA = \{ab : a, b \in A\}$. The sum–product theorem in $\mathbb{F}_p$ due to Bourgain, Katz and Tao [2] states that for $0 < \varepsilon < 1$ there exists $\delta > 0$ such that if $p^{\varepsilon} < |A| < p^{1-\varepsilon}$ then

$$\max\{|AA|, |A + A|\} \geqslant |A|^{1+\delta}. \tag{1.1}$$

Glibichuk and Konyagin [7] have shown that the condition $p^{\varepsilon} < |A|$ may be dropped.

The sum–product problem was first considered by Erdős and Szemerédi [4] over the integers. Their work led to the conjecture that for any $\varepsilon > 0$ and any finite subset $A \subseteq \mathbb{R}$,

$$\max\{|AA|, |A + A|\} \gg |A|^{2-\varepsilon},$$

with an implied constant depending only on ε. The sharpest sum–product result over $\mathbb{R}$ is due to Shakan [18].

The first and second author were supported by ARC Grant DP170100786.

By a construction due to Garaev [6], for any $N \leq p$ there exists a subset $A \subseteq \mathbb{F}_p$ with $|A| = N$ such that

$$\max\{|A + A|, |AA|\} \ll p^{1/2}N^{1/2}, \tag{1.2}$$

so the Erdős–Szemerédi conjecture cannot be true in full generality in $\mathbb{F}_p$. We expect this conjecture to be true in $\mathbb{F}_p$ if we restrict to sets of sufficiently small cardinality, and an active field of research seeks to determine the largest possible δ such that (1.1) holds. The first explicit sum–product result in $\mathbb{F}_p$ is due to Garaev [5], and there have been several improvements (see [1, 8, 10, 15]). Roche-Newton, Rudnev and Shkredov [14] made a major breakthrough based on Rudnev's point–plane incidence bound [16] by showing that if $|A| \leqslant p^{5/8}$ then

$$\max\{|A + A|, |AA|\} \gg |A|^{6/5}. \tag{1.3}$$

The idea of applying geometric incidence estimates to sum–product problems is due to Elekes [3]. Stevens and de Zeeuw [22] gave a different proof of the estimate (1.3) using their point–line incidence bound. Recently, Shakan and Shkredov [19, Theorem 1.3] have broken the 6/5 barrier for the sum–product problem over $\mathbb{F}_p$ and shown that

$$\max\{|A \pm A|, |AA|\} \gtrsim |A|^{6/5+4/305}, \quad |A| \leqslant p^{3/5}. \tag{1.4}$$

We note that their condition $|A| \leqslant p^{3/5}$ can be extended to $|A| < p^{2/3}$ (see Remark 3.7 for more details). For sets of smaller cardinality, the estimate (1.4) has recently been improved by Rudnev, Shakan and Shkredov [17] who showed that

$$\max\{|A \pm A|, |AA|\} \gtrsim |A|^{11/9}, \quad |A| \leqslant p^{18/35}. \tag{1.5}$$

The argument of Rudnev, Shakan and Shkredov [17] uses geometric incidence estimates to establish recursive inequalities for generalised energies $E^+_\alpha(A)$ as a function of α, where $E^+_\alpha(A)$ is defined as in (3.1). The estimate (1.5) is deduced from an inequality involving $E^+_{4/3}(A)$ where the exponent 4/3 arises naturally as a fixed point of the recursion. See also [12] for variations on the sum–product theorem, including sharper results for the few sums, many products problem, [13] for the few products many sums problem, and [11] for various other results related to expanders in prime fields.

In this paper we obtain a new sum–product estimate over $\mathbb{F}_p$ which improves on the estimates (1.4) and (1.5) for sets of cardinality in the range $p^{18/35} \leqslant |A| \leqslant p^{64/117}$. Our proof builds on techniques from [19] which use the eigenvalue method (see [20]) to reduce to estimating a fourth moment energy $E^+_4(A, B)$ and the additive energy $E^+(P)$ of some subset $P \subseteq A + A$. Shakan and Shkredov reduce both $E^+_4(A, B)$ and $E^+(P)$ to the point–line incidence bound of Stevens and de Zeeuw and our improvement comes from estimating $E^+(P)$ via Rudnev's point–plane incidence bound.

