© 2019 George Shakan

THE SUM-PRODUCT PROBLEM

BY

GEORGE SHAKAN

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2019

Urbana, Illinois

Doctoral Committee:

Professor Alexandru Zaharescu, Chair
Professor Kevin Ford, Director of Research
Professor József Balogh
Professor Burak Erdoğan

ABSTRACT

The sum-product problem of Erdős and Szemerédi asserts that any subset of the integers has many products or many sums. We explore quantitative aspects of the problem over both the real numbers and finite fields of prime order.

To my grandmother, who passed away while I was a PhD student.

ACKNOWLEDGMENTS

I would first like to thank my advisor, Kevin Ford. He played the role as an advisor I could count on. He allowed me a certain freedom to explore as I desired, and provided key advice that certainly shaped my career for the better.

Next I would like to thank the rest of my committee, József Balogh, Burak Erdoğan, and Alexandru Zaharescu for all putting up with my onslaught of questions in the classroom and then inviting me to work with them on joint projects.

I am forever indebted to Antal Balog, for his encouragement and support early in my career.

I benefitted in my early years at UIUC from the support of the vast graduate department. Because of this, I was able to maintain broader interests than I would have otherwise. I could write pages on the numerous personal and memorable experiences from dozens of students. To name just one, Chris Gartland inspired me, in more ways than one, to develop my analytic background. This permeates through all my work to this day and I am certain it will continue to do so.

Lastly, I would like to acknowledge Alex Dunn, whose friendship and timely advice greatly enriched my life during my time as a PhD student.

PREFACE

I was fortunate enough to have the choice of which results to include in my thesis. On the other hand, these results lie in unrelated areas and make it rather challenging to incorporate into a single unifying file. Instead, I chose to only include my two works on the sum–product problem, which were a natural choice for a thesis. The work over the real numbers is solo, while the work over finite fields is joint with Misha Rudnev and Ilya Shkredov.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Let $A, B \subset \mathbb{R}$ be finite. We define the *sumset* and *product set* via

$$A + B := \{a + b : a \in A,\ b \in B\}, \qquad AB := \{ab : a \in A,\ b \in B\}.$$

The main sum–product conjecture of Erdős and Szmerédi [1] reads as follows.

Conjecture 1 (Sum–product Conjecture)**.** *Fix $\epsilon > 0$. For any $A \subset \mathbb{Z}$ finite and sufficiently large in size, we have*

$$\max\{|A + A|, |AA|\} \geq |A|^{2-\epsilon}.$$

Note that Conjecture 1 is true for arithmetic progressions, since the product set is large. Similarly, Conjecture 1 its true for geometric progressions, since the sumset is large. Conjecture 1 is a quantitative analog of the fact that $\mathbb{Z}$ has no nontrivial finite subrings.

Conjecture 1 has a long and rich history which we outline in more Chapter 2, but here we take time to outline some key ideas. Erdős and Szemerédi themselves proved that Conjecture 1 holds for some $\epsilon < 1$. It was Elekes who first realized the connection of the sum–product conjecture and incidence geometry. In a beautiful two page paper [2] he made progress towards Conjecture 1 and highlighted a certain dictionary that has played a vital role since. His key observation was that a set, A, with few products and few sums induces a point–line incidence structure with many incidences. This is evident as the points $(A + A) \times (AA)$ and lines $y = a(x - c)$ for $a, c \in A$ have $|A|^3$ incidences of the form $(b + c, ab), y = a(x - c))$.

In mathematics, it is very useful to have a dictionary between seemingly unrelated subjects (i.e. the Nullstellensatz), and indeed the present case is no different. On the one hand, we can use ideas from incidence geometry to prove sum-product theorems. This allows us to incorporate powerful tools such as the polynomial method.

On the other hand, Conjecture 1 comes from the area of additive combinatorics [3]. A part of this subject is concerned with understanding various properties of the sumset. For instance, in what general situations can we guarantee the sumset is large? One such example is if the set is large dimensional [3, Chapter 5], then the sumset must be large. More relevant is that if the product set is small, then the sumset is large [4].

Before Konyagin and Shkredov [5], there had not been a way to incorporate techniques from additive combinatorics in conjunction with incidence geometry to attack Conjecture 1. They were able to incorporate the theory of higher order energies, largely developed by Shkredov [6]. We will get into the technical details later, but we give a brief overview here. It is common to study the additive energy, that is solutions to

$$a + b = c + d, \quad a, b, c, d \in A.$$

It turns out the additive energy is an ℓ^2 estimate for the convolution of 1_A with itself and thus makes the theory easier. Higher order energies involve higher moments, for instance the number of solutions to

$$a + b = c + d = e + f, \quad a, b, c, d, e, f \in A.$$

This turns out to be more subtle to study. One tool is the spectral theorem from linear algebra. In Chapter 2 we further develop this study. We formulate a conjecture that would yield significant progress towards Conjecture 1 and make some headway ourselves.

There is a version of Conjecture 1 over finite fields. For instance, we have the following conjecture.

Conjecture 2 (Finite Field Sum–Product)**.** *Let $A \subset \mathbb{F}_p$ of size $\leq p^{1/2}$. Then for all $\epsilon > 0$,*

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

We do not have growth in the sumset or product set if $A = \mathbb{F}_p$ so some smallness condition must be present in such a conjecture. Again, Conjecture 2 is a quantitative analog of the fact that $\mathbb{F}_p$ has no nontrivial subfields.

In [7], they made the first progress towards Conjecture 1, essentially establishing Conjecture 2 for some $\epsilon < 1$. It turns out that the finite field sum–product problem has applications to several other areas of math and computer science, some of which

were outlined in their original paper (indeed applications to Kakeya-type problems were the original motivation in [7]).

In Chapter 3, we incorporate the tools from higher order energies to make progress towards Conjecture 2. This was originally inspired by unpublished work of Shkredov and myself and that work was the first time the theory of higher order energies made an appearance in Conjecture 2. We utilized some techniques from [8] and incorporated them into the state of the art incidence bound over $\mathbb{F}_p$ [9].

CHAPTER 2

SUM-PRODUCT OVER THE REAL NUMBERS

2.1 Introduction

Let $A, B \subset \mathbb{R}$ be finite. We define the *sumset* and *product set* via

$$A + B := \{a + b : a \in A,\ b \in B\}, \qquad AB := \{ab : a \in A,\ b \in B\}.$$

In this paper, we say $b \gtrsim a$ if $a = O(b \log^c |A|)$ for some $c > 0$ and $a \sim b$ if $b \gtrsim a$ and $a \gtrsim b$. Equipped with these definitions we are ready to state the Erdős–Szemerédi sum–product conjecture.

Conjecture 3. *[1] Fix $\delta \leq 1$. Then for any finite $A \subset \mathbb{Z}$, one has*

$$|A + A| + |AA| \gtrsim |A|^{1+\delta}.$$

In the same paper, Erdős and Szemerédi showed that Conjecture 33 holds for some $\delta > 0$, which began the history of the so called "sum–product conjecture." Fourteen years passed until Nathanson [10] modified their proof and made the first quantitative estimate, showing Conjecture 33 holds for $\delta = 1/31$. Ford [11] quickly improved Nathanson's argument to obtain $\delta = 1/15$ is admissible in Conjecture 33. Ford did not have this world record for long, as within months Elekes [2] showed Conjecture 33 holds for $\delta = 1/4$. Elekes' techniques were completely different, as he remarkably made use of the Szemerédi–Trotter theorem from incidence geometry. His work marks the beginning of modern progress towards resolving Conjecture 33.

Solymosi [12] showed $\delta = 3/11$ is admissible in Conjecture 33. Later, in [13] he used elementary geometry in a clever way to improve this to $\delta = 1/3$. This remained the world record for six years, until Konyagin and Shkredov [5] combined Solymosi's argument with Shkredov's work in additive combinatorics [6, 14] to increase Solymosi's exponent. In a more recent paper [15], the same authors proved $\delta = 1/3 + 5/9813$

is admissible in Conjecture 33. Rudnev, Shkredov and Stevens [16] replaced a "few sums many products" lemma used in [15] to obtain the world record that Conjecture 33 holds for $\delta = 1/3 + 1/1509$. We make further improvements to show the following.

Theorem 4. *Let $A \subset \mathbb{R}$ be finite. Then*

$$|AA| + |A + A| \gtrsim |A|^{4/3+5/5277}.$$

Thus we improve Solymosi's exponent by nearly $\frac{1}{1000}$. We remark that Theorem 4 also holds if one replaces the product set with the quotient set.

We now turn our attention to decomposition results, which is the main motivation for the current work. About 35 years after the original sum–product conjecture, Balog and Wooley [17] provided a new way of looking at the problem of intrinsic interest and applicable (see [18] for the first application). To state their results, we recall some definitions. Again, let $A, B \subset \mathbb{R}$ be finite. We define two representation functions of $x \in \mathbb{R}$:

$$r_{A-B}(x) = \#\{(a,b) \in A \times B : x = a - b\}, \qquad r_{A/B}(x) = \#\{(a,b) \in A \times B : a = xb\}.$$

The *additive energy* and *multiplicative energy* of A and B are defined via

$$E^+(A,B) = \sum_x r_{A-B}(x)^2, \qquad E^\times(A,B) = \sum_x r_{A/B}(x)^2.$$

We set $E^+(A) = E^+(A,A)$ and $E^\times(A) = E^\times(A,A)$. Heuristically, $E^+(A)$ is large when A has additive structure. This is seen more clearly by the relation

$$E^+(A) = \#\{(a,b,c,,d) \in A^4 : a + b = c + d\}.$$

Theorem 5. *[17] Let A be a finite subset of the real numbers and $\delta = 2/33$. Then there exist B, C that partition A satisfying*

$$\max\{E^+(B), E^\times(C)\} \lesssim |A|^{3-\delta}, \qquad \max\{E^+(B,C), E^\times(B,C)\} \lesssim |A|^{3-\delta/2}.$$

Thus any set may be decomposed into two sets, one with little additive structure and one with little multiplicative structure. Note that Theorem 5 with exponent δ implies Conjecture 33 with exponent δ, via Cauchy–Schwarz:

$$|A|^2|B|^2 \leq |A+B|E^+(A,B), \qquad |A|^2|B|^2 \leq |AB|E^\times(A,B).$$

This is the so called "energy analog" of the sum–product problem. In the same paper Balog and Wooley provided the example

$$\{(2m-1)2^j : 1 \leq m \leq S, 1 \leq j \leq P\}, \tag{2.1}$$

which shows, when $S = P^2$, it is not possible to improve Theorem 5 beyond $\delta = 2/3$.

Balog and Wooley use an iterative argument to combine two key lemmas and prove Theorem 5. The first is a rather easy lemma concerning how the multiplicative energy behaves with respect to unions. The second is at the heart of the proof, which says if the additive energy is large, then there is a large subset that has small multiplicative energy. To accomplish this, they utilized Solymosi's [13] sum–product result as well as the Balog–Szemerédi–Gowers theorem from additive combinatorics. Konyagin and Shkredov [15] replaced this lemma with a completely different lemma of their own that allowed them to show $\delta = 1/5$ is admissible in Theorem 5. This lemma is what inspired the current work. Finally Rudnev, Shkredov, and Stevens [16] improved this to $\delta = 1/4$, which is the energy analog of Elekes' result towards Conjecture 33. We improve this to $\delta = 7/26$ below. To fully state our contribution, we require a few more definitions.

We now introduce the third order energies of a set:

$$E_3^+(A,B) = \sum_x r_{A-B}(x)^3, \qquad E_3^\times(A,B) = \sum_x r_{A/B}(x)^3.$$

We set $E_3^+(A) = E_3^+(A,A)$ and $E_3^\times(A) = E_3^\times(A,A)$.

We first provide motivation for working with higher moments. It starts with the Szemerédi–Trotter theorem, which has played a pivotal role in the sum–product problem since [2] (see chapter 8 of [3]).

Theorem 6. *[Szemerédi–Trotter] Let P be a finite set of points and L be a finite set of lines. Then the number of incidences between P and L is bounded from above:*

$$\#\{(p,\ell) \in P \times L : p \in \ell\} \leq 4|P|^{2/3}|L|^{2/3} + 4|P| + |L|.$$

Elekes' result can be recovered by applying Theorem 6 to $P = (A+A) \times AA$ and $L = \{y = a(x-c) : a, c \in A\}$. Now, for an arbitrary point set, P, if we apply

Szemerédi–Trotter to the set of Δ–popular lines and P, we can simplify to obtain

$$|L| \lesssim \max\{|P|^2\Delta^{-3}, |P|\Delta^{-1}\}.$$

Typically the first term is larger (for instance if $P = A \times A$), and so we see that Szemerédi–Trotter is most naturally a *third* moment estimate.

