

# Moscow Journal of Combinatorics and Number Theory

2019  
vol. 8 no. 3

$\infty$

3

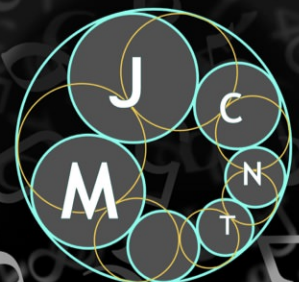
3

$\omega$

$\varepsilon$

On products of shifts in arbitrary fields

Audie Warren





# On products of shifts in arbitrary fields

Audie Warren

We adapt the approach of Rudnev, Shakan, and Shkredov (2018) to prove that in an arbitrary field  $\mathbb{F}$ , for all  $A \subset \mathbb{F}$  finite with  $|A| < p^{1/4}$  if  $p := \text{Char}(\mathbb{F})$  is positive, we have

$$|A(A+1)| \gg \frac{|A|^{11/9}}{(\log |A|)^{7/6}}, \quad |AA| + |(A+1)(A+1)| \gg \frac{|A|^{11/9}}{(\log |A|)^{7/6}}.$$

This improves upon the exponent of  $\frac{6}{5}$  given by an incidence theorem of Stevens and de Zeeuw.

## 1. Introduction and main result

For finite  $A \subseteq \mathbb{F}$ , we define the *sumset* and *product set* of  $A$  as

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

It is an active area of research to show that one of these sets must be large relative to  $A$ . The central conjecture in this area is the following.

**Conjecture 1** (Erdős–Szemerédi). *For all  $\epsilon > 0$ , and for all  $A \subseteq \mathbb{Z}$  finite, we have*

$$|AA| + |A + A| \gg |A|^{2-\epsilon}.$$

The notation  $X \ll Y$  is used to hide absolute constants; i.e.,  $X \ll Y$  if and only if there exists an absolute constant  $c > 0$  such that  $X \ll cY$ . If  $X \ll Y$  and  $Y \ll X$  we write  $X \asymp Y$ . We will let  $p$  denote the characteristic of  $\mathbb{F}$  throughout ( $p$  may be zero). Due to the possible existence of finite subfields in  $\mathbb{F}$ , extra restrictions on  $|A|$  relative to  $p$  must be imposed if  $p$  is positive; *all such conditions can be ignored if  $p = 0$ .*

Although Conjecture 1 is stated over the integers, it can be considered over fields, the real numbers being of primary interest. Current progress over  $\mathbb{R}$  places us at an exponent of  $\frac{4}{3} + c$  for some small  $c$ , due to Shakan [2018], building on [Konyagin and Shkredov 2015; Solymosi 2009]. Incidence geometry, and in particular the Szemerédi–Trotter theorem, are tools often used to prove such results in the real numbers.

Conjecture 1 can also be considered over arbitrary fields  $\mathbb{F}$ . Over arbitrary fields we replace the Szemerédi–Trotter theorem with a point-plane incidence theorem of [Rudnev 2018], which was used by Stevens and de Zeeuw [2017] to derive a point-line incidence theorem. An exponent of  $\frac{6}{5}$  was proved in 2014 by Roche-Newton, Rudnev, and Shkredov [Roche-Newton et al. 2016]. An application of the Stevens–de Zeeuw theorem also gives this exponent of  $\frac{6}{5}$  for Conjecture 1, so that  $\frac{6}{5}$  became a threshold to be broken.

MSC2010: 11B75, 68R05.

Keywords: growth, sum-product estimates, energy.

The  $\frac{6}{5}$  threshold has recently been broken; see [Shakan and Shkredov 2018; Rudnev et al. 2018; Chen et al. 2018]. The following theorem was proved by Rudnev, Shakan, and Shkredov and is the current state-of-the-art bound.

**Theorem 2** [Rudnev et al. 2018]. *Let  $A \subset \mathbb{F}$  be a finite set. If  $\mathbb{F}$  has positive characteristic  $p$ , assume  $|A| < p^{18/35}$ . Then we have*

$$|A + A| + |AA| \gg |A|^{11/9 - o(1)}.$$

Another way of considering the sum-product phenomenon is to consider the set  $A(A + 1)$ , which we would expect to be quadratic in size. This encapsulates the idea that a translation of a multiplicatively structured set should destroy its structure, which is a main theme in sum-product questions. Study of growth of  $|A(A + 1)|$  began in [Garaev and Shen 2010]; see also [Jones and Roche-Newton 2013; Zhelezov 2015; Mohammadi 2018]. Current progress for  $|A(A + 1)|$  comes from an application of the Stevens–de Zeeuw theorem, giving the same exponent of  $\frac{6}{5}$ . In this paper we use the multiplicative analogue of ideas in [Rudnev et al. 2018] to prove the following theorem.

**Theorem 3.** *Let  $A, B, C, D \subset \mathbb{F}$  be finite with the conditions*

$$|C(A + 1)||A| \leq |C|^3, \quad |C(A + 1)|^2 \leq |A||C|^3, \quad |B| \leq |D|, \quad |A|, |B|, |C|, |D| < p^{1/4}.$$

*Then we have*

$$|AB|^8 |C(A + 1)|^2 |D(B - 1)|^8 \gg \frac{|B|^{13} |A|^5 |D|^3 |C|}{(\log |A|)^{17} (\log |B|)^4}.$$

In our applications of this theorem we have  $|A| = |B| = |C| = |D|$  so that the first three conditions are trivially satisfied. The conditions involving  $p$  could likely be improved; however, for sake of exposition we do not attempt to optimise these. The main proof closely follows [Rudnev et al. 2018] (in the multiplicative setting), the central difference being a bound on multiplicative energies in terms of products of shifts. An application of Theorem 3 beats the threshold of  $\frac{6}{5}$ , matching the  $\frac{11}{9}$  appearing in Theorem 2. Specifically, we have:

**Corollary 4.** *Let  $A \subseteq \mathbb{F}$  be finite, with  $|A| < p^{1/4}$ . Then*

$$|A(A + 1)| \gg \frac{|A|^{11/9}}{(\log |A|)^{7/6}}, \quad |AA| + |(A + 1)(A + 1)| \gg \frac{|A|^{11/9}}{(\log |A|)^{7/6}}.$$

Corollary 4 can be seen by applying Theorem 3 with  $B = A + 1$ ,  $C = A$  and  $D = A + 1$  for the first result, and  $B = -A$ ,  $D = C = A + 1$  for the second result.