Asymptotic notation. For positive real numbers X and Y, we use $X \ll Y$ and $Y \gg X$ to imply the existence of an absolute constant $C > 0$ such that $X \leq CY$. We also use $X \lesssim Y$ and $Y \gtrsim X$ to mean that there exists an absolute constant $C > 0$ such that $X \ll (\log X)^C Y$.

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

2. Main results

Our first result provides an improvement on the sum–product estimate of Shakan and Shkredov [19, Theorem 1.3].

THEOREM 2.1. *Suppose* $A \subset \mathbb{F}_p$ *satisfies* $|A| \leqslant p^{64/117}$. *Then*

$$\max\{|A \pm A|, |AA|\} \gtrsim |A|^{39/32}.$$

For comparison with the estimate (1.4), we note that

$$\frac{39}{32} = \frac{6}{5} + \frac{4}{305} + \frac{11}{1952}.$$

In the case of the difference set we obtain an estimate of the same strength with weaker conditions on the cardinality of A.

THEOREM 2.2. *Suppose* $A \subset \mathbb{F}_p$ *satisfies* $|A| \ll p^{32/55}$. *Then*

$$\max\{|A - A|, |AA|\} \gtrsim |A|^{39/32}.$$

We can obtain sharper estimates for iterated sumsets. The case $k = 3$ below agrees with an estimate of Roche-Newton, Rudnev and Shkredov [14, Corollary 12].

THEOREM 2.3. *Let* $k \geqslant 3$ *be an integer and suppose* $A \subseteq \mathbb{F}_p$ *satisfies*

$$|A| \leqslant p^{(4-3\times 2^{-k})/(7-16\times 2^{-k})}.$$

Then

$$\max\{|kA|, |AA|\} \gtrsim |A|^{(5-2^{3-k})/(4-3\times 2^{1-k})}.$$

3. Preliminaries

Given subsets $A, B \subseteq \mathbb{F}_p$, let

$$r_{A\pm B}(x) = |\{(a, b) \in A \times B : a \pm b = x\}|$$

and for any real number k define

$$E_k^+(A, B) = \sum_{x \in A-B} r_{A-B}(x)^k. \tag{3.1}$$

We write simply $E_k^+(A)$ instead of $E_k^+(A, A)$ and use $E^+(A, B)$ to denote $E_2^+(A, B)$, which we refer to as the additive energy between A and B. Note that if k is a natural number, then $E_k^+(A, B)$ counts the number of solutions to the equations

$$a_1 - b_1 = \cdots = a_k - b_k, \quad a_1, \ldots, a_k \in A, \ b_1, \ldots, b_k \in B.$$

We sometimes write $\sum_x$ to represent $\sum_{x \in \mathbb{F}_p}$ for convenience when the context is clear. For $A \subset \mathbb{F}_p$, we let $A(x)$ denote the characteristic function of A. We can write $r_{A+B}(x)$ as the convolution of functions A and B, that is, $r_{A+B}(x) = (A * B)(x)$. The following lemma is due to Shkredov [20, Proposition 31] (see also [19, Lemma 6.1]).

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

Lemma 3.1. *For any subset $A \subset \mathbb{F}_p$ and any $P \subset A - A$,*

$$\Big(\sum_{x\in P} r_{A-A}(x)\Big)^8 \le |A|^8 E_4^+(A)E^+(P).$$

Similarly, for any $P \subset A + A$,

$$\Big(\sum_{x\in P} r_{A+A}(x)\Big)^8 \le |A|^8 E_4^+(A)E^+(P).$$

We also require a third moment estimate of Konyagin and Rudnev [9, Corollary 10].

Lemma 3.2. *For any subset $A \subset \mathbb{F}_p$,*

$$\frac{|A|^8}{|A-A|} \ll E_3^+(A)E^+(A, A-A).$$

Next, we recall a variation of the Plünnecke–Ruzsa inequality, which can be found in [8].