At the forefront of a number of works concerning the sum–product phenomenon, i.e. [5, 15, 16, 19, 8, 20], is the quantity $d^+(A)$.

Definition 7. *Let $A \subset \mathbb{R}$ finite. We define*

$$d^+(A) := \sup_{B\neq\emptyset} \frac{E_3^+(A,B)}{|A||B|^2},$$

and the multiplicative analog

$$d^\times(A) := \sup_{B\neq\emptyset} \frac{E_3^\times(A,B)}{|A||B|^2}.$$

It follows that $1 \leq d^+(A), d^\times(A) \leq |A|$. Intuitively, the closer $d^+(A)$ is to $|A|$, the more additive structure A has and the closer $d^\times(A)$ is to $|A|$, the more multiplicative structure A has. Observe that the supremums in Definition 7 are achieved for some $|B| \leq |A|^2$ since

$$\frac{E_3^+(A,B)}{|A||B|^2} \leq \frac{|A|^2}{|B|}, \quad \frac{E_3^\times(A,B)}{|A||B|^2} \leq \frac{|A|^2}{|B|}.$$

Remark 8. *We have that $d^+(A) \sim \widetilde{d}^+(A)$, where $\widetilde{d}^+(A)$ is the smallest quantity such that*

$$\#\{x : r_{A-B}(x) \geq \tau\} \leq \widetilde{d}^+(A)|A||B|^2\tau^{-3},$$

holds for all finite $B \subset \mathbb{R}$ and $\tau \geq 1$ [20, Lemma 17]. Indeed by Chebyshev's inequality, $\widetilde{d}^+(A) \leq d^+(A)$ since

$$\#\{x : r_{A-B}(x) \geq \tau\} \leq \tau^{-3}\sum_x r_{A-B}(x)^3 \leq \frac{E_3^+(A,B)}{|A||B|^2}|A||B|^2\tau^{-3}.$$

The reverse inequality follows, up to a logarithm, from a dyadic decomposition

$$\frac{E_3^+(A,B)}{|A||B|^2} \sim \frac{1}{|A||B|^2}\max_{1\leq\tau\leq|A|} \#\{x : \tau \leq r_{A-B}(x) < 2\tau\}\tau^3 \leq \widetilde{d}^+(A).$$

In previous literature, $\widetilde{d}^+(A)$ been taken as the definition of $d^+(A)$. Finally, we remark that $d^+(A)$ is related to the following operator norm

$$d^+(A) = \frac{1}{|A|}||T_A||^3_{\ell^{3/2}\to\ell^3}, \quad T_A(f) := \sum_x f(x)1_A(y+x).$$

Thus the quantity $d^+(A)$ arises from thinking of A as an operator *rather than a* set*.*

The quantities $d^+(A)$ and $d^\times(A)$ can be thought of as a ℓ^3 estimate for r_{A-B} and $r_{A/B}$, where we are allowed to vary B. This flexibility in choosing B has proved useful in applications.

Example 9. *Consider a random $A \subset \{1,\dots,n\}$ where each element is chosen independently and uniformly with probability $p > n^{-1/3}$. Clearly $|A| \sim pn$ with high probability. Let $B = \{1,\dots,n\}$. It follows from Chernoff's inequality (for instance, Chapter 1 of [3]) and the union bound, that every x with $r_{B-B}(x) \geq p^{-2}\log n$ satisfies*

$$r_{A-B}(x) \sim p \cdot r_{B-B}(x), \qquad r_{A-A}(x) \sim p^2 \cdot r_{B-B}(x).$$

This quickly implies

$$\frac{E_3^+(A,B)}{|A||B|^2} \sim p|A|, \quad \frac{E_3^+(A)}{|A|^3} \sim p^2|A|, \quad \frac{E^+(A,B)}{|A||B|} \sim |A|, \quad \frac{E^+(A)}{|A|^2} \sim p|A|.$$

In this example $d^+(A)$ is larger than what is predicted by the third order energy, where we only allow $B = A$ in Definition 7. Furthermore, the analog of Definition 7 for additive energy is as large as possible, that is $\gtrsim |A|$; however, using more involved techniques one can show $d^+(A) \sim p|A|$. Thus the trivial bounds

$$\frac{E_3^+(A)}{|A|^3} \leq d^+(A) \leq \max_{B\neq\emptyset} \frac{E^+(A,B)}{|A||B|},$$

are not tight in general.

Sumset and product set information can be deduced from upper bounds for $d^+(A)$ and $d^\times(A)$, respectively. For instance, a simple application of Cauchy–Schwarz and Definition 7 applied to $B = A$ reveal

$$\frac{|A|^4}{|A+A|} \leq E^+(A) \leq E_3^+(A)^{1/2}\left(\sum_x r_{A-A}(x)\right)^{1/2} \lesssim d^+(A)^{1/2}|A|^{5/2}. \tag{2.2}$$

Thus we find that using this argument, one can only show $|A+A| \gtrsim |A|^{3/2}$, even with optimal information for $d^+(A)$. Improvements have been made to (2.2), which highlights the advantage of allowing B to vary in Definition 7.

Theorem 10. *[[6, Theorem 11] , [21, Corollary 10], see also [8], [19, Theorem 13], see also [14]] Let $A \subset \mathbb{R}$. Then*

$$|A+A| \gtrsim |A|^{58/37} d^+(A)^{-21/37}, \quad |A-A| \gtrsim |A|^{8/5} d^+(A)^{-3/5}, \quad E^+(A) \lesssim d^+(A)^{\frac{7}{13}} |A|^{\frac{32}{13}}.$$

The multiplicative versions of these bounds all hold by applying the additive version to the bigger of $\log\{a \in A : a > 0\}$ and $\log -\{a \in A : a < 0\}$. Thus one basic strategy in several sum–product improvements is as follows: use Szemerédi–Trotter to obtain a third moment estimate and then use Theorem 10 to get improved sum–product bounds. The strength of such theorems can be accurately tested by setting $d^+(A) = 1$. Thus the result for difference sets is slightly stronger than that of sumsets and both are stronger than what we can say about the more general additive energy. Quantitative improvements to Theorem 10 would improve all of our main theorems.

Remark 11. *Suppose that one was able to improve upon Theorem 10 to*

$$|A+A| \gtrsim |A|^2 d^+(A)^{-1}.$$

Then, combining this with the multiplicative version:

$$|AA| \gtrsim |A|^2 d^\times(A)^{-1},$$

and applying Theorem 12 below, we would have the sum–product estimate

$$|A+A||AA| \gtrsim |A|^3.$$

With this viewpoint, the obstacle to further improvements of Conjecture 33 is our current individual understanding of "sum" and "product," rather than the combination of the two. The question is how much second moment information can be extracted from third moment information.

Information about $d^+(A)$ and $d^\times(A)$ can be used in conjunction with Theorem 10 to obtain bounds for sum–product problems. Our next theorem shows that these two quantities are related.

Theorem 12. *Let $A \subset \mathbb{R}$ be finite. Then there exists $X, Y \subset A$ such that*

(i) $X \cup Y = A$,

(ii) $|X|, |Y| \geq |A|/2$,

(iii) $d^+(X)d^\times(Y) \lesssim |A|$.

This is optimal, as can be seen by taking A to be an arithmetic or geometric progression. We point out that the sets X and Y in Theorem 12 have the convenient property that they are both of size at least $|A|/2$, which has not always been the case with decomposition results; this type of result first appeared in [16, Theorem 12]. Theorem 12 can be interpreted as a $d^+, d^\times$ analog of Elekes' [2] sum–product bound, in light of (2.2). Since Theorem 10 is better than (2.2), we can go beyond this Elekes threshold, answering a question in [16].

Theorem 13. *Let $A \subset \mathbb{R}$ be finite and $\delta = 1/4$. Then there exist B, C that partition A with*

$$\max\{d^+(B), d^\times(C)\} \lesssim |A|^{1-2\delta}.$$

Furthermore,

$$\max\{E^+(B), E^\times(C)\} \lesssim |A|^{3-\frac{14}{13}\delta}, \quad \max\{E^+(B,A), E^\times(C,A)\} \lesssim |A|^{3-\delta}.$$

This improves upon [20, Theorem 4] as well as [16, Theorem 1] and builds upon the work found there. Note that in the last inequality we have a δ in place of a $\delta/2$. While Theorem 12 is optimal, we do not expect Theorem 13 to be optimal. This lies at the heart of the sum–product phenomenon. With current technology, we are unable to fully rule out the possibility of a set with partial additive and multiplicative structure. Note the example above in (2.1) shows that one cannot prove $2\delta > 3/4$, as explained in [20].

We now mention more applications of Theorem 12. First, we consider the difference–quotient and difference–product problems. For $A \subset \mathbb{R}$, we set

$$A^{-1} = \{a^{-1} : a \in A\},$$

where we adopt the convention that $0^{-1} = 0$.

Conjecture 14. *Let $\delta \leq 1$. Then for any finite $A \subset \mathbb{R}$, one has*

$$|A-A| + |AA^{-1}| \gtrsim |A|^{1+\delta},$$

$$|A-A| + |AA| \gtrsim |A|^{1+\delta}.$$

Solymosi's [13] techniques do not work for difference sets, but Elekes' [2] do which shows that Conjecture 14 holds for $\delta = 1/4$. Solymosi's earlier work [12] implies that $\delta = 3/11$ is admissible in Conjecture 14. Konyagin and Rudnev [21] adapted techniques from [8] to show the first statement of Conjecture 14 holds for $\delta = 1 + 9/31$ and the second statement holds for $\delta = 1 + 11/39$. Using Theorem 12, we improve their results.

Theorem 15. *Let $A \subset \mathbb{R}$ be finite. Then*

$$|A-A| + |AA^{-1}| \gtrsim |A|^{1+3/10},$$

$$|A-A| + |AA| \gtrsim |A|^{1+7/24}$$

In a similar spirit to the sum–product phenomenon, there are a host of "expander problems," for instance [22, 23, 19, 24, 25]. They roughly state that when one creates a set by combining addition and multiplication, the resulting set should be large. For instance, it is of interest to find the best lower bounds for

$$|AA \pm A|, \ |AA \pm AA|, \ |A(A \pm A)|, \ \max_{a \in A} |A(A \pm a)|.$$

Typically what happens is that one can apply Szemerédi–Trotter to obtain a lower bound of the order of magnitude of $|A|^{3/2}$ (see chapter 8 of [3]) and improving upon this takes additional ideas that usually depend of the structure of the expander (see for instance [23, 19, 25]). The problem of $AA + A$ is unique in that it has resisted improvements from Szemerédi–Trotter (see [24]), until a very recent preprint of Roche–Newton, Ruzsa, Shen, and Shkredov [25]. Typically expanders are conjectured to have size $\gtrsim |A|^2$, but we are usually far from proving so.

We use Theorem 12 to improve upon the lower bound for the expanders found in [19]. Our idea is to use their techniques to the subsets of A appearing in Theorem 12 which have more suitable additive and multiplicative structure.

Theorem 16. *Let $A \subset \mathbb{R}$ be finite. Then*

$$|A(A-A)| \gtrsim |A|^{3/2+7/226},$$

$$|A(A+A)| \gtrsim |A|^{3/2+1/46},$$

$$\max_{a\in A} |A(A\pm a)| \gtrsim |A|^{3/2+1/182}.$$

Note that Solymosi's technique in [13] is better suited for sumsets, while Shkredov's and his coauthors techniques (as in Theorem 10) are better suited for difference sets. This subtlety is not at the heart of the sum–product phenomenon, so we mention the following theorem which we will prove during the proof of Theorem 4.

Theorem 17. *Let $A \subset \mathbb{R}$ be finite. Then*

$$|A+A| + |A-A| + |AA| + |AA^{-1}| \gtrsim |A|^{4/3+1/753}.$$

The work in this paper builds directly upon the works in [17, 2, 21, 19, 16, 8, 6, 20, 14, 13]. It is worth noting that there are orthogonal works addressing the sum–product phenomenon. Chang [4] and Bourgain and Chang [26] have developed interesting techniques from harmonic analysis. See Croot and Hart [27] and the references within for another perspective of the problem.

2.2 Main decomposition result

We recall that the proof of Theorem 5 [17] required two ingredients: a way to say if A has additive structure then there is a large subset without multiplicative structure and a simple lemma to understand how multiplicative energy interacts with unions. They then concluded the proof with an iterative argument. We adopt a similar strategy and begin with the former. To begin, we need another definition.