## 2. Preliminary results

We require some preliminary theorems. The first is the point-line incidence theorem of Stevens and de Zeeuw.

**Theorem 5** [Stevens and de Zeeuw 2017]. *Let  $A$  and  $B$  with  $|A| \geq |B|$  be finite subsets of a field  $\mathbb{F}$ , and let  $L$  be a set of lines. Assuming  $|L||B| \ll p^2$  and  $|B||A|^2 \leq |L|^3$ , we have*

$$I(A \times B, L) \ll |A|^{1/2} |B|^{3/4} |L|^{3/4} + |L|.$$

Note that as  $|A| \geq |B|$ , we have  $|A|^{1/2}|B|^{3/4} \leq |A|^{3/4}|B|^{1/2}$ ; in particular with the same conditions we have the above result with the exponents of  $A$  and  $B$  swapped. Because of this, the condition  $|A| \geq |B|$  is only needed to specify the second two conditions. We may therefore restate Theorem 5 as:

**Theorem 6.** *Let  $A$  and  $B$  be finite subsets of a field  $\mathbb{F}$ , and let  $L$  be a set of lines. Assuming*

$$|L| \min\{|A|, |B|\} \ll p^2 \quad \text{and} \quad |A||B| \max\{|A|, |B|\} \leq |L|^3,$$

*we have*

$$I(A \times B, L) \ll \min\{|A|^{1/2}|B|^{3/4}, |A|^{3/4}|B|^{1/2}\}|L|^{3/4} + |L|.$$

This second formulation will be how we apply Theorem 5. Before stating the next two theorems we require some definitions. For  $x \in \mathbb{F}$  we define the *representation function*

$$r_{A/D}(x) = \left| \left\{ (a, d) \in A \times D : \frac{a}{d} = x \right\} \right|.$$

Note that for all  $x$  we have  $r_{A/D}(x) \leq \min\{|A|, |D|\}$ . This is seen as fixing one of  $a, d$  in the equation  $a/d = x$  necessarily determines the other. The set  $A/D$  in this definition can be changed to any other combination of sets, changing the fraction  $a/d$  in the definition to match. For  $n \in \mathbb{R}^+$ , we define the  $n$ -th moment *multiplicative energy* of sets  $A, D \subseteq \mathbb{F}$  as

$$E_n^*(A, D) = \sum_x r_{A/D}(x)^n.$$

When  $n = 2$  we shall simply write  $E^*(A, D)$ , and when  $A = D$  we write  $E_n^*(A) := E_n^*(A, A)$ . By considering that we have  $a/a = 1$  for all  $a \in A$ , we have the trivial lower bound  $E_n^*(A) \geq |A|^n$ . When  $n$  is in fact a natural number,  $E_n^*(A, D)$  can be considered as the number of solutions to

$$\frac{a_1}{d_1} = \frac{a_2}{d_2} = \dots = \frac{a_n}{d_n}, \quad a_i \in A, \quad d_i \in D,$$

giving the trivial upper bound  $E_n^*(A, D) \leq |A|^n |D|$  by fixing  $a_1$  to  $a_n$  and then choosing a single  $d_i$ , which necessarily determines all other  $d_i$ .

We use Theorem 6 to prove two further results. The first is a bound on the fourth-order multiplicative energy relative to products of shifts.

**Theorem 7.** *For all finite nonempty  $A, C, D \subset \mathbb{F}$  with*

$$|A|^2 |C(A+1)| \leq |D| |C|^3, \quad |A| |C(A+1)|^2 \leq |D|^2 |C|^3, \quad |A| |C| |D|^2 \ll p^2,$$

*we have*

$$E_4^*(A, D) \ll \min \left\{ \frac{|C(A+1)|^2 |D|^3}{|C|}, \frac{|C(A+1)|^3 |D|^2}{|C|} \right\} \log |A|.$$

The second result is similar, but for the second moment multiplicative energy.

**Theorem 8.** *For all finite and nonempty  $A, C, D \subset \mathbb{F}$  with*

$$|A|^2 |C(A+1)| \leq |D| |C|^3, \quad |A| |C(A+1)|^2 \leq |D|^2 |C|^3, \quad |A| |C| |D| \min\{|C|, |D|\} \ll p^2,$$

*we have*

$$E^*(A, D) \ll \frac{|C(A+1)|^{3/2} |D|^{3/2}}{|C|^{1/2}} \log |A|.$$

The set  $A + 1$  appearing in these theorems can be changed to any translate  $A + \lambda$  for  $\lambda \neq 0$  by noting that  $|C(A + 1)| = |C(\lambda A + \lambda)|$  and renaming  $A' = \lambda A$ . For our purposes, we will use  $\lambda = \pm 1$ .

*Proof of Theorem 7.* Without loss of generality, we can assume that  $0 \notin A, C, D$ . We begin by proving

$$E_4^*(A, D) \ll \frac{|C(A + 1)|^2 |D|^3}{|C|} \log |A|.$$

Define the set

$$S_\tau := \{x \in A/D : \tau \leq r_{A/D}(x) < 2\tau\}.$$

By a dyadic decomposition, there is some  $\tau$  with

$$|S_\tau| \tau^4 \ll E_4^*(A, D) \ll |S_\tau| \tau^4 \log |A|.$$

Note that  $\tau \leq \min\{|A|, |D|\}$ . Take an element  $t \in S_\tau$ . It has  $\tau$  representations in  $A/D$ , so there are  $\tau$  ways to write  $t = a/d$  with  $a \in A$ ,  $d \in D$ . For all  $c \in C$ , we have

$$t = \frac{a}{d} = \frac{1}{d} \left( \frac{ac + c - c}{c} \right) = \frac{1}{d} \left( \frac{\alpha}{c} - 1 \right),$$

where  $\alpha = c(a + 1) \in C(A + 1)$ . This shows that we have  $|S_\tau| \tau |C|$  incidences between the lines

$$L = \{l_{d,c} : d \in D, c \in C\}, \quad l_{d,c} \text{ given by } y = \frac{1}{d} \left( \frac{x}{c} - 1 \right),$$

and the point set  $P = C(A + 1) \times S_\tau$ . Under the conditions  $|D||C| \min\{|S_\tau|, |C(A + 1)|\} \ll p^2$  and  $|S_\tau||C(A + 1)| \max\{|S_\tau|, |C(A + 1)|\} \leq |D|^3 |C|^3$ , we have

$$|S_\tau| \tau |C| \leq I(P, L) \ll |C(A + 1)|^{1/2} |S_\tau|^{3/4} |C|^{3/4} |D|^{3/4} + |D||C|.$$