Lemma 3.3. *Let $X, B_1, \dots, B_k \subseteq \mathbb{F}_p$. Then for any ϵ with $0 < \epsilon < 1$ there exists a subset $X' \subseteq X$ with $|X'| \ge (1-\epsilon)|X|$, such that*

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

The following point–line incidence bound is due to Stevens and de Zeeuw [22] (see also [21, Lemma 12]).

Lemma 3.4. *Let $P = X \times Y$ be a subset of $\mathbb{F}_p^2$ and L be a collection of lines in $\mathbb{F}_p^2$. Then*

$$I(P, L) \ll |X|^{3/4}|Y|^{1/2}|L|^{3/4} + |L| + |P| + p^{-1}|L||P|.$$

Remark 3.5. Using Lemma 3.4 and a technique due to Elekes [3], as outlined in [22, Corollary 9], one recovers estimate (1.3) for any set $A \subset \mathbb{F}_p$ under the condition $|A| \ll p^{5/7}$. It is worth noting that this improves on the condition $|A| \le p^{5/8}$, which was obtained in [14] and [22]. Furthermore, by (1.2), it is easy to see that this condition is optimal up to some constant.

The following lemma is due to Shakan and Shkredov [19, Proposition 3.1] and is based on Lemma 3.4. We note that their condition on the cardinality $|A| < p^{3/5}$ can be extend to $|A| < p^{2/3}$ and we provide details of this extension.

Lemma 3.6. *Let $A \subset \mathbb{F}_p$ satisfy $|A| < p^{2/3}$. Then for any subset $B \subset \mathbb{F}_p$,*

$$E_4^+(A, B) \lesssim |B|^3|AA|^2|A|^{-1}.$$

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

Proof. Define $D_\tau = \{x \in A - B : \tau \leq r_{A-B}(x) < 2\tau\}$. Taking a dyadic decomposition of $r_{A-B}(x)$, there exists a real number τ such that

$$E_4^+(A,B) = \sum_x r_{A-B}(x)^4 \lesssim \tau^4 |D_\tau|, \tag{3.2}$$

and

$$\tau |D_\tau| \ll |A||B|, \quad \tau^2 |D_\tau| \ll E^+(A,B). \tag{3.3}$$

Consider the set of points $P = D_\tau \times AA$ and the set of lines $L = \{\ell_{a,b} : a \in A, b \in B\}$ where $\ell_{a,b} = \{(x,y) \in \mathbb{F}_p^2 : y = (x+b)a\}$. For any $a \in A$ and $b \in B$,

$$|\ell_{a,b} \cap P| \geq \sum_{a_1 \in A} \mathbf{1}_{D_\tau}(a_1 - b).$$

Thus

$$I(P,L) = \sum_{a \in A, b \in B} |\ell_{a,b} \cap P| \geq \sum_{a \in A} \sum_{a_1 \in A, b \in B} \mathbf{1}_{D_\tau}(a_1 - b) = \sum_{a \in A} \sum_{x \in D_\tau} r_{A-B}(x) \gg |A||D_\tau|\tau.$$

Combining this with Lemma 3.4, we conclude that

$$|A||D_\tau|\tau \ll |D_\tau|^{3/4}|AA|^{1/2}(|A||B|)^{3/4} + |D_\tau||AA| + |A||B| + p^{-1}|D_\tau||AA||A||B|. \tag{3.4}$$

We proceed on a case-by-case basis depending on which term in (3.4) dominates.

Suppose the first term dominates, so that

$$|A||D_\tau|\tau \ll |D_\tau|^{3/4}|AA|^{1/2}(|A||B|)^{3/4}.$$

This gives the desired result after substituting in (3.2).