Definition 18. *We define the quantity $D^{\times}(A)$ to be the infimum of*

$$|Q|^2|R|^2|A|^{-1}t^{-3},$$

such that

$$A \subset \{x : r_{Q/R}(x) \geq t\}, \quad 1 \leq t \leq |Q|^{1/2}|R||A|^{-1/2}, \quad |R| \leq |Q|.$$

We similarly define $D^{+}(A)$ to be the infimum of $|Q|^2|R|^2|A|^{-1}t^{-3}$ such that

$$A \subset \{x : r_{Q-R}(x) \geq t\}, \quad 1 \leq t \leq |Q|^{1/2}|R||A|^{-1/2}, \quad |R| \leq |Q|.$$

Thus $D^\times(A)$ is small if we can efficiently place A into a set of popular quotients. The admittedly strange quantity $|Q|^2|R|^2|A|^{-1}t^{-3}$ is chosen in light of (2.4) below. To understand $D^\times(A)$ a bit better, note that taking $Q = AB$, $R = B$ and $t = |B|$ for any B finite, nonempty and not containing zero, one finds

$$D^\times(A) \leq \frac{|AB|^2}{|A||B|}. \tag{2.3}$$

Thus $D^\times(A) \leq |A|$ ($|B| = 1$) and is smaller when $|AA|$ is significantly smaller than $|A|^{3/2}$.

The sole reason for introducing these quantities is the following proposition that relates $D^\times(A)$ to $d^+(A)$, as defined in Definition 7.

Proposition 19 (Lemma 13 in [15])**.** *Let $A \subset \mathbb{R}$ be finite. Then*

$$d^+(A) \lesssim D^\times(A), \tag{2.4}$$

$$d^\times(A) \lesssim D^+(A).$$

In [15], they had a slightly different definition of $D^+(A), D^\times(A)$, replacing the condition $t \lesssim |Q|^{1/2}|R||A|^{-1/2}$ with $|A| \leq |Q|$. The condition we impose is weaker, but the proof of (2.4) works line for line as in [15, Lemma 13].

To better understand (2.4), one can check that (2.2), (2.3) and (2.4) together imply Elekes' [2] bound $|A|^{5/2} \lesssim |AA||A + A|$.

We briefly summarize the proof of (2.4) as it plays a crucial role in what lies below. Consider the following sets of points and lines:

$$P = Q \times \{x : r_{A-B}(x) \geq \tau\}, \quad L = \{y = \frac{x}{r} - b : r \in R,\ b \in B\}.$$

The number of incidences is at least

$$t\tau\#\{x : r_{A-B}(x) \geq \tau\}.$$

Then (2.4) follows from applying Theorem 6 (Szemerédi–Trotter) and a modest calculation. Thus $D^\times(A)$ allows us to efficiently transform the equation $y = a - b$ into $y = \frac{q}{r} - b$ which is better suited for Szemerédi–Trotter.

There has been a variety of notational choices for these quantities, but we made our choice for the reason that we wanted the quantity with a capital letter to be larger

than the one with a lower case letter. Note that (2.4) is the only thing we use that relates addition and multiplication and what follows is massaging this inequality for our purposes. We remark that a symmetric version of the following lemma holds with the roles of d^+ and $d^\times$ reversed.

Lemma 20. *Let $T \subset \mathbb{R}$ be a finite, nonempty set. Then there exists a nonempty $A' \subset T$ such that*

$$d^\times(T)d^+(A') \lesssim \frac{|A'|^2}{|T|}, \qquad |A'| \gtrsim d^\times(T).$$

If one had that $A' = T$, then Lemma 20 would immediately imply Theorem 12, but this is unfortunately too strong to hope for. We first sketch the main idea of the proof. If $d^\times(T)$ is large, then there is a large subset $A' \subset T$ with small $D^\times(A')$. This is believable as both quantities are defined via multiplication. Then we finish by applying (2.4) to turn this into additive information about A'.

Proof. By Definition 7 of $d^\times(T)$, there is a nonempty $B \subset \mathbb{R}$ such that

$$d^\times(T) \sim \frac{E_3^\times(T,B)}{|T||B|^2}.$$

Then by the definition of $E_3^\times(T,B)$ and a dyadic decomposition, there exists a $\Delta \geq 1$ such that

$$E_3^\times(T,B) \sim |P|\Delta^3, \quad P = \{x : \Delta \leq r_{T/B}(x) \leq 2\Delta\}.$$

By another dyadic decomposition, there $q \geq 1$ such that

$$|P|\Delta \sim \sum_{x\in P} r_{T/B}(x) = \sum_{a\in T} r_{B/P^{-1}}(a) \sim |A'|q, \quad A' = \{a' \in T : q \leq r_{B/P^{-1}}(a') \leq 2q\}.$$

From Definition 18, we then have

$$D^\times(A') \lesssim |B|^2|P|^2q^{-3}|A'|^{-1},$$

provided that

$$q \lesssim |A'|^{-1/2}\max\{|P|,|B|\}^{1/2}\min\{|P|,|B|\}.$$

Since $|A'|q \sim \Delta|P|$, it is enough to verify

$$|P|\Delta q \lesssim \max\{|P|,|B|\}\min\{|P|,|B|\}^2.$$

This follows from $\Delta \leq |B|$ and $q \leq \min\{|B|, |P|\}$. Then by (2.4), we find

$$d^+(A') \lesssim D^\times(A') \lesssim |B|^2|P|^2q^{-3}|A'|^{-1} \lesssim |B|^2|A'|^2\Delta^{-3}|P|^{-1} \lesssim \frac{|A'|^2}{d^\times(T)|T|}.$$

For the second inequality, we use $\Delta^2 q \leq |T||B|^2$ to obtain

$$|A'| \gtrsim |P|\Delta q^{-1} \sim E_3^\times(T,B)q^{-1}\Delta^{-2} \gtrsim d^\times(T).$$

□

The referee observed that Lemma 20 is in a similar spirit to the Balog–Szemerédi–Gowers theorem [3, Theorem 2.29] geared towards the sum–product problem (one should consider $d^\times(A) \geq |A|K^{-1}$ for some small $K \geq 1$). The difference is instead of concluding a large susbet with small product set as in Balog–Szemerédi–Gowers, we conclude the weaker condition that there is a large subset with no additive structure. Lemma 20 is quantitatively better since we are able to incorporate both addition and multiplication.

We now move onto the easier "union lemma." We remark that we avoid an application of Hölder's inequality, which appears in [20].

Lemma 21. *Let $A_1, \dots, A_K \subset \mathbb{R}$ be finite and disjoint. Then*

$$d^+(\bigcup_{j=1}^K A_j) \leq |\bigcup_{j=1}^K A_j|^{-1} \left(\sum_{j=1}^K d^+(A_j)^{1/3}|A_j|^{1/3}\right)^3.$$

Similarly,

$$d^\times(\bigcup_{j=1}^K A_j) \leq |\bigcup_{j=1}^K A_j|^{-1} \left(\sum_{j=1}^K d^\times(A_j)^{1/3}|A_j|^{1/3}\right)^3.$$

Proof. Let $B \subset \mathbb{R}$ be arbitrary and finite. Then by disjointness and the triangle inequality in $\ell^3(\mathbb{Z})$, we have

$$\begin{aligned} E_3^+(\bigcup_{j=1}^K A_j, B)^{1/3} &= \left(\sum_x r_{\bigcup_{j=1}^K A_j - B}(x)^3\right)^{1/3} = \left(\sum_x \left(\sum_{j=1}^K r_{A_j-B}(x)\right)^3\right)^{1/3} \\ &\leq \sum_{j=1}^K \left(\sum_x r_{A_j-B}(x)^3\right)^{1/3} = \sum_{j=1}^K E_3^+(A_j,B)^{1/3}. \end{aligned}$$

Recall Definition 7

$$d^+(A) = \sup_{B \neq \emptyset} \frac{E_3^+(A,B)}{|A||B|^2}.$$

Since B was arbitrary, we may take the B that maximizes the left hand side of the above equation, after dividing by $|B|^{2/3}$, and use $E_3^+(A_j, B) \leq d^+(A_j)|A_j||B|^2$ on the right hand side to finish the proof. The proof of the second statement follows line by line to that of the first. □

We now iterate Lemma 20 and prove Theorem 12. Set $A_0 = \emptyset$ and suppose that $A_0, A_1, \ldots, A_{j-1}$ have been defined. Put $T = A \setminus (A_0 \cup \ldots \cup A_{j-1})$ and define A_j via Lemma 20 as a nonempty set $A_j \subset T$ such that

$$d^\times(T) d^+(A_j) \lesssim |A_j|^2 |T|^{-1}.$$

We continue this process until

$$|A_1 \cup \ldots \cup A_K| \geq |A|/2.$$

This process must terminate for some finite $K \leq |A|/2$ since the A_j are nonempty and disjoint. Set $Y = A \setminus (A_1 \cup \cdots \cup A_{K-1})$ and $X = A_1 \cup \cdots \cup A_K$. It is clear that $|X| \geq |A|/2$ and $|Y| \geq |A|/2$, otherwise the process would have stopped at step $K-1$. By Lemma 20 and the monotonicity of $|A|d^\times(A)$, for $1 \leq j \leq K$,

$$|Y| d^\times(Y) d^+(A_j) \leq |A \setminus (A_1 \cup \cdots \cup A_{j-1})| d^\times(A \setminus (A_1 \cup \cdots \cup A_{j-1})) d^+(A_j) \lesssim |A_j|^2.$$

Combining with Lemma 21, we have

$$\begin{aligned} d^+(\bigcup_{j=1}^K A_j) &\leq |\bigcup_{j=1}^K A_j|^{-1} \left(\sum_{j=1}^K d^+(A_j)^{1/3} |A_j|^{1/3} \right)^3 \\ &\lesssim |X|^{-1} \left(\sum_{j=1}^K |A_j| \right)^3 |Y|^{-1} d^\times(Y)^{-1} \lesssim |X|^2 |A|^{-1} d^\times(Y)^{-1}. \end{aligned}$$

Theorem 12 follows from $|X| \leq |A|$.

2.3 Difference–quotient estimate and Balog–Wooley decomposition

We start with Theorem 15. It follows from this stronger proposition.

Proposition 22. *Let $A \subset \mathbb{R}$. Then*

$$|A-A||AA^{-1}| \gtrsim |A|^{13/5},$$

$$|A-A|^{35}|AA|^{37} \gtrsim |A|^{93}.$$

Proof. By Theorem 12, there exist $X, Y \subset A$ such that $|X|, |Y| \geq |A|/2$ and

$$d^+(X)d^\times(Y) \lesssim |A|.$$

By the second statement of Theorem 10,

$$d^+(X) \gtrsim |X|^{8/3}|X-X|^{-5/3}, \qquad d^\times(Y) \gtrsim |Y|^{8/3}|YY^{-1}|^{-5/3}.$$

Combining these, we get

$$\frac{|A|^{16/3}}{|A-A|^{5/3}|AA^{-1}|^{5/3}} \lesssim \frac{|X|^{8/3}|Y|^{8/3}}{|X-X|^{5/3}|YY^{-1}|^{5/3}} \lesssim |A|.$$

The only difference in the proof of the second statement is we use the first statement of Theorem 10 in the form

$$d^\times(Y) \gtrsim |Y|^{58/21}|YY|^{-37/21},$$

in place of $d^\times(Y) \gtrsim |Y|^{8/3}|YY^{-1}|^{-5/3}$.

□

We now prove Theorem 13, which we restate for the reader's convenience.

Theorem 13. *Let $A \subset \mathbb{R}$ be finite and $\delta = 1/4$. Then there exist B, C that partition A with*

$$\max\{d^+(B), d^\times(C)\} \lesssim |A|^{1-2\delta}.$$

Furthermore,

$$\max\{E^+(B), E^\times(C)\} \lesssim |A|^{3-\frac{14}{13}\delta}, \quad \max\{E^+(B,A), E^\times(C,A)\} \lesssim |A|^{3-\delta}.$$

The proof can be summarized as iterating Theorem 12 at most logarithmically many times, and then applying the third statement of Theorem 10 for the first inequality and Cauchy–Schwarz for the second.

Proof. By Theorem 12, there exists A_1 such that $|A_1| \geq |A|/2$ and $d^+(A_1) \lesssim |A|^{1/2}$ or $d^\times(A_1) \lesssim |A|^{1/2}$. Similarly, suppose $A_1, \dots, A_{K-1}$ are defined. Then by Theorem 12, there exists $A_K \subset A \setminus (A_1 \cup \dots \cup A_{K-1})$ such that $|A_K| \geq |A \setminus (A_1 \cup \dots \cup A_{K-1})|/2$ and $d^+(A_K) \lesssim |A|^{1/2}$ or $d^\times(A_K) \lesssim |A|^{1/2}$.