The conditions are satisfied under the assumptions  $|D||A||C| \min\{|D|, |C|\} \ll p^2$ ,  $|A|^2 |C(A + 1)| \leq |D||C|^3$ , and  $|A||C(A + 1)|^2 \leq |D|^2 |C|^3$ . Assuming that the leading term is dominant, we have

$$|S_\tau| \tau^4 |C| \ll |C(A + 1)|^2 |D|^3$$

so that as  $E_4^*(A, D)/\log |A| \ll |S_\tau| \tau^4$ , we have

$$E_4^*(A, D) \ll \frac{|C(A + 1)|^2 |D|^3}{|C|} \log |A|.$$

We therefore assume the leading term is not dominant. Suppose  $|D||C|$  is dominant so that

$$|C(A + 1)|^{1/2} |S_\tau|^{3/4} |C|^{3/4} |D|^{3/4} \leq |D||C|. \quad (1)$$

Multiplying by  $\tau^3$  and simplifying, we have

$$|C(A + 1)|^2 \frac{E_4^*(A, D)^3}{\log |A|^3} \ll |C(A + 1)|^2 |S_\tau|^3 \tau^{12} \leq |D||C| \tau^{12} \implies E_4^*(A, D) \ll \frac{|D|^{1/3} |C|^{1/3} \tau^4}{|C(A + 1)|^{2/3}} \log |A|.$$

The result now follows if

$$\frac{|D|^{1/3} |C|^{1/3} \tau^4}{|C(A + 1)|^{2/3}} \ll \frac{|C(A + 1)|^2 |D|^3}{|C|}.$$

We must therefore prove the result in the case that this is not true; we will prove the result under the assumption

$$\frac{|C(A+1)|^2 |D|^3}{|C|} \leq \frac{|D|^{1/3} |C|^{1/3} \tau^4}{|C(A+1)|^{2/3}},$$

which gives (using  $\tau \leq |A|$ )

$$|D|^8 |C|^4 |A|^4 \leq |D|^8 |C(A+1)|^8 \leq \tau^{12} |C|^4 \leq |A|^{12} |C|^4,$$

so that we have  $|D| \leq |A|$ . We then have (using  $|C(A+1)| \geq |C|^{1/2} |A|^{1/2}$ )

$$|D||C| \geq |C(A+1)|^{1/2} |S_\tau|^{3/4} |C|^{3/4} |D|^{3/4} \geq |C(A+1)|^{1/2} |C|^{3/4} |D|^{3/4} \geq |A|^{1/4} |C| |D|^{3/4} \geq |D||C|,$$

so that the two terms are in fact balanced and the result follows.

Secondly, we prove that

$$E_4^*(A, D) \ll \frac{|C(A+1)|^3 |D|^2}{|C|} \log |A|.$$

To do this, we swap the roles of  $D$  and  $S_\tau$  from above. We define the line set and point set by

$$L = \{l_{t,c} : t \in S_\tau, c \in C\}, \quad P = C(A+1) \times D.$$

Any incidence from the previous point and line sets remains an incidence for the new ones, via

$$t = \frac{1}{d} \left( \frac{\alpha}{c} - 1 \right) \iff d = \frac{1}{t} \left( \frac{\alpha}{c} - 1 \right).$$

Under the conditions

$$|S_\tau| |C| \min\{|D|, |C(A+1)|\} \ll p^2, \quad |D||C(A+1)| \max\{|D|, |C(A+1)|\} \leq |S_\tau|^3 |C|^3, \quad (2)$$

we have

$$|S_\tau| \tau |C| \leq I(P, L) \ll |C(A+1)|^{3/4} |S_\tau|^{3/4} |C|^{3/4} |D|^{1/2} + |S_\tau| |C|.$$

If the leading term dominates, the result follows from  $|S_\tau| \tau^4 \gg E_4^*(A, D)/\log |A|$ . Assume the leading term is not dominant; that is,

$$|C(A+1)|^3 |D|^2 \leq |S_\tau| |C|.$$

Then by using  $|S_\tau| \leq |A||D|$  and  $|A|, |C| \leq |C(A+1)|$  we have

$$|A||C|^2 |D|^2 \leq |C(A+1)|^3 |D|^2 \leq |S_\tau| |C| \leq |A||D||C|,$$

so that  $|C| = |D| = 1$  and the result is trivial by  $E_4^*(A, D) \leq |A||D|^4 \leq |A|$ .

We now check the conditions (2) for using Theorem 5. The first condition in (2) is satisfied if  $|A||C||D|^2 \ll p^2$ , which is true under our assumptions. The second depends on  $\max\{|D|, |C(A+1)|\}$ , which we assume is  $|D|$  (if not the first term in Theorem 7 gives stronger information, which we have already proved). Assuming the second condition does not hold, we have

$$|S_\tau|^3 |C|^3 < |D|^2 |C(A+1)|.$$

Multiplying by  $\tau^{12}$  and bounding  $\tau \leq |A|$ , we get

$$E_4^*(A, D) \ll \frac{|A|^4 |D|^{2/3} |C(A+1)|^{1/3}}{|C|} \log |A|. \quad (3)$$

We may now assume the bound

$$\frac{|C(A+1)|^3 |D|^2}{|C|} \leq \frac{|A|^4 |D|^{2/3} |C(A+1)|^{1/3}}{|C|}. \quad (4)$$