Suppose the second term in (3.4) dominates. This implies $|A||D_\tau|\tau \ll |D_\tau||AA|$, and hence $\tau \ll |AA|/|A|$. From (3.3) and the trivial bound $E^+(A,B) \leqslant |A||B|^2$,

$$\tau^4 |D_\tau| = \tau^2 E^+(A,B) \ll |B|^2|AA|^2|A|^{-1}.$$

If the third term in (3.4) dominates, then $\tau|D_\tau| \ll |B|$, so that using the trivial bound $\tau \leq \min\{|A|, |B|\}$, we obtain

$$\tau^4|D_\tau| = \tau^3 \tau |D_\tau| \ll |B|^3|A| \ll |B|^3|AA|^2|A|^{-1}.$$

Finally, consider when the last term in (3.4) dominates, so that

$$p\tau \ll |B||AA|. \tag{3.5}$$

If $\tau \leq |AA||B||A|^{-3/2}$, then

$$|D_\tau|\tau^4 = |D_\tau|\tau^2\tau^2 \ll |A|^2|B||AA|^2|B|^2|A|^{-3},$$

which gives the desired result. Otherwise, suppose $\tau > |AA||B||A|^{-3/2}$. Combined with (3.5), this implies that $p|AA||B||A|^{-3/2} \ll |B||AA|$ and contradicts our assumption $|A| < p^{2/3}$. □

REMARK 3.7. Combining Lemma 3.6 with [19, Theorem 2.5] leads to the same sum–product estimate as [19, Theorem 1.3] with the weaker condition $|A| < p^{2/3}$.

Using Hölder's inequality and Lemma 3.6 we obtain the following third moment estimate which will be used in the proof of Theorem 2.2.

LEMMA 3.8. *For any subset $A \subset \mathbb{F}_p$ satisfying $|A| < p^{2/3}$,*

$$E_3^+(A) \lesssim |AA|^{4/3}|A|^2.$$

PROOF. Writing

$$E_3^+(A) = \sum_x r_{A-A}(x)^{8/3+1/3}$$

and applying Hölder's inequality and Lemma 3.6 gives

$$E_3^+(A) \leq E_4^+(A)^{2/3}(|A||A|)^{1/3} \lesssim (|AA|^2|A|^2)^{2/3}|A|^{2/3},$$

which is the desired result. □

The following lemma is due to Roche-Newton *et al.* [14, Theorem 6] and is based on Rudnev's point–plane incidence bound [16].

LEMMA 3.9. *Let $X, Y, Z \subset \mathbb{F}_p$ and let $M = \max\{|X|, |YZ|\}$. Suppose that $|X||Y||YZ| \ll p^2$. Then*

$$E^+(X, Z) \ll (|X||YZ|)^{3/2}|Y|^{-1/2} + M|X||YZ||Y|^{-1}.$$

COROLLARY 3.10. *Let $A \subset \mathbb{F}_p$. If $|A \pm A||AA||A| \ll p^2$ then*

$$E^+(A, A \pm A) \ll (|A \pm A||AA|)^{3/2}|A|^{-1/2}.$$

PROOF. We consider only $A + A$; a similar argument applies to $A - A$. Applying Lemma 3.9 with $X = A + A$ and $Y = Z = A$ gives

$$E^+(A, A + A) \ll (|A + A||AA|)^{3/2}|A|^{-1/2} + |A + A|^2|AA||A|^{-1} + |A + A||AA|^2|A|^{-1}.$$

Observe that for any subset $A \subset \mathbb{F}_p$,

$$(|A + A||AA|)^{3/2}|A|^{-1/2} \geq \max\{|A + A|^2|AA||A|^{-1}, |A + A||AA|^2|A|^{-1}\},$$

from which the desired result follows. □

COROLLARY 3.11. *Let $A \subseteq \mathbb{F}_p$. If $|A|^2|AA| \ll p^2$ then*

$$E^+(A) \ll |AA|^{3/2}|A|.$$

In the proof of Theorem 2.3, we use the following iterative inequality for higher-order energies.

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

Lemma 3.12. *For an integer $k \geqslant 2$ and a subset $A \subseteq \mathbb{F}_q$, let $T_k(A)$ count the number of solutions to the equation*

$$a_1 + \cdots + a_k = a_{k+1} + \cdots + a_{2k}, \quad a_1, \ldots, a_{2k} \in A.$$

If A satisfies

$$|A|\,|(k-1)A|\,|AA| \leqslant p^2, \tag{3.6}$$

then

$$T_k(A) \lesssim |A|^{k-3/2} T_{k-1}(A)^{1/2} |AA|^{3/2} + |A|^{2k-3}|AA| + \frac{T_{k-1}(A)|AA|^2}{|A|}.$$