Continue this process until $|A_K| \leq |A|^{1/2}$, since then we trivially have that $d^+(A_K) \leq |A|^{1/2}$. By size considerations, this process will terminate in $\leq \log |A|$ steps.

Let $S \subset \{1, \dots, K\}$ be the set of indices j such that $d^+(A_j) \lesssim |A|^{1/2}$ and P be the remaining indices and set

$$B = \bigcup_{j \in S} A_j, \qquad C = \bigcup_{j \in P} A_j.$$

Then by Lemma 21 and Hölder's inequality, since $|S| \leq \log |A|$ and $d^+(A_j) \lesssim |A|^{1/2}$, we find

$$\begin{aligned} d^+(B) = d^+(\underset{j\in S}{\cup} A_j) &\lesssim |\underset{j\in S}{\cup} A_j|^{-1} \left(\sum_{j \in S} |A_j|^{1/3} d^+(A_j)^{1/3} \right)^3 \\ &\lesssim |\underset{j\in S}{\cup} A_j|^{-1} \sum_{j \in S} |A_j| d^+(A_j) \lesssim |A|^{1/2}. \end{aligned}$$

Similarly $d^\times(C) \lesssim |A|^{1/2}$.

To conclude the first inequality in the second statement, note by the third inequality of Theorem 10, we have

$$E^+(B) \lesssim d^+(B)^{\frac{7}{13}} |B|^{\frac{32}{13}} \lesssim |A|^{3-7/26},$$

and similarly $E^\times(C) \lesssim |A|^{3-7/26}$.

For the second inequality in the second statement, we apply Cauchy–Schwarz to

obtain

$$\begin{aligned} E^+(B,A) &\leq E_3^+(B,A)^{1/2}\left(\sum_x r_{A-B}(x)\right)^{1/2} \\ &\leq (d^+(B)|B||A|^2)^{1/2}(|A||B|)^{1/2} \\ &\lesssim |A|^{1/4}|A|^{5/2}. \end{aligned}$$

Similarly $E^\times(C,A) \lesssim |A|^{11/4}$. □

2.4 Expander inequalities

We use Theorem 12 and the techniques of [19] to establish the three inequalities of Theorem 16. We first recall the two lemmas from their paper that we use.

Lemma 23. *[[19, Lemma 8]] Let $A, B \subset \mathbb{R}$ be finite and nonempty such that $|A| \sim |B|$. Then there exists $b \in B$ such that*

$$|A|^6 \lesssim |A(A+b)|^2 E^\times(A).$$

Lemma 24. *[[19, Lemma 11]] Let $A \subset \mathbb{R}$ be finite and nonempty. Then for all nonzero $\alpha \in \mathbb{R}$,*

$$E^\times(A)^2 \lesssim |A(A+\alpha)||A|^{\frac{58}{13}} d^+(A)^{\frac{7}{13}}.$$

Note that the authors only claim Lemma 3.9 with $D^\times(A)$ in place of $d^+(A)$ which is weaker in light of (2.4). The bound we claim follows from the same proof, which the authors mention immediately following their proof of Lemma 3.9.

Proof of Theorem 16. Observe that Lemma 3.8 is good when the multiplicative energy of A is small and Lemma 3.9 is good when the multiplicative energy of A is large. We now plan to estimate

$$\max_{a\in A} |A(A \pm a)|, |A(A \pm A)|.$$

We can start all three proofs in the same way.

Lemma 25. *Let $A \subset \mathbb{R}$ be finite and nonempty. Then there exist $a, b \in A$ such that*

$$|A|^{46/13} \lesssim |A(A+a)|^2 d^\times(A)^{7/13},$$

$$|A|^{46/13} \lesssim |A(A-b)|^2 d^{\times}(A)^{7/13}.$$

Suppose further that $|A(A+a)| \leq r|A|^{3/2}$ *for all* $a \in A$. *Then there is an* $X \subset A$ *of size at least* $|A|/2$ *such that*

$$d^+(X) \lesssim r^{26/7}.$$

Proof. By Lemma 3.8, there is an $a \in A$ such that $|A|^6 \lesssim |A(A \pm a)|^2 E^{\times}(A)$. Combining this with the third inequality of Theorem 10 and simplifying yields the first statement of the lemma. To obtain the second statement, let X and Y be as given by Theorem 12. To finish, apply the first statement to Y, use $d^+(X)d^{\times}(Y) \lesssim |A|$, and simplify. □

Now we investigate each expander separately.

(i)$[A(A-A), A(A+A)]$ Suppose $|A(A \pm A)| \leq r|A|^{3/2}$. Since $A(A \pm a) \subset A(A \pm A)$ for all $a \in A$, we may apply Lemma 25 to obtain a set $X \subset A$ of size at least $|A|/2$ such that $d^+(X) \lesssim r^{26/7}$. Now, using $|A(A \pm A)| \geq |X \pm X|$ along with the first statement of Theorem 10 in the plus case and the second statement of Theorem 10 in the minus case and simplifying gives $r \gtrsim |A|^{1/46}$ and $r \gtrsim |A|^{7/226}$, respectively.

(ii)$[A(A \pm a)]$ Suppose

$$\max_{a \in A} |A(A \pm a)| \leq r|A|^{3/2}.$$

By Lemma 25, there is an $X \subset A$ of size at least $|A|/2$ such that $d^+(X) \leq r^{26/7}$. On the other hand, by Lemma 3.8 and Lemma 3.9,

$$|A|^3 \lesssim E^{\times}(X) r^2, \quad E^{\times}(X)^2 \lesssim r|A|^{3/2+58/13} d^+(X)^{7/13}.$$

Combining these and using $d^+(X) \lesssim r^{26/7}$ yields $r \gtrsim |A|^{1/182}$. □

2.5 Sum–product estimate

We now proceed to prove Theorem 4. The proof set–up is the same as in [5, 15], which we now discuss. Let $A \subset \mathbb{R}$ be finite. Konyagin and Shkredov start with the geometric approach of Solymosi [13], and can improve upon it unless $A_\lambda := A \cap \lambda A$ has additive structure for many choices of λ. They then prove an energy analog of a "few sums, many products" result in [28] and use it to conclude that $|A_\lambda A_\lambda|$ is almost as big as possible. It turns out that these sets are relatively small ($\approx |A|^{2/3}$) and this does not immediately improve Solymosi's [13] exponent of 1/3 in Conjecture 33. Konyagin and

Shkredov then use Katz–Koester [29] inclusion, that is

$$A_\lambda A_\lambda \subset AA \cap \lambda AA,$$

as well as (2.4) and the first inequality of Theorem 10, to also give an improvement in this case. In what remains, we quantitatively improve part of the argument and provide the entirety of the proof of [15] to see how our new pieces fit in.

The "few sums, many products" lemma was improved recently in [16]. We interpret this improvement as a fourth order energy estimate which allows us to more efficiently apply the lemma. The work in [16] relied on bounding the number of solutions to

$$\frac{p+b}{q+c} = \frac{p'+b'}{q'+c'}, \quad p,q,p',q' \in P, \quad b,c,b',c' \in B,$$

which was addressed [19] while studying the expanders from Theorem 16. It turns out, much like Szemerédi–Trotter is naturally a third moment estimate, their lemma is naturally a fourth moment estimate.

We use fourth order energy for the first time in the sum–product problem and define

$$E_4^+(A,B) = \sum_x r_{A-B}(x)^4, \qquad E_4^\times(A,B) = \sum_x r_{A/B}(x)^4.$$

Similar to $d^+(A)$ as in Definition 7, we define $d_4^+(A)$.

Definition 26. *Let $A \subset \mathbb{R}$ be finite. Then we define $d_4^+(A)$ via*

$$d_4^+(A) := \sup_{B \neq \emptyset} \frac{E_4^+(A,B)}{|A||B|^3}.$$

It is easy to see that one has $1 \leq d_4^+(A) \leq |A|$ and in fact we have $d_4^+(A) \leq d^+(A)$. So $d_4^+(A)$ is the fourth moment analog of $d^+(A)$. Note that the supremum in Definition 26 is obtained for some $|B| \leq |A|^{3/2}$, since

$$\frac{E_4^+(A,B)}{|A||B|^3} \leq \frac{|A|^3}{|B|^2}.$$

Similar to Remark 8, we relate $d_4^+(A)$ to an operator norm.

Remark 27. *Consider the linear operator, as in Remark 8,*

$$T_A(f) := \sum_x 1_A(x) f(y+x). \tag{2.5}$$

Then

$$d_4^+(A) = \frac{1}{|A|}||T_A||^4_{\ell^{4/3}\to\ell^4}, \quad d^+(A) = \frac{1}{|A|}||T_A||^3_{\ell^{3/2}\to\ell^3}.$$

It is easy to see that

$$||T_A||_{\ell_1\to\ell_\infty} = |A|, \quad |A|^{1/2} \le ||T_A||_{\ell_2\to\ell_2} \le |A|.$$

A bound of the form

$$||T_A||_{\ell_2\to\ell_2} \lesssim |A|^{1/2},$$

together with interpolation with $\ell_1 \to \ell_\infty$ implies $d_4^+(A) \le d^+(A) \lesssim 1$. Thus $\ell_2 \to \ell_2$ estimates are stronger, but higher moments are flexible to work with, as in Theorem 12 above and Proposition 30 below.

We now need the following quantity, which plays an important role in the Konyagin–Shkredov argument.

Definition 28. *Let $A, B, C \subset \mathbb{R}$ be finite and define*

$$\sigma(A,B,C) := \sup_{\sigma_1,\sigma_2,\sigma_3\neq 0} \#\{(a,b,c) \in A\times B\times C : \sigma_1 a + \sigma_2 b + \sigma_3 c = 0\}.$$

We have the trivial bound $\sigma(A,B,C) \le |A||B|$ and this is basically obtained when $A, B, C = \{1,\dots,n\}$. We expect that $\sigma(A,B,C)$ is small whenever A, B, or C has little additive structure. Konyagin and Shkredov [15] used that

$$\sigma(A,B,C) \le |A|^{1/2} E^+(B)^{1/4} E^+(C)^{1/4},$$

which we replace with the following.

Proposition 29. *Let $A, B, C \subset \mathbb{R}$ be finite. Then*

$$\sigma(A,B,C) \le |C|^{3/4} \left(d_4^+(A)|A||B|^3\right)^{1/4}$$

Proof. The proof is similar to what appears in [30] for third order energy. Fix $\sigma_1, \sigma_2, \sigma_3 \neq 0$. Then by Hölder's inequality, we obtain

$$\begin{aligned}\#\{(a,b,c)\in A\times B\times C : \sigma_1 a+\sigma_2 b+\sigma_3 c=0\} &= \sum_{c\in C}\#\{(a,b)\in A\times B : \sigma_1 a+\sigma_2 b=-\sigma_3 c\}\\ &\leq |C|^{3/4}\left(\sum_{c\in C}\#\{(a,b)\in A\times B : \sigma_1 a+\sigma_2 b=-\sigma_3 c\}^4\right)^{1/4}\\ &\leq |C|^{3/4}\left(\sum_{x}\#\{(a,b)\in A\times B : a+\sigma_2/\sigma_1 b=x\}^4\right)^{1/4}\\ &\leq |C|^{3/4}\left(d_4^+(A)|A||B|^3\right)^{1/4}.\end{aligned}$$

The proposition follows as $\sigma_1,\sigma_2,\sigma_3$ were arbitrary. □

The next lemma is a fourth order energy analog of [16, Theorem 12].

Proposition 30. *Let $A\subset\mathbb{R}$ be finite. Then there exists $X,Y\subset A$ such that*

(i) $X\cup Y=A$,

(ii) $|X|,|Y|\geq |A|/2$,

(iii) $d_4^+(X)E^\times(Y)\lesssim |A|^3$.

Proposition 30 is a "few sums, many products" theorem. Indeed, if $d_4^+(X)\gtrsim |A|$, then $E^\times(Y)\lesssim |A|^2$ and so by Cauchy–Schwarz,

$$|AA|\geq |YY|\gtrsim |Y|^2.$$

We begin the proof of Proposition 30 with the following lemma. We mention that there is a large overlap of the proof of Theorem 12 and Proposition 30, which are both decomposition results.

Lemma 31. *Let $A\subset\mathbb{R}$ be finite. Then there exists a nonempty $A'\subset A$ such that*

$$E^\times(A')d_4^+(A)\lesssim \frac{|A'|^4}{|A|},\quad |A'|\gtrsim d_4^+(A).$$

Note that if A' were equal to A then Proposition 30 would immediately follow, but this is too strong to hope for.