Indeed, if we were to have

$$\frac{|A|^4 |D|^{2/3} |C(A+1)|^{1/3}}{|C|} < \frac{|C(A+1)|^3 |D|^2}{|C|}$$

then we may apply this bound in (3) and the result follows. Assuming (4), we have

$$|A|^8 |D|^4 \leq |C(A+1)|^8 |D|^4 \leq |A|^{12}.$$

So that  $|D| \leq |A|$ . In turn, this implies  $|A| \geq |D| \geq |C(A+1)| \geq |A|$ , so that  $|A| = |C(A+1)| = |D|$ . Returning to (3), this gives

$$E_4^*(A, D) \ll \frac{|A|^4 |D|^{2/3} |C(A+1)|^{1/3}}{|C|} \log |A| = \frac{|C(A+1)|^3 |D|^2}{|C|} \log |A|,$$

and the result is proved.  $\square$

*Proof of Theorem 8.* The proof follows similarly to that of Theorem 7. We again define the lines and points

$$L = \{l_{d,c} : d \in D, c \in C\}, \quad l_{d,c} \text{ given by } y = \frac{1}{d} \left( \frac{x}{c} - 1 \right), \quad P = C(A+1) \times S_\tau,$$

where in this case the set  $S_\tau$  is rich with respect to  $E^*(A, D)$ , so that

$$|S_\tau| \tau^2 \ll E^*(A, D) \ll |S_\tau| \tau^2 \log |A|.$$

With the conditions  $|A||C||D| \min\{|D|, |C|\} \ll p^2$  and  $|S_\tau| |C(A+1)| \max\{|S_\tau|, |C(A+1)|\} \leq |D|^3 |C|^3$  (which are satisfied under our assumptions), we have, by Theorem 6,

$$|S_\tau| \tau |C| \leq I(P, L) \ll |S_\tau|^{1/2} |C(A+1)|^{3/4} |D|^{3/4} |C|^{3/4} + |D||C|.$$

If the leading term dominates, we have

$$|S_\tau| \tau^2 \ll \frac{|C(A+1)|^{3/2} |D|^{3/2}}{|C|^{1/2}}$$

and the result follows from  $E^*(A, D)/\log |A| \ll |S_\tau| \tau^2$ . We therefore assume that the leading term does not dominate; that is,

$$|S_\tau|^{1/2} |C(A+1)|^{3/4} |D|^{3/4} |C|^{3/4} \leq |D||C|.$$



Multiplying through by  $\tau$  and squaring, we get the bound

$$E^*(A, D) \ll \frac{|D|^{1/2} |C|^{1/2} \tau^2}{|C(A+1)|^{3/2}} \log |A|. \quad (5)$$

Much as before, we may now assume the bound

$$\frac{|D|^{3/2} |C(A+1)|^{3/2}}{|C|^{1/2}} \leq \frac{|D|^{1/2} |C|^{1/2} \tau^2}{|C(A+1)|^{3/2}}, \quad (6)$$

as assuming otherwise yields the result via (5). The bound (6) then gives

$$|D| |C(A+1)|^3 \leq |C| \tau^2.$$

Bounding  $\tau \leq |A|$  and  $|C| |A|^2 \leq |C(A+1)|^3$ , we have  $|D| = 1$ . Similarly, bounding  $\tau^2 \leq |A| |D|$  and  $|C(A+1)|^3 \geq |C|^2 |A|$ , we find  $|C| = 1$ , so that the result is trivial.  $\square$

### 3. Proof of Theorem 3

We follow a multiplicative analogue of the argument in [Rudnev et al. 2018]. Without loss of generality we may assume  $A, B \subseteq \mathbb{F}^*$ . For some  $\delta > 0$ , define a popular set of products as

$$P := \left\{ x \in AB : r_{AB}(x) \geq \frac{|A||B|}{|AB|\delta} \right\}.$$

Let  $P^c := AB \setminus P$ . Note that by writing

$$|\{(a, b) \in A \times B : ab \in P\}| + |\{(a, b) \in A \times B : ab \in P^c\}| = |A||B|$$

and noting that

$$|\{(a, b) \in A \times B : ab \in P^c\}| < |P^c| \frac{|A||B|}{|AB|\delta} \leq \frac{|A||B|}{\delta},$$

we have

$$|\{(a, b) \in A \times B : ab \in P\}| \geq \left(1 - \frac{1}{\delta}\right) |A||B|.$$

We also define a popular subset of  $A$  with respect to  $P$  as

$$A' := \{a \in A : |\{b \in B : ab \in P\}| \geq \frac{2}{3} |B|\}.$$

We have

$$|\{(a, b) \in A \times B : ab \in P\}| = \sum_{a \in A'} |\{b : ab \in P\}| + \sum_{a \in A \setminus A'} |\{b : ab \in P\}| \geq \left(1 - \frac{1}{\delta}\right) |A||B|. \quad (7)$$

Suppose that  $|A \setminus A'| = c|A|$  for some  $c \geq 0$ , so that  $|A'| = (1 - c)|A|$ . Noting that

$$\sum_{a \in A'} |\{b : ab \in P\}| \leq (1 - c) |A||B|, \quad \sum_{a \in A \setminus A'} |\{b : ab \in P\}| \leq \frac{2c}{3} |A||B|,$$

we have by (7)

$$(1 - c) |A||B| + \frac{2c}{3} |A||B| \geq \left(1 - \frac{1}{\delta}\right) |A||B| \implies c \leq \frac{3}{\delta},$$

so that  $|A'| \geq (1 - 3/\delta) |A|$ .

We use a multiplicative version of Lemma 8 in [Rudnev et al. 2018]. The proof we present is an expanded version of the proof present in that paper.