Proof. For $\lambda \in (k-1)A$, we define

$$r(\lambda) = |\{(a_1, \ldots, a_{k-1}) \in A \times \cdots \times A \ : a_1 + \cdots + a_{k-1} = \lambda\}|.$$

Then

$$T_k(A) = \sum_x (A * r)(x)^2.$$

Now we take a dyadic decomposition for r. For an integer $j \geqslant 1$, let

$$J(j) = \{\lambda \in (k-1)A \ : 2^{j-1} \leqslant r(\lambda) < 2^j\}.$$

Then

$$(A * r)(x) \ll \sum_{1 \le j \le \log|A|} 2^j (A * J(j))(x).$$

By the Cauchy–Schwarz inequality,

$$(A * r)(x)^2 \lesssim \sum_{1 \le j \le \log|A|} 2^{2j} (A * J(j))(x)^2.$$

Thus

$$T_k(A) \lesssim \sum_{1 \le j \le \log|A|} \sum_x 2^{2j} (A * J(j))(x)^2$$

and there exists some i_0 with $1 \leqslant i_0 \ll \log|A|$ such that

$$T_k(A) \lesssim 2^{2i_0} E^+(A, J(i_0)). \tag{3.7}$$

By Lemma 3.9,

$$E^+(A, J(i_0)) \ll (|J(i_0)||AA|)^{3/2}|A|^{-1/2} + \max\{|J(i_0)|, |AA|\}|J(i_0)||AA||A|^{-1}, \tag{3.8}$$

provided $|J(i_0)||A||AA| \leqslant p^2$. This condition is satisfied by (3.6) and the inclusion $J(i_0) \subseteq (k-1)A$. By (3.7) and (3.8),

$$T_k(A) \lesssim \frac{(2^{i_0}|J(i_0)|)(2^{i_0}|J(i_0)|^{1/2})|AA|^{3/2}}{|A|^{1/2}} + \frac{(2^{2i_0}|J(i_0)|^2)|AA|}{|A|} + \frac{(2^{2i_0}|J(i_0)|)|AA|^2}{|A|}.$$

Since $2^{i_0}|J(i_0)| \ll |A|^{(k-1)}$ and $2^{2i_0}|J(i_0)| \ll T_{k-1}(A)$,

$$T_k(A) \lesssim |A|^{k-3/2} T_{k-1}(A)^{1/2} |AA|^{3/2} + |A|^{2k-3}|AA| + \frac{T_{k-1}(A)|AA|^2}{|A|},$$

which completes the proof. □

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

4. Proof of Theorem 2.1

We consider the case $A + A$; a similar argument applies to $A - A$. Assuming A satisfies

$$|A| \leqslant p^{64/117}, \tag{4.1}$$

we consider two cases. Suppose first that

$$|A + A|^2|AA| \ll p^2. \tag{4.2}$$

By Lemma 3.3, we can identify a subset $B \subset A$ satisfying

$$|B| \gg |A| \quad \text{and} \quad |B + B + B| \ll \frac{|A + A|^2}{|A|}. \tag{4.3}$$

By (4.3), in order to prove Theorem 2.1, it is sufficient to show that

$$\max\{|B + B|, |BB|\} \gtrsim |B|^{39/32}.$$

Let

$$P = \left\{x \in B + B : r_{B+B}(x) \geq \frac{1}{2}\frac{|B|^2}{|B + B|}\right\}, \tag{4.4}$$

so that

$$\sum_{x\in P} r_{B+B}(x) \gg |B|^2.$$

Applying Lemma 3.1,

$$|B|^8 \ll E_4^+(B)E^+(P)$$

and, by Lemma 3.6,

$$|B|^6 \lesssim |BB|^2 E^+(P). \tag{4.5}$$

It remains to consider $E^+(P)$. Recalling (4.4), we see that for any $x \in \mathbb{F}_p$,

$$\frac{|B|^2}{|B + B|}P(x) \ll (B * B)(x)$$

and hence

$$(P * P)(x) \ll \frac{|B + B|}{|B|^2}(B * B * P)(x).$$

Thus

$$E^+(P) = \sum_x (P * P)(x)^2 \lesssim \frac{|B + B|^2}{|B|^4} \sum_x (B * B * P)(x)^2.$$