Proof. Let $B \subset \mathbb{R}$ be finite and nonempty. By a dyadic decomposition, there is a $\Delta \geq 1$ such that

$$E_4^+(A,B) \sim |P|\Delta^4, \quad P = \{x : \Delta \leq r_{A-B}(x) \leq 2\Delta\}.$$

We double count the number of solutions to

$$\frac{p+b}{q+c} = \frac{p'+b'}{q'+c'}, \quad p,q,p',q' \in P, \quad b,c,b',c' \in B. \tag{2.6}$$

By a claim in the proof of [19, Lemma 2.5], one has that the number of solutions to (2.6) is $\lesssim |P|^3|B|^3$.

By a dyadic decomposition, there is a $q \geq 1$ such that

$$|A'|q \sim \sum_{a\in A} r_{P+B}(a) \sim \sum_{x\in P} r_{A-B}(x) \sim \Delta|P|, \quad A' = \{a' \in A : q \leq r_{B+P}(a') < 2q\}.$$

Given

$$\frac{a_1}{a_2} = \frac{a_3}{a_4}, \qquad a_1,a_2,a_3,a_4 \in A',$$

we may create a solution to (2.6), via

$$\frac{a_1-b_1+b_1}{a_2-b_2+b_2} = \frac{a_3-b_3+b_3}{a_4-b_4+b_4}, \qquad b_1,b_2,b_3,b_4 \in B,$$

as long as $a_j - b_j \in P$ for all j. Since each $a_j \in A'$, there are at least q such choices for each b_j. Thus $q^4E^\times(A')$ is $\lesssim$ the number of solutions to (2.6), and so

$$E^\times(A') \sim \frac{|B|^3|P|^3}{q^4} \sim \frac{|A'|^4|B|^3}{|P|\Delta^4} \sim \frac{|A'|^4|B|^3}{E_4^+(A,B)}.$$

Finally, using $\Delta \leq |B|$ and $q \leq |A|$, we have

$$|A'| \gtrsim |P|\Delta q^{-1} \gtrsim E_4^+(A,B)|A|^{-1}|B|^{-3}.$$

The lemma now follows from Definition 26 of $d_4^+(A)$ since B is arbitrary. □

We also need the following lemma describing how $E^\times(A)$ behaves with respect to unions. The lemma will require the following application of Cauchy–Schwarz

$$E^\times(A,B)^2 \leq E^\times(A)E^\times(B). \tag{2.7}$$

Lemma 32. *Let $A_1, \dots, A_K \subset \mathbb{R}$ be finite and disjoint. Then*

$$E^\times(\bigcup_{j=1}^K A_j) \leq \left(\sum_{j=1}^K E^\times(A_j)^{1/4} \right)^4$$

Proof. By the triangle inequality in $\ell^2(\mathbb{Z})$, we have

$$\begin{aligned} E^\times(\bigcup_{j=1}^K A_j)^{1/2} &= \left(\sum_x r_{\bigcup_{j=1}^K A_j / \bigcup_{k=1}^K A_k}(x)^2 \right)^{1/2} = \left(\sum_x \left(\sum_{j,k=1}^K r_{A_j/A_k}(x) \right)^2 \right)^{1/2} \\ &\leq \sum_{j,k=1}^K \left(\sum_x r_{A_j/A_k}(x)^2 \right)^{1/2} = \sum_{j,k=1}^K E^\times(A_j, A_k)^{1/2} \end{aligned}$$

Now we apply (2.7) to obtain

$$\sum_{j,k=1}^K E^\times(A_j, A_k)^{1/2} \leq \sum_{j,k=1}^K E^\times(A_j)^{1/4} E^\times(A_k)^{1/4} = \left(\sum_{j=1}^K E^\times(A_j)^{1/4} \right)^2.$$

Combining these two inequalities completes the proof. □

We now iterate Lemma 31 and prove Proposition 30.

Proof of Proposition 30. Set $A_0 = \emptyset$ and suppose that $A_0, A_1, \dots, A_{j-1}$ have been defined. We define A_j via Lemma 31 as a nonempty set $A_j \subset A \setminus (A_0 \cup \dots \cup A_{j-1})$ such that

$$d_4^+(A \setminus (A_0 \cup \dots \cup A_{j-1})) E^\times(A_j) \lesssim |A_j|^4 |A \setminus (A_0 \cup \dots \cup A_{j-1})|^{-1}.$$

We continue this process until

$$|A_1 \cup \dots \cup A_K| \geq |A|/2.$$

This process must terminate for some $K \leq |A|/2$ as the A_j are nonempty and disjoint.

Set $X = A \setminus (A_1 \cup \dots \cup A_{K-1})$ and $Y = A_1 \cup \dots \cup A_K$. It is clear that $|Y| \geq |A|/2$ and $|X| \geq |A|/2$, otherwise the process would have stopped at step $K-1$. By Lemma 31, for $1 \leq j \leq K$,

$$d_4^+(X) E^\times(A_j) \leq d_4^+(A \setminus (A_1 \cup \dots \cup A_{j-1})) E^\times(A_j) \lesssim |A_j|^4 |A \setminus (A_1 \cup \dots \cup A_{j-1})|^{-1} \lesssim |A_j|^4 |A|^{-1}.$$

Combining this with Lemma 32, we obtain

$$E^\times(Y) = E^\times(\bigcup_{j=1}^K A_j) \leq \left(\sum_{j=1}^K E^\times(A_j)^{1/4}\right)^4$$
$$\lesssim \frac{1}{d_4^+(X)|A|}\left(\sum_{j=1}^K |A_j|\right)^4 \leq |Y|^3 d_4^+(X)^{-1}.$$

Proposition 30 follows from $|Y| \leq |A|$.

□

We now give the proof of Theorem 4, which is identical to that in [15] with some minor changes to utilize Proposition 29 and Proposition 30.

Proof of Theorem 4. Suppose that $|A+A|, |AA| \leq r|A|^{4/3}$. Thus our goal is to show

$$r \gtrsim |A|^{5/5277}.$$

Note that by Cauchy–Schwarz, $|AA| \leq r|A|^{4/3}$ implies

$$E^\times(A) \geq |A|^{8/3} r^{-1}. \tag{2.8}$$

By a dyadic decomposition, there exists a

$$t \geq E^\times(A)|A|^{-2} \geq |A|^{2/3} r^{-1},$$

such that

$$E^\times(A) \sim |S_t| t^2, \quad S_t = \{\lambda : r_{A/A}(\lambda) \sim t\}.$$

For $\lambda \in A/A$, we set

$$A_\lambda = A \cap \lambda A.$$

Thus $|A_\lambda| = r_{A/A}(\lambda)$. By Konyagin–Shkredov clustering [15] (see also Adam Sheffer's blog [31, Equation 9] or my blog [32]), which is a refinement of Solymosi's [13] argument, we have

$$|A+A|^2 \gtrsim \frac{|S_t|}{M}\left(M^2 t^2 - M^4 \max_{\lambda_1,\lambda_2,\lambda_3 \in S_t} \sigma(A_{\lambda_1}, A_{\lambda_2}, A_{\lambda_3})\right), \tag{2.9}$$

as long as $2 \leq M \leq |S_t|/2$. We apply Proposition 29 to obtain

$$|A+A|^2 \gtrsim \frac{|S_t|}{M}\left(M^2t^2 - M^4t^{7/4}\max_{\lambda\in S_t} d_4^+(A_\lambda)^{1/4}\right).$$

Set

$$M^2 := \frac{t^{1/4}}{2\max_{\lambda\in S_t} d_4^+(A_\lambda)^{1/4}}.$$

Now, we have $M \leq |S_t|/2$, since otherwise, using $d^+(A_\lambda) \geq 1$,

$$|A|^{4-4/3}r^{-1} \leq E^\times(A) \sim |S_t|t^2 \lesssim Mt^2 \lesssim t^{17/8} \leq |A|^{17/8} \leq |A|^{2+1/3},$$

and so $r \gtrsim |A|^{1/3}$. Also, if $M \geq 2$, then we may apply (2.9) to obtain

$$ME^\times(A) \lesssim |A+A|^2,$$

which implies $M \lesssim r^3$. Note that Solymosi originally proved $E^\times(A) \lesssim |A+A|^2$. We can improve unless M is very small.

Thus we just have to handle the hardest case: $M \lesssim r^3$, that is

$$\frac{t}{r^{24}} \leq d_4^+(A).$$

By a technical trick in [15], this implies for all $\lambda \in S_t$ (as opposed to maximum in λ), that

$$\frac{t}{r^{24}} \lesssim d_4^+(A_\lambda). \tag{2.10}$$

Indeed, we may partition $S_t = S_t' \cup S_t''$ where $d_4^+(A_{\lambda'}) \leq d_4^+(A_{\lambda''})$ for $\lambda' \in S_t'$ and $\lambda'' \in S_t''$. Then we apply the above argument to S_t' and see that (2.10) holds for all the elements in S_t''. Then we may replace S_t with S_t'' at the loss of just a constant. Note that (2.10) implies that $d_4^+(A_\lambda)$ is almost as large as possible and each A_λ has a lot of additive structure.

After passing to large subsets of A_λ and applying Proposition 30, we have

$$E^\times(A_\lambda) \lesssim t^2r^{24}, \quad \lambda \in S_t,$$

and by Cauchy–Schwarz we find

$$\frac{t^2}{r^{24}} \lesssim |A_\lambda A_\lambda|, \quad \lambda \in S_t.$$

Thus each A_λ has almost no multiplicative structure. By Katz–Koester inclusion [29], we have $A_\lambda A_\lambda \subset AA \cap \lambda AA$ and so

$$S_t \subset \{x : r_{AA/AA}(x) \gtrsim t^2 r^{-24}\}.$$

One issue is that S_t is a subset of AA^{-1} and not A. By a popularity argument, since

$$|S_t|t \leq \sum_{\lambda \in S_t} |A \cap \lambda A| = \sum_{a \in A} |A \cap aS_t|,$$

there is an $a \in A$ such that

$$A' = aS_t \cap A \subset \{x : r_{aAA/AA}(x) \gtrsim t^2 r^{-24}\}, \quad |A'| \gtrsim |S_t|t|A|^{-1}.$$

Thus by (2.4), we find

$$d^+(A') \leq D^\times(A') \lesssim \frac{|AA|^4 r^{72}}{|A'|t^6}.$$

We now apply the first statement of Theorem 10 (To prove Theorem 17, one should apply the second statement of Theorem 10 in place of the first) and first use that $|A'| \gtrsim |S_t|t|A|^{-1}$ and $|S_t|t^2 \sim E^\times(A)$ to obtain

$$|A+A|^{37} \geq |A'+A'|^{37} \gtrsim \frac{E^\times(A)^{79} t^{47}}{|AA|^{84}|A|^{79} r^{1512}}.$$

We now apply $t \gtrsim E^\times(A)|A|^{-2}$ and then (2.8) to find

$$|A|^{331} \lesssim r^{1512}|A+A|^{37}|AA|^{210}.$$

Theorem 4 then follows from $|AA|, |A+A| \leq r|A|^{4/3}$ and simplification. □

CHAPTER 3

SUM-PRODUCT OVER A PRIME FIELD

3.1 Introduction and results

Let F be a field with the multiplicative group F^*. Throughout we assume that F has characteristic $p > 0$, the most important case being $F = \mathbb{F}_p$ for large p. If $p = 0$, constraints in terms of p appearing throughout should be disregarded.

All the sets A, B, etc. considered are finite, of cardinality $|\cdot|$; one defines the sumset via

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

and similarly the difference, product set, as well as polynomial expressions like $AA-AA$ used herein. If $B = \{b\}$ we just write $A + b$ for $A + \{b\}$. In contrast, the notation A^n denotes the n–fold Cartesian product of A with itself.

The study of the so–called sum–product phenomenon originated in the paper [1] by Erdős and Szemerédi, who conjectured the following.

Conjecture 33 (Sum–product conjecture)**.** *[1] For $\delta < 1$ and any sufficiently large $A \subset \mathbb{Z}$, one has*

$$|A + A| + |AA| \geq |A|^{1+\delta}.$$

Elekes in his foundational paper [2] observed that if the question of Erdős and Szemerédi is asked over a field rather than a ring, then one can use incidence geometry and make good progress on it. Fields, beginning with reals, where Elekes fetched the Szemerédi-Trotter theorem as a powerful tool, have become the structure of choice for variants of Conjecture 33 ever since.

The study of asymptotic sum–product estimates in fields of positive characteristic began in the prime residue field $\mathbb{F}_p$ setting by Bourgain, Katz and Tao [7] where the first qualitative result was established. It was made quantitative by Garaev [33], whose paper was followed by a body of incremental improvements. The new wave of quanti-

tative results was initiated in [9] and [34], based on the point-plane incidence theorem of the first author [9]. Stevens and de Zeeuw [35] derived from it a point–line incidence theorem, which has enabled new applications to sum–product type estimates, in spirit similar to those over the reals, based on the Szemerédi–Trotter theorem, see e.g. [36].