**Lemma 9.** *For all finite  $A \subset \mathbb{F}$ , there exists  $A_1 \subseteq A$  with  $|A_1| \gg |A|$  such that*

$$E_{4/3}^*(A'_1) \gg E_{4/3}^*(A_1).$$

*Proof.* We give an algorithm which shows such a subset exists, as otherwise we have a contradiction. We recursively define

$$A_i = A'_{i-1}, \quad A_0 = A, \quad i \leq \log |A|,$$

where  $A'_i$  is defined relative to  $A_i$ . Using the same arguments as above, we have  $|A'_i| \geq (1 - 3/\delta)|A_i|$ . We shall set  $\delta = \log |A|$ . We have the chain of inequalities

$$|A_i| = |A'_{i-1}| \geq \left(1 - \frac{3}{\log |A|}\right) |A_{i-1}| \geq \cdots \geq \left(1 - \frac{3}{\log |A|}\right)^i |A|.$$

Note that assuming  $|A| \geq 16$  (if this is not true then the result is trivial), we have

$$\left(1 - \frac{3}{\log |A|}\right)^i \geq \left(1 - \frac{3}{\log |A|}\right)^{\log |A|} \geq \left(\frac{1}{4}\right)^4$$

since the function  $(1 - 3/z)^z$  is increasing for  $z > 3$ . We now have

$$|A_i| \geq \left(\frac{1}{4}\right)^4 |A| \gg |A|$$

at all steps  $i$ . We assume that at all steps, we have

$$E_{4/3}^*(A'_i) < \frac{E_{4/3}^*(A_i)}{4},$$

as otherwise we have  $E_{4/3}^*(A'_i) \gg E_{4/3}^*(A_i)$  and we are done. After  $\log |A|$  steps, we have a set  $A_k$  with

$$|A_k| \gg |A|, \quad E_{4/3}^*(A'_k) < \frac{E_{4/3}^*(k)}{4} < \frac{E_{4/3}^*(A_{k-1})}{16} < \cdots < \frac{E_{4/3}^*(A)}{4^{\log |A|}}.$$

But then we have

$$E_{4/3}^*(A) > E_{4/3}^*(A'_k) 4^{\log |A|} \gg |A|^{4/3+2} = |A|^{10/3},$$

which is a contradiction. Therefore at some step we have an  $A_i$  satisfying the lemma.  $\square$

We now return to the proof of Theorem 3, with  $\delta = \log |A|$  applied in the definition of  $P$ . We apply Lemma 9 to  $A$  to find a large subset  $A_1 \subset A$  with  $E_{4/3}^*(A'_1) \gg E_{4/3}^*(A_1)$ ,  $|A_1| \gg |A|$ . Noting that proving the result for  $A_1$  implies it for  $A$ , we shall rename  $A_1$  as  $A$  for simplicity.

We use a dyadic decomposition to find a set  $Q \subset A'/A'$  such that

$$|Q| \Delta^{4/3} \ll E_{4/3}^*(A') \ll |Q| \Delta^{4/3} \log |A|$$

for some  $\Delta > 0$ .

We will bound the size of the set

$$N = \left\{ (a, a', b, b') \in (A')^2 \times B^2 : \frac{a}{a'} \in Q, ab, ab', a'b, a'b' \in P \right\}.$$

By summing over all  $a, a' \in A'$  with  $a/a' \in Q$ , we have

$$|N| = \sum_{\substack{a, a' \in A' \\ a/a' \in Q}} |\{b \in B : ab, a'b \in P\}|^2$$

and we see that as  $|\{b \in B : ab \in P\}| \geq \frac{2}{3}|B|$  for all  $a \in A'$ , by considering the intersection of  $\{b \in B : ab \in P\}$  and  $\{b \in B : a'b \in P\}$ , we have  $|\{b \in B : ab, a'b \in P\}| \geq \frac{1}{3}|B|$  for all  $a, a' \in A'$ . Using that elements  $q \in Q$  have at least  $\Delta$  representations in  $A'/A'$ , we have  $|N| \geq \frac{1}{9}|B|^2|Q|\Delta$ .

We now find an upper bound on  $|N|$ . Define an equivalence relation on  $A^2 \times B^2$  via

$$(a, a', b, b') \sim (c, c', d, d') \iff \text{there exists } \lambda \text{ such that } a = \lambda c, a' = \lambda c', b = \frac{d}{\lambda}, b' = \frac{d'}{\lambda}.$$

Note that the conditions

$$\frac{a}{a'} \in Q, \quad ab, a'b, ab', a'b' \in P \tag{8}$$

are invariant in the class (i.e., if one class element satisfies these conditions, then they all do), as  $\lambda$  cancels in each condition. Let  $X$  denote the set of equivalence classes  $[a, a', b, b']$ , where the conditions (8) are satisfied. We can bound  $|N|$  by the sum of the size of each equivalence class  $[a, a', b, b']$  in  $X$ :

$$|N| \leq \sum_X |[a, a', b, b']|.$$

By the Cauchy–Schwarz inequality and completing the sum over all equivalence classes, we have

$$|Q|^2 \Delta^2 |B|^4 \ll |N|^2 \leq |X| \sum_{[a, a', b, b']} |[a, a', b, b']|^2. \tag{9}$$

We must now bound the two quantities on the right-hand side of this equation. We first claim that

$$\sum_{[a, a', b, b']} |[a, a', b, b']|^2 \leq \sum_x r_{A/A}(x)^2 r_{B/B}(x)^2. \tag{10}$$

To see this, note that the left-hand side of (10) counts pairs of elements of equivalence classes. Take any two elements  $(a, a', b, b'), (c, c', d, d') \in A^2 \times B^2$  from the same equivalence class. By definition, we may write  $(c, c', d, d') = (\lambda a, \lambda a', b/\lambda, b'/\lambda)$ . As  $0 \notin A, B$ , the 8-tuple  $(a, a', b, b', c, c', d, d')$  satisfies

$$\lambda = \frac{c}{a} = \frac{c'}{a'} = \frac{b}{d} = \frac{b'}{d'}$$

for some  $\lambda \in \mathbb{R}$ , and thus corresponds to a contribution to the quantity  $r_{A/A}(\lambda)^2 r_{B/B}(\lambda)^2$ , and thus also corresponds to a contribution to the sum  $\sum_x r_{A/A}(x)^2 r_{B/B}(x)^2$ . We also see that different pairs from equivalence classes necessarily give different 8-tuples, and so the claim is proved. We use Cauchy–Schwarz on the right-hand side of (10) to bound it by a product of fourth energies:

$$\sum_x r_{A/A}(x)^2 r_{B/B}(x)^2 \leq E_4^*(A)^{1/2} E_4^*(B)^{1/2}.$$

We use Theorem 7 to bound these energies. We bound via

$$E_4^*(A) \ll \frac{|C(A+1)|^2 |A|^3}{|C|} \log |A|, \quad E_4^*(B) \ll \frac{|D(B-1)|^2 |B|^3}{|D|} \log |B|,$$

with conditions

$$\begin{aligned} |C(A+1)||A| &\leq |C|^3, & |C(A+1)|^2 &\leq |A||C|^3, & |A|^3 |C| &\ll p^2, \\ |D(B-1)||B| &\leq |D|^3, & |D(B-1)|^2 &\leq |B||D|^3, & |B|^3 |D| &\ll p^2, \end{aligned}$$

which are all satisfied under our assumptions. Returning to (9), we now have

$$|Q|^2 \Delta^2 |B|^4 \ll |X| \frac{|C(A+1)||A|^{3/2} |D(B-1)||B|^{3/2}}{|C|^{1/2} |D|^{1/2}} (\log |A| \log |B|)^{1/2}. \quad (11)$$