Taking a dyadic decomposition for the function $(B * P)(x)$, there exists some real number Δ satisfying $1 \leq \Delta \leq |B|$ such that, defining

$$T = \{x \in B + P : \Delta \leq (B * P)(x) < 2\Delta\},$$

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

we have

$$\sum_x (P * P)(x)^2 \lesssim \frac{|B+B|^2}{|B|^4}\Delta^2 \sum_x (B * T)(x)^2 = \frac{|B+B|^2}{|B|^4}\Delta^2 E^+(B,T).$$

Since $T \subseteq B+B+B$, by (4.2) and (4.3),

$$|B||B+B+B||BB| \ll p^2,$$

and hence, by Lemma 3.9,

$$E^+(B,T) \ll |T|^{3/2}|BB|^{3/2}|B|^{-1/2} + |T|^2|BB||B|^{-1} + |T||BB|^2|B|^{-1}.$$

This gives

$$\begin{aligned}\sum_x (P * P)(x)^2 \lesssim{}& \frac{|B+B|^2}{|B|^4}(\Delta|T|)(\Delta|T|^{1/2})|BB|^{3/2}|B|^{-1/2}\\ &+ \frac{|B+B|^2}{|B|^4}(\Delta|T|)^2|BB||B|^{-1} + \frac{|B+B|^2}{|B|^4}(\Delta^2|T|)|BB|^2|B|^{-1}.\end{aligned}$$

Since $\Delta|T| \ll |B||P|$, $\Delta^2|T| \ll E^+(B,P)$ and $P \subseteq B+B$, this simplifies to

$$\begin{aligned}E^+(P) \lesssim{}& \frac{|B+B|^3|BB|^{3/2}E^+(B,B+B)^{1/2}}{|B|^{7/2}}\\ &+ \frac{|B+B|^4|BB|}{|B|^3} + \frac{|B+B|^2|BB|^2E^+(B,B+B)}{|B|^5}.\end{aligned} \tag{4.6}$$

We proceed on a case-by-case basis depending on which term in (4.6) dominates. Suppose first that

$$E^+(P) \lesssim \frac{|B+B|^3|BB|^{3/2}E^+(B,B+B)^{1/2}}{|B|^{7/2}}.$$

Assumption (4.2) implies that the conditions of Corollary 3.10 are satisfied and

$$E^+(P) \lesssim \frac{|B+B|^{15/4}|BB|^{9/4}}{|B|^{15/4}}.$$

Combining with (4.5),

$$|B|^{39} \lesssim |B+B|^{15}|BB|^{17},$$

which gives the required result.

Suppose next that

$$E^+(P) \lesssim \frac{|B+B|^4|BB|}{|B|^3}.$$

Combining with (4.5),

$$|B|^9 \lesssim |B+B|^4|BB|^3,$$

which gives a better bound than $39/32$.

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

Finally, suppose

$$E^+(P) \lesssim \frac{|B+B|^2|BB|^2E^+(B, B+B)}{|B|^5}.$$

By Corollary 3.10,

$$E^+(P) \lesssim \frac{|B+B|^{7/2}|BB|^{7/2}}{|B|^{11/2}},$$

and hence, by (4.5),

$$|B|^{23} \lesssim |B+B|^7|BB|^{11},$$

giving a better bound than 39/32. This finishes the proof in the case $|A+A|^2|AA| \leqslant p^2$.

Suppose next that $|A+A|^2|AA| \geqslant p^2$. By (4.1), $|A+A|^2|AA| \geqslant |A|^{117/32}$ and hence

$$\max\{|A+A|, |AA|\} \geqslant |A|^{39/32},$$

which completes the proof.