It was shown in [34] that

$$|A \pm A| + |AA| \gg |A|^{6/5}, \quad A \subset \mathbb{F}_p, \quad |A| \leq p^{5/8}. \tag{3.1}$$

Shakan and Shkredov [37], succeeded in improving the (3.1) to $\frac{6}{5}+c$, for a certain $c > 0$. Chen, Kerr and Mohammadi [38] have recently achieved quantitative improvements to the value of c in [37] by largely following its proofs, wherewithin they identified a more optimal way of applying incidence bounds.

Today, after much effort, it appears unlikely that (but for a few exceptions) even weaker versions of Conjecture 33, the central one being the *weak Erdős–Szemerédi conjecture*, discussed in some detail in the real setting in [39], can be fully resolved using the available incidence technology. However, the question how far partial results based thereon can be pushed appears to be, at least on a certain level, interesting. To this effect, the third author and collaborators (see e.g., [8], [40]-[41]) developed a framework of methods, based on linear algebra and combinatorics, which have enabled a steady supply of improvements of the state of the art of sum-product theory. A recent paper [39] claims to have taken advantage of the latter techniques, over the reals, in what may be the best possible way.

In a loose sense, this paper attempts to establish a positive characteristic analog of some results in [39]. In particular, Theorem 34 gives a further improvement of the sum-product inequality, relative to that in [38], replacing the original proof in [37] by an essentially different one. We do not expect to have our sum-product inequality improved further, within the reach of today's methodology. (Admittedly, there are many instances when prognoses along the lines of the latter statement turn out to be false. If so, one can say in retrospect, they were stimulating.)

In addition to the standard sum–product problem, we present Theorem 35 and its implication Theorem 36, which are "threshold–breaking" in a slightly different sense. Theorem 35, or heuristically *few products imply many differences*, appears to be in interesting development, at least in the sense that currently available techniques, in fact, allow for it, apropos of the weak Erdős–Szemerédi conjecture. The statement of Theorem 36 can be viewed as a particular case of an Erdős–type geometric question

about distinct values of bilinear forms on a plane point set, studied in the real setting in, e.g. [23].

We next present the three main inequalities, established here. Say, if $F = \mathbb{F}_p$, these inequalities clearly cannot hold for sets A, comparable in size with p. The proofs of these inequalities rely on incidence results stemming from the point–plane incidence theorem from [9] which in positive characteristic p is constrained in terms of p. It would be highly desirable to have some sort of a generalisation for a finite field $\mathbb{F}_q$, q being a power of p, with a constraint expressed in terms of q but there is no such a generalisation for now.

Since within each proof herein incidence results are used several times, the constraints may look at the first glance *ad hoc*, and one may be tempted to say "for $|A|$ sufficiently small in terms of p" instead.

We use the standard Vinogradov notations $\ll, \gg$ to hide absolute constants in inequalities, $\approx$ means both $\ll$ and $\gg$, and the symbols $\lesssim, \gtrsim$ suppress, in addition to constants, powers of $\log |A|$.

Theorem 34 (Sum–product)**.** *Let* $|AA| = M|A|$, $|A \pm A| = K|A|$, *for* $|A| \subset F^*$. *If* $|A| < p^{18/35}$, *then*

$$\max(K, M) \gtrsim |A|^{2/9} .$$

Moreover, if $K^3 M |A|^3 < p^2$, *then*

$$K^4 M^5 \gtrsim |A|^2 . \qquad (3.2)$$

We remark that using the point–plane incidence bound, one can show [35, Equation 6] that

$$|AA| \ll |A| \quad \Longrightarrow \quad |A + A| \gg |A|^{3/2}.$$

Our next result surpasses this barrier and implies that $|AA| \ll |A|$, then $|A - A| \gg |A|^{3/2+1/24}$.

Theorem 35 (Few products, many differences)**.** *Let* $|AA| = M|A|$, $|A - A| = K|A|$, *for* $|A| \subset F^*$. *If* $M^2 K^2 |A|^3 < p^2$ *or* $|A| < p^{24/49}$, *then*

$$K^{24} M^{36} \gtrsim |A|^{13} . \qquad (3.3)$$

The estimate of Theorem 35 is only better than Theorem 34 for small M. It would be interesting to obtain a similar estimate if K pertained to $A + A$, rather than $A - A$

and even more interesting if a corresponding threshold–breaking statement in the vein of *few products imply many sums* could be established apropos of additive energy of A, see [39] for the real setting.

By following the proofs, it is easy to see that the product set AA can be replaced by the ratio set A/A.

It was proved in [9, Corollary 15], [34, Corollary 4] that

$$|AA - AA| \gg |A|^{3/2}, \quad |A| \leq p^{2/3}. \tag{3.4}$$

Theorem 35 enables one to improve upon (3.4). This can also be viewed as the special case of the general open question, concerning the minimum cardinality of set of values of the symplectic form on pairs of points in a given set in the plane F^2 (here the set being $A \times A$), see [36, Theorem 4] for a general geometric bound. We formulate the next theorem in slightly more generality.

Theorem 36 (Expansion)**.** *Let $A, B, C \subseteq F^*$ be sets of approximately the same size $|A| < p^{4/9}$ and $B \cap C \neq \emptyset$. Then for some positive $c > 0$ one has*

$$|AB - AC| \gtrsim |A|^{3/2+c}.$$

One can take any $c = 1/96$ and $c = 1/56$ if $B = C$.

The powers of $\log |A|$ hidden in the $\gtrsim$ symbols can be easily tracked down, however they are not our concern.

Progress, achieved in this paper, is primarily due to further development of methodology founded by the third author, which enables a close to optimal multiple applications of incidence results (this was initiated in [37, 38]). In particular, this calls for the use of several different energies, or moments of convolution, formally introduced in the next section. Of special importance here is the fourth additive energy $E_4(A)$, owing to the forthcoming Corollary 39 of the Stevens–de–Zeeuw incidence theorem; in the Euclidean setting the same role was played by the third moment $E_3(A)$, owing to the Szemerédi–Trotter theorem. See, in particular, [40, 14, 8, 42] as well as [43] for the general description of the approach, the closely related spectral method, and various applications in the context of the sum–product phenomenon.

3.2 Preliminaries

Let $A, B \subseteq F$ be some finite sets. We use representation function notations like $r_{A-B}(x)$, which counts the number of ways $x \in F$ can be expressed as a difference $a-b$ with $a \in A$, $b \in B$, respectively.

For a real $n > 1$ we define the nth moment of the representation function, or energy (see [8]) as

$$E_n(A, B) = \sum_x r^n_{A-B}(x)\,,$$

writing just $E_n(A)$ when $A = B$.

Owing to the fact that the equation

$$a - b = a' - b' : \qquad a, a' \in A,\ b, b' \in B$$

can be rearranged, one has as well that

$$E_2(A, B) = \sum_x r^2_{A+B}(x)\,.$$

If $n \geq 2$ is integer, then after resummation one has

$$E_n(A) = \sum_{x_1,\ldots,x_{n-1}} |A \cap (A + x_1) \cap \ldots \cap (A + x_{n-1})|^2.$$

This means that if one partitions the set A^n of n-tuples $(a_1, \ldots, a_n)$ into equivalence classes by translation, then E_n is the sum, over equivalence classes $[a_1, \ldots, a_n]$ of squares of the numbers of n-tuples in an equivalence class.

Next we formulate incidence results to be used, in the form most adapted to our purposes. The first one is an adaptation of the first author's point-pane theorem [9].

Theorem 37. *Let $A, B, C \subset F$, with $\max(|A|, |B|, |C|) < \sqrt{|A||B||C|} < p$. Then*

$$|\{(a, b, c, a', b', c') :\ a, a' \in A,\ b, b' \in B,\ c, c' \in C \text{ and } a+bc = a'+b'c'\}| \ll (|A||B||C|)^{3/2}.$$

The second one is a derived statement for point–line incidences due to Stevens and de Zeeuw [35].

Theorem 38. *Let $A, B, C, D \subset F$, with $|A||B||D| < p^2$ or $|A||C||D| < p^2$. Then*

$$|\{(a,b,c,d) \in A \times B \times C \times D : \ c = ab + d\}| \ll \min[\,(|A||B||C|)^{3/4}|D|^{1/2},\, (|A||C||D|)^{3/4}|B|^{1/2}\,] + |A||D| + |B||C|.$$

As to the forthcoming applications of Theorem 38, we refer to the first term in its estimate as the *main term* and the remaining two as *trivial terms*, which in meaningful applications will be dominated by the main term.

Corollary 39. *Let $A \subseteq F^*$, $D \subseteq F$ with $|AA| \leq M|A|$ and $M|A|^2|D| < p^2$. Then*

$$E_4(A,D) := \sum_x r^4_{A-D}(x) \ll \min(M^3|A|^2|D|^2,\, M^2|A||D|^3) \log |A|\,. \tag{3.5}$$

Hence, the number of distinct equivalence classes $[a,b,c,d]$ of quadruples $(a,b,c,d) \in A^4$ by translation is $\gtrsim M^{-2}|A|^4$.

Proof. For $1 \leq k \leq \min(|A|,|D|)$, let

$$n_k := |X_k := \{x \in A - D : \ r_{A-D}(x) \geq k\}|\,.$$

We claim that

$$n_k \ll \min(M^3|A|^2|D|^2,\, M^2|A||D|^3)/k^4 + M|D|/k \ll \min(M^3|A|^2|D|^2/k^4,\, M^2|A||D|^3)/k^4\,, \tag{3.6}$$

the term $M|D|/k$ getting subsumed owing merely to the above range of k.

Estimate (3.5) then follows after dyadic summation in k. To justify (3.6), for each $x \in X_k$ there are $\geq k$ solutions to the equation $x = \alpha - d$, with $\alpha \in A$, $d \in D$. This means, there are $\geq k|A|n_k$ solutions to the equation

$$x = (\alpha/a)a - d = ab - d : \qquad a \in A^{-1}, b \in AA,\, x \in X_k.$$

Estimate (3.6) follows after comparing the above lower bound with the upper bound furnished by Theorem 38 and rearranging.

If we set $D = A$, the number N, of equivalence classes $[a,b,c,d]$ of quadruples $(a,b,c,d) \in A^4$ by translation satisfies, by the Cauchy–Schwarz inequality, the lower bound

$$N \geq |A|^8/E_4(A) \gtrsim M^{-2}|A|^4. \tag{3.7}$$

□

3.3 Proof of Theorem 34

The presented proofs involving the sum and difference sets are somewhat different, the difference set case being easier. We therefore present them separately, beginning with the difference set, despite the proof involving the sumset applies to the different set as well, in essence by replacing the truism (3.15) therein with (3.8) below.

Difference–product inequality. Let $P \subseteq A - A$ be a set of popular differences, defined as follows: for every $x \in P$, $r_{A-A}(x) \geq \frac{|A|}{2K}$. The notions of popularity, as well as the accompanying notations P, Δ, etc. vary from one proof to another.

We further say that P is popular *by mass*, meaning that, by the pigeonhole principle,

$$|\{(a_1, a_2) \in A \times A;\, a_1 - a_2 \in P\}| \gg |A|^2.$$

Consider the equation

$$c - b = (a - b) - (a - c) = (d - b) - (d - c). \tag{3.8}$$

Suppose, $x := a - b$ and $y := d - b$ are in P. Besides, $u := a - c$, $v := d - c$ are both in $A - A$. By definition of P, equation (3.8) has $\gg |A|^4$ solutions (a, b, c, d).

Clearly, equation (3.8) is translation-invariant, and an equivalence class $[a, b, c, d]$ by translation is fixed by the values of three of the five variables defined above, namely x, y, u, v, as well as $w := c - b$. Each equivalence class provides a distinct solution of the system of equations

$$x, y \in P,\, u, v, w \in A - A :\, x - u = y - v = w.$$

It follows by the Cauchy–Schwarz inequality and Corollary 39 that

$$|A|^4 \lesssim \sqrt{E_4(A)}\sqrt{|\{x, y \in P; u, v \in A - A :\, x - u = y - v \in A - A\}|} \;:=\; M|A|^2\sqrt{X}. \tag{3.9}$$

To bound the quantity X, we use popularity of the differences x, y and dyadic locali-

sation. Namely, for some $\Delta \geq 1$ and some $D \subseteq A-(A-A)$ one has

$$\begin{aligned} X &\ll \frac{K^2}{|A|^2}|\{a_1,a_2,a_3,a_4 \in A;\ u,v \in A-A:\ a_1-(a_3-u)=a_2-(a_4-v) \in A-A\}| \\ &\lesssim \frac{K^2}{|A|^2}\Delta^2|\{a_1,a_2 \in A, d_1,d_2 \in D \subseteq A-(A-A):\ a_1-d_1=a_2-d_2 \in A-A\}| \\ &\leq \frac{K^2}{|A|^2}\Delta^2 \sum_{w \in A-A} r_{A-D}(w)^2 \leq \frac{K^{5/2}}{|A|^{3/2}}\Delta^2 \left(\sum_w r_{A-D}(w)^4\right)^{1/2} = \frac{K^{5/2}}{|A|^{3/2}}\sqrt{E_4(A,D)}\,, \end{aligned} \tag{3.10}$$

where the last inequality is an application of Cauchy-Schwarz[1].