We now bound  $|X|$ , the number of equivalence classes where the conditions (8) are satisfied. Note that any  $(a, a', b, b')$  belonging to an equivalence class in  $X$  maps to a solution of the equation

$$w = \frac{s}{t} = \frac{u}{v}, \quad (12)$$

with  $w \in Q$ ,  $s, t, u, v \in P$ , by taking  $w = a/a'$ ,  $s = ab$ ,  $t = a'b$ ,  $u = ab'$ ,  $v = a'b'$ . Note that taking two solutions  $(a, a', b, b')$  and  $(c, c', d, d')$  that are *not* from the same equivalence class necessarily gives us two different solutions to (12) via the map above. Therefore we may bound  $|X|$  by the number of solutions to (12).

$$|X| \leq \left| \left\{ (w, s, t, u, v) \in Q \times P^4 : w = \frac{s}{t} = \frac{u}{v} \right\} \right| = \left| \left\{ (s, t, u, v) \in P^4 : \frac{s}{t} = \frac{u}{v} \in Q \right\} \right|.$$

The popularity of  $P$  allows us to bound this by

$$|X| \leq \frac{|AB|^4 (\log |A|)^4}{|A|^4 |B|^4} \left| \left\{ (a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4) \in A^4 \times B^4 : \frac{a_1 b_1}{a_2 b_2} = \frac{a_3 b_3}{a_4 b_4} \in Q \right\} \right|.$$

We dyadically pigeonhole the set  $BA/A$  in relation to the number of solutions to  $r/a = r'/a' \in Q$ , with  $r, r' \in BA/A$ ,  $a, a' \in A$ , to find popular subsets  $R_1, R_2 \subseteq BA/A$  in terms of these solutions. We have

$$|X| \leq \frac{|AB|^4 (\log |A|)^4}{|A|^4 |B|^4} \sum_{i=1}^{2 \log |A|} \sum_{\substack{x \in AB/A \\ 2^i \leq r_{AB/A}(x) < 2^{i+1}}} r_{AB/A}(x) \left| \left\{ (a_3, a_4, b_1, b_3, b_4) \in A^2 \times B^3 : \frac{x}{b_1} = \frac{a_3 b_3}{a_4 a_4} \in Q \right\} \right|.$$

We use the pigeonhole principle to give us  $\Delta_1 > 0$  and  $R_1 \subseteq AB/A$  such that

$$|X| \ll \Delta_1 \frac{|AB|^4 (\log |A|)^5}{|A|^4 |B|^4} \left| \left\{ (r_1, a_3, a_4, b_2, b_3, b_4) \in R_1 \times A^2 \times B^3 : \frac{r_1}{b_2} = \frac{a_3 b_3}{a_4 b_4} \in Q \right\} \right|.$$

We perform a similar dyadic decomposition to get  $\Delta'_1 > 0$  and  $R_2 \subseteq AB/A$  such that

$$|X| \ll \Delta_1 \Delta'_1 \frac{|AB|^4 (\log |A|)^6}{|A|^4 |B|^4} \left| \left\{ (r_1, r_2, b_2, b_4) \in R_1 \times R_2 \times B^2 : \frac{r_1}{b_2} = \frac{r_2}{b_4} \in Q \right\} \right|.$$

These decompositions now allow us to bound via fourth energies, as follows:

$$\begin{aligned}
|X| &\ll \Delta_1 \Delta'_1 \frac{|AB|^4 (\log |A|)^6}{|A|^4 |B|^4} \left| \left\{ (r_1, r_2, b_2, b_4) \in R_1 \times R_2 \times B^2 : \frac{r_1}{b_2} = \frac{r_2}{b_4} \in Q \right\} \right| \\
&= \Delta_1 \Delta'_1 \frac{|AB|^4 (\log |A|)^6}{|A|^4 |B|^4} \sum_{q \in Q} r_{R_1/B}(q) r_{R_2/B}(q) \\
&\leq \Delta_1 \Delta'_1 \frac{|AB|^4 (\log |A|)^6}{|A|^4 |B|^4} \left( \sum_{q \in Q} r_{R_1/B}(q)^2 \right)^{1/2} \left( \sum_{q \in Q} r_{R_2/B}(q)^2 \right)^{1/2} \\
&\leq \Delta_1 \Delta'_1 |Q|^{1/2} \frac{|AB|^4 (\log |A|)^6}{|A|^4 |B|^4} E_4^*(B, R_1)^{1/4} E_4^*(B, R_2)^{1/4}, \tag{13}
\end{aligned}$$

where the third and fourth lines follow from applications of the Cauchy–Schwarz inequality. We will now show that given  $|B||D||R_i|^2 \ll p^2$  and  $|B| \leq |D|$  (which are true under our assumptions), we have

$$E_4^*(B, R_i) \ll \frac{|D(B-1)|^3 |R_i|^2}{|D|} \log |B|. \tag{14}$$

Firstly, with the additional conditions

$$|B|^2 |D(B-1)| \leq |R_i||D|^3, \quad |B||D(B-1)|^2 \leq |R_i|^2 |D|^3 \tag{15}$$

we may bound these fourth energies by Theorem 7 to get (14). We can therefore assume one of these conditions does not hold.