5. Proof of Theroem 2.2

Suppose A satisfies

$$|A| \leqslant p^{32/55}. \tag{5.1}$$

We consider two cases. Suppose first that $|A-A||AA|A| \leqslant p^2$. By Lemma 3.2, Lemma 3.8 and Corollary 3.10,

$$\frac{|A|^8}{|A-A|} \ll (|A|^2|AA|^{4/3})(|A-A|^{3/2}|AA|^{3/2}|A|^{-1/2}),$$

which reduces to $|A-A|^{15}|AA|^{17} \gg |A|^{39}$ and gives the required result. On the other hand, if $|A-A||AA||A| \geqslant p^2$, then by (5.1), $|A-A||AA| \geqslant |A|^{39/16}$ as required.

6. Proof of Theorem 2.3

Suppose A satisfies

$$|A| \leqslant p^{(4-3\times 2^{-k})/(7-16\times 2^{-k})}. \tag{6.1}$$

We again consider two cases. Suppose first that

$$|A||(k-1)A||AA| \leqslant p^2. \tag{6.2}$$

We fix an integer $k \geqslant 3$ and consider two subcases. Suppose first that for all integers j with $3 \leqslant j \leqslant k$,

$$|A|^{j-3/2}T_{j-1}(A)^{1/2}|AA|^{3/2} \geqslant \max\left\{|A|^{2j-3}|AA|, \frac{T_{j-1}(A)|AA|^2}{|A|}\right\}.$$

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

By (6.2) and Lemma 3.12, this implies that for each j with $3 \leqslant j \leqslant k$,

$$T_j(A) \lesssim |A|^j \Big(\frac{|AA|}{|A|}\Big)^{3/2} T_{j-1}(A)^{1/2}$$

and, by induction on j,

$$T_k(A) \lesssim |A|^{k+(k-1)/2+\cdots+(k-j+1)/2^{j-1}} \Big(\frac{|AA|}{|A|}\Big)^{(3/2)(1+1/2+\cdots+1/2^{j-1})} T_{k-j}(A)^{1/2^j}.$$

Taking $j = k-2$ and using Corollary 3.11,

$$\begin{aligned} T_k(A) &\lesssim |A|^{k+(k-1)/2+\cdots+3/2^{k-3}} \Big(\frac{|AA|}{|A|}\Big)^{(3/2)(1+1/2+\cdots+1/2^{k-3})} E^+(A)^{1/2^{k-2}} \\ &\lesssim |A|^{2k-5+2^{3-k}} |AA|^{3(1-2^{1-k})}. \end{aligned} \tag{6.3}$$

For $x \in \mathbb{F}_p$, let

$$r_{A,k}(x) = |\{(x_1, \ldots, x_k) \in A^k : x_1 + \cdots + x_k = x\}|.$$

Then

$$|A|^k = \sum_x r_{A,k}(x).$$

By the Cauchy–Schwarz inequality,

$$|A|^{2k} \leqslant |kA| T_k(A),$$

since

$$\sum_x r_{A,k}(x)^2 = T_k(A).$$

Applying (6.3),

$$|A|^{5-2^{3-k}} \lesssim |kA||AA|^{3-3\times 2^{1-k}},$$

which implies

$$\max\{|kA|, |AA|\} \gtrsim |A|^{(5-2^{3-k})/(4-3\times 2^{1-k})}. \tag{6.4}$$

Suppose next that there exists some j with $3 \leqslant j \leqslant k$ such that

$$|A|^{j-3/2} T_{j-1}(A)^{1/2} |AA|^{3/2} \leqslant \max\Big\{|A|^{2j-3}|AA|, \frac{T_{j-1}(A)|AA|^2}{|A|}\Big\}.$$

If

$$|A|^{2j-3}|AA| \geqslant \frac{T_{j-1}(A)|AA|^2}{|A|},$$

then, by Lemma 3.12,

$$T_j(A) \lesssim |A|^{2j-3}|AA|.$$

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press

Using the Cauchy–Schwarz inequality as before,

$$|A|^{2j} \lesssim |A|^{2j-3}|jA||AA|,$$

which implies

$$\max\{|kA|,|AA|\} \gtrsim |A|^{3/2}$$

and is better than (6.4). If

$$\frac{T_{j-1}(A)|AA|^2}{|A|} \geqslant |A|^{2j-3}|AA|,$$

then

$$T_j(A) \lesssim \frac{T_{j-1}(A)|AA|^2}{|A|} \leqslant |A|^{2j-7}|AA|^2E^+(A),$$

and hence, by Corollary 3.11,

$$T_j(A) \lesssim |A|^{2j-6}|AA|^{7/2}.$$

This implies that

$$|A|^6 \lesssim |jA||AA|^{7/2}$$

and hence

$$\max\{|kA|,|AA|\} \gtrsim |A|^{4/3},$$

which is better than (6.4).