The above "popular" set $D \subseteq A-(A-A)$ is defined via $r_{A+(A-A)}(d) \approx \Delta$, $\forall d \in D$. (The brackets in the subscript of the notation $r_{A+(A-A)}(d)$ mean that this is the number of representations of d as the sum $d=a+x$, with $a \in A$ and $x \in A-A$, rather than $x=a+a'+a''$, with $a,a',a'' \in A$.)

We now apply Corollary 39, whose constraint in terms of p will be satisfied either under assumption $K,M < |A|^{2/9}$ or by the assumption $K^3M|A|^3 < p^2$, owing both cases to the Plünnecke's inequality $A-(A-A) \leq K^3|A|$ (see e.g. [3, Section 6.5]).

This enables one to continue the series of estimates (3.10) as

$$\begin{aligned} X &\lesssim M^{3/2}\frac{K^{5/2}}{|A|^{1/2}}M^{3/2}(|D|\Delta^2) \\ &\leq M^{3/2}\frac{K^{5/2}}{|A|^{1/2}}M^{3/2}E^+(A,A-A) \ll K^4M^3|A|^2\,, \end{aligned} \tag{3.11}$$

where the last estimate has invoked Theorem 37. Namely

$$\begin{aligned} E_2(A,A-A) &= |\{(a_1,a_2,d_1,d_2) \in A^2 \times (A-A)^2:\ a_1-d_1=a_2-d_2\}| \\ &\leq |A|^{-2}|\{(a,a',d_1,d_2,b_1,b_2) \in A^2 \times (A-A)^2 \times AA^2:\ b_1/a-d_1=b_2/a'-d_2\}| \\ &\ll M^{3/2}K^{3/2}|A|^{5/2}\,. \end{aligned}$$

Checking that conditions of Theorem 37 have been satisfied by the assumptions on $|A|,K,M$ is straightforward, for the converse of inequality (3.2) implies $KM < |A|^{1/2}$.

[1]Here, as well as further in (3.18) it is possible, on the technical level, to estimate $\sum_{w \in A-A} r_{A-D}(w)^2$ in a slightly different way along the lines of the (fairly standard) argument presented between estimates (3.21) and (3.23) in the forthcoming proof of Theorem 35. Although that would save a factor $\log|A|$, contributed by $E_4(A,D)$, we chose to do it here in a more streamlined way via Corollary 39.

Putting it together yields

$$K^4 M^5 \gtrsim |A|^2 \quad \Rightarrow \quad \max(K, M) \gtrsim |A|^{2/9} \,,$$

concluding the proof of the difference-product inequality of Theorem 34.

□

Sum–product inequality. Let $|AA| \leq M|A|$, $|A + A| \leq K|A|$. We write the input conditions as inequalities, for further we will pass to a large subset of A.

Let P be a set of popular sums, defined as follows.

$$P = P(A) := \left\{ x \in A + A : \, r_{A+A}(x) \geq \epsilon \frac{|A|}{K} \right\}, \tag{3.12}$$

for a small $\epsilon > 0$, to be later chosen as $\sim \log^{-1} |A|$. This choice of the popular set is to be justified shortly.

By the pigeonhole principle

$$|\{(a, a') \in A \times A : \, a + a' \in P\}| \geq (1 - \epsilon)|A|^2 \,.$$

Furthermore, let $A' \subseteq A$ be

$$A' = A'(A) := \{a' \in A : |\{a'' \in A : a' + a'' \in P(A)\}| \geq \frac{2}{3}|A|\} \,, \tag{3.13}$$

so $|A'| \geq (1 - 3\epsilon)|A|$. Indeed, the total mass $\sum_{x \in P} r_{A+A}(x) \geq (1 - \epsilon)|A|^2$. Consider the set of some $c|A|$ poorest abscissae, such that for each such abscissa a' there are at most $\frac{2}{3}|A|$ distinct $a'' \in A$: $a' + a'' \in P$, get the upper bund on c. The above set of poorest abscissae supports mass at most $\frac{2}{3}c|A|^2$, while its complement can support mass at most $(1 - c)|A|^2$. Adding the latter two upper bounds yields a contradiction with the lower bound $\sum_{x \in P} r_{A+A}(x) \geq (1 - \epsilon)|A|^2$ if $c > 3\epsilon$.

Let $P' \subseteq A' - A'$ be popular by energy $E_{4/3}(A')$. Namely $x \in P'$ if for some $\Delta' \geq 1$, $\Delta' \leq r_{A'-A'}(x) < 2\Delta'$, and and

$$E_{4/3}(A') := \sum_{x \in A'-A'} r_{A'-A'}(x)^{4/3} \gtrsim |P'|\Delta'^{4/3}.$$

The reason why we deal with the additive energy $E_{4/3}(A')$ will be clear from the sequel, as well as the raison d'être of the following lemma.

Lemma 40. *There exists $B \subseteq A$, with $|B| \gg |A|$, such that $E_{4/3}(B'(B)) \gg E_{4/3}(B)$, where $B' \subseteq B$ is defined relative to B replacing A in conditions* (3.12), (3.13).

Proof. Reset 3ϵ as ϵ, suppose for contradiction that, say $E_{4/3}(A'(A)) < E_{4/3}(A)/10$, i.e. at least 90 per cent of the energy is supported on a thin subset $A \setminus A'$, of cardinality $|A \setminus A'| < \epsilon |A|$. Throw away the latter subset from A, redefine what remains as A, with A' being redefined accordingly via (3.13), and attempt to repeat the procedure some ϵ^{-1} times. If this was possible, then in the end of it one is left with a subset A_ϵ of A of cardinality $|A_\epsilon| \geq (1-\epsilon)^{\epsilon^{-1}} |A| \gg |A|$, with $E_{4/3}(A_\epsilon) < 10^{-\epsilon^{-1}} E_{4/3}(A)$. Choosing $\epsilon = \log^{-1} |A|$ is clearly a contradiction, for trivially $E_{4/3}(A_\epsilon) \geq |A_\epsilon|^2 \gg |A|^2$.

□

For the rest of the proof of the sum-product estimate, without loss of generality we take $B = A$, in other words assuming that

$$E_{4/3}(A') \gg E_{4/3}(A)\,, \qquad (3.14)$$

to be used in the end of the proof. We also set $\epsilon = \log^{-1} |A|$ in (3.12), (3.13).

Consider now a variant of equation (3.8) as follows:

$$-c+b = (a+b)-(a+c) = (d+b)-(d+c)\,. \qquad (3.15)$$

Let us make popularity assumptions as to the variables a, b, c, d. By definition of the sets A' and P', it follows that the number of solutions $:= \sigma$ of equation (3.15), when the difference $b - c \in P'$ and *all* the four sums $x := a+b$, $y := a+c$, $u := d+c$ and $v := d+b$ involved are in P is bounded from below as

$$\sigma \gg |P'| \Delta |A|^2. \qquad (3.16)$$

Next we obtain the upper bound for the number of solutions (a, b, c, d) of equation (3.15) under the constraints above. Equation (3.15) is invariant to a simultaneous shift of b, c by some t and a, d simultaneously by $-t$. We say $[a, b, c, d]$ is equivalent to $[a', b', c', d']$ if

$$(a, b, c, d) = (a', b', c', d') + (t, -t, -t, t).$$

Each equivalence class $[a, b, c, d]$ yields a different solution of the system of equations

$$x, y, u, v \in P,\ w \in P' :\ x - y = v - u = w.$$

If $r([a,b,c,d])$ denotes the number of quadruples (a,b,c,d) in an equivalence class, then

$$\sum_{[a,d,c,d]} r^2([a,b,c,d]) = \sum_{x\in A-A} r^2_{A-A}(x) r^2_{A-A}(-x) = E_4(A).$$

An upper bound for the quantity σ – similar to estimate (3.9) – now follows by the Cauchy–Schwarz inequality. Invoking also the lower bound (3.16) yields

$$|A|^2|P'|\Delta' \lesssim \sqrt{E_4(A)}\sqrt{|\{x,y,u,v\in P,\, w\in P' :\, x-y=v-u=w\}|}\,. \qquad (3.17)$$

Popularity of the sums x,y,u,v together with Corollary 39 to bound $E_4(A)$ yield

$$|A|^2|P'|\Delta' \lesssim MK^2\sqrt{|\{a_1,\dots,a_8\in A :\, a_1+a_2-a_3-a_4=a_5+a_6-a_7-a_8\in P'\}|}\,.$$

We proceed similar to estimates (3.10): there exists a popular subset $D\subseteq A+A-A$ where $\forall d\in D$, $r_{A+A-A}(d)\approx\Delta$, for some $\Delta\geq 1$ (here, contrary to the difference set case $r_{A+A-A}(d)$ means the number of representations $d=a+a'-a''$, with $a,a',a''\in A$), such that one gets

$$\begin{aligned} |A|^2|P'|\Delta' &\lesssim MK^2\Delta\sqrt{|\{a_1,a_2\in A,\ d_1,d_2\in D\subseteq A+A-A :\, a_1-d_1=a_2-d_2\in P'\}|} \\ &\leq MK^2\Delta|P'|^{1/4}E_4^{1/4}(A,D)\,, \end{aligned} \qquad (3.18)$$

after another use of the Cauchy-Schwarz inequality.

Using Corollary 39 to estimate $E_4(A,D)$ – its applicability in terms of the constraints in terms of p being the same as it was in the difference set case, see the argument following (3.10) – we conclude that

$$|P'|^{3/4}\Delta' \lesssim M^{7/4}K^2|A|^{-3/2}(|D|\Delta^2)^{1/2} \leq M^{7/4}K^2|A|^{-3/2}\sqrt{T_3(A)}, \qquad (3.19)$$

where

$$T_3(A) := |\{(a_1,\dots,a_3')\in A^6 :\, a_1+a_2+a_3=a_1'+a_2'+a_3'\}|\,.$$

The quantity $T_3(A)$ can be bounded as follows. One can localise $a_2-a_3=x$, $a_2'-a_3'=x'$ to some popular set $D_1\subset A-A$ with $r_{A-A}(x)\approx\Delta_1$, $\forall x\in D_1$ and apply Theorem 37,

so

$$T_3(A) \lesssim M^{3/2}|A|(|D_1|^{3/2}\Delta_1^2) \leq M^{3/2}|A|(E_{4/3}(A))^{3/2}\,. \tag{3.20}$$

It is easy to verify that the assumptions on $|A|, K, M$ ensure that the conditions of Theorem 37 have been amply satisfied.

It follows by definition of the popular set P' after substituting bound (3.20) into (3.19) that

$$(E_{4/3}(A'))^{3/4} \lesssim |P'|^{3/4}\Delta' \lesssim M^{5/2}K^2|A|^{-1}(E_{4/3}(A))^{3/4}.$$

Hence, by (3.14), one cancel $E_{4/3}(A') \gg E_{4/3}(A)$ and be left with

$$|A| \lesssim M^{5/2}K^2\,,$$

which proves Theorem 34.

□

3.4 Proof of Theorem 35

Return to relations (3.8), (3.9), with the notations x, y, u, v, w as they were introduced apropos of (3.8), (3.9), and observe that $u - v = a - d := z \in A - A$. Suppose that z is popular my mass (i.e with say $r_{A-A}(z) \geq \frac{|A|}{10K}$) and so are x and y, set $P \subseteq A - A$ in this section again denote the set of such popular differences.

From (3.9) we have

$$u = x - w, \qquad v = y - w \qquad \Leftrightarrow \qquad u, v \;\in\; (A-A) \cap (P - w) \;:= \P_w.$$

We can now rewrite (3.9) as

$$|A|^4 \lesssim M|A|^2 \sqrt{\sum_{w \in A-A} |\{u, v \in P_w :\; u - v \in P\}|} := M|A|^2\sqrt{X}. \tag{3.21}$$

Let us estimate $|P_w|$, sorting $A - A = \{w_1, \dots, w_{A-A}\}$ in non-decreasing order by the value of $r_{P-(A-A)}(w)$.