Firstly, suppose that  $|B|^2 |D(B-1)| > |R_i||D|^3$ . We will use the trivial bound

$$E_4^*(B, R_i) \leq |R_i|^4 |B|.$$

Note that it would be enough to prove

$$E_4^*(B, R_i) \leq \frac{|D(B-1)|^3 |R_i|^2}{|D|},$$

which would follow from

$$|R_i|^4 |B| \leq \frac{|D(B-1)|^3 |R_i|^2}{|D|}, \tag{16}$$

which is true if and only if  $|R_i|^2 |B||D| \leq |D(B-1)|^3$ . Using our assumed bound  $|B|^2 |D(B-1)| > |R_i||D|^3$ , we know

$$|R_i|^2 |B||D| < \frac{|B|^5 |D(B-1)|^2}{|D|^5}.$$

By the assumption  $|B| \leq |D|$ , we have

$$|R_i|^2 |B||D| < \frac{|B|^5 |D(B-1)|^2}{|D|^5} \leq |D(B-1)|^3,$$

and so by (16) the bound on the fourth energy holds.

Now assume the second condition from (15) does not hold; that is,  $|B||D(B-1)|^2 > |R_i|^2|D|^3$ . Again, we use the trivial bound

$$E_4^*(B, R_i) \leq |R_i|^4|B|.$$

We have

$$|R_i|^4|B| \leq \frac{|D(B-1)|^3|R_i|^2}{|D|} \iff |R_i|^2|B||D| \leq |D(B-1)|^3,$$

so it is enough to prove  $|R_i|^2|B||D| \leq |D(B-1)|^3$ , as before. Using the assumption  $|B||D(B-1)|^2 > |R_i|^2|D|^3$ , we have

$$|R_i|^2|B||D| < \frac{|B|^2|D(B-1)|^2}{|D|^2}$$

and it follows from our assumption  $|B| \leq |D|$  that

$$\frac{|B|^2|D(B-1)|^2}{|D|^2} \leq |D(B-1)|^3.$$

Therefore we have  $|R_i|^2|B||D| < |D(B-1)|^3$  and so the bound on the fourth energy holds. Returning to (13), we use (14) to bound  $|X|$  as

$$\begin{aligned} |X| &\ll \Delta_1 \Delta'_1 |Q|^{1/2} \frac{|AB|^4 (\log |A|)^6}{|A|^4 |B|^4} E_4^*(B, R_1)^{1/4} E_4^*(B, R_2)^{1/4} \\ &\ll \Delta_1 \Delta'_1 |R_1|^{1/2} |R_2|^{1/2} |Q|^{1/2} \frac{|AB|^4 |D(B-1)|^{3/2}}{|A|^4 |B|^4 |D|^{1/2}} (\log |A|)^6 (\log |B|)^{1/2}. \end{aligned} \quad (17)$$

As  $|R_i| \Delta_i \leq \sum_{x \in R_i} r_{BA/A}(x)$ , the product  $|R_1|^{1/2} |R_2|^{1/2} \Delta_1 \Delta'_1$  can be bounded by

$$|R_1|^{1/2} |R_2|^{1/2} \Delta_1 \Delta'_1 \leq \left( \sum_{x \in R_1} r_{BA/A}(x)^2 \sum_{x \in R_2} r_{BA/A}(x)^2 \right)^{1/2},$$

where it is important to note that  $r_{BA/A}(x)$  gives a triple  $(b, a, a')$ . For  $i = 1, 2$ , we have

$$\sum_{x \in R_i} r_{BA/A}(x)^2 \leq \left| \left\{ (a_1, a_2, a_3, a_4, b_1, b_2) \in A^4 \times B^2 : \frac{b_1 a_1}{a_2} = \frac{b_2 a_3}{a_4} \right\} \right|.$$

Following a similar dyadic decomposition as before, we find a pair of subsets  $S_1, S_2 \subseteq A/A$  with respect to these solutions, and some  $\Delta_2, \Delta'_2 > 0$  with

$$\begin{aligned} \sum_{x \in R_i} r_{BA/A}(x)^2 &\ll \Delta_2 \Delta'_2 (\log |A|)^2 |\{(s_1, s_2, b_1, b_2) \in S_1 \times S_2 \times B^2 : s_1 b_1 = s_2 b_2\}| \\ &\leq \Delta_2 \Delta'_2 (\log |A|)^2 \sum_x r_{S_1 B}(x) r_{S_2 B}(x) \\ &\leq \Delta_2 \Delta'_2 (\log |A|)^2 E^*(B, S_1)^{1/2} E^*(B, S_2)^{1/2}, \end{aligned}$$

where the third inequality is given by the Cauchy–Schwarz inequality. We will use an argument similar to that above to prove that with the two conditions  $|B||D||S_i| \min\{|D|, |S_i|\} \ll p^2$  and  $|B| \leq |D|$  (which

are satisfied under our assumptions), we have

$$E^*(B, S_i) \ll \frac{|S_i|^{3/2} |D(B-1)|^{3/2}}{|D|^{1/2}} \log |B|. \quad (18)$$

Under the extra conditions

$$|B|^2 |D(B-1)| \leq |S_i| |D|^3, \quad |B| |D(B-1)|^2 \leq |S_i|^2 |D|^3 \quad (19)$$

we can bound this energy by Theorem 8 to get (18). We therefore assume the first condition from (19) does not hold; that is,  $|B|^2 |D(B-1)| > |S_i| |D|^3$ . We bound the energy via the trivial estimate

$$E^*(B, S_i) \leq |B| |S_i|^2.$$

It is now enough to show that

$$|B| |S_i|^2 \leq \frac{|S_i|^{3/2} |D(B-1)|^{3/2}}{|D|^{1/2}}, \quad \text{which is true if and only if } |B| |D|^{1/2} |S_i|^{1/2} \leq |D(B-1)|^{3/2}.$$