Suppose next that $|A||(k-1)A||AA| \geqslant p^2$. By (6.1),

$$|(k-1)A||AA| \geqslant |A|^{2(5-2^{3-k})/(4-3\times 2^{1-k})},$$

which completes the proof.

References

[1] 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.

[2] J. Bourgain, N. Katz and T. Tao, 'A sum-product estimate in finite fields and their applications', *Geom. Funct. Anal.* **14** (2004), 27–57.

[3] G. Elekes, 'On the number of sums and products', *Acta Arith.* **81** (1997), 365–367.

[4] P. Erdős and E. Szemerédi, 'On sums and products of integers', in: *Studies in Pure Mathematics. To the memory of Paul Turán* (Birkhäuser, Basel, 1983), 213–218.

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

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

[7] A. A. Glibichuk and S. V. Konyagin, 'Additive properties of product sets in fields of prime order', in: *Additive Combinatorics*, CRM Proceedings and Lecture Notes, 43 (American Mathematical Society, Providence, RI, 2007), 279–286.

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

[9] S. V. Konyagin and M. Rudnev, 'On new sum-product type estimates', *SIAM J. Discrete Math.* **27**(2) (2013), 973–990.
[10] L. Li, 'Slightly improved sum-product estimates in fields of prime order', *Acta Arith.* **147** (2011), 153–160.
[11] B. Murphy, O. Roche-Newton and I. Shkredov, 'Variations of the sum-product problem', *SIAM J. Discrete Math.* **29**(1) (2015), 514–540.
[12] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev and I. D. Shkredov, 'New results on sum-product type growth over fields', Preprint, 2017, arXiv:1702.01003.
[13] B. Murphy, M. Rudnev, I. Shkredov and Y. Shteinikov, 'On the few products, many sums problem', Preprint, 2017, arXiv:1712.0041v1.
[14] O. Roche-Newton, M. Rudnev and I. D. Shkredov, 'New sum-product type estimates over finite fields', *Adv. Math.* **293** (2016), 589–605.
[15] M. Rudnev, 'An improved sum-product inequality in fields of prime order', *Int. Math. Res. Not. IMRN* **2012**(16) (2012), 3693–3705.
[16] M. Rudnev, 'On the number of incidences between points and planes in three dimensions', *Combinatorica* **38**(1) (2017), 219–254.
[17] M. Rudnev, G. Shakan and I. Shkredov, 'Stronger sum-product inequalities for small sets', Preprint, 2018, arXiv:1808.08465.
[18] G. Shakan, 'On higher energy decomposition and the sum-product phenomenon', *Math. Proc. Came. Phil. Soc.*, to appear.
[19] G. Shakan and I. D. Shkredov, 'Breaking the 6/5 threshold for sums and products modulo a prime', Preprint, 2018, arXiv:1806.07091v1.
[20] I. D. Shkredov, 'Energies and structure of additive sets', *Electron. J. Combin.* **21**(3) (2014), 1–53.
[21] I. D. Shkredov, 'On asymptotic formulae in some sum-product questions', Preprint, 2018, arXiv:1802.09066.
[22] S. Stevens and F. de Zeeuw, 'An improved point-line incidence bound over arbitrary fields', *Bull. Lond. Math. Soc.* **49**(5) (2017), 842–858.

CHANGHAO CHEN, Department of Pure Mathematics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: changhao.chen@unsw.edu.au

BRYCE KERR, Department of Pure Mathematics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: bryce.kerr@unsw.edu.au

ALI MOHAMMADI, School of Mathematics and Statistics,
University of Sydney, NSW 2006, Australia
e-mail: alim@maths.usyd.edu.au

https://doi.org/10.1017/S0004972719000303 Published online by Cambridge University Press