Set

$$n_k := |W_k := \{w \in P - (A - A) :\; r_{P-(A-A)}(w) \geq k\}|.$$

This means, for every $w \in W_k$ the equation $w = x - u : x \in P, u \in A - A$ has $\geq k$ solutions. Hence, the equation

$$w = t/a - u : w \in W_k, t \in AP, u \in A - A, a \in A$$

has $\geq k|A|n_k$ solutions. Furthermore, $AP \subseteq AA - AA$, and $\forall\, t \in AP$, $r_{AA-AA}(t) \gg |A|/K$. It follows that

$$|AP| \ll M^2 K|A|\,. \tag{3.22}$$

Apply Theorem 38 to get the upper bound for the number of solutions of the latter equation. Note that the p-condition of Theorem 38 becomes $p^2 > M^2K^2|A|^3$, which is satisfied, in particular, for if $|A| < p^{24/49}$, when assuming $K^{24}M^{36} < |A|^{13}$ (or there is nothing to prove) implies that $M^2K^2 < |A|^{13/12}$.

Hence, one concludes that

$$k|A|n_k \ll M(K|A|)^{1/2}(|A|n_k)^{3/4}(K|A|)^{3/4} + M^2K^2|A|^2\,.$$

Rearranging, dropping the second term since it follows by definition of n_k that $k \leq K|A|$, yields

$$n_k \ll M^4K^5|A|^4/k^4\,.$$

Inverting the latter bound yields

$$k_n \ll MK^{5/4}|A|n^{-1/4}\,,$$

which means that for $w = w_n$ on the list, one has

$$|P_{w_n}| \ll \min(|A - A|,\, MK^{5/4}|A|n^{-1/4})\,. \tag{3.23}$$

Furthermore, given w, by another application of Theorem 38 (the p-condition check being the same as done above) one has

$$\begin{aligned} |\{u, v \in P_w : u - v = z \in P\}| &\ll \frac{1}{|A|}\{u, v \in P_w : u - v = t/a, \text{ with } a \in A,\, t \in AP\}| \\ &\ll |A|^{-1}(|P_w|^{3/2}(M^2K|A|)^{1/2}|A|^{3/4} + M^2K|A||P_w|) \\ &\ll MK^{1/2}|A|^{1/4}|P_w|^{3/2} + M^2K^2|A|\,, \end{aligned} \tag{3.24}$$

where in the last term the trivial bound $|P_w| \leq K|A|$ has been used.

It follows from (3.23) that

$$\sum_{w\in A-A}|P_w|^{3/2}\ll M^{3/2}K^{15/8}|A|^{3/2}\sum_{n=1}^{|A-A|}n^{-3/8}\ll M^{3/2}K^{5/2}|A|^{17/8}\,.$$

Substituting the latter bound into (3.24) one sees that the quantity X introduced in (3.21) obeys

$$X\ll M^{5/2}K^3|A|^{19/8}+M^2K^3|A|^2\ll M^{5/2}K^3|A|^{19/8}\,. \qquad (3.25)$$

It follows from (3.21) that

$$|A|^{13}\lesssim M^{36}K^{24}\,,$$

as claimed by Theorem 35.

3.5 Proof of Theorem 36

Proof. We give two approaches, the first one allowing for better quantitative estimates, the second one being more general. It is easy to check that the proof holds if, e.g., $|A|<p^{4/9}$.

Set $s=|AB-AC|$, $M=|AB|$. Applying Theorem 37, one has, for $M|A|^3<p^2$ (see details in [34, Corollary 4]) that

$$|AB-AC|\gg M^{1/2}|A|^{3/2}\,.$$

Otherwise, since there $B\cap C\neq\emptyset$, one has $|AB-AC|\geq|A-A|=K|A|$. The proof of Theorem 35 allows for replacing the product set AA with AB, with $|B|\approx|A|$, the same concerning inequality (3.3). I.e., with $|AB|=M|A|$, one has

$$|A|^{13}\lesssim M^{36}K^{24}\leq(s^2/|A|^3)^{36}(s/|A|)^{24}=s^{96}|A|^{-132}$$

or, in other words, $s\gtrsim|A|^{145/96}$. In the special case $B=C$, we can estimate size of $|AP|$ in (3.22) as s. It gives us $n_k\ll s^2|A|^2K^3/k^4$, further the main term in (3.25) is $K^{7/4}|A|^{9/8}s^{5/4}$. Thus the second term in (3.24) is negligible again. Hence

$$|A|^4\lesssim M^2K^{7/4}|A|^{9/8}s^{5/4}\leq(s^2/|A|^3)^2(s/|A|)^{7/4}|A|^{9/8}s^{5/4}=s^7|A|^{-53/8}$$

or, in other words, $s \gtrsim |A|^{85/56}$.

Alternatively, we present an argument, which uses the Balog–Szemerédi–Gowers Theorem, see e.g. [3, Section 2.5], which has more potential for generalisation. Set $\sigma := \sum_x r^2_{AB-AC}(x)$. By the Cauchy-Schwarz inequality

$$|A|^8 \leq s\sigma \, .$$

Write $s = N|A|^{3/2}$, for some N. Then $\sigma \geq |A|^{13/2}/N$. By [42, Theorem 32, Remark 33], one has the following estimate, provided that $K|A|^3 < p$:

$$\sigma \lesssim |A|^5 (E_2^{\times}(A,B))^{1/2} \, .$$

where $E_2^{\times}$ is multiplicative energy, defined in the standard way. Thus $E_2^{\times}(A) \gtrsim |A|^3/N^2$.

Using the Balog–Szemerédi–Gowers Theorem [3], one finds $A' \subseteq A$ such that $|A'| \gtrsim_N |A|$ and $|A'A'| \lesssim_N |A'|$, the symbols $\gtrsim_N$, $\lesssim_N$ absorbing universal powers of N.

Applying Theorem 34 to the set A' (it's easy to see that its conditions are satisfied) yields

$$|AB - AC| \geq |A' - A'| \gtrsim |A'|^{37/24} \gtrsim_N |A|^{37/24} \, ,$$

as required. □

REFERENCES

[1] P. Erdős and E. Szemerédi, "On sums and products of integers," *Birkhauser, Basel*, vol. 66, pp. 213–218, 1983.

[2] G. Elekes, "On the number of sums and products," *Acta Arith.*, vol. 81, pp. 365–367, 1997.

[3] T. Tao and V. Vu, *Additive combinatorics*. Cambridge University Press, 2006.

[4] M.-C. Chang, "The Erdős–Szemerédi problem on sum set and product set," *J. Amer. Math. Soc*, vol. 17 (2), pp. 472–497, 2004.

[5] S. Konyagin and I. Shkredov, "On sum sets of sets," *SIAM J. Discrete Mathematics*, vol. 290, pp. 288–299, 2015.

[6] I. Shkredov, "On sums of szemerédi–trotter sets," *Proc. Steklov Inst. Math.*, vol. 289 (1), pp. 300–309, 2015.

[7] J. Bourgain, N. Katz, and T. Tao, "A sum–product estimate in finite fields, and applications," *Geom. Funct. Anal.*, vol. 14, pp. 27–57, 2004.

[8] T. Schoen and I. Shkredov, "On sumsets of convex sets," *Comb. Probab. Comput.*, vol. 20, pp. 793–798, 2011.

[9] M. Rudnev, "On the number of incidences between planes and points in three dimensions," *Combinatorica*, vol. 38 (1), pp. 219–254, 2018.

[10] M. Nathanson, "On sums and products of integers," *Acta Arith.*, vol. 125, pp. 9–16, 1997.

[11] K. Ford, "Sums and products from a finite set of real numbers," *Ramanujan J.*, vol. 2, pp. 59–66, 1998.

[12] J. Solymosi, "on the number of sums and products," *Bull. Lond. Math. Soc.*, vol. 37 (4), pp. 491–494, 2005.

[13] J. Solymosi, "Bounding multiplicative energy by the sumset," *Adv. Math.*, vol. 222 (2), pp. 402–408, 2009.

[14] I. Shkredov, "Some new results on higher energies," *Transactions of MMS*, vol. 74 (1), pp. 35–73, 2013.

[15] S. Konyagin and I. Shkredov, "New results on sum–products in r," *Transactions of Steklov Mathematical Institute*, vol. 294, pp. 87–98, 2016.

[16] M. Rudnev, I. Shkredov, and S. Stevens, "On an energy variant of the sum–product conjecture," 2016, preprint, arXiv: 1607.05053.

[17] A. Balog and T. Wooley, "A low–energy decomposition theorem," *Q. J. Math.*, vol. 68 (1), pp. 207–226, 2017.

[18] B. Hanson, "Estimates for character sums with various convolutions," 2015, preprint, arXiv:1509.04354.

[19] B. Murphy, O. Roche-Newton, and I. Shkredov, "Variations of the sum–product problem," 2014, preprint, arXiv: 1312.6438.

[20] I. Shkredov, "Some remarks on the balog–wooley decomposition theorem and quantities $D^+, D^\times$," *Proc. Steklov Inst. Math.*, 2018, accepted arXiv:1605.00266.

[21] S. Konyagin and M. Rudnev, "On new sum–product type estimates," *SIAM J. Discrete Mathematics*, vol. 27 (2), pp. 973–990, 2013.

[22] A. Balog and O. Roche-Newton, "New sum–product estimates for real and complex numbers," *Comput. Geom.*, vol. 53 (4), pp. 825–846, 2015.

[23] A. Iosevich, O. Roche-Newton, and M. Rudnev, "On discrete values of bilinear forms," 2015, to appear in Sbornik: Math., arXiv: 1512.02670.

[24] I. Shkredov, "On a question of a. balog," 2015, preprint, arXiv: 1501:07498.

[25] O. Roche-Newton, I. Ruzsa, C. Shen, and I. Shkredov, "On the size of the set $AA + A$," 2018, preprint, arXiv: 1801.1043.

[26] J. Bourgain and M.-C. Chang, "On the size of k–fold sum and product sets of integers," *J. Amer. Math. Soc*, vol. 17 (2), pp. 472–497, 2004.

[27] E. Croot and D. Hart, "h–fold sums from a set with few products," *SIAM J. Discrete Math.*, vol. 24, pp. 505–519, 2010.

[28] G. Elekes and I. Ruzsa, "Few sums, many products," *Studia Sci. Math. Hungar.*, vol. 40 (3), pp. 301–308, 2003.

[29] N. Katz and P. Koester, "On additive doubling and energy," *SIAM J. on Discrete Mathematics*, vol. 24, pp. 1684–1693, 2010.

[30] L. Li and O. Roche-Newton, "Convexity and a sum–product estimate," *Acta Arith.*, vol. 156, pp. 247–255, 2012.

[31] A. Sheffer, "Konyagain–Shkredov sum–product bound," 2016, blog Post, https://adamsheffer.files.wordpress.com/2016/07/ks-sp.pdf.

[32] G. Shakan, "Konyagin–shkredov clustering," 2018, blog Post, https://gshakan.wordpress.com/konyagin-shkredov-clustering/.

[33] M. Garaev, "An explicit sum–product estimate in $\mathbb{F}_p$," *Intern. Math. Res. Notices*, vol. 11, pp. 1–11, 2007.

[34] O. Roche-Newton, M. Rudnev, and I. Shkredov, "An explicit sum–product estimate in $\mathbb{F}_p$," *Adv. Math.*, vol. 293, pp. 589–605, 2016.

[35] S. Stevens and F. D. Zeeuw, "An improved point–line incidence bound over arbitrary fields," *Bull. London Math. Soc.*, vol. 49, pp. 842–858, 2017.

[36] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, and I. D. Shkredov, "New results on sum–product type growth over fields," 2007, preprint, arXiv: 1712.0041.

[37] G. Shakan and I. Shkredov, "Breaking the 6/5 threshold for sums and products modulo a prime," 2018, unpublished, arXiv:1803.04637.

[38] C. Chen, B. Kerr, and A. Mohammadi, "A new sum–product estimate in prime fields," 2018, preprint, arXiv:1807.10998.

[39] B. Murphy, M. Rudnev, I. Shkredov, and Y. Shteinikov, "On the few products, many sums problem," 2017, preprint, arXiv: 1712.0041.

[40] I. Shkredov, "Some new inequalities in additive combinatorics," *MJCNT*, vol. 3 (2), pp. 237–268, 2013.

[41] I. Shkredov, "Energies and structure of additive sets," *Electronic Journal of Combinatorics*, vol. 21 (3), pp. 1–53, 2014.

[42] I. Shkredov, "On asymptotic formulae in some sum–product questions," 2018, preprint, arXiv:1802.09066.

[43] G. Shakan, "On higher energy decomposition and the sum–product phenomenon," 2018, accepted to Math. Proc. Cambridge Philos. Soc., arXiv:1803.04637.