Using our assumption  $|B|^2 |D(B-1)| > |S_i| |D|^3$ , we have

$$|B| |D|^{1/2} |S_i|^{1/2} < \frac{|B|^2 |D(B-1)|^{1/2}}{|D|}.$$

Our assumption that  $|B| \leq |D|$  then gives

$$\frac{|B|^2 |D(B-1)|^{1/2}}{|D|} \leq |B| |D(B-1)|^{1/2} \leq |D(B-1)|^{3/2},$$

so that  $|B| |D|^{1/2} |S_i|^{1/2} < |D(B-1)|^{3/2}$ , and the bound (18) holds. Next we assume that the second condition in (19) does not hold; that is,  $|B| |D(B-1)|^2 > |S_i|^2 |D|^3$ . We again use the trivial bound

$$E^*(B, S_i) \leq |B| |S_i|^2.$$

Comparing this to our desired bound, we have

$$|B| |S_i|^2 \leq \frac{|S_i|^{3/2} |D(B-1)|^{3/2}}{|D|^{1/2}} \iff |B| |D|^{1/2} |S_i|^{1/2} \leq |D(B-1)|^{3/2},$$

so that the desired bound would follow from the second inequality above. Using our assumption that  $|B| |D(B-1)|^2 > |S_i|^2 |D|^3$ , we know

$$|B| |D|^{1/2} |S_i|^{1/2} < \frac{|B|^{5/4} |D(B-1)|^{1/2}}{|D|^{1/4}},$$

and by our assumption that  $|B| \leq |D|$ , we have

$$\frac{|B|^{5/4} |D(B-1)|^{1/2}}{|D|^{1/4}} \leq |D(B-1)|^{3/2},$$

so that we have  $|B| |D|^{1/2} |S_i|^{1/2} < |D(B-1)|^{3/2}$  as needed.

In all cases the bound on  $E^*(B, S_i)$  holds, so that we find

$$\begin{aligned} [|R_1|^{1/2}|R_2|^{1/2}\Delta_1\Delta'_1]^2 &\ll \Delta_2^2\Delta_2'^2 E^*(B, S_1)E^*(B, S_2)(\log |A|)^4 \\ &\ll \frac{\Delta_2^2\Delta_2'^2 |S_1|^{3/2}|S_2|^{3/2}|D(B-1)|^3}{|D|}(\log |A|)^4(\log |B|)^2 \\ &\leq \frac{E_{4/3}^*(A)^3 |D(B-1)|^3}{|D|}(\log |A|)^4(\log |B|)^2, \end{aligned}$$

where the final inequality follows as  $\Delta_2$  and  $\Delta'_2$  correspond to representations of elements of  $S_1$  and  $S_2$  in  $A/A$ , so that

$$|S_1|^{3/2}\Delta_2^2 = (|S_1|\Delta_2^{4/3})^{3/2} \leq \left(\sum_x r_{A/A}(x)^{4/3}\right)^{3/2} \leq E_{4/3}^*(A)^{3/2},$$

and similarly for  $S_2$ . Combining the bounds (11), (17), and the above, we have

$$|Q|^{3/2}\Delta^2|B|^{13/2}|A|^{5/2}|D|^{3/2}|C|^{1/2} \ll |AB|^4|C(A+1)||D(B-1)|^4 E_{4/3}^*(A)^{3/2}(\log |A|)^{17/2}(\log |B|)^2,$$

which simplifies to

$$E_{4/3}^*(A')^3|B|^{13}|A|^5|D|^3|C| \ll |AB|^8|C(A+1)|^2|D(B-1)|^8 E_{4/3}^*(A)^3(\log |A|)^{17}(\log |B|)^4.$$

We know by Lemma 9 that  $E_{4/3}(A') \gg E_{4/3}(A)$ , so we have

$$|B|^{13}|A|^5|D|^3|C| \ll |AB|^8|C(A+1)|^2|D(B-1)|^8(\log |A|)^{17}(\log |B|)^4$$

as needed. □

### Acknowledgements

The author was supported by the Austrian Science Fund (FWF) Project P 30405-N32. The author would also like to thank Oliver Roche-Newton and Misha Rudnev for helpful conversations. I would also like to thank the anonymous referee for several helpful comments.

### References

- [Chen et al. 2018] C. Chen, B. Kerr, and A. Mohammadi, “A new sum-product estimate in prime fields”, preprint, 2018. [arXiv](#)
- [Garaev and Shen 2010] M. Z. Garaev and C.-Y. Shen, “On the size of the set  $A(A+1)$ ”, *Math. Z.* **265**:1 (2010), 125–132. [MR](#) [Zbl](#)
- [Jones and Roche-Newton 2013] T. G. F. Jones and O. Roche-Newton, “Improved bounds on the set  $A(A+1)$ ”, *J. Combin. Theory Ser. A* **120**:3 (2013), 515–526. [MR](#) [Zbl](#)
- [Konyagin and Shkredov 2015] S. V. Konyagin and I. D. Shkredov, “On sum sets of sets having small product set”, *Tr. Mat. Inst. Steklova* **290** (2015), 304–316. In Russian; translated in *Proc. Steklov Inst. Math.* **290**:1 (2015), 288–299. [MR](#) [Zbl](#)
- [Mohammadi 2018] A. Mohammadi, “On growth of the set  $A(A+1)$  in arbitrary finite fields”, preprint, 2018. [arXiv](#)
- [Roche-Newton et al. 2016] O. Roche-Newton, M. Rudnev, and I. D. Shkredov, “New sum-product type estimates over finite fields”, *Adv. Math.* **293** (2016), 589–605. [MR](#) [Zbl](#)
- [Rudnev 2018] M. Rudnev, “On the number of incidences between points and planes in three dimensions”, *Combinatorica* **38**:1 (2018), 219–254. [MR](#) [Zbl](#)



- [Rudnev et al. 2018] M. Rudnev, G. Shakan, and I. Shkredov, “Stronger sum-product inequalities for small sets”, preprint, 2018. arXiv
- [Shakan 2018] G. Shakan, “On higher energy decompositions and the sum-product phenomenon”, *Math. Proc. Cambridge Philos. Soc.* (online publication July 2018).
- [Shakan and Shkredov 2018] G. Shakan and I. D. Shkredov, “Breaking the  $6/5$  threshold for sums and products modulo a prime”, preprint, 2018. arXiv
- [Solymosi 2009] J. Solymosi, “Bounding multiplicative energy by the sumset”, *Adv. Math.* **222**:2 (2009), 402–408. MR Zbl
- [Stevens and de Zeeuw 2017] S. Stevens and F. de Zeeuw, “An improved point-line incidence bound over arbitrary fields”, *Bull. Lond. Math. Soc.* **49**:5 (2017), 842–858. MR Zbl
- [Zhelezov 2015] D. Zhelezov, “On additive shifts of multiplicative almost-subgroups in finite fields”, preprint, 2015. arXiv

Received 6 Dec 2018. Revised 30 Apr 2019.

AUDIE WARREN:

audie.warren@oeaw.ac.at

Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria

